Implementation and Comparison of Dilithium/Kyber and Falcon/Kyber PQC software stack on data processing units

D. C. Lawo[1,2], R. Frantz[1,2], A. Cano Aguilera[1,2], I. Tafur Monroy[1], and J.J. Vegas Olmos[2]

[1] Department of Electrical Engineering, Eindhoven University of Technology, Eindhoven, Netherlands
[2] Software Architecture, NVIDIA Corporation, Ofer Industrial Park Yokneam, Israel

The expected arrival of powerful quantum computers within the near future represents a great challenge to our modern-day cryptography. Symmetric key encryption is not considered to be vulnerable against attacks by quantum computers if the key size is doubled. Asymmetric cryptography, however, is shown to be susceptible to quantum attacks. In this paper we present an implementation of the NIST Post-Quantum Cryptography (PQC) finalists Falcon, Dilithium and Kyber on two data center grade data processing units. We compare the resulting characteristics against each other and examine use-cases for both cryptographic stacks, Dilithium/Kyber and Falcon/Kyber. The Dilithium/Kyber protocol proves to be faster but consumes more resources than the combination of Falcon/Kyber. This implies the use of Dilithium/Kyber in a data center environment while Falcon/Kyber could be more suitable for mobile applications with limited network and computing power.

Introduction

The great potential offered by quantum computing is being researched since many years. We expect to see a quantum computer within the next years. Prototype systems, digital annealers and quantum annealers that are based on comparable principles are already available. Unlike classical computers, however, computers working with quantum principles are said to be capable of breaking our most commonly used asymmetric cryptographic procedures, e.g. RSA [1]. Their emergence thereby represents a crucial challenge for the security and privacy of our commonly used communications infrastructure. The fact that everything is moving towards the cloud hence requiring more communication aggravates the potential danger further. Figure 1 shows schematically the Edge-Cloud Continuum. Herein, all devices exchange information using digital protocols, e.g. TLS [2]. In terms of communication protocols, asymmetric cryptography is responsible for digital signature algorithms and key exchange mechanisms (KEMs). Although asymmetric cryptography is expected to be broken, symmetric cryptography, e.g. AES, is assumed to be resilient against attacks by quantum computers as long as the key sizes in use are doubled [3]. We envision that every single exemplary link within the figure will be communicating quantum safely via post-quantum cryptography. The choice of algorithms the individual links encrypt their data with may differ due to the links' and the devices' capabilities

To mitigate this thread, the American National Institute of Standards and Technology (NIST) organized a competition [4]. The purpose of this competition is to find asymmetric cryptography schemes that fulfill not only the safety requirements to withstand attacks by classical computers but by quantum computers as well.

As of now, there are three candidates for digital signatures remaining in the NIST competition. These three candidates are called: Crystals-Dilithium, Falcon, and Sphincs+. Moreover, there is only one KEM algorithm, Crystals-Kyber, remaining in the NIST competition.

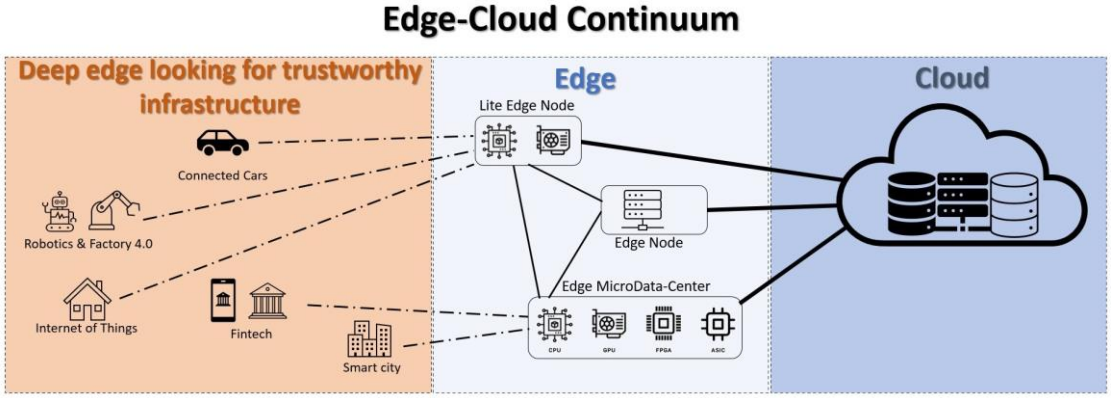

Figure 1. Edge-Cloud Continuum: Multiple different devices offload their computational tasks via the edge towards the cloud. They use PQC to encrypt their communications. Depending on the devices' capabilities and the available network bandwidth they use different PQC algorithms.

Remaining NIST candidates

A digital signature serves to ensure the identity of one communicating party. As mentioned in the previous section, the three remaining candidates for signature algorithms are Dilithium, Falcon, and Sphincs+. The security of Sphincs+ is based on hashing, a well understood technique. It offers three different parameter sets that satisfy the NIST security levels 1, 3, and 5 [5]. The other two signature algorithms, Falcon and Dilithium, are using mathematical lattices to achieve their security. Falcon has two security levels equivalent to the NIST levels 1 and 5 [6] while Dilithium has three levels that provide for NIST security levels 2, 3, and 5 [7]. Of course, the algorithms differ in a variety of characteristics. For now, Kyber is the last remaining KEM in the competition and is therefore likely to be part of the standardization. The algorithm has a 512 bit, a 768 bit, and a 1024 bit version that satisfy NIST level 1, 3, and 5, respectively [8]. Hence, a PQC handshake could be Sphincs+, Dilithium, or Falcon for digital identification followed by Kyber for the key exchange. Ultimately, the communication is encrypted by AES. The NIST recommends Dilithium and Kyber as standard due to their strong performance and high safety standards. Falcon and Kyber could be employed for use cases where the availability of network resources is limited due to Falcon's smaller signature size. Sphincs+ is also standardized in order to not only rely on the security of lattices. The security of Sphincs+ is considered to be excellent. However, the performance of Sphincs+ is significantly poorer compared to Falcon and Dilithium.

Experimental Setup

The setup with that the herein presented results have been achieved is shown in fig. 2. It is similar to the one used in [9]. Two Dell PowerEdge R750[1] are each equipped with one Nvidia BlueField 2 MBF2M516A-CEEO[2] data processing unit (DPU). Both DPUs are capable of transmitting at linerate speed of up to 100 Gb/s. They are connected to each other point-to-point using a copper cable. Moreover, the DPUs have eight on-board

[1]https://i.dell.com/sites/csdocuments/Product_Docs/en/poweredge-r750-spec-sheet.pd

[2] https://docs.nvidia.com/networking/display/bluefield2DPUENUG/specifications

ARMv8 processors clocked at 2750 MHz. Additionally, they have dedicated hardware acceleration capabilities at their disposal, for example for AES.

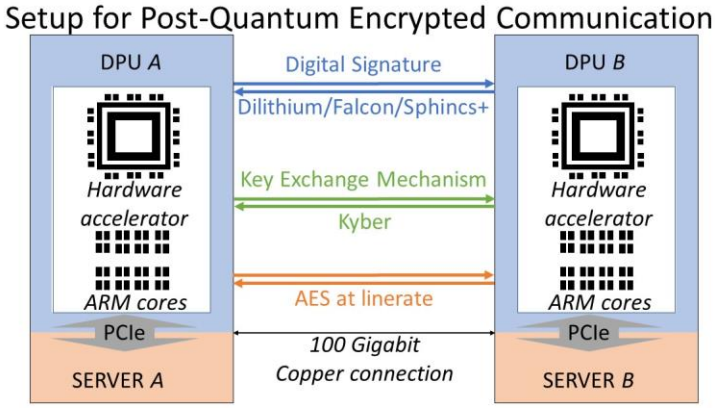

Figure 2. Two Nvidia Bluefield 2 DPUs establish post-quantum encrypted communication. They first use a PQC signature scheme for authentication, then Kyber to exchange keys, and finally AES.

Results

The signature algorithms have three main functions: the generation of a key pair, sign and verify. KEMs also have three main functions: as well the generation of a key pair, the key decapsulation, and the key encapsulation. The respective three main functions have been benchmark in terms of required cpu cycles per execution. The results are shown in fig. 3. The red bars represent the highest security version of the algorithm which is NIST level 5 for all presented algorithms. The green bars show the results of Falcon 1, Dilithium 3, and Kyber 3. Finally, the blue graph shows Dilithium 2, Kyber 2, and a 256 bit Falcon version that is not NIST secure but included for research purposes. Upgrading the security level of Kyber comes with a relatively small computationally penalty compared to the other security levels.

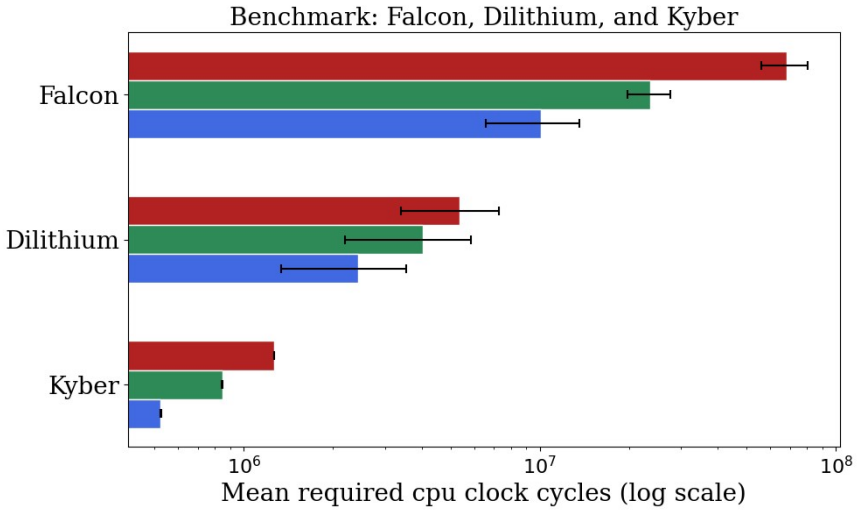

Figure 3. Benchmark in terms of cpu cycles per execution of the three main functions of Falcon, Dilithium, and Kyber performed on Nvidia Bluefield 2 DPU platform. Red represents the highest available NIST version of the algorithm, green the midlevel, and blue the lowest available level of the Implementations. Falcon only has two NIST levels, 1 and 5, but the reference implementation includes a 256 bit version that is not considered NIST secure. It is represented by the blue graph.

Falcon stands out because it is computationally very challenging with respect to Dilithium. This is due to the fact that Falcon's key generation requires intense computational steps. However, this step must be performed only once in a classic TLS procedure. To give an example, in fig. 1 when edge and cloud are communicating, powerful machines are involved, and the network bandwidth will not be a bottleneck. Hence, they will likely use Dilithium for its good performance. However, when the edge corresponds with mobile devices, the edge will likely be more powerful than the mobile device and the available network bandwidth will be limited. Hence, Falcon could be a good choice. Our results are in line with the NIST findings [4].

Conclusion

Kyber is the only remaining KEM in the NIST competition. Hence, it is very likely that Kyber will be a part of a PQC cryptography stack. Regarding signature algorithms, however, three algorithms are competing. Due to their different characteristics, we predict that they will be bound to coexist rather than one fits all use cases. Based on the available resources, such as processing power or network bandwidth, the users will employ the signature algorithm, as well as the NIST safety level that fit their purposes. Furthermore, different algorithms will likely be used in different network segments. Dilithium will be used in environments where resources are not an issue while Falcon will probably be used in circumstances where resources are limited, such as battery driven devices or low network bandwidth is at the users' disposal.

Acknowledgements

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 the CLEVER project by the Key Digital Technologies Joint Undertaking program with grant number 10109756.

References

[1] M. Sharma et al., "Leveraging the power of quantum computing for breaking rsa encryption," Cyber-Physical Syst. 7, 73–92, 2021.
[2] Eric Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, 2018.
[3] X. Bonnetain et al. "Quantum Security Analysis of AES," IACR Transactions on Symmetric Cryptology, 55–93, 2019.
[4] G. Alagic et al. "Status report on the third round of the nist post-quantum cryptography standardization process," https://doi.org/10.6028/NIST.IR.8413-upd1, 2022.
[5] D. J. Bernstein et al., "The SPHINCS+ signature framework", In CCS 2019 - Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2129-2146), 2019.
[6] P.-A. Fouque et al., "Fast-Fourier Lattice-based Compact Signatures over NTRU", Submission to the NIST's post-quantum cryptography standardization process, 2018.
[7] L. Ducas et al., "Crystals-dilithium: A lattice-based digital signature scheme", IACR Transactions on Cryptogr. Hardw. Embed. Syst., 238-268, 2018.
[8] J. Bos et al., "Crystals - kyber: A cca-secure module-lattice-based kem," in 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 353–367, 2018.
[9] A. C. Aguilera et al., "First end-to-end PQC protected DPU-to-DPU communications", Electron. Lett., 59: e12901, 2023.