Open Source Used In Duo (Free to Beyond) - AuthProxy 5.8.2

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: 78EE117C99-1724340873

This document contains licenses and notices for open source software used in this product. With respect to the free/open source software listed in this document, if you have any questions or wish to receive a copy of any source code to which you may be entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please submit this form.

In your requests please include the following reference number 78EE117C99-1724340873

Contents

1.1 openssl 1.0.2zd

1.1.1 Notifications :

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

1.1.2 Available under license :

```
#!/usr/bin/env perl

# ====================================================================
# Written by Andy Polyakov <appro@openssl.org> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
#
# Specific modes and adaptation for Linux kernel by Ard Biesheuvel
# <ard.biesheuvel@linaro.org>. Permission to use under GPL terms is
# granted.
# ====================================================================

# Bit-sliced AES for ARM NEON
#
# February 2012.
#
# This implementation is direct adaptation of bsaes-x86_64 module for
# ARM NEON. Except that this module is endian-neutral [in sense that
# it can be compiled for either endianness] by courtesy of vld1.8's
# neutrality. Initial version doesn't implement interface to OpenSSL,
# only low-level primitives and unsupported entry points, just enough
# to collect performance results, which for Cortex-A8 core are:
#
# encrypt 19.5 cycles per byte processed with 128-bit key
# decrypt 22.1 cycles per byte processed with 128-bit key
# key conv. 440  cycles per 128-bit key/0.18 of 8x block
#
# Snapdragon S4 encrypts byte in 17.6 cycles and decrypts in 19.7,
# which is [much] worse than anticipated (for further details see
# http://www.openssl.org/~appro/Snapdragon-S4.html).
#
# Cortex-A15 manages in 14.2/16.1 cycles [when integer-only code
# manages in 20.0 cycles].
#
# When comparing to x86_64 results keep in mind that NEON unit is
# [mostly] single-issue and thus can't [fully] benefit from
# instruction-level parallelism. And when comparing to aes-armv4
# results keep in mind key schedule conversion overhead (see
# bsaes-x86_64.pl for further details)...
#
#	<appro@openssl.org>

# April-August 2013
#
# Add CBC, CTR and XTS subroutines, adapt for kernel use.
#
#	<ard.biesheuvel@linaro.org>
```

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an DES implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with MIT's libdes.

This library is free for commercial and non-commercial use as long as
the following conditions are aheared to. The following conditions
apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution
as the author of that the SSL library. This can be in the form of a textual
message at program startup or in documentation (online or textual) provided
with the package.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the copyright

notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The license and distribution terms for any publically available version or
derivative of this code cannot be changed. i.e. this code cannot simply be
copied and put under another distrubution license
[including the GNU Public License.]

The reason behind this being stated in this direct manner is past
experience in code simply being copied and the attribution removed
from it and then being distributed as part of other packages. This
implementation was a non-trivial and unpaid effort.

LICENSE ISSUES
==============

The OpenSSL toolkit stays under a double license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

OpenSSL License

/* ==
* Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:

```
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
```

* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an Blowfish implementation written
by Eric Young (eay@cryptsoft.com).

This library is free for commercial and non-commercial use as long as
the following conditions are aheared to. The following conditions
apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
  must display the following acknowledgement:
  This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distrubution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

1.2 packaging 20.1

1.2.1 Available under license :

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You

institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

1.3 zope-interface 5.4.0

1.3.1 Available under license :

3. Names of the copyright holders must not be used to endorse or promote
products derived from this software without prior written permission from the
copyright holders.

4. The right to distribute this software or to use it for any purpose does not
give you the right to use Servicemarks (sm) or Trademarks (tm) of the
copyright
holders. Use of them is covered by separate agreement with the copyright
holders.

5. If any files are modified, you must cause the modified files to carry
prominent notices stating that you changed the files and the date of any
change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Zope Foundation and Contributors

1.4 psutil 5.7.2

1.4.1 Available under license :

BSD 3-Clause License

Copyright (c) 2009, Jay Loden, Dave Daeschler, Giampaolo Rodola'
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this
  list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

1.5 incremental 21.3.0

1.5.1 Available under license :

Incremental

This project includes code from the Twisted Project, which is licensed as below.

Copyright (c) 2001-2015
Allen Short
Amber Hawkie Brown
Andrew Bennetts
Andy Gayton
Antoine Pitrou
Apple Computer, Inc.
Ashwini Oruganti
Benjamin Bruheim
Bob Ippolito
Canonical Limited
Christopher Armstrong
David Reid
Divmod Inc.
Donovan Preston
Eric Mangold
Eyal Lotem
Google Inc.
Hybrid Logic Ltd.
Hynek Schlawack
Itamar Turner-Trauring
James Knight
Jason A. Mobarak
Jean-Paul Calderone

Jessica McKellar
Jonathan D. Simms
Jonathan Jacobs
Jonathan Lange
Julian Berman
Jrgen Hermann
Kevin Horn
Kevin Turner
Laurens Van Houtven
Mary Gardiner
Massachusetts Institute of Technology
Matthew Lefkowitz
Moshe Zadka
Paul Swartz
Pavel Pergamenshchik
Rackspace, US Inc.
Ralph Meijer
Richard Wall
Sean Riley
Software Freedom Conservancy
Tavendo GmbH
Thijs Triemstra
Thomas Herve
Timothy Allen
Tom Prince
Travis B. Hartwell

1.6 cryptography 2.7

1.6.1 Available under license :

incorporates Python 2.7.12 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 2.7.12.

4. PSF is making Python 2.7.12 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 2.7.12 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 2.7.12 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 2.7.12, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python 2.7.12, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Apache License
Version 2.0, January 2004
https://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes
of this License, Derivative Works shall not include works that remain
separable from, or merely link (or bind by name) to the interfaces of,
the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including
the original version of the Work and any modifications or additions
to that Work or Derivative Works thereof, that is intentionally
submitted to Licensor for inclusion in the Work by the copyright owner
or by an individual or Legal Entity authorized to submit on behalf of
the copyright owner. For the purposes of this definition, "submitted"
means any form of electronic, verbal, or written communication sent
to the Licensor or its representatives, including but not limited to
communication on electronic mailing lists, source code control systems,
and issue tracking systems that are managed by, or on behalf of, the
Licensor for the purpose of discussing and improving the Work, but
excluding communication that is conspicuously marked or otherwise
designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity
on behalf of whom a Contribution has been received by Licensor and
subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
this License, each Contributor hereby grants to You a perpetual,
worldwide, non-exclusive, no-charge, royalty-free, irrevocable

copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

https://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This software is made available under the terms of *either* of the licenses found in LICENSE.APACHE or LICENSE.BSD. Contributions to cryptography are made under the terms of *both* these licenses.

The code used in the OpenSSL locking callback and OS random engine is derived from CPython, and is licensed under the terms of the PSF License Agreement.

1.7 attrs 19.3.0

1.7.1 Available under license :

The MIT License (MIT)

Copyright (c) 2015 Hynek Schlawack

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.8 cffi 1.14.1

1.8.1 Available under license :

Except when otherwise stated (look for LICENSE files in directories or information at the beginning of each file) all software and documentation is licensed as follows:

The MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL

THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.9 dpkt 1.9.2

1.9.1 Available under license :

Copyright (c) 2004 Dug Song <dugsong@monkey.org>
All rights reserved, all wrongs reversed.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors and copyright holders may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.10 openssl-fips 2.0.16

1.10.1 Available under license :

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2001 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/uid.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/o_time.h

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2004 The OpenSSL Project.  All rights reserved
* according to the OpenSSL license [found in ../../LICENSE].
* ====================================================================
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/sha512.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/sha256.c

No license file was found, but licenses were detected in source scan.

```
#!/usr/bin/env perl

# ====================================================================
# Written by Andy Polyakov <appro@fy.chalmers.se> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================

# I let hardware handle unaligned input(*), except on page boundaries
# (see below for details). Otherwise straightforward implementation
# with X vector in register bank. The module is big-endian [which is
# not big deal as there're no little-endian targets left around].
#
# (*) this means that this module is inappropriate for PPC403? Does
#     anybody know if pre-POWER3 can sustain unaligned load?

#    -m64 -m32
# ----------------------------------
# PPC970,gcc-4.0.0 +76% +59%
# Power6,xlc-7  +68% +33%

$flavour = shift;

if ($flavour =~ /64/) {
 $SIZE_T =8;
 $LRSAVE =2*$SIZE_T;
 $UCMP ="cmpld";
 $STU ="stdu";
 $POP ="ld";
 $PUSH ="std";
} elsif ($flavour =~ /32/) {
 $SIZE_T =4;
 $LRSAVE =$SIZE_T;
 $UCMP ="cmplw";
 $STU ="stwu";
 $POP ="lwz";
 $PUSH ="stw";
} else { die "nonsense $flavour"; }

$0 =~ m/(.*[\/\\])[^\/\\]+$/; $dir=$1;
( $xlate="${dir}ppc-xlate.pl" and -f $xlate ) or
( $xlate="${dir}../../perlasm/ppc-xlate.pl" and -f $xlate) or
die "can't locate ppc-xlate.pl";

open STDOUT,"| $^X $xlate $flavour ".shift || die "can't call $xlate: $!";

$FRAME=24*$SIZE_T+64;
$LOCALS=6*$SIZE_T;

$K  ="r0";
$sp ="r1";
$toc="r2";
$ctx="r3";
$inp="r4";
$num="r5";
$t0 ="r15";
$t1 ="r6";

$A  ="r7";
$B  ="r8";
$C  ="r9";
$D  ="r10";
$E  ="r11";
$T  ="r12";

@V=($A,$B,$C,$D,$E,$T);
@X=("r16","r17","r18","r19","r20","r21","r22","r23",
   "r24","r25","r26","r27","r28","r29","r30","r31");

sub BODY_00_19 {
my ($i,$a,$b,$c,$d,$e,$f)=@_;
my $j=$i+1;
$code.=<<___ if ($i==0);
 lwz @X[$i],`$i*4`($inp)
___
$code.=<<___ if ($i<15);
```

```
 lwz @X[$j],`$j*4`($inp)
 add $f,$K,$e
 rotlwi $e,$a,5
 add $f,$f,@X[$i]
 and $t0,$c,$b
 add $f,$f,$e
 andc $t1,$d,$b
 rotlwi $b,$b,30
 or $t0,$t0,$t1
 add $f,$f,$t0
___
$code.=<<___ if ($i>=15);
 add $f,$K,$e
 rotlwi $e,$a,5
 xor @X[$j%16],@X[$j%16],@X[($j+2)%16]
 add $f,$f,@X[$i%16]
 and $t0,$c,$b
 xor @X[$j%16],@X[$j%16],@X[($j+8)%16]
 add $f,$f,$e
 andc $t1,$d,$b
 rotlwi $b,$b,30
 or $t0,$t0,$t1
 xor @X[$j%16],@X[$j%16],@X[($j+13)%16]
 add $f,$f,$t0
 rotlwi @X[$j%16],@X[$j%16],1
___
}

sub BODY_20_39 {
my ($i,$a,$b,$c,$d,$e,$f)=@_;
my $j=$i+1;
$code.=<<___ if ($i<79);
 add $f,$K,$e
 rotlwi $e,$a,5
 xor @X[$j%16],@X[$j%16],@X[($j+2)%16]
 add $f,$f,@X[$i%16]
 xor $t0,$b,$c
 xor @X[$j%16],@X[$j%16],@X[($j+8)%16]
 add $f,$f,$e
 rotlwi $b,$b,30
 xor $t0,$t0,$d
 xor @X[$j%16],@X[$j%16],@X[($j+13)%16]
 add $f,$f,$t0
 rotlwi @X[$j%16],@X[$j%16],1
___
$code.=<<___ if ($i==79);
 add $f,$K,$e
 rotlwi $e,$a,5
 lwz r16,0($ctx)
 add $f,$f,@X[$i%16]
 xor $t0,$b,$c
 lwz r17,4($ctx)
 add $f,$f,$e
 rotlwi $b,$b,30
 lwz r18,8($ctx)
 xor $t0,$t0,$d
 lwz r19,12($ctx)
 add $f,$f,$t0
 lwz r20,16($ctx)
___
}

sub BODY_40_59 {
my ($i,$a,$b,$c,$d,$e,$f)=@_;
my $j=$i+1;
$code.=<<___;
 add $f,$K,$e
 rotlwi $e,$a,5
 xor @X[$j%16],@X[$j%16],@X[($j+2)%16]
 add $f,$f,@X[$i%16]
 and $t0,$b,$c
 xor @X[$j%16],@X[$j%16],@X[($j+8)%16]
 add $f,$f,$e
 or $t1,$b,$c
 rotlwi $b,$b,30
 xor @X[$j%16],@X[$j%16],@X[($j+13)%16]
 and $t1,$t1,$d
 or $t0,$t0,$t1
 rotlwi @X[$j%16],@X[$j%16],1
 add $f,$f,$t0
___
}

$code=<<___;
.machine "any"
.text

.globl .sha1_block_data_order
.align 4
.sha1_block_data_order:
 $STU $sp,-$FRAME($sp)
 mflr r0
 $PUSH r15,`$FRAME-$SIZE_T*17`($sp)
 $PUSH r16,`$FRAME-$SIZE_T*16`($sp)
 $PUSH r17,`$FRAME-$SIZE_T*15`($sp)
 $PUSH r18,`$FRAME-$SIZE_T*14`($sp)
 $PUSH r19,`$FRAME-$SIZE_T*13`($sp)
 $PUSH r20,`$FRAME-$SIZE_T*12`($sp)
 $PUSH r21,`$FRAME-$SIZE_T*11`($sp)
 $PUSH r22,`$FRAME-$SIZE_T*10`($sp)
 $PUSH r23,`$FRAME-$SIZE_T*9`($sp)
 $PUSH r24,`$FRAME-$SIZE_T*8`($sp)
 $PUSH r25,`$FRAME-$SIZE_T*7`($sp)
 $PUSH r26,`$FRAME-$SIZE_T*6`($sp)
 $PUSH r27,`$FRAME-$SIZE_T*5`($sp)
 $PUSH r28,`$FRAME-$SIZE_T*4`($sp)
 $PUSH r29,`$FRAME-$SIZE_T*3`($sp)
 $PUSH r30,`$FRAME-$SIZE_T*2`($sp)
 $PUSH r31,`$FRAME-$SIZE_T*1`($sp)
 $PUSH r0,`$FRAME+$LRSAVE`($sp)
 lwz $A,0($ctx)
 lwz $B,4($ctx)
 lwz $C,8($ctx)
 lwz $D,12($ctx)
 lwz $E,16($ctx)
 andi. r0,$inp,3
 bne Lunaligned
Laligned:
 mtctr $num
 bl Lsha1_block_private
 b Ldone

; PowerPC specification allows an implementation to be ill-behaved
; upon unaligned access which crosses page boundary. "Better safe
; than sorry" principle makes me treat it specially. But I don't
; look for particular offending word, but rather for 64-byte input
; block which crosses the boundary. Once found that block is aligned
; and hashed separately...
.align 4
Lunaligned:
 subfic $t1,$inp,4096
 andi. $t1,$t1,4095 ; distance to closest page boundary
 srwi. $t1,$t1,6 ; t1/=64
 beq Lcross_page
 $UCMP $num,$t1
 ble Laligned ; didn't cross the page boundary
 mtctr $t1
 subfc $num,$t1,$num
 bl Lsha1_block_private
Lcross_page:
 li $t1,16
 mtctr $t1
 addi r20,$sp,$LOCALS ; spot within the frame
Lmemcpy:
 lbz r16,0($inp)
 lbz r17,1($inp)
 lbz r18,2($inp)
 lbz r19,3($inp)
 addi $inp,$inp,4
 stb r16,0(r20)
 stb r17,1(r20)
 stb r18,2(r20)
 stb r19,3(r20)
 addi r20,r20,4
 bdnz Lmemcpy

 $PUSH $inp,`$FRAME-$SIZE_T*18`($sp)
 li $t1,1
 addi $inp,$sp,$LOCALS
 mtctr $t1
 bl Lsha1_block_private
 $POP $inp,`$FRAME-$SIZE_T*18`($sp)
 addic. $num,$num,-1
 bne Lunaligned

Ldone:
 $POP r0,`$FRAME+$LRSAVE`($sp)
 $POP r15,`$FRAME-$SIZE_T*17`($sp)
 $POP r16,`$FRAME-$SIZE_T*16`($sp)
 $POP r17,`$FRAME-$SIZE_T*15`($sp)
 $POP r18,`$FRAME-$SIZE_T*14`($sp)
 $POP r19,`$FRAME-$SIZE_T*13`($sp)
 $POP r20,`$FRAME-$SIZE_T*12`($sp)
 $POP r21,`$FRAME-$SIZE_T*11`($sp)
 $POP r22,`$FRAME-$SIZE_T*10`($sp)
 $POP r23,`$FRAME-$SIZE_T*9`($sp)
 $POP r24,`$FRAME-$SIZE_T*8`($sp)
 $POP r25,`$FRAME-$SIZE_T*7`($sp)
 $POP r26,`$FRAME-$SIZE_T*6`($sp)
 $POP r27,`$FRAME-$SIZE_T*5`($sp)
 $POP r28,`$FRAME-$SIZE_T*4`($sp)
 $POP r29,`$FRAME-$SIZE_T*3`($sp)
 $POP r30,`$FRAME-$SIZE_T*2`($sp)
 $POP r31,`$FRAME-$SIZE_T*1`($sp)
 mtlr r0
 addi $sp,$sp,$FRAME
 blr
 .long 0
 .byte 0,12,4,1,0x80,18,3,0
 .long 0
___
```

```
# This is private block function, which uses tailored calling
# interface, namely upon entry SHA_CTX is pre-loaded to given
# registers and counter register contains amount of chunks to
# digest...
$code.=<<___;
.align 4
Lsha1_block_private:
___
$code.=<<___; # load K_00_19
 lis $K,0x5a82
 ori $K,$K,0x7999
___
for($i=0;$i<20;$i++) { &BODY_00_19($i,@V); unshift(@V,pop(@V)); }
$code.=<<___; # load K_20_39
 lis $K,0x6ed9
 ori $K,$K,0xeba1
___
for(;$i<40;$i++) { &BODY_20_39($i,@V); unshift(@V,pop(@V)); }
$code.=<<___; # load K_40_59
 lis $K,0x8f1b
 ori $K,$K,0xbcdc
___
for(;$i<60;$i++) { &BODY_40_59($i,@V); unshift(@V,pop(@V)); }
$code.=<<___; # load K_60_79
 lis $K,0xca62
 ori $K,$K,0xc1d6
___
for(;$i<80;$i++) { &BODY_20_39($i,@V); unshift(@V,pop(@V)); }
$code.=<<___;
 add r16,r16,$E
 add r17,r17,$T
 add r18,r18,$A
 add r19,r19,$B
 add r20,r20,$C
 stw r16,0($ctx)
 mr $A,r16
 stw r17,4($ctx)
 mr $B,r17
 stw r18,8($ctx)
 mr $C,r18
 stw r19,12($ctx)
 mr $D,r19
 stw r20,16($ctx)
 mr $E,r20
 addi $inp,$inp,`16*4`
 bdnz Lsha1_block_private
 blr
 .long 0
 .byte 0,12,0x14,0,0,0,0,0
___
$code.=<<___;
.asciz "SHA1 block transform for PPC, CRYPTOGAMS by <appro\@fy.chalmers.se>"
___

$code =~ s/\`([^\`]*)\`/eval $1/gem;
print $code;
close STDOUT;
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-ppc.pl
No license file was found, but licenses were detected in source scan.

```
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/fips_err.h
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2005 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
* Portions originally developed by SUN MICROSYSTEMS, INC., and
* contributed to the OpenSSL project.
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec_key.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2010 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
```

```
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
```

```
*
* Portions of the attached software ("Contribution") are developed by
* SUN MICROSYSTEMS, INC., and are contributed to the OpenSSL project.
*
* The Contribution is licensed pursuant to the OpenSSL open source
* license provided above.
*
* The elliptic curve binary polynomial software is originally written by
* Sheueling Chang Shantz and Douglas Stebila of Sun Microsystems Laboratories.
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec_curve.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec_lcl.h

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2000 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/e_os2.h
No license file was found, but licenses were detected in source scan.

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ==
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
* ECDH support in OpenSSL originally developed by
* SUN MICROSYSTEMS, INC., and contributed to the OpenSSL project.
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/engine/engine.h
No license file was found, but licenses were detected in source scan.

/* ==
* Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without

```
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
```

*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ossl_typ.h
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2000-2005 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
```

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ecdsa/ecs_locl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/asn1/asn1t.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ecdh/ech_locl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ecdsa/ecdsa.h
No license file was found, but licenses were detected in source scan.

/* ==
* Copyright (c) 1999-2001 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in
*   the documentation and/or other materials provided with the
*   distribution.
*
* 3. All advertising materials mentioning features or use of this
*   software must display the following acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   licensing@OpenSSL.org.
*

```
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
* ECDH support in OpenSSL originally developed by
* SUN MICROSYSTEMS, INC., and contributed to the OpenSSL project.
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/engine/eng_int.h

No license file was found, but licenses were detected in source scan.

```
# Copyright (c) 2011 The OpenSSL Project.  All rights reserved.
# Redistribution and use in source and binary forms, with or without
# modification, are permitted provided that the following conditions
# are met:
# 1. Redistributions of source code must retain the above copyright
#    notice, this list of conditions and the following disclaimer.
# 2. Redistributions in binary form must reproduce the above copyright
#    notice, this list of conditions and the following disclaimer in
#    the documentation and/or other materials provided with the
```

# 3. All advertising materials mentioning features or use of this
# 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
# 5. Products derived from this software may not be called "OpenSSL"

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/modexp512-x86_64.pl
No license file was found, but licenses were detected in source scan.

```
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/asn1/asn1_locl.h
No license file was found, but licenses were detected in source scan.

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@openssl.org> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# SHA512 for C64x+.
#
# January 2012
#
# Performance is 19 cycles per processed byte. Compared to block
# transform function from sha512.c compiled with cl6x with -mv6400+
# -o2 -DOPENSSL_SMALL_FOOTPRINT it's almost 7x faster and 2x smaller.
# Loop unroll won't make it, this implementation, any faster, because
# it's effectively dominated by SHRU||SHL pairs and you can't schedule
# more of them.
#
# !!! Note that this module uses AMR, which means that all interrupt
# service routines are expected to preserve it and for own well-being
# zero it upon entry.

while (($output=shift) && ($output!~/\w[\w\-]*\.\w+$/)) {}
open STDOUT,">$output";

($CTXA,$INP,$NUM) = ("A4","B4","A6");		# arguments
```

```
$K512="A3";

($Ahi,$Actxhi,$Bhi,$Bctxhi,$Chi,$Cctxhi,$Dhi,$Dctxhi,
$Ehi,$Ectxhi,$Fhi,$Fctxhi,$Ghi,$Gctxhi,$Hhi,$Hctxhi)=map("A$_",(16..31));
($Alo,$Actxlo,$Blo,$Bctxlo,$Clo,$Cctxlo,$Dlo,$Dctxlo,
$Elo,$Ectxlo,$Flo,$Fctxlo,$Glo,$Gctxlo,$Hlo,$Hctxlo)=map("B$_",(16..31));

($S1hi,$CHhi,$S0hi,$t0hi)=map("A$_",(10..13));
($S1lo,$CHlo,$S0lo,$t0lo)=map("B$_",(10..13));
($T1hi,         $T2hi)=         ("A6","A7");
($T1lo,$T1carry,$T2lo,$T2carry)=("B6","B7","B8","B9");
($Khi,$Klo)=("A9","A8");
($MAJhi,$MAJlo)=($T2hi,$T2lo);
($t1hi,$t1lo)=($Khi,"B2");
$CTXB=$t1lo;

($Xihi,$Xilo)=("A5","B5");   # circular/ring buffer

$code.=<<___;
 .text

 .asg B3,RA
 .asg A15,FP
 .asg B15,SP

 .if .BIG_ENDIAN
 .asg $Khi,KHI
 .asg $Klo,KLO
 .else
 .asg $Khi,KLO
 .asg $Klo,KHI
 .endif

 .global _sha512_block_data_order
_sha512_block_data_order:
 .asmfunc stack_usage(40+128)
 MV $NUM,A0    ; reassign $NUM
|| MVK -128,B0
 [!A0] BNOP RA    ; if ($NUM==0) return;
|| [A0] STW FP,*SP--(40)   ; save frame pointer
|| [A0] MV SP,FP
  [A0] STDW B13:B12,*SP[4]
|| [A0] MVK 0x00404,B1
  [A0] STDW B11:B10,*SP[3]
|| [A0] STDW A13:A12,*FP[-3]
|| [A0] MVKH 0x60000,B1
  [A0] STDW A11:A10,*SP[1]
|| [A0] MVC B1,AMR    ; setup circular addressing
|| [A0] ADD B0,SP,SP   ; alloca(128)
  [A0] AND B0,SP,SP   ; align stack at 128 bytes
|| [A0] ADDKPC _sha512_block_data_order,B1
|| [A0] MVKL (K512-_sha512_block_data_order),$K512
  [A0] MVKH (K512-_sha512_block_data_order),$K512
|| [A0] SUBAW SP,2,SP    ; reserve two words above buffer
 ADDAW SP,3,$Xilo
 ADDAW SP,2,$Xihi

|| MV $CTXA,$CTXB
 LDW *${CTXA}[0^.LITTLE_ENDIAN],$Ahi ; load ctx
|| LDW *${CTXB}[1^.LITTLE_ENDIAN],$Alo
|| ADD B1,$K512,$K512
 LDW *${CTXA}[2^.LITTLE_ENDIAN],$Bhi
|| LDW *${CTXB}[3^.LITTLE_ENDIAN],$Blo
 LDW *${CTXA}[4^.LITTLE_ENDIAN],$Chi
|| LDW *${CTXB}[5^.LITTLE_ENDIAN],$Clo
 LDW *${CTXA}[6^.LITTLE_ENDIAN],$Dhi
|| LDW *${CTXB}[7^.LITTLE_ENDIAN],$Dlo
 LDW *${CTXA}[8^.LITTLE_ENDIAN],$Ehi
|| LDW *${CTXB}[9^.LITTLE_ENDIAN],$Elo
 LDW *${CTXA}[10^.LITTLE_ENDIAN],$Fhi
|| LDW *${CTXB}[11^.LITTLE_ENDIAN],$Flo
 LDW *${CTXA}[12^.LITTLE_ENDIAN],$Ghi
|| LDW *${CTXB}[13^.LITTLE_ENDIAN],$Glo
 LDW *${CTXA}[14^.LITTLE_ENDIAN],$Hhi
|| LDW *${CTXB}[15^.LITTLE_ENDIAN],$Hlo

 LDNDW *$INP++,B11:B10   ; pre-fetch input
 LDDW *$K512++,$Khi:$Klo  ; pre-fetch K512[0]
outerloop?:
 MVK 15,B0    ; loop counters
|| MVK 64,B1
|| SUB A0,1,A0
 MV $Ahi,$Actxhi
|| MV $Alo,$Actxlo
|| MV $Bhi,$Bctxhi
|| MV $Blo,$Bctxlo
|| MV $Chi,$Cctxhi
|| MV $Clo,$Cctxlo
|| MVD $Dhi,$Dctxhi
|| MVD $Dlo,$Dctxlo
 MV $Ehi,$Ectxhi
|| MV $Elo,$Ectxlo
|| MV $Fhi,$Fctxhi
|| MV $Flo,$Fctxlo
|| MV $Ghi,$Gctxhi
|| MV $Glo,$Gctxlo
|| MVD $Hhi,$Hctxhi
|| MVD $Hlo,$Hctxlo
loop0_15?:
 .if .BIG_ENDIAN
 MV B11,$T1hi
|| MV B10,$T1lo
 .else
 SWAP4 B10,$T1hi
|| SWAP4 B11,$T1lo
 SWAP2 $T1hi,$T1hi
|| SWAP2 $T1lo,$T1lo
 .endif
loop16_79?:
 STW $T1hi,*$Xihi++[2]
|| STW $T1lo,*$Xilo++[2]   ; X[i] = T1
|| ADD $Hhi,$T1hi,$T1hi
|| ADDU $Hlo,$T1lo,$T1carry:$T1lo  ; T1 += h
|| SHRU $Ehi,14,$S1hi
|| SHL $Ehi,32-14,$S1lo
 XOR $Fhi,$Ghi,$CHhi
|| XOR $Flo,$Glo,$CHlo
|| ADD KHI,$T1hi,$T1hi
|| ADDU KLO,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += K512[i]
|| SHRU $Elo,14,$t0lo
|| SHL $Elo,32-14,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| AND $Ehi,$CHhi,$CHhi
|| AND $Elo,$CHlo,$CHlo
|| ROTL $Ghi,0,$Hhi
|| ROTL $Glo,0,$Hlo    ; h = g
|| SHRU $Ehi,18,$t0hi
|| SHL $Ehi,32-18,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| XOR $Ghi,$CHhi,$CHhi
|| XOR $Glo,$CHlo,$CHlo   ; Ch(e,f,g) = ((f^g)&e)^g
|| ROTL $Fhi,0,$Ghi
|| ROTL $Flo,0,$Glo    ; g = f
|| SHRU $Elo,18,$t0lo
|| SHL $Elo,32-18,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| OR $Ahi,$Bhi,$MAJhi
|| OR $Alo,$Blo,$MAJlo
|| ROTL $Ehi,0,$Fhi
|| ROTL $Elo,0,$Flo    ; f = e
|| SHRU $Ehi,41-32,$t0lo
|| SHL $Ehi,64-41,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| AND $Chi,$MAJhi,$MAJhi
|| AND $Clo,$MAJlo,$MAJlo
|| ROTL $Dhi,0,$Ehi
|| ROTL $Dlo,0,$Elo    ; e = d
|| SHRU $Elo,41-32,$t0hi
|| SHL $Elo,64-41,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo   ; Sigma1(e)
|| AND $Ahi,$Bhi,$t1hi
|| AND $Alo,$Blo,$t1lo
|| ROTL $Chi,0,$Dhi
|| ROTL $Clo,0,$Dlo    ; d = c
|| SHRU $Ahi,28,$S0hi
|| SHL $Ahi,32-28,$S0lo
 OR $t1hi,$MAJhi,$MAJhi
|| OR $t1lo,$MAJlo,$MAJlo   ; Maj(a,b,c) = ((a|b)&c)|(a&b)
|| ADD $CHhi,$T1hi,$T1hi
|| ADDU $CHlo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += Ch(e,f,g)
|| ROTL $Bhi,0,$Chi
|| ROTL $Blo,0,$Clo    ; c = b
|| SHRU $Alo,28,$t0lo
|| SHL $Alo,32-28,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $S1hi,$T1hi,$T1hi
|| ADDU $S1lo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += Sigma1(e)
|| ROTL $Ahi,0,$Bhi
|| ROTL $Alo,0,$Blo    ; b = a
|| SHRU $Ahi,34-32,$t0lo
|| SHL $Ahi,64-34,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $MAJhi,$T1hi,$T2hi
|| ADDU $MAJlo,$T1carry:$T1lo,$T2carry:$T2lo ; T2 = T1+Maj(a,b,c)
|| SHRU $Alo,34-32,$t0hi
|| SHL $Alo,64-34,$t0lo
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $Ehi,$T1hi,$T1hi
|| ADDU $Elo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += e
|| [B0] BNOP loop0_15?
|| SHRU $Ahi,39-32,$t0lo
|| SHL $Ahi,64-39,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| [B0] LDNDW *$INP++,B11:B10    ; pre-fetch input
||[!B1] BNOP break?
|| SHRU $Alo,39-32,$t0hi
|| SHL $Alo,64-39,$t0lo
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo   ; Sigma0(a)
|| ADD $T1carry,$T1hi,$Ehi
|| MV $T1lo,$Elo    ; e = T1
||[!B0] LDW *${Xihi}[28],$T1hi
||[!B0] LDW *${Xilo}[28],$T1lo   ; X[i+14]
 ADD $S0hi,$T2hi,$T2hi
|| ADDU $S0lo,$T2carry:$T2lo,$T2carry:$T2lo ; T2 += Sigma0(a)
|| [B1] LDDW *$K512++,$Khi:$Klo   ; pre-fetch K512[i]
 NOP      ; avoid cross-path stall
 ADD $T2carry,$T2hi,$Ahi
|| MV $T2lo,$Alo    ; a = T2
|| [B0] SUB B0,1,B0
;;===== branch to loop00_15? is taken here
 NOP
;;===== branch to break? is taken here
 LDW *${Xihi}[2],$T2hi
|| LDW *${Xilo}[2],$T2lo   ; X[i+1]
|| SHRU $T1hi,19,$S1hi
|| SHL $T1hi,32-19,$S1lo
 SHRU $T1lo,19,$t0lo
|| SHL $T1lo,32-19,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1hi,61-32,$t0lo
|| SHL $T1hi,64-61,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1lo,61-32,$t0hi
|| SHL $T1lo,64-61,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1hi,6,$t0hi
|| SHL $T1hi,32-6,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1lo,6,$t0lo
|| LDW *${Xihi}[18],$T1hi
|| LDW *${Xilo}[18],$T1lo   ; X[i+9]
 XOR $t0lo,$S1lo,$S1lo   ; sigma1(Xi[i+14])

|| LDW *${Xihi}[0],$CHhi
|| LDW *${Xilo}[0],$CHlo   ; X[i]
|| SHRU $T2hi,1,$S0hi
|| SHL $T2hi,32-1,$S0lo
 SHRU $T2lo,1,$t0lo
|| SHL $T2lo,32-1,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| SHRU $T2hi,8,$t0hi
|| SHL $T2hi,32-8,$t0lo
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| SHRU $T2lo,8,$t0lo
|| SHL $T2lo,32-8,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $S1hi,$T1hi,$T1hi
|| ADDU $S1lo,$T1lo,$T1carry:$T1lo  ; T1 = X[i+9]+sigma1()
|| [B1] BNOP loop16_79?
|| SHRU $T2hi,7,$t0hi
|| SHL $T2hi,32-7,$t0lo
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $CHhi,$T1hi,$T1hi
|| ADDU $CHlo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += X[i]
|| SHRU $T2lo,7,$t0lo
 XOR $t0lo,$S0lo,$S0lo   ; sigma0(Xi[i+1]

 ADD $S0hi,$T1hi,$T1hi
|| ADDU $S0lo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += sigma0()
|| [B1] SUB B1,1,B1
 NOP      ; avoid cross-path stall
 ADD $T1carry,$T1hi,$T1hi
;;===== branch to loop16_79? is taken here

break?:
 ADD $Ahi,$Actxhi,$Ahi  ; accumulate ctx
|| ADDU $Alo,$Actxlo,$Actxlo:$Alo
|| [A0] LDNDW *$INP++,B11:B10   ; pre-fetch input
|| [A0] ADDK -640,$K512   ; rewind pointer to K512
 ADD $Bhi,$Bctxhi,$Bhi
|| ADDU $Blo,$Bctxlo,$Bctxlo:$Blo
|| [A0] LDDW *$K512++,$Khi:$Klo  ; pre-fetch K512[0]
 ADD $Chi,$Cctxhi,$Chi
|| ADDU $Clo,$Cctxlo,$Cctxlo:$Clo
|| ADD $Actxlo,$Ahi,$Ahi
||[!A0] MV $CTXA,$CTXB
 ADD $Dhi,$Dctxhi,$Dhi
|| ADDU $Dlo,$Dctxlo,$Dctxlo:$Dlo
|| ADD $Bctxlo,$Bhi,$Bhi
||[!A0] STW $Ahi,*${CTXA}[0^.LITTLE_ENDIAN] ; save ctx
```

```
||[!A0] STW $Alo,*${CTXB}[1^.LITTLE_ENDIAN]
 ADD $Ehi,$Ectxhi,$Ehi
|| ADDU $Elo,$Ectxlo,$Ectxlo:$Elo
|| ADD $Cctxlo,$Chi,$Chi
|| [A0] BNOP outerloop?
||[!A0] STW $Bhi,*${CTXA}[2^.LITTLE_ENDIAN]
||[!A0] STW $Blo,*${CTXB}[3^.LITTLE_ENDIAN]
 ADD $Fhi,$Fctxhi,$Fhi
|| ADDU $Flo,$Fctxlo,$Fctxlo:$Flo
|| ADD $Dctxlo,$Dhi,$Dhi
||[!A0] STW $Chi,*${CTXA}[4^.LITTLE_ENDIAN]
||[!A0] STW $Clo,*${CTXB}[5^.LITTLE_ENDIAN]
 ADD $Ghi,$Gctxhi,$Ghi
|| ADDU $Glo,$Gctxlo,$Gctxlo:$Glo
|| ADD $Ectxlo,$Ehi,$Ehi
||[!A0] STW $Dhi,*${CTXA}[6^.LITTLE_ENDIAN]
||[!A0] STW $Dlo,*${CTXB}[7^.LITTLE_ENDIAN]
 ADD $Hhi,$Hctxhi,$Hhi
|| ADDU $Hlo,$Hctxlo,$Hctxlo:$Hlo
|| ADD $Fctxlo,$Fhi,$Fhi
||[!A0] STW $Ehi,*${CTXA}[8^.LITTLE_ENDIAN]
||[!A0] STW $Elo,*${CTXB}[9^.LITTLE_ENDIAN]
 ADD $Gctxlo,$Ghi,$Ghi
||[!A0] STW $Fhi,*${CTXA}[10^.LITTLE_ENDIAN]
||[!A0] STW $Flo,*${CTXB}[11^.LITTLE_ENDIAN]
 ADD $Hctxlo,$Hhi,$Hhi
||[!A0] STW $Ghi,*${CTXA}[12^.LITTLE_ENDIAN]
||[!A0] STW $Glo,*${CTXB}[13^.LITTLE_ENDIAN]
;;===== branch to outerloop? is taken here

 STW $Hhi,*${CTXA}[14^.LITTLE_ENDIAN]
|| STW $Hlo,*${CTXB}[15^.LITTLE_ENDIAN]
|| MVK -40,B0
 ADD FP,B0,SP   ; destroy circular buffer
|| LDDW *FP[-4],A11:A10
 LDDW *SP[2],A13:A12
|| LDDW *FP[-2],B11:B10
 LDDW *SP[4],B13:B12
|| BNOP RA
 LDW *++SP(40),FP   ; restore frame pointer
 MVK 0,B0
 MVC B0,AMR    ; clear AMR
 NOP 2    ; wait till FP is committed
 .endasmfunc

 .sect ".const:sha_asm"
 .align 128
K512:
 .uword 0x428a2f98,0xd728ae22, 0x71374491,0x23ef65cd
 .uword 0xb5c0fbcf,0xec4d3b2f, 0xe9b5dba5,0x8189dbbc
 .uword 0x3956c25b,0xf348b538, 0x59f111f1,0xb605d019
 .uword 0x923f82a4,0xaf194f9b, 0xab1c5ed5,0xda6d8118
 .uword 0xd807aa98,0xa3030242, 0x12835b01,0x45706fbe
 .uword 0x243185be,0x4ee4b28c, 0x550c7dc3,0xd5ffb4e2
 .uword 0x72be5d74,0xf27b896f, 0x80deb1fe,0x3b1696b1
 .uword 0x9bdc06a7,0x25c71235, 0xc19bf174,0xcf692694
 .uword 0xe49b69c1,0x9ef14ad2, 0xefbe4786,0x384f25e3
 .uword 0x0fc19dc6,0x8b8cd5b5, 0x240ca1cc,0x77ac9c65
 .uword 0x2de92c6f,0x592b0275, 0x4a7484aa,0x6ea6e483
 .uword 0x5cb0a9dc,0xbd41fbd4, 0x76f988da,0x831153b5
 .uword 0x983e5152,0xee66dfab, 0xa831c66d,0x2db43210
 .uword 0xb00327c8,0x98fb213f, 0xbf597fc7,0xbeef0ee4
 .uword 0xc6e00bf3,0x3da88fc2, 0xd5a79147,0x930aa725
 .uword 0x06ca6351,0xe003826f, 0x14292967,0x0a0e6e70
 .uword 0x27b70a85,0x46d22ffc, 0x2e1b2138,0x5c26c926
 .uword 0x4d2c6dfc,0x5ac42aed, 0x53380d13,0x9d95b3df
 .uword 0x650a7354,0x8baf63de, 0x766a0abb,0x3c77b2a8
 .uword 0x81c2c92e,0x47edaee6, 0x92722c85,0x1482353b
 .uword 0xa2bfe8a1,0x4cf10364, 0xa81a664b,0xbc423001
 .uword 0xc24b8b70,0xd0f89791, 0xc76c51a3,0x0654be30
 .uword 0xd192e819,0xd6ef5218, 0xd6990624,0x5565a910
 .uword 0xf40e3585,0x5771202a, 0x106aa070,0x32bbd1b8
 .uword 0x19a4c116,0xb8d2d0c8, 0x1e376c08,0x5141ab53
 .uword 0x2748774c,0xdf8eeb99, 0x34b0bcb5,0xe19b48a8
 .uword 0x391c0cb3,0xc5c95a63, 0x4ed8aa4a,0xe3418acb
 .uword 0x5b9cca4f,0x7763e373, 0x682e6ff3,0xd6b2b8a3
 .uword 0x748f82ee,0x5defb2fc, 0x78a5636f,0x43172f60
 .uword 0x84c87814,0xa1f0ab72, 0x8cc70208,0x1a6439ec
 .uword 0x90befffa,0x23631e28, 0xa4506ceb,0xde82bde9
 .uword 0xbef9a3f7,0xb2c67915, 0xc67178f2,0xe372532b
 .uword 0xca273ece,0xea26619c, 0xd186b8c7,0x21c0c207
 .uword 0xeada7dd6,0xcde0eb1e, 0xf57d4f7f,0xee6ed178
 .uword 0x06f067aa,0x72176fba, 0x0a637dc5,0xa2c898a6
 .uword 0x113f9804,0xbef90dae, 0x1b710b35,0x131c471b
 .uword 0x28db77f5,0x23047d84, 0x32caab7b,0x40c72493
 .uword 0x3c9ebe0a,0x15c9bebc, 0x431d67c4,0x9c100d4c
 .uword 0x4cc5d4be,0xcb3e42b6, 0x597f299c,0xfc657e2a
 .uword 0x5fcb6fab,0x3ad6faec, 0x6c44198c,0x4a475817
 .cstring "SHA512 block transform for C64x+, CRYPTOGAMS by <appro\@openssl.org>"
 .align 4
___

print $code;
close STDOUT;
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-c64xplus.pl

No license file was found, but licenses were detected in source scan.

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@openssl.org> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# February 2012
#
# The module implements bn_GF2m_mul_2x2 polynomial multiplication
# used in bn_gf2m.c. It's kind of low-hanging mechanical port from
# C for the time being... The subroutine runs in 37 cycles, which is
# 4.5x faster than compiler-generated code. Though comparison is
# totally unfair, because this module utilizes Galois Field Multiply
# instruction.

while (($output=shift) && ($output!~/\w[\w\-]*\.\w+$/)) {}
open STDOUT,">$output";

($rp,$a1,$a0,$b1,$b0)=("A4","B4","A6","B6","A8");   # argument vector

($Alo,$Alox0,$Alox1,$Alox2,$Alox3)=map("A$_",(16..20));
($Ahi,$Ahix0,$Ahix1,$Ahix2,$Ahix3)=map("B$_",(16..20));
($B_0,$B_1,$B_2,$B_3)=("B5","A5","A7","B7");
($A,$B)=($Alo,$B_1);
$xFF="B1";

sub mul_1x1_upper {
my ($A,$B)=@_;
$code.=<<___;
 EXTU $B,8,24,$B_2  ; smash $B to 4 bytes
|| AND $B,$xFF,$B_0
|| SHRU $B,24,$B_3
 SHRU $A,16,   $Ahi  ; smash $A to two halfwords
|| EXTU $A,16,16,$Alo

 XORMPY $Alo,$B_2,$Alox2 ; 16x8 bits muliplication
|| XORMPY $Ahi,$B_2,$Ahix2
|| EXTU $B,16,24,$B_1
 XORMPY $Alo,$B_0,$Alox0
|| XORMPY $Ahi,$B_0,$Ahix0
 XORMPY $Alo,$B_3,$Alox3
```

```
|| XORMPY $Ahi,$B_3,$Ahix3
 XORMPY $Alo,$B_1,$Alox1
|| XORMPY $Ahi,$B_1,$Ahix1
___
}
sub mul_1x1_merged {
my ($OUTlo,$OUThi,$A,$B)=@_;
$code.=<<___;
  EXTU $B,8,24,$B_2  ; smash $B to 4 bytes
||  AND $B,$xFF,$B_0
||  SHRU $B,24,$B_3
  SHRU $A,16,   $Ahi  ; smash $A to two halfwords
||  EXTU $A,16,16,$Alo

 XOR $Ahix0,$Alox2,$Ahix0
|| MV $Ahix2,$OUThi
||  XORMPY $Alo,$B_2,$Alox2
  XORMPY $Ahi,$B_2,$Ahix2
||  EXTU $B,16,24,$B_1
||  XORMPY $Alo,$B_0,A1  ; $Alox0
 XOR $Ahix1,$Alox3,$Ahix1
|| SHL $Ahix0,16,$OUTlo
|| SHRU $Ahix0,16,$Ahix0
 XOR $Alox0,$OUTlo,$OUTlo
|| XOR $Ahix0,$OUThi,$OUThi
||  XORMPY $Ahi,$B_0,$Ahix0
||  XORMPY $Alo,$B_3,$Alox3
|| SHL $Alox1,8,$Alox1
|| SHL $Ahix3,8,$Ahix3
 XOR $Alox1,$OUTlo,$OUTlo
|| XOR $Ahix3,$OUThi,$OUThi
||  XORMPY $Ahi,$B_3,$Ahix3
|| SHL $Ahix1,24,$Alox1
|| SHRU $Ahix1,8, $Ahix1
 XOR $Alox1,$OUTlo,$OUTlo
|| XOR $Ahix1,$OUThi,$OUThi
||  XORMPY $Alo,$B_1,$Alox1
||  XORMPY $Ahi,$B_1,$Ahix1
||  MV A1,$Alox0
___
}
sub mul_1x1_lower {
my ($OUTlo,$OUThi)=@_;
$code.=<<___;
 ;NOP
 XOR $Ahix0,$Alox2,$Ahix0
|| MV $Ahix2,$OUThi
 NOP
 XOR $Ahix1,$Alox3,$Ahix1
|| SHL $Ahix0,16,$OUTlo
|| SHRU $Ahix0,16,$Ahix0
 XOR $Alox0,$OUTlo,$OUTlo
|| XOR $Ahix0,$OUThi,$OUThi
|| SHL $Alox1,8,$Alox1
|| SHL $Ahix3,8,$Ahix3
 XOR $Alox1,$OUTlo,$OUTlo
|| XOR $Ahix3,$OUThi,$OUThi
|| SHL $Ahix1,24,$Alox1
|| SHRU $Ahix1,8, $Ahix1
 XOR $Alox1,$OUTlo,$OUTlo
|| XOR $Ahix1,$OUThi,$OUThi
___
}
$code.=<<___;
 .text

 .global _bn_GF2m_mul_2x2
_bn_GF2m_mul_2x2:
 .asmfunc
 MVK 0xFF,$xFF
___
 &mul_1x1_upper($a0,$b0);  # a0b0
$code.=<<___;
|| MV $b1,$B
 MV $a1,$A
___
 &mul_1x1_merged("A28","B28",$A,$B); # a0b0/a1b1
$code.=<<___;
|| XOR $b0,$b1,$B
 XOR $a0,$a1,$A
___
 &mul_1x1_merged("A31","B31",$A,$B); # a1b1/(a0+a1)(b0+b1)
$code.=<<___;
 XOR A28,A31,A29
|| XOR B28,B31,B29   ; a0b0+a1b1
___
 &mul_1x1_lower("A30","B30");  # (a0+a1)(b0+b1)
$code.=<<___;
|| BNOP B3
 XOR A29,A30,A30
|| XOR B29,B30,B30   ; (a0+a1)(b0+b1)-a0b0-a1b1
 XOR B28,A30,A30
|| STW A28,*${rp}[0]
 XOR B30,A31,A31
|| STW A30,*${rp}[1]
 STW A31,*${rp}[2]
 STW B31,*${rp}[3]
 .endasmfunc
___

print $code;
close STDOUT;
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/c64xplus-gf2m.pl
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ecdsa/ecs_ossl.c
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips_test_suite.c
No license file was found, but licenses were detected in source scan.

```
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# GHASH for for PowerISA v2.07.
#
# July 2014
#
# Accurate performance measurements are problematic, because it's
# always virtualized setup with possibly throttled processor.
# Relative comparison is therefore more informative. This initial
# version is ~2.1x slower than hardware-assisted AES-128-CTR, ~12x
# faster than "4-bit" integer-only compiler-generated 64-bit code.
# "Initial version" means that there is room for futher improvement.

# May 2016
#
# 2x aggregated reduction improves performance by 50% (resulting
# performance on POWER8 is 1 cycle per processed byte), and 4x
# aggregated reduction - by 170% or 2.7x (resulting in 0.55 cpb).

$flavour=shift;
$output =shift;

if ($flavour =~ /64/) {
 $SIZE_T=8;
 $LRSAVE=2*$SIZE_T;
 $STU="stdu";
 $POP="ld";
 $PUSH="std";
 $UCMP="cmpld";
 $SHRI="srdi";
} elsif ($flavour =~ /32/) {
 $SIZE_T=4;
 $LRSAVE=$SIZE_T;
 $STU="stwu";
 $POP="lwz";
 $PUSH="stw";
 $UCMP="cmplw";
 $SHRI="srwi";
} else { die "nonsense $flavour"; }

$sp="r1";
$FRAME=6*$SIZE_T+13*16; # 13*16 is for v20-v31 offload

$0 =~ m/(.*[\/\\])[^\/\\]+$/; $dir=$1;
( $xlate="${dir}ppc-xlate.pl" and -f $xlate ) or
( $xlate="${dir}../../perlasm/ppc-xlate.pl" and -f $xlate) or
die "can't locate ppc-xlate.pl";
```

```
open STDOUT,"| $^X $xlate $flavour $output" || die "can't call $xlate: $!";

my ($Xip,$Htbl,$inp,$len)=map("r$_",(3..6)); # argument block

my ($Xl,$Xm,$Xh,$IN)=map("v$_",(0..3));
my ($zero,$t0,$t1,$t2,$xC2,$H,$Hh,$Hl,$lemask)=map("v$_",(4..12));
my ($Xl1,$Xm1,$Xh1,$IN1,$H2,$H2h,$H2l)=map("v$_",(13..19));
my $vrsave="r12";

$code=<<___;
.machine "any"

.text

.globl .gcm_init_p8
.align 5
.gcm_init_p8:
 li  r0,-4096
 li  r8,0x10
 mfspr  $vrsave,256
 li  r9,0x20
 mtspr  256,r0
 li  r10,0x30
 lvx_u  $H,0,r4   # load H

 vspltisb $xC2,-16  # 0xf0
 vspltisb $t0,1   # one
 vaddubm  $xC2,$xC2,$xC2  # 0xe0
 vxor  $zero,$zero,$zero
 vor  $xC2,$xC2,$t0  # 0xe1
 vsldoi  $xC2,$xC2,$zero,15 # 0xe1...
 vsldoi  $t1,$zero,$t0,1  # ...1
 vaddubm  $xC2,$xC2,$xC2  # 0xc2...
 vspltisb $t2,7
 vor  $xC2,$xC2,$t1  # 0xc2....01
 vspltb  $t1,$H,0  # most significant byte
 vsl  $H,$H,$t0  # H<<=1
 vsrab  $t1,$t1,$t2  # broadcast carry bit
 vand  $t1,$t1,$xC2
 vxor  $IN,$H,$t1  # twisted H

 vsldoi  $H,$IN,$IN,8  # twist even more ...
 vsldoi  $xC2,$zero,$xC2,8 # 0xc2.0
 vsldoi  $Hl,$zero,$H,8  # ... and split
 vsldoi  $Hh,$H,$zero,8

 stvx_u  $xC2,0,r3  # save pre-computed table
 stvx_u  $Hl,r8,r3
 li  r8,0x40
 stvx_u  $H, r9,r3
 li  r9,0x50
 stvx_u  $Hh,r10,r3
 li  r10,0x60

 vpmsumd  $Xl,$IN,$Hl  # H.loH.lo
 vpmsumd  $Xm,$IN,$H  # H.hiH.lo+H.loH.hi
 vpmsumd  $Xh,$IN,$Hh  # H.hiH.hi

 vpmsumd  $t2,$Xl,$xC2  # 1st reduction phase

 vsldoi  $t0,$Xm,$zero,8
 vsldoi  $t1,$zero,$Xm,8
 vxor  $Xl,$Xl,$t0
 vxor  $Xh,$Xh,$t1

 vsldoi  $Xl,$Xl,$Xl,8
 vxor  $Xl,$Xl,$t2

 vsldoi  $t1,$Xl,$Xl,8  # 2nd reduction phase
 vpmsumd  $Xl,$Xl,$xC2
 vxor  $t1,$t1,$Xh
 vxor  $IN1,$Xl,$t1

 vsldoi  $H2,$IN1,$IN1,8
 vsldoi  $H2l,$zero,$H2,8
 vsldoi  $H2h,$H2,$zero,8

 stvx_u  $H2l,r8,r3  # save H^2
 li  r8,0x70
 stvx_u  $H2,r9,r3
 li  r9,0x80
 stvx_u  $H2h,r10,r3
 li  r10,0x90
___
{
my ($t4,$t5,$t6) = ($Hl,$H,$Hh);
$code.=<<___;
 vpmsumd  $Xl,$IN,$H2l  # H.loH^2.lo
  vpmsumd $Xl1,$IN1,$H2l  # H^2.loH^2.lo
 vpmsumd  $Xm,$IN,$H2  # H.hiH^2.lo+H.loH^2.hi
  vpmsumd $Xm1,$IN1,$H2  # H^2.hiH^2.lo+H^2.loH^2.hi
 vpmsumd  $Xh,$IN,$H2h  # H.hiH^2.hi
  vpmsumd $Xh1,$IN1,$H2h  # H^2.hiH^2.hi

 vpmsumd  $t2,$Xl,$xC2  # 1st reduction phase
  vpmsumd $t6,$Xl1,$xC2  # 1st reduction phase

 vsldoi  $t0,$Xm,$zero,8
 vsldoi  $t1,$zero,$Xm,8
  vsldoi  $t4,$Xm1,$zero,8
  vsldoi  $t5,$zero,$Xm1,8
 vxor  $Xl,$Xl,$t0
 vxor  $Xh,$Xh,$t1
  vxor  $Xl1,$Xl1,$t4
  vxor  $Xh1,$Xh1,$t5

 vsldoi  $Xl,$Xl,$Xl,8
  vsldoi  $Xl1,$Xl1,$Xl1,8
 vxor  $Xl,$Xl,$t2
  vxor  $Xl1,$Xl1,$t6

 vsldoi  $t1,$Xl,$Xl,8  # 2nd reduction phase
  vsldoi  $t5,$Xl1,$Xl1,8  # 2nd reduction phase
 vpmsumd  $Xl,$Xl,$xC2
  vpmsumd $Xl1,$Xl1,$xC2
 vxor  $t1,$t1,$Xh
  vxor  $t5,$t5,$Xh1
 vxor  $Xl,$Xl,$t1
  vxor  $Xl1,$Xl1,$t5

 vsldoi  $H,$Xl,$Xl,8
  vsldoi  $H2,$Xl1,$Xl1,8
 vsldoi  $Hl,$zero,$H,8
 vsldoi  $Hh,$H,$zero,8
  vsldoi  $H2l,$zero,$H2,8
  vsldoi  $H2h,$H2,$zero,8

 stvx_u  $Hl,r8,r3  # save H^3
 li  r8,0xa0
 stvx_u  $H,r9,r3
 li  r9,0xb0
 stvx_u  $Hh,r10,r3
 li  r10,0xc0
  stvx_u  $H2l,r8,r3  # save H^4
  stvx_u  $H2,r9,r3
  stvx_u  $H2h,r10,r3

 mtspr  256,$vrsave
 blr
 .long  0
 .byte  0,12,0x14,0,0,0,2,0
 .long  0
.size .gcm_init_p8,.-.gcm_init_p8
```

```
___
}
$code.=<<___;
.globl .gcm_gmult_p8
.align 5
.gcm_gmult_p8:
 lis  r0,0xfff8
 li  r8,0x10
 mfspr  $vrsave,256
 li  r9,0x20
 mtspr  256,r0
 li  r10,0x30
 lvx_u  $IN,0,$Xip  # load Xi

 lvx_u  $Hl,r8,$Htbl  # load pre-computed table
  le?lvsl $lemask,r0,r0
 lvx_u  $H, r9,$Htbl
  le?vspltisb $t0,0x07
 lvx_u  $Hh,r10,$Htbl
  le?vxor $lemask,$lemask,$t0
 lvx_u  $xC2,0,$Htbl
  le?vperm $IN,$IN,$IN,$lemask
 vxor  $zero,$zero,$zero

 vpmsumd  $Xl,$IN,$Hl  # H.loXi.lo
 vpmsumd  $Xm,$IN,$H  # H.hiXi.lo+H.loXi.hi
 vpmsumd  $Xh,$IN,$Hh  # H.hiXi.hi

 vpmsumd  $t2,$Xl,$xC2  # 1st reduction phase

 vsldoi  $t0,$Xm,$zero,8
 vsldoi  $t1,$zero,$Xm,8
 vxor  $Xl,$Xl,$t0
 vxor  $Xh,$Xh,$t1

 vsldoi  $Xl,$Xl,$Xl,8
 vxor  $Xl,$Xl,$t2

 vsldoi  $t1,$Xl,$Xl,8  # 2nd reduction phase
 vpmsumd  $Xl,$Xl,$xC2
 vxor  $t1,$t1,$Xh
 vxor  $Xl,$Xl,$t1

 le?vperm $Xl,$Xl,$Xl,$lemask
 stvx_u  $Xl,0,$Xip  # write out Xi

 mtspr  256,$vrsave
 blr
 .long  0
 .byte  0,12,0x14,0,0,0,2,0
 .long  0
.size .gcm_gmult_p8,.-.gcm_gmult_p8

.globl .gcm_ghash_p8
.align 5
.gcm_ghash_p8:
 li  r0,-4096
 li  r8,0x10
 mfspr  $vrsave,256
 li  r9,0x20
 mtspr  256,r0
 li  r10,0x30
 lvx_u  $Xl,0,$Xip  # load Xi

 lvx_u  $Hl,r8,$Htbl  # load pre-computed table
 li  r8,0x40
  le?lvsl $lemask,r0,r0
 lvx_u  $H, r9,$Htbl
 li  r9,0x50
  le?vspltisb $t0,0x07
 lvx_u  $Hh,r10,$Htbl
 li  r10,0x60
  le?vxor $lemask,$lemask,$t0
 lvx_u  $xC2,0,$Htbl
  le?vperm $Xl,$Xl,$Xl,$lemask
 vxor  $zero,$zero,$zero

 ${UCMP}i $len,64
 bge  Lgcm_ghash_p8_4x

 lvx_u  $IN,0,$inp
 addi  $inp,$inp,16
 subic.  $len,$len,16
  le?vperm $IN,$IN,$IN,$lemask
 vxor  $IN,$IN,$Xl
 beq  Lshort

 lvx_u  $H2l,r8,$Htbl  # load H^2
 li  r8,16
 lvx_u  $H2, r9,$Htbl
 add  r9,$inp,$len  # end of input
 lvx_u  $H2h,r10,$Htbl
 be?b  Loop_2x

.align 5
Loop_2x:
 lvx_u  $IN1,0,$inp
 le?vperm $IN1,$IN1,$IN1,$lemask

  subic  $len,$len,32
 vpmsumd  $Xl,$IN,$H2l  # H^2.loXi.lo
  vpmsumd $Xl1,$IN1,$Hl  # H.loXi+1.lo
  subfe  r0,r0,r0  # borrow?-1:0
 vpmsumd  $Xm,$IN,$H2  # H^2.hiXi.lo+H^2.loXi.hi
  vpmsumd $Xm1,$IN1,$H  # H.hiXi+1.lo+H.loXi+1.hi
  and  r0,r0,$len
 vpmsumd  $Xh,$IN,$H2h  # H^2.hiXi.hi
  vpmsumd $Xh1,$IN1,$Hh  # H.hiXi+1.hi
  add  $inp,$inp,r0

 vxor  $Xl,$Xl,$Xl1
 vxor  $Xm,$Xm,$Xm1

 vpmsumd  $t2,$Xl,$xC2  # 1st reduction phase

 vsldoi  $t0,$Xm,$zero,8
 vsldoi  $t1,$zero,$Xm,8
  vxor  $Xh,$Xh,$Xh1
 vxor  $Xl,$Xl,$t0
 vxor  $Xh,$Xh,$t1

 vsldoi  $Xl,$Xl,$Xl,8
 vxor  $Xl,$Xl,$t2
  lvx_u  $IN,r8,$inp
  addi  $inp,$inp,32

 vsldoi  $t1,$Xl,$Xl,8  # 2nd reduction phase
 vpmsumd  $Xl,$Xl,$xC2
  le?vperm $IN,$IN,$IN,$lemask
 vxor  $t1,$t1,$Xh
 vxor  $IN,$IN,$t1
 vxor  $IN,$IN,$Xl
 $UCMP  r9,$inp
 bgt  Loop_2x   # done yet?

 cmplwi  $len,0
 bne  Leven

Lshort:
 vpmsumd  $Xl,$IN,$Hl  # H.loXi.lo
 vpmsumd  $Xm,$IN,$H  # H.hiXi.lo+H.loXi.hi
 vpmsumd  $Xh,$IN,$Hh  # H.hiXi.hi

 vpmsumd  $t2,$Xl,$xC2  # 1st reduction phase
 vsldoi  $t0,$Xm,$zero,8
 vsldoi  $t1,$zero,$Xm,8
 vxor  $Xl,$Xl,$t0
 vxor  $Xh,$Xh,$t1

 vsldoi  $Xl,$Xl,$Xl,8
 vxor  $Xl,$Xl,$t2

 vsldoi  $t1,$Xl,$Xl,8  # 2nd reduction phase
 vpmsumd  $Xl,$Xl,$xC2
 vxor  $t1,$t1,$Xh

Leven:
 vxor  $Xl,$Xl,$t1
 le?vperm $Xl,$Xl,$Xl,$lemask
 stvx_u  $Xl,0,$Xip  # write out Xi

 mtspr  256,$vrsave
 blr
 .long  0
 .byte  0,12,0x14,0,0,0,4,0
 .long  0
___
{
my ($Xl3,$Xm2,$IN2,$H3l,$H3,$H3h,
   $Xh3,$Xm3,$IN3,$H4l,$H4,$H4h) = map("v$_",(20..31));
my $IN0=$IN;
my ($H21l,$H21h,$loperm,$hiperm) = ($Hl,$Hh,$H2l,$H2h);

$code.=<<___;
.align 5
.gcm_ghash_p8_4x:
Lgcm_ghash_p8_4x:
 $STU  $sp,-$FRAME($sp)
 li  r10,`15+6*$SIZE_T`
 li  r11,`31+6*$SIZE_T`
 stvx  v20,r10,$sp
 addi  r10,r10,32
 stvx  v21,r11,$sp
 addi  r11,r11,32
 stvx  v22,r10,$sp
 addi  r10,r10,32
 stvx  v23,r11,$sp
 addi  r11,r11,32
 stvx  v24,r10,$sp
 addi  r10,r10,32
 stvx  v25,r11,$sp
```

```
addi  r11,r11,32
stvx  v26,r10,$sp
addi  r10,r10,32
stvx  v27,r11,$sp
addi  r11,r11,32
stvx  v28,r10,$sp
addi  r10,r10,32
stvx  v29,r11,$sp
addi  r11,r11,32
stvx  v30,r10,$sp
li  r10,0x60
stvx  v31,r11,$sp
li  r0,-1
stw  $vrsave,`$FRAME-4`($sp) # save vrsave
mtspr  256,r0   # preserve all AltiVec registers

lvsl  $t0,0,r8  # 0x0001..0e0f
#lvx_u  $H2l,r8,$Htbl  # load H^2
li  r8,0x70
lvx_u  $H2, r9,$Htbl
li  r9,0x80
vspltisb $t1,8   # 0x0808..0808
#lvx_u  $H2h,r10,$Htbl
li  r10,0x90
lvx_u  $H3l,r8,$Htbl  # load H^3
li  r8,0xa0
lvx_u  $H3, r9,$Htbl
li  r9,0xb0
lvx_u  $H3h,r10,$Htbl
li  r10,0xc0
lvx_u  $H4l,r8,$Htbl  # load H^4
li  r8,0x10
lvx_u  $H4, r9,$Htbl
li  r9,0x20
lvx_u  $H4h,r10,$Htbl
li  r10,0x30

vsldoi  $t2,$zero,$t1,8  # 0x0000..0808
vaddubm  $hiperm,$t0,$t2  # 0x0001..1617
vaddubm  $loperm,$t1,$hiperm # 0x0809..1e1f

$SHRI  $len,$len,4  # this allows to use sign bit
   # as carry
lvx_u  $IN0,0,$inp  # load input
lvx_u  $IN1,r8,$inp
subic.  $len,$len,8
lvx_u  $IN2,r9,$inp
lvx_u  $IN3,r10,$inp
```

```
 addi  $inp,$inp,0x40
 le?vperm $IN0,$IN0,$IN0,$lemask
 le?vperm $IN1,$IN1,$IN1,$lemask
 le?vperm $IN2,$IN2,$IN2,$lemask
 le?vperm $IN3,$IN3,$IN3,$lemask

 vxor  $Xh,$IN0,$Xl

  vpmsumd $Xl1,$IN1,$H3l
  vpmsumd $Xm1,$IN1,$H3
  vpmsumd $Xh1,$IN1,$H3h

  vperm  $H21l,$H2,$H,$hiperm
  vperm  $t0,$IN2,$IN3,$loperm
  vperm  $H21h,$H2,$H,$loperm
  vperm  $t1,$IN2,$IN3,$hiperm
  vpmsumd $Xm2,$IN2,$H2  # H^2.loXi+2.hi+H^2.hiXi+2.lo
  vpmsumd $Xl3,$t0,$H21l  # H^2.loXi+2.lo+H.loXi+3.lo
  vpmsumd $Xm3,$IN3,$H  # H.hiXi+3.lo  +H.loXi+3.hi
  vpmsumd $Xh3,$t1,$H21h  # H^2.hiXi+2.hi+H.hiXi+3.hi

  vxor  $Xm2,$Xm2,$Xm1
  vxor  $Xl3,$Xl3,$Xl1
  vxor  $Xm3,$Xm3,$Xm2
  vxor  $Xh3,$Xh3,$Xh1

 blt  Ltail_4x

Loop_4x:
 lvx_u  $IN0,0,$inp
 lvx_u  $IN1,r8,$inp
 subic.  $len,$len,4
 lvx_u  $IN2,r9,$inp
 lvx_u  $IN3,r10,$inp
 addi  $inp,$inp,0x40
 le?vperm $IN1,$IN1,$IN1,$lemask
 le?vperm $IN2,$IN2,$IN2,$lemask
 le?vperm $IN3,$IN3,$IN3,$lemask
 le?vperm $IN0,$IN0,$IN0,$lemask

 vpmsumd  $Xl,$Xh,$H4l  # H^4.loXi.lo
 vpmsumd  $Xm,$Xh,$H4  # H^4.hiXi.lo+H^4.loXi.hi
 vpmsumd  $Xh,$Xh,$H4h  # H^4.hiXi.hi
  vpmsumd $Xl1,$IN1,$H3l
  vpmsumd $Xm1,$IN1,$H3
  vpmsumd $Xh1,$IN1,$H3h

 vxor  $Xl,$Xl,$Xl3
 vxor  $Xm,$Xm,$Xm3
 vxor  $Xh,$Xh,$Xh3
  vperm  $t0,$IN2,$IN3,$loperm
  vperm  $t1,$IN2,$IN3,$hiperm

 vpmsumd  $t2,$Xl,$xC2  # 1st reduction phase
  vpmsumd $Xl3,$t0,$H21l  # H.loXi+3.lo  +H^2.loXi+2.lo
  vpmsumd $Xh3,$t1,$H21h  # H.hiXi+3.hi  +H^2.hiXi+2.hi

 vsldoi  $t0,$Xm,$zero,8
 vsldoi  $t1,$zero,$Xm,8
 vxor  $Xl,$Xl,$t0
 vxor  $Xh,$Xh,$t1

 vsldoi  $Xl,$Xl,$Xl,8
 vxor  $Xl,$Xl,$t2

 vsldoi  $t1,$Xl,$Xl,8  # 2nd reduction phase
  vpmsumd $Xm2,$IN2,$H2  # H^2.hiXi+2.lo+H^2.loXi+2.hi
  vpmsumd $Xm3,$IN3,$H  # H.hiXi+3.lo  +H.loXi+3.hi
 vpmsumd  $Xl,$Xl,$xC2

  vxor  $Xl3,$Xl3,$Xl1
  vxor  $Xh3,$Xh3,$Xh1
 vxor  $Xh,$Xh,$IN0
  vxor  $Xm2,$Xm2,$Xm1
 vxor  $Xh,$Xh,$t1
  vxor  $Xm3,$Xm3,$Xm2
 vxor  $Xh,$Xh,$Xl
 bge  Loop_4x

Ltail_4x:
 vpmsumd  $Xl,$Xh,$H4l  # H^4.loXi.lo
 vpmsumd  $Xm,$Xh,$H4  # H^4.hiXi.lo+H^4.loXi.hi
 vpmsumd  $Xh,$Xh,$H4h  # H^4.hiXi.hi

 vxor  $Xl,$Xl,$Xl3
 vxor  $Xm,$Xm,$Xm3

 vpmsumd  $t2,$Xl,$xC2  # 1st reduction phase

 vsldoi  $t0,$Xm,$zero,8
 vsldoi  $t1,$zero,$Xm,8
  vxor  $Xh,$Xh,$Xh3
 vxor  $Xl,$Xl,$t0
 vxor  $Xh,$Xh,$t1

 vsldoi  $Xl,$Xl,$Xl,8
 vxor  $Xl,$Xl,$t2

 vsldoi  $t1,$Xl,$Xl,8  # 2nd reduction phase
 vpmsumd  $Xl,$Xl,$xC2
 vxor  $t1,$t1,$Xh
 vxor  $Xl,$Xl,$t1

 addic.  $len,$len,4
 beq  Ldone_4x

 lvx_u  $IN0,0,$inp
 ${UCMP}i $len,2
 li  $len,-4
 blt  Lone
 lvx_u  $IN1,r8,$inp
 beq  Ltwo

Lthree:
 lvx_u  $IN2,r9,$inp
 le?vperm $IN0,$IN0,$IN0,$lemask
 le?vperm $IN1,$IN1,$IN1,$lemask
 le?vperm $IN2,$IN2,$IN2,$lemask

 vxor  $Xh,$IN0,$Xl
 vmr  $H4l,$H3l
 vmr  $H4, $H3
 vmr  $H4h,$H3h

 vperm  $t0,$IN1,$IN2,$loperm
 vperm  $t1,$IN1,$IN2,$hiperm
 vpmsumd  $Xm2,$IN1,$H2  # H^2.loXi+1.hi+H^2.hiXi+1.lo
 vpmsumd  $Xm3,$IN2,$H  # H.hiXi+2.lo  +H.loXi+2.hi
 vpmsumd  $Xl3,$t0,$H21l  # H^2.loXi+1.lo+H.loXi+2.lo
 vpmsumd  $Xh3,$t1,$H21h  # H^2.hiXi+1.hi+H.hiXi+2.hi

 vxor  $Xm3,$Xm3,$Xm2
 b  Ltail_4x

.align 4
Ltwo:
 le?vperm $IN0,$IN0,$IN0,$lemask
 le?vperm $IN1,$IN1,$IN1,$lemask

 vxor  $Xh,$IN0,$Xl
 vperm  $t0,$zero,$IN1,$loperm
 vperm  $t1,$zero,$IN1,$hiperm

 vsldoi  $H4l,$zero,$H2,8
 vmr  $H4, $H2
 vsldoi  $H4h,$H2,$zero,8

 vpmsumd  $Xl3,$t0, $H21l  # H.loXi+1.lo
 vpmsumd  $Xm3,$IN1,$H  # H.hiXi+1.lo+H.loXi+2.hi
 vpmsumd  $Xh3,$t1, $H21h  # H.hiXi+1.hi

 b  Ltail_4x

.align 4
Lone:
 le?vperm $IN0,$IN0,$IN0,$lemask

 vsldoi  $H4l,$zero,$H,8
 vmr  $H4, $H
 vsldoi  $H4h,$H,$zero,8

 vxor  $Xh,$IN0,$Xl
 vxor  $Xl3,$Xl3,$Xl3
 vxor  $Xm3,$Xm3,$Xm3
 vxor  $Xh3,$Xh3,$Xh3

 b  Ltail_4x

Ldone_4x:
 le?vperm $Xl,$Xl,$Xl,$lemask
 stvx_u  $Xl,0,$Xip  # write out Xi

 li  r10,`15+6*$SIZE_T`
 li  r11,`31+6*$SIZE_T`
 mtspr  256,$vrsave
 lvx  v20,r10,$sp
 addi  r10,r10,32
 lvx  v21,r11,$sp
 addi  r11,r11,32
 lvx  v22,r10,$sp
 addi  r10,r10,32
 lvx  v23,r11,$sp
 addi  r11,r11,32
 lvx  v24,r10,$sp
 addi  r10,r10,32
 lvx  v25,r11,$sp
 addi  r11,r11,32
 lvx  v26,r10,$sp
 addi  r10,r10,32
 lvx  v27,r11,$sp
 addi  r11,r11,32
 lvx  v28,r10,$sp
 addi  r10,r10,32
 lvx  v29,r11,$sp
 addi  r11,r11,32
 lvx  v30,r10,$sp
 lvx  v31,r11,$sp
 addi  $sp,$sp,$FRAME
 blr
 .long  0
 .byte  0,12,0x04,0,0x80,0,4,0
 .long  0
___
}
$code.=<<___;
.size .gcm_ghash_p8,.-.gcm_ghash_p8

.asciz  "GHASH for PowerISA 2.07, CRYPTOGAMS by <appro\@openssl.org>"
.align  2
___

foreach (split("\n",$code)) {
 s/\`([^\`]*)\`/eval $1/geo;

 if ($flavour =~ /le$/o) { # little-endian
     s/le\?//o  or
     s/be\?/#be#/o;
 } else {
     s/le\?/#le#/o or
     s/be\?//o;
 }
 print $_,"\n";
}

close STDOUT; # enforce flush
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghashp8-ppc.pl
No license file was found, but licenses were detected in source scan.

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions

```
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
/* ====================================================================
* Copyright (c) 2003 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_randtest.c

No license file was found, but licenses were detected in source scan.

```
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rsa/fips_rsa_selftest.c
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2003 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/sha/fips_standalone_sha1.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/des/fips_des_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/aes/fips_aes_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_rand.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/sha/fips_sha1_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_rand_selftest.c
No license file was found, but licenses were detected in source scan.

```
*         devices where such combination causes the infringement.
*
* The software is originally written by Sheueling Chang Shantz and
* Douglas Stebila of Sun Microsystems Laboratories.
*
*/
/* NOTE: This file is licensed pursuant to the OpenSSL license below
* and may be modified; but after modifications, the above covenant
* may no longer apply!  In such cases, the corresponding paragraph
* ["In addition, Sun covenants ... causes the infringement."] and
* this note can be edited out; but please keep the Sun copyright
* notice and attribution. */
/* ====================================================================
* Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_gf2m.c
No license file was found, but licenses were detected in source scan.

```
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/cfb128.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/cbc128.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/ctr128.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/ofb128.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1999 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/stack/safestack.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/symhacks.h

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2004 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/des/fips_desmovs.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/aes/fips_aesavs.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1999-2007 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/md32_common.h
No license file was found, but licenses were detected in source scan.

```
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
*/
/* ====================================================================
* Copyright 2011 Thursby Software Systems, Inc. All rights reserved.
*
* The portions of the attached software ("Contribution") is developed by
* Thursby Software Systems, Inc and is licensed pursuant to the OpenSSL
* open source license.
*
* The Contribution, originally written by Paul W. Nelson of
* Thursby Software Systems, Inc, consists of the fingerprint calculation
* required for the FIPS140 integrity check.
*
* No patent licenses or other rights except those expressly stated in
* the OpenSSL open source license shall be deemed granted or received
* expressly, by implication, estoppel, or otherwise.
*
* No assurances are provided by Thursby that the Contribution does not
* infringe the patent or other intellectual property rights of any third
* party or that the license provides you with all the necessary rights
* to make use of the Contribution.
*
* THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. IN
* ADDITION TO THE DISCLAIMERS INCLUDED IN THE LICENSE, THURSBY
* SPECIFICALLY DISCLAIMS ANY LIABILITY FOR CLAIMS BROUGHT BY YOU OR ANY
* OTHER ENTITY BASED ON INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OR
* OTHERWISE.
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/iOS/incore_macho.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2006 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
* ECDH support in OpenSSL originally developed by
* SUN MICROSYSTEMS, INC., and contributed to the OpenSSL project.
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/thr_id.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/crypto.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/cryptlib.c

No license file was found, but licenses were detected in source scan.

```
/*.c>, <crypto/*/*.c>, <ssl/*.c>, <apps/*.c>)
              When this option is NOT specified, the filelist is taken from
              the commandline instead. Here, wildcards may be embedded. (Be
              sure to escape those to prevent the shell from expanding them
              for you when you wish mkerr.pl to do so instead.)
              Default: take file list to scan from the command line.

 -reindex     Discard the numeric values previously assigned to the error
              and function codes as extracted from the scanned header files;
              instead renumber all of them starting from 100. (Note that
              the numbers assigned through 'R' records in the config file
              remain intact.)
              Default: keep previously assigned numbers. (You are warned
                       when collisions are detected.)

 -nostatic    Generates a different source code, where these additional
              functions are generated for each library specified in the
              config file:
                void ERR_load_<LIB>_strings(void);
                void ERR_unload_<LIB>_strings(void);
                void ERR_<LIB>_error(int f, int r, char *fn, int ln);
```

```
  #define <LIB>err(f,r) ERR_<LIB>_error(f,r,__FILE__,__LINE__)
             while the code facilitates the use of these in an environment
             where the error support routines are dynamically loaded at
             runtime.
             Default: 'static' code generation.

 -staticloader Prefix generated functions with the 'static' scope modifier.
             Default: don't write any scope modifier prefix.

 -write      Actually (over)write the generated code to the header and C
             source files as assigned to each library through the config
             file.
             Default: don't write.

 -help / -h / -? / --help          Show this help text.

 ...         Additional arguments are added to the file list to scan,
             assuming '-recurse' was NOT specified on the command line.

EOF
  exit 1;
 } else {
  last;
 }
}

if($recurse) {
 @source = ( <crypto/*.c>, <crypto/*/*.c>, <ssl/*.c>,
   <fips/*.c>, <fips/*/*.c>);
} else {
 @source = @ARGV;
}

# Read in the config file

open(IN, "<$config") || die "Can't open config file $config";

# Parse config file

while(<IN>)
{
 if(/^L\s+(\S+)\s+(\S+)\s+(\S+)/) {
  $hinc{$1} = $2;
  $libinc{$2} = $1;
  $cskip{$3} = $1;
  if($3 ne "NONE") {
   $csrc{$1} = $3;
   $fmax{$1} = 100;
   $rmax{$1} = 100;
   $fassigned{$1} = ":";
   $rassigned{$1} = ":";
   $fnew{$1} = 0;
   $rnew{$1} = 0;
  }
 } elsif (/^F\s+(\S+)/) {
 # Add extra function with $1
 } elsif (/^R\s+(\S+)\s+(\S+)/) {
  $rextra{$1} = $2;
  $rcodes{$1} = $2;
 }
}

close IN;

# Scan each header file in turn and make a list of error codes
# and function names

while (($hdr, $lib) = each %libinc)
{
 next if($hdr eq "NONE");
 print STDERR "Scanning header file $hdr\n" if $debug;
 my $line = "", $def= "", $linenr = 0, $gotfile = 0;
 if (open(IN, "<$hdr")) {
     $gotfile = 1;
     while(<IN>) {
  $linenr++;
  print STDERR "line: $linenr\r" if $debug;

  last if(/BEGIN\s+ERROR\s+CODES/);
  if ($line ne '') {
      $_ = $line . $_;
      $line = '';
  }

  if (/\\$/) {
      $line = $_;
      next;
  }

  if(/\/\*/) {
      if (not /\*\//) {  # multiline comment...
   $line = $_;  # ... just accumulate
   next;
      } else {
   s/\/\*.*?\*\///gs; # wipe it
      }
 }

 if ($cpp) {
     $cpp++ if /^#\s*if/;
     $cpp-- if /^#\s*endif/;
     next;
 }
 $cpp = 1 if /^#.*ifdef.*cplusplus/;  # skip "C" declaration

 next if (/^\#/);                      # skip preprocessor directives

 s/{[^{}]*}//gs;                       # ignore {} blocks

 if (/\{|\/\*/) { # Add a } so editor works...
     $line = $_;
 } else {
     $def .= $_;
 }
    }
}

print STDERR "                                  \r" if $debug;
      $defnr = 0;
# Delete any DECLARE_ macros
$def =~ s/DECLARE_\w+\([\w,\s]+\)//gs;
foreach (split /;/, $def) {
    $defnr++;
    print STDERR "def: $defnr\r" if $debug;

    # The goal is to collect function names from function declarations.

    s/^[\n\s]*//g;
    s/[\n\s]*$//g;

    # Skip over recognized non-function declarations
    next if(/typedef\W/ or /DECLARE_STACK_OF/ or /TYPEDEF_.*_OF/);

    # Remove STACK_OF(foo)
    s/STACK_OF\(\w+\)/void/;

    # Reduce argument lists to empty ()
    # fold round brackets recursively: (t(*v)(t),t) -> (t{}{},t) -> {}
    while(/\(.*\)/s) {
 s/\([^\(\)]+\)/\{\}/gs;
 s/\(\s*\*\s*(\w+)\s*\{\}\s*\)/$1/gs; #(*f{}) -> f
    }
    # pretend as we didn't use curly braces: {} -> ()
    s/\{\}/\(\)/gs;
    if (/(\w+)\s*\(\).*/s) { # first token prior [first] () is
 my $name = $1;  # a function name!
 $name =~ tr/[a-z]/[A-Z]/;
 $ftrans{$name} = $1;
    } elsif (/[\(\)]/ and not (/=/)) {
 print STDERR "Header $hdr: cannot parse: $_;\n";
    }
}

print STDERR "                                   \r" if $debug;

next if $reindex;

# Scan function and reason codes and store them: keep a note of the
# maximum code used.

if ($gotfile) {
  while(<IN>) {
 if(/^\#define\s+(\S+)\s+(\S+)/) {
  $name = $1;
  $code = $2;
  next if $name =~ /^${lib}err/;
  unless($name =~ /^${lib}_([RF])_(\w+)$/) {
   print STDERR "Invalid error code $name\n";
   next;
  }
  if($1 eq "R") {
   $rcodes{$name} = $code;
   if ($rassigned{$lib} =~ /:$code:/) {
    print STDERR "!! ERROR: $lib reason code $code assigned twice (collision at $name)\n";
    ++$errcount;
   }
   $rassigned{$lib} .= "$code:";
   if(!(exists $rextra{$name}) &&
     ($code > $rmax{$lib}) ) {
    $rmax{$lib} = $code;
   }
  } else {
   if ($fassigned{$lib} =~ /:$code:/) {
    print STDERR "!! ERROR: $lib function code $code assigned twice (collision at $name)\n";
    ++$errcount;
   }
   $fassigned{$lib} .= "$code:";
   if($code > $fmax{$lib}) {
    $fmax{$lib} = $code;
   }
   $fcodes{$name} = $code;
```

```
    }
   }
    }
   }

   if ($debug) {
    if (defined($fmax{$lib})) {
     print STDERR "Max function code fmax" . "{" . "$lib" . "} = $fmax{$lib}\n";
     $fassigned{$lib} =~ m/^:(.*):$/;
     @fassigned = sort {$a <=> $b} split(":", $1);
     print STDERR "  @fassigned\n";
    }
    if (defined($rmax{$lib})) {
     print STDERR "Max reason code rmax" . "{" . "$lib" . "} = $rmax{$lib}\n";
     $rassigned{$lib} =~ m/^:(.*):$/;
     @rassigned = sort {$a <=> $b} split(":", $1);
     print STDERR "  @rassigned\n";
    }
   }

   if ($lib eq "SSL") {
    if ($rmax{$lib} >= 1000) {
     print STDERR "!! ERROR: SSL error codes 1000+ are reserved for alerts.\n";
     print STDERR "!!        Any new alerts must be added to $config.\n";
     ++$errcount;
     print STDERR "\n";
    }
   }
   close IN;
  }

  # Scan each C source file and look for function and reason codes
  # This is done by looking for strings that "look like" function or
  # reason codes: basically anything consisting of all upper case and
  # numerics which has _F_ or _R_ in it and which has the name of an
  # error library at the start. This seems to work fine except for the
  # oddly named structure BIO_F_CTX which needs to be ignored.
  # If a code doesn't exist in list compiled from headers then mark it
  # with the value "X" as a place holder to give it a value later.
  # Store all function and reason codes found in %ufcodes and %urcodes
  # so all those unreferenced can be printed out.


  foreach $file (@source) {
   # Don't parse the error source file.
   next if exists $cskip{$file};
   print STDERR "File loaded: ".$file."\r" if $debug;
   open(IN, "<$file") || die "Can't open source file $file\n";
```

```
 while(<IN>) {
  # skip obsoleted source files entirely!
  last if(/^#error\s+obsolete/);

  if(/((([A-Z0-9]+)_F_([A-Z0-9_]+))/) {
   next unless exists $csrc{$2};
   next if($1 eq "BIO_F_BUFFER_CTX");
   $ufcodes{$1} = 1;
   if(!exists $fcodes{$1}) {
    $fcodes{$1} = "X";
    $fnew{$2}++;
   }
   $notrans{$1} = 1 unless exists $ftrans{$3};
   print STDERR "Function: $1\t= $fcodes{$1} (lib: $2, name: $3)\n" if $debug;
  }
  if(/((([A-Z0-9]+)_R_[A-Z0-9_]+)/) {
   next unless exists $csrc{$2};
   $urcodes{$1} = 1;
   if(!exists $rcodes{$1}) {
    $rcodes{$1} = "X";
    $rnew{$2}++;
   }
   print STDERR "Reason: $1\t= $rcodes{$1} (lib: $2)\n" if $debug;
  }
 }
 close IN;
}
print STDERR "                                \n" if $debug;

# Now process each library in turn.

foreach $lib (keys %csrc)
{
 my $hfile = $hinc{$lib};
 my $cfile = $csrc{$lib};
 if(!$fnew{$lib} && !$rnew{$lib}) {
  print STDERR "$lib:\t\tNo new error codes\n";
  next unless $rebuild;
 } else {
  print STDERR "$lib:\t\t$fnew{$lib} New Functions,";
  print STDERR " $rnew{$lib} New Reasons.\n";
  next unless $dowrite;
 }

 # If we get here then we have some new error codes so we
 # need to rebuild the header file and C file.

 # Make a sorted list of error and reason codes for later use.
 my @function = sort grep(/^${lib}_/,keys %fcodes);
 my @reasons = sort grep(/^${lib}_/,keys %rcodes);

 # Rewrite the header file

 if (open(IN, "<$hfile")) {
     # Copy across the old file
     while(<IN>) {
  push @out, $_;
  last if (/BEGIN ERROR CODES/);
     }
     close IN;
 } else {
     push @out,
"/* ====================================================================\n",
" * Copyright (c) 2001-2011 The OpenSSL Project.  All rights reserved.\n",
" *\n",
" * Redistribution and use in source and binary forms, with or without\n",
" * modification, are permitted provided that the following conditions\n",
" * are met:\n",
" *\n",
" * 1. Redistributions of source code must retain the above copyright\n",
" *    notice, this list of conditions and the following disclaimer. \n",
" *\n",
" * 2. Redistributions in binary form must reproduce the above copyright\n",
" *    notice, this list of conditions and the following disclaimer in\n",
" *    the documentation and/or other materials provided with the\n",
" *    distribution.\n",
" *\n",
" * 3. All advertising materials mentioning features or use of this\n",
" *    software must display the following acknowledgment:\n",
" *    \"This product includes software developed by the OpenSSL Project\n",
" *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)\"\n",
" *\n",
" * 4. The names \"OpenSSL Toolkit\" and \"OpenSSL Project\" must not be used to\n",
" *    endorse or promote products derived from this software without\n",
" *    prior written permission. For written permission, please contact\n",
" *    openssl-core\@openssl.org.\n",
" *\n",
" * 5. Products derived from this software may not be called \"OpenSSL\"\n",
" *    nor may \"OpenSSL\" appear in their names without prior written\n",
" *    permission of the OpenSSL Project.\n",
" *\n",
" * 6. Redistributions of any form whatsoever must retain the following\n",
" *    acknowledgment:\n",
" *    \"This product includes software developed by the OpenSSL Project\n",
" *    for use in the OpenSSL Toolkit (http://www.openssl.org/)\"\n",
" *\n",
" * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY\n",
" * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE\n",
" * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR\n",
" * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR\n",
" * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,\n",
" * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT\n",
" * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;\n",
" * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)\n",
" * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,\n",
" * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)\n",
" * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED\n",
" * OF THE POSSIBILITY OF SUCH DAMAGE.\n",
" * ====================================================================\n",
" *\n",
" * This product includes cryptographic software written by Eric Young\n",
" * (eay\@cryptsoft.com).  This product includes software written by Tim\n",
" * Hudson (tjh\@cryptsoft.com).\n",
" *\n",
" */\n",
"\n",
"#ifndef HEADER_${lib}_ERR_H\n",
"#define HEADER_${lib}_ERR_H\n",
"\n",
"#ifdef  __cplusplus\n",
"extern \"C\" {\n",
"#endif\n",
"\n",
"/* BEGIN ERROR CODES */\n";
 }
 open (OUT, ">$hfile") || die "Can't Open File $hfile for writing\n";

 print OUT @out;
 undef @out;
 print OUT <<"EOF";
/* The following lines are auto generated by the script mkerr.pl. Any changes
* made after this point may be overwritten when the script is next run.
*/
EOF
 if($static) {
  print OUT <<"EOF";
${staticloader}void ERR_load_${lib}_strings(void);

EOF
 } else {
  print OUT <<"EOF";
${staticloader}void ERR_load_${lib}_strings(void);
${staticloader}void ERR_unload_${lib}_strings(void);
${staticloader}void ERR_${lib}_error(int function, int reason, char *file, int line);
#define ${lib}err(f,r) ERR_${lib}_error((f),(r),__FILE__,__LINE__)

EOF
 }
 print OUT <<"EOF";
/* Error codes for the $lib functions. */

/* Function codes. */
EOF

 foreach $i (@function) {
  $z=6-int(length($i)/8);
  if($fcodes{$i} eq "X") {
   $fassigned{$lib} =~ m/^:([^:]*):/;
   $findcode = $1;
   if (!defined($findcode)) {
    $findcode = $fmax{$lib};
   }
   while ($fassigned{$lib} =~ m/:$findcode:/) {
    $findcode++;
   }
   $fcodes{$i} = $findcode;
   $fassigned{$lib} .= "$findcode:";
   print STDERR "New Function code $i\n" if $debug;
  }
  printf OUT "#define $i%s $fcodes{$i}\n","\t" x $z;
 }

 print OUT "\n/* Reason codes. */\n";

 foreach $i (@reasons) {
  $z=6-int(length($i)/8);
  if($rcodes{$i} eq "X") {
   $rassigned{$lib} =~ m/^:([^:]*):/;
   $findcode = $1;
   if (!defined($findcode)) {
    $findcode = $rmax{$lib};
   }
   while ($rassigned{$lib} =~ m/:$findcode:/) {
    $findcode++;
   }
   $rcodes{$i} = $findcode;
   $rassigned{$lib} .= "$findcode:";
   print STDERR "New Reason code   $i\n" if $debug;
  }
  printf OUT "#define $i%s $rcodes{$i}\n","\t" x $z;
 }
 print OUT <<"EOF";

#ifdef  __cplusplus
}
#endif
#endif
EOF
 close OUT;

 # Rewrite the C source file containing the error details.

 # First, read any existing reason string definitions:
 my %err_reason_strings;
 if (open(IN,"<$cfile")) {
  while (<IN>) {
   if (/\b(${lib}_R_\w*)\b.*\"(.*)\"/) {
    $err_reason_strings{$1} = $2;
   }
   if (/\b${lib}_F_(\w*)\b.*\"(.*)\"/) {
    if (!exists $ftrans{$1} && ($1 ne $2)) {
     print STDERR "WARNING: Mismatched function string $2\n";
     $ftrans{$1} = $2;
    }
   }
  }
  close(IN);
 }



 my $hincf;
 if($static) {
  $hfile =~ /([^\/]+)$/;
  $hincf = "<${hprefix}$1>";
 } else {
  $hincf = "\"$hfile\"";
 }

 # If static we know the error code at compile time so use it
 # in error definitions.

 if ($static)
  {
  $pack_errcode = "ERR_LIB_${lib}";
  $load_errcode = "0";
  }
 else
  {
  $pack_errcode = "0";
  $load_errcode = "ERR_LIB_${lib}";
  }



 open (OUT,">$cfile") || die "Can't open $cfile for writing";

 print OUT <<"EOF";
/* $cfile */
/* ====================================================================
* Copyright (c) 1999-2011 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core\@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay\@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh\@cryptsoft.com).
*
*/

/* NOTE: this file was auto generated by the mkerr.pl script: any changes
* made to it will be overwritten when the script next updates this file,
* only reason strings will be preserved.
*/

#include <stdio.h>
#include <openssl/err.h>
#include $hincf

/* BEGIN ERROR CODES */
#ifndef OPENSSL_NO_ERR

#define ERR_FUNC(func) ERR_PACK($pack_errcode,func,0)
#define ERR_REASON(reason) ERR_PACK($pack_errcode,0,reason)

static ERR_STRING_DATA ${lib}_str_functs[]=
 {
EOF
 # Add each function code: if a function name is found then use it.
 foreach $i (@function) {
  my $fn;
  $i =~ /^${lib}_F_(\S+)$/;
  $fn = $1;
  if(exists $ftrans{$fn}) {
   $fn = $ftrans{$fn};
  }
#  print OUT "{ERR_PACK($pack_errcode,$i,0),\t\"$fn\"},\n";
  print OUT "{ERR_FUNC($i),\t\"$fn\"},\n";
 }
 print OUT <<"EOF";
{0,NULL}
 };

static ERR_STRING_DATA ${lib}_str_reasons[]=
 {
EOF
 # Add each reason code.
 foreach $i (@reasons) {
  my $rn;
  my $rstr = "ERR_REASON($i)";
  my $nspc = 0;
  if (exists $err_reason_strings{$i}) {
   $rn = $err_reason_strings{$i};
  } else {
   $i =~ /^${lib}_R_(\S+)$/;
   $rn = $1;
   $rn =~ tr/_[A-Z]/ [a-z]/;
  }
  $nspc = 40 - length($rstr) unless length($rstr) > 40;
  $nspc = " " x $nspc;
  print OUT "{${rstr}${nspc},\"$rn\"},\n";
 }
if($static) {
 print OUT <<"EOF";
{0,NULL}
 };

#endif

${staticloader}void ERR_load_${lib}_strings(void)
 {
#ifndef OPENSSL_NO_ERR

 if (ERR_func_error_string(${lib}_str_functs[0].error) == NULL)
  {
  ERR_load_strings($load_errcode,${lib}_str_functs);
  ERR_load_strings($load_errcode,${lib}_str_reasons);
  }
#endif
 }
EOF
} else {
 print OUT <<"EOF";
{0,NULL}
 };

#endif

#ifdef ${lib}_LIB_NAME
static ERR_STRING_DATA ${lib}_lib_name[]=
       {
{0 ,${lib}_LIB_NAME},
{0,NULL}
 };
#endif


static int ${lib}_lib_error_code=0;
static int ${lib}_error_init=1;

${staticloader}void ERR_load_${lib}_strings(void)
 {
 if (${lib}_lib_error_code == 0)
  ${lib}_lib_error_code=ERR_get_next_error_library();

 if (${lib}_error_init)
  {
  ${lib}_error_init=0;
#ifndef OPENSSL_NO_ERR
  ERR_load_strings(${lib}_lib_error_code,${lib}_str_functs);
  ERR_load_strings(${lib}_lib_error_code,${lib}_str_reasons);
#endif

#ifdef ${lib}_LIB_NAME
  ${lib}_lib_name->error = ERR_PACK(${lib}_lib_error_code,0,0);
  ERR_load_strings(0,${lib}_lib_name);
#endif
  }
 }

${staticloader}void ERR_unload_${lib}_strings(void)
 {
 if (${lib}_error_init == 0)
  {
#ifndef OPENSSL_NO_ERR
  ERR_unload_strings(${lib}_lib_error_code,${lib}_str_functs);
  ERR_unload_strings(${lib}_lib_error_code,${lib}_str_reasons);
#endif

#ifdef ${lib}_LIB_NAME
  ERR_unload_strings(0,${lib}_lib_name);
#endif
  ${lib}_error_init=1;
  }
 }

${staticloader}void ERR_${lib}_error(int function, int reason, char *file, int line)
 {
 if (${lib}_lib_error_code == 0)
  ${lib}_lib_error_code=ERR_get_next_error_library();
 ERR_PUT_error(${lib}_lib_error_code,function,reason,file,line);
 }
EOF

}

 close OUT;
 undef %err_reason_strings;
}

if($debug && defined(%notrans)) {
 print STDERR "The following function codes were not translated:\n";
 foreach(sort keys %notrans)
 {
  print STDERR "$_\n";
 }
}

# Make a list of unreferenced function and reason codes

foreach (keys %fcodes) {
 push (@funref, $_) unless exists $ufcodes{$_};
}

foreach (keys %rcodes) {
 push (@runref, $_) unless exists $urcodes{$_};
}

if($debug && defined(@funref) ) {
 print STDERR "The following function codes were not referenced:\n";
 foreach(sort @funref)
 {
  print STDERR "$_\n";
 }
}

if($debug && defined(@runref) ) {
 print STDERR "The following reason codes were not referenced:\n";
 foreach(sort @runref)
 {
  print STDERR "$_\n";
 }
}

if($errcount) {
 print STDERR "There were errors, failing...\n\n";
 exit $errcount;
}
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/util/mkerr.pl
No license file was found, but licenses were detected in source scan.

```
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
/* ====================================================================
* Copyright (c) 1998-2006 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
*
* Portions of the attached software ("Contribution") are developed by
* SUN MICROSYSTEMS, INC., and are contributed to the OpenSSL project.
*
* The Contribution is licensed pursuant to the Eric Young open source
* license provided above.
*
* The binary polynomial arithmetic software is originally written by
* Sheueling Chang Shantz and Douglas Stebila of Sun Microsystems Laboratories.
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn.h

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2001 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/mem_clr.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ui/ui_compat.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ui/ui_locl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ui/ui.h

No license file was found, but licenses were detected in source scan.

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
/* ====================================================================
* Copyright (c) 1998-2006 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_eay.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/err/err.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_mont.c

No license file was found, but licenses were detected in source scan.

### Public domain ###

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/bsaes-x86_64.pl

No license file was found, but licenses were detected in source scan.

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@openssl.org> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# December 2011
#
# The module implements GCM GHASH function and underlying single
# multiplication operation in GF(2^128). Even though subroutines
# have _4bit suffix, they are not using any tables, but rely on
# hardware Galois Field Multiply support. Streamed GHASH processes
# byte in ~7 cycles, which is >6x faster than "4-bit" table-driven
# code compiled with TI's cl6x 6.0 with -mv6400+ -o2 flags. We are
# comparing apples vs. oranges, but compiler surely could have done
# better, because theoretical [though not necessarily achievable]
# estimate for "4-bit" table-driven implementation is ~12 cycles.

while (($output=shift) && ($output!~/\w[\w\-]*\.\w+$/)) {}
open STDOUT,">$output";

($Xip,$Htable,$inp,$len)=("A4","B4","A6","B6"); # arguments

($Z0,$Z1,$Z2,$Z3, $H0, $H1, $H2, $H3,
   $H0x,$H1x,$H2x,$H3x)=map("A$_",(16..27));
($H01u,$H01y,$H2u,$H3u, $H0y,$H1y,$H2y,$H3y,
   $H0z,$H1z,$H2z,$H3z)=map("B$_",(16..27));
($FF000000,$E10000)=("B30","B31");
($xip,$x0,$x1,$xib)=map("B$_",(6..9)); # $xip zaps $len
$xia="A9";
($rem,$res)=("B4","B5");  # $rem zaps $Htable

$code.=<<___;
 .text

 .asg B3,RA

 .if 0
 .global _gcm_gmult_1bit
_gcm_gmult_1bit:
 ADDAD $Htable,2,$Htable
 .endif
 .global _gcm_gmult_4bit
_gcm_gmult_4bit:
 .asmfunc
 LDDW *${Htable}[-1],$H1:$H0 ; H.lo
 LDDW *${Htable}[-2],$H3:$H2 ; H.hi
|| MV $Xip,${xip}  ; reassign Xi
|| MVK 15,B1   ; SPLOOPD constant

 MVK 0xE1,$E10000
|| LDBU *++${xip}[15],$x1 ; Xi[15]
 MVK 0xFF,$FF000000
|| LDBU *--${xip},$x0  ; Xi[14]
 SHL $E10000,16,$E10000 ; [pre-shifted] reduction polynomial
 SHL $FF000000,24,$FF000000 ; upper byte mask
|| BNOP ghash_loop?
|| MVK 1,B0   ; take a single spin

 PACKH2 $H0,$H1,$xia  ; pack H0' and H1's upper bytes
 AND $H2,$FF000000,$H2u ; H2's upper byte
 AND $H3,$FF000000,$H3u ; H3's upper byte
```

```
|| SHRU $H2u,8,$H2u
 SHRU $H3u,8,$H3u
|| ZERO $Z1:$Z0
 SHRU2 $xia,8,$H01u
|| ZERO $Z3:$Z2
 .endasmfunc

 .global _gcm_ghash_4bit
_gcm_ghash_4bit:
 .asmfunc
 LDDW *${Htable}[-1],$H1:$H0 ; H.lo
|| SHRU $len,4,B0  ; reassign len
 LDDW *${Htable}[-2],$H3:$H2 ; H.hi
|| MV $Xip,${xip}  ; reassign Xi
|| MVK 15,B1   ; SPLOOPD constant

 MVK 0xE1,$E10000
|| [B0] LDNDW *${inp}[1],$H1x:$H0x
 MVK 0xFF,$FF000000
|| [B0] LDNDW *${inp}++[2],$H3x:$H2x
 SHL $E10000,16,$E10000 ; [pre-shifted] reduction polynomial
|| LDDW *${xip}[1],$Z1:$Z0
 SHL $FF000000,24,$FF000000 ; upper byte mask
|| LDDW *${xip}[0],$Z3:$Z2

 PACKH2 $H0,$H1,$xia  ; pack H0' and H1's upper bytes
 AND $H2,$FF000000,$H2u ; H2's upper byte
 AND $H3,$FF000000,$H3u ; H3's upper byte
|| SHRU $H2u,8,$H2u
 SHRU $H3u,8,$H3u
 SHRU2 $xia,8,$H01u

|| [B0] XOR $H0x,$Z0,$Z0  ; Xi^=inp
|| [B0] XOR $H1x,$Z1,$Z1
 .if .LITTLE_ENDIAN
  [B0] XOR $H2x,$Z2,$Z2
|| [B0] XOR $H3x,$Z3,$Z3
|| [B0] SHRU $Z1,24,$xia  ; Xi[15], avoid cross-path stall
 STDW $Z1:$Z0,*${xip}[1]
|| [B0] SHRU $Z1,16,$x0  ; Xi[14]
|| [B0] ZERO $Z1:$Z0
 .else
  [B0] XOR $H2x,$Z2,$Z2
|| [B0] XOR $H3x,$Z3,$Z3
|| [B0] MV $Z0,$xia  ; Xi[15], avoid cross-path stall
 STDW $Z1:$Z0,*${xip}[1]
|| [B0] SHRU $Z0,8,$x0  ; Xi[14]
|| [B0] ZERO $Z1:$Z0
```

```
 .endif
 STDW $Z3:$Z2,*${xip}[0]
|| [B0] ZERO $Z3:$Z2
|| [B0] MV $xia,$x1
  [B0] ADDK 14,${xip}

ghash_loop?:
 SPLOOPD 6   ; 6*16+7
|| MVC B1,ILC
|| [B0] SUB B0,1,B0
|| ZERO A0
|| ADD $x1,$x1,$xib  ; SHL $x1,1,$xib
|| SHL $x1,1,$xia
___

########______________________________
#  0    D2.     M1          M2      |
#  1            M1                  |
#  2            M1          M2      |
#  3        D1. M1          M2      |
#  4        S1. L1                  |
#  5    S2  S1x L1          D2  L2  |______________________________
#  6/0          L1  S1      L2  S2x |D2.     M1          M2      |
#  7/1          L1  S1  D1x S2  M2  |        M1                  |
#  8/2              S1  L1x S2      |        M1          M2      |
#  9/3              S1  L1x         |    D1. M1          M2      |
# 10/4                  D1x         |    S1. L1                  |
# 11/5                              |S2  S1x L1          D2  L2  |_____________
# 12/6/0                D1x       __|        L1  S1      L2  S2x |D2.     ....
#    7/1                                     L1  S1  D1x S2  M2  |        ....
#    8/2                                         S1  L1x S2      |        ....
#####...                                         ................|............
$code.=<<___;
 XORMPY $H0,$xia,$H0x  ; 0 ; HXi[i]
|| XORMPY $H01u,$xib,$H01y
|| [A0] LDBU *--${xip},$x0
 XORMPY $H1,$xia,$H1x  ; 1
 XORMPY $H2,$xia,$H2x  ; 2
|| XORMPY $H2u,$xib,$H2y
 XORMPY $H3,$xia,$H3x  ; 3
|| XORMPY $H3u,$xib,$H3y
||[!A0] MVK.D 15,A0    ; *--${xip} counter
 XOR.L $H0x,$Z0,$Z0  ; 4 ; Z^=HXi[i]
|| [A0] SUB.S A0,1,A0
 XOR.L $H1x,$Z1,$Z1  ; 5
|| AND.D $H01y,$FF000000,$H0z
|| SWAP2.L $H01y,$H1y  ; ; SHL $H01y,16,$H1y
|| SHL $x0,1,$xib
|| SHL $x0,1,$xia

 XOR.L $H2x,$Z2,$Z2  ; 6/0 ; [0,0] in epilogue
|| SHL $Z0,1,$rem  ; ; rem=Z<<1
|| SHRMB.S $Z1,$Z0,$Z0  ; ; Z>>=8
|| AND.L $H1y,$FF000000,$H1z
 XOR.L $H3x,$Z3,$Z3  ; 7/1
|| SHRMB.S $Z2,$Z1,$Z1
|| XOR.D $H0z,$Z0,$Z0   ; merge upper byte products
|| AND.S $H2y,$FF000000,$H2z
|| XORMPY $E10000,$rem,$res ; ; implicit rem&0x1FE
 XOR.L $H1z,$Z1,$Z1  ; 8/2
|| SHRMB.S $Z3,$Z2,$Z2
|| AND.S $H3y,$FF000000,$H3z
 XOR.L $H2z,$Z2,$Z2  ; 9/3
|| SHRU $Z3,8,$Z3
 XOR.D $H3z,$Z3,$Z3  ; 10/4
 NOP    ; 11/5

 SPKERNEL 0,2
|| XOR.D $res,$Z3,$Z3  ; 12/6/0; Z^=res

 ; input pre-fetch is possible where D1 slot is available...
  [B0] LDNDW *${inp}[1],$H1x:$H0x ; 8/-
  [B0] LDNDW *${inp}++[2],$H3x:$H2x ; 9/-
 NOP    ; 10/-
 .if .LITTLE_ENDIAN
 SWAP2 $Z0,$Z1   ; 11/-
|| SWAP4 $Z1,$Z0
 SWAP4 $Z1,$Z1   ; 12/-
|| SWAP2 $Z0,$Z0
 SWAP2 $Z2,$Z3
|| SWAP4 $Z3,$Z2
||[!B0] BNOP RA
 SWAP4 $Z3,$Z3
|| SWAP2 $Z2,$Z2
|| [B0] BNOP ghash_loop?
  [B0] XOR $H0x,$Z0,$Z0  ; Xi^=inp
|| [B0] XOR $H1x,$Z1,$Z1
  [B0] XOR $H2x,$Z2,$Z2
|| [B0] XOR $H3x,$Z3,$Z3
|| [B0] SHRU $Z1,24,$xia  ; Xi[15], avoid cross-path stall
 STDW $Z1:$Z0,*${xip}[1]
|| [B0] SHRU $Z1,16,$x0  ; Xi[14]
|| [B0] ZERO $Z1:$Z0
 .else
 [!B0] BNOP RA   ; 11/-
  [B0] BNOP ghash_loop?  ; 12/-
  [B0] XOR $H0x,$Z0,$Z0  ; Xi^=inp
|| [B0] XOR $H1x,$Z1,$Z1
  [B0] XOR $H2x,$Z2,$Z2
|| [B0] XOR $H3x,$Z3,$Z3
|| [B0] MV $Z0,$xia  ; Xi[15], avoid cross-path stall
 STDW $Z1:$Z0,*${xip}[1]
|| [B0] SHRU $Z0,8,$x0  ; Xi[14]
|| [B0] ZERO $Z1:$Z0
 .endif
 STDW $Z3:$Z2,*${xip}[0]
|| [B0] ZERO $Z3:$Z2
|| [B0] MV $xia,$x1
  [B0] ADDK 14,${xip}
 .endasmfunc

 .sect .const
 .cstring "GHASH for C64x+, CRYPTOGAMS by <appro\@openssl.org>"
 .align 4
___

print $code;
close STDOUT;
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-c64xplus.pl
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2010 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use is governed by OpenSSL license.
* ====================================================================
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/modes_lcl.h
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
*
* The Elliptic Curve Public-Key Crypto Library (ECC Code) included
* herein is developed by SUN MICROSYSTEMS, INC., and is contributed
* to the OpenSSL project.
*
* The ECC Code is licensed pursuant to the OpenSSL open source
* license provided below.
*
* The software is originally written by Sheueling Chang Shantz and
* Douglas Stebila of Sun Microsystems Laboratories.
*
*/
/* ====================================================================
* Copyright (c) 1998-2005 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec2_smpl.c
No license file was found, but licenses were detected in source scan.

*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the rouines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_prime.pl
No license file was found, but licenses were detected in source scan.

/* ==
* Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright

```
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_ctx.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2000 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
```

```
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
```

* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_mod.c
No license file was found, but licenses were detected in source scan.

/* ==
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
*
* The Elliptic Curve Public-Key Crypto Library (ECC Code) included
* herein is developed by SUN MICROSYSTEMS, INC., and is contributed
* to the OpenSSL project.
*
* The ECC Code is licensed pursuant to the OpenSSL open source
* license provided below.
*
* The ECDH software is originally written by Douglas Stebila of
* Sun Microsystems Laboratories.
*
*/
/* ==
* Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in
*   the documentation and/or other materials provided with the
*   distribution.
*

* 3. All advertising materials mentioning features or use of this
*   software must display the following acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   openssl-core@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ecdh/ech_ossl.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ecdh/ech_key.c
No license file was found, but licenses were detected in source scan.

/* ==
* Copyright (c) 2008 The OpenSSL Project. All rights reserved.

*
* Rights for redistribution and usage in source and binary
* forms are granted according to the OpenSSL license.
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/modes.h
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/aes.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/aes_locl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/aes_ecb.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/aes_cbc.c
No license file was found, but licenses were detected in source scan.

*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
*/

#define FIPS_AUTH_KEY "etaonrishdlcupfm"
#define FIPS_AUTH_CRYPTO_OFFICER "7f92562d409c903322c0f94a1188ae8178339a4f"
#define FIPS_AUTH_CRYPTO_USER "cb6cbdaad26cd210a8b31a5d56a876ee1d51a96c"

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips_auth.in
No license file was found, but licenses were detected in source scan.

/*
* Copyright (c) 2004, Richard Levitte <richard@levitte.org>
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/o_dir.h
No license file was found, but licenses were detected in source scan.

```
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dsa/dsa_locl.h
No license file was found, but licenses were detected in source scan.

```
/**
* rijndael-alg-fst.c
*
* @version 3.0 (December 2000)
*
* Optimised ANSI C code for the Rijndael cipher (now AES)
*
* @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
* @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
* @author Paulo Barreto <paulo.barreto@terra.com.br>
*
* This code is hereby placed in the public domain.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS
* OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
* SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
* OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
* EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/aes_core.c
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ecp_mont.c
No license file was found, but licenses were detected in source scan.

*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the rouines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/hmac/hmac.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rand/rand.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_lib.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_recp.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_prime.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/sha1dgst.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/hmac/hmac.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/objects/objects.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-

2.0.16/crypto/bn/bn_asm.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_pk1.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/lhash/lhash.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dh/dh.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/cfb64ede.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/ncbc_enc.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_x931g.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_add.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/asn1/asn1.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dsa/dsa_key.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/stack/stack.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/e_os.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dsa/dsa.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/cryptlib.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_sqr.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/set_key.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/dsa/fips_dsatest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/rpc_des.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dh/dh_key.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_crpt.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_mul.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/ofb64ede.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/evp.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/m_sha1.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_ssl.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/asn1/asn1_mac.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-

2.0.16/crypto/des/cfb_enc.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_gen.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/cfb64enc.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dh/dh_check.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_word.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/des_enc.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/m_dss1.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dsa/dsa_ossl.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/fcrypt_b.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/m_dss.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/sha.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/des_ver.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/utl/fips_enc.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/e_null.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_div.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/ecb3_enc.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dsa/dsa_gen.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/util/add_cr.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/buffer/buf_str.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/buffer/buffer.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/sha_locl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_none.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_shift.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bio/bio.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/e_des3.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/spr.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/dh/dh_gen.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2011 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
```

* ==
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/dh/fips_dhvs.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbg_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_rand_lcl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbg_rand.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/ecdh/fips_ecdhvs.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/aes/fips_gcmtest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbgvs.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/utl/fips_lck.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbg_ctr.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/ecdsa/fips_ecdsavs.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbg_lib.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbg_hmac.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbg_hash.c
No license file was found, but licenses were detected in source scan.

*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ==
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
*
* Portions of the attached software ("Contribution") are developed by
* SUN MICROSYSTEMS, INC., and are contributed to the OpenSSL project.
*
* The Contribution is licensed pursuant to the OpenSSL open source
* license provided above.
*
* The elliptic curve binary polynomial software is originally written by
* Sheueling Chang Shantz and Douglas Stebila of Sun Microsystems Laboratories.
*

*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec.h
No license file was found, but licenses were detected in source scan.

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the rouines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

```
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
/* ====================================================================
* Copyright (c) 1998-2005 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_exp.c
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/des_locl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/objects/obj_dat.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/objects/objects.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/des.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/objects/obj_mac.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/objects/obj_dat.h

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
*
* The Elliptic Curve Public-Key Crypto Library (ECC Code) included
* herein is developed by SUN MICROSYSTEMS, INC., and is contributed
* to the OpenSSL project.
*
* The ECC Code is licensed pursuant to the OpenSSL open source
* license provided below.
*
* The ECDH software is originally written by Douglas Stebila of
* Sun Microsystems Laboratories.
*
*/
/* ====================================================================
* Copyright (c) 2000-2002 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
```

```
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ecdh/ecdh.h

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2010 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/gcm128.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2006 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
```

```
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_blind.c

No license file was found, but licenses were detected in source scan.

# project. The module is, however, dual licensed under OpenSSL and

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-parisc.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/ia64-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-parisc.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aesni-x86_64.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/armv4-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha256-c64x.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-armv8.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-x86_64.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghashv8-armx.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/s390x-gf2m.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-parisc.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/via-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-c64xplus.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-s390x.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-armv4-large.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha256-586.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/x86_64-gf2m.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-x86_64.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-mips.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha256-armv4.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-armv4.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-

2.0.16/crypto/bn/asm/s390x-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/sparcv9a-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aesni-x86.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/x86-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-s390x.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/x86_64-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-thumb.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-armv4.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/ppc-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/x86_64-mont5.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-c64x.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha256-c64xplus.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-armv4.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-586.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-x86.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-ia64.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512p8-ppc.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-s390x.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-alpha.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aesv8-armx.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-mips.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-ppc.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aesni-sha1-x86_64.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/ppc64-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-

2.0.16/crypto/sha/asm/sha1-sparcv9a.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-c64xplus.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-alpha.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-parisc.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/x86-gf2m.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-sparcv9.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-mips.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/mips-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-ppc.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-c64x.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/sparcv9-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-ia64.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-586.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-ia64.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-armv8.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-s390x.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/armv4-gf2m.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/parisc-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-586.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/asm/ghash-sparcv9.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/asm/alpha-mont.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-sparcv9.pl
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aes-x86_64.pl
No license file was found, but licenses were detected in source scan.

/* ==

```
* Copyright (c) 2010 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/utl/fips_err.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/cmac/cmac.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/utl/fips_mem.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/cmac/cmac.h
No license file was found, but licenses were detected in source scan.

```
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_nist.c

No license file was found, but licenses were detected in source scan.

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@openssl.org> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# SHA1 for C64x.
#
# November 2016
#
# This is fully-unrolled SHA1 implementation. It's 25% faster than
# one with compact loops, doesn't use in-memory ring buffer, as
# everything is accomodated in registers, and has "perfect" interrupt
# agility. Drawback is obviously the code size...

while (($output=shift) && ($output!~/^\w[\w\-]*\.\w+$/)) {}
open STDOUT,">$output";

($CTX,$INP,$NUM) = ("A4","B4","A6");  # arguments

($A,$B,$C,$D,$E, $Arot,$F,$F0,$K) = map("A$_",(16..20, 21..24));
@V = ($A,$B,$C,$D,$E);
@X = map("B$_",(16..31));
($Actx,$Bctx,$Cctx,$Dctx,$Ectx) = map("A$_",(3,6..9)); # zaps $NUM
```

```
sub BODY_00_19 {
my ($i,$a,$b,$c,$d,$e) = @_;
my $j = ($i+1)&15;

$code.=<<___    if ($i<14);
 ROTL $a,5,$Arot  ;; $i
|| AND $c,$b,$F
|| ANDN $d,$b,$F0
|| ADD $K,$e,$e  ; E+=K
||  LDNW *${INP}++,@X[$i+2]
 OR $F0,$F,$F  ; F_00_19(B,C,D)
|| ROTL $b,30,$b
||  SWAP2 @X[$i+1],@X[$i+1]
|| ADD @X[$i],$e,$e  ; E+=X[i]
 ADD $Arot,$e,$e  ; E+=rot(A,5)
||  SWAP4 @X[$i+1],@X[$i+1]
 ADD $F,$e,$e  ; E+=F_00_19(B,C,D)
___
$code.=<<___    if ($i==14);
 ROTL $a,5,$Arot  ;; $i
|| AND $c,$b,$F
|| ANDN $d,$b,$F0
|| ADD $K,$e,$e  ; E+=K
 OR $F0,$F,$F  ; F_00_19(B,C,D)
|| ROTL $b,30,$b
|| ADD @X[$i],$e,$e  ; E+=X[i]
||  SWAP2 @X[$i+1],@X[$i+1]
 ADD $Arot,$e,$e  ; E+=rot(A,5)
||  SWAP4 @X[$i+1],@X[$i+1]
 ADD $F,$e,$e  ; E+=F_00_19(B,C,D)
___
$code.=<<___    if ($i==15);
||  XOR @X[($j+2)&15],@X[$j],@X[$j]
 ROTL $a,5,$Arot  ;; $i
|| AND $c,$b,$F
|| ANDN $d,$b,$F0
|| ADD $K,$e,$e  ; E+=K
||  XOR @X[($j+8)&15],@X[$j],@X[$j]
 OR $F0,$F,$F  ; F_00_19(B,C,D)
|| ROTL $b,30,$b
|| ADD @X[$i],$e,$e  ; E+=X[i]
||  XOR @X[($j+13)&15],@X[$j],@X[$j]
 ADD $Arot,$e,$e  ; E+=rot(A,5)
||  ROTL @X[$j],1,@X[$j]
 ADD $F,$e,$e  ; E+=F_00_19(B,C,D)
___
$code.=<<___    if ($i>15);
```

```
||  XOR @X[($j+2)&15],@X[$j],@X[$j]
 ROTL $a,5,$Arot  ;; $i
|| AND $c,$b,$F
|| ANDN $d,$b,$F0
|| ADD $K,$e,$e  ; E+=K
||  XOR @X[($j+8)&15],@X[$j],@X[$j]
 OR $F0,$F,$F  ; F_00_19(B,C,D)
|| ROTL $b,30,$b
|| ADD @X[$i&15],$e,$e  ; E+=X[i]
||  XOR @X[($j+13)&15],@X[$j],@X[$j]
 ADD $Arot,$e,$e  ; E+=rot(A,5)
||  ROTL @X[$j],1,@X[$j]
 ADD $F,$e,$e  ; E+=F_00_19(B,C,D)
___
}

sub BODY_20_39 {
my ($i,$a,$b,$c,$d,$e) = @_;
my $j = ($i+1)&15;

$code.=<<___    if ($i<79);
||  XOR @X[($j+2)&15],@X[$j],@X[$j]
 ROTL $a,5,$Arot  ;; $i
|| XOR $c,$b,$F
|| ADD $K,$e,$e  ; E+=K
||  XOR @X[($j+8)&15],@X[$j],@X[$j]
 XOR $d,$F,$F  ; F_20_39(B,C,D)
|| ROTL $b,30,$b
|| ADD @X[$i&15],$e,$e  ; E+=X[i]
||  XOR @X[($j+13)&15],@X[$j],@X[$j]
 ADD $Arot,$e,$e  ; E+=rot(A,5)
||  ROTL @X[$j],1,@X[$j]
 ADD $F,$e,$e  ; E+=F_20_39(B,C,D)
___
$code.=<<___    if ($i==79);
|| [A0] B loop?
|| [A0] LDNW *${INP}++,@X[0]  ; pre-fetch input
 ROTL $a,5,$Arot  ;; $i
|| XOR $c,$b,$F
|| ADD $K,$e,$e  ; E+=K
|| [A0] LDNW *${INP}++,@X[1]
 XOR $d,$F,$F  ; F_20_39(B,C,D)
|| ROTL $b,30,$b
|| ADD @X[$i&15],$e,$e  ; E+=X[i]
 ADD $Arot,$e,$e  ; E+=rot(A,5)
 ADD $F,$e,$e  ; E+=F_20_39(B,C,D)
|| ADD $Bctx,$a,$a  ; accumulate context
|| ADD $Cctx,$b,$b
```

```
 ADD $Dctx,$c,$c
|| ADD $Ectx,$d,$d
|| ADD $Actx,$e,$e
;;===== branch to loop? is taken here
___
}

sub BODY_40_59 {
my ($i,$a,$b,$c,$d,$e) = @_;
my $j = ($i+1)&15;

$code.=<<___;
||  XOR @X[($j+2)&15],@X[$j],@X[$j]
 ROTL $a,5,$Arot  ;; $i
|| AND $c,$b,$F
|| AND $d,$b,$F0
|| ADD $K,$e,$e  ; E+=K
||  XOR @X[($j+8)&15],@X[$j],@X[$j]
 XOR $F0,$F,$F
|| AND $c,$d,$F0
|| ROTL $b,30,$b
||  XOR @X[($j+13)&15],@X[$j],@X[$j]
|| ADD @X[$i&15],$e,$e  ; E+=X[i]
 XOR $F0,$F,$F  ; F_40_59(B,C,D)
|| ADD $Arot,$e,$e  ; E+=rot(A,5)
||  ROTL @X[$j],1,@X[$j]
 ADD $F,$e,$e  ; E+=F_20_39(B,C,D)
___
}

$code=<<___;
 .text

 .if .ASSEMBLER_VERSION<7000000
 .asg 0,__TI_EABI__
 .endif
 .if __TI_EABI__
 .asg sha1_block_data_order,_sha1_block_data_order
 .endif

 .asg B3,RA
 .asg A15,FP
 .asg B15,SP

 .if .BIG_ENDIAN
 .asg MV,SWAP2
 .asg MV,SWAP4
 .endif
 .global _sha1_block_data_order
_sha1_block_data_order:
 .asmfunc
 MV $NUM,A0   ; reassign $NUM
 [!A0] BNOP RA   ; if ($NUM==0) return;
|| [A0] LDW *${CTX}[0],$A  ; load A-E...
  [A0] LDW *${CTX}[1],$B
  [A0] LDW *${CTX}[2],$C
  [A0] LDW *${CTX}[3],$D
  [A0] LDW *${CTX}[4],$E
  [A0] LDNW *${INP}++,@X[0]  ; pre-fetch input
  [A0] LDNW *${INP}++,@X[1]
 NOP 3

loop?:
 SUB A0,1,A0
|| MV $A,$Actx
|| MVD $B,$Bctx
|| SWAP2 @X[0],@X[0]
|| MVKL 0x5a827999,$K
 MVKH 0x5a827999,$K  ; K_00_19
|| MV $C,$Cctx
|| MV $D,$Dctx
|| MVD $E,$Ectx
|| SWAP4 @X[0],@X[0]
___
for ($i=0;$i<20;$i++) { &BODY_00_19($i,@V); unshift(@V,pop(@V)); }
$code.=<<___;
|| MVKL 0x6ed9eba1,$K
 MVKH 0x6ed9eba1,$K  ; K_20_39
___
for (;$i<40;$i++) { &BODY_20_39($i,@V); unshift(@V,pop(@V)); }
$code.=<<___;
|| MVKL 0x8f1bbcdc,$K
 MVKH 0x8f1bbcdc,$K  ; K_40_59
___
for (;$i<60;$i++) { &BODY_40_59($i,@V); unshift(@V,pop(@V)); }
$code.=<<___;
|| MVKL 0xca62c1d6,$K
 MVKH 0xca62c1d6,$K  ; K_60_79
___
for (;$i<80;$i++) { &BODY_20_39($i,@V); unshift(@V,pop(@V)); }
$code.=<<___;
 BNOP RA   ; return
 STW $A,*${CTX}[0]  ; emit A-E...
 STW $B,*${CTX}[1]
 STW $C,*${CTX}[2]
 STW $D,*${CTX}[3]
 STW $E,*${CTX}[4]
 .endasmfunc

 .sect .const
 .cstring "SHA1 block transform for C64x, CRYPTOGAMS by <appro\@openssl.org>"
 .align 4
___

print $code;
close STDOUT;
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha1-c64x-large.pl
No license file was found, but licenses were detected in source scan.

```
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/e_aes.c
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec_cvt.c
No license file was found, but licenses were detected in source scan.

#! /usr/bin/env perl

```
# Copyright 2016 The OpenSSL Project Authors. All Rights Reserved.
#
# Licensed under the OpenSSL license (the "License").  You may not use
# this file except in compliance with the License.  You can obtain a copy
# in the file LICENSE in the source distribution or at
# https://www.openssl.org/source/license.html

while (($output=shift) && ($output!~/\w[\w\-]*\.\w+$/)) {}
open STDOUT,">$output";

$code.=<<___;
 .text

 .if .ASSEMBLER_VERSION<7000000
 .asg 0,__TI_EABI__
 .endif
 .if __TI_EABI__
 .asg OPENSSL_rdtsc,_OPENSSL_rdtsc
 .asg OPENSSL_cleanse,_OPENSSL_cleanse
 .asg CRYPTO_memcmp,_CRYPTO_memcmp
 .asg OPENSSL_atomic_add,_OPENSSL_atomic_add
 .asg OPENSSL_wipe_cpu,_OPENSSL_wipe_cpu
 .asg OPENSSL_instrument_bus,_OPENSSL_instrument_bus
 .asg OPENSSL_instrument_bus2,_OPENSSL_instrument_bus2
 .endif

 .asg B3,RA
 .asg 0x01AC0000,TIMER_BASE ; Timer 2

 .global _OPENSSL_rdtsc
_OPENSSL_rdtsc:
 .asmfunc
 MVKL TIMER_BASE,A5
 MVKH TIMER_BASE,A5
 LDW *A5[0],A2 ; load CTL
 LDW *A5[2],A4 ; load CTN
 NOP 2
 .if .BIG_ENDIAN
 MVK 0x2c0,A7 ; internal clock source, don't hold, go
|| MVK -1,A6  ; maximum period
 .else
 MVK 0x2c0,A6 ; internal clock source, don't hold, go
|| MVK -1,A7  ; maximum period
 .endif
 [!A2] STDW A7:A6,*A5[0] ; fire it up
|| BNOP RA,5
 .endasmfunc
 .global _OPENSSL_cleanse
_OPENSSL_cleanse:
 .asmfunc
 ZERO A3:A2
|| ZERO B2
|| SHRU B4,3,B0  ; is length >= 8
|| ADD 1,A4,B6
 [!B0] BNOP RA
|| [B0] SUB B0,1,B2
|| ZERO A1
|| ZERO B1
  [B2] BDEC cleanse_loop?,B2
||[!B0] CMPLT 0,B4,A1
||[!B0] CMPLT 1,B4,B1
|| ZERO B5
  [A1] STB A2,*A4++[2]
|| [B1] STB B5,*B6++[2]
|| [B2] BDEC cleanse_loop?,B2
||[!B0] CMPLT 2,B4,A1
||[!B0] CMPLT 3,B4,B1
  [A1] STB A2,*A4++[2]
|| [B1] STB B5,*B6++[2]
|| [B2] BDEC cleanse_loop?,B2
||[!B0] CMPLT 4,B4,A1
||[!B0] CMPLT 5,B4,B1
  [A1] STB A2,*A4++[2]
|| [B1] STB B5,*B6++[2]
|| [B2] BDEC cleanse_loop?,B2
||[!B0] CMPLT 6,B4,A1
  [A1] STB A2,*A4++[2]
|| [B2] BDEC cleanse_loop?,B2

cleanse_loop?:
 STNDW A3:A2,*A4++
|| SUB B4,8,B4
|| [B2] BDEC cleanse_loop?,B2

 MV B4,B0  ; remaining bytes
|| ADD 1,A4,B6
|| BNOP RA
  [B0] CMPLT 0,B0,A1
|| [B0] CMPLT 1,B0,B1
  [A1] STB A2,*A4++[2]
|| [B1] STB B5,*B6++[2]
|| [B0] CMPLT 2,B0,A1
|| [B0] CMPLT 3,B0,B1
  [A1] STB A2,*A4++[2]
|| [B1] STB B5,*B6++[2]
|| [B0] CMPLT 4,B0,A1
|| [B0] CMPLT 5,B0,B1
  [A1] STB A2,*A4++[2]
|| [B1] STB B5,*B6++[2]
|| [B0] CMPLT 6,B0,A1
  [A1] STB A2,*A4++[2]
 .endasmfunc

 .if 0
 .global _CRYPTO_memcmp
_CRYPTO_memcmp:
 .asmfunc
 MV A6,B0
 [!B0] BNOP RA
||[!B0] ZERO A4
|| [B0] ZERO A1:A0
  [B0] LDBU *A4++,A5
|| [B0] LDBU *B4++,B5
|| [B0] BDEC memcmp_loop?,B0
  [B0] LDBU *A4++,A5
|| [B0] LDBU *B4++,B5
|| [B0] BDEC memcmp_loop?,B0
  [B0] LDBU *A4++,A5
|| [B0] LDBU *B4++,B5
|| [B0] BDEC memcmp_loop?,B0
  [B0] LDBU *A4++,A5
|| [B0] LDBU *B4++,B5
|| [B0] BDEC memcmp_loop?,B0
  [B0] LDBU *A4++,A5
|| [B0] LDBU *B4++,B5
|| [B0] BDEC memcmp_loop?,B0
 XOR A5,B5,A1
|| [B0] LDBU *A4++,A5
|| [B0] LDBU *B4++,B5
|| [B0] BDEC memcmp_loop?,B0

memcmp_loop?:
 OR A1,A0,A0
|| XOR A5,B5,A1
|| [B0] LDBU *A4++,A5
|| [B0] LDBU *B4++,B5
|| [B0] BDEC memcmp_loop?,B0

 BNOP RA,3
 ZERO A4
 [A0] MVK 1,A4
 .endasmfunc
 .endif
 .global _OPENSSL_atomic_add
_OPENSSL_atomic_add:
 .asmfunc
 BNOP atomic_store? ; pre-C64x+ systems are uni-processor, it's
|| LDW *A4,B5  ; enough to hold interrupts off through
    ; the load-update-store cycle to achieve
    ; atomicity
 NOP
 BNOP RA,3  ; and this branch stretches even over store
 ADD B4,B5,B5
atomic_store?:
 STW B5,*A4
|| MV B5,A4
 .endasmfunc

 .global _OPENSSL_wipe_cpu
_OPENSSL_wipe_cpu:
 .asmfunc
 ZERO A0
|| ZERO B0
|| ZERO A1
|| ZERO B1
 ZERO A3:A2
|| MVD B0,B2
|| ZERO A4
|| ZERO B4
|| ZERO A5
|| ZERO B5
|| BNOP RA
 ZERO A7:A6
|| ZERO B7:B6
|| ZERO A8
|| ZERO B8
|| ZERO A9
|| ZERO B9
 ZERO A17:A16
|| ZERO B17:B16
|| ZERO A18
|| ZERO B18
|| ZERO A19
|| ZERO B19
 ZERO A21:A20
|| ZERO B21:B20
|| ZERO A22
|| ZERO B22
|| ZERO A23
|| ZERO B23
```

```
 ZERO A25:A24
|| ZERO B25:B24
|| ZERO A26
|| ZERO B26
|| ZERO A27
|| ZERO B27
 ZERO A29:A28
|| ZERO B29:B28
|| ZERO A30
|| ZERO B30
|| ZERO A31
|| ZERO B31
 .endasmfunc

CLFLUSH .macro CONTROL,ADDR,LEN
 B passthrough?
|| STW ADDR,*CONTROL[0]
 STW LEN,*CONTROL[1]
spinlock?:
 LDW *CONTROL[1],A0
 NOP 3
passthrough?:
 NOP
 [A0] BNOP spinlock?,5
 .endm

 .global _OPENSSL_instrument_bus
_OPENSSL_instrument_bus:
 .asmfunc
 MV B4,B0   ; reassign sizeof(output)
|| MV A4,B4   ; reassign output
|| MVK 0x00004030,A3
|| MVKL TIMER_BASE,B16
 MV B0,A4   ; return value
|| MVK 1,A1
|| MVKH 0x01840000,A3  ; L1DWIBAR
|| MVKH TIMER_BASE,B16
 LDW *B16[2],B8  ; collect 1st tick
|| MVK 0x00004010,A5
 NOP 4
 MV B8,B9   ; lasttick = tick
|| MVK 0,B7   ; lastdiff = 0
|| MVKH 0x01840000,A5  ; L2WIBAR
 CLFLUSH A3,B4,A1  ; write-back and invalidate L1D line
 CLFLUSH A5,B4,A1  ; write-back and invalidate L2 line
 LDW *B4,B5
 NOP 4
 ADD B7,B5,B5
 STW B5,*B4
bus_loop1?:
 LDW *B16[2],B8
|| [B0] SUB B0,1,B0
 NOP 4
 SUB B8,B9,B7  ; lastdiff = tick - lasttick
|| MV B8,B9   ; lasttick = tick
 CLFLUSH A3,B4,A1  ; write-back and invalidate L1D line
 CLFLUSH A5,B4,A1  ; write-back and invalidate L2 line
 LDW *B4,B5
 NOP 4
 ADD B7,B5,B5
 STW B5,*B4   ; [!B1] is removed to flatten samples
|| ADDK 4,B4
|| [B0] BNOP bus_loop1?,5

 BNOP RA,5
 .endasmfunc

 .global _OPENSSL_instrument_bus2
_OPENSSL_instrument_bus2:
 .asmfunc
 MV A6,B0   ; reassign max
|| MV B4,A6   ; reassing sizeof(output)
|| MVK 0x00004030,A3
|| MVKL TIMER_BASE,B16
 MV A4,B4   ; reassign output
|| MVK 0,A4   ; return value
|| MVK 1,A1
|| MVKH 0x01840000,A3  ; L1DWIBAR
|| MVKH TIMER_BASE,B16

 LDW *B16[2],B8  ; collect 1st tick
|| MVK 0x00004010,A5
 NOP 4
 MV B8,B9   ; lasttick = tick
|| MVK 0,B7   ; lastdiff = 0
|| MVKH 0x01840000,A5  ; L2WIBAR
 CLFLUSH A3,B4,A1  ; write-back and invalidate L1D line
 CLFLUSH A5,B4,A1  ; write-back and invalidate L2 line
 LDW *B4,B5
 NOP 4
 ADD B7,B5,B5
 STW B5,*B4

 LDW *B16[2],B8  ; collect 1st diff
 NOP 4
 SUB B8,B9,B7  ; lastdiff = tick - lasttick
```

```
|| MV B8,B9   ; lasttick = tick
|| SUB B0,1,B0
bus_loop2?:
 CLFLUSH A3,B4,A1  ; write-back and invalidate L1D line
 CLFLUSH A5,B4,A1  ; write-back and invalidate L2 line
 LDW *B4,B5
 NOP 4
 ADD B7,B5,B5
 STW B5,*B4   ; [!B1] is removed to flatten samples
||[!B0] BNOP bus_loop2_done?,2
|| SUB B0,1,B0
 LDW *B16[2],B8
 NOP 4
 SUB B8,B9,B8
|| MV B8,B9
 CMPEQ B8,B7,B2
|| MV B8,B7
 [!B2] ADDAW B4,1,B4
||[!B2] ADDK 1,A4
 CMPEQ A4,A6,A2
 [!A2] BNOP bus_loop2?,5

bus_loop2_done?:
 BNOP RA,5
 .endasmfunc

 .if __TI_EABI__
 .sect ".init_array"
 .else
 .sect ".pinit"
 .endif
 .align 4
 .long _OPENSSL_rdtsc  ; auto-start timer
___

print $code;
close STDOUT;
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/c64xcpuid.pl
No license file was found, but licenses were detected in source scan.

```
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
```

```
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
/* ====================================================================
 * Copyright (c) 1998-2000 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_exp2.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_lcl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rand/rand_lcl.h
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/des/des_old.h
No license file was found, but licenses were detected in source scan.

```
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rsa/fips_rsa_sign.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rsa/fips_rsa_lib.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/dh/fips_dh_lib.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/ecdsa/fips_ecdsa_lib.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/dsa/fips_dsa_lib.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2003 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/o_str.h

No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/evp_locl.h
No license file was found, but licenses were detected in source scan.

```
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/dsa/fips_dsa_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips_auth.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips_post.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/hmac/fips_hmac_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips_utl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/cmac/fips_cmac_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/fips_locl.h
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_rand_lib.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2007 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
```

```
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
/* ====================================================================
 * Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
 * Portions of this software developed by SUN MICROSYSTEMS, INC.,
 * and contributed to the OpenSSL project.
 */
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec_mult.c

No license file was found, but licenses were detected in source scan.

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rsa/fips_rsagtest.c
No license file was found, but licenses were detected in source scan.

/*
 tlhelp32.h - Include file for Tool help functions.

 Written by Mumit Khan <khan@nanotech.wisc.edu>

 This file is part of a free library for the Win32 API.

 This library is distributed in the hope that it will be useful,
 but WITHOUT ANY WARRANTY; without even the implied warranty of
 MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/ms/tlhelp32.h
No license file was found, but licenses were detected in source scan.

/* ==
* Copyright (c) 2002-2006 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in
*   the documentation and/or other materials provided with the
*   distribution.

*
* 3. All advertising materials mentioning features or use of this
*   software must display the following acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/aes_ofb.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/aes_cfb.c
No license file was found, but licenses were detected in source scan.

/* ==
* Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions

```
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/evp/m_ecdsa.c
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_drbg_selftest.h
No license file was found, but licenses were detected in source scan.

```
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
* Portions of this software developed by SUN MICROSYSTEMS, INC.,
* and contributed to the OpenSSL project.
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ecp_nist.c
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
* Portions of this software developed by SUN MICROSYSTEMS, INC.,
* and contributed to the OpenSSL project.
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ecp_smpl.c

No license file was found, but licenses were detected in source scan.

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
/* ====================================================================
* Copyright (c) 1998-2001 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_prime.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_gcd.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/utl/fips_md.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_rand.c
No license file was found, but licenses were detected in source scan.

```
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rand/fips_rand.c
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 1998-2003 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
```

*
* 3. All advertising materials mentioning features or use of this
*   software must display the following acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
/* ==
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
* Binary polynomial ECC support in OpenSSL originally developed by
* SUN MICROSYSTEMS, INC., and contributed to the OpenSSL project.
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec_lib.c

No license file was found, but licenses were detected in source scan.

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@openssl.org> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# This module implements support for AES instructions as per PowerISA
# specification version 2.07, first implemented by POWER8 processor.
# The module is endian-agnostic in sense that it supports both big-
# and little-endian cases. Data alignment in parallelizable modes is
# handled with VSX loads and stores, which implies MSR.VSX flag being
# set. It should also be noted that ISA specification doesn't prohibit
# alignment exceptions for these instructions on page boundaries.
# Initially alignment was handled in pure AltiVec/VMX way [when data
# is aligned programmatically, which in turn guarantees exception-
# free execution], but it turned to hamper performance when vcipher
# instructions are interleaved. It's reckoned that eventual
# misalignment penalties at page boundaries are in average lower
# than additional overhead in pure AltiVec approach.
#
# May 2016
#
# Add XTS subroutine, 9x on little- and 12x improvement on big-endian
# systems were measured.
#
#########################################################################
# Current large-block performance in cycles per byte processed with
# 128-bit key (less is better).
#
#  CBC en-/decrypt CTR XTS
# POWER8[le] 3.96/0.72 0.74 1.1
# POWER8[be] 3.75/0.65 0.66 1.0

$flavour = shift;

if ($flavour =~ /64/) {
 $SIZE_T =8;
 $LRSAVE =2*$SIZE_T;
 $STU ="stdu";
 $POP ="ld";
 $PUSH ="std";
 $UCMP ="cmpld";
 $SHL ="sldi";
```

```
} elsif ($flavour =~ /32/) {
 $SIZE_T =4;
 $LRSAVE =$SIZE_T;
 $STU ="stwu";
 $POP ="lwz";
 $PUSH ="stw";
 $UCMP ="cmplw";
 $SHL ="slwi";
} else { die "nonsense $flavour"; }

$LITTLE_ENDIAN = ($flavour=~/le$/) ? $SIZE_T : 0;

$0 =~ m/(.*[\/\\])[^\/\\]+$/; $dir=$1;
( $xlate="${dir}ppc-xlate.pl" and -f $xlate ) or
( $xlate="${dir}../../perlasm/ppc-xlate.pl" and -f $xlate) or
die "can't locate ppc-xlate.pl";

open STDOUT,"| $^X $xlate $flavour ".shift || die "can't call $xlate: $!";

$FRAME=8*$SIZE_T;
$prefix="aes_p8";

$sp="r1";
$vrsave="r12";

########################################################################
{{{ # Key setup procedures      #
my ($inp,$bits,$out,$ptr,$cnt,$rounds)=map("r$_",(3..8));
my ($zero,$in0,$in1,$key,$rcon,$mask,$tmp)=map("v$_",(0..6));
my ($stage,$outperm,$outmask,$outhead,$outtail)=map("v$_",(7..11));

$code.=<<___;
.machine "any"

.text

.align 7
rcon:
.long 0x01000000, 0x01000000, 0x01000000, 0x01000000 ?rev
.long 0x1b000000, 0x1b000000, 0x1b000000, 0x1b000000 ?rev
.long 0x0d0e0f0c, 0x0d0e0f0c, 0x0d0e0f0c, 0x0d0e0f0c ?rev
.long 0,0,0,0      ?asis
Lconsts:
 mflr r0
 bcl 20,31,\$+4
 mflr $ptr  #vvvvv "distance between . and rcon
 addi $ptr,$ptr,-0x48
 mtlr r0
 blr
 .long 0
 .byte 0,12,0x14,0,0,0,0,0
.asciz "AES for PowerISA 2.07, CRYPTOGAMS by <appro\@openssl.org>"

.globl .${prefix}_set_encrypt_key
.align 5
.${prefix}_set_encrypt_key:
Lset_encrypt_key:
 mflr  r11
 $PUSH  r11,$LRSAVE($sp)

 li  $ptr,-1
 ${UCMP}i $inp,0
 beq-  Lenc_key_abort  # if ($inp==0) return -1;
 ${UCMP}i $out,0
 beq-  Lenc_key_abort  # if ($out==0) return -1;
 li  $ptr,-2
 cmpwi  $bits,128
 blt-  Lenc_key_abort
 cmpwi  $bits,256
 bgt-  Lenc_key_abort
 andi.  r0,$bits,0x3f
 bne-  Lenc_key_abort

 lis  r0,0xfff0
 mfspr  $vrsave,256
 mtspr  256,r0

 bl  Lconsts
 mtlr  r11

 neg  r9,$inp
 lvx  $in0,0,$inp
 addi  $inp,$inp,15  # 15 is not typo
 lvsr  $key,0,r9  # borrow $key
 li  r8,0x20
 cmpwi  $bits,192
 lvx  $in1,0,$inp
 le?vspltisb $mask,0x0f  # borrow $mask
 lvx  $rcon,0,$ptr
 le?vxor  $key,$key,$mask  # adjust for byte swap
 lvx  $mask,r8,$ptr
 addi  $ptr,$ptr,0x10
 vperm  $in0,$in0,$in1,$key # align [and byte swap in LE]
 li  $cnt,8
 vxor  $zero,$zero,$zero
 mtctr  $cnt
 ?lvsr  $outperm,0,$out
 vspltisb $outmask,-1
 lvx  $outhead,0,$out
 ?vperm  $outmask,$zero,$outmask,$outperm

 blt  Loop128
 addi  $inp,$inp,8
 beq  L192
 addi  $inp,$inp,8
 b  L256

.align 4
Loop128:
 vperm  $key,$in0,$in0,$mask # rotate-n-splat
 vsldoi  $tmp,$zero,$in0,12 # >>32
  vperm  $outtail,$in0,$in0,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
 vcipherlast $key,$key,$rcon
  stvx  $stage,0,$out
  addi  $out,$out,16

 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
  vadduwm $rcon,$rcon,$rcon
 vxor  $in0,$in0,$key
 bdnz  Loop128

 lvx  $rcon,0,$ptr  # last two round keys

 vperm  $key,$in0,$in0,$mask # rotate-n-splat
 vsldoi  $tmp,$zero,$in0,12 # >>32
  vperm  $outtail,$in0,$in0,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
 vcipherlast $key,$key,$rcon
  stvx  $stage,0,$out
  addi  $out,$out,16

 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
```

```
  vadduwm $rcon,$rcon,$rcon
 vxor  $in0,$in0,$key

 vperm  $key,$in0,$in0,$mask # rotate-n-splat
 vsldoi  $tmp,$zero,$in0,12 # >>32
  vperm  $outtail,$in0,$in0,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
 vcipherlast $key,$key,$rcon
  stvx  $stage,0,$out
  addi  $out,$out,16

 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
 vxor  $in0,$in0,$key
  vperm  $outtail,$in0,$in0,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
  stvx  $stage,0,$out

 addi  $inp,$out,15  # 15 is not typo
 addi  $out,$out,0x50

 li  $rounds,10
 b  Ldone

.align 4
L192:
 lvx  $tmp,0,$inp
 li  $cnt,4
  vperm  $outtail,$in0,$in0,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
  stvx  $stage,0,$out
  addi  $out,$out,16
 vperm  $in1,$in1,$tmp,$key # align [and byte swap in LE]
 vspltisb $key,8   # borrow $key
 mtctr  $cnt
 vsububm  $mask,$mask,$key # adjust the mask

Loop192:
 vperm  $key,$in1,$in1,$mask # roate-n-splat
 vsldoi  $tmp,$zero,$in0,12 # >>32
 vcipherlast $key,$key,$rcon
```

```
vxor  $in0,$in0,$tmp
vsldoi  $tmp,$zero,$tmp,12 # >>32
vxor  $in0,$in0,$tmp
vsldoi  $tmp,$zero,$tmp,12 # >>32
vxor  $in0,$in0,$tmp

 vsldoi  $stage,$zero,$in1,8
vspltw  $tmp,$in0,3
vxor  $tmp,$tmp,$in1
vsldoi  $in1,$zero,$in1,12 # >>32
 vadduwm $rcon,$rcon,$rcon
vxor  $in1,$in1,$tmp
vxor  $in0,$in0,$key
vxor  $in1,$in1,$key
 vsldoi  $stage,$stage,$in0,8

vperm  $key,$in1,$in1,$mask # rotate-n-splat
vsldoi  $tmp,$zero,$in0,12 # >>32
 vperm  $outtail,$stage,$stage,$outperm # rotate
 vsel  $stage,$outhead,$outtail,$outmask
 vmr  $outhead,$outtail
vcipherlast $key,$key,$rcon
 stvx  $stage,0,$out
 addi  $out,$out,16

 vsldoi  $stage,$in0,$in1,8
vxor  $in0,$in0,$tmp
vsldoi  $tmp,$zero,$tmp,12 # >>32
 vperm  $outtail,$stage,$stage,$outperm # rotate
 vsel  $stage,$outhead,$outtail,$outmask
 vmr  $outhead,$outtail
vxor  $in0,$in0,$tmp
vsldoi  $tmp,$zero,$tmp,12 # >>32
vxor  $in0,$in0,$tmp
 stvx  $stage,0,$out
 addi  $out,$out,16

vspltw  $tmp,$in0,3
vxor  $tmp,$tmp,$in1
vsldoi  $in1,$zero,$in1,12 # >>32
 vadduwm $rcon,$rcon,$rcon
vxor  $in1,$in1,$tmp
vxor  $in0,$in0,$key
vxor  $in1,$in1,$key
 vperm  $outtail,$in0,$in0,$outperm # rotate
 vsel  $stage,$outhead,$outtail,$outmask
 vmr  $outhead,$outtail
 stvx  $stage,0,$out
```

```
  addi  $inp,$out,15  # 15 is not typo
  addi  $out,$out,16
 bdnz  Loop192

 li  $rounds,12
 addi  $out,$out,0x20
 b  Ldone

.align 4
L256:
 lvx  $tmp,0,$inp
 li  $cnt,7
 li  $rounds,14
  vperm  $outtail,$in0,$in0,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
  stvx  $stage,0,$out
  addi  $out,$out,16
 vperm  $in1,$in1,$tmp,$key # align [and byte swap in LE]
 mtctr  $cnt

Loop256:
 vperm  $key,$in1,$in1,$mask # rotate-n-splat
 vsldoi  $tmp,$zero,$in0,12 # >>32
  vperm  $outtail,$in1,$in1,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
 vcipherlast $key,$key,$rcon
  stvx  $stage,0,$out
  addi  $out,$out,16

 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in0,$in0,$tmp
  vadduwm $rcon,$rcon,$rcon
 vxor  $in0,$in0,$key
  vperm  $outtail,$in0,$in0,$outperm # rotate
  vsel  $stage,$outhead,$outtail,$outmask
  vmr  $outhead,$outtail
  stvx  $stage,0,$out
  addi  $inp,$out,15  # 15 is not typo
  addi  $out,$out,16
 bdz  Ldone

 vspltw  $key,$in0,3  # just splat
 vsldoi  $tmp,$zero,$in1,12 # >>32
 vsbox  $key,$key

 vxor  $in1,$in1,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in1,$in1,$tmp
 vsldoi  $tmp,$zero,$tmp,12 # >>32
 vxor  $in1,$in1,$tmp

 vxor  $in1,$in1,$key
 b  Loop256

.align 4
Ldone:
 lvx  $in1,0,$inp  # redundant in aligned case
 vsel  $in1,$outhead,$in1,$outmask
 stvx  $in1,0,$inp
 li  $ptr,0
 mtspr  256,$vrsave
 stw  $rounds,0($out)

Lenc_key_abort:
 mr  r3,$ptr
 blr
 .long  0
 .byte  0,12,0x14,1,0,0,3,0
 .long  0
.size .${prefix}_set_encrypt_key,.-.${prefix}_set_encrypt_key

.globl .${prefix}_set_decrypt_key
.align 5
.${prefix}_set_decrypt_key:
 $STU  $sp,-$FRAME($sp)
 mflr  r10
 $PUSH  r10,$FRAME+$LRSAVE($sp)
 bl  Lset_encrypt_key
 mtlr  r10

 cmpwi  r3,0
 bne-  Ldec_key_abort

 slwi  $cnt,$rounds,4
 subi  $inp,$out,240  # first round key
 srwi  $rounds,$rounds,1
 add  $out,$inp,$cnt  # last round key
 mtctr  $rounds

Ldeckey:
 lwz  r0, 0($inp)
 lwz  r6, 4($inp)
 lwz  r7, 8($inp)
 lwz  r8, 12($inp)
 addi  $inp,$inp,16
 lwz  r9, 0($out)
 lwz  r10,4($out)
 lwz  r11,8($out)
 lwz  r12,12($out)
 stw  r0, 0($out)
 stw  r6, 4($out)
 stw  r7, 8($out)
 stw  r8, 12($out)
 subi  $out,$out,16
 stw  r9, -16($inp)
 stw  r10,-12($inp)
 stw  r11,-8($inp)
 stw  r12,-4($inp)
 bdnz  Ldeckey

 xor  r3,r3,r3  # return value
Ldec_key_abort:
 addi  $sp,$sp,$FRAME
 blr
 .long  0
 .byte  0,12,4,1,0x80,0,3,0
 .long  0
.size .${prefix}_set_decrypt_key,.-.${prefix}_set_decrypt_key
___
}}}
#########################################################################
{{{ # Single block en- and decrypt procedures   #
sub gen_block () {
my $dir = shift;
my $n   = $dir eq "de" ? "n" : "";
my ($inp,$out,$key,$rounds,$idx)=map("r$_",(3..7));

$code.=<<___;
.globl .${prefix}_${dir}crypt
.align 5
.${prefix}_${dir}crypt:
 lwz  $rounds,240($key)
 lis  r0,0xfc00
 mfspr  $vrsave,256
 li  $idx,15   # 15 is not typo
 mtspr  256,r0

 lvx  v0,0,$inp
 neg  r11,$out
 lvx  v1,$idx,$inp
 lvsl  v2,0,$inp  # inpperm
 le?vspltisb v4,0x0f
 ?lvsl  v3,0,r11  # outperm
 le?vxor  v2,v2,v4
 li  $idx,16
 vperm  v0,v0,v1,v2  # align [and byte swap in LE]
 lvx  v1,0,$key
 ?lvsl  v5,0,$key  # keyperm
 srwi  $rounds,$rounds,1
 lvx  v2,$idx,$key
 addi  $idx,$idx,16
 subi  $rounds,$rounds,1
 ?vperm  v1,v1,v2,v5  # align round key

 vxor  v0,v0,v1
 lvx  v1,$idx,$key
 addi  $idx,$idx,16
 mtctr  $rounds

Loop_${dir}c:
 ?vperm  v2,v2,v1,v5
 v${n}cipher v0,v0,v2
 lvx  v2,$idx,$key
 addi  $idx,$idx,16
 ?vperm  v1,v1,v2,v5
 v${n}cipher v0,v0,v1
 lvx  v1,$idx,$key
 addi  $idx,$idx,16
 bdnz  Loop_${dir}c

 ?vperm  v2,v2,v1,v5
 v${n}cipher v0,v0,v2
 lvx  v2,$idx,$key
 ?vperm  v1,v1,v2,v5
 v${n}cipherlast v0,v0,v1

 vspltisb v2,-1
 vxor  v1,v1,v1
 li  $idx,15   # 15 is not typo
 ?vperm  v2,v1,v2,v3  # outmask
 le?vxor  v3,v3,v4
 lvx  v1,0,$out  # outhead
 vperm  v0,v0,v0,v3  # rotate [and byte swap in LE]
 vsel  v1,v1,v0,v2
 lvx  v4,$idx,$out
 stvx  v1,0,$out
 vsel  v0,v0,v4,v2
 stvx  v0,$idx,$out

 mtspr  256,$vrsave
 blr
 .long  0
 .byte  0,12,0x14,0,0,0,3,0
 .long  0
.size .${prefix}_${dir}crypt,.-.${prefix}_${dir}crypt
___
}
&gen_block("en");
&gen_block("de");
}}}
#########################################################################
{{{ # CBC en- and decrypt procedures    #
my ($inp,$out,$len,$key,$ivp,$enc,$rounds,$idx)=map("r$_",(3..10));
my ($rndkey0,$rndkey1,$inout,$tmp)=  map("v$_",(0..3));
my ($ivec,$inptail,$inpperm,$outhead,$outperm,$outmask,$keyperm)=
      map("v$_",(4..10));
$code.=<<___;
.globl .${prefix}_cbc_encrypt
.align 5
.${prefix}_cbc_encrypt:
 ${UCMP}i $len,16
 bltlr-

 cmpwi  $enc,0   # test direction
 lis  r0,0xffe0
 mfspr  $vrsave,256
 mtspr  256,r0

 li  $idx,15
 vxor  $rndkey0,$rndkey0,$rndkey0
 le?vspltisb $tmp,0x0f

 lvx  $ivec,0,$ivp  # load [unaligned] iv
 lvsl  $inpperm,0,$ivp
 lvx  $inptail,$idx,$ivp
 le?vxor  $inpperm,$inpperm,$tmp
 vperm  $ivec,$ivec,$inptail,$inpperm

 neg  r11,$inp
 ?lvsl  $keyperm,0,$key  # prepare for unaligned key
 lwz  $rounds,240($key)

 lvsr  $inpperm,0,r11  # prepare for unaligned load
 lvx  $inptail,0,$inp
 addi  $inp,$inp,15  # 15 is not typo
 le?vxor  $inpperm,$inpperm,$tmp

 ?lvsr  $outperm,0,$out  # prepare for unaligned store
 vspltisb $outmask,-1
 lvx  $outhead,0,$out
 ?vperm  $outmask,$rndkey0,$outmask,$outperm
 le?vxor  $outperm,$outperm,$tmp

 srwi  $rounds,$rounds,1
 li  $idx,16
 subi  $rounds,$rounds,1
 beq  Lcbc_dec

Lcbc_enc:
 vmr  $inout,$inptail
 lvx  $inptail,0,$inp
 addi  $inp,$inp,16
 mtctr  $rounds
 subi  $len,$len,16  # len-=16

 lvx  $rndkey0,0,$key
  vperm  $inout,$inout,$inptail,$inpperm
 lvx  $rndkey1,$idx,$key
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key
 addi  $idx,$idx,16
 vxor  $inout,$inout,$ivec

Loop_cbc_enc:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vcipher  $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key
 addi  $idx,$idx,16
 bdnz  Loop_cbc_enc

 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key
 li  $idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vcipherlast $ivec,$inout,$rndkey0
 ${UCMP}i $len,16
 vperm  $tmp,$ivec,$ivec,$outperm
 vsel  $inout,$outhead,$tmp,$outmask
 vmr  $outhead,$tmp
 stvx  $inout,0,$out
 addi  $out,$out,16
 bge  Lcbc_enc

 b  Lcbc_done

.align 4
Lcbc_dec:
 ${UCMP}i $len,128
 bge  _aesp8_cbc_decrypt8x
 vmr  $tmp,$inptail
 lvx  $inptail,0,$inp
 addi  $inp,$inp,16
 mtctr  $rounds
 subi  $len,$len,16  # len-=16

 lvx  $rndkey0,0,$key
  vperm  $tmp,$tmp,$inptail,$inpperm
 lvx  $rndkey1,$idx,$key
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $inout,$tmp,$rndkey0
 lvx  $rndkey0,$idx,$key
 addi  $idx,$idx,16

Loop_cbc_dec:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vncipher $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vncipher $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key
 addi  $idx,$idx,16
 bdnz  Loop_cbc_dec

 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vncipher $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key
 li  $idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vncipherlast $inout,$inout,$rndkey0
 ${UCMP}i $len,16
 vxor  $inout,$inout,$ivec
 vmr  $ivec,$tmp
 vperm  $tmp,$inout,$inout,$outperm
 vsel  $inout,$outhead,$tmp,$outmask
 vmr  $outhead,$tmp
 stvx  $inout,0,$out
 addi  $out,$out,16
 bge  Lcbc_dec

Lcbc_done:
 addi  $out,$out,-1
 lvx  $inout,0,$out  # redundant in aligned case
 vsel  $inout,$outhead,$inout,$outmask
 stvx  $inout,0,$out

 neg  $enc,$ivp  # write [unaligned] iv
 li  $idx,15   # 15 is not typo
 vxor  $rndkey0,$rndkey0,$rndkey0
 vspltisb $outmask,-1
 le?vspltisb $tmp,0x0f
 ?lvsl  $outperm,0,$enc
 ?vperm  $outmask,$rndkey0,$outmask,$outperm
 le?vxor  $outperm,$outperm,$tmp
 lvx  $outhead,0,$ivp
 vperm  $ivec,$ivec,$ivec,$outperm
 vsel  $inout,$outhead,$ivec,$outmask
 lvx  $inptail,$idx,$ivp
 stvx  $inout,0,$ivp
 vsel  $inout,$ivec,$inptail,$outmask
 stvx  $inout,$idx,$ivp

 mtspr  256,$vrsave
 blr
 .long  0
 .byte  0,12,0x14,0,0,0,6,0
 .long  0
___
#########################################################################
{{ # Optimized CBC decrypt procedure    #
my $key_="r11";
my ($x00,$x10,$x20,$x30,$x40,$x50,$x60,$x70)=map("r$_",(0,8,26..31));
   $x00=0 if ($flavour =~ /osx/);
my ($in0, $in1, $in2, $in3, $in4, $in5, $in6, $in7 )=map("v$_",(0..3,10..13));
my ($out0,$out1,$out2,$out3,$out4,$out5,$out6,$out7)=map("v$_",(14..21));
my $rndkey0="v23"; # v24-v25 rotating buffer for first found keys
   # v26-v31 last 6 round keys
my ($tmp,$keyperm)=($in3,$in4); # aliases with "caller", redundant assignment
```

```
$code.=<<___;
.align 5
_aesp8_cbc_decrypt8x:
 $STU  $sp,-`($FRAME+21*16+6*$SIZE_T)`($sp)
 li  r10,`$FRAME+8*16+15`
 li  r11,`$FRAME+8*16+31`
 stvx  v20,r10,$sp  # ABI says so
 addi  r10,r10,32
 stvx  v21,r11,$sp
 addi  r11,r11,32
 stvx  v22,r10,$sp
 addi  r10,r10,32
 stvx  v23,r11,$sp
 addi  r11,r11,32
 stvx  v24,r10,$sp
 addi  r10,r10,32
 stvx  v25,r11,$sp
 addi  r11,r11,32
 stvx  v26,r10,$sp
 addi  r10,r10,32
 stvx  v27,r11,$sp
 addi  r11,r11,32
 stvx  v28,r10,$sp
 addi  r10,r10,32
 stvx  v29,r11,$sp
 addi  r11,r11,32
 stvx  v30,r10,$sp
 stvx  v31,r11,$sp
 li  r0,-1
 stw  $vrsave,`$FRAME+21*16-4`($sp) # save vrsave
 li  $x10,0x10
 $PUSH  r26,`$FRAME+21*16+0*$SIZE_T`($sp)
 li  $x20,0x20
 $PUSH  r27,`$FRAME+21*16+1*$SIZE_T`($sp)
 li  $x30,0x30
 $PUSH  r28,`$FRAME+21*16+2*$SIZE_T`($sp)
 li  $x40,0x40
 $PUSH  r29,`$FRAME+21*16+3*$SIZE_T`($sp)
 li  $x50,0x50
 $PUSH  r30,`$FRAME+21*16+4*$SIZE_T`($sp)
 li  $x60,0x60
 $PUSH  r31,`$FRAME+21*16+5*$SIZE_T`($sp)
 li  $x70,0x70
 mtspr  256,r0

 subi  $rounds,$rounds,3 # -4 in total
 subi  $len,$len,128  # bias
 lvx  $rndkey0,$x00,$key # load key schedule
 lvx  v30,$x10,$key
 addi  $key,$key,0x20
 lvx  v31,$x00,$key
 ?vperm  $rndkey0,$rndkey0,v30,$keyperm
 addi  $key_,$sp,$FRAME+15
 mtctr  $rounds

Load_cbc_dec_key:
 ?vperm  v24,v30,v31,$keyperm
 lvx  v30,$x10,$key
 addi  $key,$key,0x20
 stvx  v24,$x00,$key_  # off-load round[1]
 ?vperm  v25,v31,v30,$keyperm
 lvx  v31,$x00,$key
 stvx  v25,$x10,$key_  # off-load round[2]
 addi  $key_,$key_,0x20
 bdnz  Load_cbc_dec_key

 lvx  v26,$x10,$key
 ?vperm  v24,v30,v31,$keyperm
 lvx  v27,$x20,$key
 stvx  v24,$x00,$key_  # off-load round[3]
 ?vperm  v25,v31,v26,$keyperm
 lvx  v28,$x30,$key
 stvx  v25,$x10,$key_  # off-load round[4]
 addi  $key_,$sp,$FRAME+15 # rewind $key_
 ?vperm  v26,v26,v27,$keyperm
 lvx  v29,$x40,$key
 ?vperm  v27,v27,v28,$keyperm
 lvx  v30,$x50,$key
 ?vperm  v28,v28,v29,$keyperm
 lvx  v31,$x60,$key
 ?vperm  v29,v29,v30,$keyperm
 lvx  $out0,$x70,$key  # borrow $out0
 ?vperm  v30,v30,v31,$keyperm
 lvx  v24,$x00,$key_  # pre-load round[1]
 ?vperm  v31,v31,$out0,$keyperm
 lvx  v25,$x10,$key_  # pre-load round[2]

 #lvx  $inptail,0,$inp  # "caller" already did this
 #addi  $inp,$inp,15  # 15 is not typo
 subi  $inp,$inp,15  # undo "caller"

  le?li  $idx,8
 lvx_u  $in0,$x00,$inp  # load first 8 "words"
  le?lvsl $inpperm,0,$idx
  le?vspltisb $tmp,0x0f
 lvx_u  $in1,$x10,$inp
  le?vxor $inpperm,$inpperm,$tmp # transform for lvx_u/stvx_u
 lvx_u  $in2,$x20,$inp
  le?vperm $in0,$in0,$in0,$inpperm
 lvx_u  $in3,$x30,$inp
  le?vperm $in1,$in1,$in1,$inpperm
 lvx_u  $in4,$x40,$inp
  le?vperm $in2,$in2,$in2,$inpperm
 vxor  $out0,$in0,$rndkey0
 lvx_u  $in5,$x50,$inp
  le?vperm $in3,$in3,$in3,$inpperm
 vxor  $out1,$in1,$rndkey0
 lvx_u  $in6,$x60,$inp
  le?vperm $in4,$in4,$in4,$inpperm
 vxor  $out2,$in2,$rndkey0
 lvx_u  $in7,$x70,$inp
 addi  $inp,$inp,0x80
  le?vperm $in5,$in5,$in5,$inpperm
 vxor  $out3,$in3,$rndkey0
  le?vperm $in6,$in6,$in6,$inpperm
 vxor  $out4,$in4,$rndkey0
  le?vperm $in7,$in7,$in7,$inpperm
 vxor  $out5,$in5,$rndkey0
 vxor  $out6,$in6,$rndkey0
 vxor  $out7,$in7,$rndkey0

 mtctr  $rounds
 b  Loop_cbc_dec8x
.align 5
Loop_cbc_dec8x:
 vncipher $out0,$out0,v24
 vncipher $out1,$out1,v24
 vncipher $out2,$out2,v24
 vncipher $out3,$out3,v24
 vncipher $out4,$out4,v24
 vncipher $out5,$out5,v24
 vncipher $out6,$out6,v24
 vncipher $out7,$out7,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vncipher $out0,$out0,v25
 vncipher $out1,$out1,v25
 vncipher $out2,$out2,v25
 vncipher $out3,$out3,v25
 vncipher $out4,$out4,v25
 vncipher $out5,$out5,v25
 vncipher $out6,$out6,v25
 vncipher $out7,$out7,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Loop_cbc_dec8x

 subic  $len,$len,128  # $len-=128
 vncipher $out0,$out0,v24
 vncipher $out1,$out1,v24
 vncipher $out2,$out2,v24
 vncipher $out3,$out3,v24
 vncipher $out4,$out4,v24
 vncipher $out5,$out5,v24
 vncipher $out6,$out6,v24
 vncipher $out7,$out7,v24

 subfe.  r0,r0,r0  # borrow?-1:0
 vncipher $out0,$out0,v25
 vncipher $out1,$out1,v25
 vncipher $out2,$out2,v25
 vncipher $out3,$out3,v25
 vncipher $out4,$out4,v25
 vncipher $out5,$out5,v25
 vncipher $out6,$out6,v25
 vncipher $out7,$out7,v25

 and  r0,r0,$len
 vncipher $out0,$out0,v26
 vncipher $out1,$out1,v26
 vncipher $out2,$out2,v26
 vncipher $out3,$out3,v26
 vncipher $out4,$out4,v26
 vncipher $out5,$out5,v26
 vncipher $out6,$out6,v26
 vncipher $out7,$out7,v26

 add  $inp,$inp,r0  # $inp is adjusted in such
    # way that at exit from the
    # loop inX-in7 are loaded
    # with last "words"
 vncipher $out0,$out0,v27
 vncipher $out1,$out1,v27
 vncipher $out2,$out2,v27
 vncipher $out3,$out3,v27
 vncipher $out4,$out4,v27
 vncipher $out5,$out5,v27
 vncipher $out6,$out6,v27
 vncipher $out7,$out7,v27

 addi  $key_,$sp,$FRAME+15 # rewind $key_
```

```
vncipher $out0,$out0,v28
vncipher $out1,$out1,v28
vncipher $out2,$out2,v28
vncipher $out3,$out3,v28
vncipher $out4,$out4,v28
vncipher $out5,$out5,v28
vncipher $out6,$out6,v28
vncipher $out7,$out7,v28
lvx  v24,$x00,$key_  # re-pre-load round[1]

vncipher $out0,$out0,v29
vncipher $out1,$out1,v29
vncipher $out2,$out2,v29
vncipher $out3,$out3,v29
vncipher $out4,$out4,v29
vncipher $out5,$out5,v29
vncipher $out6,$out6,v29
vncipher $out7,$out7,v29
lvx  v25,$x10,$key_  # re-pre-load round[2]

vncipher $out0,$out0,v30
 vxor  $ivec,$ivec,v31  # xor with last round key
vncipher $out1,$out1,v30
 vxor  $in0,$in0,v31
vncipher $out2,$out2,v30
 vxor  $in1,$in1,v31
vncipher $out3,$out3,v30
 vxor  $in2,$in2,v31
vncipher $out4,$out4,v30
 vxor  $in3,$in3,v31
vncipher $out5,$out5,v30
 vxor  $in4,$in4,v31
vncipher $out6,$out6,v30
 vxor  $in5,$in5,v31
vncipher $out7,$out7,v30
 vxor  $in6,$in6,v31

vncipherlast $out0,$out0,$ivec
vncipherlast $out1,$out1,$in0
 lvx_u  $in0,$x00,$inp  # load next input block
vncipherlast $out2,$out2,$in1
 lvx_u  $in1,$x10,$inp
vncipherlast $out3,$out3,$in2
 le?vperm $in0,$in0,$in0,$inpperm
 lvx_u  $in2,$x20,$inp
vncipherlast $out4,$out4,$in3
 le?vperm $in1,$in1,$in1,$inpperm
 lvx_u  $in3,$x30,$inp
```

```
vncipherlast $out5,$out5,$in4
 le?vperm $in2,$in2,$in2,$inpperm
 lvx_u  $in4,$x40,$inp
vncipherlast $out6,$out6,$in5
 le?vperm $in3,$in3,$in3,$inpperm
 lvx_u  $in5,$x50,$inp
vncipherlast $out7,$out7,$in6
 le?vperm $in4,$in4,$in4,$inpperm
 lvx_u  $in6,$x60,$inp
vmr  $ivec,$in7
 le?vperm $in5,$in5,$in5,$inpperm
 lvx_u  $in7,$x70,$inp
 addi  $inp,$inp,0x80

le?vperm $out0,$out0,$out0,$inpperm
le?vperm $out1,$out1,$out1,$inpperm
stvx_u  $out0,$x00,$out
 le?vperm $in6,$in6,$in6,$inpperm
 vxor  $out0,$in0,$rndkey0
le?vperm $out2,$out2,$out2,$inpperm
stvx_u  $out1,$x10,$out
 le?vperm $in7,$in7,$in7,$inpperm
 vxor  $out1,$in1,$rndkey0
le?vperm $out3,$out3,$out3,$inpperm
stvx_u  $out2,$x20,$out
 vxor  $out2,$in2,$rndkey0
le?vperm $out4,$out4,$out4,$inpperm
stvx_u  $out3,$x30,$out
 vxor  $out3,$in3,$rndkey0
le?vperm $out5,$out5,$out5,$inpperm
stvx_u  $out4,$x40,$out
 vxor  $out4,$in4,$rndkey0
le?vperm $out6,$out6,$out6,$inpperm
stvx_u  $out5,$x50,$out
 vxor  $out5,$in5,$rndkey0
le?vperm $out7,$out7,$out7,$inpperm
stvx_u  $out6,$x60,$out
 vxor  $out6,$in6,$rndkey0
stvx_u  $out7,$x70,$out
addi  $out,$out,0x80
 vxor  $out7,$in7,$rndkey0

mtctr  $rounds
beq  Loop_cbc_dec8x  # did $len-=128 borrow?

addic.  $len,$len,128
beq  Lcbc_dec8x_done
nop
```

```
 nop

Loop_cbc_dec8x_tail:	# up to 7 "words" tail...
 vncipher $out1,$out1,v24
 vncipher $out2,$out2,v24
 vncipher $out3,$out3,v24
 vncipher $out4,$out4,v24
 vncipher $out5,$out5,v24
 vncipher $out6,$out6,v24
 vncipher $out7,$out7,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vncipher $out1,$out1,v25
 vncipher $out2,$out2,v25
 vncipher $out3,$out3,v25
 vncipher $out4,$out4,v25
 vncipher $out5,$out5,v25
 vncipher $out6,$out6,v25
 vncipher $out7,$out7,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Loop_cbc_dec8x_tail

 vncipher $out1,$out1,v24
 vncipher $out2,$out2,v24
 vncipher $out3,$out3,v24
 vncipher $out4,$out4,v24
 vncipher $out5,$out5,v24
 vncipher $out6,$out6,v24
 vncipher $out7,$out7,v24

 vncipher $out1,$out1,v25
 vncipher $out2,$out2,v25
 vncipher $out3,$out3,v25
 vncipher $out4,$out4,v25
 vncipher $out5,$out5,v25
 vncipher $out6,$out6,v25
 vncipher $out7,$out7,v25

 vncipher $out1,$out1,v26
 vncipher $out2,$out2,v26
 vncipher $out3,$out3,v26
 vncipher $out4,$out4,v26
 vncipher $out5,$out5,v26
 vncipher $out6,$out6,v26
 vncipher $out7,$out7,v26

 vncipher $out1,$out1,v27
vncipher $out2,$out2,v27
vncipher $out3,$out3,v27
vncipher $out4,$out4,v27
vncipher $out5,$out5,v27
vncipher $out6,$out6,v27
vncipher $out7,$out7,v27

vncipher $out1,$out1,v28
vncipher $out2,$out2,v28
vncipher $out3,$out3,v28
vncipher $out4,$out4,v28
vncipher $out5,$out5,v28
vncipher $out6,$out6,v28
vncipher $out7,$out7,v28

vncipher $out1,$out1,v29
vncipher $out2,$out2,v29
vncipher $out3,$out3,v29
vncipher $out4,$out4,v29
vncipher $out5,$out5,v29
vncipher $out6,$out6,v29
vncipher $out7,$out7,v29

vncipher $out1,$out1,v30
 vxor  $ivec,$ivec,v31  # last round key
vncipher $out2,$out2,v30
 vxor  $in1,$in1,v31
vncipher $out3,$out3,v30
 vxor  $in2,$in2,v31
vncipher $out4,$out4,v30
 vxor  $in3,$in3,v31
vncipher $out5,$out5,v30
 vxor  $in4,$in4,v31
vncipher $out6,$out6,v30
 vxor  $in5,$in5,v31
vncipher $out7,$out7,v30
 vxor  $in6,$in6,v31

cmplwi  $len,32   # switch($len)
blt  Lcbc_dec8x_one
nop
beq  Lcbc_dec8x_two
cmplwi  $len,64
blt  Lcbc_dec8x_three
nop
beq  Lcbc_dec8x_four
cmplwi  $len,96
blt  Lcbc_dec8x_five
```

```
 nop
 beq  Lcbc_dec8x_six

Lcbc_dec8x_seven:
 vncipherlast $out1,$out1,$ivec
 vncipherlast $out2,$out2,$in1
 vncipherlast $out3,$out3,$in2
 vncipherlast $out4,$out4,$in3
 vncipherlast $out5,$out5,$in4
 vncipherlast $out6,$out6,$in5
 vncipherlast $out7,$out7,$in6
 vmr  $ivec,$in7

 le?vperm $out1,$out1,$out1,$inpperm
 le?vperm $out2,$out2,$out2,$inpperm
 stvx_u  $out1,$x00,$out
 le?vperm $out3,$out3,$out3,$inpperm
 stvx_u  $out2,$x10,$out
 le?vperm $out4,$out4,$out4,$inpperm
 stvx_u  $out3,$x20,$out
 le?vperm $out5,$out5,$out5,$inpperm
 stvx_u  $out4,$x30,$out
 le?vperm $out6,$out6,$out6,$inpperm
 stvx_u  $out5,$x40,$out
 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out6,$x50,$out
 stvx_u  $out7,$x60,$out
 addi  $out,$out,0x70
 b  Lcbc_dec8x_done

.align 5
Lcbc_dec8x_six:
 vncipherlast $out2,$out2,$ivec
 vncipherlast $out3,$out3,$in2
 vncipherlast $out4,$out4,$in3
 vncipherlast $out5,$out5,$in4
 vncipherlast $out6,$out6,$in5
 vncipherlast $out7,$out7,$in6
 vmr  $ivec,$in7

 le?vperm $out2,$out2,$out2,$inpperm
 le?vperm $out3,$out3,$out3,$inpperm
 stvx_u  $out2,$x00,$out
 le?vperm $out4,$out4,$out4,$inpperm
 stvx_u  $out3,$x10,$out
 le?vperm $out5,$out5,$out5,$inpperm
 stvx_u  $out4,$x20,$out
 le?vperm $out6,$out6,$out6,$inpperm
 stvx_u  $out5,$x30,$out
 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out6,$x40,$out
 stvx_u  $out7,$x50,$out
 addi  $out,$out,0x60
 b  Lcbc_dec8x_done

.align 5
Lcbc_dec8x_five:
 vncipherlast $out3,$out3,$ivec
 vncipherlast $out4,$out4,$in3
 vncipherlast $out5,$out5,$in4
 vncipherlast $out6,$out6,$in5
 vncipherlast $out7,$out7,$in6
 vmr  $ivec,$in7

 le?vperm $out3,$out3,$out3,$inpperm
 le?vperm $out4,$out4,$out4,$inpperm
 stvx_u  $out3,$x00,$out
 le?vperm $out5,$out5,$out5,$inpperm
 stvx_u  $out4,$x10,$out
 le?vperm $out6,$out6,$out6,$inpperm
 stvx_u  $out5,$x20,$out
 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out6,$x30,$out
 stvx_u  $out7,$x40,$out
 addi  $out,$out,0x50
 b  Lcbc_dec8x_done

.align 5
Lcbc_dec8x_four:
 vncipherlast $out4,$out4,$ivec
 vncipherlast $out5,$out5,$in4
 vncipherlast $out6,$out6,$in5
 vncipherlast $out7,$out7,$in6
 vmr  $ivec,$in7

 le?vperm $out4,$out4,$out4,$inpperm
 le?vperm $out5,$out5,$out5,$inpperm
 stvx_u  $out4,$x00,$out
 le?vperm $out6,$out6,$out6,$inpperm
 stvx_u  $out5,$x10,$out
 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out6,$x20,$out
 stvx_u  $out7,$x30,$out
 addi  $out,$out,0x40
 b  Lcbc_dec8x_done
```

```
.align 5
Lcbc_dec8x_three:
 vncipherlast $out5,$out5,$ivec
 vncipherlast $out6,$out6,$in5
 vncipherlast $out7,$out7,$in6
 vmr  $ivec,$in7

 le?vperm $out5,$out5,$out5,$inpperm
 le?vperm $out6,$out6,$out6,$inpperm
 stvx_u  $out5,$x00,$out
 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out6,$x10,$out
 stvx_u  $out7,$x20,$out
 addi  $out,$out,0x30
 b  Lcbc_dec8x_done

.align 5
Lcbc_dec8x_two:
 vncipherlast $out6,$out6,$ivec
 vncipherlast $out7,$out7,$in6
 vmr  $ivec,$in7

 le?vperm $out6,$out6,$out6,$inpperm
 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out6,$x00,$out
 stvx_u  $out7,$x10,$out
 addi  $out,$out,0x20
 b  Lcbc_dec8x_done

.align 5
Lcbc_dec8x_one:
 vncipherlast $out7,$out7,$ivec
 vmr  $ivec,$in7

 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out7,0,$out
 addi  $out,$out,0x10

Lcbc_dec8x_done:
 le?vperm $ivec,$ivec,$ivec,$inpperm
 stvx_u  $ivec,0,$ivp  # write [unaligned] iv

 li  r10,`$FRAME+15`
 li  r11,`$FRAME+31`
 stvx  $inpperm,r10,$sp # wipe copies of round keys
 addi  r10,r10,32
 stvx  $inpperm,r11,$sp
 addi  r11,r11,32
	stvx	$inpperm,r10,$sp
	addi	r10,r10,32
	stvx	$inpperm,r11,$sp
	addi	r11,r11,32
	stvx	$inpperm,r10,$sp
	addi	r10,r10,32
	stvx	$inpperm,r11,$sp
	addi	r11,r11,32
	stvx	$inpperm,r10,$sp
	addi	r10,r10,32
	stvx	$inpperm,r11,$sp
	addi	r11,r11,32

	mtspr	256,$vrsave
	lvx	v20,r10,$sp		# ABI says so
	addi	r10,r10,32
	lvx	v21,r11,$sp
	addi	r11,r11,32
	lvx	v22,r10,$sp
	addi	r10,r10,32
	lvx	v23,r11,$sp
	addi	r11,r11,32
	lvx	v24,r10,$sp
	addi	r10,r10,32
	lvx	v25,r11,$sp
	addi	r11,r11,32
	lvx	v26,r10,$sp
	addi	r10,r10,32
	lvx	v27,r11,$sp
	addi	r11,r11,32
	lvx	v28,r10,$sp
	addi	r10,r10,32
	lvx	v29,r11,$sp
	addi	r11,r11,32
	lvx	v30,r10,$sp
	lvx	v31,r11,$sp
	$POP	r26,`$FRAME+21*16+0*$SIZE_T`($sp)
	$POP	r27,`$FRAME+21*16+1*$SIZE_T`($sp)
	$POP	r28,`$FRAME+21*16+2*$SIZE_T`($sp)
	$POP	r29,`$FRAME+21*16+3*$SIZE_T`($sp)
	$POP	r30,`$FRAME+21*16+4*$SIZE_T`($sp)
	$POP	r31,`$FRAME+21*16+5*$SIZE_T`($sp)
	addi	$sp,$sp,`$FRAME+21*16+6*$SIZE_T`
	blr
	.long	0
	.byte	0,12,0x04,0,0x80,6,6,0
	.long	0
.size	.${prefix}_cbc_encrypt,.-.${prefix}_cbc_encrypt
```

```
___
}} }}}

#########################################################################
{{{ # CTR procedure[s]      #
my ($inp,$out,$len,$key,$ivp,$x10,$rounds,$idx)=map("r$_",(3..10));
my ($rndkey0,$rndkey1,$inout,$tmp)=  map("v$_",(0..3));
my ($ivec,$inptail,$inpperm,$outhead,$outperm,$outmask,$keyperm,$one)=
      map("v$_",(4..11));
my $dat=$tmp;

$code.=<<___;
.globl .${prefix}_ctr32_encrypt_blocks
.align 5
.${prefix}_ctr32_encrypt_blocks:
 ${UCMP}i $len,1
 bltlr-

 lis  r0,0xfff0
 mfspr  $vrsave,256
 mtspr  256,r0

 li  $idx,15
 vxor  $rndkey0,$rndkey0,$rndkey0
 le?vspltisb $tmp,0x0f

 lvx  $ivec,0,$ivp  # load [unaligned] iv
 lvsl  $inpperm,0,$ivp
 lvx  $inptail,$idx,$ivp
  vspltisb $one,1
 le?vxor  $inpperm,$inpperm,$tmp
 vperm  $ivec,$ivec,$inptail,$inpperm
  vsldoi  $one,$rndkey0,$one,1

 neg  r11,$inp
 ?lvsl  $keyperm,0,$key  # prepare for unaligned key
 lwz  $rounds,240($key)

 lvsr  $inpperm,0,r11  # prepare for unaligned load
 lvx  $inptail,0,$inp
 addi  $inp,$inp,15  # 15 is not typo
 le?vxor  $inpperm,$inpperm,$tmp

 srwi  $rounds,$rounds,1
 li  $idx,16
 subi  $rounds,$rounds,1

 ${UCMP}i $len,8
 bge  _aesp8_ctr32_encrypt8x

 ?lvsr  $outperm,0,$out  # prepare for unaligned store
 vspltisb $outmask,-1
 lvx  $outhead,0,$out
 ?vperm  $outmask,$rndkey0,$outmask,$outperm
 le?vxor  $outperm,$outperm,$tmp

 lvx  $rndkey0,0,$key
 mtctr  $rounds
 lvx  $rndkey1,$idx,$key
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $inout,$ivec,$rndkey0
 lvx  $rndkey0,$idx,$key
 addi  $idx,$idx,16
 b  Loop_ctr32_enc

.align 5
Loop_ctr32_enc:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vcipher  $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key
 addi  $idx,$idx,16
 bdnz  Loop_ctr32_enc

 vadduwm  $ivec,$ivec,$one
  vmr  $dat,$inptail
  lvx  $inptail,0,$inp
  addi  $inp,$inp,16
  subic.  $len,$len,1  # blocks--

 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key
  vperm  $dat,$dat,$inptail,$inpperm
  li  $idx,16
 ?vperm  $rndkey1,$rndkey0,$rndkey1,$keyperm
  lvx  $rndkey0,0,$key
 vxor  $dat,$dat,$rndkey1 # last round key
 vcipherlast $inout,$inout,$dat

  lvx  $rndkey1,$idx,$key
  addi  $idx,$idx,16
 vperm  $inout,$inout,$inout,$outperm
 vsel  $dat,$outhead,$inout,$outmask
  mtctr  $rounds
  ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vmr  $outhead,$inout
  vxor  $inout,$ivec,$rndkey0
  lvx  $rndkey0,$idx,$key
  addi  $idx,$idx,16
 stvx  $dat,0,$out
 addi  $out,$out,16
 bne  Loop_ctr32_enc

 addi  $out,$out,-1
 lvx  $inout,0,$out  # redundant in aligned case
 vsel  $inout,$outhead,$inout,$outmask
 stvx  $inout,0,$out

 mtspr  256,$vrsave
 blr
 .long  0
 .byte  0,12,0x14,0,0,0,6,0
 .long  0
___
#########################################################################
{{ # Optimized CTR procedure     #
my $key_="r11";
my ($x00,$x10,$x20,$x30,$x40,$x50,$x60,$x70)=map("r$_",(0,8,26..31));
   $x00=0 if ($flavour =~ /osx/);
my ($in0, $in1, $in2, $in3, $in4, $in5, $in6, $in7 )=map("v$_",(0..3,10,12..14));
my ($out0,$out1,$out2,$out3,$out4,$out5,$out6,$out7)=map("v$_",(15..22));
my $rndkey0="v23"; # v24-v25 rotating buffer for first found keys
   # v26-v31 last 6 round keys
my ($tmp,$keyperm)=($in3,$in4); # aliases with "caller", redundant assignment
my ($two,$three,$four)=($outhead,$outperm,$outmask);

$code.=<<___;
.align 5
_aesp8_ctr32_encrypt8x:
 $STU  $sp,-`($FRAME+21*16+6*$SIZE_T)`($sp)
 li  r10,`$FRAME+8*16+15`
 li  r11,`$FRAME+8*16+31`
 stvx  v20,r10,$sp  # ABI says so
 addi  r10,r10,32
 stvx  v21,r11,$sp
 addi  r11,r11,32
 stvx  v22,r10,$sp
 addi  r10,r10,32
 stvx  v23,r11,$sp
 addi  r11,r11,32
 stvx  v24,r10,$sp
 addi  r10,r10,32
 stvx  v25,r11,$sp
 addi  r11,r11,32
 stvx  v26,r10,$sp
 addi  r10,r10,32
 stvx  v27,r11,$sp
 addi  r11,r11,32
 stvx  v28,r10,$sp
 addi  r10,r10,32
 stvx  v29,r11,$sp
 addi  r11,r11,32
 stvx  v30,r10,$sp
 stvx  v31,r11,$sp
 li  r0,-1
 stw  $vrsave,`$FRAME+21*16-4`($sp) # save vrsave
 li  $x10,0x10
 $PUSH  r26,`$FRAME+21*16+0*$SIZE_T`($sp)
 li  $x20,0x20
 $PUSH  r27,`$FRAME+21*16+1*$SIZE_T`($sp)
 li  $x30,0x30
 $PUSH  r28,`$FRAME+21*16+2*$SIZE_T`($sp)
 li  $x40,0x40
 $PUSH  r29,`$FRAME+21*16+3*$SIZE_T`($sp)
 li  $x50,0x50
 $PUSH  r30,`$FRAME+21*16+4*$SIZE_T`($sp)
 li  $x60,0x60
 $PUSH  r31,`$FRAME+21*16+5*$SIZE_T`($sp)
 li  $x70,0x70
 mtspr  256,r0

 subi  $rounds,$rounds,3 # -4 in total

 lvx  $rndkey0,$x00,$key # load key schedule
 lvx  v30,$x10,$key
 addi  $key,$key,0x20
 lvx  v31,$x00,$key
 ?vperm  $rndkey0,$rndkey0,v30,$keyperm
 addi  $key_,$sp,$FRAME+15
 mtctr  $rounds

Load_ctr32_enc_key:
 ?vperm  v24,v30,v31,$keyperm
 lvx  v30,$x10,$key
 addi  $key,$key,0x20
 stvx  v24,$x00,$key_  # off-load round[1]
 ?vperm  v25,v31,v30,$keyperm
```

```
lvx  v31,$x00,$key
stvx  v25,$x10,$key_  # off-load round[2]
addi  $key_,$key_,0x20
bdnz  Load_ctr32_enc_key

lvx  v26,$x10,$key
?vperm  v24,v30,v31,$keyperm
lvx  v27,$x20,$key
stvx  v24,$x00,$key_  # off-load round[3]
?vperm  v25,v31,v26,$keyperm
lvx  v28,$x30,$key
stvx  v25,$x10,$key_  # off-load round[4]
addi  $key_,$sp,$FRAME+15 # rewind $key_
?vperm  v26,v26,v27,$keyperm
lvx  v29,$x40,$key
?vperm  v27,v27,v28,$keyperm
lvx  v30,$x50,$key
?vperm  v28,v28,v29,$keyperm
lvx  v31,$x60,$key
?vperm  v29,v29,v30,$keyperm
lvx  $out0,$x70,$key  # borrow $out0
?vperm  v30,v30,v31,$keyperm
lvx  v24,$x00,$key_  # pre-load round[1]
?vperm  v31,v31,$out0,$keyperm
lvx  v25,$x10,$key_  # pre-load round[2]

vadduwm  $two,$one,$one
subi  $inp,$inp,15  # undo "caller"
$SHL  $len,$len,4

vadduwm  $out1,$ivec,$one # counter values ...
vadduwm  $out2,$ivec,$two
vxor  $out0,$ivec,$rndkey0 # ... xored with rndkey[0]
 le?li  $idx,8
vadduwm  $out3,$out1,$two
vxor  $out1,$out1,$rndkey0
 le?lvsl $inpperm,0,$idx
vadduwm  $out4,$out2,$two
vxor  $out2,$out2,$rndkey0
 le?vspltisb $tmp,0x0f
vadduwm  $out5,$out3,$two
vxor  $out3,$out3,$rndkey0
 le?vxor $inpperm,$inpperm,$tmp # transform for lvx_u/stvx_u
vadduwm  $out6,$out4,$two
vxor  $out4,$out4,$rndkey0
vadduwm  $out7,$out5,$two
vxor  $out5,$out5,$rndkey0
vadduwm  $ivec,$out6,$two # next counter value
```

```
 vxor  $out6,$out6,$rndkey0
 vxor  $out7,$out7,$rndkey0

 mtctr  $rounds
 b  Loop_ctr32_enc8x
.align 5
Loop_ctr32_enc8x:
 vcipher  $out0,$out0,v24
 vcipher  $out1,$out1,v24
 vcipher  $out2,$out2,v24
 vcipher  $out3,$out3,v24
 vcipher  $out4,$out4,v24
 vcipher  $out5,$out5,v24
 vcipher  $out6,$out6,v24
 vcipher  $out7,$out7,v24
Loop_ctr32_enc8x_middle:
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vcipher  $out0,$out0,v25
 vcipher  $out1,$out1,v25
 vcipher  $out2,$out2,v25
 vcipher  $out3,$out3,v25
 vcipher  $out4,$out4,v25
 vcipher  $out5,$out5,v25
 vcipher  $out6,$out6,v25
 vcipher  $out7,$out7,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Loop_ctr32_enc8x

 subic  r11,$len,256  # $len-256, borrow $key_
 vcipher  $out0,$out0,v24
 vcipher  $out1,$out1,v24
 vcipher  $out2,$out2,v24
 vcipher  $out3,$out3,v24
 vcipher  $out4,$out4,v24
 vcipher  $out5,$out5,v24
 vcipher  $out6,$out6,v24
 vcipher  $out7,$out7,v24

 subfe  r0,r0,r0  # borrow?-1:0
 vcipher  $out0,$out0,v25
 vcipher  $out1,$out1,v25
 vcipher  $out2,$out2,v25
 vcipher  $out3,$out3,v25
 vcipher  $out4,$out4,v25
 vcipher  $out5,$out5,v25
 vcipher  $out6,$out6,v25
 vcipher  $out7,$out7,v25

 and  r0,r0,r11
 addi  $key_,$sp,$FRAME+15 # rewind $key_
 vcipher  $out0,$out0,v26
 vcipher  $out1,$out1,v26
 vcipher  $out2,$out2,v26
 vcipher  $out3,$out3,v26
 vcipher  $out4,$out4,v26
 vcipher  $out5,$out5,v26
 vcipher  $out6,$out6,v26
 vcipher  $out7,$out7,v26
 lvx  v24,$x00,$key_  # re-pre-load round[1]

 subic  $len,$len,129  # $len-=129
 vcipher  $out0,$out0,v27
 addi  $len,$len,1  # $len-=128 really
 vcipher  $out1,$out1,v27
 vcipher  $out2,$out2,v27
 vcipher  $out3,$out3,v27
 vcipher  $out4,$out4,v27
 vcipher  $out5,$out5,v27
 vcipher  $out6,$out6,v27
 vcipher  $out7,$out7,v27
 lvx  v25,$x10,$key_  # re-pre-load round[2]

 vcipher  $out0,$out0,v28
  lvx_u  $in0,$x00,$inp  # load input
 vcipher  $out1,$out1,v28
  lvx_u  $in1,$x10,$inp
 vcipher  $out2,$out2,v28
  lvx_u  $in2,$x20,$inp
 vcipher  $out3,$out3,v28
  lvx_u  $in3,$x30,$inp
 vcipher  $out4,$out4,v28
  lvx_u  $in4,$x40,$inp
 vcipher  $out5,$out5,v28
  lvx_u  $in5,$x50,$inp
 vcipher  $out6,$out6,v28
  lvx_u  $in6,$x60,$inp
 vcipher  $out7,$out7,v28
  lvx_u  $in7,$x70,$inp
  addi  $inp,$inp,0x80

 vcipher  $out0,$out0,v29
  le?vperm $in0,$in0,$in0,$inpperm
 vcipher  $out1,$out1,v29
  le?vperm $in1,$in1,$in1,$inpperm
```

```
vcipher  $out2,$out2,v29
 le?vperm $in2,$in2,$in2,$inpperm
vcipher  $out3,$out3,v29
 le?vperm $in3,$in3,$in3,$inpperm
vcipher  $out4,$out4,v29
 le?vperm $in4,$in4,$in4,$inpperm
vcipher  $out5,$out5,v29
 le?vperm $in5,$in5,$in5,$inpperm
vcipher  $out6,$out6,v29
 le?vperm $in6,$in6,$in6,$inpperm
vcipher  $out7,$out7,v29
 le?vperm $in7,$in7,$in7,$inpperm

add  $inp,$inp,r0  # $inp is adjusted in such
     # way that at exit from the
     # loop inX-in7 are loaded
     # with last "words"
subfe.  r0,r0,r0  # borrow?-1:0
vcipher  $out0,$out0,v30
 vxor  $in0,$in0,v31  # xor with last round key
vcipher  $out1,$out1,v30
 vxor  $in1,$in1,v31
vcipher  $out2,$out2,v30
 vxor  $in2,$in2,v31
vcipher  $out3,$out3,v30
 vxor  $in3,$in3,v31
vcipher  $out4,$out4,v30
 vxor  $in4,$in4,v31
vcipher  $out5,$out5,v30
 vxor  $in5,$in5,v31
vcipher  $out6,$out6,v30
 vxor  $in6,$in6,v31
vcipher  $out7,$out7,v30
 vxor  $in7,$in7,v31

bne  Lctr32_enc8x_break # did $len-129 borrow?

vcipherlast $in0,$out0,$in0
vcipherlast $in1,$out1,$in1
 vadduwm $out1,$ivec,$one # counter values ...
vcipherlast $in2,$out2,$in2
 vadduwm $out2,$ivec,$two
 vxor  $out0,$ivec,$rndkey0 # ... xored with rndkey[0]
vcipherlast $in3,$out3,$in3
 vadduwm $out3,$out1,$two
 vxor  $out1,$out1,$rndkey0
vcipherlast $in4,$out4,$in4
 vadduwm $out4,$out2,$two
```

```
  vxor  $out2,$out2,$rndkey0
 vcipherlast $in5,$out5,$in5
  vadduwm $out5,$out3,$two
  vxor  $out3,$out3,$rndkey0
 vcipherlast $in6,$out6,$in6
  vadduwm $out6,$out4,$two
  vxor  $out4,$out4,$rndkey0
 vcipherlast $in7,$out7,$in7
  vadduwm $out7,$out5,$two
  vxor  $out5,$out5,$rndkey0
 le?vperm $in0,$in0,$in0,$inpperm
  vadduwm $ivec,$out6,$two # next counter value
  vxor  $out6,$out6,$rndkey0
 le?vperm $in1,$in1,$in1,$inpperm
  vxor  $out7,$out7,$rndkey0
 mtctr  $rounds

  vcipher $out0,$out0,v24
 stvx_u  $in0,$x00,$out
 le?vperm $in2,$in2,$in2,$inpperm
  vcipher $out1,$out1,v24
 stvx_u  $in1,$x10,$out
 le?vperm $in3,$in3,$in3,$inpperm
  vcipher $out2,$out2,v24
 stvx_u  $in2,$x20,$out
 le?vperm $in4,$in4,$in4,$inpperm
  vcipher $out3,$out3,v24
 stvx_u  $in3,$x30,$out
 le?vperm $in5,$in5,$in5,$inpperm
  vcipher $out4,$out4,v24
 stvx_u  $in4,$x40,$out
 le?vperm $in6,$in6,$in6,$inpperm
  vcipher $out5,$out5,v24
 stvx_u  $in5,$x50,$out
 le?vperm $in7,$in7,$in7,$inpperm
  vcipher $out6,$out6,v24
 stvx_u  $in6,$x60,$out
  vcipher $out7,$out7,v24
 stvx_u  $in7,$x70,$out
 addi  $out,$out,0x80

 b  Loop_ctr32_enc8x_middle

.align 5
Lctr32_enc8x_break:
 cmpwi  $len,-0x60
 blt  Lctr32_enc8x_one
 nop
 beq  Lctr32_enc8x_two
 cmpwi  $len,-0x40
 blt  Lctr32_enc8x_three
 nop
 beq  Lctr32_enc8x_four
 cmpwi  $len,-0x20
 blt  Lctr32_enc8x_five
 nop
 beq  Lctr32_enc8x_six
 cmpwi  $len,0x00
 blt  Lctr32_enc8x_seven

Lctr32_enc8x_eight:
 vcipherlast $out0,$out0,$in0
 vcipherlast $out1,$out1,$in1
 vcipherlast $out2,$out2,$in2
 vcipherlast $out3,$out3,$in3
 vcipherlast $out4,$out4,$in4
 vcipherlast $out5,$out5,$in5
 vcipherlast $out6,$out6,$in6
 vcipherlast $out7,$out7,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 le?vperm $out1,$out1,$out1,$inpperm
 stvx_u  $out0,$x00,$out
 le?vperm $out2,$out2,$out2,$inpperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$inpperm
 stvx_u  $out2,$x20,$out
 le?vperm $out4,$out4,$out4,$inpperm
 stvx_u  $out3,$x30,$out
 le?vperm $out5,$out5,$out5,$inpperm
 stvx_u  $out4,$x40,$out
 le?vperm $out6,$out6,$out6,$inpperm
 stvx_u  $out5,$x50,$out
 le?vperm $out7,$out7,$out7,$inpperm
 stvx_u  $out6,$x60,$out
 stvx_u  $out7,$x70,$out
 addi  $out,$out,0x80
 b  Lctr32_enc8x_done

.align 5
Lctr32_enc8x_seven:
 vcipherlast $out0,$out0,$in1
 vcipherlast $out1,$out1,$in2
 vcipherlast $out2,$out2,$in3
 vcipherlast $out3,$out3,$in4
 vcipherlast $out4,$out4,$in5
 vcipherlast $out5,$out5,$in6
 vcipherlast $out6,$out6,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 le?vperm $out1,$out1,$out1,$inpperm
 stvx_u  $out0,$x00,$out
 le?vperm $out2,$out2,$out2,$inpperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$inpperm
 stvx_u  $out2,$x20,$out
 le?vperm $out4,$out4,$out4,$inpperm
 stvx_u  $out3,$x30,$out
 le?vperm $out5,$out5,$out5,$inpperm
 stvx_u  $out4,$x40,$out
 le?vperm $out6,$out6,$out6,$inpperm
 stvx_u  $out5,$x50,$out
 stvx_u  $out6,$x60,$out
 addi  $out,$out,0x70
 b  Lctr32_enc8x_done

.align 5
Lctr32_enc8x_six:
 vcipherlast $out0,$out0,$in2
 vcipherlast $out1,$out1,$in3
 vcipherlast $out2,$out2,$in4
 vcipherlast $out3,$out3,$in5
 vcipherlast $out4,$out4,$in6
 vcipherlast $out5,$out5,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 le?vperm $out1,$out1,$out1,$inpperm
 stvx_u  $out0,$x00,$out
 le?vperm $out2,$out2,$out2,$inpperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$inpperm
 stvx_u  $out2,$x20,$out
 le?vperm $out4,$out4,$out4,$inpperm
 stvx_u  $out3,$x30,$out
 le?vperm $out5,$out5,$out5,$inpperm
 stvx_u  $out4,$x40,$out
 stvx_u  $out5,$x50,$out
 addi  $out,$out,0x60
 b  Lctr32_enc8x_done

.align 5
Lctr32_enc8x_five:
 vcipherlast $out0,$out0,$in3
 vcipherlast $out1,$out1,$in4
 vcipherlast $out2,$out2,$in5
 vcipherlast $out3,$out3,$in6
 vcipherlast $out4,$out4,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 le?vperm $out1,$out1,$out1,$inpperm
 stvx_u  $out0,$x00,$out
 le?vperm $out2,$out2,$out2,$inpperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$inpperm
 stvx_u  $out2,$x20,$out
 le?vperm $out4,$out4,$out4,$inpperm
 stvx_u  $out3,$x30,$out
 stvx_u  $out4,$x40,$out
 addi  $out,$out,0x50
 b  Lctr32_enc8x_done

.align 5
Lctr32_enc8x_four:
 vcipherlast $out0,$out0,$in4
 vcipherlast $out1,$out1,$in5
 vcipherlast $out2,$out2,$in6
 vcipherlast $out3,$out3,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 le?vperm $out1,$out1,$out1,$inpperm
 stvx_u  $out0,$x00,$out
 le?vperm $out2,$out2,$out2,$inpperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$inpperm
 stvx_u  $out2,$x20,$out
 stvx_u  $out3,$x30,$out
 addi  $out,$out,0x40
 b  Lctr32_enc8x_done

.align 5
Lctr32_enc8x_three:
 vcipherlast $out0,$out0,$in5
 vcipherlast $out1,$out1,$in6
 vcipherlast $out2,$out2,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 le?vperm $out1,$out1,$out1,$inpperm
 stvx_u  $out0,$x00,$out
 le?vperm $out2,$out2,$out2,$inpperm
 stvx_u  $out1,$x10,$out
 stvx_u  $out2,$x20,$out
 addi  $out,$out,0x30
 b  Lcbc_dec8x_done

.align 5
Lctr32_enc8x_two:
 vcipherlast $out0,$out0,$in6
 vcipherlast $out1,$out1,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 le?vperm $out1,$out1,$out1,$inpperm
 stvx_u  $out0,$x00,$out
 stvx_u  $out1,$x10,$out
 addi  $out,$out,0x20
 b  Lcbc_dec8x_done

.align 5
Lctr32_enc8x_one:
 vcipherlast $out0,$out0,$in7

 le?vperm $out0,$out0,$out0,$inpperm
 stvx_u  $out0,0,$out
 addi  $out,$out,0x10

Lctr32_enc8x_done:
 li  r10,`$FRAME+15`
 li  r11,`$FRAME+31`
 stvx  $inpperm,r10,$sp # wipe copies of round keys
 addi  r10,r10,32
 stvx  $inpperm,r11,$sp
 addi  r11,r11,32
 stvx  $inpperm,r10,$sp
 addi  r10,r10,32
 stvx  $inpperm,r11,$sp
 addi  r11,r11,32
 stvx  $inpperm,r10,$sp
 addi  r10,r10,32
 stvx  $inpperm,r11,$sp
 addi  r11,r11,32
 stvx  $inpperm,r10,$sp
 addi  r10,r10,32
 stvx  $inpperm,r11,$sp
 addi  r11,r11,32

 mtspr  256,$vrsave
 lvx  v20,r10,$sp  # ABI says so
 addi  r10,r10,32
 lvx  v21,r11,$sp
 addi  r11,r11,32
 lvx  v22,r10,$sp
 addi  r10,r10,32
 lvx  v23,r11,$sp
 addi  r11,r11,32
 lvx  v24,r10,$sp
 addi  r10,r10,32
 lvx  v25,r11,$sp
 addi  r11,r11,32
 lvx  v26,r10,$sp
 addi  r10,r10,32
 lvx  v27,r11,$sp
 addi  r11,r11,32
 lvx  v28,r10,$sp
 addi  r10,r10,32
 lvx  v29,r11,$sp
 addi  r11,r11,32
 lvx  v30,r10,$sp
 lvx  v31,r11,$sp
 $POP  r26,`$FRAME+21*16+0*$SIZE_T`($sp)
 $POP  r27,`$FRAME+21*16+1*$SIZE_T`($sp)
 $POP  r28,`$FRAME+21*16+2*$SIZE_T`($sp)
 $POP  r29,`$FRAME+21*16+3*$SIZE_T`($sp)
 $POP  r30,`$FRAME+21*16+4*$SIZE_T`($sp)
 $POP  r31,`$FRAME+21*16+5*$SIZE_T`($sp)
 addi  $sp,$sp,`$FRAME+21*16+6*$SIZE_T`
 blr
 .long  0
 .byte  0,12,0x04,0,0x80,6,6,0
 .long  0
.size .${prefix}_ctr32_encrypt_blocks,.-.${prefix}_ctr32_encrypt_blocks
___
}} }}}

#########################################################################
{{{ # XTS procedures      #
my ($inp,$out,$len,$key1,$key2,$ivp,$rounds,$idx) = map("r$_",(3..10));
my ($rndkey0,$rndkey1,$inout) =    map("v$_",(0..2));
my ($output,$inptail,$inpperm,$leperm,$keyperm) = map("v$_",(3..7));
my ($tweak,$seven,$eighty7,$tmp,$tweak1) =  map("v$_",(8..12));
my $taillen = $key2;

  ($inp,$idx) = ($idx,$inp);    # reassign

$code.=<<___;
.globl .${prefix}_xts_encrypt
.align 5
.${prefix}_xts_encrypt:
 mr  $inp,r3    # reassign
 li  r3,-1
 ${UCMP}i $len,16
 bltlr-

 lis  r0,0xfff0
 mfspr  r12,256    # save vrsave
 li  r11,0
 mtspr  256,r0

 vspltisb $seven,0x07   # 0x070707..07
 le?lvsl  $leperm,r11,r11
 le?vspltisb $tmp,0x0f
 le?vxor  $leperm,$leperm,$seven

 li  $idx,15
 lvx  $tweak,0,$ivp   # load [unaligned] iv
 lvsl  $inpperm,0,$ivp
 lvx  $inptail,$idx,$ivp
 le?vxor  $inpperm,$inpperm,$tmp
 vperm  $tweak,$tweak,$inptail,$inpperm

 ?lvsl  $keyperm,0,$key2  # prepare for unaligned key
 lwz  $rounds,240($key2)
 srwi  $rounds,$rounds,1
 subi  $rounds,$rounds,1
 li  $idx,16

 neg  r11,$inp
 lvsr  $inpperm,0,r11   # prepare for unaligned load
 lvx  $inout,0,$inp
 addi  $inp,$inp,15   # 15 is not typo
 le?vxor  $inpperm,$inpperm,$tmp

 lvx  $rndkey0,0,$key2
 lvx  $rndkey1,$idx,$key2
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $tweak,$tweak,$rndkey0
 lvx  $rndkey0,$idx,$key2
 addi  $idx,$idx,16
 mtctr  $rounds

Ltweak_xts_enc:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $tweak,$tweak,$rndkey1
 lvx  $rndkey1,$idx,$key2
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vcipher  $tweak,$tweak,$rndkey0
```

```
lvx  $rndkey0,$idx,$key2
addi  $idx,$idx,16
bdnz  Ltweak_xts_enc

?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
vcipher  $tweak,$tweak,$rndkey1
lvx  $rndkey1,$idx,$key2
li  $idx,16
?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
vcipherlast $tweak,$tweak,$rndkey0

lvx  $inptail,0,$inp
addi  $inp,$inp,16

?lvsl  $keyperm,0,$key1  # prepare for unaligned key
lwz  $rounds,240($key1)
srwi  $rounds,$rounds,1
subi  $rounds,$rounds,1
li  $idx,16

vslb  $eighty7,$seven,$seven  # 0x808080..80
vor  $eighty7,$eighty7,$seven # 0x878787..87
vspltisb $tmp,1    # 0x010101..01
vsldoi  $eighty7,$eighty7,$tmp,15 # 0x870101..01

${UCMP}i $len,96
bge  _aesp8_xts_encrypt6x

andi.  $taillen,$len,15
subic  r0,$len,32
subi  $taillen,$taillen,16
subfe  r0,r0,r0
and  r0,r0,$taillen
add  $inp,$inp,r0

lvx  $rndkey0,0,$key1
lvx  $rndkey1,$idx,$key1
addi  $idx,$idx,16
vperm  $inout,$inout,$inptail,$inpperm
?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
vxor  $inout,$inout,$tweak
vxor  $inout,$inout,$rndkey0
lvx  $rndkey0,$idx,$key1
addi  $idx,$idx,16
mtctr  $rounds
b  Loop_xts_enc

.align 5
```

```
Loop_xts_enc:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key1
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vcipher  $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key1
 addi  $idx,$idx,16
 bdnz  Loop_xts_enc

 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key1
 li  $idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $rndkey0,$rndkey0,$tweak
 vcipherlast $output,$inout,$rndkey0

 le?vperm $tmp,$output,$output,$leperm
 be?nop
 le?stvx_u $tmp,0,$out
 be?stvx_u $output,0,$out
 addi  $out,$out,16

 subic.  $len,$len,16
 beq  Lxts_enc_done

 vmr  $inout,$inptail
 lvx  $inptail,0,$inp
 addi  $inp,$inp,16
 lvx  $rndkey0,0,$key1
 lvx  $rndkey1,$idx,$key1
 addi  $idx,$idx,16

 subic  r0,$len,32
 subfe  r0,r0,r0
 and  r0,r0,$taillen
 add  $inp,$inp,r0

 vsrab  $tmp,$tweak,$seven  # next tweak value
 vaddubm  $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
 vand  $tmp,$tmp,$eighty7
 vxor  $tweak,$tweak,$tmp

 vperm  $inout,$inout,$inptail,$inpperm
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $inout,$inout,$tweak
 vxor  $output,$output,$rndkey0 # just in case $len<16
 vxor  $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key1
 addi  $idx,$idx,16

 mtctr  $rounds
 ${UCMP}i $len,16
 bge  Loop_xts_enc

 vxor  $output,$output,$tweak
 lvsr  $inpperm,0,$len   # $inpperm is no longer needed
 vxor  $inptail,$inptail,$inptail # $inptail is no longer needed
 vspltisb $tmp,-1
 vperm  $inptail,$inptail,$tmp,$inpperm
 vsel  $inout,$inout,$output,$inptail

 subi  r11,$out,17
 subi  $out,$out,16
 mtctr  $len
 li  $len,16
Loop_xts_enc_steal:
 lbzu  r0,1(r11)
 stb  r0,16(r11)
 bdnz  Loop_xts_enc_steal

 mtctr  $rounds
 b  Loop_xts_enc   # one more time...

Lxts_enc_done:
 mtspr  256,r12    # restore vrsave
 li  r3,0
 blr
 .long  0
 .byte  0,12,0x04,0,0x80,6,6,0
 .long  0
.size .${prefix}_xts_encrypt,.-.${prefix}_xts_encrypt

.globl .${prefix}_xts_decrypt
.align 5
.${prefix}_xts_decrypt:
 mr  $inp,r3    # reassign
 li  r3,-1
 ${UCMP}i $len,16
 bltlr-

 lis  r0,0xfff8
 mfspr  r12,256    # save vrsave
 li  r11,0
 mtspr  256,r0

 andi.  r0,$len,15
 neg  r0,r0
 andi.  r0,r0,16
 sub  $len,$len,r0

 vspltisb $seven,0x07   # 0x070707..07
 le?lvsl  $leperm,r11,r11
 le?vspltisb $tmp,0x0f
 le?vxor  $leperm,$leperm,$seven

 li  $idx,15
 lvx  $tweak,0,$ivp   # load [unaligned] iv
 lvsl  $inpperm,0,$ivp
 lvx  $inptail,$idx,$ivp
 le?vxor  $inpperm,$inpperm,$tmp
 vperm  $tweak,$tweak,$inptail,$inpperm

 ?lvsl  $keyperm,0,$key2  # prepare for unaligned key
 lwz  $rounds,240($key2)
 srwi  $rounds,$rounds,1
 subi  $rounds,$rounds,1
 li  $idx,16

 neg  r11,$inp
 lvsr  $inpperm,0,r11   # prepare for unaligned load
 lvx  $inout,0,$inp
 addi  $inp,$inp,15   # 15 is not typo
 le?vxor  $inpperm,$inpperm,$tmp

 lvx  $rndkey0,0,$key2
 lvx  $rndkey1,$idx,$key2
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $tweak,$tweak,$rndkey0
 lvx  $rndkey0,$idx,$key2
 addi  $idx,$idx,16
 mtctr  $rounds

Ltweak_xts_dec:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $tweak,$tweak,$rndkey1
 lvx  $rndkey1,$idx,$key2
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vcipher  $tweak,$tweak,$rndkey0
 lvx  $rndkey0,$idx,$key2
 addi  $idx,$idx,16
 bdnz  Ltweak_xts_dec

 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vcipher  $tweak,$tweak,$rndkey1
 lvx  $rndkey1,$idx,$key2
 li  $idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vcipherlast $tweak,$tweak,$rndkey0

 lvx  $inptail,0,$inp
 addi  $inp,$inp,16

 ?lvsl  $keyperm,0,$key1  # prepare for unaligned key
 lwz  $rounds,240($key1)
 srwi  $rounds,$rounds,1
 subi  $rounds,$rounds,1
 li  $idx,16

 vslb  $eighty7,$seven,$seven  # 0x808080..80
 vor  $eighty7,$eighty7,$seven # 0x878787..87
 vspltisb $tmp,1    # 0x010101..01
 vsldoi  $eighty7,$eighty7,$tmp,15 # 0x870101..01

 ${UCMP}i $len,96
 bge  _aesp8_xts_decrypt6x

 lvx  $rndkey0,0,$key1
 lvx  $rndkey1,$idx,$key1
 addi  $idx,$idx,16
 vperm  $inout,$inout,$inptail,$inpperm
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $inout,$inout,$tweak
 vxor  $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key1
 addi  $idx,$idx,16
 mtctr  $rounds

 ${UCMP}i $len,16
 blt  Ltail_xts_dec
 be?b  Loop_xts_dec

.align 5
Loop_xts_dec:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vncipher $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key1
```

```
addi  $idx,$idx,16
?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
vncipher $inout,$inout,$rndkey0
lvx  $rndkey0,$idx,$key1
addi  $idx,$idx,16
bdnz  Loop_xts_dec

?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
vncipher $inout,$inout,$rndkey1
lvx  $rndkey1,$idx,$key1
li  $idx,16
?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
vxor  $rndkey0,$rndkey0,$tweak
vncipherlast $output,$inout,$rndkey0

le?vperm $tmp,$output,$output,$leperm
be?nop
le?stvx_u $tmp,0,$out
be?stvx_u $output,0,$out
addi  $out,$out,16

subic.  $len,$len,16
beq  Lxts_dec_done

vmr  $inout,$inptail
lvx  $inptail,0,$inp
addi  $inp,$inp,16
lvx  $rndkey0,0,$key1
lvx  $rndkey1,$idx,$key1
addi  $idx,$idx,16

vsrab  $tmp,$tweak,$seven  # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
vand  $tmp,$tmp,$eighty7
vxor  $tweak,$tweak,$tmp

vperm  $inout,$inout,$inptail,$inpperm
?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
vxor  $inout,$inout,$tweak
vxor  $inout,$inout,$rndkey0
lvx  $rndkey0,$idx,$key1
addi  $idx,$idx,16

mtctr  $rounds
${UCMP}i $len,16
bge  Loop_xts_dec
```

```
Ltail_xts_dec:
 vsrab  $tmp,$tweak,$seven  # next tweak value
 vaddubm  $tweak1,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
 vand  $tmp,$tmp,$eighty7
 vxor  $tweak1,$tweak1,$tmp

 subi  $inp,$inp,16
 add  $inp,$inp,$len

 vxor  $inout,$inout,$tweak  # :-(
 vxor  $inout,$inout,$tweak1  # :-)

Loop_xts_dec_short:
 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vncipher $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key1
 addi  $idx,$idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vncipher $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key1
 addi  $idx,$idx,16
 bdnz  Loop_xts_dec_short

 ?vperm  $rndkey1,$rndkey1,$rndkey0,$keyperm
 vncipher $inout,$inout,$rndkey1
 lvx  $rndkey1,$idx,$key1
 li  $idx,16
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm
 vxor  $rndkey0,$rndkey0,$tweak1
 vncipherlast $output,$inout,$rndkey0

 le?vperm $tmp,$output,$output,$leperm
 be?nop
 le?stvx_u $tmp,0,$out
 be?stvx_u $output,0,$out

 vmr  $inout,$inptail
 lvx  $inptail,0,$inp
 #addi  $inp,$inp,16
 lvx  $rndkey0,0,$key1
 lvx  $rndkey1,$idx,$key1
 addi  $idx,$idx,16
 vperm  $inout,$inout,$inptail,$inpperm
 ?vperm  $rndkey0,$rndkey0,$rndkey1,$keyperm

 lvsr  $inpperm,0,$len   # $inpperm is no longer needed
 vxor  $inptail,$inptail,$inptail # $inptail is no longer needed
 vspltisb $tmp,-1
 vperm  $inptail,$inptail,$tmp,$inpperm
 vsel  $inout,$inout,$output,$inptail

 vxor  $rndkey0,$rndkey0,$tweak
 vxor  $inout,$inout,$rndkey0
 lvx  $rndkey0,$idx,$key1
 addi  $idx,$idx,16

 subi  r11,$out,1
 mtctr  $len
 li  $len,16
Loop_xts_dec_steal:
 lbzu  r0,1(r11)
 stb  r0,16(r11)
 bdnz  Loop_xts_dec_steal

 mtctr  $rounds
 b  Loop_xts_dec   # one more time...

Lxts_dec_done:
 mtspr  256,r12    # restore vrsave
 li  r3,0
 blr
 .long  0
 .byte  0,12,0x04,0,0x80,6,6,0
 .long  0
.size .${prefix}_xts_decrypt,.-.${prefix}_xts_decrypt
___
#########################################################################
{{ # Optimized XTS procedures     #
my $key_="r11";
my ($x00,$x10,$x20,$x30,$x40,$x50,$x60,$x70)=map("r$_",(0,8,26..31));
   $x00=0 if ($flavour =~ /osx/);
my ($in0,  $in1,  $in2,  $in3,  $in4,  $in5 )=map("v$_",(0..5));
my ($out0, $out1, $out2, $out3, $out4, $out5)=map("v$_",(7,12..16));
my ($twk0, $twk1, $twk2, $twk3, $twk4, $twk5)=map("v$_",(17..22));
my $rndkey0="v23"; # v24-v25 rotating buffer for first found keys
   # v26-v31 last 6 round keys
my ($keyperm)=($out0); # aliases with "caller", redundant assignment
my $taillen=$x70;

$code.=<<___;
.align 5
_aesp8_xts_encrypt6x:
 $STU  $sp,-`($FRAME+21*16+6*$SIZE_T)`($sp)
 mflr  r0
 li  r7,`$FRAME+8*16+15`
 li  r8,`$FRAME+8*16+31`
 $PUSH  r0,`$FRAME+21*16+6*$SIZE_T+$LRSAVE`($sp)
 stvx  v20,r7,$sp  # ABI says so
 addi  r7,r7,32
 stvx  v21,r8,$sp
 addi  r8,r8,32
 stvx  v22,r7,$sp
 addi  r7,r7,32
 stvx  v23,r8,$sp
 addi  r8,r8,32
 stvx  v24,r7,$sp
 addi  r7,r7,32
 stvx  v25,r8,$sp
 addi  r8,r8,32
 stvx  v26,r7,$sp
 addi  r7,r7,32
 stvx  v27,r8,$sp
 addi  r8,r8,32
 stvx  v28,r7,$sp
 addi  r7,r7,32
 stvx  v29,r8,$sp
 addi  r8,r8,32
 stvx  v30,r7,$sp
 stvx  v31,r8,$sp
 mr  r7,r0
 li  r0,-1
 stw  $vrsave,`$FRAME+21*16-4`($sp) # save vrsave
 li  $x10,0x10
 $PUSH  r26,`$FRAME+21*16+0*$SIZE_T`($sp)
 li  $x20,0x20
 $PUSH  r27,`$FRAME+21*16+1*$SIZE_T`($sp)
 li  $x30,0x30
 $PUSH  r28,`$FRAME+21*16+2*$SIZE_T`($sp)
 li  $x40,0x40
 $PUSH  r29,`$FRAME+21*16+3*$SIZE_T`($sp)
 li  $x50,0x50
 $PUSH  r30,`$FRAME+21*16+4*$SIZE_T`($sp)
 li  $x60,0x60
 $PUSH  r31,`$FRAME+21*16+5*$SIZE_T`($sp)
 li  $x70,0x70
 mtspr  256,r0

 subi  $rounds,$rounds,3 # -4 in total

 lvx  $rndkey0,$x00,$key1 # load key schedule
 lvx  v30,$x10,$key1
 addi  $key1,$key1,0x20
 lvx  v31,$x00,$key1
```

```
 ?vperm  $rndkey0,$rndkey0,v30,$keyperm
 addi  $key_,$sp,$FRAME+15
 mtctr  $rounds

Load_xts_enc_key:
 ?vperm  v24,v30,v31,$keyperm
 lvx  v30,$x10,$key1
 addi  $key1,$key1,0x20
 stvx  v24,$x00,$key_  # off-load round[1]
 ?vperm  v25,v31,v30,$keyperm
 lvx  v31,$x00,$key1
 stvx  v25,$x10,$key_  # off-load round[2]
 addi  $key_,$key_,0x20
 bdnz  Load_xts_enc_key

 lvx  v26,$x10,$key1
 ?vperm  v24,v30,v31,$keyperm
 lvx  v27,$x20,$key1
 stvx  v24,$x00,$key_  # off-load round[3]
 ?vperm  v25,v31,v26,$keyperm
 lvx  v28,$x30,$key1
 stvx  v25,$x10,$key_  # off-load round[4]
 addi  $key_,$sp,$FRAME+15 # rewind $key_
 ?vperm  v26,v26,v27,$keyperm
 lvx  v29,$x40,$key1
 ?vperm  v27,v27,v28,$keyperm
 lvx  v30,$x50,$key1
 ?vperm  v28,v28,v29,$keyperm
 lvx  v31,$x60,$key1
 ?vperm  v29,v29,v30,$keyperm
 lvx  $twk5,$x70,$key1 # borrow $twk5
 ?vperm  v30,v30,v31,$keyperm
 lvx  v24,$x00,$key_  # pre-load round[1]
 ?vperm  v31,v31,$twk5,$keyperm
 lvx  v25,$x10,$key_  # pre-load round[2]

  vperm  $in0,$inout,$inptail,$inpperm
  subi  $inp,$inp,31  # undo "caller"
 vxor  $twk0,$tweak,$rndkey0
 vsrab  $tmp,$tweak,$seven # next tweak value
 vaddubm  $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
 vand  $tmp,$tmp,$eighty7
  vxor  $out0,$in0,$twk0
 vxor  $tweak,$tweak,$tmp

  lvx_u  $in1,$x10,$inp
 vxor  $twk1,$tweak,$rndkey0
```

```
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in1,$in1,$in1,$leperm
vand  $tmp,$tmp,$eighty7
 vxor  $out1,$in1,$twk1
vxor  $tweak,$tweak,$tmp

 lvx_u  $in2,$x20,$inp
 andi.  $taillen,$len,15
vxor  $twk2,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in2,$in2,$in2,$leperm
vand  $tmp,$tmp,$eighty7
 vxor  $out2,$in2,$twk2
vxor  $tweak,$tweak,$tmp

 lvx_u  $in3,$x30,$inp
 sub  $len,$len,$taillen
vxor  $twk3,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in3,$in3,$in3,$leperm
vand  $tmp,$tmp,$eighty7
 vxor  $out3,$in3,$twk3
vxor  $tweak,$tweak,$tmp

 lvx_u  $in4,$x40,$inp
 subi  $len,$len,0x60
vxor  $twk4,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in4,$in4,$in4,$leperm
vand  $tmp,$tmp,$eighty7
 vxor  $out4,$in4,$twk4
vxor  $tweak,$tweak,$tmp

 lvx_u  $in5,$x50,$inp
 addi  $inp,$inp,0x60
vxor  $twk5,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in5,$in5,$in5,$leperm
 vand  $tmp,$tmp,$eighty7
  vxor  $out5,$in5,$twk5
 vxor  $tweak,$tweak,$tmp

 vxor  v31,v31,$rndkey0
 mtctr  $rounds
 b  Loop_xts_enc6x

.align 5
Loop_xts_enc6x:
 vcipher  $out0,$out0,v24
 vcipher  $out1,$out1,v24
 vcipher  $out2,$out2,v24
 vcipher  $out3,$out3,v24
 vcipher  $out4,$out4,v24
 vcipher  $out5,$out5,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vcipher  $out0,$out0,v25
 vcipher  $out1,$out1,v25
 vcipher  $out2,$out2,v25
 vcipher  $out3,$out3,v25
 vcipher  $out4,$out4,v25
 vcipher  $out5,$out5,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Loop_xts_enc6x

 subic  $len,$len,96  # $len-=96
  vxor  $in0,$twk0,v31  # xor with last round key
 vcipher  $out0,$out0,v24
 vcipher  $out1,$out1,v24
  vsrab  $tmp,$tweak,$seven # next tweak value
  vxor  $twk0,$tweak,$rndkey0
  vaddubm $tweak,$tweak,$tweak
 vcipher  $out2,$out2,v24
 vcipher  $out3,$out3,v24
  vsldoi  $tmp,$tmp,$tmp,15
 vcipher  $out4,$out4,v24
 vcipher  $out5,$out5,v24

 subfe.  r0,r0,r0  # borrow?-1:0
  vand  $tmp,$tmp,$eighty7
 vcipher  $out0,$out0,v25
 vcipher  $out1,$out1,v25
  vxor  $tweak,$tweak,$tmp
 vcipher  $out2,$out2,v25
 vcipher  $out3,$out3,v25
  vxor  $in1,$twk1,v31
  vsrab  $tmp,$tweak,$seven # next tweak value
  vxor  $twk1,$tweak,$rndkey0
 vcipher  $out4,$out4,v25
 vcipher  $out5,$out5,v25

 and  r0,r0,$len
  vaddubm $tweak,$tweak,$tweak
  vsldoi  $tmp,$tmp,$tmp,15
 vcipher  $out0,$out0,v26
 vcipher  $out1,$out1,v26
  vand  $tmp,$tmp,$eighty7
 vcipher  $out2,$out2,v26
 vcipher  $out3,$out3,v26
  vxor  $tweak,$tweak,$tmp
 vcipher  $out4,$out4,v26
 vcipher  $out5,$out5,v26

 add  $inp,$inp,r0  # $inp is adjusted in such
      # way that at exit from the
      # loop inX-in5 are loaded
      # with last "words"
  vxor  $in2,$twk2,v31
  vsrab  $tmp,$tweak,$seven # next tweak value
  vxor  $twk2,$tweak,$rndkey0
  vaddubm $tweak,$tweak,$tweak
 vcipher  $out0,$out0,v27
 vcipher  $out1,$out1,v27
  vsldoi  $tmp,$tmp,$tmp,15
 vcipher  $out2,$out2,v27
 vcipher  $out3,$out3,v27
  vand  $tmp,$tmp,$eighty7
 vcipher  $out4,$out4,v27
 vcipher  $out5,$out5,v27

 addi  $key_,$sp,$FRAME+15 # rewind $key_
  vxor  $tweak,$tweak,$tmp
 vcipher  $out0,$out0,v28
 vcipher  $out1,$out1,v28
  vxor  $in3,$twk3,v31
  vsrab  $tmp,$tweak,$seven # next tweak value
  vxor  $twk3,$tweak,$rndkey0
 vcipher  $out2,$out2,v28
 vcipher  $out3,$out3,v28
  vaddubm $tweak,$tweak,$tweak
  vsldoi  $tmp,$tmp,$tmp,15
 vcipher  $out4,$out4,v28
 vcipher  $out5,$out5,v28
```

```
lvx  v24,$x00,$key_  # re-pre-load round[1]
 vand  $tmp,$tmp,$eighty7

vcipher  $out0,$out0,v29
vcipher  $out1,$out1,v29
 vxor  $tweak,$tweak,$tmp
vcipher  $out2,$out2,v29
vcipher  $out3,$out3,v29
 vxor  $in4,$twk4,v31
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk4,$tweak,$rndkey0
vcipher  $out4,$out4,v29
vcipher  $out5,$out5,v29
lvx  v25,$x10,$key_  # re-pre-load round[2]
 vaddubm $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15

vcipher  $out0,$out0,v30
vcipher  $out1,$out1,v30
 vand  $tmp,$tmp,$eighty7
vcipher  $out2,$out2,v30
vcipher  $out3,$out3,v30
 vxor  $tweak,$tweak,$tmp
vcipher  $out4,$out4,v30
vcipher  $out5,$out5,v30
 vxor  $in5,$twk5,v31
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk5,$tweak,$rndkey0

vcipherlast $out0,$out0,$in0
 lvx_u  $in0,$x00,$inp  # load next input block
 vaddubm $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
vcipherlast $out1,$out1,$in1
 lvx_u  $in1,$x10,$inp
vcipherlast $out2,$out2,$in2
 le?vperm $in0,$in0,$in0,$leperm
 lvx_u  $in2,$x20,$inp
 vand  $tmp,$tmp,$eighty7
vcipherlast $out3,$out3,$in3
 le?vperm $in1,$in1,$in1,$leperm
 lvx_u  $in3,$x30,$inp
vcipherlast $out4,$out4,$in4
 le?vperm $in2,$in2,$in2,$leperm
 lvx_u  $in4,$x40,$inp
 vxor  $tweak,$tweak,$tmp
vcipherlast $tmp,$out5,$in5  # last block might be needed
     # in stealing mode
```

```
  le?vperm $in3,$in3,$in3,$leperm
  lvx_u  $in5,$x50,$inp
  addi  $inp,$inp,0x60
  le?vperm $in4,$in4,$in4,$leperm
  le?vperm $in5,$in5,$in5,$leperm

 le?vperm $out0,$out0,$out0,$leperm
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
  vxor  $out0,$in0,$twk0
 le?vperm $out2,$out2,$out2,$leperm
 stvx_u  $out1,$x10,$out
  vxor  $out1,$in1,$twk1
 le?vperm $out3,$out3,$out3,$leperm
 stvx_u  $out2,$x20,$out
  vxor  $out2,$in2,$twk2
 le?vperm $out4,$out4,$out4,$leperm
 stvx_u  $out3,$x30,$out
  vxor  $out3,$in3,$twk3
 le?vperm $out5,$tmp,$tmp,$leperm
 stvx_u  $out4,$x40,$out
  vxor  $out4,$in4,$twk4
 le?stvx_u $out5,$x50,$out
 be?stvx_u $tmp, $x50,$out
  vxor  $out5,$in5,$twk5
 addi  $out,$out,0x60

 mtctr  $rounds
 beq  Loop_xts_enc6x  # did $len-=96 borrow?

 addic.  $len,$len,0x60
 beq  Lxts_enc6x_zero
 cmpwi  $len,0x20
 blt  Lxts_enc6x_one
 nop
 beq  Lxts_enc6x_two
 cmpwi  $len,0x40
 blt  Lxts_enc6x_three
 nop
 beq  Lxts_enc6x_four

Lxts_enc6x_five:
 vxor  $out0,$in1,$twk0
 vxor  $out1,$in2,$twk1
 vxor  $out2,$in3,$twk2
 vxor  $out3,$in4,$twk3
 vxor  $out4,$in5,$twk4
 bl  _aesp8_xts_enc5x

 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk5  # unused tweak
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 le?vperm $out2,$out2,$out2,$leperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$leperm
 stvx_u  $out2,$x20,$out
 vxor  $tmp,$out4,$twk5 # last block prep for stealing
 le?vperm $out4,$out4,$out4,$leperm
 stvx_u  $out3,$x30,$out
 stvx_u  $out4,$x40,$out
 addi  $out,$out,0x50
 bne  Lxts_enc6x_steal
 b  Lxts_enc6x_done

.align 4
Lxts_enc6x_four:
 vxor  $out0,$in2,$twk0
 vxor  $out1,$in3,$twk1
 vxor  $out2,$in4,$twk2
 vxor  $out3,$in5,$twk3
 vxor  $out4,$out4,$out4

 bl  _aesp8_xts_enc5x

 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk4  # unused tweak
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 le?vperm $out2,$out2,$out2,$leperm
 stvx_u  $out1,$x10,$out
 vxor  $tmp,$out3,$twk4 # last block prep for stealing
 le?vperm $out3,$out3,$out3,$leperm
 stvx_u  $out2,$x20,$out
 stvx_u  $out3,$x30,$out
 addi  $out,$out,0x40
 bne  Lxts_enc6x_steal
 b  Lxts_enc6x_done

.align 4
Lxts_enc6x_three:
 vxor  $out0,$in3,$twk0
 vxor  $out1,$in4,$twk1
 vxor  $out2,$in5,$twk2
 vxor  $out3,$out3,$out3
 vxor  $out4,$out4,$out4

 bl  _aesp8_xts_enc5x

 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk3  # unused tweak
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 vxor  $tmp,$out2,$twk3 # last block prep for stealing
 le?vperm $out2,$out2,$out2,$leperm
 stvx_u  $out1,$x10,$out
 stvx_u  $out2,$x20,$out
 addi  $out,$out,0x30
 bne  Lxts_enc6x_steal
 b  Lxts_enc6x_done

.align 4
Lxts_enc6x_two:
 vxor  $out0,$in4,$twk0
 vxor  $out1,$in5,$twk1
 vxor  $out2,$out2,$out2
 vxor  $out3,$out3,$out3
 vxor  $out4,$out4,$out4

 bl  _aesp8_xts_enc5x

 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk2  # unused tweak
 vxor  $tmp,$out1,$twk2 # last block prep for stealing
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 stvx_u  $out1,$x10,$out
 addi  $out,$out,0x20
 bne  Lxts_enc6x_steal
 b  Lxts_enc6x_done

.align 4
Lxts_enc6x_one:
 vxor  $out0,$in5,$twk0
 nop
Loop_xts_enc1x:
 vcipher  $out0,$out0,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vcipher  $out0,$out0,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Loop_xts_enc1x
 add  $inp,$inp,$taillen
 cmpwi  $taillen,0
 vcipher  $out0,$out0,v24

 subi  $inp,$inp,16
 vcipher  $out0,$out0,v25

 lvsr  $inpperm,0,$taillen
 vcipher  $out0,$out0,v26

 lvx_u  $in0,0,$inp
 vcipher  $out0,$out0,v27

 addi  $key_,$sp,$FRAME+15 # rewind $key_
 vcipher  $out0,$out0,v28
 lvx  v24,$x00,$key_  # re-pre-load round[1]

 vcipher  $out0,$out0,v29
 lvx  v25,$x10,$key_  # re-pre-load round[2]
  vxor  $twk0,$twk0,v31

 le?vperm $in0,$in0,$in0,$leperm
 vcipher  $out0,$out0,v30

 vperm  $in0,$in0,$in0,$inpperm
 vcipherlast $out0,$out0,$twk0

 vmr  $twk0,$twk1  # unused tweak
 vxor  $tmp,$out0,$twk1 # last block prep for stealing
 le?vperm $out0,$out0,$out0,$leperm
 stvx_u  $out0,$x00,$out  # store output
 addi  $out,$out,0x10
 bne  Lxts_enc6x_steal
 b  Lxts_enc6x_done

.align 4
Lxts_enc6x_zero:
 cmpwi  $taillen,0
 beq  Lxts_enc6x_done

 add  $inp,$inp,$taillen
 subi  $inp,$inp,16
 lvx_u  $in0,0,$inp
 lvsr  $inpperm,0,$taillen # $in5 is no more
 le?vperm $in0,$in0,$in0,$leperm
 vperm  $in0,$in0,$in0,$inpperm
 vxor  $tmp,$tmp,$twk0
```

```
Lxts_enc6x_steal:
 vxor  $in0,$in0,$twk0
 vxor  $out0,$out0,$out0
 vspltisb $out1,-1
 vperm  $out0,$out0,$out1,$inpperm
 vsel  $out0,$in0,$tmp,$out0 # $tmp is last block, remember?

 subi  r3,$out,17
 subi  $out,$out,16
 mtctr  $taillen
Loop_xts_enc6x_steal:
 lbzu  r0,1(r3)
 stb  r0,16(r3)
 bdnz  Loop_xts_enc6x_steal

 li  $taillen,0
 mtctr  $rounds
 b  Loop_xts_enc1x  # one more time...

.align 4
Lxts_enc6x_done:
 mtlr  r7
 li  r10,`$FRAME+15`
 li  r11,`$FRAME+31`
 stvx  $seven,r10,$sp  # wipe copies of round keys
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32
 stvx  $seven,r10,$sp
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32
 stvx  $seven,r10,$sp
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32
 stvx  $seven,r10,$sp
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32

 mtspr  256,$vrsave
 lvx  v20,r10,$sp  # ABI says so
 addi  r10,r10,32
 lvx  v21,r11,$sp
 addi  r11,r11,32
 lvx  v22,r10,$sp
 addi  r10,r10,32
 lvx  v23,r11,$sp
 addi  r11,r11,32
 lvx  v24,r10,$sp
 addi  r10,r10,32
 lvx  v25,r11,$sp
 addi  r11,r11,32
 lvx  v26,r10,$sp
 addi  r10,r10,32
 lvx  v27,r11,$sp
 addi  r11,r11,32
 lvx  v28,r10,$sp
 addi  r10,r10,32
 lvx  v29,r11,$sp
 addi  r11,r11,32
 lvx  v30,r10,$sp
 lvx  v31,r11,$sp
 $POP  r26,`$FRAME+21*16+0*$SIZE_T`($sp)
 $POP  r27,`$FRAME+21*16+1*$SIZE_T`($sp)
 $POP  r28,`$FRAME+21*16+2*$SIZE_T`($sp)
 $POP  r29,`$FRAME+21*16+3*$SIZE_T`($sp)
 $POP  r30,`$FRAME+21*16+4*$SIZE_T`($sp)
 $POP  r31,`$FRAME+21*16+5*$SIZE_T`($sp)
 addi  $sp,$sp,`$FRAME+21*16+6*$SIZE_T`
 blr
 .long  0
 .byte  0,12,0x04,1,0x80,6,6,0
 .long  0

.align 5
_aesp8_xts_enc5x:
 vcipher  $out0,$out0,v24
 vcipher  $out1,$out1,v24
 vcipher  $out2,$out2,v24
 vcipher  $out3,$out3,v24
 vcipher  $out4,$out4,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vcipher  $out0,$out0,v25
 vcipher  $out1,$out1,v25
 vcipher  $out2,$out2,v25
 vcipher  $out3,$out3,v25
 vcipher  $out4,$out4,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  _aesp8_xts_enc5x

 add  $inp,$inp,$taillen
 cmpwi  $taillen,0
```

```
vcipher  $out0,$out0,v24
vcipher  $out1,$out1,v24
vcipher  $out2,$out2,v24
vcipher  $out3,$out3,v24
vcipher  $out4,$out4,v24

subi  $inp,$inp,16
vcipher  $out0,$out0,v25
vcipher  $out1,$out1,v25
vcipher  $out2,$out2,v25
vcipher  $out3,$out3,v25
vcipher  $out4,$out4,v25
 vxor  $twk0,$twk0,v31

vcipher  $out0,$out0,v26
lvsr  $inpperm,r0,$taillen # $in5 is no more
vcipher  $out1,$out1,v26
vcipher  $out2,$out2,v26
vcipher  $out3,$out3,v26
vcipher  $out4,$out4,v26
 vxor  $in1,$twk1,v31

vcipher  $out0,$out0,v27
lvx_u  $in0,0,$inp
vcipher  $out1,$out1,v27
vcipher  $out2,$out2,v27
vcipher  $out3,$out3,v27
vcipher  $out4,$out4,v27
 vxor  $in2,$twk2,v31

addi  $key_,$sp,$FRAME+15 # rewind $key_
vcipher  $out0,$out0,v28
vcipher  $out1,$out1,v28
vcipher  $out2,$out2,v28
vcipher  $out3,$out3,v28
vcipher  $out4,$out4,v28
lvx  v24,$x00,$key_  # re-pre-load round[1]
 vxor  $in3,$twk3,v31

vcipher  $out0,$out0,v29
le?vperm $in0,$in0,$in0,$leperm
vcipher  $out1,$out1,v29
vcipher  $out2,$out2,v29
vcipher  $out3,$out3,v29
vcipher  $out4,$out4,v29
lvx  v25,$x10,$key_  # re-pre-load round[2]
 vxor  $in4,$twk4,v31
 vcipher  $out0,$out0,v30
 vperm  $in0,$in0,$in0,$inpperm
 vcipher  $out1,$out1,v30
 vcipher  $out2,$out2,v30
 vcipher  $out3,$out3,v30
 vcipher  $out4,$out4,v30

 vcipherlast $out0,$out0,$twk0
 vcipherlast $out1,$out1,$in1
 vcipherlast $out2,$out2,$in2
 vcipherlast $out3,$out3,$in3
 vcipherlast $out4,$out4,$in4
 blr
       .long    0
       .byte    0,12,0x14,0,0,0,0,0

.align 5
_aesp8_xts_decrypt6x:
 $STU  $sp,-`($FRAME+21*16+6*$SIZE_T)`($sp)
 mflr  r0
 li  r7,`$FRAME+8*16+15`
 li  r8,`$FRAME+8*16+31`
 $PUSH  r0,`$FRAME+21*16+6*$SIZE_T+$LRSAVE`($sp)
 stvx  v20,r7,$sp  # ABI says so
 addi  r7,r7,32
 stvx  v21,r8,$sp
 addi  r8,r8,32
 stvx  v22,r7,$sp
 addi  r7,r7,32
 stvx  v23,r8,$sp
 addi  r8,r8,32
 stvx  v24,r7,$sp
 addi  r7,r7,32
 stvx  v25,r8,$sp
 addi  r8,r8,32
 stvx  v26,r7,$sp
 addi  r7,r7,32
 stvx  v27,r8,$sp
 addi  r8,r8,32
 stvx  v28,r7,$sp
 addi  r7,r7,32
 stvx  v29,r8,$sp
 addi  r8,r8,32
 stvx  v30,r7,$sp
 stvx  v31,r8,$sp
 mr  r7,r0
 li  r0,-1
 stw  $vrsave,`$FRAME+21*16-4`($sp) # save vrsave
 li  $x10,0x10
 $PUSH  r26,`$FRAME+21*16+0*$SIZE_T`($sp)
 li  $x20,0x20
 $PUSH  r27,`$FRAME+21*16+1*$SIZE_T`($sp)
 li  $x30,0x30
 $PUSH  r28,`$FRAME+21*16+2*$SIZE_T`($sp)
 li  $x40,0x40
 $PUSH  r29,`$FRAME+21*16+3*$SIZE_T`($sp)
 li  $x50,0x50
 $PUSH  r30,`$FRAME+21*16+4*$SIZE_T`($sp)
 li  $x60,0x60
 $PUSH  r31,`$FRAME+21*16+5*$SIZE_T`($sp)
 li  $x70,0x70
 mtspr  256,r0

 subi  $rounds,$rounds,3 # -4 in total

 lvx  $rndkey0,$x00,$key1 # load key schedule
 lvx  v30,$x10,$key1
 addi  $key1,$key1,0x20
 lvx  v31,$x00,$key1
 ?vperm  $rndkey0,$rndkey0,v30,$keyperm
 addi  $key_,$sp,$FRAME+15
 mtctr  $rounds

Load_xts_dec_key:
 ?vperm  v24,v30,v31,$keyperm
 lvx  v30,$x10,$key1
 addi  $key1,$key1,0x20
 stvx  v24,$x00,$key_  # off-load round[1]
 ?vperm  v25,v31,v30,$keyperm
 lvx  v31,$x00,$key1
 stvx  v25,$x10,$key_  # off-load round[2]
 addi  $key_,$key_,0x20
 bdnz  Load_xts_dec_key

 lvx  v26,$x10,$key1
 ?vperm  v24,v30,v31,$keyperm
 lvx  v27,$x20,$key1
 stvx  v24,$x00,$key_  # off-load round[3]
 ?vperm  v25,v31,v26,$keyperm
 lvx  v28,$x30,$key1
 stvx  v25,$x10,$key_  # off-load round[4]
 addi  $key_,$sp,$FRAME+15 # rewind $key_
 ?vperm  v26,v26,v27,$keyperm
 lvx  v29,$x40,$key1
 ?vperm  v27,v27,v28,$keyperm
 lvx  v30,$x50,$key1
```

```
?vperm  v28,v28,v29,$keyperm
lvx  v31,$x60,$key1
?vperm  v29,v29,v30,$keyperm
lvx  $twk5,$x70,$key1 # borrow $twk5
?vperm  v30,v30,v31,$keyperm
lvx  v24,$x00,$key_  # pre-load round[1]
?vperm  v31,v31,$twk5,$keyperm
lvx  v25,$x10,$key_  # pre-load round[2]

 vperm  $in0,$inout,$inptail,$inpperm
 subi  $inp,$inp,31  # undo "caller"
vxor  $twk0,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
vand  $tmp,$tmp,$eighty7
 vxor  $out0,$in0,$twk0
vxor  $tweak,$tweak,$tmp

 lvx_u  $in1,$x10,$inp
vxor  $twk1,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in1,$in1,$in1,$leperm
vand  $tmp,$tmp,$eighty7
 vxor  $out1,$in1,$twk1
vxor  $tweak,$tweak,$tmp

 lvx_u  $in2,$x20,$inp
 andi.  $taillen,$len,15
vxor  $twk2,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in2,$in2,$in2,$leperm
vand  $tmp,$tmp,$eighty7
 vxor  $out2,$in2,$twk2
vxor  $tweak,$tweak,$tmp

 lvx_u  $in3,$x30,$inp
 sub  $len,$len,$taillen
vxor  $twk3,$tweak,$rndkey0
vsrab  $tmp,$tweak,$seven # next tweak value
vaddubm  $tweak,$tweak,$tweak
vsldoi  $tmp,$tmp,$tmp,15
 le?vperm $in3,$in3,$in3,$leperm
vand  $tmp,$tmp,$eighty7
```

```
  vxor  $out3,$in3,$twk3
 vxor  $tweak,$tweak,$tmp

  lvx_u  $in4,$x40,$inp
  subi  $len,$len,0x60
 vxor  $twk4,$tweak,$rndkey0
 vsrab  $tmp,$tweak,$seven # next tweak value
 vaddubm  $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
  le?vperm $in4,$in4,$in4,$leperm
 vand  $tmp,$tmp,$eighty7
  vxor  $out4,$in4,$twk4
 vxor  $tweak,$tweak,$tmp

  lvx_u  $in5,$x50,$inp
  addi  $inp,$inp,0x60
 vxor  $twk5,$tweak,$rndkey0
 vsrab  $tmp,$tweak,$seven # next tweak value
 vaddubm  $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
  le?vperm $in5,$in5,$in5,$leperm
 vand  $tmp,$tmp,$eighty7
  vxor  $out5,$in5,$twk5
 vxor  $tweak,$tweak,$tmp

 vxor  v31,v31,$rndkey0
 mtctr  $rounds
 b  Loop_xts_dec6x

.align 5
Loop_xts_dec6x:
 vncipher $out0,$out0,v24
 vncipher $out1,$out1,v24
 vncipher $out2,$out2,v24
 vncipher $out3,$out3,v24
 vncipher $out4,$out4,v24
 vncipher $out5,$out5,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vncipher $out0,$out0,v25
 vncipher $out1,$out1,v25
 vncipher $out2,$out2,v25
 vncipher $out3,$out3,v25
 vncipher $out4,$out4,v25
 vncipher $out5,$out5,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Loop_xts_dec6x
```

```
subic  $len,$len,96  # $len-=96
 vxor  $in0,$twk0,v31  # xor with last round key
vncipher $out0,$out0,v24
vncipher $out1,$out1,v24
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk0,$tweak,$rndkey0
 vaddubm $tweak,$tweak,$tweak
vncipher $out2,$out2,v24
vncipher $out3,$out3,v24
 vsldoi  $tmp,$tmp,$tmp,15
vncipher $out4,$out4,v24
vncipher $out5,$out5,v24

subfe.  r0,r0,r0  # borrow?-1:0
 vand  $tmp,$tmp,$eighty7
vncipher $out0,$out0,v25
vncipher $out1,$out1,v25
 vxor  $tweak,$tweak,$tmp
vncipher $out2,$out2,v25
vncipher $out3,$out3,v25
 vxor  $in1,$twk1,v31
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk1,$tweak,$rndkey0
vncipher $out4,$out4,v25
vncipher $out5,$out5,v25

and  r0,r0,$len
 vaddubm $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
vncipher $out0,$out0,v26
vncipher $out1,$out1,v26
 vand  $tmp,$tmp,$eighty7
vncipher $out2,$out2,v26
vncipher $out3,$out3,v26
 vxor  $tweak,$tweak,$tmp
vncipher $out4,$out4,v26
vncipher $out5,$out5,v26

add  $inp,$inp,r0  # $inp is adjusted in such
     # way that at exit from the
     # loop inX-in5 are loaded
     # with last "words"
 vxor  $in2,$twk2,v31
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk2,$tweak,$rndkey0
 vaddubm $tweak,$tweak,$tweak
vncipher $out0,$out0,v27
vncipher $out1,$out1,v27
 vsldoi  $tmp,$tmp,$tmp,15
vncipher $out2,$out2,v27
vncipher $out3,$out3,v27
 vand  $tmp,$tmp,$eighty7
vncipher $out4,$out4,v27
vncipher $out5,$out5,v27

addi  $key_,$sp,$FRAME+15 # rewind $key_
 vxor  $tweak,$tweak,$tmp
vncipher $out0,$out0,v28
vncipher $out1,$out1,v28
 vxor  $in3,$twk3,v31
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk3,$tweak,$rndkey0
vncipher $out2,$out2,v28
vncipher $out3,$out3,v28
 vaddubm $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
vncipher $out4,$out4,v28
vncipher $out5,$out5,v28
lvx  v24,$x00,$key_  # re-pre-load round[1]
 vand  $tmp,$tmp,$eighty7

vncipher $out0,$out0,v29
vncipher $out1,$out1,v29
 vxor  $tweak,$tweak,$tmp
vncipher $out2,$out2,v29
vncipher $out3,$out3,v29
 vxor  $in4,$twk4,v31
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk4,$tweak,$rndkey0
vncipher $out4,$out4,v29
vncipher $out5,$out5,v29
lvx  v25,$x10,$key_  # re-pre-load round[2]
 vaddubm $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15

vncipher $out0,$out0,v30
vncipher $out1,$out1,v30
 vand  $tmp,$tmp,$eighty7
vncipher $out2,$out2,v30
vncipher $out3,$out3,v30
 vxor  $tweak,$tweak,$tmp
vncipher $out4,$out4,v30
vncipher $out5,$out5,v30
 vxor  $in5,$twk5,v31
 vsrab  $tmp,$tweak,$seven # next tweak value
 vxor  $twk5,$tweak,$rndkey0

vncipherlast $out0,$out0,$in0
 lvx_u  $in0,$x00,$inp  # load next input block
 vaddubm $tweak,$tweak,$tweak
 vsldoi  $tmp,$tmp,$tmp,15
vncipherlast $out1,$out1,$in1
 lvx_u  $in1,$x10,$inp
vncipherlast $out2,$out2,$in2
 le?vperm $in0,$in0,$in0,$leperm
 lvx_u  $in2,$x20,$inp
 vand  $tmp,$tmp,$eighty7
vncipherlast $out3,$out3,$in3
 le?vperm $in1,$in1,$in1,$leperm
 lvx_u  $in3,$x30,$inp
vncipherlast $out4,$out4,$in4
 le?vperm $in2,$in2,$in2,$leperm
 lvx_u  $in4,$x40,$inp
 vxor  $tweak,$tweak,$tmp
vncipherlast $out5,$out5,$in5
 le?vperm $in3,$in3,$in3,$leperm
 lvx_u  $in5,$x50,$inp
 addi  $inp,$inp,0x60
 le?vperm $in4,$in4,$in4,$leperm
 le?vperm $in5,$in5,$in5,$leperm

le?vperm $out0,$out0,$out0,$leperm
le?vperm $out1,$out1,$out1,$leperm
stvx_u  $out0,$x00,$out  # store output
 vxor  $out0,$in0,$twk0
le?vperm $out2,$out2,$out2,$leperm
stvx_u  $out1,$x10,$out
 vxor  $out1,$in1,$twk1
le?vperm $out3,$out3,$out3,$leperm
stvx_u  $out2,$x20,$out
 vxor  $out2,$in2,$twk2
le?vperm $out4,$out4,$out4,$leperm
stvx_u  $out3,$x30,$out
 vxor  $out3,$in3,$twk3
le?vperm $out5,$out5,$out5,$leperm
stvx_u  $out4,$x40,$out
 vxor  $out4,$in4,$twk4
stvx_u  $out5,$x50,$out
 vxor  $out5,$in5,$twk5
addi  $out,$out,0x60

mtctr  $rounds
beq  Loop_xts_dec6x  # did $len-=96 borrow?
```

```
 addic.  $len,$len,0x60
 beq  Lxts_dec6x_zero
 cmpwi  $len,0x20
 blt  Lxts_dec6x_one
 nop
 beq  Lxts_dec6x_two
 cmpwi  $len,0x40
 blt  Lxts_dec6x_three
 nop
 beq  Lxts_dec6x_four

Lxts_dec6x_five:
 vxor  $out0,$in1,$twk0
 vxor  $out1,$in2,$twk1
 vxor  $out2,$in3,$twk2
 vxor  $out3,$in4,$twk3
 vxor  $out4,$in5,$twk4

 bl  _aesp8_xts_dec5x

 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk5  # unused tweak
 vxor  $twk1,$tweak,$rndkey0
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 vxor  $out0,$in0,$twk1
 le?vperm $out2,$out2,$out2,$leperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$leperm
 stvx_u  $out2,$x20,$out
 le?vperm $out4,$out4,$out4,$leperm
 stvx_u  $out3,$x30,$out
 stvx_u  $out4,$x40,$out
 addi  $out,$out,0x50
 bne  Lxts_dec6x_steal
 b  Lxts_dec6x_done

.align 4
Lxts_dec6x_four:
 vxor  $out0,$in2,$twk0
 vxor  $out1,$in3,$twk1
 vxor  $out2,$in4,$twk2
 vxor  $out3,$in5,$twk3
 vxor  $out4,$out4,$out4

 bl  _aesp8_xts_dec5x
 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk4  # unused tweak
 vmr  $twk1,$twk5
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 vxor  $out0,$in0,$twk5
 le?vperm $out2,$out2,$out2,$leperm
 stvx_u  $out1,$x10,$out
 le?vperm $out3,$out3,$out3,$leperm
 stvx_u  $out2,$x20,$out
 stvx_u  $out3,$x30,$out
 addi  $out,$out,0x40
 bne  Lxts_dec6x_steal
 b  Lxts_dec6x_done

.align 4
Lxts_dec6x_three:
 vxor  $out0,$in3,$twk0
 vxor  $out1,$in4,$twk1
 vxor  $out2,$in5,$twk2
 vxor  $out3,$out3,$out3
 vxor  $out4,$out4,$out4

 bl  _aesp8_xts_dec5x

 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk3  # unused tweak
 vmr  $twk1,$twk4
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 vxor  $out0,$in0,$twk4
 le?vperm $out2,$out2,$out2,$leperm
 stvx_u  $out1,$x10,$out
 stvx_u  $out2,$x20,$out
 addi  $out,$out,0x30
 bne  Lxts_dec6x_steal
 b  Lxts_dec6x_done

.align 4
Lxts_dec6x_two:
 vxor  $out0,$in4,$twk0
 vxor  $out1,$in5,$twk1
 vxor  $out2,$out2,$out2
 vxor  $out3,$out3,$out3
 vxor  $out4,$out4,$out4

 bl  _aesp8_xts_dec5x
 le?vperm $out0,$out0,$out0,$leperm
 vmr  $twk0,$twk2  # unused tweak
 vmr  $twk1,$twk3
 le?vperm $out1,$out1,$out1,$leperm
 stvx_u  $out0,$x00,$out  # store output
 vxor  $out0,$in0,$twk3
 stvx_u  $out1,$x10,$out
 addi  $out,$out,0x20
 bne  Lxts_dec6x_steal
 b  Lxts_dec6x_done

.align 4
Lxts_dec6x_one:
 vxor  $out0,$in5,$twk0
 nop
Loop_xts_dec1x:
 vncipher $out0,$out0,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vncipher $out0,$out0,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Loop_xts_dec1x

 subi  r0,$taillen,1
 vncipher $out0,$out0,v24

 andi.  r0,r0,16
 cmpwi  $taillen,0
 vncipher $out0,$out0,v25

 sub  $inp,$inp,r0
 vncipher $out0,$out0,v26

 lvx_u  $in0,0,$inp
 vncipher $out0,$out0,v27

 addi  $key_,$sp,$FRAME+15 # rewind $key_
 vncipher $out0,$out0,v28
 lvx  v24,$x00,$key_  # re-pre-load round[1]

 vncipher $out0,$out0,v29
 lvx  v25,$x10,$key_  # re-pre-load round[2]
  vxor  $twk0,$twk0,v31

 le?vperm $in0,$in0,$in0,$leperm
 vncipher $out0,$out0,v30
 mtctr  $rounds
 vncipherlast $out0,$out0,$twk0

 vmr  $twk0,$twk1  # unused tweak
 vmr  $twk1,$twk2
 le?vperm $out0,$out0,$out0,$leperm
 stvx_u  $out0,$x00,$out  # store output
 addi  $out,$out,0x10
 vxor  $out0,$in0,$twk2
 bne  Lxts_dec6x_steal
 b  Lxts_dec6x_done

.align 4
Lxts_dec6x_zero:
 cmpwi  $taillen,0
 beq  Lxts_dec6x_done

 lvx_u  $in0,0,$inp
 le?vperm $in0,$in0,$in0,$leperm
 vxor  $out0,$in0,$twk1
Lxts_dec6x_steal:
 vncipher $out0,$out0,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vncipher $out0,$out0,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  Lxts_dec6x_steal

 add  $inp,$inp,$taillen
 vncipher $out0,$out0,v24

 cmpwi  $taillen,0
 vncipher $out0,$out0,v25

 lvx_u  $in0,0,$inp
 vncipher $out0,$out0,v26

 lvsr  $inpperm,0,$taillen # $in5 is no more
 vncipher $out0,$out0,v27

 addi  $key_,$sp,$FRAME+15 # rewind $key_
 vncipher $out0,$out0,v28
 lvx  v24,$x00,$key_  # re-pre-load round[1]

 vncipher $out0,$out0,v29
 lvx  v25,$x10,$key_  # re-pre-load round[2]
  vxor  $twk1,$twk1,v31
 le?vperm $in0,$in0,$in0,$leperm
 vncipher $out0,$out0,v30

 vperm  $in0,$in0,$in0,$inpperm
 vncipherlast $tmp,$out0,$twk1

 le?vperm $out0,$tmp,$tmp,$leperm
 le?stvx_u $out0,0,$out
 be?stvx_u $tmp,0,$out

 vxor  $out0,$out0,$out0
 vspltisb $out1,-1
 vperm  $out0,$out0,$out1,$inpperm
 vsel  $out0,$in0,$tmp,$out0
 vxor  $out0,$out0,$twk0

 subi  r3,$out,1
 mtctr  $taillen
Loop_xts_dec6x_steal:
 lbzu  r0,1(r3)
 stb  r0,16(r3)
 bdnz  Loop_xts_dec6x_steal

 li  $taillen,0
 mtctr  $rounds
 b  Loop_xts_dec1x  # one more time...

.align 4
Lxts_dec6x_done:
 mtlr  r7
 li  r10,`$FRAME+15`
 li  r11,`$FRAME+31`
 stvx  $seven,r10,$sp  # wipe copies of round keys
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32
 stvx  $seven,r10,$sp
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32
 stvx  $seven,r10,$sp
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32
 stvx  $seven,r10,$sp
 addi  r10,r10,32
 stvx  $seven,r11,$sp
 addi  r11,r11,32

 mtspr  256,$vrsave
 lvx  v20,r10,$sp  # ABI says so
 addi  r10,r10,32
 lvx  v21,r11,$sp
 addi  r11,r11,32
 lvx  v22,r10,$sp
 addi  r10,r10,32
 lvx  v23,r11,$sp
 addi  r11,r11,32
 lvx  v24,r10,$sp
 addi  r10,r10,32
 lvx  v25,r11,$sp
 addi  r11,r11,32
 lvx  v26,r10,$sp
 addi  r10,r10,32
 lvx  v27,r11,$sp
 addi  r11,r11,32
 lvx  v28,r10,$sp
 addi  r10,r10,32
 lvx  v29,r11,$sp
 addi  r11,r11,32
 lvx  v30,r10,$sp
 lvx  v31,r11,$sp
 $POP  r26,`$FRAME+21*16+0*$SIZE_T`($sp)
 $POP  r27,`$FRAME+21*16+1*$SIZE_T`($sp)
 $POP  r28,`$FRAME+21*16+2*$SIZE_T`($sp)
 $POP  r29,`$FRAME+21*16+3*$SIZE_T`($sp)
 $POP  r30,`$FRAME+21*16+4*$SIZE_T`($sp)
 $POP  r31,`$FRAME+21*16+5*$SIZE_T`($sp)
 addi  $sp,$sp,`$FRAME+21*16+6*$SIZE_T`
 blr
 .long  0
 .byte  0,12,0x04,1,0x80,6,6,0
 .long  0

.align 5
_aesp8_xts_dec5x:
 vncipher $out0,$out0,v24
 vncipher $out1,$out1,v24
 vncipher $out2,$out2,v24
 vncipher $out3,$out3,v24
 vncipher $out4,$out4,v24
 lvx  v24,$x20,$key_  # round[3]
 addi  $key_,$key_,0x20

 vncipher $out0,$out0,v25
 vncipher $out1,$out1,v25
 vncipher $out2,$out2,v25
 vncipher $out3,$out3,v25
 vncipher $out4,$out4,v25
 lvx  v25,$x10,$key_  # round[4]
 bdnz  _aesp8_xts_dec5x

 subi  r0,$taillen,1
 vncipher $out0,$out0,v24
 vncipher $out1,$out1,v24
 vncipher $out2,$out2,v24
 vncipher $out3,$out3,v24
 vncipher $out4,$out4,v24

 andi.  r0,r0,16
 cmpwi  $taillen,0
 vncipher $out0,$out0,v25
 vncipher $out1,$out1,v25
 vncipher $out2,$out2,v25
 vncipher $out3,$out3,v25
 vncipher $out4,$out4,v25
  vxor  $twk0,$twk0,v31

 sub  $inp,$inp,r0
 vncipher $out0,$out0,v26
 vncipher $out1,$out1,v26
 vncipher $out2,$out2,v26
 vncipher $out3,$out3,v26
 vncipher $out4,$out4,v26
  vxor  $in1,$twk1,v31

 vncipher $out0,$out0,v27
 lvx_u  $in0,0,$inp
 vncipher $out1,$out1,v27
 vncipher $out2,$out2,v27
 vncipher $out3,$out3,v27
 vncipher $out4,$out4,v27
  vxor  $in2,$twk2,v31

 addi  $key_,$sp,$FRAME+15 # rewind $key_
 vncipher $out0,$out0,v28
 vncipher $out1,$out1,v28
 vncipher $out2,$out2,v28
 vncipher $out3,$out3,v28
 vncipher $out4,$out4,v28
 lvx  v24,$x00,$key_  # re-pre-load round[1]
  vxor  $in3,$twk3,v31
 vncipher $out0,$out0,v29
 le?vperm $in0,$in0,$in0,$leperm
 vncipher $out1,$out1,v29
 vncipher $out2,$out2,v29
 vncipher $out3,$out3,v29
 vncipher $out4,$out4,v29
 lvx  v25,$x10,$key_  # re-pre-load round[2]
  vxor  $in4,$twk4,v31

 vncipher $out0,$out0,v30
 vncipher $out1,$out1,v30
 vncipher $out2,$out2,v30
 vncipher $out3,$out3,v30
 vncipher $out4,$out4,v30

 vncipherlast $out0,$out0,$twk0
 vncipherlast $out1,$out1,$in1
 vncipherlast $out2,$out2,$in2
 vncipherlast $out3,$out3,$in3
 vncipherlast $out4,$out4,$in4
 mtctr  $rounds
 blr
       .long    0
       .byte    0,12,0x14,0,0,0,0,0
___
}} }}}

my $consts=1;
foreach(split("\n",$code)) {
       s/\`([^\`]*)\`/eval($1)/geo;

 # constants table endian-specific conversion
 if ($consts && m/\.(long|byte)\s+(.+)\s+(\?[a-z]*)$/o) {
     my $conv=$3;
     my @bytes=();

     # convert to endian-agnostic format
     if ($1 eq "long") {
       foreach (split(/,\s*/,$2)) {
  my $l = /^0/?oct:int;
  push @bytes,($l>>24)&0xff,($l>>16)&0xff,($l>>8)&0xff,$l&0xff;
       }
     } else {
  @bytes = map(/^0/?oct:int,split(/,\s*/,$2));
     }

     # little-endian conversion
     if ($flavour =~ /le$/o) {
```

```
  SWITCH: for($conv)  {
      /\?inv/ && do   { @bytes=map($_^0xf,@bytes); last; };
      /\?rev/ && do   { @bytes=reverse(@bytes);    last; };
  }
     }

     #emit
     print ".byte\t",join(',',map (sprintf("0x%02x",$_),@bytes)),"\n";
     next;
 }
 $consts=0 if (m/Lconsts:/o); # end of table

 # instructions prefixed with '?' are endian-specific and need
 # to be adjusted accordingly...
 if ($flavour =~ /le$/o) { # little-endian
     s/le\?//o  or
     s/be\?/#be#/o or
     s/\?lvsr/lvsl/o or
     s/\?lvsl/lvsr/o or
     s/\?(vperm\s+v[0-9]+,\s*)(v[0-9]+,\s*)(v[0-9]+,\s*)(v[0-9]+)/$1$3$2$4/o or
     s/\?(vsldoi\s+v[0-9]+,\s*)(v[0-9]+,)\s*(v[0-9]+,\s*)([0-9]+)/$1$3$2 16-$4/o or
     s/\?(vspltw\s+v[0-9]+,\s*)(v[0-9]+,)\s*([0-9])/$1$2 3-$3/o;
 } else {   # big-endian
     s/le\?/#le#/o or
     s/be\?//o  or
     s/\?([a-z]+)/$1/o;
 }

       print $_,"\n";
}

close STDOUT;
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/aes/asm/aesp8-ppc.pl

No license file was found, but licenses were detected in source scan.

```
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/dsa/fips_dsa_sign.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/test/fips_algvs.c

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/ecdsa/fips_ecdsa_sign.c
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2005 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/bn/bn_x931p.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rsa/fips_rsavtest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_pss.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/rsa/fips_rsastest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/sha/fips_shatest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/rsa/rsa_x931.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/hmac/fips_hmactest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/cmac/fips_cmactest.c

No license file was found, but licenses were detected in source scan.

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@openssl.org> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# SHA512 for C64x.
#
# November 2016
#
# Performance is ~19 cycles per processed byte. Compared to block
# transform function from sha512.c compiled with cl6x with -mv6400+
# -o2 -DOPENSSL_SMALL_FOOTPRINT it's almost 7x faster and 2x smaller.
# Loop unroll won't make it, this implementation, any faster, because
# it's effectively dominated by SHRU||SHL pairs and you can't schedule
# more of them.
```

```
#
# !!! Note that this module uses AMR, which means that all interrupt
# service routines are expected to preserve it and for own well-being
# zero it upon entry.

while (($output=shift) && ($output!~/^\w[\w\-]*\.\w+$/)) {}
open STDOUT,">$output";

($CTXA,$INP,$NUM) = ("A4","B4","A6");          # arguments
$K512="A3";

($Ahi,$Actxhi,$Bhi,$Bctxhi,$Chi,$Cctxhi,$Dhi,$Dctxhi,
$Ehi,$Ectxhi,$Fhi,$Fctxhi,$Ghi,$Gctxhi,$Hhi,$Hctxhi)=map("A$_",(16..31));
($Alo,$Actxlo,$Blo,$Bctxlo,$Clo,$Cctxlo,$Dlo,$Dctxlo,
$Elo,$Ectxlo,$Flo,$Fctxlo,$Glo,$Gctxlo,$Hlo,$Hctxlo)=map("B$_",(16..31));

($S1hi,$CHhi,$S0hi,$t0hi)=map("A$_",(10..13));
($S1lo,$CHlo,$S0lo,$t0lo)=map("B$_",(10..13));
($T1hi,        $T2hi)=        ("A6","A7");
($T1lo,$T1carry,$T2lo,$T2carry)=("B6","B7","B8","B9");
($Khi,$Klo)=("A9","A8");
($MAJhi,$MAJlo)=($T2hi,$T2lo);
($t1hi,$t1lo)=($Khi,"B2");
$CTXB=$t1lo;

($Xihi,$Xilo)=("A5","B5");   # circular/ring buffer

$code.=<<___;
 .text

 .if .ASSEMBLER_VERSION<7000000
 .asg 0,__TI_EABI__
 .endif
 .if __TI_EABI__
 .nocmp
 .asg sha512_block_data_order,_sha512_block_data_order
 .endif


 .asg B3,RA
 .asg A15,FP
 .asg B15,SP

 .if .BIG_ENDIAN
 .asg $Khi,KHI
 .asg $Klo,KLO
 .else
 .asg $Khi,KLO
 .asg $Klo,KHI
 .endif

 .global _sha512_block_data_order
_sha512_block_data_order:
__sha512_block:
 .asmfunc stack_usage(40+128)
 MV $NUM,A0    ; reassign $NUM
|| MVK -128,B0
 [!A0] BNOP RA    ; if ($NUM==0) return;
|| [A0] STW FP,*SP--(40)   ; save frame pointer
|| [A0] MV SP,FP
  [A0] STDW B13:B12,*SP[4]
|| [A0] MVK 0x00404,B1
  [A0] STDW B11:B10,*SP[3]
|| [A0] STDW A13:A12,*FP[-3]
|| [A0] MVKH 0x60000,B1
  [A0] STDW A11:A10,*SP[1]
|| [A0] MVC B1,AMR    ; setup circular addressing
|| [A0] ADD B0,SP,SP   ; alloca(128)
 .if __TI_EABI__
  [A0] AND B0,SP,SP   ; align stack at 128 bytes
|| [A0] ADDKPC __sha512_block,B1
|| [A0] MVKL \$PCR_OFFSET(K512,__sha512_block),$K512
  [A0] MVKH \$PCR_OFFSET(K512,__sha512_block),$K512
|| [A0] SUBAW SP,2,SP    ; reserve two words above buffer
 .else
  [A0] AND B0,SP,SP   ; align stack at 128 bytes
|| [A0] ADDKPC __sha512_block,B1
|| [A0] MVKL (K512-__sha512_block),$K512
  [A0] MVKH (K512-__sha512_block),$K512
|| [A0] SUBAW SP,2,SP    ; reserve two words above buffer
 .endif
 ADDAW SP,3,$Xilo
 ADD SP,4*2,$Xihi   ; ADDAW SP,2,$Xihi

|| MV $CTXA,$CTXB
 LDW *${CTXA}[0^.LITTLE_ENDIAN],$Ahi ; load ctx
|| LDW *${CTXB}[1^.LITTLE_ENDIAN],$Alo
|| ADD B1,$K512,$K512
 LDW *${CTXA}[2^.LITTLE_ENDIAN],$Bhi
|| LDW *${CTXB}[3^.LITTLE_ENDIAN],$Blo
 LDW *${CTXA}[4^.LITTLE_ENDIAN],$Chi
|| LDW *${CTXB}[5^.LITTLE_ENDIAN],$Clo
 LDW *${CTXA}[6^.LITTLE_ENDIAN],$Dhi
|| LDW *${CTXB}[7^.LITTLE_ENDIAN],$Dlo
 LDW *${CTXA}[8^.LITTLE_ENDIAN],$Ehi
|| LDW *${CTXB}[9^.LITTLE_ENDIAN],$Elo
 LDW *${CTXA}[10^.LITTLE_ENDIAN],$Fhi
```

```
|| LDW *${CTXB}[11^.LITTLE_ENDIAN],$Flo
 LDW *${CTXA}[12^.LITTLE_ENDIAN],$Ghi
|| LDW *${CTXB}[13^.LITTLE_ENDIAN],$Glo
 LDW *${CTXA}[14^.LITTLE_ENDIAN],$Hhi
|| LDW *${CTXB}[15^.LITTLE_ENDIAN],$Hlo

 LDNDW *$INP++,B11:B10   ; pre-fetch input
 LDDW *$K512++,$Khi:$Klo  ; pre-fetch K512[0]
outerloop?:
 MVK 15,B0    ; loop counters
|| MVK 64,B1
|| SUB A0,1,A0
 MV $Ahi,$Actxhi
|| MV $Alo,$Actxlo
|| MV $Bhi,$Bctxhi
|| MV $Blo,$Bctxlo
|| MV $Chi,$Cctxhi
|| MV $Clo,$Cctxlo
|| MVD $Dhi,$Dctxhi
|| MVD $Dlo,$Dctxlo
 MV $Ehi,$Ectxhi
|| MV $Elo,$Ectxlo
|| MV $Fhi,$Fctxhi
|| MV $Flo,$Fctxlo
|| MV $Ghi,$Gctxhi
|| MV $Glo,$Gctxlo
|| MVD $Hhi,$Hctxhi
|| MVD $Hlo,$Hctxlo
loop0_15?:
 .if .BIG_ENDIAN
 MV B11,$T1hi
|| MV B10,$T1lo
 .else
 SWAP4 B10,$T1hi
|| SWAP4 B11,$T1lo
 SWAP2 $T1hi,$T1hi
|| SWAP2 $T1lo,$T1lo
 .endif
 STW $T1hi,*$Xihi++[2]   ; original loop16_79?
|| STW $T1lo,*$Xilo++[2]   ; X[i] = T1
|| ADD $Hhi,$T1hi,$T1hi
|| ADDU $Hlo,$T1lo,$T1carry:$T1lo  ; T1 += h
|| SHRU $Ehi,14,$S1hi
|| SHL $Ehi,32-14,$S1lo
loop16_79?:
 XOR $Fhi,$Ghi,$CHhi
|| XOR $Flo,$Glo,$CHlo
|| ADD KHI,$T1hi,$T1hi
|| ADDU KLO,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += K512[i]
|| SHRU $Elo,14,$t0lo
|| SHL $Elo,32-14,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| AND $Ehi,$CHhi,$CHhi
|| AND $Elo,$CHlo,$CHlo
|| ROTL $Ghi,0,$Hhi
|| ROTL $Glo,0,$Hlo    ; h = g
|| SHRU $Ehi,18,$t0hi
|| SHL $Ehi,32-18,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| XOR $Ghi,$CHhi,$CHhi
|| XOR $Glo,$CHlo,$CHlo   ; Ch(e,f,g) = ((f^g)&e)^g
|| ROTL $Fhi,0,$Ghi
|| ROTL $Flo,0,$Glo    ; g = f
|| SHRU $Elo,18,$t0lo
|| SHL $Elo,32-18,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| OR $Ahi,$Bhi,$MAJhi
|| OR $Alo,$Blo,$MAJlo
|| ROTL $Ehi,0,$Fhi
|| ROTL $Elo,0,$Flo    ; f = e
|| SHRU $Ehi,41-32,$t0lo
|| SHL $Ehi,64-41,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| AND $Chi,$MAJhi,$MAJhi
|| AND $Clo,$MAJlo,$MAJlo
|| ROTL $Dhi,0,$Ehi
|| ROTL $Dlo,0,$Elo    ; e = d
|| SHRU $Elo,41-32,$t0hi
|| SHL $Elo,64-41,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo   ; Sigma1(e)
|| AND $Ahi,$Bhi,$t1hi
|| AND $Alo,$Blo,$t1lo
|| ROTL $Chi,0,$Dhi
|| ROTL $Clo,0,$Dlo    ; d = c
|| SHRU $Ahi,28,$S0hi
|| SHL $Ahi,32-28,$S0lo
 OR $t1hi,$MAJhi,$MAJhi
|| OR $t1lo,$MAJlo,$MAJlo   ; Maj(a,b,c) = ((a|b)&c)|(a&b)
|| ADD $CHhi,$T1hi,$T1hi
|| ADDU $CHlo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += Ch(e,f,g)
|| ROTL $Bhi,0,$Chi
|| ROTL $Blo,0,$Clo    ; c = b
|| SHRU $Alo,28,$t0lo
|| SHL $Alo,32-28,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $S1hi,$T1hi,$T1hi
|| ADDU $S1lo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += Sigma1(e)
|| ROTL $Ahi,0,$Bhi
|| ROTL $Alo,0,$Blo    ; b = a
|| SHRU $Ahi,34-32,$t0lo
|| SHL $Ahi,64-34,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $MAJhi,$T1hi,$T2hi
|| ADDU $MAJlo,$T1carry:$T1lo,$T2carry:$T2lo ; T2 = T1+Maj(a,b,c)
|| SHRU $Alo,34-32,$t0hi
|| SHL $Alo,64-34,$t0lo
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $Ehi,$T1hi,$T1hi
|| ADDU $Elo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += e
|| SHRU $Ahi,39-32,$t0lo
|| SHL $Ahi,64-39,$t0hi
  [B0] BNOP loop0_15?
|| [B0] LDNDW *$INP++,B11:B10    ; pre-fetch input
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| SHRU $Alo,39-32,$t0hi
|| SHL $Alo,64-39,$t0lo
||[!B0] LDW *${Xihi}[28],$T1hi
||[!B0] LDW *${Xilo}[28],$T1lo   ; X[i+14]
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo   ; Sigma0(a)
|| ADD $T1carry,$T1hi,$Ehi
|| ROTL $T1lo,0,$Elo    ; e = T1, "ghost" value
||[!B1] BNOP break?
 ADD $S0hi,$T2hi,$T2hi
|| ADDU $S0lo,$T2carry:$T2lo,$T2carry:$T2lo ; T2 += Sigma0(a)
|| [B1] LDDW *$K512++,$Khi:$Klo   ; pre-fetch K512[i]
 NOP      ; avoid cross-path stall
 ADD $T2carry,$T2hi,$Ahi
|| MV $T2lo,$Alo    ; a = T2
|| [B0] SUB B0,1,B0
;;===== branch to loop00_15? is taken here
  [B1] LDW *${Xihi}[2],$T2hi
|| [B1] LDW *${Xilo}[2],$T2lo   ; X[i+1]
|| [B1] SHRU $T1hi,19,$S1hi
|| [B1] SHL $T1hi,32-19,$S1lo
```

```
  [B1] SHRU $T1lo,19,$t0lo
|| [B1] SHL $T1lo,32-19,$t0hi
;;===== branch to break? is taken here
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1hi,61-32,$t0lo
|| SHL $T1hi,64-61,$t0hi
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1lo,61-32,$t0hi
|| SHL $T1lo,64-61,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1hi,6,$t0hi
|| SHL $T1hi,32-6,$t0lo
 XOR $t0hi,$S1hi,$S1hi
|| XOR $t0lo,$S1lo,$S1lo
|| SHRU $T1lo,6,$t0lo
|| LDW *${Xihi}[18],$T1hi
|| LDW *${Xilo}[18],$T1lo   ; X[i+9]
 XOR $t0lo,$S1lo,$S1lo   ; sigma1(Xi[i+14])

|| LDW *${Xihi}[0],$CHhi
|| LDW *${Xilo}[0],$CHlo   ; X[i]
|| SHRU $T2hi,1,$S0hi
|| SHL $T2hi,32-1,$S0lo
 SHRU $T2lo,1,$t0lo
|| SHL $T2lo,32-1,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| SHRU $T2hi,8,$t0hi
|| SHL $T2hi,32-8,$t0lo
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| SHRU $T2lo,8,$t0lo
|| SHL $T2lo,32-8,$t0hi
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $S1hi,$T1hi,$T1hi
|| ADDU $S1lo,$T1lo,$T1carry:$T1lo  ; T1 = X[i+9]+sigma1()
|| SHRU $T2hi,7,$t0hi
|| SHL $T2hi,32-7,$t0lo
 XOR $t0hi,$S0hi,$S0hi
|| XOR $t0lo,$S0lo,$S0lo
|| ADD $CHhi,$T1hi,$T1hi
|| ADDU $CHlo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += X[i]
|| SHRU $T2lo,7,$t0lo
|| [B1] BNOP loop16_79?
```

```
 XOR $t0lo,$S0lo,$S0lo   ; sigma0(Xi[i+1]

 ADD $S0hi,$T1hi,$T1hi
|| ADDU $S0lo,$T1carry:$T1lo,$T1carry:$T1lo ; T1 += sigma0()
|| [B1] SUB B1,1,B1
 NOP      ; avoid cross-path stall
 ADD $T1carry,$T1hi,$T1hi

   STW $T1hi,*$Xihi++[2]   ; copied "top" bundle
|| STW $T1lo,*$Xilo++[2]   ; X[i] = T1
|| ADD $Hhi,$T1hi,$T1hi
|| ADDU $Hlo,$T1lo,$T1carry:$T1lo  ; T1 += h
|| SHRU $Ehi,14,$S1hi
|| SHL $Ehi,32-14,$S1lo
;;===== branch to loop16_79? is taken here

break?:
 ADD $Ahi,$Actxhi,$Ahi  ; accumulate ctx
|| ADDU $Alo,$Actxlo,$Actxlo:$Alo
|| [A0] LDNDW *$INP++,B11:B10   ; pre-fetch input
|| [A0] ADDK -640,$K512   ; rewind pointer to K512
 ADD $Bhi,$Bctxhi,$Bhi
|| ADDU $Blo,$Bctxlo,$Bctxlo:$Blo
|| [A0] LDDW *$K512++,$Khi:$Klo  ; pre-fetch K512[0]
 ADD $Chi,$Cctxhi,$Chi
|| ADDU $Clo,$Cctxlo,$Cctxlo:$Clo
|| ADD $Actxlo,$Ahi,$Ahi
||[!A0] MV $CTXA,$CTXB
 ADD $Dhi,$Dctxhi,$Dhi
|| ADDU $Dlo,$Dctxlo,$Dctxlo:$Dlo
|| ADD $Bctxlo,$Bhi,$Bhi
||[!A0] STW $Ahi,*${CTXA}[0^.LITTLE_ENDIAN] ; save ctx
||[!A0] STW $Alo,*${CTXB}[1^.LITTLE_ENDIAN]
 ADD $Ehi,$Ectxhi,$Ehi
|| ADDU $Elo,$Ectxlo,$Ectxlo:$Elo
|| ADD $Cctxlo,$Chi,$Chi
|| [A0] BNOP outerloop?
||[!A0] STW $Bhi,*${CTXA}[2^.LITTLE_ENDIAN]
||[!A0] STW $Blo,*${CTXB}[3^.LITTLE_ENDIAN]
 ADD $Fhi,$Fctxhi,$Fhi
|| ADDU $Flo,$Fctxlo,$Fctxlo:$Flo
|| ADD $Dctxlo,$Dhi,$Dhi
||[!A0] STW $Chi,*${CTXA}[4^.LITTLE_ENDIAN]
||[!A0] STW $Clo,*${CTXB}[5^.LITTLE_ENDIAN]
 ADD $Ghi,$Gctxhi,$Ghi
|| ADDU $Glo,$Gctxlo,$Gctxlo:$Glo
|| ADD $Ectxlo,$Ehi,$Ehi
||[!A0] STW $Dhi,*${CTXA}[6^.LITTLE_ENDIAN]
```

```
||[!A0] STW $Dlo,*${CTXB}[7^.LITTLE_ENDIAN]
 ADD $Hhi,$Hctxhi,$Hhi
|| ADDU $Hlo,$Hctxlo,$Hctxlo:$Hlo
|| ADD $Fctxlo,$Fhi,$Fhi
||[!A0] STW $Ehi,*${CTXA}[8^.LITTLE_ENDIAN]
||[!A0] STW $Elo,*${CTXB}[9^.LITTLE_ENDIAN]
 ADD $Gctxlo,$Ghi,$Ghi
||[!A0] STW $Fhi,*${CTXA}[10^.LITTLE_ENDIAN]
||[!A0] STW $Flo,*${CTXB}[11^.LITTLE_ENDIAN]
 ADD $Hctxlo,$Hhi,$Hhi
||[!A0] STW $Ghi,*${CTXA}[12^.LITTLE_ENDIAN]
||[!A0] STW $Glo,*${CTXB}[13^.LITTLE_ENDIAN]
;;===== branch to outerloop? is taken here

 STW $Hhi,*${CTXA}[14^.LITTLE_ENDIAN]
|| STW $Hlo,*${CTXB}[15^.LITTLE_ENDIAN]
|| MVK -40,B0
 ADD FP,B0,SP   ; destroy circular buffer
|| LDDW *FP[-4],A11:A10
 LDDW *SP[2],A13:A12
|| LDDW *FP[-2],B11:B10
 LDDW *SP[4],B13:B12
|| BNOP RA
 LDW *++SP(40),FP   ; restore frame pointer
 MVK 0,B0
 MVC B0,AMR    ; clear AMR
 NOP 2    ; wait till FP is committed
 .endasmfunc

 .if __TI_EABI__
 .sect ".text:sha_asm.const"
 .else
 .sect ".const:sha_asm"
 .endif
 .align 128
K512:
 .uword 0x428a2f98,0xd728ae22, 0x71374491,0x23ef65cd
 .uword 0xb5c0fbcf,0xec4d3b2f, 0xe9b5dba5,0x8189dbbc
 .uword 0x3956c25b,0xf348b538, 0x59f111f1,0xb605d019
 .uword 0x923f82a4,0xaf194f9b, 0xab1c5ed5,0xda6d8118
 .uword 0xd807aa98,0xa3030242, 0x12835b01,0x45706fbe
 .uword 0x243185be,0x4ee4b28c, 0x550c7dc3,0xd5ffb4e2
 .uword 0x72be5d74,0xf27b896f, 0x80deb1fe,0x3b1696b1
 .uword 0x9bdc06a7,0x25c71235, 0xc19bf174,0xcf692694
 .uword 0xe49b69c1,0x9ef14ad2, 0xefbe4786,0x384f25e3
 .uword 0x0fc19dc6,0x8b8cd5b5, 0x240ca1cc,0x77ac9c65
 .uword 0x2de92c6f,0x592b0275, 0x4a7484aa,0x6ea6e483
 .uword 0x5cb0a9dc,0xbd41fbd4, 0x76f988da,0x831153b5
 .uword 0x983e5152,0xee66dfab, 0xa831c66d,0x2db43210
 .uword 0xb00327c8,0x98fb213f, 0xbf597fc7,0xbeef0ee4
 .uword 0xc6e00bf3,0x3da88fc2, 0xd5a79147,0x930aa725
 .uword 0x06ca6351,0xe003826f, 0x14292967,0x0a0e6e70
 .uword 0x27b70a85,0x46d22ffc, 0x2e1b2138,0x5c26c926
 .uword 0x4d2c6dfc,0x5ac42aed, 0x53380d13,0x9d95b3df
 .uword 0x650a7354,0x8baf63de, 0x766a0abb,0x3c77b2a8
 .uword 0x81c2c92e,0x47edaee6, 0x92722c85,0x1482353b
 .uword 0xa2bfe8a1,0x4cf10364, 0xa81a664b,0xbc423001
 .uword 0xc24b8b70,0xd0f89791, 0xc76c51a3,0x0654be30
 .uword 0xd192e819,0xd6ef5218, 0xd6990624,0x5565a910
 .uword 0xf40e3585,0x5771202a, 0x106aa070,0x32bbd1b8
 .uword 0x19a4c116,0xb8d2d0c8, 0x1e376c08,0x5141ab53
 .uword 0x2748774c,0xdf8eeb99, 0x34b0bcb5,0xe19b48a8
 .uword 0x391c0cb3,0xc5c95a63, 0x4ed8aa4a,0xe3418acb
 .uword 0x5b9cca4f,0x7763e373, 0x682e6ff3,0xd6b2b8a3
 .uword 0x748f82ee,0x5defb2fc, 0x78a5636f,0x43172f60
 .uword 0x84c87814,0xa1f0ab72, 0x8cc70208,0x1a6439ec
 .uword 0x90befffa,0x23631e28, 0xa4506ceb,0xde82bde9
 .uword 0xbef9a3f7,0xb2c67915, 0xc67178f2,0xe372532b
 .uword 0xca273ece,0xea26619c, 0xd186b8c7,0x21c0c207
 .uword 0xeada7dd6,0xcde0eb1e, 0xf57d4f7f,0xee6ed178
 .uword 0x06f067aa,0x72176fba, 0x0a637dc5,0xa2c898a6
 .uword 0x113f9804,0xbef90dae, 0x1b710b35,0x131c471b
 .uword 0x28db77f5,0x23047d84, 0x32caab7b,0x40c72493
 .uword 0x3c9ebe0a,0x15c9bebc, 0x431d67c4,0x9c100d4c
 .uword 0x4cc5d4be,0xcb3e42b6, 0x597f299c,0xfc657e2a
 .uword 0x5fcb6fab,0x3ad6faec, 0x6c44198c,0x4a475817
 .cstring "SHA512 block transform for C64x, CRYPTOGAMS by <appro\@openssl.org>"
 .align 4
___

print $code;
close STDOUT;
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/sha/asm/sha512-c64x.pl

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2011 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
```

*   notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in
*   the documentation and/or other materials provided with the
*   distribution.
*
* 3. All advertising materials mentioning features or use of this
*   software must display the following acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*/

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/ccm128.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/modes/xts128.c
No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright 2002 Sun Microsystems, Inc. ALL RIGHTS RESERVED.
*
* The Elliptic Curve Public-Key Crypto Library (ECC Code) included
* herein is developed by SUN MICROSYSTEMS, INC., and is contributed
* to the OpenSSL project.
*
* The ECC Code is licensed pursuant to the OpenSSL open source
* license provided below.
*
* The software is originally written by Sheueling Chang Shantz and
* Douglas Stebila of Sun Microsystems Laboratories.
*
*/
/* ====================================================================
* Copyright (c) 1998-2003 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
```

```
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

Found in path(s):

* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/crypto/ec/ec2_mult.c

No license file was found, but licenses were detected in source scan.

```
/* ====================================================================
* Copyright (c) 2011 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    licensing@OpenSSL.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
*/
```

Found in path(s):
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/ecdsa/fips_ecdsa_selftest.c
* /opt/cola/permits/1298757353_1648826790.95/0/openssl-fips-2-0-16-tar-gz/openssl-fips-2.0.16/fips/ecdh/fips_ecdh_selftest.c

1.11 constantly 15.1.0

1.11.1 Available under license :

Copyright (c) 2011-2015 Twisted Matrix Laboratories &
Individual Contributors (see CREDITS)

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.12 ldaptor 21.2.0

1.12.1 Available under license :

Copyright (c) 2002-2020, Ldaptor Contributors (see ./docs/source/AUTHORS.rst)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.13 automat 20.2.0

1.13.1 Available under license :

Copyright (c) 2014
Rackspace

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to

1.14 pytest 5.3.5

1.14.1 Available under license :

1.15 decorator 4.4.1

1.15.1 Available under license :

LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.16 duo-client-python 4.0.0

1.16.1 Available under license :

Copyright (c) 2013, Duo Security, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: The open-source component https_wrapper.py included with this distribution is under the terms of the Apache License, Version 2.0, a copy of which has been included as 'apache-license-2.0.txt'.

Apache License
Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or

implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

1.17 six 1.15.0

1.17.1 Available under license :

The primary author and maintainer of six is Benjamin Peterson. He would like to acknowledge the following people who submitted bug reports, pull requests, and otherwise worked to improve six:

Marc Abramowitz
immerrr again
Alexander Artemenko
Aymeric Augustin
Lee Ball
Ben Bariteau
Ned Batchelder
Wouter Bolsterlee
Brett Cannon
Jason R. Coombs
Julien Danjou
Ben Darnell
Ben Davis
Jon Dufresne

Tim Graham
Thomas Grainger
Max Grender-Jones
Joshua Harlow
Toshiki Kataoka
Hugo van Kemenade
Anselm Kruis
Ivan Levkivskyi
Alexander Lukanin
James Mills
Jordan Moldow
Berker Peksag
Sridhar Ratnakumar
Erik Rose
Mirko Rossini
Peter Ruibal
Miroslav Shubernetskiy
Eli Schwartz
Anthony Sottile
Jonathan Vanasco
Lucas Wiman
Jingxin Zhu

If you think you belong on this list, please let me know! --Benjamin

1.18 atomicwrites 1.4.0

1.18.1 Available under license :

1.19 setuptools-scm 2.1.0

1.19.1 Available under license :

1.20 typing-extensions 4.2.0

1.20.1 Available under license :

A. HISTORY OF THE SOFTWARE
==========================

Python was created in the early 1990s by Guido van Rossum at Stichting
Mathematisch Centrum (CWI, see http://www.cwi.nl) in the Netherlands
as a successor of a language called ABC. Guido remains Python's
principal author, although it includes many contributions from others.

In 1995, Guido continued his work on Python at the Corporation for
National Research Initiatives (CNRI, see http://www.cnri.reston.va.us)
in Reston, Virginia where he released several versions of the
software.

In May 2000, Guido and the Python core development team moved to
BeOpen.com to form the BeOpen PythonLabs team. In October of the same
year, the PythonLabs team moved to Digital Creations (now Zope
Corporation, see http://www.zope.com). In 2001, the Python Software
Foundation (PSF, see http://www.python.org/psf/) was formed, a
non-profit organization created specifically to own Python-related
Intellectual Property. Zope Corporation is a sponsoring member of
the PSF.

All Python releases are Open Source (see http://www.opensource.org for the Open Source Definition). Historically, most, but not all, Python releases have also been GPL-compatible; the table below summarizes the various releases.

Release	Derived from	Year	Owner	GPL-compatible? (1)
0.9.0 thru 1.2		1991-1995	CWI	yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI	yes
1.6	1.5.2	2000	CNRI	no
2.0	1.6	2000	BeOpen.com	no
1.6.1	1.6	2001	CNRI	yes (2)
2.1	2.0+1.6.1	2001	PSF	no
2.0.1	2.0+1.6.1	2001	PSF	yes
2.1.1	2.1+2.0.1	2001	PSF	yes
2.1.2	2.1.1	2002	PSF	yes
2.1.3	2.1.2	2002	PSF	yes
2.2 and above	2.1.1	2001-now	PSF	yes

Footnotes:

(1) GPL-compatible doesn't mean that we're distributing Python under the GPL. All Python licenses, unlike the GPL, let you distribute a modified version without making your changes open source. The GPL-compatible licenses make it possible to combine Python with other software that is released under the GPL; the others don't.

(2) According to Richard Stallman, 1.6.1 is not GPL-compatible, because its license has a choice of law clause. According to CNRI, however, Stallman's lawyer has told CNRI's lawyer that 1.6.1 is "not incompatible" with the GPL.

Thanks to the many outside volunteers who have worked under Guido's direction to make these releases possible.

B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING PYTHON
===

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
----

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an

office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the
Individual or Organization ("Licensee") accessing and otherwise using
this software in source or binary form and its associated
documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License
Agreement, BeOpen hereby grants Licensee a non-exclusive,
royalty-free, world-wide license to reproduce, analyze, test, perform
and/or display publicly, prepare derivative works, distribute, and
otherwise use the Software alone or in any derivative version,
provided, however, that the BeOpen Python License is retained in the
Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS"
basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE
SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS
AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY
DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

6. This License Agreement shall be governed by and interpreted in all
respects by the law of the State of California, excluding conflict of
law provisions. Nothing in this License Agreement shall be deemed to
create any relationship of agency, partnership, or joint venture
between BeOpen and Licensee. This License Agreement does not grant
permission to use BeOpen trademarks or trade names in a trademark
sense to endorse or promote products or services of Licensee, or any
third party. As an exception, the "BeOpen Python" logos available at
http://www.pythonlabs.com/logos.html may be used according to the
permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
----

1. This LICENSE AGREEMENT is between the Corporation for National

Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. This License Agreement shall be governed by the federal intellectual property law of the United States, including without limitation the federal copyright law, and, to the extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions.

Notwithstanding the foregoing, with regard to derivative works based
on Python 1.6.1 that incorporate non-separable material that was
previously distributed under the GNU General Public License (GPL), the
law of the Commonwealth of Virginia shall govern this License
Agreement only as to issues arising under or with respect to
Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this
License Agreement shall be deemed to create any relationship of
agency, partnership, or joint venture between CNRI and Licensee. This
License Agreement does not grant permission to use CNRI trademarks or
trade name in a trademark sense to endorse or promote products or
services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying,
installing or otherwise using Python 1.6.1, Licensee agrees to be
bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam,
The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of Stichting Mathematisch
Centrum or CWI not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior
permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE
FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

1.21 python-setuptools 42.0.2

1.21.1 Available under license :

1.22 pyparsing 3.0.0a2

1.22.1 Available under license :

1.23 pyopenssl 17.5.0

1.23.1 Available under license :

of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You

meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor,

except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

1.24 service-identity 18.1.0

1.24.1 Available under license :

1.25 pyrad 2.4

1.25.1 Available under license :

All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors
  may be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.26 idna 2.7

1.26.1 Available under license :

No license file was found, but licenses were detected in source scan.

License

Copyright (c) 2013-2018, Kim Davies. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

#. Redistributions of source code must retain the above copyright
  notice, this list of conditions and the following disclaimer.

#. Redistributions in binary form must reproduce the above
  copyright notice, this list of conditions and the following
  disclaimer in the documentation and/or other materials provided with
  the distribution.

#. Neither the name of the copyright holder nor the names of the contributors may be used to endorse or promote products derived from this software without specific prior written permission.

#. THIS SOFTWARE IS PROVIDED BY THE CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the codec implementation and unit tests are derived from the Python standard library, which carries the `Python Software Foundation License <https://docs.python.org/2/license.html>`_:

Copyright (c) 2001-2014 Python Software Foundation; All Rights Reserved

Portions of the unit tests are derived from the Unicode standard, which is subject to the Unicode, Inc. License Agreement:

Copyright (c) 1991-2014 Unicode, Inc. All rights reserved.
Distributed under the Terms of Use in
<http://www.unicode.org/copyright.html>.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that

(a) this copyright and permission notice appear with all copies of the Data Files or Software,

(b) this copyright and permission notice appear in associated documentation, and

(c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

Found in path(s):
* /opt/cola/permits/1673010570_1683816445.4652283/0/kjd-idna-v2-7-0-g5d76cb6-1-tar-gz/kjd-idna-77c8bce/LICENSE.rst
No license file was found, but licenses were detected in source scan.

```
"""
A library to support the Internationalised Domain Names in Applications
(IDNA) protocol as specified in RFC 5890 et.al. This new methodology,
known as IDNA 2008, can generate materially different results to the
previous standard. The library can act as a drop-in replacement for
the "encodings.idna" module.
"""

import io, sys
from setuptools import setup


def main():

    python_version = sys.version_info[:2]
    if python_version < (2,6):
        raise SystemExit("Sorry, Python 2.6 or newer required")

    package_data = {}
    exec(open('idna/package_data.py').read(), package_data)

    arguments = {
        'name': 'idna',
        'packages': ['idna'],
        'version': package_data['__version__'],
        'description': 'Internationalized Domain Names in Applications (IDNA)',
        'long_description': io.open("README.rst", encoding="UTF-8").read(),
        'author': 'Kim Davies',
        'author_email': 'kim@cynosure.com.au',
        'license': 'BSD-like',
        'url': 'https://github.com/kjd/idna',
        'classifiers': [
            'Development Status :: 5 - Production/Stable',
            'Intended Audience :: Developers',
            'Intended Audience :: System Administrators',
            'License :: OSI Approved :: BSD License',
            'Operating System :: OS Independent',
            'Programming Language :: Python',
            'Programming Language :: Python :: 2.6',
            'Programming Language :: Python :: 2.7',
            'Programming Language :: Python :: 3',
            'Programming Language :: Python :: 3.3',
            'Programming Language :: Python :: 3.4',
            'Programming Language :: Python :: 3.5',
            'Programming Language :: Python :: 3.6',
            'Topic :: Internet :: Name Service (DNS)',
            'Topic :: Software Development :: Libraries :: Python Modules',
            'Topic :: Utilities',
        ],
        'test_suite': 'tests',
    }

    setup(**arguments)

if __name__ == '__main__':
    main()
```

Found in path(s):
* /opt/cola/permits/1673010570_1683816445.4652283/0/kjd-idna-v2-7-0-g5d76cb6-1-tar-gz/kjd-idna-77c8bce/setup.py

1.27 python3-asn1crypto 1.2.0

1.27.1 Available under license :

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.28 py 1.11.0

1.28.1 Available under license :

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

1.29 twisted_connect_proxy 1.0.0

1.29.1 Available under license :

1.30 twisted_iocpsupport 1.0.2

1.30.1 Available under license :

Antoine Pitrou
Apple Computer, Inc.
Ashwini Oruganti
Benjamin Bruheim
Bob Ippolito
Canonical Limited
Christopher Armstrong
Ciena Corporation
David Reid
Divmod Inc.
Donovan Preston
Eric Mangold
Eyal Lotem
Google Inc.
Hybrid Logic Ltd.
Hynek Schlawack
Itamar Turner-Trauring
James Knight
Jason A. Mobarak
Jean-Paul Calderone
Jessica McKellar
Jonathan D. Simms
Jonathan Jacobs
Jonathan Lange
Julian Berman
Jrgen Hermann
Kevin Horn
Kevin Turner
Laurens Van Houtven
Mary Gardiner
Massachusetts Institute of Technology
Matthew Lefkowitz
Moshe Zadka
Paul Swartz
Pavel Pergamenshchik
Rackspace, US Inc.
Ralph Meijer
Richard Wall
Sean Riley
Software Freedom Conservancy
Tavendo GmbH
Thijs Triemstra
Thomas Grainger
Thomas Herve
Timothy Allen
Tom Most
Tom Prince
Travis B. Hartwell

and others that have contributed code to the public domain.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.31 pyasn1-modules 0.2.8

1.31.1 Available under license :

Copyright (c) 2005-2019, Ilya Etingof <etingof@gmail.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

1.32 pywin32-win32 227

1.32.1 Available under license :

Unless stated in the specfic source file, this work is
Copyright (c) 1994-2008, Mark Hammond
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in
the documentation and/or other materials provided with the distribution.

Neither name of Mark Hammond nor the name of contributors may be used
to endorse or promote products derived from this software without
specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.33 pycparser 2.10

1.33.1 Available under license :

Copyright (c) 2012, Eli Bendersky
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

1.34 pyasn1 0.4.8

1.34.1 Available under license :

No license file was found, but licenses were detected in source scan.

ASN.1 library for Python

[![PyPI](https://img.shields.io/pypi/v/pyasn1.svg?maxAge=2592000)](https://pypi.org/project/pyasn1)
[![Python Versions](https://img.shields.io/pypi/pyversions/pyasn1.svg)](https://pypi.org/project/pyasn1/)
[![Build status](https://travis-ci.org/etingof/pyasn1.svg?branch=master)](https://secure.travis-ci.org/etingof/pyasn1)
[![Coverage
Status](https://img.shields.io/codecov/c/github/etingof/pyasn1.svg)](https://codecov.io/github/etingof/pyasn1)
[![GitHub license](https://img.shields.io/badge/license-BSD-blue.svg)](https://raw.githubusercontent.com/etingof/pyasn1/master/LICENSE.txt)

This is a free and open source implementation of ASN.1 types and codecs
as a Python package. It has been first written to support particular
protocol (SNMP) but then generalized to be suitable for a wide range
of protocols based on
[ASN.1 specification](https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.208-198811-W!!PDF-E&type=items).

Features
----

* Generic implementation of ASN.1 types (X.208)
* Standards compliant BER/CER/DER codecs

* Dumps/loads ASN.1 structures from Python types
* 100% Python, works with Python 2.4 up to Python 3.7
* MT-safe
* Contributed ASN.1 compiler [Asn1ate](https://github.com/kimgr/asn1ate)

Why using pyasn1

ASN.1 solves the data serialisation problem. This solution was designed long ago by the wise Ancients. Back then, they did not have the luxury of wasting bits. That is why ASN.1 is designed to serialise data structures of unbounded complexity into something compact and efficient when it comes to processing the data.

That probably explains why many network protocols and file formats still rely on the 30+ years old technology. Including a number of high-profile Internet protocols and file formats.

Quite a number of books cover the topic of ASN.1.
[Communication between heterogeneous systems](http://www.oss.com/asn1/dubuisson.html)
by Olivier Dubuisson is one of those high quality books freely available on the Internet.

The pyasn1 package is designed to help Python programmers tackling network protocols and file formats at the comfort of their Python prompt. The tool struggles to capture all aspects of a rather complicated ASN.1 system and to represent it on the Python terms.

How to use pyasn1

With pyasn1 you can build Python objects from ASN.1 data structures.
For example, the following ASN.1 data structure:

```bash
Record ::= SEQUENCE {
 id        INTEGER,
 room  [0] INTEGER OPTIONAL,
 house [1] INTEGER DEFAULT 0
}
```

Could be expressed in pyasn1 like this:

```python
class Record(Sequence):
   componentType = NamedTypes(
    NamedType('id', Integer()),
    OptionalNamedType(
      'room', Integer().subtype(
        implicitTag=Tag(tagClassContext, tagFormatSimple, 0)
      )
    ),
    DefaultedNamedType(
      'house', Integer(0).subtype(
        implicitTag=Tag(tagClassContext, tagFormatSimple, 1)
      )
    )
  )
```

It is in the spirit of ASN.1 to take abstract data description
and turn it into a programming language specific form.
Once you have your ASN.1 data structure expressed in Python, you
can use it along the lines of similar Python type (e.g. ASN.1
`SET` is similar to Python `dict`, `SET OF` to `list`):

```python
>>> record = Record()
>>> record['id'] = 123
>>> record['room'] = 321
>>> str(record)
Record:
id=123
room=321
>>>
```

Part of the power of ASN.1 comes from its serialisation features. You
can serialise your data structure and send it over the network.

```python
>>> from pyasn1.codec.der.encoder import encode
>>> substrate = encode(record)
>>> hexdump(substrate)
00000: 30 07 02 01 7B 80 02 01 41
```

Conversely, you can turn serialised ASN.1 content, as received from
network or read from a file, into a Python object which you can
introspect, modify, encode and send back.

```python
>>> from pyasn1.codec.der.decoder import decode
>>> received_record, rest_of_substrate = decode(substrate, asn1Spec=Record())
```

```
>>>
>>> for field in received_record:
>>>    print('{} is {}'.format(field, received_record[field]))
id is 123
room is 321
house is 0
>>>
>>> record == received_record
True
>>> received_record.update(room=123)
>>> substrate = encode(received_record)
>>> hexdump(substrate)
00000: 30 06 02 01 7B 80 01 7B
```

The pyasn1 classes struggle to emulate their Python prototypes (e.g. int, list, dict etc.). But ASN.1 types exhibit more complicated behaviour. To make life easier for a Pythonista, they can turn their pyasn1 classes into Python built-ins:

```python
>>> from pyasn1.codec.native.encoder import encode
>>> encode(record)
{'id': 123, 'room': 321, 'house': 0}
```

Or vice-versa -- you can initialize an ASN.1 structure from a tree of Python objects:

```python
>>> from pyasn1.codec.native.decoder import decode
>>> record = decode({'id': 123, 'room': 321, 'house': 0}, asn1Spec=Record())
>>> str(record)
Record:
id=123
room=321
>>>
```

With ASN.1 design, serialisation codecs are decoupled from data objects, so you could turn every single ASN.1 object into many different serialised forms. As of this moment, pyasn1 supports BER, DER, CER and Python built-ins codecs. The extremely compact PER encoding is expected to be introduced in the upcoming pyasn1 release.

More information on pyasn1 APIs can be found in the [documentation](http://snmplabs.com/pyasn1/), compiled ASN.1 modules for different protocols and file formats

could be found in the pyasn1-modules
[repo](https://github.com/etingof/pyasn1-modules).

How to get pyasn1

The pyasn1 package is distributed under terms and conditions of 2-clause
BSD [license](http://snmplabs.com/pyasn1/license.html). Source code is freely
available as a GitHub [repo](https://github.com/etingof/pyasn1).

You could `pip install pyasn1` or download it from [PyPI](https://pypi.org/project/pyasn1).

If something does not work as expected,
[open an issue](https://github.com/etingof/pyasn1/issues) at GitHub or
post your question [on Stack Overflow](https://stackoverflow.com/questions/ask)
or try browsing pyasn1
[mailing list archives](https://sourceforge.net/p/pyasn1/mailman/pyasn1-users/).

Found in path(s):
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/README.md
No license file was found, but licenses were detected in source scan.

# License: http://snmplabs.com/pyasn1/license.html

Found in path(s):
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/test_univ.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/native/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/compat/test_integer.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/cer/test_decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/ber/test_decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/der/test_decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/compat/integer.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/compat/test_binary.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/native/test_decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-

pyasn1-70c1bbd/tests/codec/der/test_encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/useful.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/namedtype.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/setup.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/test_char.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/cer/encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/debug.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/test_opentype.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/constraint.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/compat/string.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/test_debug.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/native/test_encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/compat/calling.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/der/encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/error.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/compat/binary.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/namedval.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/native/encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/test_namedval.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/ber/decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/compat/test_octets.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/compat/dateandtime.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/char.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/native/decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-

pyasn1-70c1bbd/tests/base.py

* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/test_useful.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/compat/octets.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/compat/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/tag.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/cer/test_encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/test_constraint.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/opentype.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/ber/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/der/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/ber/eoo.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/error.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/base.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/tagmap.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/type/test_namedtype.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/cer/decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/der/decoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/ber/test_encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/codec/ber/encoder.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/tests/codec/cer/__main__.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/pyasn1/type/univ.py
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-

pyasn1-70c1bbd/tests/type/test_tag.py
No license file was found, but licenses were detected in source scan.

Found in path(s):
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/LICENSE.rst
No license file was found, but licenses were detected in source scan.

```
ASN.1 library for Python
========================

.. toctree::
   :maxdepth: 1

Abstract Syntax Notation One (`ASN.1
<http://en.wikipedia.org/wiki/Abstract_Syntax_Notation_1x>`_) is a
technology for exchanging structured data in a universally understood,
hardware agnostic way. Many industrial, security and telephony
applications heavily rely on ASN.1.

The `pyasn1 <https://pypi.org/project/pyasn1/>`_ library implements
ASN.1 support in pure-Python.
```

What is ASN.1

ASN.1 is a large, arguably over-engineered and extremely old data modelling and
serialisation tool. It is probably among the first serialisation protocols in
the history of computer science and technology.

ASN.1 started its life over 30 years ago as a serialisation mechanism for the first
electronic mail (known as X.400). Later on if was split off the e-mail application
and become a stand-alone tech still being actively supported by its designers
and widely used in industry and technology.

Since then ASN.1 is sort of haunted by its relations with the OSI model -- the
first, unsuccessful, version of the Internet. You can read many interesting
`discussions <https://news.ycombinator.com/item?id=8871453>`_ on that topic.

In the following years, generations of software engineers tackled the serialisation
problem many times. We can see that in Google's `ProtoBuffers <https://developers.google.com/protocol-buffers/>`_
or `FlatBuffers <https://google.github.io/flatbuffers/>`_, for example.
Interestingly, many new takes on binary protocol design do not depart
far from ASN.1 from technical perspective. It's more of a matter of striking
a balance between processing overhead, wire format overhead and human
readability.

Looking at what ASN.1 has to offer, it has three loosely coupled parts:

* Data types: the standard introduces a collection of basic data types
  (integers, bits, strings, arrays and records) that can be used for describing
  arbitrarily complex, nested data structures.

* Serialisation protocols: the above data structures could be converted into a
  series of octets for storage or transmission over the wire as well as
  recovered back into their structured form. The system is fully agnostic
  to hardware architectures differences.

* Schema language: ASN.1 data structures could be described in terms
  of a schema language for ASN.1 compiler to turn it into platform-specific
  implementation.

ASN.1 applications

Being an old and generally successful standard, ASN.1 is widely
adopted for many uses. To give you an example, these technologies
use ASN.1 for their data exchange needs:

* Signaling standards for the public switched telephone network (SS7 family)

* Network management standards (SNMP, CMIP)
* Directory standards (X.500 family, LDAP)
* Public Key Infrastructure standards (X.509, etc.)
* PBX control (CSTA)
* IP-based Videoconferencing (H.323 family)
* Biometrics (BIP, CBEFF, ACBio)
* Intelligent transportation (SAE J2735)
* Cellular telephony (GSM, GPRS/EDGE, UMTS, LTE)

ASN.1 gotchas

Apparently, ASN.1 is hard to implement properly. Quality open-source
ASN.1 tools are rare, but ad-hoc implementations are numerous. Judging from the
`statistics <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ASN.1>`_ on discovered
security vulnerabilities, many people have implemented ASN.1 parsers
and oftentimes fell victim to its edge cases.

On the bright side, ASN.1 has been around for a long time, it is well understood
and security reviewed.

Documentation

```
.. toctree::
  :maxdepth: 2

  /pyasn1/contents
```

Use case

```
.. toctree::
  :maxdepth: 2

  /example-use-case
```

Download & Install

```
.. toctree::
  :maxdepth: 2

  /download
```

Changes

```
All changes and release history is maintained in changelog.  There you
could also download the latest unreleased pyasn1 tarball containing
the latest fixes and improvements.

.. toctree::
  :maxdepth: 1

  /changelog

License
-------

The PyASN1 software is distributed under 2-clause BSD License.

.. toctree::
  :maxdepth: 2

  /license

Getting help
------------

Please, file your `issues <https://github.com/etingof/pyasn1/issues>`_
and `PRs <https://github.com/etingof/pyasn1/pulls>`_ at GitHub.
Alternatively, you could ask for help at
`Stack Overflow <http://stackoverflow.com/questions/tagged/pyasn1>`_
or search
`pyasn1-users <https://lists.sourceforge.net/lists/listinfo/pyasn1-users>`_
mailing list archive.

Books on ASN.1
--------------

The pyasn1 implementation is largely based on reading up the following awesome
books:

* `ASN.1 - Communication between heterogeneous systems <http://www.oss.com/asn1/dubuisson.html>`_ by
Olivier Dubuisson
* `ASN.1 Complete <http://www.oss.com/asn1/resources/books-whitepapers-pubs/larmouth-asn1-book.pdf>`_ by
Prof John Larmouth

Here you can get the official standards which is hard to read:

* `ITU standards <http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-X.693-0207w.zip>`_

On the other end of the readability spectrum, here is a quick and sweet write up:

* `A Layman's Guide to a Subset of ASN.1, BER, and DER <ftp://ftp.rsasecurity.com/pub/pkcs/ascii/layman.asc>`_
```

by Burton S. Kaliski

If you are working with ASN.1, we'd highly recommend reading a proper
book on the subject.

Found in path(s):
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/docs/source/contents.rst
No license file was found, but licenses were detected in source scan.

.. _license:

License
=======

.. include:: ../../LICENSE.rst

Found in path(s):
* /opt/cola/permits/1673010604_1683816449.4330244/0/etingof-pyasn1-v0-4-8-0-g70c1bbd-1-tar-gz/etingof-pyasn1-70c1bbd/docs/source/license.rst

1.35 colorama 0.3.9

1.35.1 Available under license :

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.36 hyperlink 18.0.0

1.36.1 Available under license :

Copyright (c) 2017
Glyph Lefkowitz
Itamar Turner-Trauring
Jean Paul Calderone
Adi Roiban
Amber Hawkie Brown
Mahmoud Hashemi

and others that have contributed code to the public domain.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.37 netaddr 0.7.10

1.37.1 Available under license :

Here are the licenses applicable to the use of the netaddr library.

----
netaddr

COPYRIGHT AND LICENSE

----
intset.py

COPYRIGHT AND LICENSE

Here are the copyright notices applicable to the netaddr library.

----
netaddr

----
intset.py

IANA (Internet Assigned Numbers Authority)
----

netaddr is not sponsored nor endorsed by IANA.

Use of data from IANA (Internet Assigned Numbers Authority) is subject to copyright and is provided with prior written permission.

IANA data files included with netaddr are not modified in any way but are parsed and made available to end users through an API.

See README file and source code for URLs to latest copies of the relevant files.

IEEE (Institution of Electrical Engineers)
----

netaddr is not sponsored nor endorsed by the IEEE.

Use of data from the IEEE (Institute of Electrical and Electronics
Engineers) is subject to copyright. See the following URL for
details :-

http://www.ieee.org/web/publications/rights/legal.html

IEEE data files included with netaddr are not modified in any way but are
parsed and made available to end users through an API. There is no
guarantee that referenced files are not out of date.

See README file and source code for URLs to latest copies of the relevant
files.

1.38 twisted 22.4.0

1.38.1 Available under license :

Jrgen Hermann
Kevin Horn
Kevin Turner
Laurens Van Houtven
Mary Gardiner
Massachusetts Institute of Technology
Matthew Lefkowitz
Moshe Zadka
Paul Swartz
Pavel Pergamenshchik
Rackspace, US Inc.
Ralph Meijer
Richard Wall
Sean Riley
Software Freedom Conservancy
Tavendo GmbH
Thijs Triemstra
Thomas Grainger
Thomas Herve
Timothy Allen
Tom Most
Tom Prince
Travis B. Hartwell

and others that have contributed code to the public domain.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

1.39 python 3.8.12

1.39.1 Available under license :

Copyright (c) 2002 Jorge Acereda <jacereda@users.sourceforge.net> &
Peter O'Gorman <ogorman@users.sourceforge.net>

Portions may be copyright others, see the AUTHORS file included with this distribution.

Maintained by Peter O'Gorman <ogorman@users.sourceforge.net>

Bug Reports and other queries should go to <ogorman@users.sourceforge.net>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Additional Conditions for this Windows binary build

This program is linked with and uses Microsoft Distributable Code, copyrighted by Microsoft Corporation. The Microsoft Distributable Code is embedded in each .exe, .dll and .pyd file as a result of running the code through a linker.

If you further distribute programs that include the Microsoft Distributable Code, you must comply with the restrictions on distribution specified by Microsoft. In particular, you must require distributors and external end users to agree to terms that protect the Microsoft Distributable Code at least as much as Microsoft's own

requirements for the Distributable Code. See Microsoft's documentation
(included in its developer tools and on its website at microsoft.com)
for specific details.

Redistribution of the Windows binary build of the Python interpreter
complies with this agreement, provided that you do not:

- alter any copyright, trademark or patent notice in Microsoft's
Distributable Code;

- use Microsoft's trademarks in your programs' names or in a way that
suggests your programs come from or are endorsed by Microsoft;

- distribute Microsoft's Distributable Code to run on a platform other
than Microsoft operating systems, run-time technologies or application
platforms; or

- include Microsoft Distributable Code in malicious, deceptive or
unlawful programs.

These restrictions apply only to the Microsoft Distributable Code as
defined above, not to Python itself or any programs running on the
Python interpreter. The redistribution of the Python interpreter and
libraries is governed by the Python Software License included with this
file, or by other licenses as marked.
X Window System License - X11R6.4

Copyright (c) 1998 The Open Group

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR
OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,
ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

A. HISTORY OF THE SOFTWARE
==========================

Python was created in the early 1990s by Guido van Rossum at Stichting
Mathematisch Centrum (CWI, see http://www.cwi.nl) in the Netherlands
as a successor of a language called ABC. Guido remains Python's
principal author, although it includes many contributions from others.

In 1995, Guido continued his work on Python at the Corporation for
National Research Initiatives (CNRI, see http://www.cnri.reston.va.us)
in Reston, Virginia where he released several versions of the
software.

In May 2000, Guido and the Python core development team moved to
BeOpen.com to form the BeOpen PythonLabs team. In October of the same
year, the PythonLabs team moved to Digital Creations, which became
Zope Corporation. In 2001, the Python Software Foundation (PSF, see
https://www.python.org/psf/) was formed, a non-profit organization
created specifically to own Python-related Intellectual Property.
Zope Corporation was a sponsoring member of the PSF.

All Python releases are Open Source (see http://www.opensource.org for the Open Source Definition). Historically, most, but not all, Python releases have also been GPL-compatible; the table below summarizes the various releases.

Release	Derived from	Year	Owner	GPL-compatible? (1)
0.9.0 thru 1.2		1991-1995	CWI	yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI	yes
1.6	1.5.2	2000	CNRI	no
2.0	1.6	2000	BeOpen.com	no
1.6.1	1.6	2001	CNRI	yes (2)
2.1	2.0+1.6.1	2001	PSF	no
2.0.1	2.0+1.6.1	2001	PSF	yes
2.1.1	2.1+2.0.1	2001	PSF	yes
2.1.2	2.1.1	2002	PSF	yes
2.1.3	2.1.2	2002	PSF	yes
2.2 and above	2.1.1	2001-now	PSF	yes

Footnotes:

(1) GPL-compatible doesn't mean that we're distributing Python under the GPL. All Python licenses, unlike the GPL, let you distribute a modified version without making your changes open source. The GPL-compatible licenses make it possible to combine Python with other software that is released under the GPL; the others don't.

(2) According to Richard Stallman, 1.6.1 is not GPL-compatible, because its license has a choice of law clause. According to CNRI, however, Stallman's lawyer has told CNRI's lawyer that 1.6.1 is "not incompatible" with the GPL.

Thanks to the many outside volunteers who have worked under Guido's direction to make these releases possible.

B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING PYTHON

Python software and documentation are licensed under the Python Software Foundation License Version 2.

Starting with Python 3.8.6, examples, recipes, and other code in the documentation are dual licensed under the PSF License Version 2 and the Zero-Clause BSD license.

Some software incorporated into Python is under different licenses. The licenses are listed with code falling under that license.

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
----

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee

agrees to be bound by the terms and conditions of this License Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

6. This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
----

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1,

OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

7. This License Agreement shall be governed by the federal
intellectual property law of the United States, including without
limitation the federal copyright law, and, to the extent such
U.S. federal law does not apply, by the law of the Commonwealth of
Virginia, excluding Virginia's conflict of law provisions.
Notwithstanding the foregoing, with regard to derivative works based
on Python 1.6.1 that incorporate non-separable material that was
previously distributed under the GNU General Public License (GPL), the
law of the Commonwealth of Virginia shall govern this License
Agreement only as to issues arising under or with respect to
Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this
License Agreement shall be deemed to create any relationship of
agency, partnership, or joint venture between CNRI and Licensee. This
License Agreement does not grant permission to use CNRI trademarks or
trade name in a trademark sense to endorse or promote products or
services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying,
installing or otherwise using Python 1.6.1, Licensee agrees to be
bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam,
The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of Stichting Mathematisch
Centrum or CWI not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior
permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE
FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES

WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ZERO-CLAUSE BSD LICENSE FOR CODE IN THE PYTHON DOCUMENTATION

Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR
OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
Copyright (c) 1998-2000 Thai Open Source Software Center Ltd and Clark Cooper
Copyright (c) 2001-2019 Expat maintainers

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
This license applies to the bootstrapper application that is embedded within the installer. It has no impact on the licensing for the rest of the installer or Python itself, as no code covered by this license exists in any other part of the product.

Microsoft Reciprocal License (MS-RL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions
The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.
A "contribution" is the original software, or any additions or changes to the software.
A "contributor" is any person that distributes its contribution under this license.
"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights
(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.
(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations
(A) Reciprocal Grants- For any file you distribute that contains code from the software (in source code or binary format), you must provide recipients the source code to that file along with a copy of this license, which license will govern that file. You may license other files that are entirely your own work and do not contain code from the software under any terms you choose.
(B) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.
(C) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.
(D) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.
(E) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.
(F) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

Copyright and License Information

See the file "LICENSE" for information on the history of this software, terms & conditions for usage, and a DISCLAIMER OF ALL WARRANTIES.

This Python distribution contains *no* GNU General Public License (GPL) code, so it may be used in proprietary projects. There are interfaces to some GNU code but these are entirely optional.

All trademarks referenced herein are property of their respective holders.