First Demonstration of 200 Gbps Regime Line-Rate Quantum-Secure MACsec Optical Links Using Commodity Hardware Offloads

Abraham Cano Aguilera,[1,3] Carlos Rubio Garcia,[1], Daniel C. Lawo [1,3] Idelfonso Tafur [1], J.L Imaña[2] , J.J Vegas Olmos [3]

[1] *Department of Electrical Engineering Eindhoven University of Technology, Eindhoven, The Netherlands*
[2]*Department of Computer Architecture and Automation, Complutense University of Madrid, Madrid, Spain*
[3]*NVIDIA Corporation, Yokneam, Israel*

[*]*acanoaguiler@nvidia.com*

Abstract: We demonstrate the first MACsec implementation at 196 Gbps over an end-to-end quantum-secure link using Quantum Key Distribution, Post-Quantum Cryptography, and Classical Cryptography with network offloads and hardware accelerators.

1. Introduction

When quantum computers emerge, today's public key infrastructure (PKI) will be vulnerable, compromising communication confidentiality, integrity, and authenticity. Two main contingency plans are being explored: Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). PQC algorithms, designed to resist quantum and classical attacks, saw a breakthrough in August 2024 when NIST standardized three algorithms [1] namely Dilithium (FIPS 203), Kyber (FIPS 204), and Sphincs+ (FIPS 205).

However, PQC's computational intensity complicates its integration into communication systems, especially within networking. QKD, while promising, faces technical challenges in range and integration, making it less suitable for high-speed systems like cloud and HPC clusters. Additionally, the need for scalable and interoperable cryptographic solutions has become increasingly urgent as organizations prepare for the quantum era. Crypto-agility—the ability to switch between cryptographic primitives—will be essential for future systems to establish hybrid quantum links with low latency while offloading tasks to dedicated components.

By offloading traffic to Data Processing Units (DPUs) [2], our approach aims to significantly reduce CPU load while ensuring high transmission throughput. These enhancements, along with the integration of QKD and PQC to the PKI, facilitate future intra-data center communication that is secure against quantum computing threats.

Following NIST's hybrid security guidelines [3], we present the first lab demonstration of crypto-agile end-to-end quantum-secure communication using Dilithium and Kyber on DPUs, alongside QKD for 200G optical networks. Both PQC and classical methods, such as Ellipictic-Curve Digital Signature Algorithm and Diffie-Hellman [4], run concurrently. The quantum-secure keys generated are used to encrypt data with AES-256 [5], ensuring secure, efficient communication in the evolving cryptographic landscape.

2. Experimental set-up for a quantum secure line-rate MACsec link

Fig. 1 illustrates the methodology for creating a quantum-secure link using Media Access Control security (MACsec) as per the IEEE 802.1AE standard [6]. MACsec provides encryption, integrity, and authentication at layer 2 of the OSI model for Ethernet traffic, safeguarding data in local area networks (LANs) with key management via the MACsec Key Agreement (MKA) protocol [7]. Our software stack, shown in Fig. 1, implements both MACsec and MKA.

In the optical networking experiment (Fig. 1, Left), we replicate inter-data center communications between two autonomous servers, each with a central processing unit (CPU) and two DPUs BF3 model [2] supporting 200G connections through ConnectX-7 NICs, integrating 16 ARMv8 A72 cores for hardware offloading. Connections between servers and DPUs utilize PCIe bridges, while the DPUs interconnect via a fiber-based Mellanox SN3420 switch with QSFP112 coherent modules. Both DPUs interface with an ETSI-GS014 [8] key negotiation API to establish a quantum-secure MACsec tunnel between **DPU_A** and **DPU_B**.

Authentication of both peers begins with a quantum-secure key exchange via a QKD-enabled TLS handshake [9]. We utilize Dilithium and ECDSA for user authentication, with Kyber, ECDH, and QKD for exchanging a hybrid quantum-secure Master Secret Key (MSK) at both ends.

After the MSK exchange, the Linux kernel offloads MKA to the *wpa_supplicant* module (Fig. 1, Right). **DPU_A** and **DPU_B** agree on security parameters, including AES-256 in Galois Counter Mode (GCM) to meet quantum security requirements. The exchanged MSK expands the Connectivity Association Key (CAK) and Connectivity Association Key Name (CKN). Subsequently, a server agreement process selects a server for encapsulating the secure association key (SAK).

Once a server is chosen, both parties derive the Key Encryption Key (KEK) and Integrity Check Key (ICK) using a KDF on the CKN and CAK material. The selected server (**DPU_A**) encrypts the SAK with the KEK, enabling **DPU_B** to obtain a triple-hybrid quantum-secure key. Finally, Server A and Server B use this SAK to offload MACsec operations to the DPUs, which encrypt quantum-secure data at 196 Gbps.

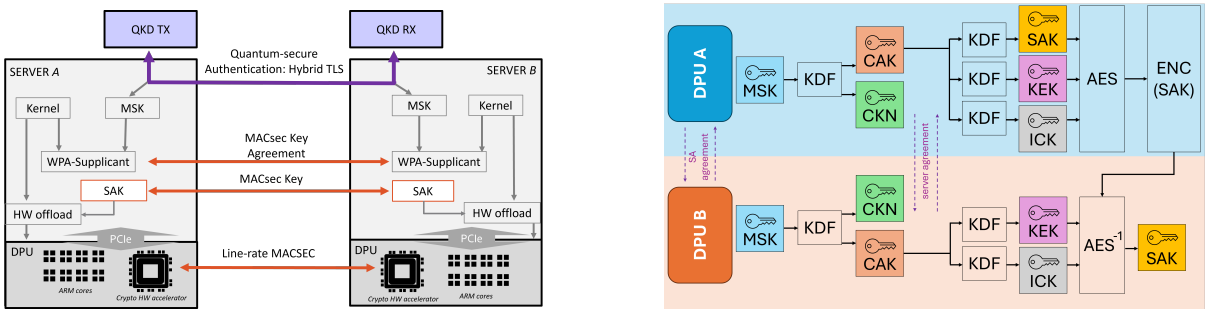

Fig. 1: (Left) Setup for establishing a quantum-secure MACsec channel. (Right) Quantum-secure MKA for deriving encryption keys at both ends.

3. Experimental results and discussion

Fig. 2 presents the experimental results of transmitting encrypted data over our quantum-secure encrypted link. To highlight the advantages of offloading encryption to the DPU, we evaluated the following scenarios: **1) No Tunnel:** No encryption is applied, resulting in maximum throughput, which serves as the baseline. **2) Quantum-Secure Tunnel using Linux Kernel MACsec:** This simulates a typical data center use case where software-based encryption is required.In this scenario, packets are encrypted on the server before being sent through the NIC. **3) Quantum-Secure Tunnel with Linux Kernel MACsec and DPU Offload:** This scenario is similar to case 2 but with encryption offloaded to the DPU, meaning the encryption occurs on the NIC rather than on the server.

The results in Fig. 2 (Left) show that the highest throughput is achieved when transmitting unencrypted data, regardless of MTU size. Once standard MTU sizes (around 1000 bytes) are used, the link can be saturated, reaching the maximum data transfer rate of 200 Gbps. When the MACsec Linux application is implemented with the triple hybrid scheme, a secure link is achieved, but throughput drops drastically. It goes from 300 Mbps with small MTU sizes (due to header processing saturation) to 5 Gbps with standard MTU sizes, and 13 Gbps with jumbo frames (above 8000 bytes). This represents about 5% of the channel capacity, attributed to server-side encryption without dedicated hardware acceleration.

In contrast, when MACsec encryption is offloaded to the DPU, performance improves significantly. Although throughput remains lower than unencrypted data at small MTU sizes (reaching 2 Gbps), performance increases dramatically when MTUs are around 1000 bytes, achieving 93.4 Gbps, which is 45% of the channel capacity and sufficient for high-performance applications. With jumbo frames, throughput reaches 196 Gbps, over 99% of the channel capacity. These results demonstrate that line-rate quantum-secure MACsec links are achievable when encryption is offloaded to the DPU.

Fig. 2 (right) illustrates the CPU usage on the server side while utilizing 64 cores for sending and receiving encrypted data. CPU usage is closely related to energy consumption and resource allocation on the servers, thereby this figure offers insights into system telemetry. The results indicate that when one client sends data continuously, the CPU load dedicated to performing the cryptographic operations of the tunnel reaches 81% for processing both small and big packets.

When the same experiment is conducted with the cryptographic operations offloaded to the DPUs, the CPU load decreases to 45%, effectively liberating up 35% of CPU resources. This reduction stems from the fact that the primary cryptographic tasks executed in the kernel, such as AES-256 computation and MACsec frame processing, are significantly more resource-intensive than the operations associated with hardware offloading to the DPU. This underscores the high costs in computational load and energy consumption associated with encrypting data on servers. Consequently, servers may not be ideal for applications expecting a high volume of incoming connection requests to set-up encrypted links along with encrypting data itself, while DPU offloading helps maintain

throughput and relieve CPU resources.

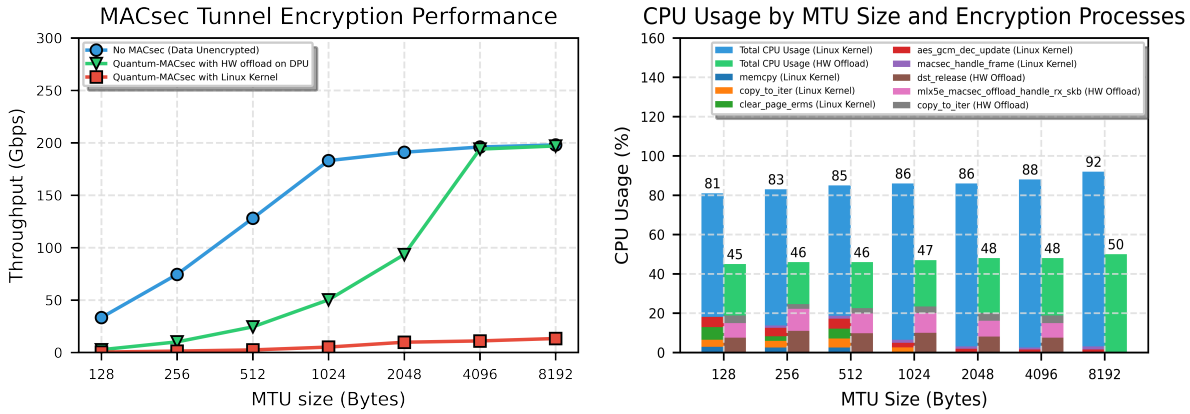

Fig. 2: (Left) Throughput comparison between unencrypted data and data encrypted with MACsec with both HW offloads to DPUs and with Linux Kernel application. (Right) CPU usage related to cryptograpahic processes when implementing the MACsec link with the linux kernel module and when offloading the processes to the DPU.

4. Conclusions

This work introduced a major advancement in achieving line-rate, end-to-end, quantum-secure encrypted communication over optical fiber between data centers. The first practical implementation of a MACsec link using DPUs at a line rate of 200 Gbps is demonstrated. An extended TLS-based protocol is employed to secure the control plane and mutually authenticate both peers using classical and PQC. Afterward, initial key material is exchanged by integrating classical, PQC and QKD methods, fully enabling crypto-agility. MACsec encryption keys are then expanded through the MKA protocol and utilized by two DPUs, which encrypt the data plane via AES-GCM over a point-to-point optical link. This work shows that offloading network operations to the DPU maintains high-speed communication while reducing CPU load on the server. Additionally, the necessary modifications to the PKI prove that quantum-secure high-speed communications are achievable, paving the way for high-capacity quantum-secure communications in dense network fabrics.

5. Acknowledgements

This work was partly funded by EC-funded QUARC (101073355) and CLEVER (101097560) projects.

References

1. National Institute of Standards and Technology (NIST). Announcing approval of three federal information processing standards (fips) for post-quantum cryptography. https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved, August 13 2024. Accessed: 2024-10-23.
2. NVIDIA. Nvidia bluefield datasheet. https://resources.nvidia.com/en-us-accelerated-networking-resource-library/datasheet-nvidia-bluefield.
3. Post-quantum cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs.
4. Standards for Efficient Cryptography Group (SECG). SEC 1: ECC. Technical report, SECG, 2009.
5. Morris Dworkin et al. Advanced encryption standard (aes), 11 2001.
6. IEEE. Ieee standard for local and metropolitan area networks: Media access control (mac) security, 2006. IEEE Std 802.1AE-2006.
7. IEEE. Ieee standard for local and metropolitan area networks - port-based network access control, 2010. IEEE Std 802.1X-2010, including MACsec Key Agreement (MKA).
8. ETSI. Quantum key distribution (qkd); protocol and data format of rest-based key delivery api. Technical report, ETSI, February 2019.
9. Carlos Rubio Garcia, Abraham Cano Aguilera, Juan José Vegas Olmos, Simon Rommel, and Idelfonso Tafur Monroy. Integrating quantum key distribution into tls 1.3: A transport layer approach to quantum-resistant communications in optical networks. In *Optical Fiber Communication Conference 2024*. Optica Publishing Group, March 2024. 2024 Optical Fiber Communications Conference and Exhibition (OFC) ; Conference date: 24-03-2024 Through 28-03-2024.