Accelerate Post-Quantum Cryptography with Intel Crypto Technologies

Intel supports the transition to Post-Quantum Cryptography (PQC) through a range of quantum resilient platforms that deliver best-in-class performance on PQC algorithms.

Authors

Divya Pendyala

Stephen Doyle

Sankar Chokkalingam

Intel Corporation

Introduction

In a world driven by information and connectivity, safeguarding data and ensuring secure communication are paramount. Cryptography provides the means to protect sensitive information, preserve privacy, and ensure authenticity in today's digital era where information can be easily intercepted, manipulated or stolen. Recent advancements in quantum computing have introduced the possibility of a cryptographically relevant quantum computer (CRQC) becoming a reality. Such a development poses a significant threat to traditional encryption methods, which rely on mathematical problems that are difficult for conventional computers to solve but could be efficiently tackled by quantum computers.

As cyber threats evolve, the field of cryptography is advancing to address these emerging quantum challenges. This new development of cryptographic algorithms that are secure against quantum computers is referred to as post-quantum cryptography (PQC).

Rise of Quantum Computing

The security of our modern digital infrastructure is largely built upon public-key cryptographic algorithms such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). These systems rely on the computational difficulty of certain mathematical problems for conventional computers. For instance, the security of RSA is rooted in the immense difficulty of factoring the product of two large prime numbers. For conventional computers, solving these problems would take an infeasible amount of time, effectively securing the encrypted data. However, the advent of quantum computing poses a fundamental threat to this security paradigm. Unlike conventional computers that use bits to represent either a 0 or a 1, quantum computers use qubits. Due to the principles of quantum mechanics, such as superposition and entanglement, qubits can represent both 0 and 1 simultaneously, allowing quantum computers to perform a vast number of calculations in parallel. This capability will enable a sufficiently powerful quantum computer, using algorithms like Shor's algorithm, to quickly solve the underlying mathematical problems of RSA and ECC, rendering them insecure. While quantum computers are not generally available as of this writing, the expected capabilities of the CRQC create an immediate threat known as "Harvest Now, Decrypt Later," where adversaries can collect and store currently encrypted data with the intention of decrypting it once a sufficiently powerful quantum computer is available. This impending vulnerability has catalyzed the field of Post-Quantum Cryptography (PQC), which aims to develop new cryptographic standards that are secure against attacks from both conventional and quantum computers.

Quantum computers excel at processing large datasets, optimizing complex problems, simulating quantum systems, and pattern recognition that can potentially

Table of Contents

revolutionize tasks in fields like cryptography, medicine, finance, AI/ML and more. Unlike conventional computers that follow a sequential execution model, they can perform numerous calculations in parallel. Their unprecedented speed allows them to easily break today's encryption methods—such as RSA, ECC, and Digital Signature Algorithm (DSA), that rely on certain mathematical problems like integer factorization and discrete algorithms. Quantum computers rely on Shor's algorithm that can factor large numbers exponentially faster.

Since traditional public-key cryptography remains primarily reliant on RSA and ECC, proactive changes are needed to safeguard data before quantum computers render these legacy methods vulnerable. The need to adopt quantum-safe encryption is an immediate mandate, ensuring that sensitive information remains secure even as technology advances.

Post-Quantum Cryptography Standards

The National Institute of Standards and Technology (NIST) initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.

In August 2024, NIST standardized a new set of cryptographic “primitives” that are secure against quantum computers. These well-vetted and practical post-quantum algorithms use fundamentally different mathematical techniques than the related math problems underlying RSA and ECC. They're equipped to protect sensitive data in a quantum-threatened environment.

These PQC algorithms include:

1. ML-KEM (CRYSTALS-Kyber) – Module-Lattice-based Key Exchange Mechanism (KEM) for public key encryption and key establishment, mainly for accessing secure websites.
2. ML-DSA (CRYSTALS-Dilithium) – Module-Lattice-based Digital Signature scheme for generating and verifying digital signatures.
3. SLH-DSA (SPHINCS+) – Stateless Hash-based Digital Signature Algorithm based on SPHINCS+
4. FALCON (FN-DSA) – Lattice-based Digital Signature Algorithm, known for its speed and small signature size, selected for standardization.

NIST recommends using ML-DSA as the primary algorithm and FALCON for smaller signatures.

The Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) lists quantum-resistant algorithms, based on NIST standards, approved for National Security Systems (NSS) use. These algorithms include:

1. ML-KEM - Key Exchange
2. ML-DSA - Digital Signature
3. SHA - Hashing
4. AES (256-bit keys) - Symmetric encryption
5. LMS/XMSS - Firmware and software signing

CNSA2.0 recommends beginning the transition to quantum-safe cryptography for software and firmware signing on new equipment immediately and completing the transition for other equipment such as web browsers, servers, operating systems (OS), traditional networking and niche equipment by 2033.

Transitioning to post-quantum cryptography can be a tedious process. Intel technologies are aimed to simplify PQC transition process while providing Intel crypto technologies to accelerate the performance of quantum safe cryptography.

Intel's Post-Quantum Cryptography Framework

Following NIST standards and CNSA2.0 guidelines closely, Intel developed PQC acceleration software based on Open Quantum-Safe (OQS) liboqs library, optimized to perform with Intel Crypto technologies – such as Intel® QuickAssist Technology (Intel® QAT), Intel® Advanced Vector Extensions, and Intel® Crypto Acceleration, that accelerate PQC algorithms.

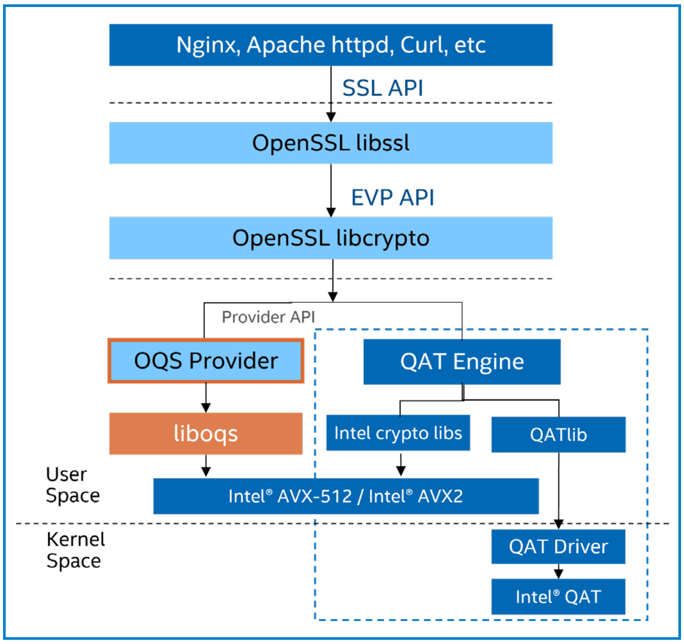


Figure 1. Intel's Post-Quantum Cryptography Software

Open Quantum Safe (OQS) Library

The Open Quantum Safe (OQS) project, part of the Linux Foundation's Post-Quantum Cryptography Alliance, is an open-source project that aims to support the development and prototyping of quantum-resistant cryptography. It consists of two main lines of work:

1. liboqs - an open-source C library for quantum-resistant cryptographic algorithms and
2. oqs_provider - a provider for OpenSSL3.x to enable quantum-safe cryptography.

Intel Crypto Technologies

Intel offers a variety of cryptographic solutions that include both hardware and software solutions. These can be used in conjunction or individually based on the chosen platform's features and performance needs.

- Intel QAT is a hardware accelerator designed to enhance performance by offloading cryptographic and compression tasks from the CPU cores. Intel QAT supports various cryptographic algorithms, accelerating tasks like encryption, decryption, and key exchange, which are crucial for securing data in transit and at rest.

- Intel Crypto Acceleration is a software-based acceleration of cryptographic workloads using Intel crypto libraries, namely Intel® Cryptography Primitives Library and Intel® Multi-Buffer Crypto for IPsec (Intel IPsec_mb). It utilizes Intel® Advanced Vector Extensions 512 (Intel® AVX-512) that provide vector processing capabilities to accelerate cryptographic performance.
- Intel® QAT Engine for OpenSSL* is a software package that supports acceleration via hardware and software options, based on vectorized instructions. The Intel QAT Engine for OpenSSL supports the ability to accelerate the standard OpenSSL using either the hardware accelerator path (Intel QAT) or the software path (Intel Crypto Acceleration).
- Intel Advanced Vector Extensions 512 (Intel AVX-512) is an advanced set of instructions in CPU cores, introduced by Intel, that enhances the performance of compute-intensive and data-centric workloads.
- Intel® Cryptography Primitives Library is a set of cryptographic building blocks, highly optimized for various Intel® CPUs. This library supports acceleration of cryptographic algorithms like RSA, ECDH, and ECDSA.
- Intel® Multi-Buffer Crypto (Intel® IPsec_mb) library for IPsec provides software acceleration primarily targeting encrypted packet processing applications. It simplifies the implementation of multi-buffer processing for authentication and encryption algorithms.

Intel PQC Software Implementation

Intel developed PQC software leveraging existing Intel crypto technologies to accelerate post-quantum cryptographic algorithms, both hybrid and full. Hybrid PQC algorithms combine traditional and PQC algorithms, while full PQC algorithms are solely the new quantum-resistant algorithms.

Intel's PQC software encompasses open-source OQS components: liboqs and oqs_provider that enable quantum-safe cryptography and Intel QAT_engine to accelerate cryptographic operations. Both providers – oqs_provider and QAT_engine are registered into OpenSSL 3.x for key establishment in TLS 1.3 via the OpenSSL 3.x provider interface. While QAT_engine accelerates the traditional portion of hybrid PQC algorithms using underlying Intel QAT and/or Intel crypto software, oqs_provider accelerates the new quantum-resistant algorithms.

Furthermore, optimizations based on Intel AVX-512 that accelerate the performance of full PQC algorithms have been contributed into liboqs v0.14.0 and are available for adoption.

Benchmarks and Key Performance Indicators (KPIs)

TLS Connections-Per-Second (CPS)

Clients send HTTPS requests without requesting data. TLS 1.3 key exchange and certificate authentication are exercised with no data transfer.

Bulk Throughput (Gbps)

Clients send HTTPS connections with data transfer of 10MB files. NGINX throughput is measured under a specific load from all clients.

Test Setup

This test is executed on two generations of Intel® Xeon® SoCs to analyze post-quantum cryptographic algorithm performance, transition costs and gen-to-gen improvements. Intel's latest Intel® Xeon® 6 SoC – Intel® Xeon® 6563P-B processor and prior generation SoC - Intel® Xeon® D-2798NT processor are used.

A Device Under Test (DUT) with Intel Xeon 6563P-B SoC is connected to a Cisco Nexus C3232C router with a total possible aggregated link bandwidth of 600 GbE (6 x 100 GbE links), along with six client machines capable of sending 2000 requests using OpenSSL s_time for 300 seconds over a single https connection. Refer to Figure 2. Multiple clients are used to send requests to the server simultaneously. Each client establishes a secure connection with the server and exits gracefully, and sends new requests again to establish a secure connection. The total number of connections per second from each client is summed up and displayed on the server.

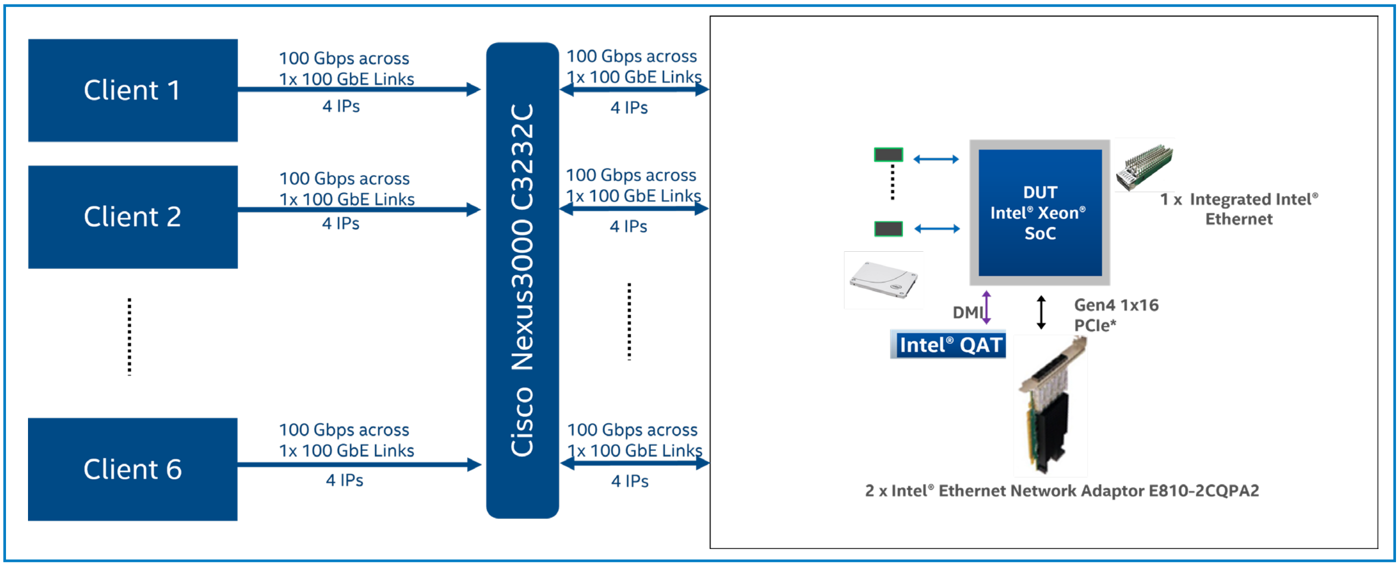

Client 1
100 Gbps across 1x 100 GbE Links
4 IPs
Client 2
100 Gbps across 1x 100 GbE Links
4 IPs
Client 6
100 Gbps across 1x 100 GbE Links
4 IPs
Cisco Nexus3000 C3232C
100 Gbps across 1x 100 GbE Links
4 IPs
100 Gbps across 1x 100 GbE Links
4 IPs
100 Gbps across 1x 100 GbE Links
4 IPs
DUT Intel® Xeon® SoC
1 x Integrated Intel® Ethernet
DMI
Gen4 1x16 PCIe*
Intel® QAT
2 x Intel® Ethernet Network Adaptor E810-2CQPA2

Figure 2. Hardware configuration

The TLS handshake test is performed using three different software variants (as shown in Figure 3) to uncover the performance gains with Intel crypto technologies.

1. Over native TLS stack with liboqs
2. Offloading to Intel crypto libraries in combination with liboqs
3. Offloading to Intel QAT in combination with liboqs

While testing NGINX bulk throughput, multiple clients send TLS connection requests concurrently and for each connection, the clients request 10 MB files to be transmitted using 4 IP addresses over a https connection. As the NGINX server completes one request, new requests are sent. The total data transfer that NGINX DUT can process is measured as throughput in Gbps.

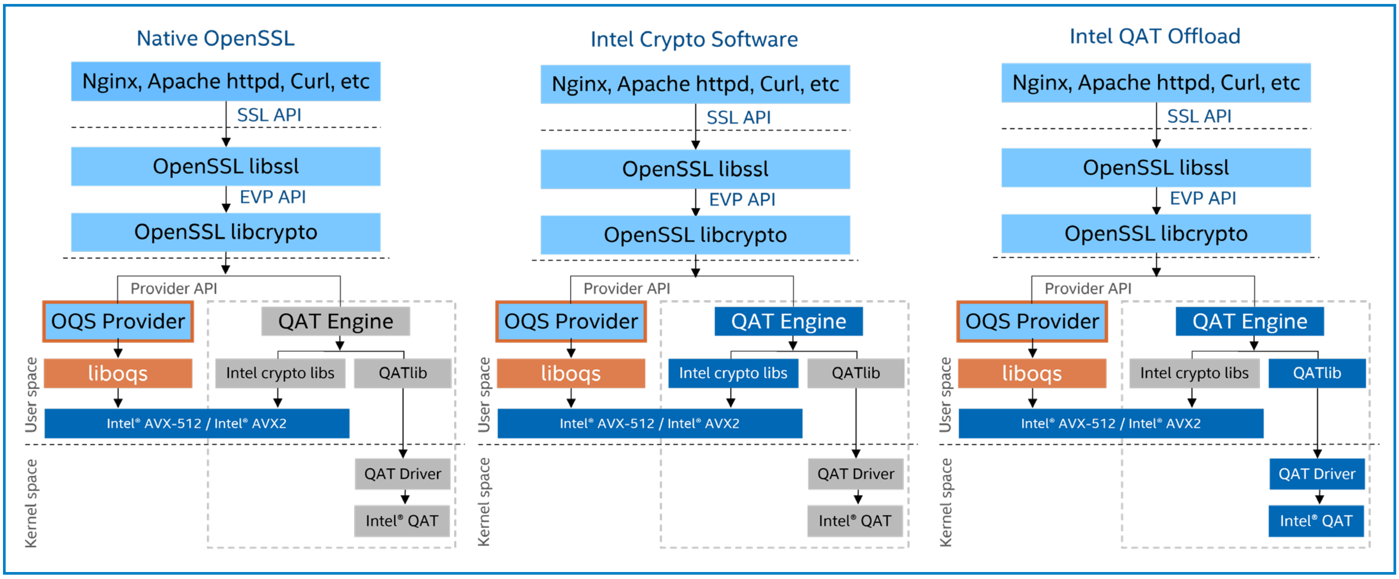
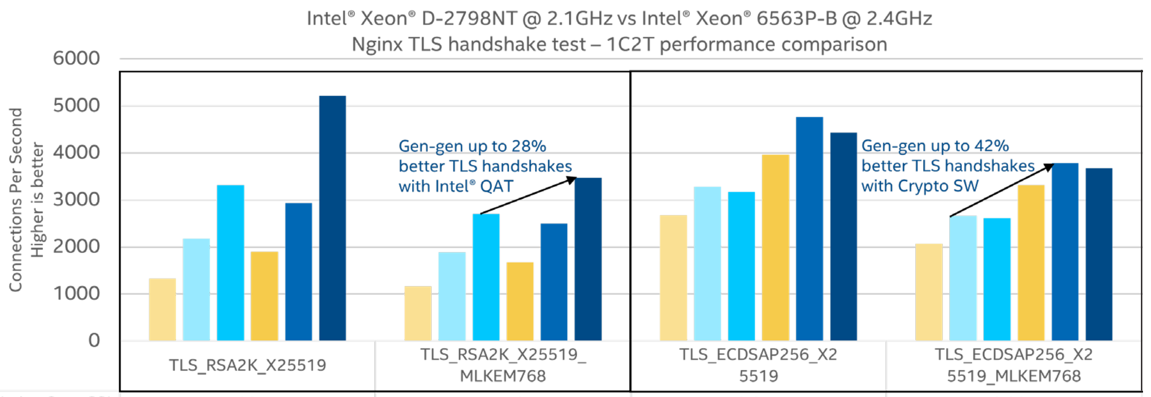


Figure 3. Software variants to measure NGINX TLS PQC handshakes

Performance Results

Test results in Figure 4 show NGINX webserver TLS 1.3 handshakes measured in Connections-Per-Second (CPS) with traditional and hybrid PQC key exchange. Hybrid key exchange performance on the latest Intel Xeon 6563P-B SoC on single core is up to 28% better with integrated Intel QAT for RSA algorithm and up to 42% better with Intel's crypto software for ECDSA than that of the previous generation SoC.

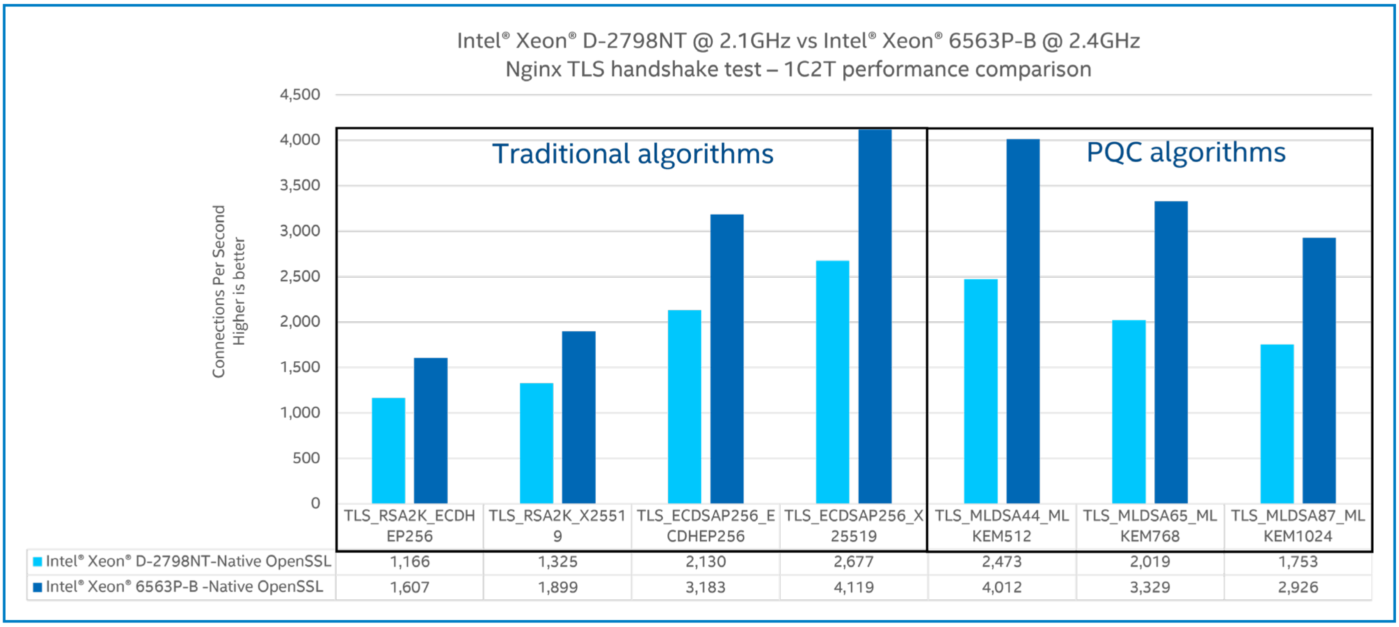


	TLS_RSA2K_X25519	TLS_RSA2K_X25519_MLKEM768	TLS_ECDSAP256_X25519	TLS_ECDSAP256_X25519_MLKEM768
Intel® Xeon® D-2798NT-Native OpenSSL	1325	1,159	2,677	2,067
Intel® Xeon® D-2798NT-Intel CryptoSW	2,181	1,884	3,280	2,663
Intel® Xeon® D-2798NT-Intel® QAT	3,313	2,699	3,171	2,611
Intel® Xeon® 6563P-B -Native OpenSSL	1,899	1,678	3,965	3,313
Intel® Xeon® 6563P-B -Intel CryptoSW	2,933	2,495	4,762	3,782
Intel® Xeon® 6563P-B -Intel® QAT	5,213	3,478	4,433	3,680

Figure 4. NGINX webserver TLS handshakes with traditional and hybrid PQC algorithms on Intel® Xeon® SoC platforms

Transitioning from traditional algorithms to hybrid PQC algorithms can have performance consequences of up to 15% with RSA algorithms and up to 21% with ECDSAP256 with software acceleration. These algorithms combine traditional and PQC algorithms for higher security, effectively carrying out both traditional and post-quantum cryptographic computations, thus needing more compute resources.

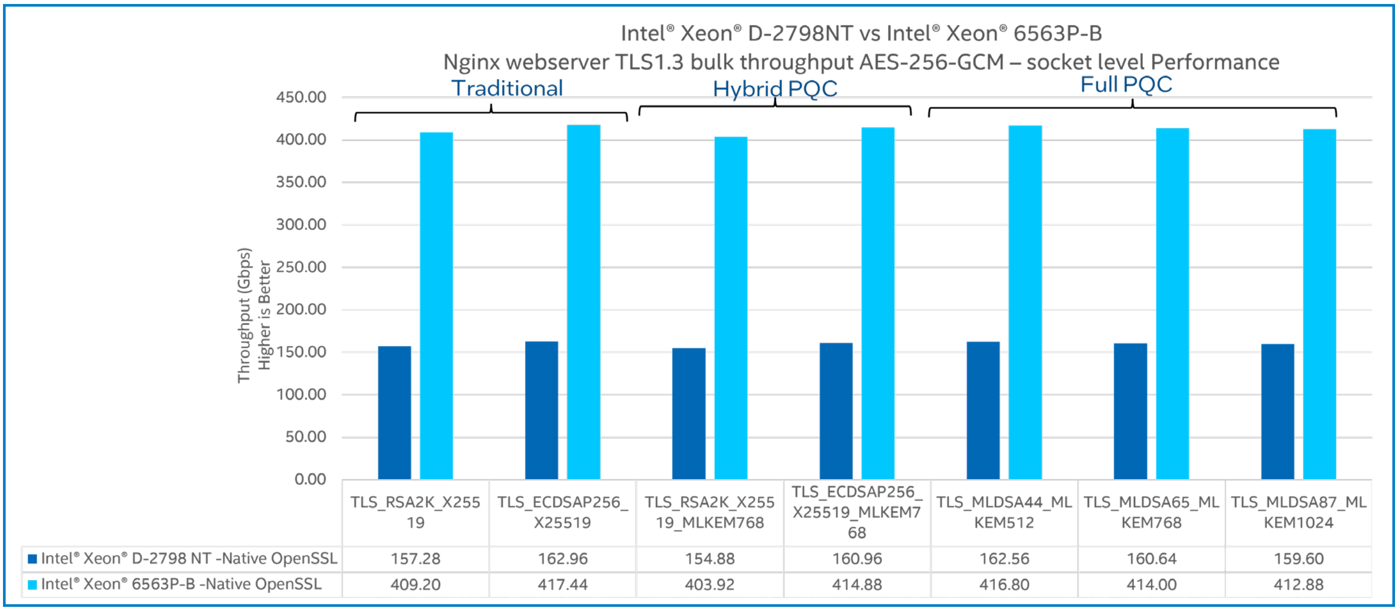
Figure 5 shows NGINX webserver TLS 1.3 handshake performance with both traditional and full PQC algorithms on Intel Xeon 6563P-B processor compared to previous generation CPU with native OpenSSL. Full PQC algorithm with highest key strength – TLS_MLDSA87_MLKEM1024 can achieve up to 2,926 TLS handshakes per second on a single core of Intel Xeon 6563P-B processor, providing up to 66% of gain than that of previous gen CPU. The full PQC algorithm performance is dominated by the use of MLDSA for signatures. This algorithm is found to be slower than ECDSA but faster than RSA.



	TLS_RSA2K_ECDHEP256	TLS_RSA2K_X25519	TLS_ECDSAP256_ECDHEP256	TLS_ECDSAP256_X25519	TLS_MLDSA44_MLKEM512	TLS_MLDSA65_MLKEM768	TLS_MLDSA87_MLKEM1024
■ Intel® Xeon® D-2798NT-Native OpenSSL	1,166	1,325	2,130	2,677	2,473	2,019	1,753
■ Intel® Xeon® 6563P-B -Native OpenSSL	1,607	1,899	3,183	4,119	4,012	3,329	2,926

Figure 5. NGINX webserver TLS handshakes with traditional and PQC algorithms on Intel® Xeon® SoC platforms

NGINX webserver bulk throughput with traditional, hybrid and full PQC algorithms on Intel Xeon 6563P-B processor and previous generation SoC with native OpenSSL is compared in Figure 6. Intel Xeon 6563P-B processor can deliver up to 415 Gbps of NGINX bulk throughput with 42 cores, up to 2.6x better than previous generation CPU. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) built into these processors accelerate AES algorithm, by enabling parallel processing of data blocks, enhancing overall throughput.



	TLS_RSA2K_X25519	TLS_ECDSAP256_X25519	TLS_RSA2K_X25519_MLKEM768	TLS_ECDSAP256_X25519_MLKEM768	TLS_MLDSA44_MLKEM512	TLS_MLDSA65_MLKEM768	TLS_MLDSA87_MLKEM1024
■ Intel® Xeon® D-2798 NT -Native OpenSSL	157.28	162.96	154.88	160.96	162.56	160.64	159.60
■ Intel® Xeon® 6563P-B -Native OpenSSL	409.20	417.44	403.92	414.88	416.80	414.00	412.88

Figure 6. NGINX bulk throughput performance on Intel® Xeon® D platforms with traditional, hybrid, and full PQC algorithms

Summary

Quantum computers capable of breaking traditional cryptography are expected to become available within the next decade; however, the “Harvest Now, Decrypt Later” threat is real now, raising major security concerns. To protect data from quantum threats, it is critical to begin transitioning to post-quantum cryptography as early as possible.

Intel supports post-quantum transitions with PQC firmware signing and PQC algorithm acceleration, starting from the Intel Xeon 6 family. Intel Xeon 6 SoCs with increased core count, integrated Intel QAT and Intel AVX-512 instruction set deliver up to 40% better hybrid TLS handshakes, up to 66% better PQC TLS handshakes and up to 2.6x better throughput compared to previous generation SoC. Intel QAT can significantly boost hybrid PQC handshake performance and Intel crypto software enhances PQC algorithm acceleration.

References

Intel® Advanced Vector Extensions 512

Intel® QuickAssist Technology

Intel® QuickAssist Technology Engine for Open SSL*

Intel® Cryptography Primitives Library

Intel® Advanced Encryption Standard New Instructions

Open Quantum Safe-liboqs

Open Quantum Safe provider for OpenSSL(3.x)

Table 1. Hardware System Configuration

Component	Description	
CPU	Intel® Xeon® D-2798NT Processor	Intel® Xeon® 6563P-B Processor
Frequency	2.1 GHz	2.4 GHz
Cores/Threads	20/40	38/76
Memory	64 GB (4 x 16 GB DDR4 3200 MT/s [3200 MT/s])	128 GB (4 x 32 GB DDR5 6400 MT/s [6400 MT/s])
Disk	1x 223.6G Intel® SSDSC2KB240G8	1x 223.6G KINGSTON SA400S37240G
Ethernet	2x PCIe Gen 4 x16 NICs Intel® Ethernet Network Adapter E810-2CQDA2 (3 ports used, total 300 Gbps)	2x PCIe Gen 4 x16 NICs Intel® Ethernet Network Adapter E810-2CQDA2 for QSFP (total 400 Gbps) 1 x PCIe Gen4 x16 NIC Intel® Ethernet Connection E825-C for QSFP (total 200 Gbps)

Table 2. Software System Configuration

Component	Description	
CPU	Intel® Xeon® D-2798NT Processor	Intel® Xeon® 6563P-B Processor
OS	Ubuntu 24.04 LTS	Ubuntu 24.04.1 LTS
Kernel	6.8.0-44-generic	6.8.0-54-generic
OpenSSL	3.3.1	3.3.1
Oqs_provider	0.6.1	0.6.1
Liboqs	0.10.1	0.10.1
NGINX	1.22.1	1.22.1
Intel QAT driver	QAT.L.4.26.0-00008	QAT22. L.0.8.1-00011
QAT_engine	v1.6.1	v1.6.1
IPP_crypto	ippcp_2021.12.1	ippcp_2021.12.1
IPsec_mb	v1.5	v1.5

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 Tables 1 and 2 for configuration details. No product or component can be absolutely secure.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

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

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

The products described 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.

0925/DP/PDF 366990-001US