

SUPERMICRO'S GRANDTWIN[™] EXCELS AT OPENSSL FOR CRYPTOGRAPHY WORKLOADS

Supermicro GrandTwin with Intel[®] QuickAssist Technology Demonstrates Tremendous Performance Increase for Cryptography Algorithms

TABLE OF CONTENTS

Executive Summary	1
What is OpenSSL?	2
What is Intel [®] QuickAssist Technology?	2
Testing Environment	2
Test Results:	3
Raw Test Results	4
Significance of Results	4
Summary	5



Supermicro GrandTwin™

Executive Summary

Supermicro's GrandTwin servers, the latest entry in the hyperconverged product line, provide a modular system architecture in a hyper-converged platform. These servers enable companies to achieve

high scalability and speed using the latest CPU, memory, and I/O technologies. In addition, it provides companies with the performance they need and the flexibility to adapt to the requirements of any application. To demonstrate the exceptional capabilities of GrandTwin for cryptographic algorithms, Supermicro and Intel conducted an OpenSSL benchmark test combined with Intel® QuickAssist Technology (Intel® QAT). This test showed remarkable results, demonstrating significant improvements of up to 33.23 times increase in performance in cryptographic algorithms when Intel® QAT was enabled. This feature highlights GrandTwin as a high-performance, cost-effective solution for customers seeking to optimize their computing power while minimizing their footprint. Additionally, the 4th Gen Intel Xeon Scalable processors will feature a built-in Intel® QAT accelerator that is expected to outperform servers based on the 3rd Gen Intel Xeon Scalable processors, and Supermicro will conduct a comparative analysis in the future to provide further insights.

The Supermicro GrandTwin provides a modular design that can be easily configured to provide complete flexibility within a system. This feature allows the system to be modified to the changing needs of the application and business. With cold aisle serviceability and easy front-node access, GrandTwin offers four hot-swappable nodes in a compact 2U form factor with up to 60 cores in a uniprocessor platform, up to 4TB of memory, and up to 6 NVMe/SATA drives per node. Each node can be configured

with an AIOM (OCP 3.0) card and different types of I/O modules to give customers the flexibility to customize the system to a specific network requirement.

This system is optimized for virtualization, cloud, hosting, content delivery, hyper-scale/hyper-converged, and other generalpurpose computing workloads. The latest Supermicro X13 GrandTwin has been enhanced with the latest 4th Gen Intel[®] Xeon Scalable processor, enabling even faster processing speeds that can be optimized for a wide range of workloads. With its builtin acceleration capabilities, this new processor offers an improved performance that can help boost application performance, productivity, and efficiency across various applications.

What is OpenSSL?

OpenSSL is an open-source software library that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols and provides a full-length general-purpose cryptography library. Therefore, anyone interested in securing the communication between clients and servers may benefit from using OpenSSL to benchmark performance.

What is Intel[®] QuickAssist Technology?

Intel[®] QuickAssist Technology (Intel[®] QAT) is an acceleration engine that significantly increases the performance and efficiency of standard platform solutions in the cloud, networking, big data, and storage by providing a framework for accelerators supporting software and hardware offload of popular cryptography, hash public key and compression/decompression algorithms. As a result, applications utilizing Intel[®] QAT will see significantly reduced CPU utilization and greatly increased performance for encryption, secure client tunnels, and/or secure storage compression.

Intel[®] Quick Assist Technology has been expanded to provide software-based acceleration of cryptographic operations through instructions in the Intel[®] Advanced Vector Extensions 512 (Intel[®] AVX-512) family. This software-based acceleration has been incorporated into the Intel[®] QAT Engine for OpenSSL. This dynamically loadable module uses the OpenSSL framework, allowing administrators to add this capability to OpenSSL without having to rebuild or replace their existing OpenSSL libraries. When combined, Intel[®] QuickAssist Technology and OpenSSL work together to provide fast and more secure encryption and decryption performance.

Supermicro and Intel ran OpenSSL Speed performance testing on a Supermicro X12 GrandTwin system showing performance gains when Intel[®] QuickAssist Technology software engine is enabled. These results demonstrate that organizations can benefit from increased performance and enhanced security for their encryption and decryption operations when Intel's technology is used on a highly versatile Supermicro platform.

Testing Environment

In the Supermicro's test lab, engineers ran an OpenSSL Speed test on the Supermicro <u>SYS-210GT-HNTF</u> GrandTwin system. The platform used an Intel[®] Xeon Scalable 6312U processor running at 2.4 GHz, 512GB DDR4 memory, 480GB SSD, and Ubuntu 20.04 LTS operating system. In addition, both Hyper-Threading and Turbo Boost were enabled.

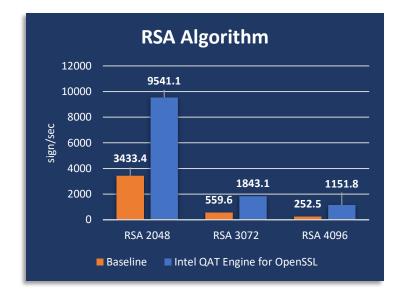
System	SuperMicro® SYS-210GT-HNTF (BMC: 1.00.02; BIOS: 1.04a)					
CPU	1x Intel® QXRW/M1 ICX 6312U 24C 2.4G 36MB FC-LGA16A 185W					
CPU FEATURES	Intel® Hyper-Threading Technology enabled					
CPU FEATURES	Intel® Turbo Boost Technology 2.0 enabled					
Memory	512 GB (16x 32GB) DDR4 Registered SDRAM 3200 MT/s					
Storage	Micron 7450 PRO 480GB NVMe PCIe 4.0 M.2 22x80mm					
OS	Ubuntu 20.04 LTS					

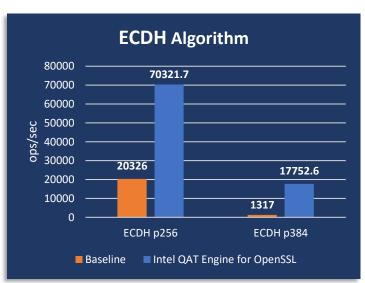
Test Results:

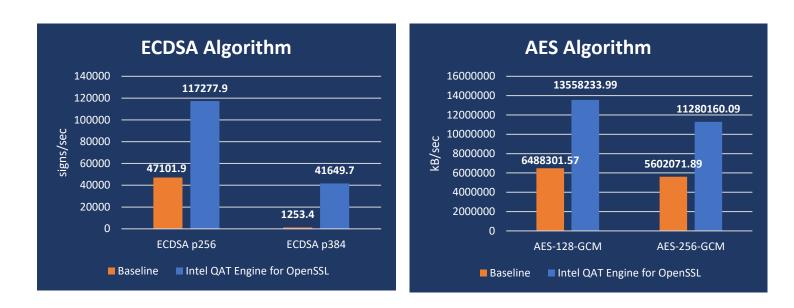
Supermicro achieved significant performance gains in the tests by enabling the Intel[®] QuickAssist Technology engine. Improvements up to 33.23x were observed compared to our baseline across all the tests.

The most substantial performance gains were observed in more secure algorithms, which tend to be more compute intensive. The increased performance of these algorithms over less secure ones can be quite significant. For example, our baseline, non-QAT test for ECDSA p384 (384 bit) achieved 1,253.4 signs/sec. However, when we enabled the Intel® QAT software engine, the performance increased drastically, achieving 41,649.7 signs/sec, which is 33.23x more than the baseline. Similarly, ECDH p384 baseline achieved 1,317 ops/sec, then 17,752.6 ops/sec with Intel® QAT software engine enabled, a 13.48x performance improvement over the baseline test.

Overall, the Intel[®] Quick Assist Technology is highly effective in handling cryptographic workloads and delivering impressive performance gains, as summarized in the plots below:







Raw Test Results

Algorithm	Baseline	Intel QAT Engine for OpenSSL	Measure	Speedup
RSA 2048	3433.4	9541.1	signs/sec	2.78
RSA 3072	559.6	1843.1	signs/sec	3.29
RSA 4096	252.5	1151.8	signs/sec	4.56
ECDH p256	20326	70321.7	ops/sec	3.46
ECDH p384	1317	17752.6	ops/sec	13.48
ECDSA p256	47101.9	117277.9	signs/sec	2.49
ECDSA p384	1253.4	41649.7	signs/sec	33.23
AES-128-GCM	6488301.57	13558233.99	kB/sec	2.09
AES-256-GCM	5602071.89	11280160.09	kB/sec	2.01

Significance of Results

OpenSSL is an open-source and widely used cryptography library that provides cryptographic functions for various applications such as web servers, VPNs, and software encryption. Getting good results for OpenSSL and then combining OpenSSL with Intel[®] QAT for even better results is critical to ensure the reliability and security of these applications in Supermicro GrandTwin. Cryptographic libraries like OpenSSL are used by millions of websites worldwide, and a good performance can significantly impact the user experience. Therefore, these benchmark results assure users and industries that their data is protected solidly and efficiently.

Intel[®] Quick Assist Technology is an accelerator engine that improves the performance of cryptographic algorithms. Enabling this accelerator to OpenSSL and improving the benchmark results give us insights into the speed and efficiency these cryptographic algorithms can reach in a real-world application with a reliable GrandTwin system. For example, Intel[®] QAT can help improve the performance of digital signature generation and verification, which is widely used in the financial industry.

As the market evolves with new technologies and the volume of data and transactions grows, security and data protection must keep up with the increasing demand. Security and data protection are essential for everyone, especially industries that need to protect sensitive data and information from the outside world. For Supermicro, providing the latest, most secure environments is very important.

Significant benchmark results can be important for various markets to show cryptographic functions' reliability, security, and performance. Some of these markets include:

1. Finance: Cryptography is critical for this market to secure financial transactions and sensitive data such as bank accounts, credit card numbers, and personal information.

- 2. Healthcare: This market relies on cryptography to protect patient's personal information and records.
- 3. Government: This market uses cryptography to secure classified data and other intelligence gatherings.

4. E-commerce: The increasing number of users makes cryptography critical for this market to secure transactions, credit card numbers, and other personal information from users.

Summary

Security is an extremely important consideration in today's world. Intel[®] Quick Assist Technology can significantly increase the number of encrypted connections in choosing more secure cryptography algorithms. When used with the Supermicro GrandTwin, significant performance gains are achieved, resulting in decreased processing time with no additional cost to the end user. Our reliable GrandTwin platform provides an efficient foundation for real-world applications that demand high-speed cryptographic functions. When combined with OpenSSL and Intel[®] QAT, the results are remarkable. We have achieved significant improvements in the performance of widely used cryptographic algorithms.

Supermicro's GrandTwin, combined with Intel[®] Quick Assist Technology, provides the efficiency that applications heavily rely on, even as user demands and data encryption and decryption keep increasing. The resulting boost in speed and security means businesses and organizations can confidently manage large-scale data processing and financial transactions, knowing that reliable cryptographic solutions protect their data. Users of both 3rd and 4th Gen Intel[®] Xeon[®] Scalable processors can take advantage of this power. The newest improvements and higher performance gains are expected on the X13 GrandTwin platforms featuring 4th Gen Intel[®] Xeon[®] Scalable processors with Intel[®] QAT built-in acceleration. This combination provides a powerful, low-cost solution to the most secure cryptography environments. For More Information:

Supermicro X13 GrandTwin – <u>https://www.supermicro.com/en/products/grandtwin</u>

Intel[®] Quick Assist Technology - <u>https://www.intel.com/content/www/us/en/architecture-and-technology/intel-quick-assist-technology-overview.html</u>