Intel® Integrated Performance Primitives (Intel® IPP) 2018 Update 4 Release Notes

20 Sep, 2018

Contents

Overview

This document provides a general summary of new features and important notes about the Intel® Integrated Performance Primitives (Intel® IPP) library software product.

Please see the following resources available online for the latest information regarding the Intel® Integrated Performance Primitives (Intel® IPP):

- Intel® IPP Main Product Page
- Intel® IPP Installation Guide
- Intel® IPP 2018 System Requirements

Please register your product using your preferred email address. This helps Intel recognize you as a valued customer in the support forum and insures that you will be notified of product updates. You can read Intel Privacy Policy if you have any questions regarding the use of your email address for software product registration.

What's New in Intel® IPP 2018 Update 4

- Added new APIs to compute CRC24 and CRC16 checksum with 1U input data. The APIs support CRC24A, CRC24B, CRC24C and CRC16 polynomial functions, and are included in the Intel® IPP embedded domain.
- Fixed a number of internal and external defects. For more details, please, visit Intel® IPP 2018 Bug Fixes.

What's New in Intel® IPP 2018 Update 3.1

- Minor improvements in mitigation for security vulnerability CVE-2018-3617 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-3617) in the Intel® IPP Cryptography libraries.

  Note: Intel® IPP 2018 Update 3.1 provides an update package for the Cryptography functions, and does not include Intel® IPP main package. This Cryptography release can work with Intel® IPP 2018 Update 3 main packages.

What's New in Intel® IPP 2018 Update 3

- Improved LZ4 compression and decompression performance on data with high entropy.

- Fixed a number of internal and external defects. Visit the Intel® IPP 2018 bug fixes for more information.

What's New in Intel® IPP 2018 Update 2.1

- Mitigated security vulnerability CVE-2018-3617 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-3617) in the Intel® IPP Cryptography libraries.

Note: Intel® IPP 2018 Update 2.1 provides an update package for the Cryptography functions, and does not include Intel® IPP main package. This Cryptography release can work with Intel® IPP 2018 Update 2 main packages.

What's New in Intel® IPP 2018 Update 2

- Added the new APIs to computes the CRC24 and CRC16 checksum. The APIs support CRC24A, CRC24B, CRC24C and CRC16 polynomial functions, and are included in the Intel® IPP embedded domain within the Intel® System Studio package.

- Added new APIs in the image processing domain for fixed point Resize functionality. The functionality provides faster resize operations with less accuracy.

- Extended optimization for Intel®AVX2 and Intel® AVX-512 instruction set in the following functions:
  - Image processing: ippiSeparableFilter, ippiNorm, ipprFilterBorder_L
  - Signal processing: ippsAdd_32u

- Extended optimization for Intel® SSE4.2 and Intel®AVX2 instruction set for LZ4 data compression functions.

- Fixed the problem on the incorrect code dispatching for the Intel® AVX512 processor systems running with the OS that does not support AVX-512 instructions. The problem caused some Intel® IPP functions report "illegal instructions" errors.

- Fixed a number of internal and external defects. For more details, please, visit Intel® IPP 2018 Bug Fixes.

What's New in Intel® IPP 2018 Update 1

- Added new Platform-Aware APIs ipprFilterBorder for 3D data filtering, and ipprCopyBorder for 3D border data copying.

- Extended optimization for Intel® AVX-512 instruction set in the following functions:
  - Image processing: ippiFilterBorder_<16u|16s>_C1R; ippiResizeAntialiasing_8u_C4; ippiResizeLanczos_8u

    - Signal processing: ippsSqrt_<8u|16s|16u|16sc|32s>;ippsCopyBE_1u;
    - FFT transform functions for order size larger than 17.

- Extended optimization for Intel® SSE4.2 instruction set in the following functions:
    - Image processing: ippiFilterBoxBorder_<16s|8u>; ippiFilterBoxBorder_<16s|8u>_C3, ippiResizeLenear for scale size 0.5, ippiMean_StdDev
    - Signal processing: ippsMagnitude_<64f|32f>

- Fixed a number of internal and external defects. Visit the Intel® IPP 2018 bug fixes for more information.

What's New in Intel® IPP 2018

- Added new functions to support the LZ4 data compression and decompression. This release also introduces the patch files for LZ4 source to provide drop-in optimization with the Intel® IPP functions.

- Introduced the standalone cryptography packages. The cryptography functions no longer depend on the main Intel® IPP packages, and can be used without the main Intel® IPP packages.

- Introduced the optimization code for the GraphicsMagick source. The code can provide drop-in optimization on GraphicsMagick with the Intel® IPP functions:

    - The code supports GraphicsMagick version 1.3.25, and provides optimization for the following GraphicsMagick APIs: ResizeImage, ScaleImage, GaussianBlurImage, FlipImage, and FlopImage.
    - The optimization code can improve the APIs performance by up to 4x, depending on the functionality, input parameters, and processors.

- Made the Integration Wrappers APIs part of the Intel® IPP packages.

- Computer Vision:

    - Added the 64-bit data length support to Canny edge detection functions (ippiCanny_32f8u_C1R_L).

- Color Conversion:

    - Added the ippiDemosaicVNG functions that support the demosaicing algorithm with VNG interpolation.

- Cryptography:
    - Added the Elliptic Curves key generation and Elliptic Curves based Diffie-Hellman shared secret functionality.
    - Added the Elliptic Curves sign generation and verification functionalities for the DSA, NR, and SM2 algorithms.
    - Added CBC-CTS mode encryption and decryption to AES and SMS4 block ciphers.
- Performance:
    - Extended optimization for the Intel® Advanced Vector Extensions 512 (Intel® AVX-512) and Intel® Advanced Vector Extensions 2 (Intel® AVX2) instruction sets.
    - Improved performance of LZO data compression functions on Intel® AVX2 and Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2).
- Other Changes:
    - Removed support for Intel® Pentium® III processor. The minimal supported instruction set is Intel® Streaming SIMD Extensions 2 (Intel® SSE2).
    - Removed support for the Intel® Xeon Phi™ x100 product family coprocessor (formerly code name Knights Corner) in this release.
        - The Intel® Xeon Phi™ x100 product family coprocessor (formerly code named Knights Corner) was officially announced end of life in January 2017. As part of the end of life process, the support for this family will only be available in the Intel® Parallel Studio XE 2017 version. Intel® Parallel Studio XE 2017 will be supported for a period of 3 years ending in January 2020 for the Intel® Xeon Phi™ x100 product family. Support will be provided for those customers with active support.

Threading Notes

To support the internal threading in the Intel® IPP functions, Intel® IPP provides the Threading Layer APIs in the platform-aware functions. These APIs can support both 64-bit object sizes (for large size images and signal data) and internal threading in Intel® IPP functions. Check the “Threading Layer Functions” pat in the Intel® IPP Developer Reference to get more information on these APIs. Your feedback on extending the new threading functions is welcome.

The legacy Intel IPP threaded libraries are available by the custom installation, and the code written with these libraries will still work as before. However, the threaded library will not expand its threading functions, and the new threading will be developed only in

the new Intel® IPP threading layer APIs. User's application is recommended to use the new Intel® IPP threading layer APIs or implement the external threading in their applications.

Known Intel® IPP 2018 Update 4 Issues and Limitations

- The LZO decoding functions have about 20% performance degradation after the fix of a buffer overflow issue.

- Some unused symbols are exposed, and building shared objects statically linking with Intel® IPP libraries may fail. This problem will be fixed in future product releases. The workaround for this release is to build shared objects with export definition lists.

System Requirements

For information about the Intel® IPP system requirements, please visit Intel® Integrated Performance Primitives (Intel® IPP) 2018 System Requirements page.

Intel® IPP 2018 Documentation

Starting with this version of Intel IPP, most of the documentation is only available online at Intel® Software Documentation Library. You can also download it from the Intel® Software Development Products Registration Center > Product List > Intel® Parallel Studio XE(or Intel® System Studio) Documentation.

Product Contents

The Intel® IPP for Windows*, Linux* OS, and macOS* is provided as part of the Intel® Parallel Studio XE and Intel® System Studio product. It is also available from the free Intel® performance libraries program:

- Installation package only supports 64-bit host system. It includes both the 64-bit and 32-bit target libraries.
- Installation package also provides the online installer that downloads materials chosen during installation

Intel® IPP Cryptography is provided as the following optional packages:

- Intel® IPP Cryptography for Windows*
- Intel® IPP Cryptography for Linux* OS
- Intel® IPP Cryptography for macOS*

Intel® IPP Cryptography

Intel® IPP Cryptography is a separate installation package that contains the binaries and header files needed to utilize the functions contained in the Intel IPP cryptography domain. Intel® IPP 2018 removed the cryptography code dependency on the main package, and the cryptography functions are provided as the standalone packages. To obtain the Intel IPP Cryptography libraries, please review the knowledge base article: where do I download the Intel® IPP cryptography libraries.

Technical Support

If you did not register your Intel® software product during installation, please do so now at the Intel® Software Development Products Registration Center. Registration entitles you to free technical support, product updates and upgrades for the duration of the support term.

For technical information about the Intel® IPP, including FAQ's, tips and tricks, and other support information, please visit the Intel® IPP forum: http://software.intel.com/en-us/forums/intel-integrated-performance-primitives/ and browse the Intel® IPP support page: https://software.intel.com/en-us/intel-ipp-support/.

For general information about Intel technical support, product updates, user forums, FAQs, tips and tricks and other support questions, please visit http://www.intel.com/software/products/support/.

Note: If your distributor provides technical support for this product, please contact them rather than Intel.

License Definitions

Any software source code included with this product is furnished under a software license and may only be used or copied in accordance with the terms of that license. Please see the Intel® Software Products End User License Agreement for license definitions and restrictions on the library.

Third Party Licenses

Intel® Integrated Performance Primitives (Intel® IPP) includes content from several 3rd party sources that was originally governed by the licenses referenced below:

- zlib library:

  zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.8, April 28th, 2013
  Copyright© 1995-2013 Jean-loup Gailly and Mark Adler
  This software is provided 'as-is', without any express or implied warranty. In no event will

the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution
   Jean-loup Gailly Mark Adler
   jloup@gzip.org madler@alumni.caltech.eduzlib

- bzip2:

  Copyright© 1996 - 2015 julian@bzip.org

Legal Information

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below. You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER

OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.
The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.
Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.
Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to:
http://www.intel.com/design/literature.htm.

MPEG-1, MPEG-2, MPEG-4, H.261, H.263, H.264, MP3, DV, VC-1, MJPEG, AC3, AAC, G.711, G.722, G.722.1, G.722.2, AMRWB, Extended AMRWB (AMRWB+), G.167, G.168, G.169, G.723.1, G.726, G.728, G.729, G.729.1, GSM AMR, GSM FR are international standards promoted by ISO, IEC, ITU, ETSI, 3GPP and other organizations. Implementations of these standards, or the standard enabled platforms may require licenses from various entities, including Intel Corporation.

BlueMoon, BunnyPeople, Celeron, Centrino, Cilk, Flexpipe, Intel, the Intel logo, the Intel Anti-Theft technology logo, Intel AppUp, the Intel AppUp logo, Intel Atom, Intel CoFluent, Intel Core, Intel Inside, the Intel Inside logo, Intel Insider, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel Sponsors of Tomorrow., the Intel Sponsors of Tomorrow. logo, Intel vPro, Intel Xeon Phi, Intel XScale, InTru, the InTru logo, the InTru Inside logo, InTru soundmark, Iris, Itanium, Look Inside, the Look Inside logo, MCS, MMX, Pentium, Puma, RealSense, skoool, the skoool logo, SMARTi, Sound Mark, Stay With It, the Engineering Stay With It logo, The Creators Project, The Journey Inside, Thunderbolt, the Thunderbolt logo, Ultrabook, VTune, Xeon, X-GOLD and XMM are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.
Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.
Java is a registered trademark of Oracle and/or its affiliates.

Optimization Notice

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Notice revision #20110804