THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 3 (2024)
https://doi.org/ 10.62019/abbdm.v4i3.189

ASIAN BULLETIN OF BIG DATA MANAGEMENT
ISSN (Print): 2959-0795
http://abbdm.com/
ISSN (online): 2959-0809

Exploration of PQC-Based Digital Signature Schemes in TLS Certificates

Muhammad Umer Akram*, Muhammad Ashraf, Tayyab Rehman, Muhammad Abdur Rehman Javaid, Muhammad Ali Khalid

Chronicle

Article history

Received: July 19, 2024
Received in the revised format: July 26, 2024
Accepted: July 30, 2024
Available online: Aug 1, 2024

Muhammad Umer Akram is currently affiliated with Department of Avionics Engineering, Air University, E-9, Islamabad, Pakistan.
Email: 230426@students.au.edu.pk

Muhammad Ashraf & Muhammad Ali Khalid are currently affiliated with National University of Sciences and Technology (NUST), Islamabad.
Email: muhammad.ashraf@seecs.edu.pk
Email: ali.khalid@seecs.edu.pk

Tayyab Rehman is currently affiliated with IP Centric Systems R&D, Air University, Pakistan.
Email: rehmantayyab786@gmail.com

Muhammad Abdur Rehman Javaid is currently affiliated with Department of Avionics Engineering, Air University, E-9, Islamabad, Pakistan.
Email: 222576@students.au.edu.pk

Corresponding Author*

Abstract

The rapid development in quantum computers brings huge risks to traditional cryptographic systems. This paper talks about the integration of PQC-based digital signature schemes to solve challenges posed on Transport Layer Security certificates. In this paper, we give an analysis of the efficacy, security, and performance implications of various schemes in PQC—particularly lattice-based, hash-based, and multivariate polynomial-based algorithms. We detail more closely the challenges of the real deployment, directly connected with these digital signatures, considering communication overhead and computational costs. Our findings indicate that hybrid certificate chains, which integrate multiple PQC schemes, offer a feasible solution for a seamless transition to quantum-resistant standards with manageable performance trade-offs. Moreover, our study extends to the quantification of security benefits these PQC schemes provide against both quantum and classical computational attacks, underscoring their potential in enhancing the resilience of digital communication systems. This paper aims to contribute valuable insights to ongoing standardization discussions and support the broader adoption of PQC, thereby ensuring robust and future-proof security in digital communications amidst the advancing quantum computing era.

Keywords: Post-Quantum Cryptography (PQC), PQC Digital Signature Algorithms, Quantum-Resistant TLS, SPHINCS+ Digital Signatures, Lattice-Based Cryptography, Hash-Based Signatures.

INTRODUCTION

Quantum computing technology advances to change the computational landscape, and with it, there are huge implications for cryptography. Quantum computers can execute intricate mathematical problems, such as integer factorization and discrete logarithms, exponentially faster than classical computers. This breaks the security of several rather widely used cryptographic schemes, including RSA and ECC, which underpin much of today's secure communication infrastructure (Shor, 1999). This has caused a surge in the development of Post-Quantum Cryptography, targeted at obtaining algorithms resistant to quantum attacks. To that end, NIST is one of the leading standardization bodies in standardizing these PQC algorithms, among others, like the Internet Engineering Task Force and the European Telecommunications Standards Institute (Chen et al., 2023). Quantum-resistant cryptographic techniques, encompassing encryption, key exchange, authentication, and digital signing, rely on problems believed to be secure against quantum and classical computing threats. Recently, lattice-based methods like NewHope (Alkim et .al 2016) and Frodo (Bos et.al 2016) have emerged as viable solutions for key exchange. Beyond conventional cryptographic defenses, alternative strategies offering quantum immunity are gaining attention, such as quantum key distribution in optics and secrecy coding for wireless networks—the primary focus of this discussion (Humble et. al 2013). Physical layer security, an emerging field of research, leverages the inherent properties of radio communication channels to severely hinder eavesdropping (William et. al 2016). This domain can be broadly segmented into secrecy coding techniques, which transmit information covertly through the characteristics of the wireless medium, and extraction techniques, which generate secret information from the unique spatial, temporal, and frequency traits of the channel (Yener et. al 2015). For instance, secrecy coding may involve creating specialized jamming signals that disrupt all but the intended receiver (Mukherjee et.al 2015), thereby ensuring a more secure channel for legitimate parties compared to potential eavesdroppers. Alternatively, extraction methods exploit channel attributes to facilitate the secure exchange of shared secrets, potentially enhancing the confidentiality of quantum-resistant systems.

In-depth examination of post-quantum security has predominantly focused on the difficulty and security levels of algorithms. The practicality of these solutions has been affirmed through computational analysis and experimental evaluation (De Clercq et.al 2015) . Lattice-based schemes, like CRYSTALS-Dilithium and Falcon, are very promising for PQC due to their strong foundations in security and efficient implementations. These schemes are based on hardness assumptions related to lattice problems thought to be hard against classical and quantum attacks (Cine et. al 2023). Security is very essential to any IoT system; therefore, this implies that in the evolution, lightweight devices ought to be robustly secure using PQC. Nevertheless, quantum-resistant encryption and signature schemes have a larger computational footprint compared to the current public-key cryptosystems, which makes them inherently resource-intensive (L. Malina et. al 2021).

This might eventually turn adversely on IoT systems, which are majorly constrained by limited energy, memory, or processing capabilities. New research studies now realize this, and, consequently, numerous works have started to scrutinize the performance and optimization of PQC algorithms on resource-constrained devices (T. M. Fernandez-Caram ´ es et. al 2020). One of the key works in this area is, which studies in detail the feasibility of high-level PQC algorithms within the context of the IoT. This paper surveys conventional IoT network architectures, and past efforts towards integrating PQC, and provides an in-depth performance review of various candidates from a major PQC standardization effort by the United States National Institute of Standards and Technology. Even if the lessons learned from this survey remain relevant, progress within the field calls for an update to its conclusions (NIST et.al 2017). Specifically, this survey showed that there was a lack of Post-Quantum solutions specifically oriented toward resource-constrained IoT environments. Thus, given the recent events happening across the globe, there is a pressing need to update the findings to bring them closer to today's technological and security demands (Liu et.al 2024).

In this initiating step in the TLS Handshake integrating Post-Quantum Cryptography, both the client and server are referring to their respective root Certificate Authority certificates. More specifically, in this first verification chain, there will be DSA1 public keys and their signatures leading up to DSA2 signatures so that from the outset, parties are assured of not only being entirely authentic but also intact. Following this, a TCP connection is established using a SYN message from the client and a SYN-ACK from the server to provide a reliable channel of communication. As the handshake evolves, a 'Hello' exchange follows. The groups supported for key exchange, its preferred signature algorithms, and a PSK starting off the quantum secure cryptographic process will be contained in the client's 'Hello'. It replies with its own 'Hello' message, carrying a suite of cryptographic parameters that will be used along with a key share. Here KEM comes into play: the parties each generate a key and encapsulate it to protect the session keys against any quantum computer, as shown in the figure.

The received key material is then decapsulated to derive a shared quantum-resistant secret. The next step will be rigorous authentication, where both parties exchange and verify each other's certificates with DSA1 and DSA2 algorithms for the legitimacy and quantum resistance of cryptographic parameters. After this authentication process, the session will be secured, and henceforth, all data transmissions will be encrypted with the PQC-secured keys established. Finally, the handshake is completed with 'Finished' messages from the client and server: the secured communication session commences, underpinned by robust quantum-resistant cryptographic protocols. No doubt, Figure 1 reflects this all-in-one sequence of steps in securing every step of communication with robust PQC methods against future quantum computing threats.

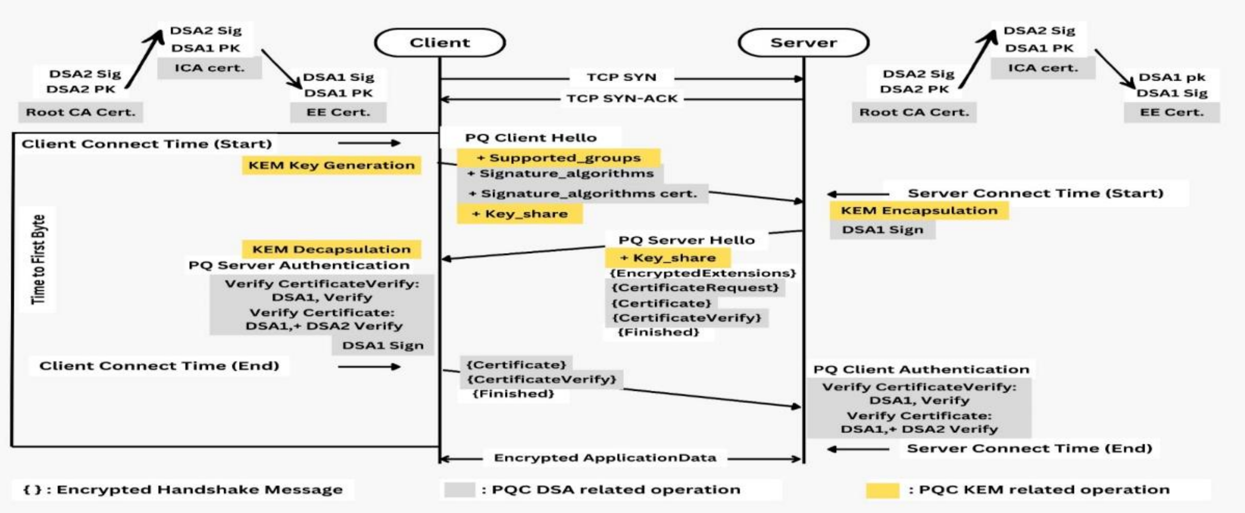

Figure 1.
PQC-Enhanced TLS Handshake Process

The table 1 summarizes some key aspects related to PQC and their implications. This comprises the potential threats that quantum computing may have on conventional cryptographic techniques, the development and need for PQC, methods, and algorithms necessary for security in quantum attacks, challenges in the implementation of PQC in resource-constrained environments like IoT systems, and standardization efforts being made by leading organizations.

Table 1.
Key Aspects of Post-Quantum Cryptography (PQC) and Their Implications

Subject of research	Implication	Key Methods/Algorithms	Key References
Quantum Threat to Cryptography	Threatens traditional schemes like RSA, ECC	Shor's algorithms	Shor (1999)
Development of PQC	Spurred by quantum computing threats	Lattice-based methods, NewHope, Frodo	Chen et al. (2023), Alkim et al. (2016), Bos et al. (2016)
Quantum-Resistant Techniques	Ensures security against quantum attacks	Quantum key distribution, Secrecy coding	Humble et al. (2013), Mukherjee et al. (2015)
PQC in IoT Systems	Highlights resource-intensive nature in constrained environments	Optimization and performance evaluation	L. Malina et al. (2021), T. M. Fernandez-Caramés et al. (2020), Liu et al. (2024)
Standardization Efforts	Essential for global interoperability and security in quantum era	NIST PQC project, ETSI efforts	Chen et al. (2023)
Physical Layer Security	Adds an additional layer of security through hardware and transmission channels	Physical properties of communication channels, Jamming signals	William et al. (2016), Yener et al. (2015)
Challenges in PQC Implementation	Computational overhead and integration issues	Studies on computational complexity	De Clercq et al. (2015)
Future of Cryptography	Anticipating quantum supremacy	Post-quantum solutions, Hybrid cryptographic systems	Liu et al. (2024), NIST et al. (2017)

The major contributions of this survey are as follows:

- This paper assesses the performance of hybrid certificate chains within Transport Layer Security and their potential for bridging current cryptographic practices with quantum-resistant standards to realize a secure transition.
- The survey paper present detailed performance impacts caused by PQC-based digital signatures on connection establishment times and resource utilization, two critical metrics of real-world applications.
- In this paper, we will give a comparative security analysis concerning the various PQC algorithms, lattice-based and hash-based schemes, and their suitability and robustness against quantum attacks within the TLS framework.
- The standardization process of the PQC algorithms is ongoing, and in this paper, we present it with related challenges. Moreover, the authors underline the need for interoperability and flexible strategies for adoption during the transition phase.

LITERATURE REVIEW

This literature review was conducted by systematically searching for peer-reviewed articles, conference papers, and industry reports related to Post-Quantum Cryptography (PQC) and its integration into Transport Layer Security (TLS) certificates. The sources were selected based on their relevance, contribution to the field, and publication date to ensure the inclusion of recent advancements and studies. The findings were then categorized based on key themes such as algorithm types (lattice-based, hash-based) and specific applications in blockchain, IoT systems, and classical cryptographic integrations. QKD is a cryptographic process that generates a secret key and sends quantum signals between the communicating authenticated parties (Scarani et. al 2009). In the process, there are two major communications channels involved. First is the quantum channel through which quantum signals are sent specifically for forming the basis of secret key distillation. One more resource is an authenticated classical channel, which has to be used for the distillation and the associated post-processing, namely error correction and privacy amplification, to keep the key intact and secret (Aguado et.. al 2019). By measuring the Quantum Bit Error Rate (QBER), the transmitter and receiver can estimate and minimize information leakage during key distribution.

In the study by Thanalakshmi et al. (2023), the scalability challenges in integrating post-quantum cryptography into blockchain systems were investigated, focusing on the implementation of the NTRU algorithm in Ethereum. Through a case study analysis, significant computational and network overheads originating from PQC integration were highlighted. The study stressed the need for a modular approach in integration strategies for easy adaptation across different blockchain architectures to achieve optimization without compromising security. Halak et al. (2024) focused their research on investigating the environmental impacts of PQC implementations in blockchain. In this respect, it evaluated the trends of energy consumption by the Rainbow algorithm. Their findings referred to an increased load of processing due to post-quantum algorithms that put into question the sustainability of a cryptographic system of this nature within blockchain environments. Comparing their results to the existing energy footprints from different PQC algorithms and traditional cryptographic methods, they bring into sharp relief the need to develop and deploy energy-efficient cryptographic solutions within the blockchain ecosystem (Javid et. al 2024).

A study by Darzi et al. (2023) introduced an optimized variant of the SPHINCS+ algorithm, achieving a reduction in both signature size and verification time through innovative use of parallel processing techniques. This advancement is crucial for applications in constrained environments where computational resources are limited. Another study by Murat et.al (2024) the integration of hash-based signatures into blockchain systems, highlighting their potential to enhance the security and integrity of blockchain transactions against quantum threats. Their work provides a roadmap for adopting hash-based cryptographic methods in decentralized systems, ensuring long-term security and robustness. PQC refers to the suite of cryptographic algorithms designed to protect data against the possible power of fault-tolerant quantum computers. In contrast with QKD, PQC adheres to normal asymmetric cryptographic classical functions for asymmetric key-pair generation, key establishment or key encapsulation/decapsulation, and digital signatures (Bernstein et. al 2017). On the other hand, classical cryptographic foundations, such as large factorization or discrete logarithms, offer no resistance against quantum computing attacks. Compared with this, PQC relies on mathematical constructs that are resistant to quantum computational speed advantages, such as lattice-based or hash-based cryptography, to ensure robust security in a quantum-enabled future. Mink et al. (2010) demonstrated how QKD could be integrated with existing communication protocols such as TLS and IPsec to enhance efficiency and overall security. However, they noted that PQC, based on hypothetical assumptions of computational complexity, could still be at risk if these assumptions are debunked, making QKD a more reliable security blueprint for future implementations.

The researchers outlined a theoretical perspective on integrating a QKD-based secret into TLS, particularly the pre-master or master secrets, and elaborated on the necessary protocol adjustments. Giron et al. (2021) contributed a conceptual critique of the challenges involved in designing a post-quantum hybrid key exchange, focusing on the notion of "transitional security." The authors claimed that security against a quantum-resistant key exchange should be the priority instead of authentication against quantum attacks. Briefly, it mentioned the possibility of a solution that combined PQC and QKD to set up a quantum-resistant TLS system but fell short of detailing the procedures and impacts of such a solution. The paper has particularly pointed out the need to consider different approaches of key agreement using concatenation or Exclusive-OR techniques, which can be an alternative way for improving security in cryptographic systems against quantum attacks.

Balamurugan et. al (2021) discusses code-based cryptography for scalability and error management, he also does so by key parameters related to security that are desirable for its integration into digital communications systems like TLS; what they turn up is that although these cryptographic methods have robust protection against quantum attacks, the complexity of decoding may bring about practical implementation challenges in a high-speed network environment. Their work also proclaimed development in the line of code construction and error-correction capabilities, very necessary for getting rid of the boundaries posed on error rates and decoding efficiency. In fact, these enhancements are indispensable if code-based cryptographic solutions have to meet the stringent requirements of real-time communication applications. Sabani ME et. al (2023) discussed Lattice-based key exchange mechanisms have also been thoroughly investigated with compatibility and performance issues in regard to present TLS protocols by Peikert and Shiehian. In this respect, it seems that lattice-based schemes form a promising solution for quantum-safe communications; however, implementation of such schemes requires a complete redesign of current protocol architectures that may lead to increased implementation complexity and performance overheads.

The balanced type of integration of these mechanisms that actually contributes to security enhancements hoped for at the expense of system performance is what the study brings out. The study by Rissi et. al (2024) explores the integration of hybrid PQC systems, combining classical and quantum-resistant algorithms, into TLS protocols. They offer insights into maintaining backward compatibility and transitional security, highlighting the complexities associated with these hybrid systems. Notably, the research points out that while such systems can provide robust security during the transition to quantum-resistant technologies, they also introduce significant challenges in terms of key management and protocol design, necessitating a careful and strategic implementation approach. Lattice-based cryptography has emerged as a robust solution for post-quantum security due to its strong theoretical foundations and resistance to both classical and quantum attacks. Recent advancements in lattice-based schemes have focused on optimizing performance and reducing computational overhead. Hasan et al. (2023) explored efficient implementations of the CRYSTALS-Kyber algorithm, demonstrating significant improvements in key generation and encapsulation times. Their findings suggest that with optimized hardware acceleration, lattice-based algorithms can be made viable for real-time applications.

Furthermore, Chen et al. (2024) conducted a comprehensive security analysis of lattice-based digital signatures in IoT environments, addressing challenges related to resource constraints and providing strategies for efficient key management and storage. These studies underline the importance of continuous optimization and practical implementation strategies to ensure the scalability and efficiency of lattice-based cryptographic solutions in diverse application domains. Table 2 provides a concise overview of significant studies in quantum cryptography, focusing on integrating and implications of Post-Quantum Cryptography (PQC) in various digital systems. Each entry summarizes the study's focus, methodology, key findings, and broader implications for advancing cryptographic practices in response to quantum computing advancements. This format facilitates quick comparisons and a clear understanding of the current landscape in quantum-resistant cryptographic research.

Table 2.
Summary of Key Studies on the Integration of Post-Quantum Cryptography in Digital Communication Systems

Study	Key Focus	Methodology	Findings	Implications
Scarani et al. (2009)	Quantum Key Distribution (QKD)	Analytical review	Uses quantum and classical channels for secure key exchange.	Highlights QKD's robustness in cryptographic communications.
P. Thanalakshmi et al. (2023)	Integration of PQC in blockchain	Case study analysis	Identifies computational and network overheads with NTRU in Ethereum.	Stresses the need for modular PQC integration in blockchain.
Halak et al. (2024)	Environmental impact of PQC	Comparative analysis	Increased energy use by Rainbow algorithm in blockchain.	Calls for energy-efficient cryptographic solutions in blockchain.
Bernstein et al. (2017)	Post-Quantum Cryptography (PQC)	Theoretical review	PQC provides resistance against quantum attacks.	Urges transition to quantum-resistant cryptographic practices.
Mink et al. (2010)	Integration of QKD in TLS	Theoretical and experimental analysis	Outlines methods for integrating QKD-based secrets into TLS.	Suggests QKD as a dependable security blueprint for TLS.
Giron et al. (2021)	Hybrid key exchange design	Conceptual critique	Discusses challenges in designing post-quantum hybrid key exchanges.	Highlights the need for new key agreement techniques.

Balamurugan et al. (2021)	Code-based cryptography	Technical analysis	Notes decoding complexity and error management challenges.	Advocates for advancements in code construction and error-correction.
Sabani ME et al. (2023)	Lattice-based key exchange	Detailed investigation	Lattice schemes need significant protocol redesigns for TLS integration.	Calls for balanced integration to maintain performance while enhancing security.
Rissi et al. (2024)	Hybrid PQC systems in TLS	Exploratory study	Highlights complexities of integrating classical and quantum-resistant algorithms.	Stresses strategic implementation for security during transition to PQC.

Mathematical Foundations and Theoretical Approaches in PQC Systems

This section deals with the very mathematical foundations that will enable the robust implementation of a PQC system within the digital communication infrastructure, for example, TLS. Quantum computing will definitely provide capabilities to break traditional cryptographic schemes; therefore, quantum-resistant methods are being explored (Ahn et.al 2023). We will consider only the root algorithms that form the backbone of PQC: lattice-based, hash-based, and multivariate polynomial-based cryptography. We outline each of these methodologies in terms of their core mathematical constructs, problem formulations, and the inherent quantum resistance they provide. This discussion elaborates on not only how these cryptographic techniques work but also assesses their practicality of implementation in running systems with regard to scalability, security, and computational efficiency (Huang et. al 2020). Theoretical models and equations are given for the operation mechanisms of these algorithms, drawing a clear view of the potential of these algorithms to secure communications against the threat of quantum decryption techniques.

Lattice-based cryptography

The lattice-based cryptography corresponds to computational hardness related to lattice problems. One of the basic questions in this field was introduced by Oded Regev in 2005: the Learning With Errors problem. The learning-with-errors problem has served as the base in the construction of myriad primitives, cryptographic in nature, because it supplies security proofs from worst-case hardness assumptions and possible quantum resistance (Wang et.al 2023).

Mathematical Representation

The general form of the LWE problem can be described as follows: given a set of linear equations where each equation adds a small error term to the result, the challenge is to solve for the unknowns despite these errors (John et al 2023). The equations are typically represented in the form: $A\,x \;\equiv\; b\,mod\;q$ where:

- A is a known matrix of dimensions m×nm,
- x is an unknown vector of length n
- b is a vector of length mmm that is the result of Ax perturbed by some small errors,

- q is a large prime number (modulus).

In the context of cryptography, the matrix A and the vector b would be public, while the vector x represents the secret key.

Key Generation and Encryption Processes

The classic private key in lattice-based cryptography is usually the vector S, while the public key is obtained from it with a process involving the generation of a random matrix A and the computation of another vector $\mathrm{p} = \mathrm{As} + \mathrm{e}$ where represents some small noise. In this case, recovering s from P directly is computationally infeasible without extra information. One-way Function: In encrypting a message, a sender uses the public key to create from the message a ciphertext that merges with aspects of the public matrix and vector (Huang et.al 2023). This process is often carried out with randomness and extra error added to smudge the real message.

Security Considerations

The security of lattice-based cryptography is rooted in the hardness of the LWE problem for classical and quantum computers. Indeed, we know such hardness from the worst-case complexity of the problems of finding short vectors in lattices, so-called SVP and CVP problems, which are presumably computationally hard (Aikata et.al 2023).

- **Classical Security:** The fact that the average-case LWE problem reduces from worst-case lattice problems can be interpreted as saying that an efficient algorithm for breaking LWE would translate to an efficient solution of these hard lattice problems, which, with currently available classical algorithms, is not likely (Mashhadi et.al 2023).
- **Quantum Security:** There do not exist, to date, quantum algorithms like Shor's algorithm, which efficiently solve problems such as integer factorization and discrete logarithms and have their equivalent to efficiently solve the LWE problem. Thus, LWE and its derivates are a promising way to deal with quantum-resistant cryptography (Wong et.al 2023).

The security level is often adjustable by changing parameters like the lattice dimension n, the modulus q. The error distribution characteristics balance computational efficiency against resistance to various attacks, wherein q.

Hash-Based Cryptography

Hash-based cryptography relies on cryptographic hash functions for the construction of digital signatures. One of the most famous hash-based schemes for digital signatures is the Merkle Signature Scheme, MSS (Sim et.al 2023). The system makes use of a binary tree where leaves are the hashes of message digests, whereas internal nodes are derived by hashing pairs of child nodes up to the root (Fregly et. al 2023).

Merkle Signature Scheme (MSS)

- Generate a large number of one-time key pairs; each consists of a private key and a corresponding public key.
- Tree Construction: Compute a hash value for each public key and use such values to form leaves of a binary tree. This way, the root will be representative of the public key for the whole Merkle tree.

- Signature Generation: To sign a message, a user needs to pick one of the one-time keys, sign the message using the private key, and finally supply the signature together with the authentication path, defined as the set of sibling nodes that are needed to reconstruct the root hash.
- Verification: It allows verifying a signature by reconstructing the root hash using a given public key, message signature, and an authentication path. If the reconstructed root hash turns out to be as in the public key, then it is a valid signature.

The following pseudocode outlines the key steps involved in the Merkle signature scheme:

```
$Algorithm\ KeyGeneration()$
  $for\ i = 1\ to\ n\ do$
    $(sk\_i, pk\_i) = GenerateOneTimeKeyPair()$
    $pk\_hash\_i = Hash(pk\_i)$
    $leaves[i] = pk\_hash\_i$
  $end\ for$
  $root = BuildMerkleTree(leaves)$
  $return\ (sk, pk = root)$


$Algorithm\ SignMessage(message, sk, leaves)$
  $i = SelectUnusedKeyPair(sk)$
  $signature = SignWithOneTimeKey(sk[i], message)$
  $auth\_path = ComputeAuthPath(leaves, i)$
  $return\ (signature, auth\_path)$


$Algorithm\ VerifySignature(message, signature, auth\_path, pk)$
  $root = ReconstructRootFromAuthPath(auth\_path)$
  $if\ root == pk\ and\ VerifyWithOneTimeKey(message, signature)\ then$
    $return\ true$
  $else$
    $return\ false$
  $end\ if$
```

Performance and Security Analysis

Efficiency: All in all, hash-based signatures provide decent computational efficiency at signature and verification ends. However, it adds latency due to the large number of hash calculations involved that may pose a problem in constrained resource environments.

Storage: Public keys and signatures can be large in size. Each OTS key pair has to be stored, and the size of the Merkle tree grows as the height of the tree h, grows. Security Considerations:

Quantum resistance: Due to the fact that it bases its security on the fundamental property of collision resistance of the underlying hash functions, hash-based cryptography is considered quantum-resistant. No known quantum algorithm demonstrates an efficient way to break this property.

Uses only once: Each signature key is usable only once, which complicates key management. In case of key reuse attacks, if not properly managed, it may introduce risks.

Forward Security: Due to the use of a Merkle tree, the scheme is forward secure; that is, even in the case when some keys are compromised, the past signatures remain safe.

▪ **Empirical Data:**

Empirical studies have established that, in fact, most hash-based signature schemes—SPHINCS+ included—are capable of reaching very high security levels with quite tolerable performance overheads. For example, benchmarking of SPHINCS+ assures 128-bit security with a signature size of about 41 KB and verification time below 1 ms on standard hardware, which should be sufficient in practice for most applications (López-Valdivieso et.al 2024).

Integration into TLS Protocols

This huge difference between classical and quantum-resistant cryptographic algorithms will make the integration process for PQC into the TLS protocols difficult. In this section, an analysis of challenges and propositions of corresponding solutions for the embedding of PQC into existing TLS frameworks is made (Tasopoulos et. al 2023).

▪ **Key Management and Distribution:** Turns out PQC algorithms often do require keys larger than those used in RSA and ECC. Handling and distribution of such large keys efficiently remains a problem given the constraints of existing TLS infrastructure.

▪ **Mathematical Equation:** Let $kclassic$ be the key size for classical cryptography and *kpqc* for PQC. Typically, $kpqc > kclassic$ increased size affects storage and transmission bandwidth: $Storage\ overhead = kpqc - kclassic$

▪ **Performance Overheads**

Challenge: On average, most post-quantum cryptographic algorithms add high computational and communication overheads. For instance, lattice-based algorithms involve complex mathematical operations that might slow the handshake within TLS.

Mathematical Equation: If $Tclassic$ is the time complexity for classical operations and *Tpq* for PQC operations, typically $Tpqc > Tclassic$. The increase in time complexity can be represented as: *Performance overhead=Tpqc−Tclassic*

- **Protocol Compatibility:**

Challenge: It should be integrated in a way that is guaranteed to coexist with previous versions of the TLS protocol. This means having backward compatibility with systems not supporting PQC.

Mathematical Equation: The compatibility could be checked with the protocol transition matrix PPP.*where: p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix} \]*. Here, \(p_{ij} \) is a depiction of the transition probability from classical to a state which is PQC compatible.

Case Study: SPHINCS+ Integration into TLS

The Figure 2 : is represented the integration of SPHINCS+ and Kyber into the TLS Handshake, protecting against quantum threats. First, a ClientHello message is sent by the client supporting PQC algorithms. Afterwards, the server replies with its ServerHello message and its certificate chain, signed under the algorithm SPHINCS+. This will include the root CA, intermediate CA, and server certificates. It then generates the key upon instruction from the server using Kyber and signs it with SPHINCS+; it sends the key back to the client. The latter verifies the certificate from the server, then does the key exchange with Kyber, sending back the certificate chain signed with SPHINCS+. Both client and server verify each other's certificates chain and perform the cryptographic operations needed to establish a secure session. The last steps update the cipher suite with ChangeCipherSpec messages and finish the handshake by sending Finished messages, setting up a strong quantum-resistant communication channel.

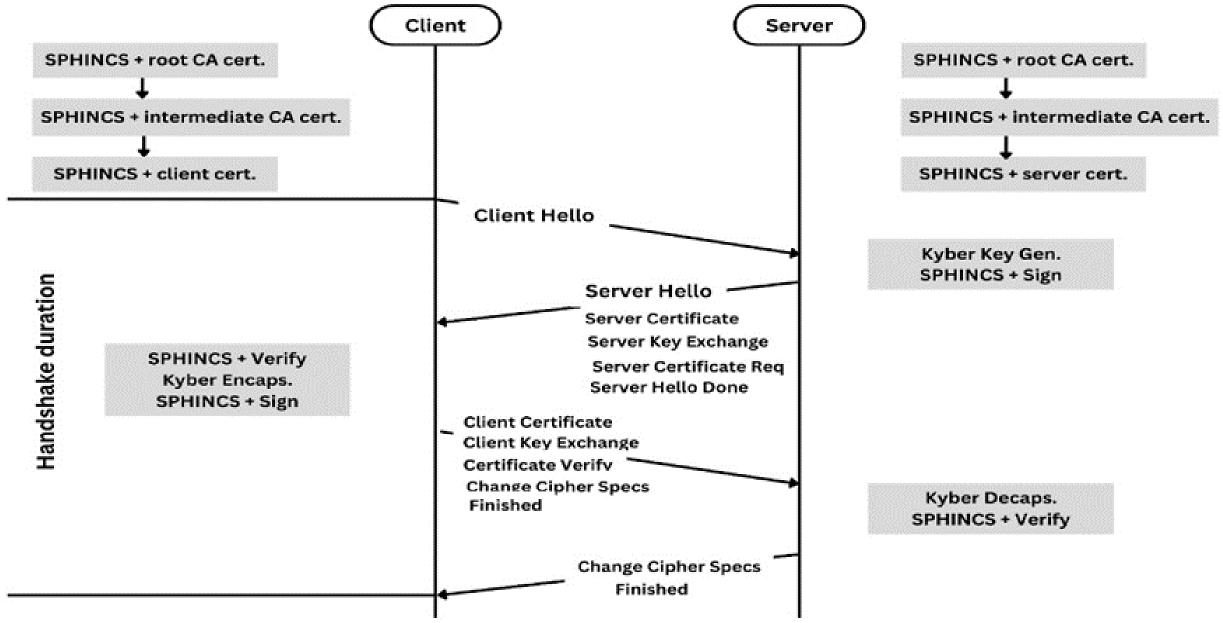

Figure 2.
SPHINCS+ Integration into TLS

Implementation Challenges

Implementation of post-quantum cryptography into existing TLS frameworks has many challenges. One of the essential challenges is the increase in key-size and computational requirements. Most PQC algorithms, in particular lattice-based, have larger key sizes than conventional cryptographic algorithms like RSA and ECC. Such an increase in key size would directly impact both storage and transmission bandwidth, leading to potential bottlenecks in performance. Besides, most of the PQC algorithms have been characterized by increased computational overhead, which obviously makes handshakes in TLS slower, mostly in computationally constrained environments. Integration also needs to ensure backward compatibility with existing versions of TLS; this careful design would mean smooth interoperability with non-PQC systems.

Integrate Proposed Solutions

Several modifications are proposed for the handshake process to effectively integrate PQC algorithms into TLS. This could be done by incorporating a hybrid mechanism of key exchange in adherence to both classical and PQC algorithms, so that even when one algorithm is compromised, the communication is still secure. In this regard, the TLS handshake process would have to be modified in support of these hybrid cipher suites including classical and PQC components. The ClientHello and ServerHello messages need an update for the inclusion of the respective added functionality. During the certificate exchange, the server and the client will be able to provide certificates signed with PQC algorithms like SPHINCS+. During the key exchange, algorithms like Kyber can be used in which the client and the server will perform the encapsulation and decapsulation operation for key exchange to share a secret. At the end of the handshake process, ChangeCipherSpec and Finished messages will be exchanged to establish a secure session using the keys secured by PQC.

Evaluation and Comparison of PQC Digital Signature Algorithms and TLS Certificates

The digital signature algorithms in PQC shall be evaluated for their adoption into the TLS Certificate, involving the following criteria for each. The effectiveness, efficiency, and security measures vary with every cryptographic algorithm in different practical applications; therefore, every one of these criteria is central to deciding the overall effectivity of the algorithms. Some of the critical criteria by which a reasonable evaluation can be done are as follows:

Security

- **Quantum Resistance:** This non-functional requirement checks the strength of the algorithm against quantum attacks. Quantum computers can solve some problems exponentially faster than classical computers, and based on this fact, some classical cryptographic algorithms are vulnerable. The algorithms should therefore resist possible quantum attacks by using Shor's algorithm to factor large integers and Grover's algorithm to search unsorted databases (Soni et. al 2024).
- **Classical Resistance:** In contributing a quantum-resistant algorithm, it has to be equally ensured that the algorithm faces no threat from classical attacks. This requires it

to be resistant to several cryptanalytic techniques and brute force attacks (Ruiz et. al 2024).

- **Security Assumptions:** Evaluation must consider the basic assumptions on the security that the algorithm has. Lattice-based cryptography can, for example, be based on hardness assumptions on lattice problems, and hash-based algorithms are based on the collision resistance of hash functions.

Computational Efficiency

- **Key Generation Speed:** Computational time taken to generate cryptographic keys is of great essence, especially in environments that require key changes quite often.
- **Encryption and Decryption Speed:** The time taken for the algorithm to compute both the encryption and decryption processes. This includes the real-time applications and computational overhead imposed by the algorithm on system performance.
- The digital signature algorithms are very essential, especially when it comes to the time required for generating and verifying the signature. Fast generation and verification of the signature are very important, particularly where the application has high throughputs and low latencies.

Key Size

- **Public Key Size:** The size of the public key is important because larger keys take up more storage and bandwidth for sending them. This is especially true in resource-constrained environments like IoT devices.
- **Private Key Size**: This is the size of the private key, which also affects storage and the general efficiency of the cryptographic operations.

Signature Size

- **Compactness:** The digital signatures by the algorithm should be as compact as possible. The smaller the size of the signature, the less data to be stored and sent over the network, hence increasing the efficiency in the process.
- The algorithm needs to be scaled up with large data sizes and computational resources. Scalability ensures that an algorithm will remain relevant to larger datasets and higher computational loads with increased performance. The algorithm has to be stable in cases of both cloud computing and blockchain technologies.
- **Error Rates:** The stability of any cryptographic algorithm can be judged by the error rates upon carrying out key generation, message encryption/decryption, and signature verification. An algorithm with a high error rate will make many retransmissions, and therefore, it will be less reliable in practice.
- **Ease of Integration:** This is how painless or not the algorithm would be integrated into existing systems and protocols, such as TLS. Algorithms that are fairly easy to implement, quite painless, and won't cause major overhauls in the current infrastructure should be preferred.
- **Resource Requirements:** This factor looks at the resources needed to run this algorithm, considering memory, processing power, and bandwidth for its smooth running on different hardware and software environments.

Resistance to Implementation Attacks

- **Side-channel attacks**: A degree in which an algorithm is resistant to both timing and power analysis attacks. Countermeasures for it should be in place to ensure a strong algorithm. Resistance to fault-injection attacks: this is where an algorithm is broken into by intentionally introducing some errors into it to be able to allow insecurity.
- The criteria for evaluation may be considered to make comprehensive the assessment toward the appropriateness of the different algorithms for PQC related to digital signatures in embedding within a TLS certificate for strong and efficient security in post-quantum computing environments.

Comparative Analysis

In order to give clear comparison, various PQC digital signature algorithms will be analyzed according to the criteria mentioned above. This will help in realizing the strengths and weaknesses of each algorithm under different scenarios. The evaluation of some key PQC digital signature algorithms can be summarized in the following table 3:

Table 3.
Comparative Analysis of PQC Digital Signature Algorithms

Criteria	XMSS	SPHINCS	FALCON	Analysis
Quantum Resistance	High	High	High	All are resistant to quantum attacks
Classical Resistance	High	Moderate	High	XMSS and FALCON offer better classical security
Key Size	2 KB	1 KB	700 B	FALCON has the smallest key size, advantageous in bandwidth-limited scenarios
Signature Size	4 KB	41 KB	1 KB	FALCON offers the smallest signatures, beneficial for frequent communications
Operation Speed	Slow	Moderate	Fast	FALCON provides the fastest operations, suitable for high-throughput environments
Scalability	Moderate	Good	Excellent	FALCON excels in scalability, ideal for large-scale applications
Error Rate	Low	Low	Very Low	FALCON shows the highest reliability
Integration Ease	Moderate	Moderate	Easy	FALCON is easier to integrate due to smaller sizes and higher speed
Resistance to Side-channel Attacks	Good	Poor	Excellent	FALCON provides robust security against side-channel attacks
Fault-injection Resistance	Good	Moderate	Excellent	FALCON shows superior resistance to fault attacks

Practical Implementation and Challenges

Intrinsic technical and logistical issues need to be accounted for when deploying PQC algorithms in real-world systems: hardware specifications, software compatibility, and seamless integration into existing cryptographic frameworks. PQC algorithms have progressively been used for secure communications, digital signature protocols, and blockchain technologies—each of these poses different challenges and requirements.

- **Hardware Requirements**: Almost all the PQC algorithms are computationally expensive, requiring good computational firepower. The hardware should support high-speed processing to accommodate the increased computational overhead of PQC algorithms without degradation of system performance.

- **Software Compatibility:** This is one more area that has to be taken care of while integrating PQC into the present software architectures. There can be incompatibility problems with older systems not designed for advanced features in PQC algorithms.

- **Cryptographic Infrastructure:** The integration process shall ensure that PQC algorithms can coexist with, and complement, classical cryptographic measures. In other words, cryptographic libraries and protocols will need to be upgraded to accommodate the use of classical and quantum-resistant techniques.

CHALLENGES AND SOLUTIONS

Challenges

- **Computational Overhead: The majority of algorithms in the PQC segment are computationally more** expensive than their classical equivalents. This additional computational overhead can cause slower system performance, especially during resource-constrained setup scenarios.

- **Key Size and Storage:** A lot of algorithms in PQC have keys of larger sizes; these require correspondingly higher storage and bandwidth for distribution and management. This can be particularly challenging in setup scenarios like mobile and IoT devices.

- **Backward Compatibility:** Any PQC solution should be compatible with older systems and protocols. Backward compatibility is challenging to maintain, more so because most of the older systems were not designed to accommodate PQC.

Solutions

- **Optimization Techniques:** Various advanced optimization techniques can be deployed that minimize the computational load of the PQC algorithms. Some techniques for reducing the burden on system resources may include fine-tuning algorithms, hardware acceleration, and improvement in software.

- **Hybrid Systems:** Provide hybrid cryptographic systems that have a mix of classical and quantum-resistant algorithms to make them compatible with previously installed infrastructure while not compromising on the security front.

- **Standardization:** Participate in ongoing standardization processes that are happening across global organizations like NIST. Standardization would ensure PQC implementation interoperability and adherence to benchmarks universally accepted, hence broadening its adoption and integration.

FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

The changing landscapes of quantum computing bring challenges and opportunities to cryptography. There exist some critical areas in which future PQC research needs to dwell, ensuring that digital security remains up to par with progress. Even though currently, most of the cryptographic algorithms being advocated are lattice-based, hash-based, and multivariate polynomial-based, future studies shall be backed by many more cryptographic algorithms. This shall underpin a robust cryptographic standard, resilient against unexpected vulnerabilities in any one algorithmic approach. Research will further concentrate on spotting and validating new intractable problems that are finally to form the bases of cryptographic systems to guarantee that they will not just be quantum-resistant but also efficient and practical for general use. There is an increasing call for collaboration between different scientific disciplines, making the development of PQC more effective. Significant breakthroughs in quantum-resistant cryptographic methods will be expected by drawing from computer science, mathematics, physics, and engineering. For instance, using principles of quantum mechanics in cryptographic algorithms could bring the most radical security solutions, which would stand a priori resistant to quantum attacks. Understanding the power of emerging technologies like machine learning in the optimization of cryptographic algorithms could be promising research. While this theoretical advancement is made, real-world implementation and testing of these quantum-resistant algorithms will come first; more emphasis will be required. This comprises full-scale field tests to determine the performance across a gamut of hardware and software configurations, most importantly in resource-constrained devices like IoT. Above all, completely new frameworks have to be designed so that these new algorithms are integrated into the present system without disruption of prevailing operations.

This shall include their scalability to hold up worldwide communication networks and adaptability to varied regulatory requirements from different jurisdictions. Especially in the realm of PQC integration, this is the case with digital signatures and TLS certificate integration. Digital signatures play a core role in checking message integrity and authenticity, while TLS certificates do the same in securing web links. In the future, careful study of the strength of PQC signatures in the Transport Layer Security protocol as a function of different network conditions and attack scenarios will have to be made. This is critical since TLS forms the backbone of secure Internet communications; any changes to certificate or encryption standards need to pass rigorous scrutiny. These directions indicate not only the continuous need for creative research in PQC but also underline the attention that needs to be placed in preparing for a quantum future. In this way, by focusing on these areas, the cryptographic community can anticipate and mitigate the risks associated with quantum computing much better and establish robust and secure digital communications in the post-quantum era.

CONCLUSION

This paper has explored the integration of Post-Quantum Cryptography (PQC) into TLS certificates to mitigate the emerging threats posed by quantum computing. We show that while PQC-based digital signature schemes available today especially the lattice-based, hash-based, and multivariate polynomial-based algorithms do support robust security enhancements, they also add complications regarding computational overhead and integration complexity. Further research in this regard should be focused on how to optimize PQC algorithms in general with respect to their computational footprint, specifically for resource-constrained deployments such as IoT devices. Some possible areas that can be looked at in the future are new key generation algorithms that could make the process more efficient and maybe lower latency in cryptographic operations. Another critical area of research in this direction is the adaptability of these PQC systems within existing network architectures, where minimal disruption while upgrading to quantum-resistant protocols might be desired. Broad deployment of PQC poses a number of challenges, one of which concerns how such solutions scale across different systems while remaining interoperable with the prevailing cryptographic infrastructure. Integration challenges must therefore become the focus of future studies in an attempt to facilitate transition processes for different industries, as well as to ensure that these new cryptographic measures do not cause any impairment in a system's performance. PQC in TLS certificates also comes with significant policy and regulatory considerations.

Global standardizing bodies are working toward harmonizing the protocols for quantum resistance. There is an important need for a dialogue with the policymaker to ensure that regulatory frameworks are evolved, securing the adoption of these technologies. These changes will have implications on global data protection laws, cybersecurity policies, and international commerce that must carefully be considered in order to guide the development of comprehensive and enforceable standards. Although technical challenges of every type crop up in this shift to PQC, this is a development the cryptographic world cannot afford to do without if threats from a quantum computing world are to be countered. Continued refinement of PQC technologies and cross-sector collaboration in handling practical and regulatory challenges allow the cryptographic community to set a safe pathway for digital communications in the post-quantum era.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor of research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., ... & Martin, V. (2019). The engineering of software-defined quantum key distribution networks. *IEEE Communications Magazine*, *57*(7), 20-26.

Aguilera, M. K., Burgelin, C., Guerraoui, R., Murat, A., Xygkis, A., & Zablotchi, I. (2024). DSig: Breaking the Barrier of Signatures in Data Centers. *arXiv preprint arXiv:2406.07215*.

Ahn, J., Kwon, H. Y., Ahn, B., Park, K., Kim, T., Lee, M. K., ... & Chung, J. (2022). Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). *Energies*, *15*(3), 714.

Aikata, A., Basso, A., Cassiers, G., Mert, A. C., & Roy, S. S. (2023). Kavach: Lightweight masking techniques for polynomial arithmetic in lattice-based cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(3), 366-390.

Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-quantum Key Exchange-A New Hope. In Proceedings of the USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016; pp. 327–343

Balamurugan C, Singh K, Ganesan G, Rajarajan M. Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions. *Cryptography*. 2021; 5(4):38. https://doi.org/10.3390/cryptography5040038

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188-194

Bos, J.; Costello, C.; Ducas, L.; Mironov, I.; Naehrig, M.; Nikolaenko, V.; Raghunathan, A.; Stebila, D. Frodo:Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE. In Proceedings of the 2016 ACMSIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; ACM:New York, NY, USA, 2016; pp. 1006–1018.

Chen, J., Deng, H., Su, H., Yuan, M., & Ren, Y. (2024). Lattice-Based Threshold Secret Sharing Scheme and Its Applications: A Survey. *Electronics*, *13*(2), 287.

Chen, L., et al. (2023). *Post-Quantum Cryptography: Current Status and Future Directions*. Journal of Cryptographic Engineering.

Cini, V., Lai, R. W., & Malavolta, G. (2023, August). Lattice-based succinct arguments from vanishing polynomials. In *Annual International Cryptology Conference* (pp. 72-105). Cham: Springer Nature Switzerland.

Darzi, S., Ahmadi, K., Aghapour, S., Yavuz, A. A., & Kermani, M. M. (2023). Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities. *arXiv preprint arXiv:2310.12037*.

De Clercq, R.; Roy, S.S.; Vercauteren, F.; Verbauwhede, I. Efficient software implementation of ring-LWEencryption. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE),Grenoble, France, 9–13 March 2015; pp. 339–344.

Fregly, A., Harvey, J., Kaliski Jr, B. S., & Sheth, S. (2023, April). Merkle tree ladder mode: reducing the size impact of NIST PQC signature algorithms in practice. In *Cryptographers' Track at the RSA Conference* (pp. 415-441). Cham: Springer International Publishing.

Giron, A. A. (2021). Encouraging the adoption of post-quantum hybrid key exchange in network security. In *Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6–9, 2021, Proceedings, Part II 17* (pp. 363-371). Springer International Publishing.

Halak, B., Gibson, T., Henley, M., Botea, C. B., Heath, B., & Khan, S. (2024). Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices. *IEEE Access*.

Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W., ... & McKague, M. (2024). A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies. *IEEE Access*.

Huang, B., Gao, J., & Li, X. (2023). Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing. *Journal of Cloud Computing*, *12*(1), 37.

Huang, Y., Huang, M., Lei, Z., & Wu, J. (2020). A pure hardware implementation of CRYSTALS-KYBER PQC algorithm through resource reuse. *IEICE Electronics Express*, *17*(17), 20200234-20200234.

Humble, T.S. Quantum security for the physical layer. IEEE Commun. Mag. 2013,51, 56–62

Javaid, M. A. R., Ashraf, M., Rehman, T., & Tariq, N. (2024). Impact of Post Quantum Digital Signatures On Block Chain: Comparative Analysis. *The Asian Bulletin of Big Data Management*, *4*(1), Science-4.

John, M. N., Udoaka, O. G., & Udoakpan, I. U. (2023). Group Theory in Lattice-Based Cryptography. *International Journal of Mathematics And Its Applications*, *11*(4), 111-125.

L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevicius, A.-A. O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post- ˇ quantum era privacy protection for intelligent infrastructures," IEEE Access, vol. 9, pp. 36038–36077, 2021

Liu, T., Ramachandran, G., & Jurdak, R. (2024). Post-quantum cryptography for internet of things: a survey on performance and optimization. *arXiv preprint arXiv:2401.17538*.

López-Valdivieso, J., & Cumplido, R. (2024). Design and implementation of hardware-software architecture based on hashes for SPHINCS+. *ACM Transactions on Reconfigurable Technology and Systems*.

Mashhadi, S., & Saeedi, Z. (2023). A (t, n)-Secret image sharing with steganography based on Rook polynomial and LWE problem. *Multimedia Tools and Applications*, *82*(25), 39077-39097.

Mink, A., Frankel, S., & Perlner, R. (2010). Quantum key distribution (QKD) and commodity security protocols: Introduction and integration. arXiv preprint arXiv:1004.0605.

Mukherjee, A. Physical-layer security in the Internet of Things: Sensing and communication confidentialityunder resource constraints. Proc. IEEE 2015,103, 1747–1761

NIST, "Post-quantum cryptography." https://csrc.nist.gov/projects/postquantum-cryptography, Jan 2017. Accessed 2023-3-24.

Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. *IEEE Access*.

Ruiz, J. (2024). Unusual and Unconsidered Mechanisms of Bacterial Resilience and Resistance to Quinolones. *Life*, *14*(3), 383.

Sabani ME, Savvas IK, Poulakis D, Garani G, Makris GC. Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era. *Electronics*. 2023; 12(12):2643. https://doi.org/10.3390/electronics12122643

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of modern physics*, *81*(3), 1301-1350.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), 303-332.

Sim, M., Eum, S., Song, G., Yang, Y., Kim, W., & Seo, H. (2023). K-XMSS and K-SPHINCS+: Enhancing Security in Next-Generation Mobile Communication and Internet Systems with Hash Based Signatures Using Korean Cryptography Algorithms. *Sensors*, *23*(17), 7558.

Soni, L., Chandra, H., Gupta, D. S., & Keval, R. (2024). Quantum-resistant public-key encryption and signature schemes with smaller key sizes. *Cluster Computing*, *27*(1), 285-297.

T. M. Fernandez-Caram ´ es, "From pre-quantum to post-quantum iot ´ security: A survey on quantum-resistant cryptosystems for the internet of things," IEEE Internet of Things Journal, vol. 7, pp. 6457–6480, July 2020

Thanalakshmi, P., Rishikhesh, A., Marion Marceline, J., Joshi, G. P., & Cho, W. (2023). A quantum-resistant blockchain system: a comparative analysis. *Mathematics*, *11*(18), 3947.

Wang, X., Xu, G., & Yu, Y. (2023). Lattice-Based Cryptography: A Survey. *Chinese Annals of Mathematics, Series B*, *44*(6), 945-960.

Williams, B.P.; Britt, K.A.; Humble, T.S. Tamper-indicating quantum seal. Phys. Rev. Appl. 2016,5, 014001

Wong, H. Y. (2023). Shor's Algorithm. In *Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps* (pp. 289-298). Cham: Springer International Publishing.

Yener, A.; Ulukus, S. Wireless Physical-layer security: Lessons learned from information theory. Proc. IEEE2015,103, 1814–1825