First Line-rate End-to-End Post-Quantum Encrypted Optical Fiber Link Using Data Processing Units (DPUs)

A. Cano Aguilera,[1,4,*] R. Abu Bakar,[2], F. Alhamed [2], C. Rubio Garcia [1], J.L. Imaña [3], I.Tafur Monroy[1], F. Cugini[3] and J.J Vegas Olmos [4]

[1] *Quantum & Terahertz Systems, Eindhoven University of Technology, 5600MB, The Netherlands*
[2] *CNIT, 56124 Pisa, Italy*
[3] *Universidad Complutense de Madrid, 28040 Madrid, Spain*
[4] *NVIDIA Corporation, 2066730 Yokneam Illit, Israel*

[*] *a.c.a.cano.aguilera@tue.nl*

Abstract: We demonstrate the first 92.3-Gbits/s line-rate, end-to-end post-quantum cryptography optical fiber link based on HW accelerators and processing offloading. © 2023 The Author(s)

1. Introduction

Post-quantum cryptography (PQC) refers to cryptographic algorithms that are designed to be secure against cryptanalytic attacks by both quantum and classical computers. After years of fundamental research, in August 2023 the National Institute of Standards and Technology (NIST) standardizing body of PQC algorithms released four standard drafts [1]. PQC is inherently a part of the networking stack; as a computationally intensive process, its integration into communication systems is therefore challenging. Recent demonstrations using Field-Programmable Gate Arrays (FPGA) or Graphic Processing Units (GPU) have been demonstrated for some of the different candidates for standarization [2–4], as well as initial attempts on Application-Specific Integrated Circuits (ASIC) solutions for other PQ schemes like SPHINCS+ [5] or SABER [6], which are reported at synthesis level. Prior research primarily targets low/mid-bitrate contexts (e.g., Internet-of-Things, Trusted Platform Module for automotive, Space communications) and often lacks cost and energy efficiency.

High-speed communications operating in intra-/inter-Edge/Cloud/ High Performance Computing (HPC) clusters need to be able to establish PQC links at low latency and maintaining state-of-the-art line-rates, while freeing up server resources and offloading networking operations to the network components. We present the first experimental demonstration of end-to-end PQC communications implementing Dilithium and Kyber on Data Processing Units (DPUs) [7] operating at line-rate over optical networks. Our complete stack implements Dilithium [4] for post-quantum digital signature authentication, Kyber [8] to execute the exchange of post-quantum keys. Both the PQ-based digital signature and key exchange are done in parallel to their classical counterparts, namely Elliptic Curve (EC) Digital Signature [9] Algorithm and EC Diffie-Hellman [10]. The hybrid approach follows NIST recommendations, since such hybrid schemes are safe as long as one of its components is secure [11]. This hybrid approach is coherent with NIST recommendations since such schemes are secure as long as one of its components is secure [11]. Finally, these PQC keys are used to encrypt and decrypt data through 256 bit Advanced Encryption Standard (AES)/Rijndael [12] cipher. This hybrid approach paves the way for efficient and secure communication in the era of evolving cryptographic requirements, ensuring compatibility between classical and post-quantum cryptographic systems.

2. PQC tunneling and Experimental Setup

Figure 1a shows the methodology to establish a PQC communication channel between two DPUs in a point-to-point link configuration. Our software stack includes an Internet Protocol Security (IPsec) tunnel for secure communication over a public network. We use the *ovs-ipsec* tool to create the tunnel, offloading packet traffic to the Linux kernel's traffic classification (TC) on a virtual bridge connecting two DPUs in an optical network. Within the tunnel, classical AES keys are exchanged to encrypt data traffic, followed by NIST-approved algorithms, Dilithium for user identity verification and Kyber for key exchange. After this sequence and the establishment of the PQC link, data is encrypted using an XORed AES-256 key (Classical+Post Quantum) with corresponding PQC headers. As shown in Figure 1b and Figure 1c, our optical networking experiment is aimed at replicating inter-data center communications comprising two autonomous servers, each equipped with its own central processing unit (CPU),

and two DPUs capable of 100G connections, integrating ARMv8 A72 cores for hardware offloading. The linkage between the servers and DPUs is facilitated by Peripheral Component Interconnect Express (PCIe) bridges. The DPUs are connected to EdgeCore Sonic white boxes equipped with 400 Zero Return + (ZR+) coherent pluggable modules. The optical link between the white boxes, 240 km long with three spans of 80 km, is operated with 16 Quadrature Amplitude Modulation (QAM) format at 400 Gbps. The setup involves the creation of a PQC-based IPSec tunnel between DPU A and DPU B.

3. Experimental results and discussion

Figure 2 shows the experimental results for the communication throughput. To prove the benefits of our implementation we consider the following cases: **1) No tunnel**. No encryption is on. **2) PQ Tunnel with computational offloading to the DPU and with HW accelerations**. In this scenario we use HW accelerations for encrypting and decrypting the packets going through the tunnel. **3) PQ Tunnel with computational offloading to the DPU without HW accelerations**. This is the case of a standard Smart Network Interface Card (SmartNIC) without dedicated hardware to handle the cryptographic operations. **4) PQ Tunnel on the server**. This scenario shows the normal configuration in nowadays servers in which a tunnel between 2 NICs is configured on the server.

Figure 2 (left) shows that the highest throughput is achieved when transmitting unencrypted data (98.2 Gbps - blue bar), which is set as baseline. We can observe that when using the DPU with HW offloads (Scenario 2 - green bar) to establish the PQ-IPsec tunnel (including authentication, key exchange and encryption), the throughput remains close to the baseline, confirming almost no penalty at 92.3 Gbps. However, when using the DPU without HW offloads (Scenario 3 - red bar), the throughput drops drastically to 13.3 Gbps, making it infeasible for high speed optical networks. Furthermore, when the IPsec PQC tunnel is set up on the server, it achieves rates of less than 5 Gbps, indicating that current server architectures without dedicated hardware for encryption are unable to simultaneously handle the high bandwidth demands and the computational complexity of PQC.

Figure 2 (right) shows the CPU usage on the server side when using 8 cores for sending and receiving encrypted data; since CPU usage is related to energy consumption and resource allocation of the servers, the figure provides a glimpse on system saturation. Results show that the isolation of the CPU load for computing the cryptographic operations of the tunnel is over 80% for processing both small packets of 128 or 256 bytes and big packets of more than 8000 bytes, when one client was sending data uninterruptedly. The CPU load is reduced to 20% when performing the same experiment but offloading the cryptographic operations to the DPUs (60% CPU freeing). This highlights that encrypting data on servers comes at high cost in terms of both computational load and energy consumption. As a result, servers are not really suitable for applications that anticipate a high volume of incoming connection requests, whereas DPU offloading maintains throughput and frees up CPU resources.

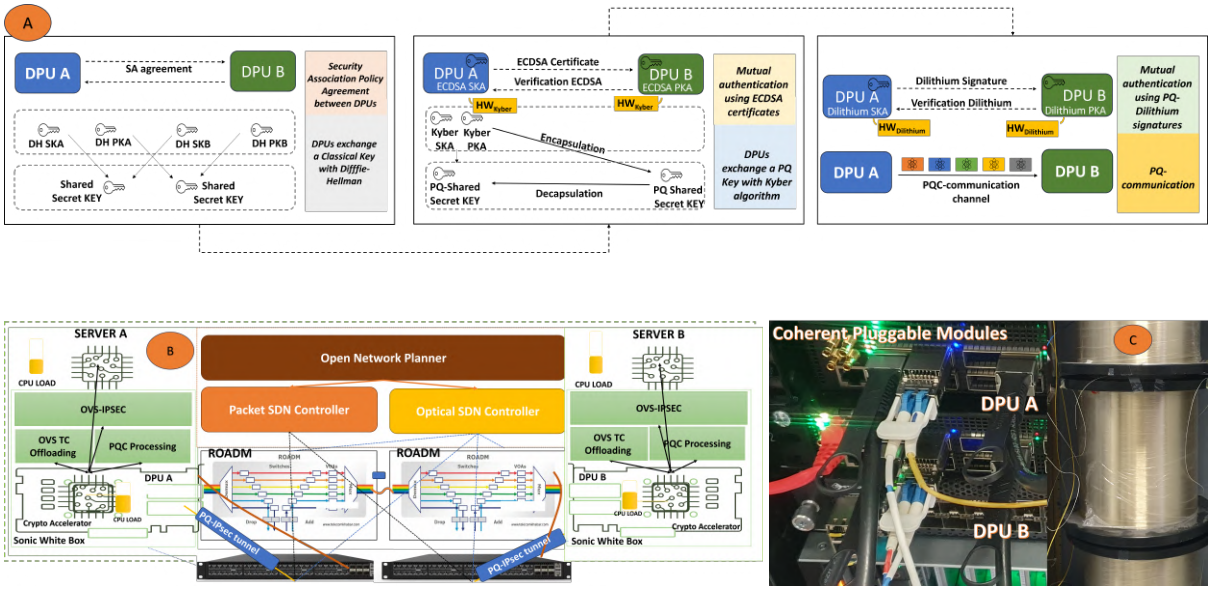

Fig. 1: (a): Protocol for end-to-end PQC-establishment. (b): PQC Testbed topology for Secure PQC IPSec tunneling on Software Defined Networks (SDN). (c): Photography of our laboratory set-up.

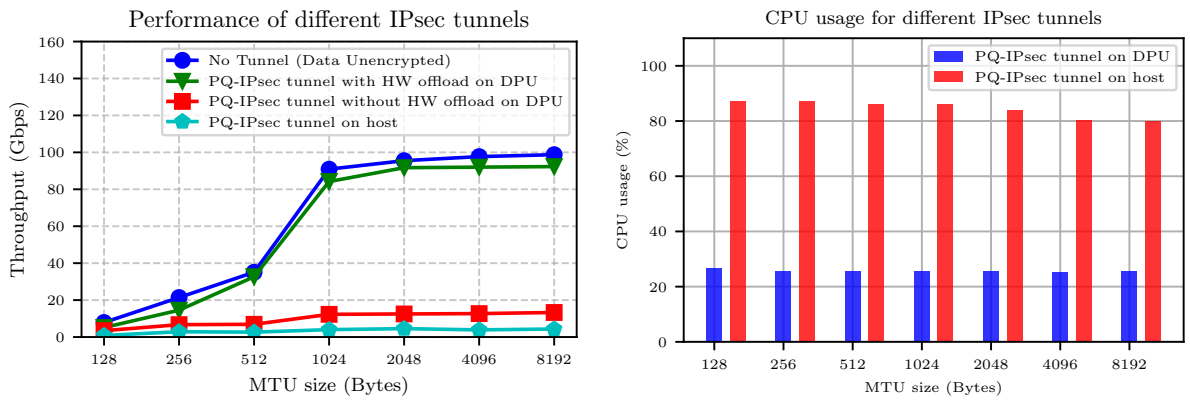

Fig. 2: Left) Throughput comparison for unencrypted data and PQC tunnels with/without HW offloads at DPU and full server PQC processing. Right) CPU usage as a function of packet size for the case of PQ-IPsec tunnel deployed on a server (Red) and a PQ-IPsec tunnel deployed on a DPU (Blue).

4. Conclusions

This work presented a breakthrough in line-rate, end-to-end, post-quantum encrypted optical fiber inter datacenter communication. The first reported link establishing between two independent servers which use data processing units to carry out the PQC operations and transmits data at high bandwidth is presented. DPUs are responsible of establishing a hybrid IPsec tunnel which initially employs classical ECDSA certificates with classical Key Exchange (Diffie-Hellman) and then PQ authentication with Dilithium and Key Exchange with Kyber. Once the control plane is secured, both servers can transmit encrypted data using AES-256. We have shown that when offloading the cryptographic tasks from the server to the DPUs, the throughput is increased tenfold and the computational load is reduced by 60%. Our experimental implementation shows for the first time that it is possible to integrate PQC in realistic optical fiber transmission scenarios, at line-rate, which is essential for quantum secure communication infrastructures operating at high-speed.

5. Acknowledgements

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

References

1. G. Alagic *et al.*, "Status report on the third round of the NIST post-quantum cryptography standardization process," Tech. Rep. NIST IR 8413, National Institute of Standards and Technology (2022).
2. V. B. Dang *et al.*, "High-speed hardware architectures and fpga benchmarking of crystals-kyber, ntru, and saber," IEEE Trans. on Comput. **72**, 306–320 (2023).
3. M. Li *et al.*, "Reconfigurable and high-efficiency polynomial multiplication accelerator for crystals-kyber," IEEE Trans. on Comput. Des. Integr. Circuits Syst. **42**, 2540–2551 (2023).
4. L. Ducas *et al.*, "Crystals-dilithium: A lattice-based digital signature scheme," .
5. Y. Dai *et al.*, "High-throughput hardware implementation for haraka in sphincs+," in *2023 24th International Symposium on Quality Electronic Design (ISQED),* (2023), pp. 1–6.
6. M. Imran *et al.*, "High-speed design of post quantum cryptography with optimized hashing and multiplication," IEEE Trans. on Circuits Syst. II: Express Briefs (2023).
7. I. Burstein, "Nvidia data center processing unit (dpu) architecture," in *2021 IEEE Hot Chips 33 Symposium (HCS),* (2021), pp. 1–20.
8. J. Bos *et al.*, "Crystals - kyber: A cca-secure module-lattice-based kem," (2018), pp. 353–367.
9. National Institute of Standards and Technology, "Digital signature standard (dss)," FIPS Publication 186 (1994).
10. E. Barker *et al.*, "Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography," (2018).
11. "Post-quantum cryptography," https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs. Accessed: 2023-09-30.
12. M. Dworkin *et al.*, "Advanced encryption standard (aes)," (2001).