Integrating Post-Quantum Cryptography Plugins for IPsec Offloads to Data Processing Units in the Cloud-Edge Continuum

1st Abraham Cano
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
a.c.a.cano.aguilera@tue.nl

2nd Carlos Rubio Garcia
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
c.rubio.garcia@tue.nl

3rd Raphaël Frantz
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
r.r.a.frantz@tue.nl

4th Idelfonso Tafur Monroy
Department of Electrical Engineering
Eindhoven University of Technology
Eindhoven, The Netherlands
i.tafur.monroy@tue.nl

5th José Luis Imaña
Department of Computer Architecture and Automation
Complutense University of Madrid
Madrid, Spain
jluimana@ucm.es

6th Juan José Vegas
Software Architecture
NVIDIA corporation
Yokneam, Israel
juanj@nvidia.com

***Abstract*—The imminent advent of Quantum Computers poses a significant threat to the cryptographic algorithms supporting the public key infrastructure (PKI) of widely used communication protocols. High Performance Computing (HPC) data centers among other interested parties are well aware of the catastrophic consequences quantum attacks could have on their PKI and are consequently transitioning to Post-Quantum Cryptographic (PQC) methods, despite the substantial overhead this introduces for handling incoming network packets. This work addresses the transition to PQC within the context of the Cloud-Edge Continuum by integrating the Open Quantum Safe (OQS) library into the accelerated strongSwan developed by Mellanox for Data Processing Units (DPUs). This integration offloads cryptographic operations from central servers to data DPUs distributed across the cloud-edge continuum. Our solution ensures quantum security by providing PQ authentication through CRYSTALS-Dilithium or CRYSTALS-FALCON, PQ key exchanges via CRYSTALS-Kyber, and confidential data transmission using AES-256. Additionally, the deployment of this implementation on DPUs helps reduce the computational load on both HPC data centers and edge devices, promoting more efficient and secure operations across the entire cloud-edge continuum.**

***Index Terms*—Quantum-resistant cryptography, Cloud-Edge Continuum, network offloads, data processing units, PQ crytography, public key infrastructure**

I. Introduction

Post-quantum Cryptography (PQC) focuses on developing cryptographic algorithms resistant to both classical and quantum attacks. Traditional schemes like RSA [1] and ECC [2], [3] rely on problems such as integer factorization and elliptic curve discrete logarithm, which quantum computers are expected to solve. This has led entities, including governments and cloud providers, to migrate their Public Key Infrastructure (PKI) to withstand quantum threats.

Among the quantum-resistant solutions, PQC and Quantum Key Distribution (QKD) receive significant attention. PQC is favored for its seamless integration with existing infrastructure and comprehensive cryptographic framework, including Key Encapsulation Mechanisms (KEM) , digital signatures, and encryption schemes. In August 2023, NIST proposed standards for Kyber (KEM) [4], and Dilithium [5], Falcon, and Sphincs+ [6] (digital signatures), designed to withstand quantum attacks. Implementing PQC poses challenges due to its computational demands, often making it inefficient on conventional CPUs. Initial PQC implementations on Field-Programmable Gate Arrays (FPGAs) have shown significant speed improvements but come with trade-offs in circuit size and cost.

Beyond High-Performance Computing (HPC) architectures, PQC is also being optimized for microprocessors and constrained devices. For example, the Neon-NTT [7] project provided optimized implementations for ARM Cortex architectures, significantly enhancing performance.

However, the integration of PQC is not just related to one specific type of architecture. The Cloud-Edge Continuum (CEC) is a transformative computing paradigm that integrates the immense computing power and storage capacity of the cloud with localized data processing capabilities of edge, IoT and resource constrained devices. This approach is really useful because combining both technologies can evolve to faster response times, lower latency and more efficient network bandwidth utilization. This paper will explore the integration of Data Processing Units (DPUs) and PQC in the context of CEC.

DPUs are a combination of specialized processors, such as hardware accelerators with energy-efficient processors like ARM cores to offload an accelerate data-intensive tasks that traditionally are perfomed on the CPUs, thereby enhancing system performance and efficiency. In the CEC, DPUs play a crucial role in terms of efficient data handling, network

offloading and providing security between the nodes.
Both KEM and signatures are crucial for various communication protocols. Migrating protocols like IPsec and TLS to PQC is essential, though IPsec has received less attention compared to TLS [8], [9]. Efforts from the IETF have provided drafts for PQ key exchanges in IPsec [10], [11].
This work presents:

- First integration of the Open Quantum Safe (OQS) [12] plugin into an accelerated IPsec software stack
- Benchmarks for all the PQ algorithms implemented in OQS.

The paper is structured as follows: first we introduce a potential architecture employing DPUs on a CEC scenario. Subsequently, the acceralated IPsec architecture section outlines the methodology for integrating PQC into IPsec by offloading its tasks to the DPU and it is followed by experimental results testing all classical, PQC and hybrid schemes (a combination of both technologies) . The conclusion section summarizes the main output results of this work.

II. Data Processing Units on the Cloud-Edge Continuum

In this section, we present a potential architecture (Fig. 1) illustrating how DPUs could be employed in a CEC environment. Constrained devices, such as sensors, may be connected to DPUs A and B which act as edge nodes, which might be used to perform computations over the communication flow, such as encrypting data in transit, all on the Network Interface Card (NIC). This setup frees the main central units (HPC server A and HPC server B) for other tasks.
The relevant information is then forwarded, with the processed data from multiple DPUs routed through a switch to the DPUs hosted on the edge-cloud servers (DPUs C, D, and E). The switch manages data traffic, ensuring high-speed, low-latency transfer, and data integrity. Finally, the edge-cloud servers can perform more sophisticated tasks such as real-time data processing, advanced analytics, machine learning inference, and data storage. They also send control commands back to the DPUs or directly to the constrained devices based on the analyzed data to optimize operations, prevent failures, and maintain efficiency.
In this paper, we will demonstrate the integration of PQC in the communication between HPC servers and the edge, also known as east-west encryption (blue link in Fig. 1), by means of integrating plugins with PQC operations on accelerated software for DPUs. To that end, we need the necessary software to compute IPsec functions. StrongSwan is the most widely adopted software library for implementing IPsec, and as such, there has been extensive research into integrating hardware accelerators for specific cryptographic tasks. However, at present, there is no implementation of post-quantum cryptography with hardware accelerators on StrongSwan for DPUs. The easiest way to achieve quantum-secure IPsec communications is by integrating external plugins within the StrongSwan source code. OQS [12] appears to be the most promising open-source library for implementing post-quantum cryptography. In this article, we focus on integrating a plugin based on OQS into the hardware-accelerated StrongSwan library from Mellanox to achieve both quantum-secure communications and line-rate data encryption.

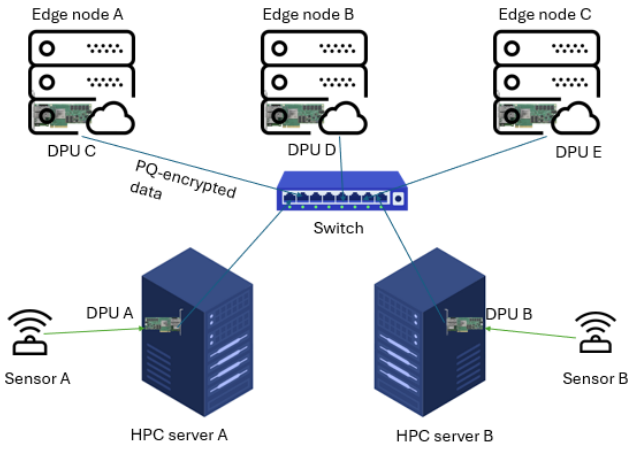

Fig. 1. DPUs on the CEC

III. Accelerated IPsec Architecture

A. PQ-IPsec

Internet Protocol Security (IPsec) and its Internet Key Exchange (IKE) protocol provide encryption, authentication, and integrity protection at the network layer. IPsec is commonly used to secure virtual private networks (VPNs) and communications over insecure channels such as the internet. IKE operates in two phases: the first secures the control plane, and the second protects the data plane by encrypting data with a symmetric cipher. Both phases rely on a PKI stack, and current implementations are based on classical security, which is vulnerable to quantum-enabled adversaries. The classical protocol is summarised in Fig. 2.

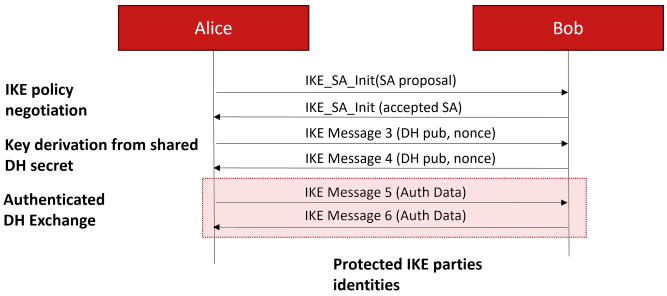

Fig. 2. Classical IPsec protocol phase 1

Which can be decomposed into:

1) Peers agree upon a security association, which includes the security levels and other relevant parameters.
2) A classical Key exchange (KEX) occurs between the peers to exchange a shared secret key (SSK) for encryption.

3) Classical authentication is performed between the peers to validate the server receiving the information.
4) Classical keys are derived through a key derivation function. This include session keys, temporary keys and shared secrets.

In order to extend a classical IPsec to a quantum-resistant one, we use hybrid cryptography, a combination of PQC and classical cryptography. While hybrid cryptography is less performant than classical by virtue of having to compute two key exchanges instead of one, it has the advantage of providing much greater security as the scheme is secure as long as one of the primitives is secure, thus minimizing possible attacks by quantum computers or side channel attacks on PQC [13], making the transition to PQC more reliable and cryptanalysis resistant. A PQ-IPsec application is depicted in Fig. 3, where we can see that through the addition of PQ key exchanges and the mixing of the keys through Pseudo Random Function (PRF) one can achieve quantum-resistant communications.

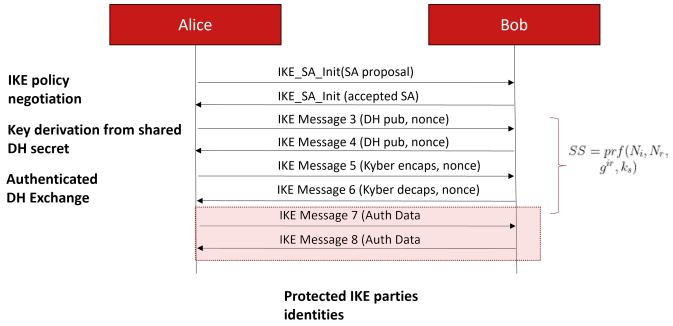

Fig. 3. PQ IPsec protocol phase 1

B. Integration of PQ plugins in IPsec

In order to obtain a quantum-resistant IPsec, it is necessary to provide the necessary software stack to compute PQC efficiently. However, PQC is not enough since it also needs to be integrated within current communication software frameworks to ensure seamless functionality and compatibility. Integrating PQ plugins in Strongswan is crucial as it enables the implementation of quantum-resistant cryptographic algorithms within the widely-used IPsec protocol. This integration ensures that encrypted communications remain secure against potential quantum computing attacks, thus preserving the confidentiality and integrity of sensitive data in the face of advancing technological threats.

We decided to integrate the OQS code, the most well-known library for PQ-cryptography which is employed in numerous projects like PQ-TLS [8] and which implements Dilithium, Falcon, Kyber and Sphincs+ among other pq cryptographic schemes. In Fig. 4, we can see the file system architecture for the integration of the OQS plugin within mellanox strongswan [14]. In that case the PQ algorithms are implemented by OQS shared library while the mellanox strongswan code provides the necessary framework to register such algorithm by means of the asn1.c and oid.txt files and to call such algorithms within the IKE. To that end, the files in credentials must be updated to call Dilithium, Falcon and Sphincs+ and the file key_exchange.c within the crypto directory to call kyber operations and to perform the key mixing of the keys via the PRF. The rest of the changes are the definition of PQ digital signatures in the plugins used for certificate handling, i.e pkcs8 and pem and the redefinition of the pki tool for generate PQ certificates.

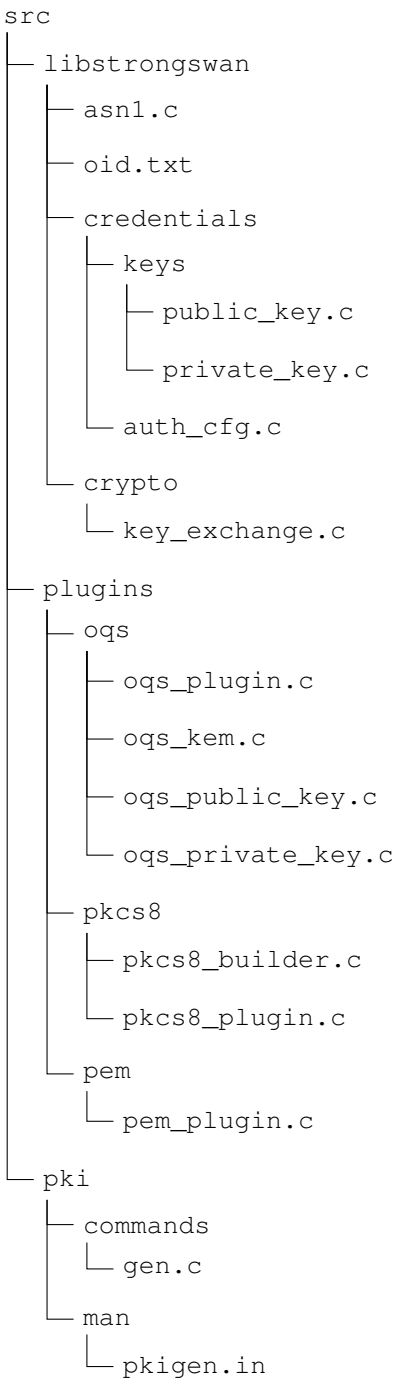

Fig. 4. File System Diagram of the integration of OQS in strongswan Mellanox

C. Offloading to DPUs

Such cryptographic operations are expensive and thus, general purpose processors might get overwhelmed when making computations in real time. To address that issue, offloads to cryptographic oriented devices have been considered; FPGAs being the best positioned due to their performance. However, such offloads might not have the expected outcome if the delays between the operations carried out in the devices and the NICs are bigger than the improvement in the computation of cryptographic operations, thus making FPGAs impractical in real-case scenarios [15].

Given that FPGAs are impractical for line-rate encryption of data, we propose the use of DPUs to leverage the cryptographic operations involved in strongswan. To that end we offload the heavy cryptographic operations in strongswan to the DPU. The whole procedure is exposed in Fig 5 in which servers offload the request of an IPsec connection to the DPU through Remote direct memory access (RDMA). Then the DPUs would use the ARM8 cores to perform simple tasks and use the IPsec accelerated strongswan with the OQS plugin for PQC. Strongswan makes also use of the openssl plugin to use an openssl engine based on dedicated hardware to accelerate both classical cryptographic operations and symmetric cryptography. This engine is connected to HW accelerators designated for accelerating symmetric cryptography.

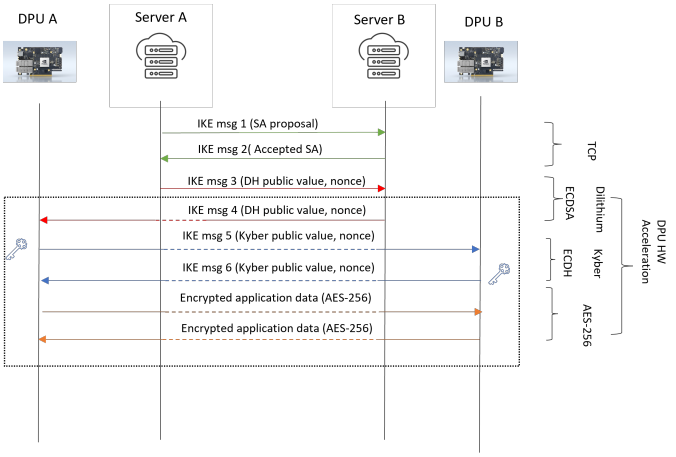

Fig. 5. Architecture of accelerated IPsec using the OQS plugin. All the PQ-operations and encryption of data are offload to the DPUs which by means of the HW accelerators can boost the performance of the quantum-resistant communications.

IV. Results

This section shows the experimental results of our implementation of the OQS plugin within the mellanox strongswan. We provide results for both line-rate cryptography, handshake authentication and handhsake key-exchange. For each of the schemes we provide the results based on its security level according to NIST. In that case, following an ascendant security order we have tested Kyber512, Kyber768, Kyber1024, Dilithium2, Dilithium3, Dilithium5, and the ECDH and ECDSA variants of the curves P-192, P-224, P-384 and P-512.

A. Handshake signatures

In Fig 6 we expose the throughput achieved by the Classical, Hybrid and PQ-signatures integrated in the OQS plugin within IPsec. Sphincs+ provides the lowest throughput due to the complexity of computing hash-based signatures. This issue is more pronounced in the hybrid set-up due to the necessity of computing more than one signature for each certificate. Falcon achieves the highest verification throughput, while Dilithium offers the best trade-off between signing and verifying. Finally, we can see that the best balance between security and performance it is offered by a combination between ECDSA and Dilithium/Falcon showing that hybrid schemes can still be competitive and provide a seamless transition to quantum-resistant cryptography. We can also observe that other schemes, such as Sphincs+, exhibit worse performance compared to their post-quantum counterparts. This is because Sphincs+ relies on the hardness of hash functions, whereas Dilithium and Falcon are based on lattice cryptography. While Falcon and Dilithium are likely to become the most widely adopted solutions due to their superior performance, their security properties have been less extensively studied than those of hash-based systems. Therefore, Sphincs+ may be preferred in scenarios where security is the primary concern, and bandwidth limitations are not an issue.

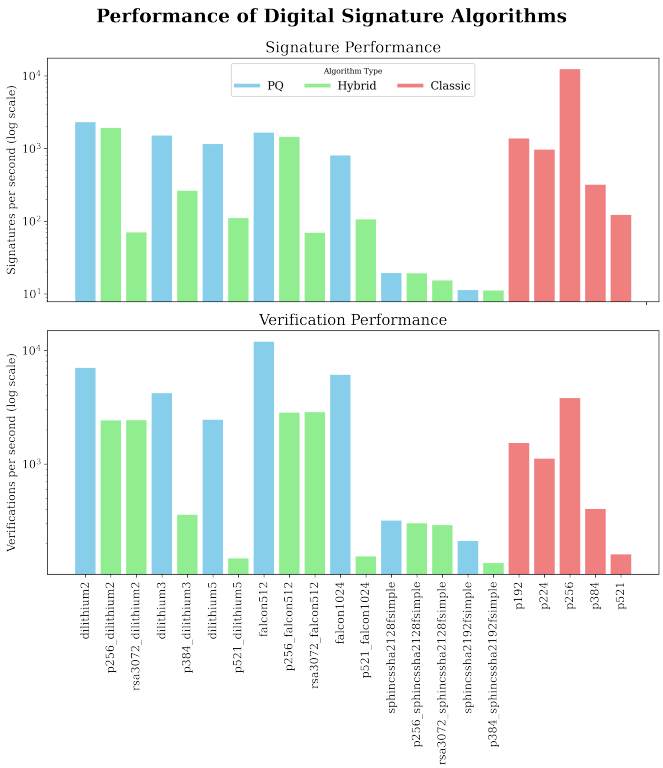

Fig. 6. Throughput of Classical, Hybrid and PQ-only signatures provided by the OQS plugin in mellanox strongswan when executed on DPUs.

B. Handshake key-exchanges

In high-performance computing data centers it is essential to compute many key-exchanges between the two nodes involved in the communication. Maximizing the keys exchanged per second is of paramount importance in order to not overwhelm the network when multiple connections are trying to send data. Fig 7 illustrates the experimental results of exchanging keys through our optical point-to-point link. Even though PQC has bigger public and secret key sizes its computation is faster and thus it is ideal in all scenarios but the ones with constrained memory.

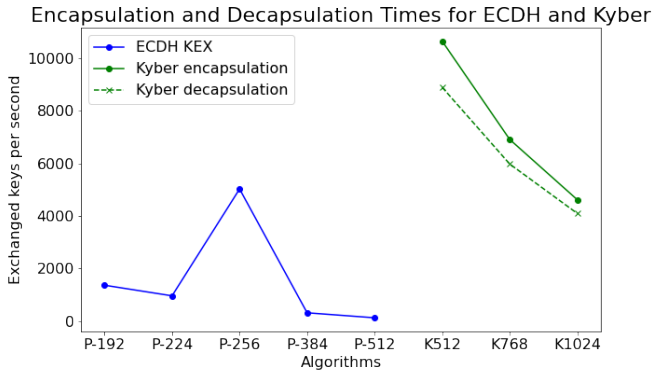

Fig. 7. Throughput of Classical, Hybrid and PQ-only signatures provided by the OQS plugin in mellanox strongswan while executed on DPUs.

C. In-line rate cryptography

Despite the necessity of PQC for public key system and its crucial role in authentication and key exchange within the IKE, the most computationally demanding part in any secure communication system lies in encrypting the data plane. Fig. 8 illustrates the throughput of our optical link based on the size of the Maximum Transmission Unit (MTU). For our experiment we considered two scenarios; sending data on clear, i.e plaintext, which is vulnerable since it does not provide any kind of confidentiality (maximum expected throughput) and encrypting the data with an IPsec tunnel established between the DPUs. The graph demonstrates that there is a small penalty wehn implementing the IPsec tunnel between the two DPUs. This penalty becomes more pronounced when increasing the MTU sizes, however all these penaltis are always under the threshold of 10% making DPUs an attractive alternative to encrypt data at high speed while liberating resources in the data-center.

V. Conclusions

This work presents a significant advancement in the field of HPC data center communication within the CEC. For the first time, a OQ plugin has been succesfully integrated into an accelerated IPsec software stack, specifically Mellanox StrongSwan. The results of this workre promising since they can be extended to many other user applications that require

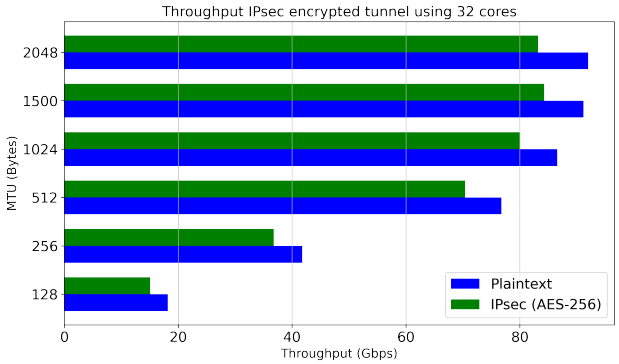

Fig. 8. Comparison of throughput of data encrypted with AES-256 supplied by PQ keys and throughput of plaintext messages.

communication point-to-point, thus providing secrue line-rate quantum resistant communications between independent servers.

In this research, it has been highlighted that hybrid signatrues and KEXs offer competitive performance, therefore they seem a potential solution for a short-term transition towards PQC. Additionally, with the utilization of DPUs for offloading, it becomes feasible to encrypt data with only a marginal penalty, making quantum resistant communication scalable within CEC environments and HPC data enters.

Acknowledgment

This work was partly funded by the QUARC project by the European Union Horizon Europe research and innovation program within the framework of Marie Skłodowska-Curie Actions with grant number 101073355, and by the grant PID2021-123041OB-I00 funded by MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe".

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, p. 120–126, feb 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[2] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, "Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography," 2018-04-16 2018.

[3] L. Chen, D. Moody, A. Regenscheid, and A. Robinson, "Digital signature standard (dss)," 2023-02-02 05:02:00 2023.

[4] National Institute of Standards and Technology, "Module-lattice-based key encapsulation mechanism standard," Department of Commerce, Washington, D.C., Federal Information Processing Standards Publication (FIPS) NIST FIPS 203 ipd, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.203.ipd

[5] ——, "Module-lattice-based digital signature standard," Department of Commerce, Washington, D.C., Federal Information Processing Standards Publication (FIPS) NIST FIPS 204 ipd, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.204.ipd

[6] ——, "Stateless hash-based digital signature standard," Department of Commerce, Washington, D.C., Federal Information Processing Standards Publication (FIPS) NIST FIPS 205 ipd, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.205.ipd

[7] D. O. C. Greconici, M. J. Kannwischer, and A. Sprenkels, "Compact dilithium implementations on cortex-m3 and cortex-m4," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2021, no. 1, p. 1–24, Dec. 2020. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8725

[8] M. Sosnowski, F. Wiedner, E. Hauser, L. Steger, D. Schoinianakis, S. Gallenmüller, and G. Carle, "The performance of post-quantum tls 1.3," in *Companion of the 19th International Conference on Emerging Networking EXperiments and Technologies*, ser. CoNEXT 2023. New York, NY, USA: Association for Computing Machinery, 2023, p. 19–27. [Online]. Available: https://doi.org/10.1145/3624354.3630585

[9] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Assessing the overhead of post-quantum cryptography in tls 1.3 and ssh," in *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, ser. CoNEXT '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 149–156. [Online]. Available: https://doi.org/10.1145/3386367.3431305

[10] S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security," RFC 8784, Jun. 2020. [Online]. Available: https://www.rfc-editor.org/info/rfc8784

[11] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. V. Geest, O. Garcia-Morchon, and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 9370, May 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9370

[12] O. Q. Safe, "liboqs: C library for quantum-resistant cryptographic algorithms," 2023. [Online]. Available: https://github.com/open-quantum-safe/liboqs

[13] E. Dubrova, K. Ngo, J. Gärtner, and R. Wang, "Breaking a fifth-order masked implementation of crystals-kyber by copy-paste," in *Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop*, ser. APKC '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 10–20. [Online]. Available: https://doi.org/10.1145/3591866.3593072

[14] Mellanox, "Mellanox strongswan," https://github.com/Mellanox/strongswan, 2022.

[15] E. F. Kfoury, S. Choueiri, A. Mazloum, A. AlSabeh, J. Gomez, and J. Crichigno, "A comprehensive survey on smartnics: Architectures, development models, applications, and research directions," *IEEE Access*, vol. 12, p. 107297–107336, 2024. [Online]. Available: http://dx.doi.org/10.1109/ACCESS.2024.3437203