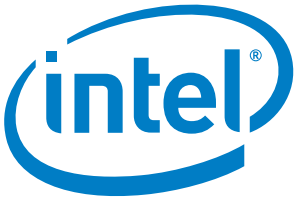


ISA-L Performance Report
Release 2.19

Test Date: Sept 29th 2017

Revision History

Date	Revision	Comment
Sept 29th, 2017	1.0	Initial document for release

Contents

Audience and Purpose

The Intel® Intelligent Storage Acceleration Library (Intel® ISA-L) is a library of highly-optimized algorithms released as free and open-source code under the BSD license [https://opensource.org/licenses/BSD-3-Clause]. ISA-L is intended for software application developers, particularly within the storage domain, seeking performance advantage from data protection algorithms (e.g. RAID5, RAID6, or Reed-Solomon erasure coding), data integrity (CRC variants), encryption ciphers, hash computation, and compression. The library is designed for software-defined infrastructure use cases, abstracting away the requirement to be platform aware in performance-path code by intelligently using the appropriate version at runtime for the underlying processor hardware implementation. Due to its low-level implementation (in hand-coded assembly instead of high-level languages) ISA-L is able to run effectively in any OS or virtualization environment.

This document is intended to provide a detailed performance and configuration reference for architects and developers to correlate relative and absolute performance measurements to hardware. This should assist in sizing platform capabilities and requirements for a given workload. For example, take an architect who needs to determine which CPU SKU should be targeted for their product. They will need to plan for a sufficient number of cores to keep up with a network encryption workload, plus CRC and hashing functions on all written data to prepare for de-duplication. This document provides metrics that should allow the architect to estimate the number of CPU cycles required to meet their design objectives, to assist in making a SKU recommendation.

Test setup:

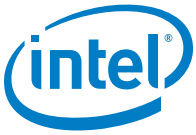
The device under test (DUT) consists of a system with an Intel® architecture motherboard populated with the following:

- A single or dual processor and PCH chip, except for System on Chip (SoC) cases
- DRAM memory size and frequency varies (normally single DIMM per channel)
- BIOS settings noting those that are updated from the default setting
- Operating System containing ISA-L library and dependencies

Benchmarking with Intel® ISA-L requires knowledge of the algorithms offered, and how they allocate and use system resources. An understanding of a platforms CPU features and capabilities as well as memory performance capability will help in analyzing the performance metrics behind the benchmark results. System tuning via BIOS setting can optimize the platform for best performance. Performance results will vary based on system hardware and software configurations. The measurements provided in this document are a result of the documented system configurations.

To build and install Intel® ISA-L for performance testing a number of dependencies are required:

- Automake
- Gcc
- Gcc-c++
- Yasm
- Nasm
- Openssl
- Openssl-devel
- Libssl-dev



ISA-L function unit tests are a set of micro benchmarks that exercise many of the algorithms in the library. Using the included Makefile, benchmark binary files are created with the command 'make perfs' and are located in their respective directories. Each benchmark measures system performance by timing a number of iterations of an algorithm on a buffer, and reporting throughput. Unit tests run using a single CPU core, and by default run cache cold. An optional test configuration will pre-fill the buffer before starting the test for a cache warm measurement.

ISA-L compression unit tests are a set of micro benchmarks that exercise compression and decompression levels offered in the library. Using the included Makefile, benchmark binary files are created with the command 'make other' and are located in their respective directories. Each benchmark takes an input file to compress, measures performance by timing a number of iterations of compression or decompression on the input file, and reports throughput. Unit tests run using a single CPU core. Results of a compression test will vary depending on the corpus used as input. The two corpora used in this document for performance are the Silesia corpus and the Calgary corpus.

ISA-L API: Documentation may be found at

https://github.com/01org/isa-l/wiki/Documentation

ISA-L source and benchmarks: May be cloned from GitHub.

https://github.com/01org/isa-l.git

https://github.com/01org/isa-l_crypto

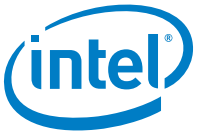
Intel® Xeon® Platinum 8180 Processor (38.5M Cache, 2.50 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	Intel® Neon City CRB
CPU	Intel® Xeon® Platinum 8180 Processor (38.5M Cache, 2.50 GHz) http://ark.intel.com/products/120496/Intel-Xeon-Platinum-8180-Processor-38_5M-Cache-2_50-GHz Number of cores 28, Number of threads 56.
Memory	6x 16 GB DDR4 2666 MT/s ECC RDIMM
Operating System	RHEL 7.3
BIOS	PLYCRB1.86B.0128.R08.1703242666
Linux kernel version	4.9.4
GCC version	4.8.5
Yasm version	1.3.0
Nasm version	2.11.08
OpenSSL version	1.0.2j
Zlib version	1.2.11
ISA-L version	2.19

Boot and BIOS settings

Item	Description	Setting
BIOS	CPU Power and Performance Policy	Performance
	CPU C-state	Disabled
	CPU P-state	Disabled
	SpeedStep	Disabled
	Turbo Boost	Disabled
	Memory Power Savings	Disabled



Function Unit testing

Item	Description
Test case	Unit function tests
Test parameters	Single core performance Cache cold
Command line	make –k perf

Test Result:

	ISA-L		OpenSSL	
ISA-L Function	**Cycle/Byte Performance**	**Single Core Throughput**	**Cycle/Byte Performance**	**Single Core Throughput**
Cryptographic Hashing				
Rolling Hash 64 bit	2.53	988 MB/s	-	-
Multihash SHA-1	0.42	5.8 GB/s	-	-
Multihash SHA-1 Murmur	0.63	3.8 GB/s	-	-
Multihash SHA-256	0.82	2.9 GB/s	-	-
Multibuffer SHA-1	0.45	5.4 GB/s	4.13	605 MB/s*
Multibuffer SHA-256	0.88	2.7 GB/s	11.56	216 MB/s*
Multibuffer SHA-512	1.08	2.2 GB/s	7.48	334 MB/s*
Multibuffer MD5	0.25	9.7 GB/s	4.99	401 MB/s*
Encryption				
AES-XTS 128	0.64	3.8 GB/s	0.64	3.8 GB/s
AES-XTS 256	0.88	2.7 GB/s	0.89	2.7 GB/s
AES-CBC 128 Decode	0.64	3.8 GB/s	0.64	3.8 GB/s
AES-CBC 192 Decode	0.76	3.2 GB/s	0.76	3.2 GB/s
AES-CBC 256 Decode	0.88	2.7 GB/s	0.88	2.7 GB/s
AES-GCM 128	0.67	3.6 GB/s	1.58	1.5 GB/s
AES-GCM 256	0.89	2.7 GB/s	1.83	1.3 GB/s
Data Protection				
PQ Gen (16+2)	0.10	23.4 GB/s	-	-
XOR Gen (16+1)	0.10	24.2 GB/s	-	-
Reed Solomon EC (10+4)	0.19	12.7 GB/s	-	-
Data Integrity				
CRC16 T10	0.22	11.0 GB/s	-	-
CRC32 IEEE (802.3)	0.22	11.1 GB/s	-	-
CRC32 iSCSI	0.18	13.8 GB/s	-	-
CRC32 GZIP Reflective	0.24	10.3 GB/s	-	-
CRC64 Normal	0.22	11.0 GB/s	-	-
CRC64 Reflective	0.19	12.9 GB/s	-	-

*Performance based on single buffer hashing

Compression testing

Item	Description
Test Case	Compression tests
Test parameters	Single core performance Iterations vary based on input size
Command line	Make other D='-D ZLIB_COMPARE'
	./igzip/igzip_stateless_file_perf
	./igzip/igzip_inflate_perf
Corpa	Silesia Corpus http://sun.aei.polsl.pl/~sdeor/index.php?page=silesia
	Calgary Corpus http://corpus.canterbury.ac.nz/descriptions/#calgary

Test Result:

	ISA-L			ZLIB		
ISA-L Function	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**
Stateless Compress Level 0 Calgary Corpus	8.21	304 MB/s	40.52%	51.80	48 MB/s	39.24%
Stateless Compress Level 0 Silesia	7.03	355 MB/s	41.35%	49.29	50 MB/s	38.33%
Stateless Compress Level 1 Calgary Corpus	8.54	292 MB/s	37.51%	-	-	-
Stateless Compress Level 1 Silesia	7.25	344 MB/s	36.86%	-	-	-
Decompress "Inflate" Calgary Corpus	6.23	400 MB/s	40.52%	12.69	197 MB/s	39.24%
Decompress "Inflate" Silesia	5.30	471 MB/s	41.35%	12.25	204 MB/s	38.33%

Intel® Xeon® Processor E5-2650 v4 (30M Cache, 2.20 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	Intel® Aztec City CRB
CPU	Intel® Xeon® Processor E5-2650 v4 (30M Cache, 2.20 GHz) http://ark.intel.com/products/91767/Intel-Xeon-Processor-E5-2650-v4-30M-Cache-2_20-GHz Number of cores 12, Number of threads 24.
Memory	4x 8 GB DDR4 2400 MT/s ECC RDIMM
Operating System	RHEL 7.3
BIOS	GRRFCRB1.86B.0276.R02.1606020546
Linux kernel version	4.9.4
GCC version	4.8.5
Yasm version	1.3.0
Nasm version	2.11.08
OpenSSL version	1.0.2j
Zlib version	1.2.11
ISA-L version	2.19

Boot and BIOS settings

Item	Description	Setting
BIOS	CPU Power and Performance Policy	Performance
	CPU C-state	Disabled
	CPU P-state	Disabled
	SpeedStep	Disabled
	Turbo Boost	Disabled
	Memory Power Savings	Disabled

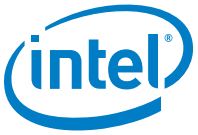
Function Unit testing

Item	Description
Test case	Unit function tests
Test parameters	Single core performance Cache cold
Command line	make –k perf

Test Result:

	ISA-L		OpenSSL	
ISA-L Function	**Cycle/Byte Performance**	**Single Core Throughput**	**Cycle/Byte Performance**	**Single Core Throughput**
Cryptographic Hashing				
Rolling Hash 64 bit	2.67	822 MB/s	-	-
Multihash SHA-1	1.09	2.0 GB/s	-	-
Multihash SHA-1 Murmur	1.37	1.5 GB/s	-	-
Multihash SHA-256	2.56	860 MB/s	-	-
Multibuffer SHA-1	1.14	1.8 GB/s	4.17	527 MB/s*
Multibuffer SHA-256	2.61	842 MB/s	12.44	176 MB/s*
Multibuffer SHA-512	3.25	676 MB/s	7.95	276 MB/s*
Multibuffer MD5	0.60	3.5 GB/s	4.97	443 MB/s*
Encryption				
AES-XTS 128	0.73	2.9 GB/s	0.87	2.4 GB/s
AES-XTS 256	0.93	2.2 GB/s	1.15	1.8 GB/s
AES-CBC 128 Decode	0.65	3.3 GB/s	0.81	2.6 GB/s
AES-CBC 192 Decode	0.76	2.8 GB/s	0.93	2.3 GB/s
AES-CBC 256 Decode	0.89	2.4 GB/s	1.06	2.0 GB/s
AES-GCM 128	0.80	2.7 GB/s	1.97	1.0 GB/s
AES-GCM 256	1.05	2.1 GB/s	2.26	972 MB/s
Data Protection				
PQ Gen (16+2)	0.11	18.7 GB/s	-	-
XOR Gen (16+1)	0.10	21.4 GB/s	-	-
Reed Solomon EC (10+4)	0.40	5.3 GB/s	-	-
Data Integrity				
CRC16 T10	0.18	12.0 GB/s	-	-
CRC32 IEEE (802.3)	0.18	12.0 GB/s	-	-
CRC32 iSCSI	0.19	11.6 GB/s	-	-
CRC32 GZIP Reflective	0.18	11.9 GB/s	-	-
CRC64 Normal	0.18	11.9 GB/s	-	-
CRC64 Reflective	0.18	11.8 GB/s	-	-

*Performance based on single buffer hashing



Compression testing

Item	Description
Test Case	Compression tests
Test parameters	Single core performance Iterations vary based on input size
Command line	Make other D='-D ZLIB_COMPARE'
	./igzip/igzip_stateless_file_perf
	./igzip/igzip_inflate_perf
Corpa	Silesia Corpus http://sun.aei.polsl.pl/~sdeor/index.php?page=silesia
	Calgary Corpus http://corpus.canterbury.ac.nz/descriptions/#calgary

Test Result:

	ISA-L			ZLIB		
ISA-L Function	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**
Stateless Compress Level 0 Calgary Corpus	7.87	279 MB/s	40.52%	50.82	43 MB/s	39.24%
Stateless Level 0 Compress Silesia	6.78	324 MB/s	41.35%	48.59	45 MB/s	38.33%
Stateless Compress Level 1 Calgary Corpus	8.41	261 MB/s	37.51%	-	-	-
Stateless Compress Level 1 Silesia	7.21	305 MB/s	36.86%	-	-	-
Decompress "Inflate" Calgary Corpus	6.07	362 MB/s	40.52%	12.56	175 MB/s	39.24%
Decompress "Inflate" Silesia	5.20	422 MB/s	41.35%	12.08	182 MB/s	38.33%

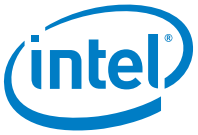
Intel® Xeon® Processor E5-2650 v3 (25M Cache, 2.30 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	Intel® Aztec City CRB
CPU	Intel® Xeon® Processor E5-2650 v3 (25M Cache, 2.30 GHz) http://ark.intel.com/products/81705/Intel-Xeon-Processor-E5-2650-v3-25M-Cache-2_30-GHz Number of cores 10, Number of threads 20.
Memory	4x 8 GB DDR4 2133 MT/s ECC RDIMM
Operating System	RHEL 7.3
BIOS	GRRFCRB1.86B.0276.R02.1606020546
Linux kernel version	4.9.4
GCC version	4.8.5
Yasm version	1.3.0
Nasm version	2.11.08
OpenSSL version	1.0.2j
Zlib version	1.2.11
ISA-L version	2.19

Boot and BIOS settings

Item	Description	Setting
BIOS	CPU Power and Performance Policy	Performance
	CPU C-state	Disabled
	CPU P-state	Disabled
	SpeedStep	Disabled
	Turbo Boost	Disabled
	Memory Power Savings	Disabled



Function Unit testing

Item	Description
Test case	Unit function tests
Test parameters	Single core performance Cache cold
Command line	make –k perf

Test Result:

	ISA-L		OpenSSL	
ISA-L Function	**Cycle/Byte Performance**	**Single Core Throughput**	**Cycle/Byte Performance**	**Single Core Throughput**
Cryptographic Hashing				
Rolling Hash 64 bit	2.83	811 MB/s	-	-
Multihash SHA-1	1.11	2.0 GB/s	-	-
Multihash SHA-1 Murmur	1.38	1.6 GB/s	-	-
Multihash SHA-256	2.55	900 MB/s	-	-
Multibuffer SHA-1	1.15	1.9 GB/s	4.24	542 MB/s*
Multibuffer SHA-256	2.61	881 MB/s	12.60	183 MB/s*
Multibuffer SHA-512	3.34	689 MB/s	8.05	286 MB/s*
Multibuffer MD5	0.60	3.7 GB/s	4.95	465 MB/s*
Encryption				
AES-XTS 128	0.74	3.0 GB/s	0.87	2.5 GB/s
AES-XTS 256	0.94	2.4 GB/s	1.16	1.9 GB/s
AES-CBC 128 Decode	0.65	3.4 GB/s	0.82	2.7 GB/s
AES-CBC 192 Decode	0.77	2.9 GB/s	0.93	2.4 GB/s
AES-CBC 256 Decode	0.89	2.5 GB/s	1.08	2.0 GB/s
AES-GCM 128	1.18	1.9 GB/s	2.03	1.1 GB/s
AES-GCM 256	1.46	1.5 GB/s	2.32	990 MB/s
Data Protection				
PQ Gen (16+2)	0.14	16.5 GB/s	-	-
XOR Gen (16+1)	0.13	17.8 GB/s	-	-
Reed Solomon EC (10+4)	0.42	5.3 GB/s	-	-
Data Integrity				
CRC16 T10	0.26	8.6 GB/s	-	-
CRC32 IEEE (802.3)	0.26	8.6 GB/s	-	-
CRC32 iSCSI	0.18	12.7 GB/s	-	-
CRC32 GZIP Reflective	0.26	8.6 GB/s	-	-
CRC64 Normal	0.26	8.6 GB/s	-	-
CRC64 Reflective	0.26	8.6 GB/s	-	-

*Performance based on single buffer hashing

Compression testing

Item	Description
Test Case	Compression tests
Test parameters	Single core performance Iterations vary based on input size
Command line	Make other D='-D ZLIB_COMPARE'
	./igzip/igzip_stateless_file_perf
	./igzip/igzip_inflate_perf
Corpa	Silesia Corpus http://sun.aei.polsl.pl/~sdeor/index.php?page=silesia
	Calgary Corpus http://corpus.canterbury.ac.nz/descriptions/#calgary

Test Result:

	ISA-L			ZLIB		
ISA-L Function	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**
Stateless Compress Level 0 Calgary Corpus	7.94	289 MB/s	40.52%	51.73	44 MB/s	39.24%
Stateless Level 0 Compress Silesia	6.82	337 MB/s	41.35%	49.45	46 MB/s	38.33%
Stateless Compress Level 1 Calgary Corpus	8.83	260 MB/s	37.51%	-	-	-
Stateless Compress Level 1 Silesia	7.57	303 MB/s	36.86%	-	-	-
Decompress "Inflate" Calgary Corpus	6.21	369 MB/s	40.52%	12.66	181 MB/s	39.24%
Decompress "Inflate" Silesia	5.31	432 MB/s	41.35%	12.23	188 MB/s	38.33%

Intel® Xeon® Processor D-1541 (12M Cache, 2.10 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	Intel® Camelback Mountain CRB
CPU	Intel® Xeon® Processor D-1541 (12M Cache, 2.10 GHz) http://ark.intel.com/products/91199/Intel-Xeon-Processor-D-1541-12M-Cache-2_10-GHz Number of cores 8, Number of threads 16.
Memory	2x 8 GB DDR4 2400 MT/s ECC RDIMM
Operating System	RHEL 7.3
BIOS	GNVDINT1.86B.0085.V13.1512071751
Linux kernel version	4.9.4
GCC version	4.8.5
Yasm version	1.3.0
Nasm version	2.11.08
OpenSSL version	1.0.2j
Zlib version	1.2.11
ISA-L version	2.19

Boot and BIOS settings

Item	Description	Setting
BIOS	CPU Power and Performance Policy	Performance
	CPU C-state	Disabled
	CPU P-state	Disabled
	SpeedStep	Disabled
	Turbo Boost	Disabled
	Memory Power Savings	Disabled

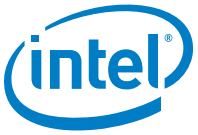
Function Unit testing

Item	Description
Test case	Unit function tests
Test parameters	Single core performance Cache cold
Command line	make –k perf

Test Result:

	ISA-L		OpenSSL	
ISA-L Function	**Cycle/Byte Performance**	**Single Core Throughput**	**Cycle/Byte Performance**	**Single Core Throughput**
Cryptographic Hashing				
Rolling Hash 64 bit	2.68	783 MB/s	-	-
Multihash SHA-1	1.12	1.8 GB/s	-	-
Multihash SHA-1 Murmur	1.38	1.4 GB/s	-	-
Multihash SHA-256	2.59	810 MB/s	-	-
Multibuffer SHA-1	1.14	1.8 GB/s	4.18	502 MB/s*
Multibuffer SHA-256	2.61	804 MB/s	12.46	168 MB/s*
Multibuffer SHA-512	3.26	643 MB/s	7.96	263 MB/s*
Multibuffer MD5	0.60	3.4 GB/s	4.96	422 MB/s*
Encryption				
AES-XTS 128	0.74	2.7 GB/s	0.87	2.3 GB/s
AES-XTS 256	0.95	2.1 GB/s	1.16	1.7 GB/s
AES-CBC 128 Decode	0.65	3.1 GB/s	0.81	2.5 MB/s
AES-CBC 192 Decode	0.76	2.6 GB/s	0.93	2.2 GB/s
AES-CBC 256 Decode	0.89	2.3 GB/s	1.06	1.9 GB/s
AES-GCM 128	0.80	2.5 GB/s	1.97	1.0 GB/s
AES-GCM 256	1.05	1.9 GB/s	2.26	927 MB/s
Data Protection				
PQ Gen (16+2)	0.16	12.6 GB/s	-	-
XOR Gen (16+1)	0.16	12.4 GB/s	-	-
Reed Solomon EC (10+4)	0.44	4.6 GB/s	-	-
Data Integrity				
CRC16 T10	0.17	12.1 GB/s	-	-
CRC32 IEEE (802.3)	0.17	12.1 GB/s	-	-
CRC32 iSCSI	0.17	11.7 GB/s	-	-
CRC32 GZIP Reflective	0.17	12.0 GB/s	-	-
CRC64 Normal	0.17	12.1 GB/s	-	-
CRC64 Reflective	0.17	12.1 GB/s	-	-

*Performance based on single buffer hashing



Compression testing

Item	Description
Test Case	Compression tests
Test parameters	Single core performance Iterations vary based on input size
Command line	Make other D='-D ZLIB_COMPARE'
	./igzip/igzip_stateless_file_perf
	./igzip/igzip_inflate_perf
Corpa	Silesia Corpus http://sun.aei.polsl.pl/~sdeor/index.php?page=silesia
	Calgary Corpus http://corpus.canterbury.ac.nz/descriptions/#calgary

Test Result:

	ISA-L			ZLIB		
ISA-L Function	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**
Stateless Compress Level 0 Calgary Corpus	7.85	267 MB/s	40.52%	50.87	41 MB/s	39.24%
Stateless Level 0 Compress Silesia	6.79	308 MB/s	41.35%	48.63	45 MB/s	38.33%
Stateless Compress Level 1 Calgary Corpus	8.41	249 MB/s	37.51%	-	-	-
Stateless Compress Level 1 Silesia	7.21	290 MB/s	36.86%	-	-	-
Decompress "Inflate" Calgary Corpus	6.08	345 MB/s	40.52%	12.55	175 MB/s	39.24%
Decompress "Inflate" Silesia	5.21	402 MB/s	41.35%	12.14	182 MB/s	38.33%

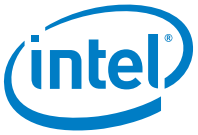
Intel® Atom™ Processor C3958 (16M Cache, 2.00 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	Intel® Ostrich Bay CRB
CPU	Intel® Atom® Processor C3958 (16M Cache, 2.0 GHz) http://ark.intel.com/products/97927/Intel-Atom-Processor-C3958-16M-Cache-2_00-GHz Number of cores 16, Number of threads 16.
Memory	2x 16 GB DDR4 2400 MT/s ECC RDIMM
Operating System	RHEL 7.3
BIOS	HAVLCRB1.X64.0015.D15.1706022059
Linux kernel version	4.9.4
GCC version	4.8.5
Yasm version	1.3.0
Nasm version	2.11.08
OpenSSL version	1.0.2j
Zlib version	1.2.11
ISA-L version	2.19

Boot and BIOS settings

Item	Description	Setting
BIOS	CPU Power and Performance Policy	Performance
	CPU C-state	Disabled
	CPU P-state	Disabled
	SpeedStep	Disabled
	Turbo Boost	Disabled
	Memory Power Savings	Disabled



Function Unit testing

Item	Description
Test case	Unit function tests
Test parameters	Single core performance Cache cold
Command line	make –k perf

Test Result:

	ISA-L		OpenSSL	
ISA-L Function	**Cycle/Byte Performance**	**Single Core Throughput**	**Cycle/Byte Performance**	**Single Core Throughput**
Cryptographic Hashing				
Rolling Hash 64 bit	4.78	418 MB/s	-	-
Multihash SHA-1	3.43	613 MB/s	-	-
Multihash SHA-1 Murmur	3.52	568 MB/s	-	-
Multihash SHA-256	7.83	255 MB/s	-	-
Multibuffer SHA-1	1.64	1.1 GB/s	6.54	305 MB/s*
Multibuffer SHA-256	4.03	496 MB/s	19.53	102 MB/s*
Multibuffer SHA-512	11.47	174 MB/s	12.43	160 MB/s*
Multibuffer MD5	1.46	1.3 GB/s	4.94	405 MB/s*
Encryption				
AES-XTS 128	1.47	1.3 GB/s	1.49	1.3 GB/s
AES-XTS 256	1.92	1.0 GB/s	2.00	1.0 GB/s
AES-CBC 128 Decode	1.38	1.4 GB/s	1.40	1.3 GB/s
AES-CBC 192 Decode	1.68	1.1 GB/s	1.65	1.1 GB/s
AES-CBC 256 Decode	1.91	1.0 GB/s	1.90	1.0 GB/s
AES-GCM 128	2.07	968 MB/s	2.77	722 MB/s
AES-GCM 256	2.58	776 MB/s	3.27	612 MB/s
Data Protection				
PQ Gen (16+2)	0.33	5.8 GB/s	-	-
XOR Gen (16+1)	0.24	7.9 GB/s	-	-
Reed Solomon EC (10+4)	1.09	1.7 GB/s	-	-
Data Integrity				
CRC16 T10	0.67	2.9 GB/s	-	-
CRC32 IEEE (802.3)	0.66	2.9 GB/s	-	-
CRC32 iSCSI	0.45	4.3 GB/s	-	-
CRC32 GZIP Reflective	0.62	3.1 GB/s	-	-
CRC64 Normal	0.67	2.9 GB/s	-	-
CRC64 Reflective	0.62	3.1 GB/s	-	-

*Performance based on single buffer hashing

Compression testing

Item	Description
Test Case	Compression tests
Test parameters	Single core performance Iterations vary based on input size
Command line	Make other D='-D ZLIB_COMPARE'
	./igzip/igzip_stateless_file_perf
	./igzip/igzip_inflate_perf
Corpa	Silesia Corpus http://sun.aei.polsl.pl/~sdeor/index.php?page=silesia
	Calgary Corpus http://corpus.canterbury.ac.nz/descriptions/#calgary

Test Result:

	ISA-L			ZLIB		
ISA-L Function	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**ISA-L Function**	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**ISA-L Function**
Stateless Compress Level 0 Calgary Corpus	12.60	185 MB/s	40.52%	62.27	32 MB/s	39.24%
Stateless Compress Level 0 Silesia	11.17	178 MB/s	41.35%	59.07	33 MB/s	38.33%
Stateless Compress Level 1 Calgary Corpus	16.05	124 MB/s	37.51%	-	-	-
Stateless Compress Level 1 Silesia	14.23	140 MB/s	36.86%	-	-	-
Decompress "Inflate" Calgary Corpus	8.50	235 MB/s	40.52%	13.47	148 MB/s	39.24%
Decompress "Inflate" Silesia	7.62	262 MB/s	41.35%	12.71	157 MB/s	38.33%

Intel® Atom™ Processor C2750 (4M Cache, 2.40 GHz)

Hardware & Software Ingredients

Item	Description
Server Platform	Intel® Mohon Peak CRB
CPU	Intel® Atom™ Processor C2750 (4M Cache, 2.40 GHz) http://ark.intel.com/products/77987/Intel-Atom-Processor-C2750-4M-Cache-2_40-GHz Number of cores 8, Number of threads 8.
Memory	2x 8 GB DDR4 1600 MT/s ECC RDIMM
Operating System	RHEL 7.3
BIOS	EDVLCRB1.86B.0040.R00.1404141653
Linux kernel version	4.9.4
GCC version	4.8.5
Yasm version	1.3.0
Nasm version	2.11.08
OpenSSL version	1.0.2j
Zlib version	1.2.11
ISA-L version	2.19

Boot and BIOS settings

Item	Description	Setting
BIOS	CPU Power and Performance Policy	Performance
	CPU C-state	Disabled
	CPU P-state	Disabled
	SpeedStep	Disabled
	Turbo Boost	Disabled

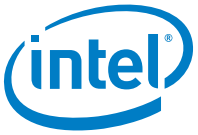
Function Unit testing

Item	Description
Test case	Unit function tests
Test parameters	Single core performance Cache cold
Command line	make –k perf

Test Result:

	ISA-L		OpenSSL	
ISA-L Function	**Cycle/Byte Performance**	**Single Core Throughput**	**Cycle/Byte Performance**	**Single Core Throughput**
Cryptographic Hashing				
Rolling Hash 64 bit	8.16	294 MB/s	-	-
Multihash SHA-1	6.47	370 MB/s	-	-
Multihash SHA-1 Murmur	6.50	369 MB/s	-	-
Multihash SHA-256	14.33	167 MB/s	-	-
Multibuffer SHA-1	6.36	377 MB/s	9.90	242 MB/s*
Multibuffer SHA-256	13.28	180 MB/s	27.97	85 MB/s*
Multibuffer SHA-512	21.03	114 MB/s	17.79	134 MB/s*
Multibuffer MD5	2.71	884 MB/s	6.26	383 MB/s*
Encryption				
AES-XTS 128	3.97	605 MB/s	4.70	510 MB/s
AES-XTS 256	5.34	449 MB/s	6.14	390 MB/s
AES-CBC 128 Decode	5.51	435 MB/s	4.28	560 MB/s
AES-CBC 192 Decode	5.52	435 MB/s	5.06	474 MB/s
AES-CBC 256 Decode	7.73	310 MB/s	5.86	409 MB/s
AES-GCM 128	7.12	337 MB/s	7.73	310 MB/s
AES-GCM 256	8.57	280 MB/s	9.19	261 MB/s
Data Protection				
PQ Gen (16+2)	0.40	5.9 GB/s	-	-
XOR Gen (16+1)	0.38	6.1 GB/s	-	-
Reed Solomon EC (10+4)	2.77	865 MB/s	-	-
Data Integrity				
CRC16 T10	1.65	1.4 GB/s	-	-
CRC32 IEEE (802.3)	1.65	1.4 GB/s	-	-
CRC32 iSCSI	0.75	3.1 GB/s	-	-
CRC32 GZIP Reflective	1.72	1.3 GB/s	-	-
CRC64 Normal	2.22	1.0 GB/s	-	-
CRC64 Reflective	1.72	1.3 GB/s	-	-

*Performance based on single buffer hashing



Compression testing

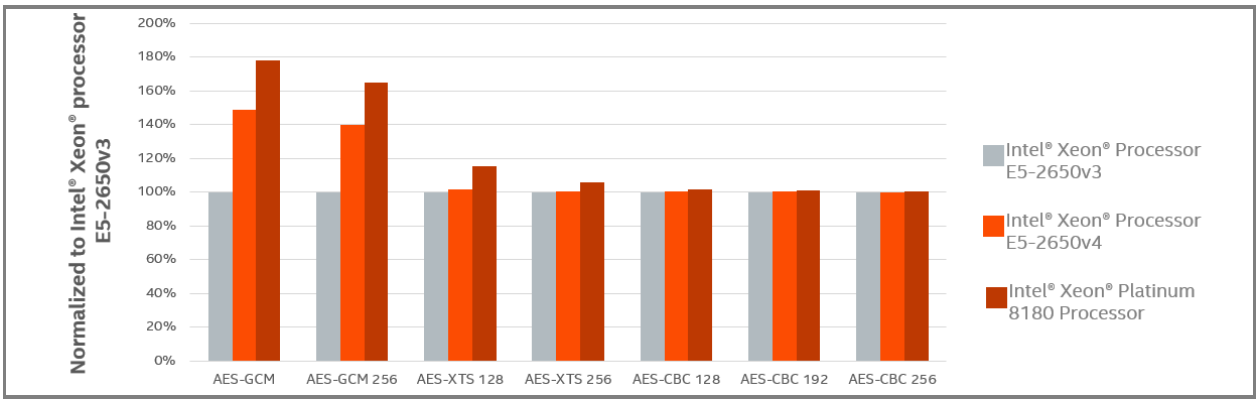
Item	Description
Test Case	Compression tests
Test parameters	Single core performance Iterations vary based on input size
Command line	Make other D='-D ZLIB_COMPARE'
	./igzip/igzip_stateless_file_perf
	./igzip/igzip_inflate_perf
Corpa	Silesia Corpus http://sun.aei.polsl.pl/~sdeor/index.php?page=silesia
	Calgary Corpus http://corpus.canterbury.ac.nz/descriptions/#calgary

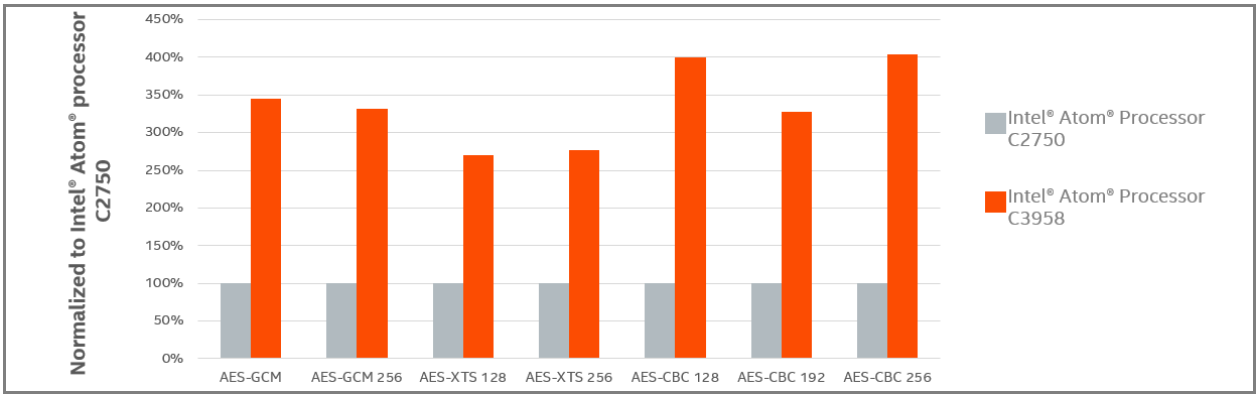
Test Result:

	ISA-L			ZLIB		
ISA-L Function	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**	**Cycle/Byte Weighted Average**	**Single Core Throughput**	**Compression Ratio**
Stateless Compress Level 0 Calgary Corpus	16.96	141 MB/s	40.52%	87.05	27 MB/s	39.24%
Stateless Compress Level 0 Silesia	15.07	159 MB/s	41.35%	70.89	33 MB/s	38.33%
Stateless Compress Level 1 Calgary Corpus	20.40	117 MB/s	37.51%	-	-	-
Stateless Compress Level 1 Silesia	18.28	131 MB/s	36.86%	-	-	-
Decompress "Inflate" Calgary Corpus	11.66	205 MB/s	40.52%	16.44	145 MB/s	39.24%
Decompress "Inflate" Silesia	10.43	230 MB/s	41.35%	16.00	149 MB/s	38.33%

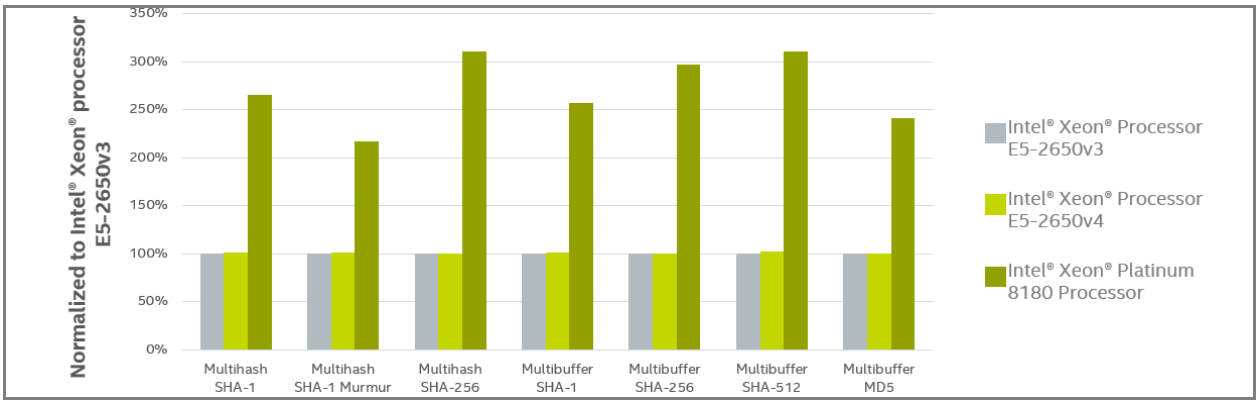
Intel® ISA-L Generational Performance Comparison

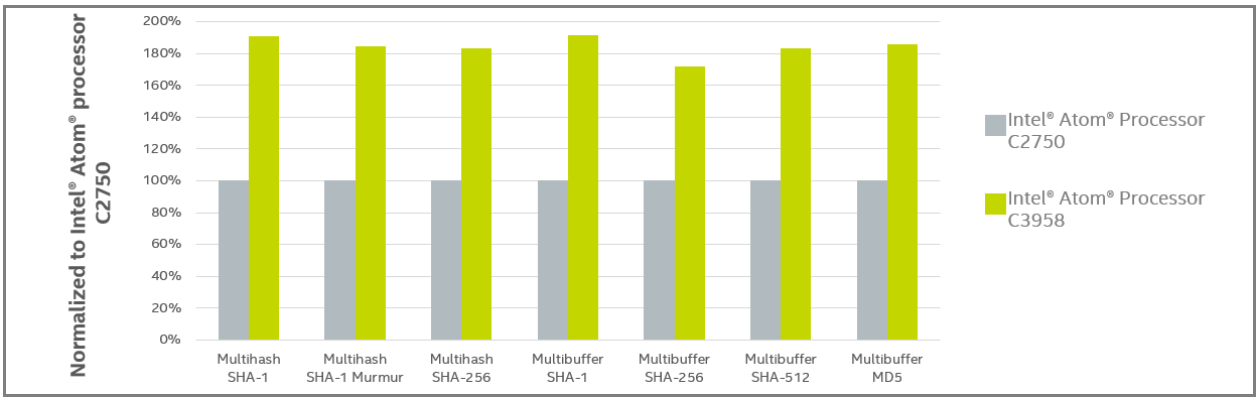
Encryption



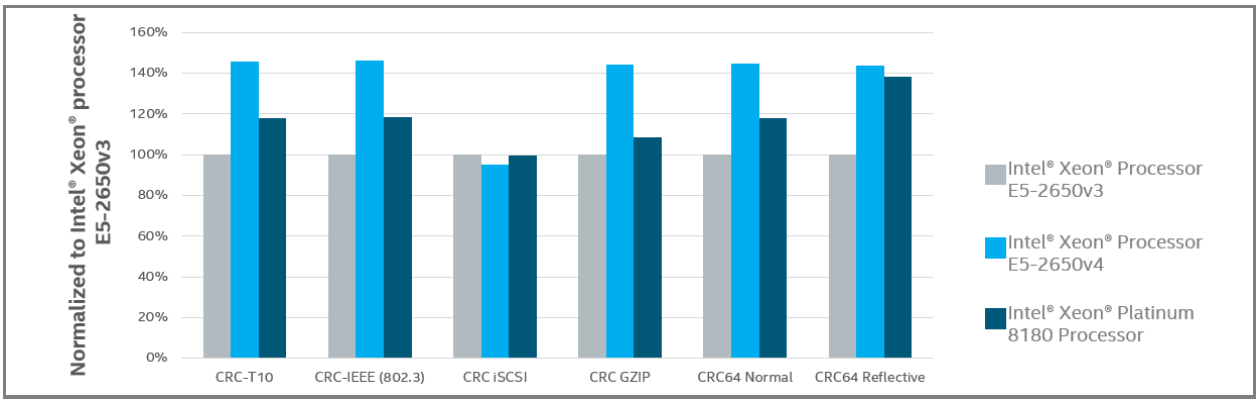


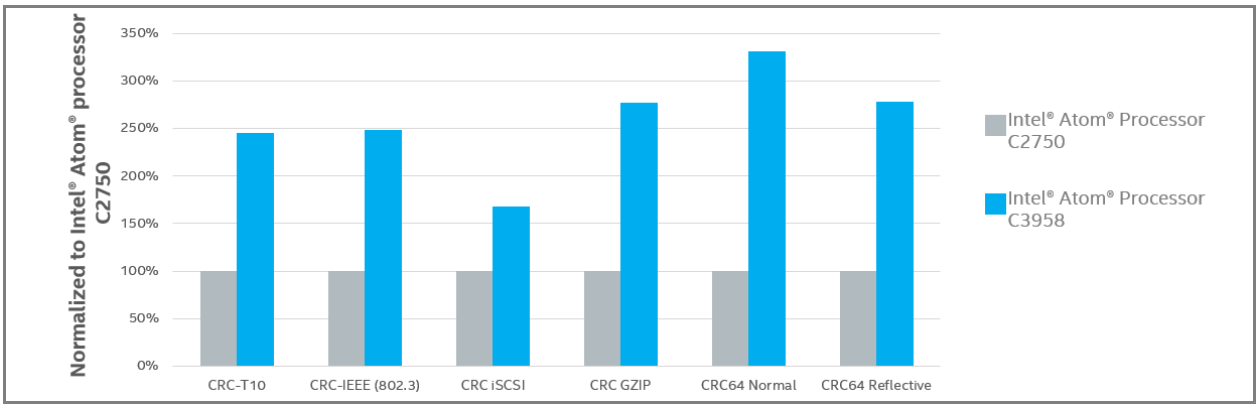
Cryptographic Hashing



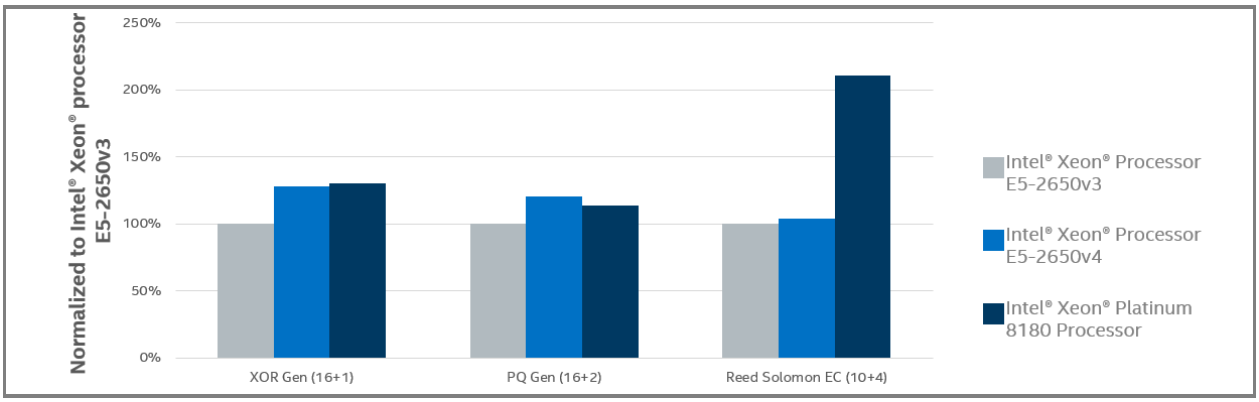


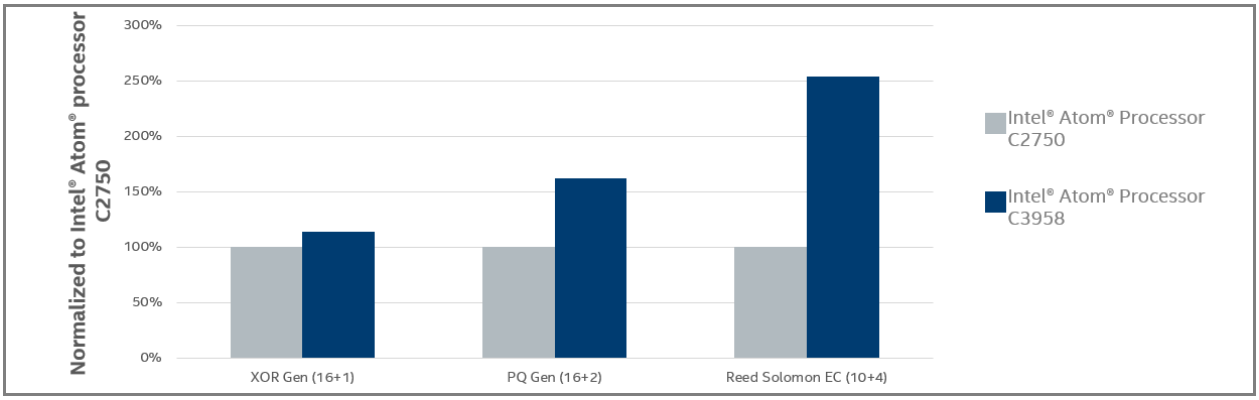
Data Integrity

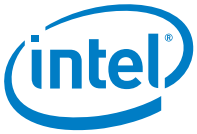




Data Protection







DISCLAIMERS

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.

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.

Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

For more information go to http://www.intel.com/performance

Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. **For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/**

§