Proceedings of the 5th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/15/20230814

A research on quantum digital signatures

Haoxuan Duan

School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland, 1010, New Zealand

xtd8436@autuni.ac.nz

Abstract. This paper provides an overview of the basic principles, types, recent works, and applications of quantum digital signatures. The security of traditional digital signature schemes is compromised by the rise of quantum computing, leading to a need for post-quantum cryptography. Quantum digital signatures, which rely on the principles of quantum mechanics, offer a potential solution to this problem. This paper aims to provide a comprehensive overview of quantum digital signatures and post-quantum digital signatures. The paper introduces the basic principles of quantum mechanics, then explains key distribution in quantum digital signatures. The paper then provides a detailed description of both quantum and post-quantum digital signatures, including their differences and applications. Finally, the paper summarizes the main findings in the field, highlights potential future directions, and discusses challenges that humans must address. In addition, the paper examines the widespread applications of quantum digital signatures and post-quantum digital signatures in various fields such as Bitcoin, smart city blockchain, and finance. Finally, the paper summarizes the key findings in the field, highlighting potential future directions and discussing challenges that humans must address. Overall, this paper aims to provide readers with a comprehensive understanding of quantum digital signatures and post-quantum digital signatures and their applications in various domains.

Keywords: digital signatures, post-digital signatures, bitcoin, blockchain.

1. Introduction

In recent years, quantum computing has emerged as a promising technology that could revolutionize the field of cryptography. While quantum computers offer many potential benefits, they also pose a significant threat to traditional cryptographic schemes, which rely on challenging mathematical problems that classical computers can effectively solve. The solution to the mathematical problem led to the development of post-quantum cryptography schemes to resist attacks by classical and quantum computers. This survey aims to understand quantum digital signatures and their security potential comprehensively.

A highly promising approach in post-quantum cryptography is the utilization of quantum digital signatures. Quantum digital signatures use the tenets of quantum mechanics to derive secure digital signatures resilient to the attacks of classical and quantum computers. These signatures are all based on properties of quantum states, such as superposition and entanglement, and provide a way to verify the authenticity and integrity of digital information.

This paper's structure is as follows. The first section outlines the basic principles of quantum mechanics and cryptography, including required distribution, message signing, and verification. Section

DOI: 10.54254/2755-2721/15/20230814

2 discusses quantum digital signature schemes, including lattice-based, code-based, multivariate-based, LPN-based, and hash-based schemes. In the third part, this paper discusses the applications of quantum digital signatures in various fields, such as finance, blockchain, and innovative city systems. Finally, this paper summarizes the paper's main findings and discusses future research directions in quantum digital signatures.

2. Basic principles of quantum digital signature

2.1. Basic principles of quantum mechanics

2.1.1. Quantum bits (Qubits). Quantum bit is an abbreviation for a quantum bit, the basic unit of quantum information, which plays a crucial role in quantum computing. They are a quantum analogy of classical bits, but unlike classical bits, they can exist as a superposition of two possible states |0⟩ and|1⟩ [1].

For simplicity, the general rule is$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$,$|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$.

These states form a standard set of orthogonal bases in quantum computing, commonly called computational bases. An arbitrary quantum state |φ⟩ can express as a linear combination of |0⟩ and |1⟩: $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle=\begin{bmatrix}\alpha\\\beta\end{bmatrix}$…… ①, with α and β being complex coefficients.

A quantum state |φ⟩ shaped like a ① is called a quantum bit or qubit. Eq. ① demonstrates the superposition nature of the quantum state, i.e., |φ⟩ is at |0⟩ and|1⟩ any superposition state, while a classical bit can only be 0 or 1.

Because $|\alpha|^2+|\beta|^2=1$, The superposition state of qubits can write as $|\varphi\rangle=e^{i\gamma}\left(cos\frac{\theta}{2}\middle|0\rangle+e^{i\varphi}sin\frac{\theta}{2}|1\rangle\right)$. Here, θ, φ, and γ are real numbers. Since $e^{i\gamma}$ has no pronounced effect, this paper can ignore it. So, it can abbreviate as $|\varphi\rangle=e^{i\gamma}\left(cos\frac{\theta}{2}\middle|0\rangle+e^{i\varphi}sin\frac{\theta}{2}|1\rangle\right)$. θ and φ define a point on the unit's three-dimensional sphere. This ball calls a Bloch ball, as shown in Figure 1.

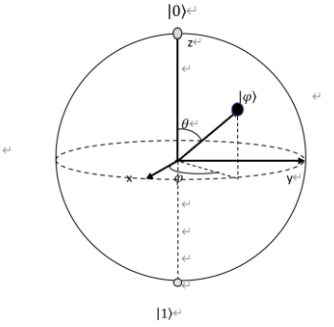

Figure 1. Bloch sphere representation of a Qubit.

2.1.2. Quantum superposition. Quantum superposition is a foundational concept of quantum mechanics, describing the ability of a quantum system to survive in multiple states simultaneously. In classic physics, an object may only be in one place simultaneously, but in the quantum world, particles can be simultaneously in multiple locations.

The concept of quantum superposition has been confirmed experimentally through numerous experiments, such as the double-slit experiment, where a beam of particles is sent through two slits and forms an interference pattern on a screen [2]. The pattern can only be explained by the particles existing in a superposition of states, with a probability distribution determined by the wave function.

In a quantum computer, quantum bits, or qubits, can survive in numerous states simultaneously, allowing for massively parallel processing. However, superposition is a fragile state easily disrupted by external

DOI: 10.54254/2755-2721/15/20230814

factors, such as noise and environmental interactions. Thus, understanding and controlling superposition is a crucial challenge in developing practical quantum technologies.

2.1.3. Quantum entanglement. Quantum entanglement describes a phenomenon where the states of two or more quantum systems become correlated, even when separated by large distances. This phenomenon has been observed experimentally and now recognize as a fundamental property of quantum mechanics.

Einstein, Podolsky, and Rosen first introduced the concept of quantum entanglement in a 1935 paper. They argued that entanglement violates the principle of local realism, which states that physical processes should be explainable without the need for non-local influences [3]. However, many experiments have experimentally confirmed entanglement, including the famous Bell test, which proved that local hidden variables could not explain entanglement [4].

In quantum cryptography, entanglement is used to distribute cryptographic keys that are secure against eavesdropping. Attempting to intercept the keys will change the entangled state, and the parties will immediately detect the interference. In quantum computing, entanglement performs operations on multiple qubits simultaneously, enabling massively parallel processing that is impossible with classical computers [5].

Despite its potential applications, quantum entanglement remains challenging to understand and control. Its fragility makes it difficult to maintain entangled states in real-world conditions, and decoherence can quickly destroy entanglement. However, ongoing research continues to explore the possibilities and limitations of entanglement in various fields, from quantum computing to quantum metrology. It expects to play a significant role in developing future technologies.

2.2. Quantum digital signatures

2.2.1. Quantum cryptography. (1) Key distribution. Quantum key distribution (QKD) is an encryption protocol that empowers two sides to share a secret key over an unsecured transmission channel in a provably secure manner [6]. QKD, based on the laws of quantum mechanics, provides a means to detect any eavesdropper attempting to intercept or manipulate the transmitted information [6]. The securities of QKD are based on several fundamental tenants of quantum mechanics, for instance, the no-cloning theorem, the Indeterminacy Principle, and the entanglement of quantum states [6].

While practical implementations of QKD can be subject to various attacks and vulnerabilities, research has proposed techniques to mitigate them, such as decoy-state protocols, measurement-device-independent QKD, and trusted-device architectures [6]. QKD has attracted growing interest as a potential technology for secure communication in various applications, such as financial transactions, military communications, and data privacy [7].

QKD's development milestones include the first demonstration by Bennett and Brassard in 1984 [8], the introduction of the BB84 protocol by Bennett and Brassard in 1984 [9], and the first long-distance demonstration over a fiber-optic network by Hughes et al. in 2002 [10]. Numerous experimental demonstrations of QKD have been reported in the scientific literature [11].

Overall, QKD provides a strong foundation for developing future cryptographic technologies to enhance security in various applications.

(2) Using Quantum Mechanics for Message Signing and Verification. a) Eve, as the legitimate party, intercepts and manipulates the quantum gateway between the corresponding parties to perform a man-in-the-middle attack. See Figure 2.

b) During quantum key distribution (QKD), the sender transmits a quantum signal to the receiver through a quantum channel, while classical processing occurs over a classical channel using the shared information. To validate the information, Alice and Bob generate a summary using a hash function. Bob encrypts his summary using a pre-shared or private key and sends the encrypted label to Alice. Alice decrypts the label using the same key and compares it to her summary. If they coincide, authentication is successful. A two-way verification is conducted, with Bob also authenticating Alice's identity, as illustrated in Figure 2.

DOI: 10.54254/2755-2721/15/20230814

c) Alice and Bob exchange credentials and nonce, employing the certificate authority's public key to verify each other's public keys. They sign the message digest and non-nonce using their respective private keys to create a signature. They then use each other's confirmed public keys to verify the signatures and confirm that the messages are legally signed. Bit strings are concatenated using ‖ notation [12].

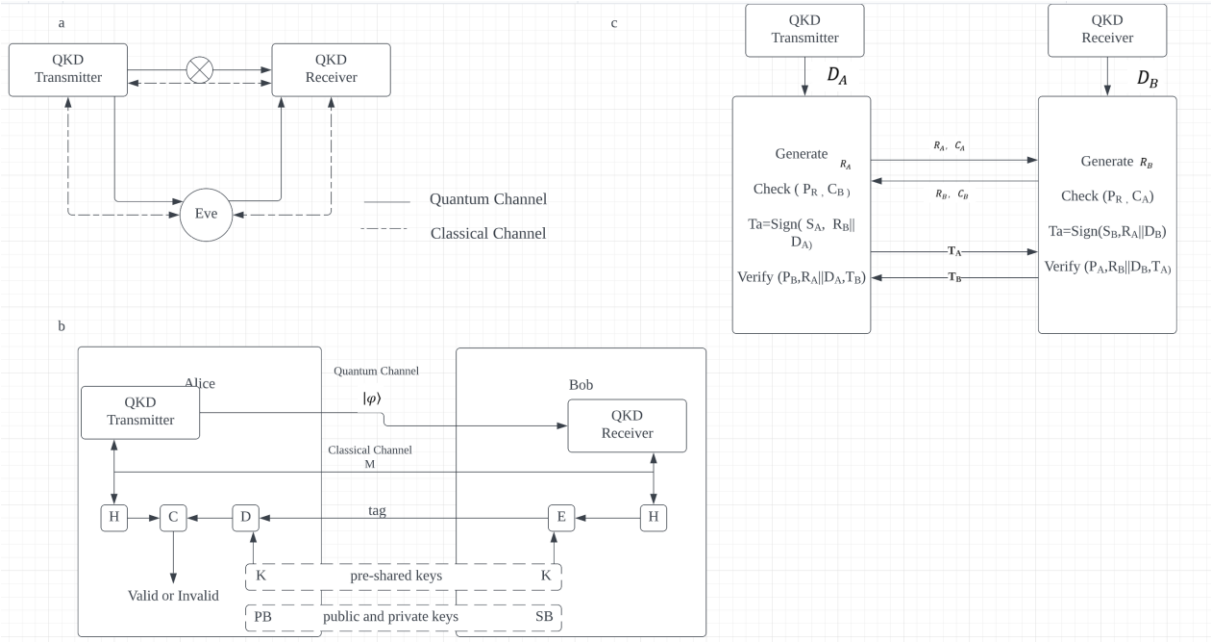

Figure 2. Schematic of a man-in-the-middle attack and flow diagram of post-quantum cryptography authentication. (From Experimental authentication of quantum key distribution with post-quantum cryptography).

2.2.2. Quantum digital signatures. Quantum digital signatures (QDS) offer a secure method for validating the authenticity and integrity of digital data by leveraging quantum mechanics principles, including quantum superposition, quantum entanglement, and the no-cloning theorem [8]. Quantum superposition allows quantum states to exist simultaneously in multiple states, while quantum entanglement links the properties of separate quantum particles, even when they are far apart. It is impossible to make an exact duplicate of an unidentified quantum state, according to the no-cloning theorem, which is a fundamental premise of quantum mechanics. This feature prevents an attacker from forging a quantum signature.

The working principle of QDS involves encoding a message into a quantum state, performing a series of quantum operations to generate a signature, and transmitting the signature along with the message over a classical communication channel. The message recipient can subsequently employ a quantum measurement to confirm the message's authenticity and integrity [7].

One advantage of using quantum signatures is their inherent security, as they rely on the laws of quantum mechanics to prevent tampering or eavesdropping by an attacker. Additionally, quantum signatures can provide a secure method for key distribution, allowing two parties to establish a shared secret key for use in encryption and other cryptographic protocols.

Challenges and limitations of quantum digital signature schemes include maintaining and transmitting quantum states and the need to develop practical and scalable quantum communication technologies. As quantum states are susceptible to their environment, preserving their coherence and preventing decoherence during transmission is a significant challenge.

2.2.3. The post-quantum digital signature. Post-quantum digital signatures are a crucial cryptography component that provides secure communication channels resistant to quantum computer attacks. With

DOI: 10.54254/2755-2721/15/20230814

the increasing power of quantum computers, traditional signature schemes become vulnerable to attacks, and therefore, post-quantum digital signatures offer a solution for maintaining the security of digital communications. In recent years, significant research has been conducted on post-quantum digital signature schemes, including lattice-based, code-based, multivariable-based, hash-based, and LPN-based schemes. For example, in a paper published in 2021, Tang et al. proposed a new post-quantum digital signature scheme based on binary Goppa codes [13]. The proposed scheme has a minor key size and faster signing and verification than other code-based signature schemes, making it a promising candidate for resource-constrained environments. Such research on post-quantum digital signature schemes is essential for ensuring the security of digital communications in the face of the growing threat of quantum computers.

3. Types of post-quantum digital signature schemes

Table 1. Basic types of quantum digital signatures.

Method	Description	Advantage	Disadvantage
Lattice-based [14-16]	Uses private critical operations on a message to create a digital signature	Minor key size resists classical & quantum attacks, widely used	Vulnerable to channel attacks (e.g., power analysis, timing)
Code-based [17-18]	Encodes message into linear code, adds extra info using the private key	Post-quantum security, relatively simple, well-researched	Limited adoption, expensive, large key, low efficiency
Multivariable-based [19-20]	Applies mathematical operations using a private key	Fast computation speed	Sizeable key size, prone to channel attacks
Hash function–based [21-22]	Hashes message generates a signature using hash and private key	Highly simple and efficient	Slight risk of information leakage
LPN-based [23-24]	Based on the hardness of the LPN problem	Smaller key size compared to other schemes	Vulnerable to quantum attacks

Table 1 compares five post-quantum digital signature schemes: lattice-based, code-based, multivariable-based, hash-based, and LPN-based. Lattice-based schemes are small in size but vulnerable to channel attacks [14][15][16]. Code-based schemes are resistant to quantum attacks but expensive and inefficient [17][18]. Multivariable-based schemes are fast and efficient but have a large key size and are prone to channel attacks [19][20]. Hash-based schemes are simple and efficient but have little information leakage risk due to hash functions [21][22]. LPN-based schemes have a minor key size but are vulnerable to quantum attacks [23][24]. Choosing a post-quantum digital signature scheme depends on specific application requirements, including security level, available resources, and acceptable trade-offs between efficiency and security.

3.1. Lattice-based

In recent years, lattice-based cryptography has gained attention as a potential solution for post-quantum digital signature schemes. A review of lattice-based cryptography and its potential for quantum digital signatures is provided in [14]. This article discusses the advantages and limitations of lattice-based schemes, including their ability to resist classical and quantum attacks but vulnerability to certain types of side-channel attacks. Another article [15] focuses on applying lattice-based cryptography in digital signature schemes, highlighting the potential advantages of smaller key sizes, faster signature generation times, and post-quantum security. However, the authors also acknowledge the limitations and vulnerabilities of these schemes. Finally, article [16] assesses the practical security of lattice-based post-

DOI: 10.54254/2755-2721/15/20230814

quantum cryptographic schemes against side-channel and fault-injection attacks. This article emphasizes the need for careful implementation and testing to ensure the security of these schemes. Despite the challenges and limitations, lattice-based digital signatures offer a promising approach to achieving secure and efficient digital signature schemes resistant to quantum attacks.

3.2. *Code-based*

The article [17] presents a quantum-resistant digital signature scheme based on the Lyubashevsky framework, which incorporates principles of quantum mechanics to ensure security against quantum computer attacks. The motivation for this work is to develop post-quantum digital signatures resistant to quantum computer attacks, considering the potential threat of quantum computers to traditional digital signature schemes. The proposed scheme uses a code-based construction resistant to classical and quantum attacks, leveraging the underlying principles of quantum mechanics to achieve this level of security.

The survey of code-based digital signatures in [18] provides a comprehensive overview of these post-quantum encryption schemes that resist attacks from classical and quantum computers. While the article does not explicitly emphasize quantum digital signatures, it presents code-based digital signatures as a potential solution to the threat posed by quantum computers. The survey acknowledges some limitations of these schemes, such as their relatively large vital sizes and slow computation times compared to traditional schemes. It also highlights the most recent research and developments in the field of quantum digital signatures, providing readers with the most up-to-date information on state of the art in this area. Overall, the proposed code-based signature scheme from the Lyubashevsky framework in [17] addresses the need for quantum-resistant digital signatures and presents a scheme resistant to classical and quantum attacks. The scheme has several advantages, including small signature and public key sizes, fast signing and verification, and resistance to classical and quantum attacks. However, it also has some limitations, such as the need for a trusted setup and the potential for some side-channel attacks.

3.3. Multivariable-based

The article [19] proposes a new digital signature scheme based on multivariate polynomial cryptography resistant to classical and quantum attacks. The scheme aims to provide post-quantum security in digital signatures, as traditional signature schemes are vulnerable to quantum computers. The article analyzes the proposed scheme's security and performance compared to other post-quantum signature schemes, highlighting its advantages, such as small vital sizes, fast signing, and verification. However, the scheme may be vulnerable to side-channel attacks. The article emphasizes the importance of developing quantum-safe digital signature schemes to prepare for the potential threat of quantum computers to traditional signature schemes.

The article [20] investigates the security of two post-quantum signature schemes, UOV and Rainbow, against fault attacks. The authors present a detailed analysis of the vulnerabilities of these schemes to fault attacks and propose countermeasures to mitigate these attacks. The article discusses the advantages and disadvantages of these schemes compared to other post-quantum signature schemes. However, the article does not explicitly focus on quantum digital signatures but rather on the vulnerability of post-quantum signature schemes to fault attacks. Nonetheless, the article provides important insights into the security of post-quantum signature schemes. It highlights the need for further research to ensure the robustness of these schemes against both classical and quantum attackers.

3.4. Hash function-based

The article [21] reports on an experimental implementation of a secure quantum network that uses digital signatures and encryption. The proposed scheme employs quantum key distribution for encryption and a hash-based digital signature scheme for authentication. The motivation for this work is to provide secure communication channels resistant to quantum computer attacks. The article describes the implementation of the network and presents a detailed analysis of its security and performance. The proposed scheme has several advantages, including resistance to classical and quantum attacks and

DOI: 10.54254/2755-2721/15/20230814

providing secure communication channels over long distances. The plan does have some drawbacks, though, such as the requirement for specialist tools and the potential for some side-channel attacks. The paper highlights the potential of secure quantum networks in achieving secure communication channels resistant to attacks from quantum computers.

In their paper [22], Li et al. propose a one-time universal hashing quantum digital signature scheme that does not rely on perfect keys. The authors describe their method for constructing one-time universal hash functions using the Gottesman-Chuang stabilizer formalism and show how these can be used to sign messages in a quantum digital signature scheme. The motivation for this work is to develop more secure digital signatures that can resist attacks from quantum computers. The advantages of this approach include its simplicity, efficiency, and security against quantum attacks. However, the scheme has some limitations, such as a higher rate of false positives than traditional digital signatures and the need to manage secret keys carefully. Further research could focus on improving the scheme's performance and addressing these limitations to make it more suitable for practical applications.

The second article [22] proposes a one-time universal hashing quantum digital signature scheme resistant to attacks from quantum computers but also has some limitations, such as a higher rate. In contrast, the first article [21] presents an experimental implementation of a secure quantum network using digital signatures and encryption based on hash functions, which may have some limitations in terms of security and potential side-channel attacks. Therefore, further research and development are needed to improve the security and performance of quantum digital signature schemes based on hash functions.

3.5. LPN-based

Article [23] provides an overview of post-quantum cryptography (PQC), discussing its challenges and prospects for strong and secure hardware design. The authors emphasize the learning parity-with-noise (LPN) problem, which underpins numerous PQC schemes, including digital signature schemes. This paper introduces the LPN problem and its security properties and describes several LPN-based digital signature schemes, including the recent GeMSS scheme. The authors discuss the advantages and limitations of LPN-based digital signature schemes, such as their resilience to quantum attacks and relatively low computational cost. They also point out the need for careful parameter selection to ensure security. This paper provides valuable insights into the challenges and opportunities of PQC- and LPN-based digital signature schemes for robust and secure hardware designs.

The paper [24] proposes a machine-learning framework that tolerates physical noise or errors in hardware. The authors describe their approach to modeling physical noise or errors in hardware and show how it can be incorporated into the training process to improve the accuracy of machine learning models. The advantages of this approach include its ability to improve the robustness of machine learning models in the presence of physical noise or errors and its potential to reduce the need for expensive and time-consuming hardware testing. However, the scheme also has some limitations, such as the need to carefully calibrate the noise or error model and the potential for increased computational complexity. Although the paper by Kamel et al. [24] proposes a machine-learning framework that can tolerate physical noise or hardware errors, it is not directly related to LPN-based quantum digital signatures.

When comparing quantum digital signature schemes, the survey considers key size, efficiency, and security factors. To provide a more detailed comparison, specific security levels or performance benchmarks should be included as criteria, allowing for a clearer understanding of the strengths and weaknesses of each scheme. Additionally, discussing practical implementations and real-world applications of quantum digital signature schemes would offer insight into the potential use cases and practical implications of these schemes in various industries and contexts.

Future research directions in quantum digital signatures include addressing open problems and challenges related to efficiency, key size, and resistance to side-channel attacks. Furthermore, the research could focus on developing new cryptographic primitives based on quantum mechanics principles to enhance the security of digital signature schemer further.

DOI: 10.54254/2755-2721/15/20230814

4. Application of quantum digital signature

Table 2. Applications of quantum digital signatures.

Application	Description
Bitcoin [25-26]	Using quantum digital signatures to secure Bitcoin.
Smart city blockchain [27]	Everyone can protect the blockchain, and Everyone can still mine it.
Finance [28]	In finance, only security analysis and proposals must be widely used after people agree.

Table 2 summarizes several potential applications of quantum digital signatures. In the case of Bitcoin, researchers have compared classical and post-quantum digital signature algorithms to protect Bitcoin transactions. In the context of intelligent city blockchains, quantum digital signatures can help protect the blockchain while still allowing mining. Finally, quantum digital signatures can be used in the financial sector for security analysis and proposals after people have consented. These applications demonstrate the potential versatility of quantum digital signatures in various fields and highlight their importance for protecting sensitive information.

4.1. Bitcoin

Noel et al. conducted a comparison between classical and post-quantum digital signature algorithms employed in Bitcoin transactions [25]. The authors evaluate the performance of several post-quantum algorithms based on the hash function, including the XMSS, SPHINCS+, and WOTS+ schemes, and compare them to the widely used ECDSA algorithm. They show that post-quantum algorithms provide better security against quantum attacks but with increased computational complexity and larger signature sizes. León-Chávez et al. propose a hash-based digital signature scheme resistant to quantum attacks and can be implemented on current Bitcoin hardware [26]. The authors assess their scheme's performance by examining the signature size and verification time, and they compare these results with other post-quantum digital signature schemes. The proposed scheme is compatible with existing Bitcoin infrastructure and has a low computational cost. However, the scheme also has some limitations, such as its larger signature size compared to some classical schemes and the need for careful parameter selection. Both papers highlight the need for post-quantum algorithms to ensure the long-term security of the Bitcoin blockchain. These studies provide valuable insights into applying post-quantum digital signatures based on hash functions in protecting Bitcoin transactions.

4.2. Smart city blockchain

The article by Chen et al. presents a post-quantum blockchain construction for innovative city applications using quantum digital signatures [27]. The motivation behind this work is to address the security challenges of existing blockchain systems in the era of quantum computing. The authors propose a post-quantum blockchain framework that employs quantum digital signatures based on hash functions to ensure the security and privacy of innovative city applications. They evaluate the performance of their proposed framework using various innovative city scenarios and show that it outperforms existing blockchain solutions in terms of security and efficiency. The advantages of using quantum digital signatures include their resistance to quantum attacks, enhanced security and privacy, and the ability to support new cryptographic primitives. However, the authors also acknowledge some limitations, such as the need for specialized hardware and software to implement quantum digital signatures and the potential impact of future developments in quantum computing. Overall, this article provides valuable insights into the potential applications of quantum digital signatures in blockchain systems for innovative city applications.

DOI: 10.54254/2755-2721/15/20230814

4.3. Finance

The essay by J. Hayes [28] explains how quantum computing might be used in the financial sector. This work is motivated by the need for faster and more secure financial transactions and the limitations of classical computing in meeting these challenges. The authors emphasize the potential of quantum computing in fields like portfolio optimization, risk assessment, fraud detection, and cryptography. They discuss quantum computing methods and algorithms, such as Shor's algorithm, Grover's algorithm, and quantum annealing, which can be applied in the financial sector. The advantages of quantum computing in finance include faster and more efficient computing, better risk management, and improved security through quantum digital signatures. However, there are challenges and limitations to adopting quantum computing in finance, such as the need for dedicated hardware, the high cost of quantum computing, and the potential security risks associated with quantum cryptography. Overall, this research offers insightful information about the possible uses and restrictions of quantum computing in the financial services industry.

5. Conclusion

This investigative paper provides an overview of quantum digital signatures, a promising approach to secure and real-world digital communication in the post-quantum era. This article first describes the importance of digital signatures in modern communications and the threat of quantum computers. This article then explores the fundamental principles of quantum mechanics and quantum cryptography and how they can be used for message signing and verification. This paper then discusses the types of quantum digital signature schemes, including lattice-based, code-based, multivarious-based, and hash-based LPN-based. The advantages and limitations of each scenario are discussed. The challenges and opportunities of future research in quantum digital signatures are summarized. Future research directions in quantum digital signatures should address the open problems and challenges related to efficiency, key size, and resistance to side-channel attacks. Developing new cryptographic primitives based on quantum mechanics principles could further enhance the security of digital signature schemes. Additionally, exploring practical implementations and real-world applications of quantum digital signature schemes will offer valuable insights into their potential use cases and implications in various industries and contexts. Researchers should also investigate the integration of quantum digital signatures with other emerging technologies, such as blockchain, to leverage their potential for secure and efficient communication and transactions in the quantum era.

References

[1] Mullamuri B 2021 *ProQuest Dissertations* Publishing Enabling Quantum Cryptography Using Quantum Computer Programming p 28864879.
[2] Bouwmeester D and Zeilinger A 2000 *The Physics of Quantum Information* The Physics of Quantum Information: Basic Concepts Berlin Heidelberg.
[3] A. EinsteinPodolsky and N. RosenB 1935 Can Quantum-Mechanical Description of Physical Reality Be Complete?
[4] Bell JS 1964 Physics On the Einstein-Podolsky-Rosen paradox vol 1 pp 195-200.
[5] Chuang DG 2001 Quantum digital signatures.
[6] J. Mullins 2001 *IEEE Spectrum* The topsy turvy world of quantum computing.
[7] 2018 *Springer Science and Business Media LLC* Applied Cryptography and Network Security
[8] D. Gottesman and I. Chuang, 2001 *arXiv preprint* Quantum digital signatures.
[9] Pramode K. Verma, Mayssaa El Rifai and Kam Wai Clifford Chan 2019 *Springer Science and Business Media LLC* Multi-photon Quantum Secure Communication.
[10] Delpech De Saint Guilhem and Cyprien P. R. 2021 *University of Bristol (United Kingdom) ProQuest Dissertations* Publishing On the Theory and Design of Post-Quantum Authenticated Key-Exchange, Encryption, and Signatures.
[11] Marius Nagy and Selim G. Akl 2006 *International Journal of Parallel Emergent and Distributed Systems* Quantum computation and quantum information.

DOI: 10.54254/2755-2721/15/20230814

[12] Liu-Jun WangZhang, Jia-Yong Wang, Jie Cheng, Yong-Hua Yang, Shi-Biao Tang, Di Yan, Yan-Lin Tang, Zhen Liu, Yu Yu, Qiang Zhang and Jian-Wei PanKai-Yi 2021 *npj Quantum Information* Experimental authentication of quantum key distribution with post-quantum cryptography vol 7.
[13] TangLi X, Hu X, Wang R and Zeng XY 2021 *IEEE Access* A New Post-Quantum Digital Signature Scheme Based on Binary Goppa Codes pp 164530-164543.
[14] Yu Y 2021 *National Science* Review Preface to special topic on lattice-based cryptography vol 8.
[15] Lyubashevsky V 2021 *National Science Review* Lattice-based digital signatures vol 8.
[16] Ravi, Chattopadhyay, A, D'Anvers, J. P and Baksi A 2022 Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results.
[17] Song Y, Huang X, Mu Y, Wu W and Wang H 2020 *Theoretical Computer Science* A code-based signature scheme from the Lyubashevsky framework vol 835 p 15-30.
[18] SONG Y. 2021 *Chinese Journal of Network and Information Security* Survey of code-based digital signatures vol 7 pp 1-17.
[19] Kuang R, Perepechaenko M and Barbeau M 2022 *Scientific Reports* A new quantum-safe multivariate polynomial public key digital signature algorithm.
[20] Krämer J and Loiero M 2019 *Lecture Notes in Computer Science book series (LNSC)* Fault attacks on UOV and Rainbow vol 11421 pp 193-214.
[21] Yin H, Fu Y, Li C, Weng C, Li B, Gu J, Lu Y, Huang S and Chen Z 2022 *National Science Review* Experimental quantum secure network with digital signatures and encryption.
[22] Li B, Xie Y, Cao X, Li C, Fu Y, Yin H and Chen Z 2023 *Quantum Physics (quant-ph) Cryptography and Security* One-Time Universal Hashing Quantum Digital Signatures without Perfect Keys.
[23] Bellizia D, El Mrabet N, Fournaris A. P, Pontié S, Regazzoni F, & Standaert F. X, Tasso É and Valea E 2021 *IEEE International Symposium on Hardware* Oriented Security and Trust Challenges and Opportunities for Robust and Secure HW Design.
[24] Kamel D, Standaert F, Duc A, Flandre D and Berti F 2020 *IEEE Transactions on Dependable and Secure Computing* Learning with physical noise or error vol 17 pp 957-971.
[25] Noel MD, Waziri OV, Abdulhamid MS, Ojeniyi AJ and Okoro MU 2020 *IEEE* Comparative Analysis of Classical and Post-quantum Digital Signature Algorithms used in Bitcoin Transactions.
[26] León-Chávez M Á, Perin LP and Rodríguez-Henríquez F 2022 *Springer* Post-Quantum Digital Signatures for Bitcoin Principles and Practice of Blockchains pp 251-270.
[27] Chen J, Gan W, Hu M and Chen C M 2021 *Journal of Information Security and Applications* On constructing a post-quantum blockchain for a smart city vol 102780.
[28] Hayes J 2019 *Engineering & Technology Quantum* on the money: Quantum computing in financial services sector vol 14 pp 34–37.