A Survey on Post-Quantum Cryptography for 5G/6G Communications

Rongjie Zhou
Singapore Institute of Technology & WizVision Pte Ltd
Singapore
2203812@sit.singaporetech.edu.sg

Huaqun Guo
Singapore Institute of Technology
Singapore
huaqun.guo@singaporetech.edu.sg

Francis E C Teo
WizVision Pte Ltd
Singapore
francis.teo@wizvision.com

Spiridon Bakiras
Singapore Institute of Technology
Singapore
spiridon.bakiras@singaporetech.edu.sg

2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) | 979-8-3503-9600-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/SOLI60636.2023.10425346

***Abstract*—As quantum computing capabilities accelerate, together with the discovery of Shor's Algorithm, existing encryption protocols, such as TLS (Transport Layer Security) and IPsec (Internet Protocol Security), face the risk of becoming obsolete. This vulnerability poses a significant challenge for 5G and 6G mobile networks, which rely on these protocols for data transmission. This survey explores the potential of Post-Quantum Cryptography (PQC) algorithms as viable alternatives for securing mobile communications. Through a comprehensive review of NIST-shortlisted PQC algorithms, this paper examines their relevance, efficiency, and adaptability in 5G and 6G architectures. Case studies, including real-world implementations by Amazon Web Services (AWS) and IBM, illustrate the growing acceptance and practical applicability of these quantum-resistant algorithms.**

Keywords—5G, 6G, Mobile Communication, Post Quantum Cryptography, IPsec, TLS, Public Key Infrastructure, Security, Key Establishment Mechanism

I. INTRODUCTION

This survey focuses on the unique implications of Post-Quantum Cryptography (PQC) in the rapidly evolving landscapes of 5G and 6G mobile networks. While previous works, including [1], have laid foundational insights into quantum computing's challenges for security protocols, our survey advances this discussion by delving into the latest developments and practical implementations of PQC. We particularly emphasize the distinctive requirements and potential solutions for 5G/6G infrastructures, including a detailed analysis of NIST's shortlisted PQC algorithms and their specific adaptability to the high-speed, low-latency, and highly connected nature of these future networks. This comparative analysis underscores our work's novelty in addressing network security's evolving landscape in the era of quantum computing.

As smartphones become increasingly ubiquitous, they have evolved into essential computing devices for many people. Some individuals even own multiple smartphones to accommodate work requirements or to take advantage of the unique ecosystems offered by different operating systems like iOS and Android. This widespread adoption [2] highlights the critical role of advanced mobile networks, such as 5G and 6G, and raises pressing questions about the security protocols in place to protect sensitive data.

Data encryption serves as a safeguard by converting plaintext—readable and understandable data—into ciphertext, which appears as a scrambled and seemingly random format [3]. This transformation is crucial for maintaining the confidentiality and authenticity of data as it is transmitted across a network. On the receiving end, decryption is employed to convert the ciphertext back into its original plaintext form. Utilizing encryption for data transmission is particularly important for mitigating the risk of "Man-in-the-Middle" (MITM) attacks [4], where unauthorized intermediaries could potentially intercept and alter the data being communicated between two parties.

Beginning with Android 9 and iOS 9, smartphones require the use of HTTPS for data transmission. All data traffic during transit is encrypted through the Transport Layer Security (TLS) protocol [5].

TLS initiates a handshake shown in Fig.1 with a server to establish a secure connection for data transmission, ensuring the data's confidentiality, integrity, and authenticity. Once the connection is secure, transmitted data is encrypted using a shared secret key, typically relying on Advanced Encryption Standards (AES) [6]. Most major Internet services today employ TLS for encrypted communication [4][7].

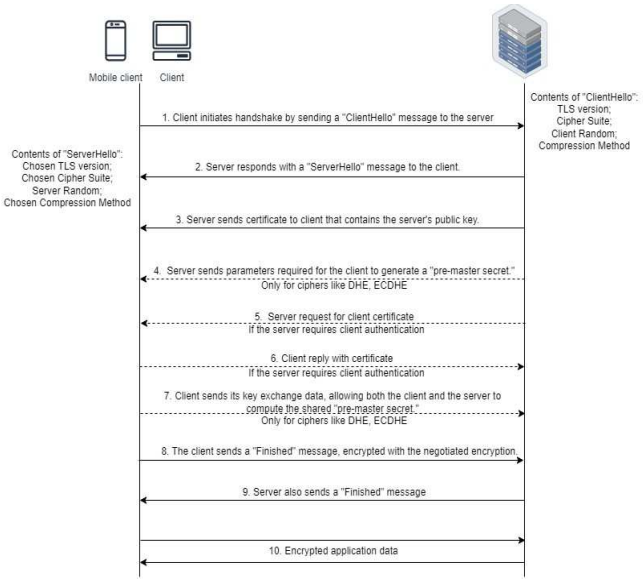

Fig. 1. TLS Handshake Overview

While TLS has become a standard for internet security, the advent of quantum computing and the discovery of Shor's Algorithm pose significant challenges to its efficacy [8]. Specifically, Shor's Algorithm, when executed on a sufficiently powerful quantum computer, has the potential to

break the asymmetric encryption algorithms that form the basis of TLS security.

In both 5G and 6G networks, the underlying architecture is predominantly based on a Service-Based Architecture (SBA) (Fig. 2). Unlike the older, hierarchical models, SBA provides a more modular and flexible framework where various network functions are decoupled and interact through standardized interfaces. This design enables more agile deployment and scaling of services, facilitating the rapid rollout of new features and technologies.

In the SBA model, core network entities such as the Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) are defined as individual services. These services interact via application programming interfaces (APIs) on a service-based interface. This allows each entity to request services from one another in a loosely-coupled manner, enabling easier management and orchestration of network functionalities [9].

The Radio Access Network (RAN), responsible for the actual radio transmissions, also communicates with these core entities. While the RAN and core services are logically separated, their interactions are essential for tasks such as handover management, Quality of Service (QoS) adjustments, and user data routing [10].

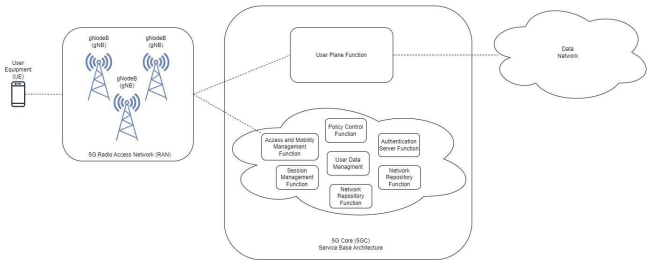

Fig. 2. 5G Standalone Architecture Diagram

For securing these interactions and data transmissions, protocols like TLS and IPsec are often employed [11]. TLS is predominantly used for securing data exchanges over the service-based interfaces within the core network [12]. It initiates a "handshake" with the receiving entity to establish a secure connection, ensuring the confidentiality and integrity of the transmitted data.

On the other hand, IPsec is commonly used for securing the communication paths between the RAN and the core network entities. It adds an additional layer of security, providing capabilities such as data encryption, authentication, and anti-replay protection. This dual approach—using both TLS and IPsec—adds multiple layers of security to the network architecture [11].

However, the current security measures raise concerns in the face of emerging threats from quantum computing. Due to its potential to compromise the cryptographic algorithms that underpin TLS and IPsec, there is a pressing need to examine alternative security solutions, such as Post-Quantum Cryptography (PQC).

In this survey, we will examine various Post-Quantum Cryptography (PQC) algorithms that have been shortlisted by NIST, exploring their relevance and potential for implementation in 5G and 6G mobile communication.

II. Survey Methodology

The methodology adopted entails a comprehensive review of academic and industry literature focusing on PQC algorithms and their application in 5G/6G networks. We selected sources published within the last five years to ensure the inclusion of the most recent advancements. The selection criteria for PQC algorithms were based on their performance metrics, relevance to mobile network requirements, and the extent of their evaluation or implementation in real-world scenarios. This involved a thorough analysis of peer-reviewed journals, conference papers from leading technology firms, and reports from standards organizations like NIST. We aim to compare these algorithms not only in terms of their theoretical robustness against quantum threats but also their practical applicability in the unique context of 5G and 6G networks.

III. Threats from Quantum Computing

The increasing computational power of quantum computers poses existential threats to current public key encryption algorithms such as Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and the Diffie-Hellman (DH) key exchange. One study noted, "Quantum computers can solve complex mathematical problems in seconds, significantly faster than their classical counterparts" [13]. This computational advantage could render existing encryption methods obsolete, breaking encryption schemes that currently take hundreds of years to crack.

Public Key Infrastructure (PKI) relies on asymmetric cryptographic algorithms [14]. Algorithms like RSA, DH, and ECC are commonly used for these public keys, while digital signatures often use the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), along with the Secure Hash Algorithm (SHA), for encryption [14].

Shor's Algorithm, proposed by mathematician Peter Shor in 1994, is a quantum algorithm that efficiently factors large composite numbers, a problem that classically requires exponential time [15]. The implications of Shor's Algorithm are significant for traditional public-key cryptosystems such as RSA, DH and ECC.

The actual threat of Shor's Algorithm is contingent on the development of a sufficiently large and fault-tolerant quantum computer. While smaller quantum computers exist today [8], they are not yet powerful and stable enough to break real-world encryption keys using Shor's Algorithm. However, as quantum computers are rapidly in development, it is only a matter of time where the traditional public-key cryptosystems will be broken [16].

A study has shown that a quantum computer with 372 Qubits could break a 2048-bit RSA algorithm [17]. As of 2022, IBM's quantum road map includes "Osprey," a 433-qubit quantum processor, and is on track to develop "Condor," a 1121-qubit quantum processor by 2023[18]. With the development of a quantum processor with higher qubit count, this opens more processing power and better capabilities in solving difficult mathematical problems used in cryptography.

RSA, like other public key cryptography algorithm, generates a pair of keys, public and private keys, that are mathematically related [8]. While the public key is disseminated widely and is accessible to anyone wishing to

send encrypted data to the key owner, the private key remains confidential, safeguarded by the recipient and used exclusively for decryption purposes. The interplay between these keys facilitates a secure communication pathway, allowing for data to be encrypted by the sender using the recipient's public key and subsequently decrypted only by the intended recipient possessing the corresponding private key.

The compromise of private keys [19] would undermine the essential attributes of secure communication: confidentiality, integrity, authentication, and non-repudiation.

Confidentially: Attackers could decrypt past and/or future communications encrypted with the compromised private key, gaining unauthorized access to sensitive information like medical records and financial data.

Integrity: Attackers could modify the content of the encrypted message or create fake messages that appears to be from the authentic sender.

Authentication: Attackers could impersonate the legitimate party and requesting sensitive data or access to a particular system or service.

Non-repudiation: As digital signatures rely on private keys to provide evidence that a specific party sent a message or authorized a transaction. Compromised private keys could undermine the trustworthiness of digital signatures, making it difficult to prove the origin or authenticity of a message or transaction.

This significant risks not only affects individual privacy but also to sectors reliant on encrypted communications, such as financial services, healthcare, and national security.

Another particularly concerning threat vector that arises with the advent of quantum computing is the "store-now-decrypt-later" attack, as pointed out in a Google security blog [20]. In this type of attack, adversaries do not attempt to break the encryption immediately. Instead, they store encrypted data now, waiting for quantum computing technologies to become sufficiently advanced. Once a quantum computer capable of breaking the current cryptographic algorithms becomes available, the stored data can be decrypted retroactively.

This strategy poses significant risks, as it undermines the long-term security of encrypted information. Even data that is securely encrypted today, and thus safe from immediate decryption using existing technology, may be vulnerable in the future when quantum computers become sufficiently powerful. This is particularly worrisome for data that has a long shelf-life and remains sensitive over extended periods, such as healthcare records, financial transaction logs, and national security documents.

Such a delayed decryption attack makes it imperative to transition to quantum-resistant cryptographic algorithms sooner rather than later. This is not just to secure current data transmissions but also to protect the integrity and confidentiality of valuable data that could be targeted and stored now for decryption at a later time.

IV. The Need for Post-Quantum Algorithms

5G and 6G mobile networks predominantly employ TLS and IPsec as their cryptographic protocols for secure communications [21][22]. These protocols are responsible for key functions such as authentication, key exchange, and transport security. However, the key establishment algorithms underpinning TLS and IPsec, namely RSA, ECC, and DH, are highly susceptible to quantum computing capabilities [23]. With the advent of quantum computers, breaking these traditionally secure algorithms could become a trivial task, thereby making our current security infrastructures obsolete.

Recognizing the urgency to address these vulnerabilities, the National Institute of Standards and Technology (NIST) has initiated a call for proposals to develop Post-Quantum Cryptography (PQC) algorithms. These proposals are aimed at replacing or complementing the existing cryptographic systems with algorithms that can resist potential quantum attacks.

The transition to PQC is not merely a technological necessity but also a strategic imperative for both national and enterprise-level cybersecurity postures. As quantum computing technology advances, the window for making this transition shrinks. Failure to adopt PQC algorithms in time could result in wide-ranging security vulnerabilities, including data breaches, identity theft, and compromised national security.

While PQC offers a pathway to secure future communications, it comes with its own set of challenges, such as increased computational overhead or larger key sizes. These challenges require careful consideration, especially in resource-constrained environments like mobile networks. Therefore, optimizing PQC algorithms for mobile applications without sacrificing security is a vital area of ongoing research.

V. Shortlisted PQC Algorithms by NIST

A. Key Establishment Mechanism (KEM)

The shortlisted algorithm for public-key encryption and key establishment is CRYSTALS-Kyber (Table I). Developed as a part of the Cryptographic Suite for Algebraic Lattices (CRYSTALS), Kyber utilizes lattice-based cryptography to offer robust security against quantum attacks. It operates with high efficiency and low computational overhead, making it a prime candidate for implementation in resource-constrained environments like mobile networks.

TABLE I. SHORTLISTED PQC KEY ESTABLISHMENT MECHANISM

Algorithm	**PQC - KEM**			
	Security Level	***Private key length***	***Public key length***	***Ciphertext length***
Kyber512	1	1632	800	768
Kyber768	3	2400	1184	1088
Kyber1024	5	3168	1568	1568

B. Digital Signature Algorithms

For digital signatures, three algorithms have been shortlisted: CRYSTALS-Dilithium, FALCON, and SPHINCS+ (Table II).

CRYSTALS- Dilithium is a part of the CRYSTALS suite, Dilithium provides a secure and efficient digital signature mechanism. It offers strong security guarantees against quantum attacks and is optimized for performance, even in constrained devices [24].

Fast-Fourier Lattice-based Compact Signatures over NTRU (FALCON) aims to minimize the signature size while

maintaining a high level of security. It's especially noted for its efficiency and speed, making it another attractive option for mobile applications.

Unlike CRYSTALS-DILITHIUM and FALCON, which are based on lattice cryptography, SPHINCS+ employs hash-based cryptography. It provides long-term security and is designed to function well in a variety of settings.

Based on [25][26], lattice-based PQC algorithms performs better in terms of time, power and energy consumption. This is important especially in the implementation for mobile communications as resource are limited on such devices.

TABLE II. SHORTLISTED PQC DIGITAL SIGNATURE SCHEMES

Algorithm	**PQC Digital Signature Schemes**			
	Security Level	***Private key length***	***Public key length***	***Signature length***
Dilithium2	2	2528	1312	2420
Dilithium3	3	4000	1952	3293
Dilithium5	5	4864	2592	4595
Falcon512	1	1281	897	690
Falcon1024	5	2305	1793	1330
SPHINCS+-Haraka-128f	1	64	32	17088
SPHINCS+-Haraka-128s	1	64	32	7856
SPHINCS+-Haraka-192f	3	96	48	35664
SPHINCS+-Haraka-192s	3	96	48	16224
SPHINCS+-Haraka-256f	5	128	64	49856
SPHINCS+-Haraka-256s	5	128	64	29792
SPHINCS+-SHA256-128f	1	64	32	17088
SPHINCS+-SHA256-128s	1	64	32	7856
SPHINCS+-SHA256-192f	3	96	48	35664
SPHINCS+-SHA256-192s	3	96	48	16224
SPHINCS+-SHA256-256f	5	128	64	49856
SPHINCS+-SHA256-256s	5	128	64	29792
SPHINCS+-SHAKE256-128f	1	64	32	17088
SPHINCS+-SHAKE256-128s	1	64	32	7856
SPHINCS+-SHAKE256-192f	3	96	48	35664
SPHINCS+-SHAKE256-192s	3	96	48	16224
SPHINCS+-SHAKE256-256f	5	128	64	49856
SPHINCS+-SHAKE256-256s	5	128	64	29792

VI. COMPARISIONS OF THE VARIOUS PQM CATEGORIES

Given that the shortlisted PQC algorithms differ significantly, parameters such as secret key length, signature length, and public key length will vary as well. As the primary focus of this survey is on 5G networks and beyond, it is essential to consider factors like memory usage, transmission time, computational overhead, user experience, and cross-device compatibility. Longer keys and signatures can lead to increased memory usage, extended transmission times, and suboptimal user experiences.

A. KEM

A study [27] compared various PQC Key KEMs based on their security strengths. Lattice-based algorithms generally excel in speed of key generation. According to the statistics provided, CRYSTALS-Kyber outperforms other KEM algorithms in terms of computational efficiency, requiring fewer CPU cycles. However, it is worth noting that Kyber does not generate the smallest key sizes. Despite this, Kyber offers a favorable trade-off in performance, making it a strong candidate for mobile communications, where resource constraints are a primary concern.

B. Digital Signatures

Another study [28], originating from the same source, compared various PQC digital signature algorithms based on their security strengths. Among the shortlisted algorithms by NIST, Dilithium consumes fewer CPU cycles than both FALCON and SPHINCS+.

VII. INTEROPERABILITY OF PQC WITH TLS

Since the announcement of the finalists for the PQC algorithms, some research has focused on their integration with the TLS protocol [29]. These studies have analyzed performance on x86 and Advanced RISC Machine (ARM) architectures, the latter of which is commonly used in mobile phones. Research indicates that PQC algorithms like Dilithium and New Hope perform better on ARM architecture compared to x86.

Another study evaluated the integration of various PQC algorithms with the TLS protocol [26]. It demonstrated that the integration of PQC and TLS reduces power, time, and energy consumption compared to the classic TLS protocol.

Given that most devices connecting to 5G or 6G networks will likely be mobile phones, it is crucial to understand their performance when implementing PQC, especially in resource-limited environments.

VIII. PQC Algorithms Implemented Today

Amazon Web Service (AWS) has announced updates to its security protocols, incorporating Kyber into some of its core services. These services include the AWS Key Management Service (KMS), AWS Certificate Manager (ACM) Secrets Manager TLS endpoints, and Secure File Transfer Protocol (SFTP) file transfer service [30][31]. As many mobile apps utilize AWS for backend services, this move has the potential to extend quantum-safe security protocols to a large number of mobile devices.

IBM [32] have also implemented Kyber and Dilithium from CRYSTALS into their IBM z16 System. Promising quantum-safe capabilities in their product pipeline. IBM's hardware often serves as part of the backbone for telecom networks. This means that their adoption of PQC has the potential to influence security measures in future 5G and 6G architectures.

In a similar vein to AWS and IBM, Cloudflare, a prominent player in the domain of internet infrastructure, has also recognized the impending threat posed by quantum computing to existing cryptographic systems. As reported in their company blog [33][34], Cloudflare has keenly adopted and implemented Kyber for key agreement in its TLS 1.3 traffic, which includes HTTP/3. This ensures enhanced security for data in transit, safeguarding it against potential future quantum-based threats. Their approach is a hybrid one, seamlessly integrating classical cryptography with post-quantum cryptography to strike a balance between speed and security. Cloudflare's strategic move to embrace PQC not only fortifies their own infrastructure but also sets a precedent for other web service providers, pushing the envelope for universal quantum-safe web security.

IX. PQC Challenges for 5G/6G Communiications

As the world gears up to embrace the potential of 5G and looks forward to 6G, integrating PQC is crucial to ensure long-term security. However, the integration of PQC with these advanced communication technologies is not without challenges. These networks, characterized by their high data rates, low latency, and vast device connectivity, demand cryptographic solutions that are not only robust but also highly efficient and adaptable to diverse and rapidly changing conditions. For instance, ensuring seamless cryptographic handovers and maintaining Quality of Service (QoS) during high-speed mobility are critical requirements unique to these advanced networks. Further, the scalability of PQC solutions must align with the dynamic and dense network topologies of 5G/6G, where traditional cryptographic approaches might falter in terms of performance and reliability

A. Lack of Standardization

Although NIST are actively working on standardizing PQC algorithms, the lack of finalized standards can create uncertainty. It's risky for telecommunication operators to invest heavily in a particular algorithm that might later be deemed insecure or suboptimal.

B. Interoperability Issues

The coexistence of classical cryptographic systems and PQC during the transitional period can lead to interoperability challenges. Systems need to be designed to handle both types of cryptography, especially during the handshakes between different network entities.

C. Hardware Constraints

PQC requires changes not only at the software level but also potentially at the hardware level, especially when aiming for optimized performance. Low to mid ranged mobile phones may struggle when handling the overheads required by PQC due to the resource constraints.

X. Conclusion

As the progression towards 5G and 6G mobile networks continues, the imperative to address security vulnerabilities exacerbated by quantum computing becomes more urgent. Existing cryptographic algorithms, which have served us well for decades, stand on the brink of obsolescence as quantum computers advance.

In this survey, we've examined the promising field of Post-Quantum Cryptography (PQC), focusing on algorithms that have been shortlisted by NIST for their potential applicability in 5G and 6G mobile networks.

Lattice-based algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium have shown notable performance benefits, particularly in resource-constrained environments such as mobile devices. These algorithms not only offer strong security guarantees against quantum attacks but are also highly efficient, minimizing computational overhead.

Current implementations, such as those by AWS, IBM and Cloudflare, indicate a proactive industry move towards adopting these quantum-resistant cryptographic algorithms. Given their applicability and the urgent need for enhanced security protocols, it is likely that we will see a broader range of PQC algorithms integrated into both cloud-based services and network hardware that form the backbone of our mobile communications infrastructure.

However, there are still challenges to be addressed. The transition from current algorithms to PQC should be done in a way that ensures backward compatibility and seamless user experience.

Future research should also focus on standardizing these new algorithms, optimizing their performance on mobile devices, and exploring their interoperability with existing protocols.

As quantum computing technology matures, the window for preparing our digital infrastructure narrows. The development and deployment of Post-Quantum Cryptography in 5G and 6G networks not only seem advisable but indeed, inevitable.

Acknowledgements

This research is funded by the scholarship from the Future Communications Research and Development Programme (FCP), Infocomm Media Development Authority (IMDA) and National Research Foundation Singapore (NRF), Singapore.

References

[1] Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., & Hassija, V. (2021). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications, 176, 99–118. https://doi.org/10.1016/j.comcom.2021.05.019

[2] GSM Association, “The Mobile Economy” Retrieved October 12 2023 from https://www.gsma.com/mobileeconomy/

[3] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

[4] M. Kim, Y. Shin and T. Shon, "MitM Tool Analysis for TLS Forensics," 2021 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, Republic of, 2021, pp. 1-4, doi: 10.1109/PlatCon53246.2021.9680752.

[5] D. Mankowski, T. Wiggers and V. Moonsamy, "TLS → Post-Quantum TLS: Inspecting the TLS landscape for PQC adoption on Android," 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Delft, Netherlands, 2023, pp. 526-538, doi: 10.1109/EuroSPW59978.2023.00065.

[6] IBM, "How SSL and TLS provide identification authentication confidentiality and integrity", IBM MQ 7.5, 30th April 2018. Retrieved October 12, 2023 from https://www.ibm.com/docs/en/ibm-mq/7.5?topic=ssl-how-tls-provide-authentication-confidentiality-integrity.

[7] I. Kotuliak, P. Rybár and P. Trúchly, "Performance comparison of IPsec and TLS based VPN technologies," the 9th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stara Lesna, Slovakia, 2011, pp. 217-221, 2011, doi: 10.1109/ICETA.2011.6112567

[8] G. R. Mounica, G. Manimaran, L. B. Jerome and P. Bhattacharjee, "Implementation of 5-Qubit approach-based Shor's Algorithm in IBM Qiskit," 2021 IEEE Pune Section International Conference (PuneCon), Pune, India, 2021, pp. 1-6, doi: 10.1109/PuneCon52575.2021.9686492.

[9] G. Amponis et al., "Towards Securing Next-Generation Networks: Attacking 5G Core/RAN Testbed," 2022 Panhellenic Conference on Electronics & Telecommunications (PACET), Tripolis, Greece, 2022, pp. 1-4, doi: 10.1109/PACET56979.2022.9976365.

[10] H. Yang et al., "Data-Driven Network Slicing From Core to RAN for 5G Broadcasting Services," in IEEE Transactions on Broadcasting, vol. 67, no. 1, pp. 23-32, March 2021, doi: 10.1109/TBC.2020.3031742.

[11] A. K. Yerrapragada, T. Eisman and B. Kelley, "Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2232-2242, 2021, doi: 10.1109/OJCOMS.2021.3105185.

[12] Kim, J., Choudhary, G., Heo, J. et al., "5G wireless P2MP backhaul security protocol: an adaptive approach," J Wireless Com Network 2019, 265 (2019).

[13] F. Bene and A. Kiss, "Public Key Infrastructure in the Post-Quantum Era," 2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2023, pp. 000077-000082, doi: 10.1109/SACI58269.2023.10158562.

[14] F. Bene and A. Kiss, "Public Key Infrastructure in the Post-Quantum Era," 2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2023, pp. 000077-000082, doi: 10.1109/SACI58269.2023.10158562.

[15] PW. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal of Computing, vol. 26, no. 5, pp.1484–509, 1997.

[16] V. Bhatia and K. R. Ramkumar, "An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm," IEEE 5th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2020, pp. 89-94, doi: 10.1109/ICCCA49541.2020.9250806.

[17] B. Yan, Z. Tan, S. Wei, H. Jiang, W. Wang, H. Wang, L. Zuo, Q. Duan, Y. Liu, W. Shi, Y. Fei, X. Meng, Y. Han, Z. Shan, J. Chen, X. Zhu, C. Zhang, F. Jin, H. Li, C. Song, Z. Wang, Z. Ma, H. Wang and G. Long, "Factoring integers with sublinear resources on a superconducting quantum processor", arxiv:2212.12372v1, 23 Dec 2022.

[18] IBM, "The IBM Quantum Development Roadmap." Retrieved October 12, 2023 from https://www.ibm.com/quantum/roadmap.

[19] J. Arora, K. Saluja, S. Gupta, S. Sharma and G. Kaur, "Handling Secret Key Compromise by Deriving Multiple Asymmetric Keys based on Diffie-Hellman Algorithm," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2023, pp. 492-498, doi: 10.1109/ICCES57224.2023.10192607.

[20] Google, "Securing tomorrow today: Why Google now protects its internal communications from quantum threats," Google cloud. Retrieved October 12, 2023 from https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms.

[21] M. Mehic et al., "Quantum Cryptography in 5G Networks: A Comprehensive Overview," in IEEE Communications Surveys & Tutorials, doi: 10.1109/COMST.2023.3309051.

[22] C. Jose, and B. Smeets, "Security for 5G Service-Base Architecture: What you need to know", ericsson. Retrieved October 12, 2023 from https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture.

[23] E. Zeydan, Y. Turk, B. Aksoy and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A Survey," the Seventh International Conference On Mobile And Secure Services (MobiSecServ), Gainesville, FL, USA, 2022, pp. 1-8, doi: 10.1109/MobiSecServ50855.2022.9727214.

[24] N. Gupta, A. Jati, A. Chattopadhyay and G. Jha, "Lightweight Hardware Accelerator for Post-Quantum Digital Signature CRYSTALS-Dilithium," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 70, no. 8, pp. 3234-3243, Aug. 2023, doi: 10.1109/TCSI.2023.3274599.

[25] B. B. OBE, "Energy Consumption of Post Quantum Cryptography: Dilithium and Kyber Beat Our Existing TLS 1.3 Performance", ASecuritySite: When Bob Met Alice. Retrieved October 12, 2023 from https://medium.com/asecuritysite-when-bob-met-alice/energy-consumption-of-post-quantum-cryptography-dilithium-and-kyber-beat-our-existing-tls-1-3-ccadd04dd4c7.

[26] G. Tasopoulos. C. Dimopoulos, A. P. Fournaris, R. K. Zhao, A. Sakzad and R. Steinfeld, "Energy Consumption Evaluation of Post-Quantum TLS 1.3 for Resource-Constrained Embedded Devices," Cryptology ePrint Archive, Paper 2023/506.

[27] W. J Buchanan, "PQC Key Encapsulation Mechanism (KEM) Speed Tests," Asecuritysite.com, 2023. Retrieved October 12, 2023 from https://asecuritysite.com/pqc/pqc_kem.

[28] W. J Buchanan, "PQC Digital Signature Speed Tests," Asecuritysite.com, 2023. Retrived October 12, 2023 from https://asecuritysite.com/pqc/pqc_sig.

[29] A. F. De Abiega-L'Eglisse, K. A. Delgado-Vargas, F. Q. Valencia-Rodriguez, V. G. Gonzalez-Quiroga, G. Gallegos-Garcia and M. Nakano-Miyatake, "Performance of New Hope and CRYSTALS-Dilithium Postquantum Schemes in the Transport Layer Security Protocol," in IEEE Access, vol. 8, pp. 213968-213980, 2020, doi: 10.1109/ACCESS.2020.3040324.

[30] P. Kampanakis, T. Hansen, A. Volanis and G. Ravago, "Post-quantum hybrid SFTP file transfers using AWS Transfer Family", AWS Security Blog, June 3, 2023. Retrieved October 12, 2023 from https://aws.amazon.com/blogs/security/post-quantum-hybrid-sftp-file-transfers-using-aws-transfer-family/.

[31] B. Jarvis, "How to tune TLS for hybrid post-quantum cryptography with Kyber", AWS Security Blog, July 5, 2022. Retrieved October 12, 2023 from https://aws.amazon.com/blogs/security/how-to-tune-tls-for-hybrid-post-quantum-cryptography-with-kyber/.

[32] A. Dames, "Available on IBM z16: Future-Proof Digital Signatures with a Quantum-Safe Algorithm Selected by NIST", IBM Blog, July 26, 2022. Retrieved October 12, 2023 from https://www.ibm.com/blog/announcement/available-on-ibm-z16-future-proof-digital-signatures-with-a-quantum-safe-algorithm-selected-by-nist/.

[33] B. Westerbaan, and C. D. Rubin, "Defending against future threats: Cloudflare goes post-quantum", The Cloudflare Blog, October 3, 2022. Retrieved October 12, 2023 from https://blog.cloudflare.com/post-quantum-for-all/.

[34] W. Evans, and B. Westerbaan, "Post-quantum crypto should be free, so we're including it for free, forever", The Cloudflare Blog, March 16, 2023. Retrieved October 12, 2023 from https://blog.cloudflare.com/post-quantum-crypto-should-be-free/.