Recent Advances in Post-Quantum Cryptography for Networks: A Survey

Conference Paper · February 2022

DOI: 10.1109/MobiSecServ50855.2022.9727214

4 authors, including:

Engin Zeydan
CTTC Catalan Telecommunications Technology Centre
134 PUBLICATIONS **1,298** CITATIONS
SEE PROFILE

Buğrahan Saim Öztürk
ASELSAN Inc.
3 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Recent Advances in Post-Quantum Cryptography for Networks: A Survey

Engin Zeydan*, Yekta Turk◇, Berkin Aksoy◇ and S. Bugrahan Ozturk◇
*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Castelldefels, Barcelona, Spain, 08860.
◇Aselsan Corp., Istanbul, Turkey, 34396.
engin.zeydan@cttc.cat, [yektaturk, berkinaksoy, sbozturk]@aselsan.com.tr

***Abstract*—The development of quantum computers poses a new security threat to network infrastructures and services, as they will be powerful enough to break the most common forms of digital encryption. Existing encryption services based on Rivest–Shamir–Adleman (RSA), Diffie-Hellman (DH), Elliptic Curve Cryptography (ECC) and so on are vulnerable to attacks by quantum computers. Although the gap between today's quantum computers and the threats they pose to current public-key cryptography is large, the telecommunications landscape should begin planning for the transition to the post-quantum era as early as possible. In this paper, we examine recent advances in Post Quantum Cryptography (PQC) algorithms from the perspective of the networking and telecommunications industries. The efforts are categorized at three levels, namely communication, computation (consisting of design, implementation and Public Key System (PKS)), and network. Some of the existing challenges and future recommendations for securing communication networks in the post-quantum era are also listed at the end of the paper.**

***Keywords*—post-quantum, cryptography, security, survey.**

I. Introduction

Currently, the modern world relies on the concept of public key cryptography for secure communication which is a foundation for Public Key Infrastructure (PKI). PKIs play a key role in protecting all stages of product development and their distribution in production environments. It has been found that the factorization problem, which is a hard problem, can be cracked using quantum computers [1]. This is actually one of the first known proof of the power of quantum computers which can be used to break todays' public-key cryptography in the future. It may also give an indication of what problems can be solved in the future. Using Shor's factoring algorithm [2] and Grover's search algorithm [3], quantum computers can solve the problems behind the security of popular cryptographic primitives in polynomial time (e.g., solutions to factorization and discrete logarithm problems can break Rivest–Shamir–Adleman (RSA) and Elliptic-Curve Cryptography (ECC) respectively). Enterprises such as Amazon, IBM, Google, and Microsoft have already launched commercial limited quantum-computing cloud services. Schnorr's algorithms is expected to break RSA-2048 with 4096-qubits quantum computer [4].

Hash algorithms such as Secure Hash Algorithm (SHA)-2, SHA-3 are evaluated as quantum-secure. SHA-256 already has the minimum number of operations as $2^{(256/2)}$ due to the birthday paradox. In the post-quantum era, the complexity of finding a collision reduces to $2^{(256/3)}$ in quantum computers after efficient search of Grover's algorithm. Nowadays, the lack of demonstrations could lead one to believe that the performance of quantum computers is limited by decrypting RSA or ECC. It is not certain whether large-scale and robust quantum computers (with millions of so-called qubits) will be built in the next decade. To make an estimate, physicists have shown that the number of entangled particles that are important for quantum computers could be in the millions [5]. In this case, the creation of partial states could provide more parallel processing capacity than expected. Moreover, algorithms that reduce quantum complexity will push the limits of quantum computers. However, the planning of migration to the world of PQC should start as early as possible for telecommunication ecosystem. PQC algorithms are researched at great expense and are currently being standardized by National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization.

Our main observations during surveying recent works on networking with PQC can be summarized as follows. Currently, recent frameworks and platforms that enable networking with PQC are mainly focused on academia and research labs rather than industry. Therefore, com-

mercial development and deployment of PQC-driven networking services are not yet on the rise. On the other hand, thanks to advances in algorithms coupled with hardware design and vectorized operations, significant advances in post-quantum techniques are expected to influence the transfer of this knowledge into practical applications or commercial products and services in telecommunications and networks in the coming decades. Moreover, we evaluate that the PQC driven network services concept can progress from academia to real-world applications. However, the standardization efforts are currently at their infancy period. Furthermore, developing specific hardware/software that supports post-quantum algorithms (which can be either expensive, time-consuming, or impractical) is a major challenge, both in terms of standardization and platform development. The rest of the paper is organized as follows: Section II describes the technology development life-cycle and its components. Section III discusses about the developments for post-quantum networking with the outcomes of the survey and give future directions. Finally, in Section IV, we give conclusions.

II. Post-Quantum Networking Technology Development Life-Cycle

A. Life-Cycle Components

Fig. 1 shows the post quantum technology development life cycle from telecommunication perspective. In this figure, there are mainly three different layers, namely, communications, computation and network. In general, Fig. 1 shows how post-quantum technology is evolving for networking from different perspectives (in terms of device and network) and how different developments affect each other.

1-) Communication: Post-quantum era will first change the security protocol that will be used for communication between the end-points. From a device perspective, the protocol will have the most impact on the device architecture and is involved in the communication layer of Fig. 1. End-to-end protection requires authentication, key exchange and transport protection. The protocols will allow different nodes to coordinate with each other for quantum-secure communication. However, the cryptographic algorithms that will be included in the protocol will change. In this case, it should be assessed how existing methods will evolve and what impact post-quantum technology will have on existing protocols [6]. These assessments have been made, for example, for the Transport Layer Security (TLS) protocol, which is used in many places, especially in web applications [7].

Similar studies are needed for other protocols such as Datagram Transport Layer Security (DTLS), Internet Protocol Security (IPSec), Wi-Fi Protected Access 3 (WPA3), etc. These evaluations will show whether the new algorithms are suitable for use in existing protocols [8]. If algorithms cannot be integrated into existing protocols, new protocols must be created. Even if algorithms can be implemented in protocols, there may be slowdowns that fall short of performance expectations. In this case, the performance of protocols using post-quantum algorithms should also be evaluated [9]. The high degree of slowness in protocols will also affect protocol redesign.

The protocols affected by quantum computers can be classified based on three dimensions of telecommunications products:

- **In user equipments (UEs) and digital signatures** mainly asymmetric cryptography based on RSA, Diffie–Hellman (DH) or Elliptic Curve Digital Signature Algorithm (ECDSA) will be vulnerable due to Shor's algorithm which can solve factorization and discrete logarithm problem in polynomial time.
- **For encrypted data and data centers** symmetric cryptography needs to be upgraded due to the efficient search optimization of Grover's algorithm. This can compromise encrypted data stored in online databases if they are kept significant in time.
- **Blockchain networks** commonly use Hash functions in blocks of the public ledger. Although hash functions are irreversible and there is no immediate threat from quantum computing, Grover's efficient search algorithms can help reduce the bit security level to third of their original value (although still a large number of search attempts exist).

2-) Computation: is mainly divided into three different categories, namely, design, Public Key System (PKS) and implementation.

(i) Design: The protocols to be used indicate how the design phase should be arranged. This allows devices to run post-quantum protocols and create a *secure processing* environment. The decisions during the feasibility study of the design are key factors influencing the final product. These decisions are the selection of the algorithm, selection of the appropriate computation technique (Karatsuba, Toom-Cook, etc.), power consumption anal-

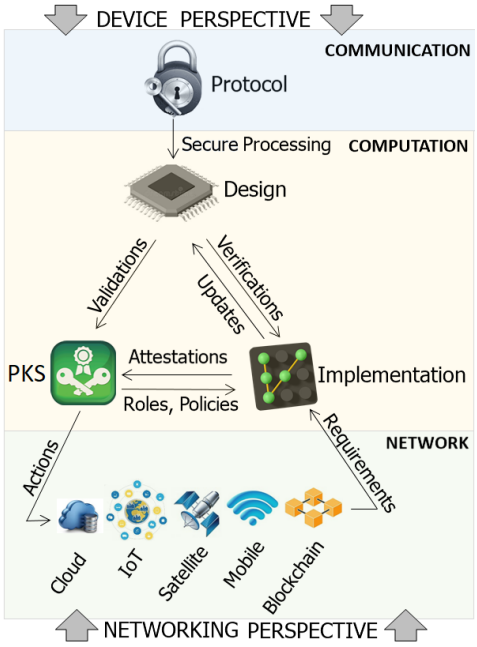

Fig. 1: Illustration of post-quantum technology development life-cycle and interactions of life-cycle components in different levels.

ysis, robustness against side-channel attacks, response time of the device for encryption/decryption, etc. that are evaluated based on the network use case. Use cases may involve the satellite networks, 5G communication systems or heterogeneous deployment scenarios [10]. A detailed functionality study with well reasoned choices such as the processor subsystem, Field-Programmable Gate Array (FPGA) model, power supply, possible operating system (OS) type, etc. are essential for the implementation phase [11]. Thus, a specified security architecture with determining the functional components on the selected software/hardware can be designed.

Post-quantum algorithms need to be designed in a way to accelerate the protocol that is based on the implemented algorithm and make appropriate use of device resources [12]. There are several candidates to PQC algorithms in the NIST standardization. For Key Encapsulation Mechanism (KEM) candidates, NTRU (lattice-based), Kyber (lattice-based), SABER (lattice-based), Classic McEliece (code-based), SIKE (isogeny-based). For digital signature candidates Falcon (lattice-based), Dilithium (lattice-based), Rainbow (multivariate-based), SPHINCS+ (stateless hash-based).

Most of the network devices have conceptual model called *planes*. In general, these *planes* describe how packets travel to, from, and through a network device. Control plane describes the decisions of a node in the network. Data plane can be summarized as the high speed path. In the design process these concepts needs to be turned into software/hardware component. To accelerate the overall performance of the post-quantum cryptographic protocol, studies to accelerate these components independently can be done. The acceleration can be performed in the processor level [13], [14] or in System-on-Chip (SoC) with granularity of the instruction set level [15].

(ii) PKS: is the overall system that allows all parties to cooperate in PKI as well as in an insecure network structure. The main components of PKS include the key distribution mechanism, digital signatures, challenge-response based identification protocols, and encryption/decryption operations. Existing primitives used in PKI should be replaced to ensure quantum-safe computations. The main reason is that it is not enough to just reconsider the key size. There must be a trusted association between the PKI server and between the network devices. The trusted association during the key distribution phase may be performed by a cryptographic binding of the key and the digital signature of the PKI entities. The trusted association between network devices may be enforced by a trusted process (e.g., key exchange prior to the communication proves the opposite entity is known and trusted.)

For practical use of the developed PQC, alternative approaches can be used to solve the structural problems of huge amounts of key data and relatively low data rate by exploring the use of different data representation techniques. [16], [17]. Security extensions such as (authentication, randomness, etc.) can also be added to the currently used PKS architectures [18], [19]. Quantum Key Distribution (QKD), PQC or hybrid quantum-secured cryptography are some ways to solve problems related to key distribution and digital signatures which are currently based on public-key cryptography principles.

(iii) Implementation: A significant portion of the computational cost of PQC algorithms comes from high-order polynomial or matrix-vector products. NIST emphasizes that in the PQC standardization, besides security against difficult problems and quantum threats on which the algorithms are based, an efficient, platform-compatible implementation will be an important criterion for the selection of the algorithm to be standardized. For

this reason, the efficient use of multiplication methods such as NTT, Toom-Cook, Karatsuba, etc. occupies an important place in the software and hardware implementation of algorithms.

Performance analysis multiplication techniques (Toom-Cook and Karatsuba), which are among the main building blocks of PQC algorithms implemented with parallel computing techniques based on the number of processors and hardware platform utilization in the network was given in [20]. Therefore, post-quantum algorithms can be implemented in hardware or software and implementation phases can vary [21]. For example, device specific constraints can be solved by using various hardware entities such as Graphical Processing Units (GPUs), memory caches, etc. Thus, runtime computation schemes can be accelerated [22], [23]. Another approach is to use post-quantum techniques for internal security of devices by allowing secure boot and secure software update services. Moreover, hardware entities can be used to offload key storage to the hardware [24].

Post-quantum algorithm implementations can run on software within the operating system. Hardware may be processors or customized FPGAs [25]. For applications with low network traffic, encryption operations can work well without adding extra latency. However, this design perspective for low network traffic can create problems for high network traffic applications, however optimizations can be done using various alternative methods (e.g. changing the digital signature schemes, offloading software tasks to hardware, FPGA module re-design) [26], [27]

3-) Network: At the network layer, the adaptation of post-quantum technologies to various network technologies such as wired, wireless, cloud and Internet of Things (IoT) as well as the devices designed for these technologies are discussed. Nowadays, telecommunication providers want to deliver both high capacity and low latency in 5G and 6G with a scalable and security effective approach. Therefore, security in the post-quantum era for next-generation cellular networks should be considered at the design stage [28]. Some security functionalities such as primary authentication, access key management, identification, ciphering and generation of integrity protection keys should be reconsidered. These evaluation of these functionalities must also take into account the security of the air interface of cellular systems [29].

IoT devices will be supported in new cellular systems and there will be a significant need to develop security methods specifically for the IoT domain [30]. Processing IoT data obtained at the edge of the network is a concept that is trending in recent years due to low latency requirements. However, data obtained at the edge may require long-term protection over periods of ten or more years. This long-term security can be achieved with post-quantum cryptography [31]. Communication between edge and cloud can be secured by information-theoretic security with public-key cryptography [32]. Blockchain architecture can be used to synchronize and protect edge data in a distributed manner. Unfortunately, transactions based on currently used digital signature methods are inherently vulnerable to quantum attacks. Therefore, these digital signatures need to be improved by using Post-Quantum Signatures [33] for blockchain transactions.

B. Interactions

In this section, we discuss the interaction between the components of the technology lifecycle depicted in Fig. 1, which are at different levels. A development in one of the defined components of the lifecycle also affects other components. The direction of this interaction is also shown in this figure. From the perspective of the device, the most important unit of development is initially the security protocol of the device. Which protocol is used depends on what functions the system will perform. The security applications and protocols that an edge/cloud system and an IoT device with post-quantum cryptography will provide differ. While lightweight protocols will work in IoT devices or there will be protocols that work in lower latency satellite systems, the encryption keys in cloud systems will be longer and higher level of security protocols will be used. In this context, the input describing how *Secure Processing* will be is transferred to the computation level.

In the computation layer, Design provides the input to PKS and Implementation. The Design also specifies the *Verification* steps to complete the implementation in software/hardware. If the implementation cannot implement the design (e.g., because GPU acceleration is not possible or code is written that consumes too many device resources), the Implementation provides the necessary *Updates* to update the design. The *Validation* that the protocol works in accordance with the entire network comes out in the PKS environment. A device that is not compatible with PKS cannot safely communicate with

TABLE I

CHARACTERISTICS OF LEVELS FOR POST-QUANTUM NETWORKING & CORRESPONDING RELATED WORKS

Levels		Characteristics	Related Works
Communication		— Higher-level declaration of impact for security on communication networks. — Provide evaluation on existing protocols and perform enhancements. — Detect performance of post-quantum algorithms on protocols and resolve by new design.	[1], [2], [3], [4] [6], [7] [8], [9]
Computation	**Design**	— Model the security architecture that maps functional components on software/hardware. — Design structural properties at the granularity of the network node's components. — Develop optimal solutions with reasonable computational resources.	[10], [11] [12] [13], [14], [15]
	PKS	— Manage public-key encryption to validate the information being transferred. — Define entities to securely communicate over an insecure network.	[16], [17] [18], [19]
	Implementation	— Investigate the hardware/software compatibility challenges and capability enhancements. — Provide competitive run-time scheme against device specific constraints. — Demonstrate the performance of the cryptosystem and focus on optimization of the code.	[20], [21] [22], [23], [24] [25], [26], [27]
Network		— Provide requirements specified to the network technology to consume resources effectively. — Allowing shorter signatures, faster key generation, signing and verification time. — Detect and resolve vulnerabilities with alternative approaches.	[28], [30], [31], [34] [29], [33] [32], [35]

other devices on the network. With PKS, the rules for how devices on the network operate (master, slave, peer-to-peer communication, key exchange roles, CA/Sub-CA signature control, etc.) are provided to the Implementation with *Roles, policies*. *Attestations* ensures that the correct roles and policies are implemented and that the device works harmoniously in the PKS system.

PKS defines the *Actions* for the key, signature distribution processes of the devices at the network level. However, each network system has its own *Requirements*. For example, the main purpose of an encryption device is to perform network encryption, while the main purpose of the base station is to provide mobile services. Security is an additional function for a base station. From this point of view, there will be differences in the development of the post-quantum technology of the encryption device and the *Requirements* for the base station.

III. EFFORTS ON QUANTUM RESISTANT NETWORK PLATFORMS

A. Standardization

NIST, the leading authority on the standardization of security algorithms (which previously included hash functions and Advanced Encryption System (AES) NIST contests), has already begun work on novel post-quantum algorithms for stateless digital signatures and public-key encryption/key encapsulation mechanisms and corresponding updated protocols. These efforts can help to define the equipment and interfaces to have a robust PKS. Among the 3rd round finalists of the NIST competition, It can be discussed that hash-based systems will come to the fore more. The reason for this is that structural lattice-based systems are new and have not been studied in details by in academia and industry. Although this is not certain, it is possible that weak points may be found in the future for lattice-based systems. However, studies have been carried out on hash-based systems for many years and the risks for the vulnerabilities (which are not much) of the systems are analyzed and strengthening steps are taken already. In summary, NIST's vision can be described to ensure that the keys to be used for symmetric algorithms are transmitted to devices in quantum resistant format, since the operations of symmetric algorithms are quantum resistant by definition.

On the other hand, Internet Engineering Task Force (IETF) has prepared an Request for Comment (RFC) [18] that can provide a modification for quantum resistance of the widely used Internet Key Exchange (IKE) protocol. This modification involves the use of lists for post-quantum preshared keys along with their identifiers within devices. The IKE initiator device selects a key and randomly modifies that key. Quantum computing algorithms (especially structural lattice-based algorithms) have long been studied in the literature, in contrast to algorithms such as the ECC, RSA, or DH key agreement protocol. The hybrid use of algorithms based on different mathematical problems can be considered as a temporary step towards fully secure post-quantum computing or as a way to provide additional security. In this way, security against the quantum threat is provided without losing existing security. The IETF draft in [35] is an example of using the hybrid keys for the TLS 1.3 protocol. In this study, it is mentioned that a session key is obtained by using the output of a classical key agreement algorithm along with the output of a quantum computer resistant key agreement algorithm. In general, the goal of IETF is to use existing methods with some modifications rather

than defining new methods specifically for the post-quantum era.

Organizations such as International Organization for Standardization (ISO) [1] and Federal Information Processing Standards (FIPS) [2] have programs that verify whether the cryptographic modules are implemented correctly and reliably in network devices. ISO is collaborating with the Horizon2020 project called PQCRYPTO (Post-Quantum Cryptography for Long-Term Security). They will benefit from the results of this project for standardization activities related to the security of cryptographic modules in the post-quantum period. FIPS has prepared a draft roadmap on post-quantum hardware/software module evaluations.

B. Commercial/Open Source Products

The practical security applications of PQC are still not certain and no applications are foreseen to be developed in the medium-scale quantum computers. So far, QKD[3] (that can be used for conventional symmetric encryption, e.g. AES to refresh keys frequently) and Quantum Random Number Generators (QRNGs) (e.g., applicable to generate keys for RSA and ECDSA) are some initial types of quantum cryptographs that have attracted interest of enterprises, e.g. Quantum Origin from Honeywell Quantum (generates truly random seeds using the unpredictable quantum mechanics). However, solutions such as QKD require a suitable quantum architecture based on either satellites or optical fibers to remotely exchange private keys. Besides, military product started to implement QRNGs. [4]

QKD products can be used to create session keys in a communication protocol. These products use conventional hardware and use a quantum channel with a wavelength in the O-Band of telecommunication. [5] On the other hand, the project in [36] combines OpenVPN software with post-quantum cryptography. Unfortunately, it is said that this project is experimental and not yet mature. It is not recommended to protect sensitive data or communications and requires further cryptanalysis in the coming years to determine which algorithms are truly post-quantum secure.

[1]ISO/IEC 19790:2012

[2]https://csrc.nist.gov/publications/detail/fips/140/2/final

[3]https://www.idquantique.com/quantum-safe-security/overview/

[4]https://cpl.thalesgroup.com/encryption

[5]https://www.toshiba.co.jp/qkd/en/products.htm

C. Discussions, Challenges & Future Directions

A summary of related works corresponding to each layer in the technology development life-cycle with descriptions of characteristics for each layer is presented in Table I. The challenges that can assist improvements with future studies are presented as follows:

Communication Overhead: New PQC algorithms will have longer signature and key lengths compared to classical asymmetric algorithms. For example, all PQC algorithms have about 10-20 times larger public key and signature sizes than ECDSA [6]. Lattice-based algorithms have key encapsulations, digital signatures, and public keys in the range of 600-900 bytes. In comparison, existing ECC algorithms are typically 32-64 bytes long [6]. Security level which is defined as the number of operations required to break a cryptographic algorithm or system also affects the overhead. In fact, security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256} [37]. For this reason, PQC algorithms with their corresponding security levels can stress network communications and cause packet fragmentation because they exceed standard Ethernet packet sizes. A good trade-off between the communication overhead and efficient running time are needed in PQC algorithm design (e.g., similar to design of "Cryptographic Suite for Algebraic Lattices" (CRYSTALS) [6]).

Symmetric Cryptography: Authentication, key generation, encryption and integrity used in cellular mobile networks that rely purely on symmetric cryptography (AES, SHA3, etc) are secure against quantum computers [34]. Because of AES-256 requires $(2^{256})/2$ operations in classical computers, but it reduces to $2^{\frac{256}{2}}$ operations in quantum computers, therefore AES-256 is considered quantum-secure with 128 bits of quantum security [3].

Approximate Computing (AC): is an emerging concept that pursues an energy-efficient and high-performance goal. In AC, a possibly inaccurate result is computed instead of a guaranteed accurate result. This approach can increase the processing speed for PQC. However, in this case, the question arises whether it is safe to work with encryption keys computed based on probability calculations and statistical analysis. From this point of view, AC can be taken into account for some specific intermediate steps instead of using it to calculate the whole system.

[6]https://pq-crystals.org/index.shtml

Homomorphic Encryption (HE): Encrypted data is vulnerable to the hacks of quantum computing algorithms either locally or in the cloud. HE can address many of these concerns about quantum computing by encrypting data at all times and making it resistant to quantum thanks to the use of lattice cryptography. Therefore, HE (more specifically fully HE) falls into the post-quantum era of encryption types [12].

Hybrid Deployment Aspects: The deployment of the post-quantum algorithm can be done together with existing public-key cryptography methods to increase their effectiveness. It has been on the agenda of many researchers to use the more durable classical cryptographic methods (e.g., elliptic curve-based methods) to address security concerns over lattice-based methods [29]. As mentioned earlier, classical cryptographic algorithms and their cryptanalysis have been studied for a long time. Therefore, the hybrid use of lattice-based methods (one of the most important PQCs) with classical cryptographic algorithms is an improvement that increases the level of security in the implementation [35].

Side-channel Attacks: Side-channel analysis can be used to attack devices to capture encryption keys. For this reason, when implementing algorithms on devices, care should be taken to ensure that the implementation is resistant to side channel attacks. However, in this case, the performance of the algorithm may change and decrease drastically due to the side-channel-resistant implementation. Therefore, it is challenging to create an implementation that is resistant to side-channel attacks at the moment.

IV. Conclusions & Future Work

Although the current practical implementations of quantum cryptography have still a long way to proceed, the planning of migration to PQC should be started as early as possible for telecommunication ecosystem. In this survey paper, we provided an overview of recent advances in PQC algorithms concentrating on networking aspects. We first provide an illustrative life-cycle components in PQC development process from networking and device perspectives. Then, we concentrate on developments in on quantum-resistant network platforms including technology development interactions, latest activities on standardization and commercial/open source frameworks/products. Finally, we discuss about the challenges and future directions towards building a PQC-based networking system for the telecommunication networks.

Our analysis show that, recent advances in algorithms coupled with hardware design tailored to large polynomial and vectorized operations, significant advances in post-quantum techniques can be expected in the coming decades. This will influence the transfer of this knowledge into practical applications or commercial products and services in telecommunications and networks. On the other hand, the development of such specific hardware/software supporting post-quantum algorithms is still a major challenge, both in terms of standardization and platform development, the development of quantum computers is still in its infancy.

Acknowledgment

This work was partially funded by Generalitat de Catalunya grant 2017 SGR 1195 and the national program on equipment and scientific and technical infrastructure, EQC2018-005257-P under the European Regional Development Fund (FEDER).

References

[1] Z. Kirsch and M. Chow, "Quantum computing: The risk to existing encryption methods," *Retrieved from URL: http://www. cs. tufts. edu/comp/116/archive/fall2015/zkir sch. pdf*, 2015.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[3] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[4] C. P. Schnorr, "Fast factoring integers by SVP algorithms, corrected." Cryptology ePrint Archive, Report 2021/933, 2021. https://ia.cr/2021/933.

[5] J. Kong *et al.*, "Measurement-induced, spatially-extended entanglement in a hot, strongly-interacting atomic system," *Nature Communications*, vol. 11, no. 2415, pp. 86–99, 2020.

[6] 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*, CoNEXT '20, (New York, NY, USA), p. 149–156, Association for Computing Machinery, 2020.

[7] J. W. Bos *et al.*, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," in *2015 IEEE Symposium on Security and Privacy*, pp. 553–570, 2015.

[8] J. Bobrysheva and S. Zapechnikov, "Post-quantum security of messaging protocols: Analysis of double ratcheting algorithm," in *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 2041–2044, 2020.

[9] F. Borges, P. R. Reis, and D. Pereira, "A comparison of security and its performance for key agreements in post-quantum cryptography," *IEEE Access*, vol. 8, pp. 142413–142422, 2020.

[10] R. G. L. D'Oliveira, A. Cohen, J. Robinson, T. Stahlbuhk, and M. Médard, "Post-quantum security for ultra-reliable low-latency heterogeneous networks," *CoRR*, vol. abs/2108.06409, 2021.

[11] K. Basu, D. Soni, M. Nabeel, and R. Karri, "NIST post-quantum cryptography - A hardware evaluation study." Cryptology ePrint Archive, Report 2019/047, 2019. https://ia.cr/2019/047.

[12] K. Lauter, "Postquantum opportunities: lattices, homomorphic encryption, and supersingular isogeny graphs," *IEEE Security & Privacy*, vol. 15, no. 4, pp. 22–27, 2017.

[13] G. Xin *et al.*, "VPQC: A domain-specific vector processor for post-quantum cryptography based on RISC-V architecture," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 8, pp. 2672–2684, 2020.

[14] T. Fritzmann, G. Sigl, and J. Sepúlveda, "RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 239–280, 2020.

[15] T. Fritzmann *et al.*, "Masked accelerators and instruction set extensions for post-quantum cryptography.," *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 479, 2021.

[16] A. Kuznetsov, I. Svatovskij, N. Kiyan, and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period," in *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T)*, pp. 125–130, 2017.

[17] M. Iavich, G. Iashvili, R. Bocu, and S. Gnatyuk, "Post-quantum digital signature scheme for personal data security in communication network systems," in *International Conference of Artificial Intelligence, Medical Engineering, Education*, pp. 303–314, Springer, 2020.

[18] 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." IETF RFC 8784, 2020.

[19] S. H. Islam, "Provably secure two-party authenticated key agreement protocol for post-quantum environments," *Journal of Information Security and Applications*, vol. 52, p. 102468, 2020.

[20] E. Zeydan *et al.*, "Post-quantum era in V2X security: Convergence of orchestration and parallel computation," *arXiv preprint arXiv:2112.06814*, 2021, *[Accepted to IEEE Communications Standards Magazine]*.

[21] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Comput. Surv.*, vol. 51, jan 2019.

[22] N. Gupta, A. Jati, A. K. Chauhan, and A. Chattopadhyay, "PQC Acceleration Using GPUs: FrodoKEM, NewHope, and Kyber," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 3, pp. 575–586, 2020.

[23] D. Dharminder, S. Kumari, and U. Kumar, "Post quantum secure conditional privacy preserving authentication for edge based vehicular communication," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, p. e4346, 2021.

[24] S. Paul, F. Schick, and J. Seedorf, "TPM-based post-quantum cryptography: A case study on quantum-resistant and mutually authenticated TLS for IoT environments," ARES 2021, (New York, NY, USA), Association for Computing Machinery, 2021.

[25] B. Koziel *et al.*, "Post-quantum cryptography on FPGA based on isogenies on elliptic curves," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 1, pp. 86–99, 2017.

[26] Y.-L. Gao *et al.*, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.

[27] D. Butin, J. Wälde, and J. Buchmann, "Post-quantum authentication in OpenSSL with hash-based signatures," in *2017 Tenth International Conference on Mobile Computing and Ubiquitous Network (ICMU)*, pp. 1–6, IEEE, 2017.

[28] V. Chamola *et al.*, "Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography," Elsevier, 2021.

[29] Y. Qassim, M. E. Magaña, and A. Yavuz, "Post-quantum hybrid security mechanism for MIMO systems," in *2017 International Conference on Computing, Networking and Communications (ICNC)*, pp. 684–689, IEEE, 2017.

[30] S. Paul and P. Scheible, "Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication," in *European Symposium on Research in Computer Security*, pp. 295–316, Springer, 2020.

[31] Z. Liu *et al.*, "Securing edge devices in the post-quantum internet of things using lattice-based cryptography," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 158–162, 2018.

[32] A. Cohen, R. G. D'Oliveira, S. Salamatian, and M. Médard, "Network coding-based post-quantum cryptography," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 49–64, 2021.

[33] K. Chalkias *et al.*, "Blockchained post-quantum signatures," in *2018 IEEE International Conference on Internet of Things (iThings)*, pp. 1196–1203, 2018.

[34] J. P. Mattsson, B. Smeets, and E. Thormarker, "Quantum technology and its impact on security in mobile networks." Ericsson Technology Review, 2021. https://bit.ly/3lIpfHU.

[35] D. Steblia, S. Fluhrer, and S. Gueron, "Hybrid key exchange in TLS 1.3," tech. rep., Internet-Draft draft-ietf-tls-hybrid-design-00. IETF, 2020.

[36] Microsoft, "PQCrypto-VPN: An OpenVPN with post-quantum cryptography." https://github.com/microsoft/PQCrypto-VPN/releases/tag/PQCrypto-1.3, July 2020. [Online; accessed December-2021].

[37] Committee on National Security Systems, "(CNSS) Glossary." CNSSI No. 4009, 2015. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.