Solution Brief

Intel® Crypto Acceleration
Intel® Xeon® Scalable Processors

Tapping into Cryptographic Acceleration

Enhance security and protect performance with Intel Crypto Acceleration instructions in 3rd Gen Intel Xeon Scalable processors.

Highlights

- Encryption is now pervasive in the data center, which creates performance overhead challenges for CPUs.
- Intel Crypto Acceleration instructions embedded in 3rd Gen Intel Xeon Scalable processors can dramatically increase the efficiency of cryptographic operations.
- Many open source and commercial software packages have been optimized to take advantage of Intel Crypto Acceleration.
- Developer tools and libraries developed by Intel enable you to support Intel Crypto Acceleration in your own software development.

In the past, cryptography was used in the data center mostly for specific purposes involving perimeter defense. Now, encryption is pervasive within data center networking, storage, and data-compression processes. This expansion of cryptography has led to an explosion in the number of encryption cycles that need to be performed by CPUs, which can create performance overhead, sometimes known as a "security tax." The negative impact on performance resulting from CPUs spending so many cycles on encryption tasks can cause a degradation of the end-user experience.

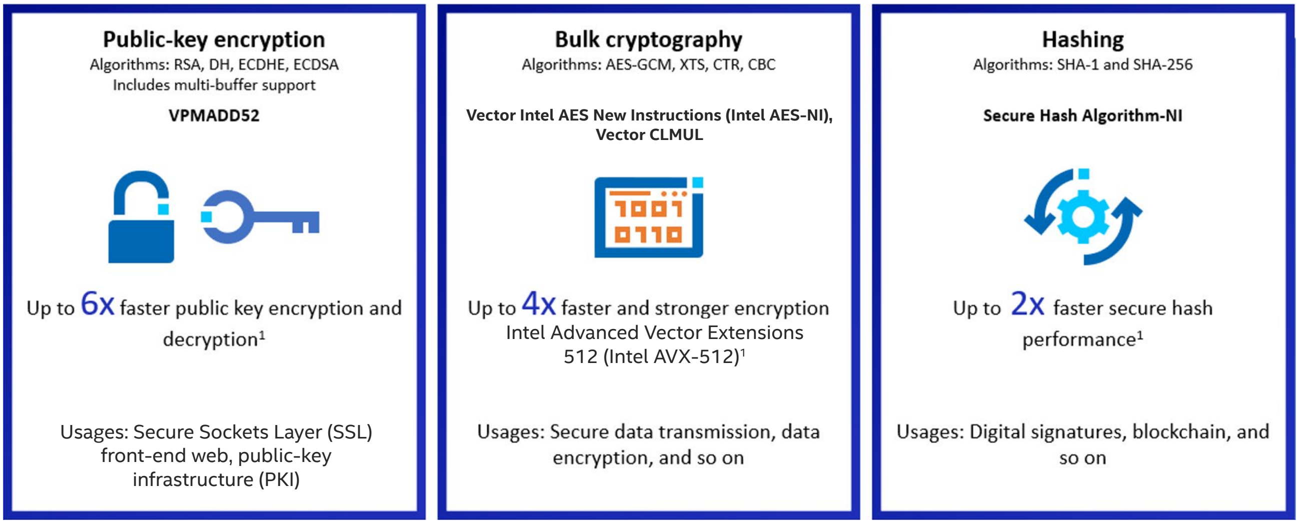
Data center architects and software developers face a choice if they want to avoid a degraded user experience (UX): limit the amount of encryption being performed—which could increase security risk and endanger data privacy—or find ways to accelerate the encryption process. The expensive solution is simply to add more processors and more cores to the data center; but there's a better way.

Instructions for cryptographic acceleration

Intel builds acceleration technologies into its processors that can significantly improve performance for particular kinds of operations, including cryptography. These are not discrete hardware accelerators that offload processing operations to alternative hardware, such as graphics processing units (GPUs) or field-programmable gate arrays (FPGAs). Rather, these specialized instruction sets are embedded directly into the CPU in the form of new CPU instructions that dramatically increase the efficiency of the underlying operations making up the security algorithms.

The Intel Crypto Acceleration instructions in 3rd Gen Intel Xeon Scalable processors enable high levels of cryptographic security, enhanced performance, and a more seamless UX. Impressive levels of acceleration can be achieved in three of the most common cryptographic scenarios, as detailed in Figure 1:[1]

- Up to 6x faster public-key encryption and decryption for uses such as Secure Sockets Layer (SSL) front end, web services, and proxies
- Up to 4x faster bulk cryptography for uses such as file, block, or streaming video encryption, when using Intel Advanced Vector Extensions 512 (Intel AVX-512)
- Up to 2x faster secure hash performance for uses such as digital signatures, authentication, and integrity checking using algorithms such as Secure Hash Algorithm 1 (SHA-1) and Secure Hash Algorithm 2 (SHA-2, also known as SHA-256), which is used by SSL



Public-key encryption
Algorithms: RSA, DH, ECDHE, ECDSA
Includes multi-buffer support

VPMADD52

Up to 6x faster public key encryption and decryption[1]

Usages: Secure Sockets Layer (SSL) front-end web, public-key infrastructure (PKI)

Bulk cryptography
Algorithms: AES-GCM, XTS, CTR, CBC

Vector Intel AES New Instructions (Intel AES-NI), Vector CLMUL

Up to 4x faster and stronger encryption Intel Advanced Vector Extensions 512 (Intel AVX-512)[1]

Usages: Secure data transmission, data encryption, and so on

Hashing
Algorithms: SHA-1 and SHA-256

Secure Hash Algorithm-NI

Up to 2x faster secure hash performance[1]

Usages: Digital signatures, blockchain, and so on

Figure 1. Accelerating cryptographic instructions

New cryptography instructions

Fifteen new cryptography instructions were added to 3rd Gen Intel Xeon Scalable processors, including:[2]

- VPMADD52 added two new instructions, also known as “multiply and accumulate.” This fused multiply add operation can execute ((A*B)+C) for 52-bit precision integer values in a single instruction. This is critical for public key cryptography, which makes use of big-number arithmetic. VMPADD52 is based on the Intel AVX-512 integer FMA engine(s); up to two per Intel Xeon processor.
- Vector AES uses AES, which is the de facto cipher for strong and efficient bulk encryption. These six new instructions, often referred to as VAES, support vectorized AES cipher implementations, processing up to four 128-bit blocks per instruction.
- Vector carry-less multiply is a key aspect of the computation need for Galois hash message digestion commonly used for message authentication. When combined with AES, it creates AES-GCM (an AES mode that allows parallel processing), which is likely the most widely deployed bulk-encryption cipher.
- Galois Field New Instructions (GFNI) are three new instructions that are useful not just for encryption algorithms, but also in error-correction algorithms and bit matrix multiplication.
- SHA-NI is a set of three new instructions that offer hardware acceleration of Secure Hash Algorithm 2 (also known as SHA-256) message digests. SHA-256 is used in SSL, IPsec, TLS, and for message integrity.

How to get the benefits of Intel Crypto Acceleration

Software needs to be optimized to take advantage of the Intel Crypto Acceleration instructions in 3rd Gen Intel Xeon Scalable processors. The good news is that many software packages have already been optimized, so all you need to do is make sure you are using an optimized version of your software, which might mean updating to the latest version of that software, its libraries, or the underlying run-time environment.

There are several different paths to getting the benefits of Intel Crypto Acceleration:

- Use commercial software optimized by the ISV. Companies like Microsoft, SAP, VMware, and Oracle have optimized their products for Intel architecture, including Intel Crypto Acceleration. Check with your ISV to determine if you are using an optimized software version, and if not, how you can move to one.
- Use open source software optimized by Intel. Numerous Linux distributions have been optimized for Intel Crypto Acceleration, as have applications including NGINX, WordPress, the Java OpenJDK runtime, and the OpenSSL library—which results in significantly higher OpenSSL performance by 3rd Gen Intel Xeon Scalable processors than the competition.[3] Search engines such as Elasticsearch have also been crypto-optimized, and the list continues to grow.
- Use developer tools and libraries developed by Intel to support Intel Crypto Acceleration in your own software. Use the Crypto API Toolkit to run cryptographic operations more securely inside an Intel Software Guard Extensions (Intel SGX) enclave. The Intel Integrated Performance Primitives (Intel IPP) cryptography library automatically takes advantage of available CPU capabilities. Java applications benefit from Intel crypto optimizations already integrated into the latest Java Development Kit (JDK) release.

Seeing success with Intel Crypto Acceleration

Companies are seeing real benefits from Intel Crypto Acceleration, available in 3rd Gen Intel Xeon Scalable processors. With the higher core performance and the new crypto instructions, communications service providers (CoSPs), for example, can achieve up to 72 percent better cable modem termination system (CMTS) platform performance.[4] For another example, Kingsoft Cloud, a top cloud provider in China offering content-delivery network (CDN) services that distribute user content to the edge to avoid network congestion, was able to serve 2.3x more HTTPS requests after implementing enhanced Intel Crypto Acceleration.[5] Read about the Kingsoft Cloud story at intel.com/content/www/us/en/customer-spotlight/stories/kingsoft-cloud-cdn-customer-story.html.

Learn more and get started

Reduce the compute cycles you spend on cryptography processing. Increase developer agility, gain DevOps efficiency, and improve the UX in the enterprise by taking advantage of the built-in cryptographic acceleration capabilities of 3rd Gen Intel Xeon Scalable processors.

Learn more by reading the "Cryptography Processing with 3rd Gen Intel Xeon Scalable Processors" white paper: intel.com/content/www/us/en/architecture-and-technology/crypto-acceleration-in-xeon-scalable-processors-wp.html

Additional resources:

- WordPress and NGINX optimized images: https://community.intel.com/t5/Blogs/Tech-Innovation/Cloud/Intel-Collaborates-with-Bitnami-to-Deliver-Optimized-Workload/post/1360993
- Intel Crypto API Toolkit: https://github.com/intel/crypto-api-toolkit
- The Intel IPP cryptography library: intel.com/content/www/us/en/develop/documentation/ipp-crypto-for-oneapi-dev-guide/top/crypto-introduction.html

[1] Performance varies by use, configuration and other factors. For workloads and configurations visit intel.com/performanceindex. Results may vary.

[2] For details, see Intel. "Cryptography Processing with 3rd Gen Intel Xeon Scalable Processors." May 2021. intel.com/content/dam/www/central-libraries/us/en/documents/cryptography-processing-with-3rd-gen-intel-xeon-scalable-processors-19-may-2021.pdf. And Intel. "Galois Field New Instructions (GFNI)." December 2021. https://networkbuilders.intel.com/solutionslibrary/galois-field-new-instructions-gfni-technology-guide.

[3] Up to 3.20x higher OpenSSL RSA signature 2048 performance with 3rd Gen Intel Xeon Scalable processor versus AMD Milan: See (40) at intel.com/3gen-xeon-config. Up to 2.03x higher OpenSSL ECDHE x25519 performance with 3rd Gen Intel Xeon Scalable processor versus AMD Milan: See (40) at intel.com/3gen-xeon-config.

[4] See claims 91 and 92 at: Intel. "Performance Index – 3rd Generation Intel Xeon Scalable Processors." https://edc.intel.com/content/www/us/en/products/performance/benchmarks/3rd-generation-intel-xeon-scalable-processors/?r=1525214932&r=730476595.

[5] Intel. "Kingsoft Cloud Accelerates Digital Transformation." intel.com/content/www/us/en/customer-spotlight/stories/kingsoft-cloud-storage-customer-story.html.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for additional details.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Printed in USA 0622/MG/PRW/PDF Please Recycle 351488-001US