# Post-Quantum Cryptography for Quantum Resilient Data Transfer

1st Abraham Cano
Software Architecture
NVIDIA corporation
Milan, Italy
acanoaguiler@nvidia.com

2nd José Luis Imaña
Departament of Computer Architecture and Automation
Universidad Complutense
Madrid, Spain
jluimana@ucm.es

3rd Idelfonso Tafur Monroy
Departament of Electrical Engineering
Eind. University of Technology
Eindhoven , The Netherlands
i.tafur.monroy@tue.nl

4th Juan José Vegas
Software Architecture
NVIDIA corporation
Yokenam, Israel
juanj@nvidia.com

***Abstract*—Post-quantum cryptography is essential for ensuring quantum-resilient data transfer, as quantum computers have the potential to break widely used cryptographic algorithms, such as RSA and ECC, which secure most of today's digital communications. With quantum computing advancing rapidly, the ability of these machines to factor large numbers and solve complex mathematical problems at unprecedented speeds poses a serious threat to current encryption methods. Post-quantum cryptography develops new algorithms that are resistant to attacks from quantum computers, safeguarding sensitive information and critical infrastructures. This transition is crucial to maintaining data security and privacy in the future, as governments, financial institutions, and businesses increasingly rely on quantum-resilient protocols to protect against potential breaches in a post-quantum world. This talk will present the implementations of IPsec and MACsec of the three standardized protocols for PQC (FIPS 203, 204 and 205) operating at full-line rate (100Gbit/s) and (200 Gbit/s).**

***Keywords—Quantum-resistant cryptography, network offloads, data processing units, PQ cryptography, public key infrastructure.***

## I. Introduction

As quantum computers become a reality, the current public key infrastructure (PKI) will be at risk due to the attacks that might be implemented against the discrete logarithm and integer factorization problems, the mathematical basis of modern cryptography. These attacks will threaten the confidentiality, integrity and authenticity of our communications. To address this issue, two main strategies are being considered nowadays, Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). PQC focuses on mathematical solutions that prove complex computational problems and for this the National Institute of Standards (NIST) achieved a major milestone in August 2024, when they release the first three PQC algorithms for standardization. Namely Dilithium (FIPS 203) [1], Kyber (FIPS 204) [2] and Sphincs+ (FIPS 205) [3].

Despite these advancements, the high computational demands of PQC present challenges for its adoption in communication systems, particularly in networking. Although QKD offers promising security benefits as its security is not based on computational complexity but on the laws of quantum physics, its limitations in range and integration make it less suitable for high-speed environments like cloud services and HPC clusters. The increasing urgency for scalable and interoperable cryptographic solutions highlights the importance of crypto-agility—the ability to seamlessly switch between cryptographic primitives—to enable hybrid quantum-secure links with minimal latency and task offloading to specialized components.

The most evident use of quantum-resistant cryptography is its implementation in secure communication protocols. In this work we will focus on providing quantum-resistant solutions for encrypting ethernet frames and IP packets.

Ethernet is one of the most widely adopted technologies for connecting devices within local area networks (LANs). Since its invention in the 1970s, Ethernet has faced and adapted to various challenges, including the demand for higher speeds, the need for stronger security, and more recently, the emerging quantum threat.
To address security concerns, the IEEE developed the *Media Access Control Security* (MACsec) [4] [5] standard for local and metropolitan area networks. MACsec is designed to provide data confidentiality, integrity, and authentication at Layer 2 of the Open Systems Interconnection (OSI) model. It plays a critical role in securing the link layer by offering encryption, authentication, and protection against attacks such as eavesdropping, tampering, and replay. MACsec ensures trusted communications across LANs, data centers, and modern networks like 5G and IoT, working in conjunction with higher-layer security protocols such as TLS and IPsec.
MACsec specifies the cipher suites available for encrypting data on the Ethernet layer.

On the other hand, Internet Protocol Security (IPsec) [6] and its key exchange (IKE) [7]. IPsec protocol aims to provide encryption, authentication and integrity protection at the

network layer. IPsec main use case is to secure virtual private networks (VPNs) and to secure communication between network interfaces through insecure channels as the internet. IKE is composed by two phases, in phase one the control plane is secured. Right after, the second phase is used to protect the data plane sending encrypted data with a symmetric cipher. Both phases use PKI stack and state of the art relies its security exclusively in classical security, thus, levering it weaker adversaries with quantum advantage.

In this work we show how both protocols can be implemented efficiently on Data Processing Units. Data Processing Units (DPUs) offer an alternative to traditional architectures in which the central processing units (CPUs) take care of all the tasks. DPUs might allow hosts to offload specific tasks such as network processing and encryption, thereby enhancing system performance and reducing power consumption. In this work, we leverage DPUs to establish a quantum-safe communication link. This is accomplished by utilizing specialized hardware components such as digital signal processors (DSPs), semiconductor intellectual property (IP) blocks, and graphics processing units (GPUs).

In this work we revisited which approaches might be followed to implement quantum-resistant versions of IPsec and MACsec on different DPUs models and how them can be combined to have data encrypted at multiple protocol levels.

## II. MACsec set-up

### A. Architecture

Figure 1, presents the methodology for establishing a quantum-secure link using Media Access Control security (MACsec), following the IEEE 802.1AE standard as presented in [8]. MACsec ensures encryption, integrity, and authentication at the OSI model's layer 2 for Ethernet traffic, securing data transmission within local area networks (LANs) and relying on the MACsec Key Agreement (MKA) protocol for key management. Our software stack, depicted in Figure 1, implements both MACsec and MKA functionalities. We emulate inter-data center communication between two independent servers, each one equipped with a central processing unit and two BF3. The DPUs support link speeds of 200G connected through ConnectX-7 network interface cards (NICs). Each DPU also incorporates 16 ARMv8 A72 cores. 6 ARMv8 A72 cores to accelerate hardware offloading. Server-to-DPU connections are established via PCIe bridges, while DPUs interconnect through a fiber-based Mellanox SN3420 switch using QSFP112 coherent modules. Both DPUs interface with the ETSI-GS014 key negotiation API.

Peer authentication is initiated through a quantum-secure key exchange using a QKD-enabled TLS as seen in Figure 2. For user authentication, we deploy Dilithium and ECDSA, while the hybrid Master Secret Key (MSK) exchange relies on Kyber, ECDH, and QKD.

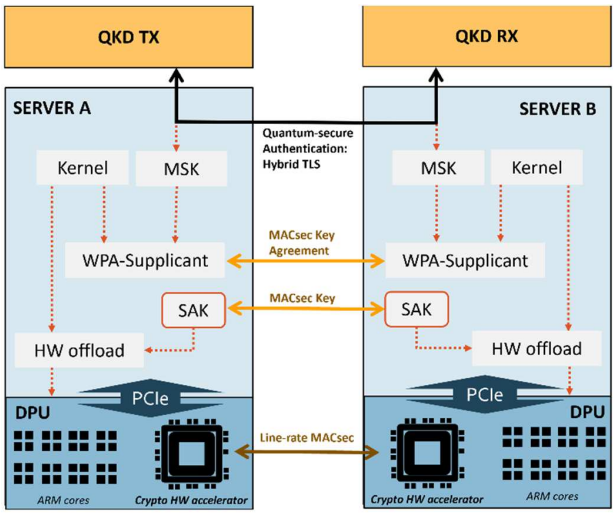


*Figure 1:Set-up for establishing Quantum-Secure MACsec key agreement between DPUs.*

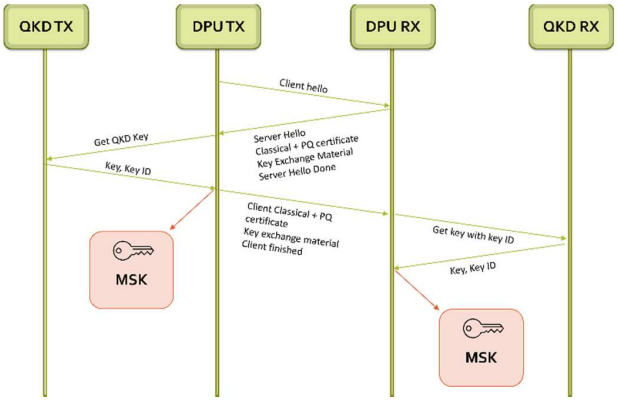


*Figure 2:TLS protocol for authenticating MACsec peers with PQC and QKD*

## III. IPsec set-up

### A. Architecture

Figure 1 illustrates the approach used to establish a PQC communication channel between two DPUs configured in a point-to-point link and presented in [9]. Our software stack features an Internet Protocol Security (IPsec) tunnel to ensure secure communications over a public network. The tunnel is created using the ovs-ipsec tool, which offloads packet handling to the Linux kernel's traffic classification (TC) system, implemented over a virtual bridge connecting the two DPUs across an optical network. Inside the tunnel, classical AES encryption keys are first exchanged to secure data traffic. Following this, post-quantum cryptographic operations are performed using Dilithium for user authentication and Kyber for key exchange, in line with NIST-approved algorithms. Once the PQC-secured link is established, data is encrypted using an

XORed AES-256 key that combines classical and post-quantum material, along with corresponding PQC-specific headers.

The optical networking experiment, illustrated in Figures 2 and 3, emulates inter-data center communications between two independent servers. Each server is equipped with its own central processing unit (CPU) and two DPUs capable of 100G network connections, featuring ARMv8 A72 cores to support hardware offloading. Connectivity between servers and their respective DPUs is achieved through Peripheral Component Interconnect Express (PCIe) bridges.

The DPUs are linked to EdgeCore Sonic white box switches, each outfitted with 400G Zero Return Plus (ZR+) coherent optical modules. The optical connection between the white boxes spans a total of 240 kilometers, divided into three segments of 80 kilometers each. The optical signals are transmitted using a 16 Quadrature Amplitude Modulation (16-QAM) format at a line rate of 400 gigabits per second. This setup establishes a PQC-based IPsec tunnel between DPU A and DPU B.

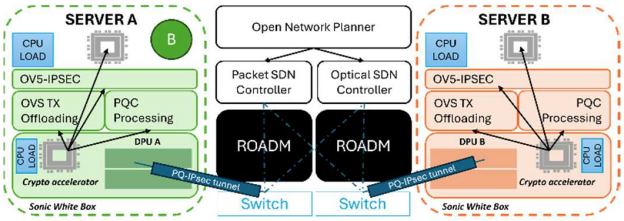


*Figure 3:Optical set-up for an IPsec quantum-secure channel*

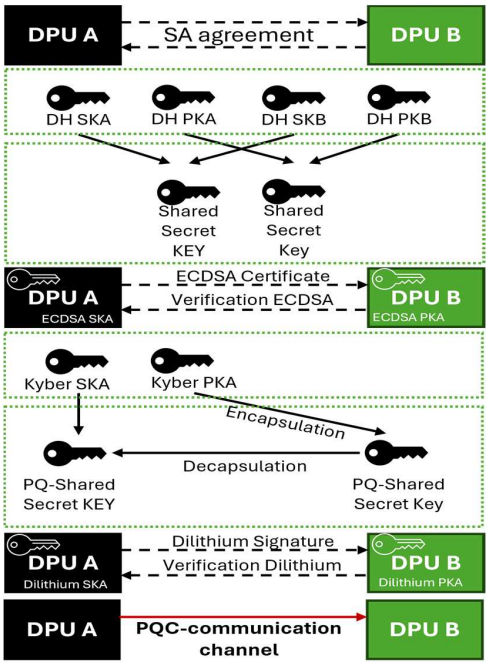


*Figure 4:IPsec key material and authentication protocol with quantum-resistant enhancement*

## IV. COMBINING MULTIPLE NETWORK PROTOCOLS

To build a resilient framework against quantum threats, securing multiple layers of the network stack is critical. In this work, we demonstrate how the combined use of quantum-secure MACsec and IPsec provides multilayer encryption, protecting data both at the Ethernet frame level and at the IP packet level. This approach ensures end-to-end confidentiality, integrity, and authenticity, even in the presence of future quantum-capable adversaries.

MACsec operates at Layer 2 of the OSI model, providing frame-level encryption, integrity, and authentication for Ethernet traffic. It secures communications within local and metropolitan area networks, immediately protecting data upon leaving a device's network interface. IPsec, in contrast, functions at Layer 3, safeguarding IP packets across routed and potentially untrusted networks such as the public internet. Combining both protocols results in defense-in-depth, with independent, complementary layers of protection that substantially raise the bar for potential attackers.

Different generations of Data Processing Units (DPUs) are utilized to optimize for the specific requirements of each protocol. For IPsec, we employ BlueField-2 (BF2) DPUs operating at 100 Gbit/s. In this configuration, both the control plane and the data plane are fully managed within the DPUs. The BF2 devices autonomously establish quantum-secure IPsec tunnels, using Dilithium for authentication and Kyber for key exchange. Once established, encrypted traffic flows directly between the DPUs without host intervention. The host simply transmits and receives encrypted IP packets through standard interfaces, minimizing CPU overhead and enabling secure communication with maximum transparency.

In contrast, MACsec is implemented using BlueField-3 (BF3) DPUs connected at 200 Gbit/s. In this case, the control plane operations, including peer authentication, key negotiation, and session establishment, are computed at the host level. We leverage a QKD-enabled TLS protocol combined with hybrid post-quantum authentication mechanisms such as Dilithium and ECDSA, and hybrid key exchange using Kyber, ECDH, and QKD material. After the host derives a shared secret, it securely transfers the session key to the BF3 DPU, which then assumes responsibility for encrypting and decrypting Ethernet frames at full line rate. This division of labor allows the host to maintain cryptographic agility, while the DPU focuses exclusively on high-performance data path encryption.

By deploying MACsec and IPsec together, we achieve layered security that covers multiple protocol levels, from the local link layer to end-to-end network communications. This not only provides comprehensive protection against both classical and quantum attacks but also ensures that a breach at one layer does not expose the underlying data. Furthermore, offloading

cryptographic operations to DPUs reduces the burden on host CPUs, improving overall system performance and efficiency. The combined architecture leverages the strengths of each DPU generation: the complete data and control offload capabilities of BF2 for IPsec, and the ultra-high-speed data encryption capabilities of BF3 for MACsec. Such an approach establishes a practical and scalable path toward quantum-resilient networks in both data center and wide-area deployments.

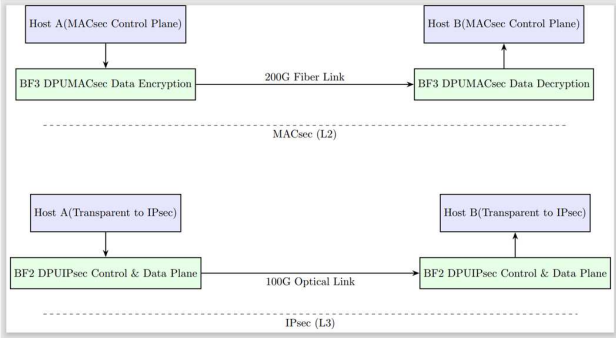


*Figure 5:Combined Architecture for Quantum-Resilient Data Transfer*

Figure 5 illustrates the joint deployment of MACsec and IPsec quantum-secure protocols. In the MACsec setup, the host executes the control plane to derive a hybrid quantum-resistant session key using PQC and QKD technologies before offloading encryption tasks to BF3 DPUs operating at 200 Gbit/s. In the IPsec setup, BF2 DPUs at 100 Gbit/s manage both the control and data planes independently, establishing a quantum-secure IPsec tunnel between the DPUs. Host systems interact with the encrypted traffic transparently. The integration ensures multilayer protection with efficient hardware offloading and end-to-end quantum-safe security.

## V. Conclusion

In this work, we demonstrated practical implementations of post-quantum cryptography to secure data transfer at both the Ethernet and IP layers, leveraging specialized Data Processing Units. By combining quantum-resistant MACsec and IPsec protocols, we achieved multilayer protection that enhances the confidentiality, integrity, and authenticity of network communications against quantum-enabled adversaries. Our architecture illustrates how cryptographic agility and hardware offloading can be effectively integrated to build scalable, high-performance, quantum-resilient infrastructures. As quantum computing advances, adopting such hybrid and layered security strategies will be crucial for safeguarding critical systems and maintaining trust in digital communications.

## VI. References


[1] (NIST), National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard (ML-DSA)," U.S. Department of Commerce, 2024.

[2] "National Institute of Standards and Technology (NIST)," U.S. Department of Commerce , FIPS 204: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).

[3] "FIPS 205: Stateless Hash-Based Digital Signature Standard (SPHINCS+)," U.S. Department of Commerce, 2024.

[4] IEEE, "IEEE 802.1AE: Media Access Control (MAC) Security (MACsec) Protocol," IEEE, 2010.

[5] IEEE, "eee standard for local and metropolitan area networks - port-based network access control, 2010. IEEE Std," IEEE, 2010.

[6] IETF, "RFC 4301 — Security Architecture for the Internet Protocol (for IPsec)," IETF, 2005.

[7] Internet Engineering Task Force (IETF), "Internet Key Exchange Protocol Version 2 (IKEv2)," IETF, 2014.

[8] A. Aguilera, C.Rubio, D. Lawo, J. Imana, J. Vegas and I. T. Monroy, "First Demonstration of 200 Gbps Regime Line-Rate Quantum-Secure MACsec Optical Links Using Commodity Hardware Offloads," in *Optical Fiber Communication Conference (OFC)*, San Francisco, 2025.

[9] A. C. Aguilera, R. Abu Bakar, F. Alhamed, C. R. Garcia, J. L. Imaña, I. T. Monroy, F. Cugini and O. J. J. V., "First Line-rate End-to-End Post-Quantum Encrypted Optical Fiber Link Using Data Processing Units (DPUs)," in *Optical Fiber Communication Conference (OFC)*, San Diego, 2024.