Assessing the Vulnerability of Traditional and Post-Quantum Cryptographic Systems through Penetration Testing and Strengthening Cyber Defenses with Zero Trust Security in the Era of Quantum Computing

Nonso Okika[1]; Gift Aruchi Nwatuzie[2]; Hamed Salam Olarinoye[3]; Augustine A. Nwaka[4]; Emmanuel Igba[5]; Roland Dunee[6]

[1]Network Planning Analyst University of Michigan, USA.
[2]Department of Computer Systems Engineering, University of East London, United Kingdom
[3]Department of Information Technology and Decision Sciences, Walsh College, Troy Michigan, USA
[4]School of Cyber Security and Privacy, Georgia Institute of Technology, Atlanta, Georgia, USA
[5]Department of Human Resource, Secretary to the Commission, National Broadcasting Commission Headquarters, Aso-Villa, Abuja, Nigeria.
[6]College of Engineering, Carnegie Mellon University Africa, Kigali, Rwanda

Publication Date: 2025/03/04

Abstract: The rapid advancement of quantum computing poses a significant threat to traditional cryptographic systems, necessitating a comprehensive evaluation of their vulnerabilities and the transition toward quantum-resistant security models. This review explores the security implications of quantum computing on classical cryptographic algorithms, such as RSA and ECC, through penetration testing methodologies designed to assess their resilience against quantum attacks. Additionally, it examines the effectiveness of post-quantum cryptographic (PQC) solutions, including lattice-based, hash-based, and multivariate cryptographic schemes, in mitigating these emerging risks. Furthermore, the study highlights the role of Zero Trust Security (ZTS) as a robust cybersecurity framework for strengthening defenses in the quantum era. By integrating continuous authentication, least privilege access, and micro-segmentation, Zero Trust Security enhances resilience against both classical and quantum threats. Through an analysis of real-world case studies, industry standards, and regulatory developments, this review provides insights into best practices for organizations to proactively fortify their cryptographic infrastructures. The findings emphasize the urgency of adopting hybrid security approaches that combine PQC with Zero Trust principles to ensure long-term data protection and cyber resilience in the face of quantum-enabled adversaries.

Keywords: *Quantum Cryptography, Photon Detection, Polarization, Key Exchange, Post-Quantum Security, Encryption.*

How to Cite: Nonso Okika; Gift Aruchi Nwatuzie; Hamed Salam Olarinoye; Augustine A. Nwaka; Emmanuel Igba; Roland Dunee (2025). Assessing the Vulnerability of Traditional and Post-Quantum Cryptographic Systems through Penetration Testing and Strengthening Cyber Defenses with Zero Trust Security in the Era of Quantum Computing. *International Journal of Innovative Science and Research Technology*, 10(2), 1240-1258. https://doi.org/10.5281/zenodo.14959440

I. INTRODUCTION

- *Background and Significance of the Study*

The rapid advancement of quantum computing technology is poised to revolutionize various sectors, including cryptography. Quantum computers leverage principles of superposition and entanglement, enabling them to perform complex computations at unprecedented speeds. This capability, while promising for fields like optimization and material science, poses significant challenges to traditional cryptographic systems. Notably, Shor's algorithm demonstrates that quantum computers can factor large integers efficiently, undermining the security of widely used public-key cryptographic schemes such as RSA and elliptic-curve cryptography (Shor's algorithm, 2023). The potential for quantum computers to break existing encryption protocols has led to increased attention on post-quantum cryptography (PQC). PQC aims to develop cryptographic algorithms resistant to quantum attacks, ensuring data security in the quantum era. Organizations like the National Institute of Standards and Technology (NIST) have been proactive in standardizing such algorithms to facilitate a seamless transition to quantum-resistant security measures (Mavroeidis et al., 2018). In parallel, the Zero Trust security model has emerged as a robust framework to enhance cybersecurity defenses. Zero Trust operates on the principle of "never trust, always verify," requiring continuous authentication and authorization of all entities within a network. This approach minimizes potential attack surfaces and is particularly pertinent in the context of quantum computing threats, as it emphasizes stringent access controls and real-time monitoring (Saxena.et al., 2023). The convergence of these developments necessitates a comprehensive assessment of both traditional and post-quantum cryptographic systems. Penetration testing serves as a critical methodology in this context, enabling the identification and mitigation of vulnerabilities within cryptographic implementations. By simulating potential attack vectors, penetration testing provides actionable insights into the resilience of cryptographic systems against both classical and quantum threats (Ezeh, et al., 2024). Moreover, integrating Zero Trust principles with post-quantum cryptographic solutions offers a multifaceted defense strategy. This integration ensures that, even if certain cryptographic elements are compromised, the overarching security architecture remains robust through continuous verification and adaptive access controls. Such a layered defense mechanism is essential in preempting and countering sophisticated cyber threats in the quantum computing era (Ajayi et al., 2024).

In summary, the advent of quantum computing presents both opportunities and challenges. To safeguard sensitive information, it is imperative to evaluate the vulnerabilities of existing cryptographic systems and fortify cyber defenses through the adoption of post-quantum algorithms and Zero Trust security models. This study aims to provide a detailed analysis of these aspects, offering strategic insights for organizations navigating the complexities of cybersecurity in the quantum age.

➢ *The Rise of Quantum Computing and its Impact on Cybersecurity*

Quantum computing represents a paradigm shift in computational capabilities, leveraging the principles of quantum mechanics to process information in ways that classical computers cannot. Unlike traditional bits, which exist in a state of 0 or 1, quantum bits, or qubits, can exist in multiple states simultaneously, a phenomenon known as superposition. This allows quantum computers to perform complex calculations at unprecedented speeds, posing significant implications for various fields, notably cybersecurity (Ezeh, et al., 2024). One of the most profound impacts of quantum computing on cybersecurity is its potential to break widely used cryptographic algorithms. Public key cryptography, which underpins the security of many digital communications, relies on the computational difficulty of problems like prime factorization and discrete logarithms. Shor's algorithm, introduced in 1997, demonstrated that a sufficiently powerful quantum computer could solve these problems in polynomial time, rendering many current encryption schemes vulnerable (Shor, 1997). The urgency of this threat is amplified by the concept of "harvest now, decrypt later," where adversaries collect encrypted data today with the intention of decrypting it once quantum capabilities mature. This strategy jeopardizes the confidentiality of sensitive information, including financial records, personal data, and state secrets. As Mosca (2018) emphasizes, the advent of quantum computing necessitates a proactive approach to cybersecurity to mitigate potential risks. In response to these challenges, researchers are exploring quantum-resistant cryptographic algorithms and integrating quantum cryptography with blockchain technology. Ajayi et al. (2024) propose a dual approach that combines quantum cryptography with blockchain-based social media platforms to secure financial transactions in Central Bank Digital Currencies (CBDCs) and combat misinformation in elections. This integration aims to enhance data integrity and authenticity in the digital landscape (Igba, et al.,2024). Furthermore, the application of interpretable data analytics in blockchain networks is gaining traction as a means to enhance anomaly detection and cybersecurity. Tiamiyu et al. (2024) discuss the use of variational autoencoders and model-agnostic explanation techniques to improve the interpretability of machine learning models in detecting anomalies within blockchain networks. This approach facilitates the identification of potential security breaches and ensures the robustness of blockchain-based systems (Ezeh, et al., 2024).

In summary, the rise of quantum computing presents both opportunities and challenges for cybersecurity. While it offers unprecedented computational power, it also threatens the foundations of current cryptographic practices. Proactive measures, including the development of quantum-resistant algorithms and the integration of advanced data analytics, are essential to safeguard digital information in the quantum era (Igba, et al.,2024).

➢ *Objective of the Study*

The objective of this study is to examine the transformative impact of quantum cryptography and blockchain technology in securing digital financial transactions and combating misinformation in decentralized ecosystems. As financial systems increasingly migrate towards digital platforms, the need for robust security mechanisms to protect sensitive data and ensure transaction integrity has never been more critical. This study seeks to analyze the vulnerabilities posed by emerging quantum computing technologies and explore the adoption of quantum-resistant cryptographic techniques as a countermeasure.

A key goal of this research is to investigate the integration of quantum cryptography with blockchain technology to enhance security in financial transactions, particularly in Central Bank Digital Currencies (CBDCs). The study aims to evaluate how quantum-resistant cryptographic solutions, such as lattice-based and hash-based encryption models, can fortify blockchain networks against quantum threats. Additionally, it will assess the feasibility of implementing post-quantum cryptographic algorithms to future-proof digital financial infrastructures. Another critical objective is to explore the application of blockchain-based social media platforms in mitigating misinformation and ensuring data authenticity. In the wake of increasing concerns over misinformation in elections, this study seeks to examine how blockchain's immutable ledger and decentralized verification mechanisms can be leveraged to authenticate information and enhance transparency. This investigation will provide insights into how quantum cryptography can be integrated with blockchain systems to create a secure framework for information dissemination. Furthermore, the study aims to assess how machine learning-driven anomaly detection models, such as variational autoencoders, can enhance the interpretability of blockchain data analytics. By applying advanced interpretability techniques, the research will provide a comprehensive evaluation of how blockchain networks can detect fraudulent transactions, prevent data breaches, and improve cybersecurity resilience. Ultimately, this study aims to contribute to the growing body of knowledge on securing financial transactions in decentralized finance and enhancing information integrity in digital ecosystems. It will provide practical insights for policymakers, financial institutions, and technology developers in implementing quantum-resistant security frameworks for the future of digital finance.

➢ *Organization of the Paper*

This paper is organized into several key sections to provide a comprehensive exploration of post-quantum cryptography (PQC) and its implications for cybersecurity. Section 1 introduces the fundamental concepts of cryptography and the growing need for quantum-resistant encryption methods. Section 2 provides an overview of classical encryption techniques, including RSA and ECC, highlighting their vulnerabilities against quantum computing. Section 3 discusses the importance of penetration testing in cybersecurity, emphasizing its role in identifying system weaknesses. Section 4 introduces PQC, explaining its necessity and the ongoing standardization efforts. Section 5 explores various PQC approaches, including lattice-based, hash-based, multivariate, and code-based cryptography, detailing their strengths and challenges. Section 6 addresses regulatory and compliance considerations, analyzing global standards and best practices for adopting PQC solutions. Finally, Section 7 presents future research directions, potential advancements, and recommendations for the successful integration of PQC in modern security frameworks**.**

II. VULNERABILITIES OF TRADITIONAL CRYPTOGRAPHIC SYSTEMS

➢ *Overview of RSA, ECC, and Other Classical Encryption Methods*

Classical encryption methods form the backbone of secure digital communication, with RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography) being two of the most prominent asymmetric algorithms. RSA, introduced in 1977, relies on the computational difficulty of factoring large prime numbers. Its widespread adoption is attributed to its robustness and the extensive understanding of its security properties. However, RSA requires relatively large key sizes to maintain security, which can be computationally intensive (Cloudflare, 2013) as represented in figure 1. In contrast, ECC offers comparable security with significantly smaller key sizes. This efficiency is particularly advantageous for devices with limited computational resources, such as mobile devices and IoT gadgets. ECC's strength lies in the mathematics of elliptic curves over finite fields, making it a preferred choice in modern cryptographic applications (Sectigo, n.d.). Other classical encryption methods include the Digital Signature Algorithm (DSA), which, like RSA, is based on the difficulty of discrete logarithm problems. DSA is recognized for its efficiency in generating digital signatures, a critical component in verifying the authenticity and integrity of digital messages. Symmetric encryption algorithms, such as the Advanced Encryption Standard (AES), also play a vital role in securing data by using the same key for both encryption and decryption processes (Igba, et al.,2024).

The security of these classical encryption methods is fundamentally based on the computational infeasibility of solving specific mathematical problems, such as prime factorization in RSA and the elliptic curve discrete logarithm problem in ECC. As computational power increases and new mathematical techniques are developed, the robustness of these algorithms must be continually assessed to ensure the confidentiality and integrity of sensitive information (Ezeh, et al.,2024).

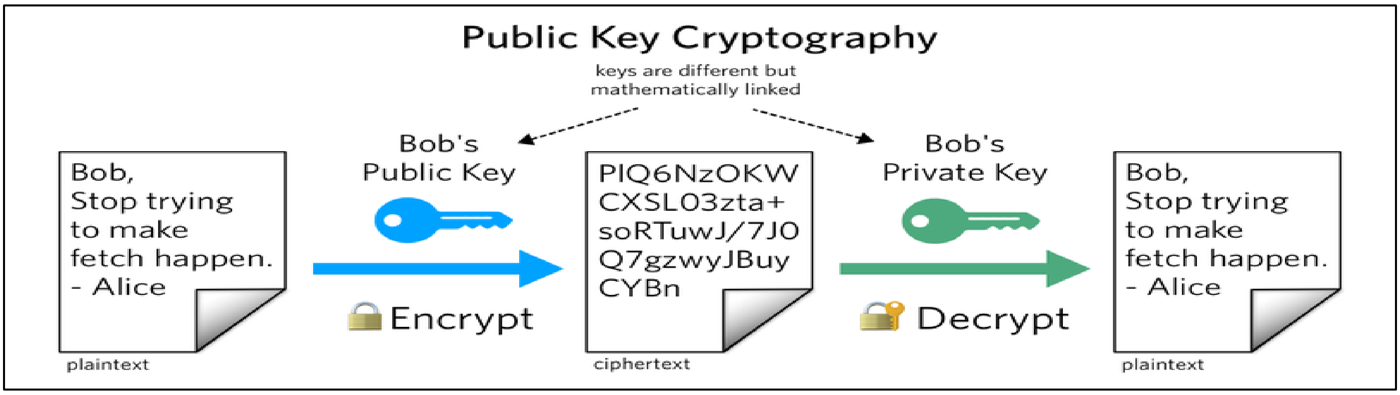
Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSL03zta+ soRTuwJ/7JO Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

Fig 1 Picture of "Public Key Cryptography: Secure Encryption and Decryption Using Asymmetric Keys" (M. Jarjar 2024)

Figure 1 illustrates the fundamental concept of Public Key Cryptography, which underpins encryption methods such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). It depicts the encryption and decryption process using asymmetric keys, where Bob's public key is used to encrypt a plaintext message from Alice, converting it into an unreadable ciphertext. Only Bob's private key, mathematically linked to the public key, can decrypt the message back into plaintext. This method ensures secure communication, even over untrusted channels, as only the intended recipient can decrypt the message. RSA, one of the earliest public-key encryptions schemes, relies on the difficulty of factoring large prime numbers, while ECC provides similar security with smaller key sizes, making it more efficient for modern applications. These encryption techniques are critical for securing digital transactions, email communications, and blockchain technologies.

➢ *Susceptibility to Quantum Attacks (Shor's Algorithm)*

The advent of quantum computing presents a formidable challenge to classical encryption methods, particularly those underpinning public-key cryptography. Shor's algorithm, introduced by mathematician Peter Shor in 1994, has demonstrated the potential to factor large integers and compute discrete logarithms in polynomial time, tasks that are computationally infeasible for classical computers. This capability directly threatens the security of widely used cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC) (Igba, et al.,2024). RSA encryption relies on the difficulty of factoring large composite numbers. In classical computing, the time required to factorize such numbers increases exponentially with their size, rendering RSA secure against traditional attacks. However, Shor's algorithm can factor these large numbers efficiently on a quantum computer, effectively breaking RSA encryption. This means that any data encrypted with RSA could be decrypted if an adversary possesses a sufficiently powerful quantum computer (Shor, 1994). Similarly, ECC is based on the hardness of the elliptic curve discrete logarithm problem. While ECC offers comparable security to RSA with smaller key sizes, making it attractive for systems with limited resources, it is not immune to quantum attacks. Shor's algorithm can also solve the discrete logarithm problem on elliptic curves, compromising the security of ECC-based systems. The efficiency of Shor's algorithm in this context implies that ECC, like RSA, would be vulnerable once large-scale quantum computers become operational (Shor, 1994). The practical implementation of Shor's algorithm requires a quantum computer with a substantial number of qubits and low error rates. Current quantum computers have not yet reached the necessary scale to break RSA or ECC encryption. However, research and development in quantum computing are progressing rapidly. Estimates suggest that within the next decade, quantum computers may achieve the capability to execute Shor's algorithm on cryptographically relevant key sizes, posing a significant threat to current encryption standards (Bernstein et al., 1997). In anticipation of this threat, the cryptographic community is actively exploring post-quantum cryptography—algorithms designed to be secure against quantum attacks. Transitioning to these quantum-resistant algorithms is imperative to protect sensitive information from future quantum-enabled adversaries. Organizations are urged to assess their cryptographic infrastructures and develop migration strategies to post-quantum schemes to ensure long-term data security (Bernstein, et al., 1997).

➢ *Limitations of Current Cryptographic Defenses*

The advent of quantum computing poses significant challenges to existing cryptographic systems, revealing inherent limitations in their ability to withstand quantum attacks. Traditional public-key cryptographic algorithms, such as RSA and Elliptic Curve Cryptography (ECC), are particularly vulnerable due to their reliance on mathematical problems that quantum computers can solve efficiently (Akindotei, et al., 2024) as presented in table 1. One primary limitation is the susceptibility of these algorithms to Shor's algorithm, which enables quantum computers to factor large integers and compute discrete logarithms in polynomial time, effectively breaking RSA and ECC (Alvarado et al., 2023). This vulnerability undermines the foundational security assumptions of these cryptographic schemes, rendering them inadequate in a post-quantum era (Ezeh, et al.,2024). Symmetric key cryptography, while more resilient, is not immune to quantum threats. Grover's algorithm allows quantum computers to perform brute-force searches quadratically faster than classical computers, effectively reducing the security of symmetric algorithms by half. For instance, AES-256 would offer a security level equivalent to AES-128 against quantum attacks, necessitating the adoption of larger key sizes to maintain security (Cintas Canto et al., 2023).

Moreover, the transition to post-quantum cryptographic algorithms introduces new challenges. Many proposed quantum-resistant algorithms require significantly larger key sizes and computational resources, leading to increased latency and bandwidth consumption. These performance drawbacks can hinder their practical deployment, especially in resource-constrained environments (Alvarado, et al., 2023). Additionally, the security of post-quantum algorithms against side-channel attacks remains an area of concern. Implementation vulnerabilities can be exploited to extract secret keys, even if the underlying algorithm is theoretically secure. Ensuring robust implementations that resist such attacks is crucial for the effective adoption of post-quantum cryptographic defenses (Cintas Canto et al., 2023).

In summary, the limitations of current cryptographic defenses in the face of quantum computing advancements necessitate a comprehensive reevaluation of security protocols. Developing and implementing quantum-resistant algorithms that balance security and performance is imperative to protect sensitive information in the emerging quantum era (Ezeh, et al.,2024).

Table 1 Limitations of Current Cryptographic Defenses

Limitation	Description	Impact	Potential Mitigation
Vulnerability to Quantum Attacks	Traditional cryptographic algorithms like RSA and ECC rely on factorization and discrete logarithm problems, which quantum computers can solve efficiently using Shor's algorithm.	This threatens the security of encrypted data, potentially rendering current encryption obsolete.	Adoption of Post-Quantum Cryptography (PQC) and hybrid encryption methods.
Scalability and Performance Issues	Some cryptographic defenses impose high computational overhead, making them inefficient for large-scale or real-time applications.	Reduced efficiency in processing transactions and securing communications, especially in decentralized networks.	Optimization of cryptographic algorithms for better performance and hardware acceleration.
Key Management Complexities	Managing, storing, and distributing cryptographic keys securely is challenging, particularly in large enterprises and distributed systems.	Increased risk of key leaks, improper key rotation, and human errors leading to security breaches.	Development of automated key management systems and the use of blockchain-based key distribution.
Regulatory and Compliance Challenges	Compliance with evolving security standards (e.g., GDPR, NIST) requires frequent cryptographic updates and adaptations.	Organizations face operational and legal risks if their cryptographic measures do not align with regulatory requirements.	Continuous monitoring of regulatory changes and proactive updates to cryptographic frameworks.

III. PENETRATION TESTING FOR CRYPTOGRAPHIC RESILIENCE

➢ *Importance of Penetration Testing in Cybersecurity*

Penetration testing, often referred to as ethical hacking, is a critical component in the cybersecurity landscape. It involves simulating real-world attacks on computer systems, networks, or applications to identify and address security vulnerabilities before malicious actors can exploit them. This proactive approach is essential for maintaining robust security postures in organizations (Akindotei, et al.,2024) as represented in figure 2. One of the primary benefits of penetration testing is its ability to uncover hidden weaknesses within an organization's infrastructure. By emulating the tactics, techniques, and procedures of potential attackers, penetration testers can identify vulnerabilities that automated tools might overlook. This comprehensive assessment ensures that security measures are not only theoretically sound but also practically effective against sophisticated threats. As highlighted by Cintas Canto et al. (2023), penetration testing plays a crucial role in identifying and mitigating security weaknesses, thereby enhancing the overall security posture of organizations (Akindotei, et al.,2024). Moreover, penetration testing provides valuable insights into the effectiveness of an organization's existing security policies and controls. The findings from these tests enable security teams to prioritize remediation efforts, allocate resources efficiently, and implement targeted security measures. This iterative process fosters a culture of continuous improvement in cybersecurity practices. (Alvarado et al. 2023) emphasize that penetration testing is a key practice toward engineering secure software, as it helps organizations understand potential vulnerabilities and address them proactively (Enyejo, et al.,2024).

In addition to vulnerability identification, penetration testing serves as a training ground for cybersecurity professionals. Engaging in simulated attack scenarios hones the skills of security teams, equipping them with the knowledge and experience necessary to respond effectively to actual security incidents. This hands-on experience is invaluable in preparing organizations to defend against an ever-evolving threat landscape. The importance of penetration testing knowledge and experience in cybersecurity education is widely recognized, as it prepares professionals to tackle real-world security challenges (Cintas Canto et al., 2023).

Furthermore, regular penetration testing is often a regulatory requirement in various industries. Compliance with standards such as the Payment Card Industry Data Security Standard (PCI DSS) necessitates periodic testing to ensure that organizations maintain a secure environment for sensitive data. Adhering to these regulations not only fulfills legal obligations but also reinforces customer trust and confidence in the organization's commitment to data protection (Akindotei, et al.,2024). In summary, penetration testing is an indispensable tool in the cybersecurity arsenal. It enables organizations to proactively identify and remediate vulnerabilities, assess the efficacy of security controls, train personnel, and comply with regulatory mandates. By integrating regular penetration testing into their security strategies, organizations can significantly enhance their resilience against cyber threats (Enyejo, et al.,2024).

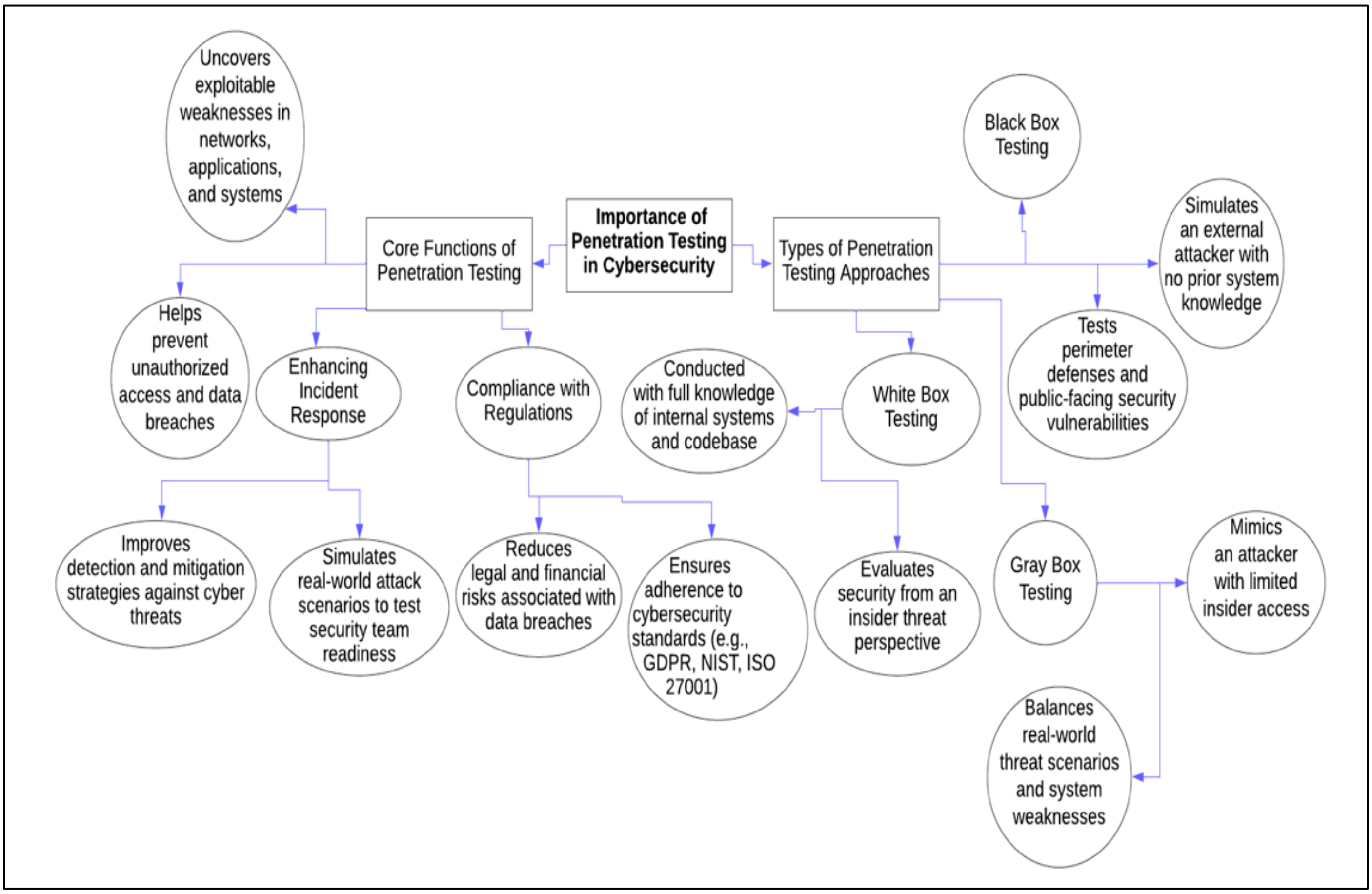
Importance of Penetration Testing in Cybersecurity
Core Functions of Penetration Testing
Types of Penetration Testing Approaches
Uncovers exploitable weaknesses in networks, applications, and systems
Helps prevent unauthorized access and data breaches
Enhancing Incident Response
Compliance with Regulations
Improves detection and mitigation strategies against cyber threats
Simulates real-world attack scenarios to test security team readiness
Reduces legal and financial risks associated with data breaches
Ensures adherence to cybersecurity standards (e.g., GDPR, NIST, ISO 27001)
Black Box Testing
Simulates an external attacker with no prior system knowledge
Tests perimeter defenses and public-facing security vulnerabilities
White Box Testing
Conducted with full knowledge of internal systems and codebase
Evaluates security from an insider threat perspective
Gray Box Testing
Mimics an attacker with limited insider access
Balances real-world threat scenarios and system weaknesses

Fig 2 Diagram of Importance of Penetration Testing in Cybersecurity

Figure 1 visually represents the importance of penetration testing in cybersecurity, structured into two primary branches: Core Functions of Penetration Testing and Types of Penetration Testing Approaches. The first branch highlights key functions, including identifying security vulnerabilities by uncovering exploitable weaknesses, enhancing incident response through real-world attack simulations, and ensuring compliance with cybersecurity regulations such as GDPR and ISO 27001. The second branch categorizes penetration testing approaches into three types: Black Box Testing, which simulates an external attacker with no prior knowledge of the system; White Box Testing, which evaluates security from an insider perspective with full system access; and Gray Box Testing, which mimics an attacker with partial insider knowledge for balanced risk assessment. By combining these elements, the diagram illustrates how penetration testing strengthens cybersecurity defenses, improves regulatory adherence, and proactively mitigates cyber threats.

- *Techniques for Assessing Cryptographic Vulnerabilities*

Assessing cryptographic vulnerabilities is a critical aspect of ensuring the security and integrity of information systems. Effective evaluation of cryptographic implementations involves a combination of automated tools and manual analysis to identify potential weaknesses that could be exploited by adversaries (Akindotei, et al.,2024) as presented in table 2. One prevalent technique is static code analysis, which involves examining the source code of applications to detect improper use of cryptographic APIs. Tools designed for this purpose analyze codebases to identify patterns indicative of vulnerabilities, such as hard-coded cryptographic keys, use of deprecated algorithms, or insecure configurations. For instance, the study by (Afrose et al. 2021) highlights the development of comprehensive benchmarks to evaluate static vulnerability detection tools, emphasizing the importance of precise detection mechanisms in identifying cryptographic API misuses (Tiamiyu, et al., 2024). Another essential method is dynamic analysis, which entails monitoring the behavior of applications during runtime to uncover vulnerabilities that static analysis might miss. This approach can identify issues such as insecure key generation processes, improper handling of cryptographic exceptions, or vulnerabilities arising from the interaction between different system components. Dynamic analysis provides insights into how cryptographic functions operate under various conditions, enabling the detection of flaws that could be exploited in real-world scenarios (Enyejo, et al.,2024).

Penetration testing serves as a practical approach to assessing cryptographic vulnerabilities by simulating attacks on systems to evaluate their defenses. This method involves attempting to exploit identified weaknesses in cryptographic implementations to determine their potential impact. Penetration testers employ various techniques, including cipher text manipulation and cryptographic protocol analysis, to assess the robustness of encryption schemes. This hands-on approach helps organizations understand the practical implications of vulnerabilities and prioritize remediation efforts accordingly (Tiamiyu, et al., 2024).

In addition to these techniques, the use of specialized cryptographic vulnerability detection **tools** has become increasingly important. For example, CryptoGuard is a tool designed to detect cryptographic vulnerabilities in large-scale Java projects. It employs refined program slicing algorithms to reduce false positives and has been effective in identifying issues such as exposed secrets and predictable random numbers. The tool's application to high-impact projects has led to significant security improvements, as noted by (Rahaman et al. 2018).

Regular **security** audits and code reviews are also vital in the assessment process. These practices involve systematic examination of cryptographic implementations by security professionals to ensure adherence to best practices and compliance with relevant standards. Audits and reviews can uncover subtle vulnerabilities that automated tools might overlook, such as logic flaws or improper error handling in cryptographic processes (Enyejo, et al.,2024)

In summary, a comprehensive assessment of cryptographic vulnerabilities necessitates a multifaceted approach that combines static and dynamic analysis, penetration testing, specialized tools, and thorough security audits. By employing these techniques, organizations can effectively identify and mitigate weaknesses in their cryptographic implementations, thereby enhancing the overall security posture of their information systems (Tiamiyu, et al., 2024).

- *Case Studies on Penetration Testing of Encryption Systems*

Penetration testing serves as a critical tool in evaluating the robustness of encryption systems by simulating real-world attacks to identify and rectify vulnerabilities. Several notable case studies illustrate the efficacy of this approach in enhancing cryptographic security (Tiamiyu, et al., 2024). In 2019, researchers Gaudry and Golovnev conducted a penetration test on the encryption scheme of Moscow's Internet voting system. The system employed a variant of the ElGamal encryption over finite fields. The initial assessment revealed that the cryptographic keys utilized were inadequately sized, allowing the researchers to retrieve private keys from public keys within minutes using standard computational resources. Upon addressing this issue, a subsequent evaluation uncovered that the new implementation lacked semantic security, enabling the potential to count votes cast for a candidate. This case underscores the necessity for rigorous testing and validation of encryption protocols prior to deployment, especially in critical applications like electronic voting (Gaudry & Golovnev, 2019). Another significant case involves the DESCHALL Project of 1997, which aimed to demonstrate the vulnerability of the Data Encryption Standard (DES) to brute-force attacks. Coordinated by a group of computer scientists, the project harnessed the collective processing power of approximately 78,000 computers distributed across the internet. The collaborative effort successfully tested about a quarter of the DES key space, ultimately discovering the correct key and decrypting the message. This endeavor highlighted the practical feasibility of brute-force attacks against DES, leading to increased advocacy for stronger encryption standards and influencing the transition to more secure algorithms (Kumar, et al., 2006). These case studies exemplify the critical role of penetration testing in identifying and mitigating vulnerabilities within encryption systems. By proactively uncovering weaknesses through simulated attacks, organizations can enhance their cryptographic defenses, ensuring the confidentiality and integrity of sensitive information (Igb a, et al.,2024)

Table 2 Case Studies on Penetration Testing of Encryption Systems

Case Study	Objective	Findings	Implications & Recommendations
Penetration Testing of AES-256 in Cloud Storage	Assess the resilience of AES-256 encryption in protecting cloud-stored data from unauthorized access.	Attackers exploited weak key management practices and side-channel vulnerabilities, gaining partial access to encrypted files.	Strengthen key management protocols, implement hardware security modules (HSMs), and monitor access controls rigorously.
RSA Cryptosystem Vulnerability in Enterprise VPNs	Evaluate the effectiveness of RSA encryption in securing VPN traffic against man-in-the-middle (MITM) attacks.	Found susceptibility to RSA key factoring using inadequate key lengths, allowing interception of sensitive data.	Transition to post-quantum cryptography (PQC) and enforce a minimum key length of 4096 bits for RSA-based VPNs.
Blockchain-Based Encryption in Financial Transactions	Test blockchain encryption schemes for vulnerabilities in transaction integrity and confidentiality.	Identified flaws in elliptic curve cryptography (ECC) implementations, leading to potential transaction forgery risks.	Adopt standardized and quantum-resistant ECC curves while reinforcing multi-signature authentication mechanisms.
Zero Trust Model Testing in Government Data Systems	Evaluate the effectiveness of Zero Trust security in protecting classified government records.	Successful breaches occurred due to improper identity verification and misconfigured encryption policies.	Enhance multi-factor authentication (MFA), regularly audit encryption settings, and integrate AI-driven anomaly detection.

IV. POST-QUANTUM CRYPTOGRAPHIC SOLUTIONS

- *Introduction to Post-Quantum Cryptography (PQC)*

The advent of quantum computing heralds a paradigm shift in computational capabilities, posing significant challenges to classical cryptographic systems. Traditional encryption methods, such as RSA and ECC, rely on the computational difficulty of problems like integer factorization and discrete logarithms. Quantum algorithms, notably Shor's algorithm, can solve these problems efficiently, rendering many existing cryptographic protocols vulnerable (Shor, 1994) as represented in figure 3.

This impending threat has catalyzed the development of Post-Quantum Cryptography (PQC), which aims to create cryptographic algorithms resistant to attacks from both classical and quantum computers (Ayoola, et al., 2024). PQC encompasses a diverse array of cryptographic approaches designed to withstand quantum attacks. Prominent among these are lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash-based signatures.

Lattice-based schemes, for instance, derive their security from the hardness of lattice problems, which remain intractable even for quantum adversaries (Regev, 2009). Similarly, code-based cryptographic systems, such as the McEliece cryptosystem, rely on the difficulty of decoding random linear codes, a problem also believed to be resistant to quantum attacks (Bernstein et al., 2008). The National Institute of Standards and Technology (NIST) has been at the forefront of standardizing PQC algorithms. In 2016, NIST initiated a multi-round process to evaluate and standardize quantum-resistant public-key cryptographic algorithms.

This rigorous evaluation aims to ensure that the selected algorithms meet stringent security and performance criteria, facilitating their integration into existing communication protocols and systems (NIST, 2016). Transitioning to PQC is a complex and imperative task. Organizations must assess their current cryptographic infrastructures, identify components susceptible to quantum attacks, and develop strategies for implementing quantum-resistant solutions.

This proactive approach is essential to safeguard sensitive information against future quantum-enabled threats, ensuring the continued confidentiality and integrity of data in the quantum era.

- *Lattice-Based, Hash-Based, Multivariate, and Code-Based Cryptography*

Post-Quantum Cryptography (PQC) encompasses several approaches designed to withstand attacks from quantum computers. Among these, lattice-based, hash-based, multivariate, and code-based cryptographic schemes are prominent (Igb a, et al.,2024). Lattice-based cryptography relies on the complexity of mathematical lattices—grid-like structures extending into multiple dimensions. The security of these schemes is rooted in the difficulty of problems such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem, which remain hard even for quantum computers (Bernstein et al., 2008). Notably, lattice-based algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium have been selected by the National Institute of Standards and Technology (NIST) for standardization, underscoring their robustness and efficiency (Igba, et al., 2024). Hash-based cryptography utilizes the properties of cryptographic hash functions to construct secure digital signatures. Schemes like the Merkle Signature Scheme (MSS) and its variant, eXtended Merkle Signature Scheme (XMSS), offer strong security guarantees based on the preimage resistance and collision resistance of the underlying hash functions. These schemes are particularly valued for their simplicity and reliance on well-understood cryptographic primitives (Igba, et al.,2024). Multivariate cryptography is founded on the difficulty of solving systems of multivariate polynomial equations over finite fields. Public-key schemes in this category, such as the Unbalanced Oil and Vinegar (UOV) signature scheme, present challenges for both classical and quantum adversaries due to the NP-hard nature of the underlying problem. Despite their potential, some multivariate schemes have faced security challenges, necessitating ongoing research to ensure their resilience (Ding, et al.,2017). Code-based cryptography derives its security from the hardness of decoding linear error-correcting codes. The McEliece cryptosystem, for example, uses the difficulty of decoding general linear codes as its security foundation. While offering strong security, code-based schemes often require large key sizes, which can pose practical implementation challenges (Ayoola, et al., 2024). Each of these cryptographic approaches offers unique advantages and potential drawbacks. The selection of an appropriate scheme depends on specific application requirements, including security needs, performance constraints, and implementation considerations. As quantum computing continues to advance, the development and standardization of these PQC schemes remain critical to ensuring the security of information in the quantum era.

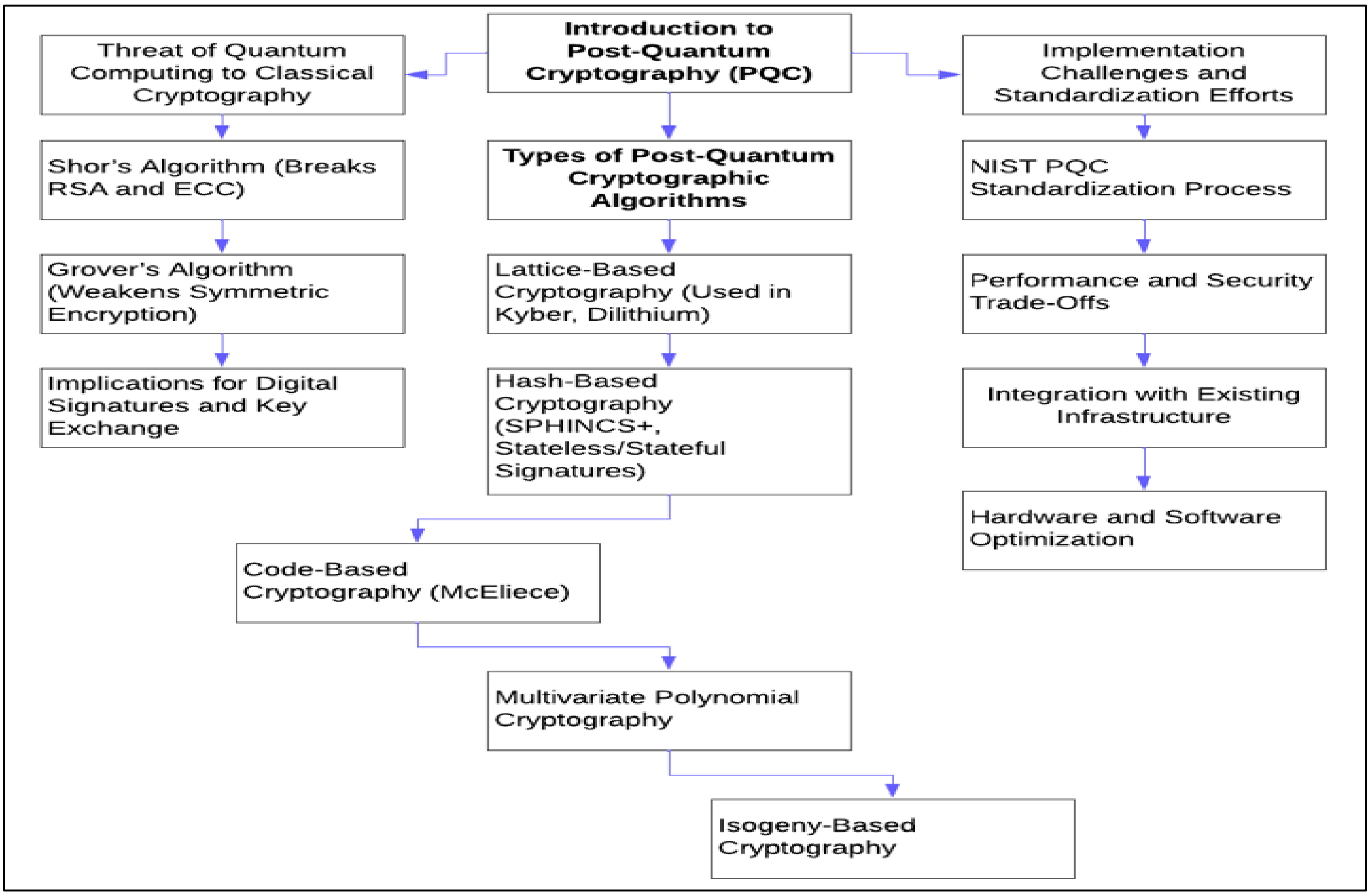
Introduction to Post-Quantum Cryptography (PQC)
Threat of Quantum Computing to Classical Cryptography
Shor's Algorithm (Breaks RSA and ECC)
Grover's Algorithm (Weakens Symmetric Encryption)
Implications for Digital Signatures and Key Exchange
Types of Post-Quantum Cryptographic Algorithms
Lattice-Based Cryptography (Used in Kyber, Dilithium)
Hash-Based Cryptography (SPHINCS+, Stateless/Stateful Signatures)
Code-Based Cryptography (McEliece)
Multivariate Polynomial Cryptography
Isogeny-Based Cryptography
Implementation Challenges and Standardization Efforts
NIST PQC Standardization Process
Performance and Security Trade-Offs
Integration with Existing Infrastructure
Hardware and Software Optimization

Fig 3 Diagram of Introduction to Post-Quantum Cryptography (PQC)

Figure 3 presents an overview of Post-Quantum Cryptography (PQC) and its significance in countering threats posed by quantum computers. The first branch highlights the vulnerability of classical cryptographic methods, emphasizing how quantum algorithms like Shor's and Grover's can compromise current encryption standards. The second branch categorizes the leading PQC algorithms under development, such as lattice-based, hash-based, code-based, and multivariate polynomial cryptography, each offering resistance to quantum attacks. The third branch addresses the practical challenges of PQC implementation, including ongoing NIST standardization efforts, balancing security vs. performance, and ensuring compatibility with existing cryptographic infrastructure. This structured view provides a comprehensive understanding of PQC's role in the evolving cybersecurity landscape.

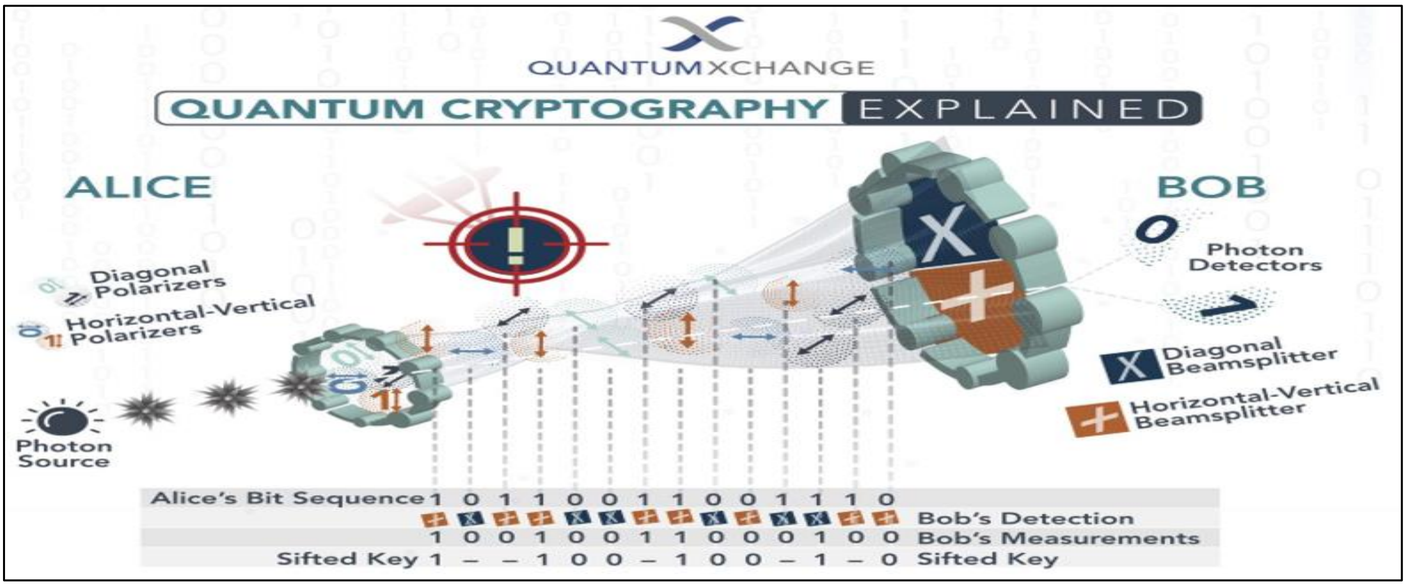
QUANTUMXCHANGE
QUANTUM CRYPTOGRAPHY EXPLAINED
ALICE
BOB
Diagonal Polarizers
Horizontal-Vertical Polarizers
Photon Source
Photon Detectors
Diagonal Beamsplitter
Horizontal-Vertical Beamsplitter
Alice's Bit Sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's Detection
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's Measurements
Sifted Key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted Key

Fig 4 Quantum Cryptography and Post-Quantum Security: Ensuring Secure Communication in the Quantum Era" (Dilmegani 2025)

Figure 4 visually explains quantum cryptography using the BB84 protocol, where Alice transmits a sequence of polarized photons to Bob, who measures them using randomly chosen bases (diagonal or horizontal-vertical). This concept relates to post-quantum cryptography, particularly lattice-based, hash-based, multivariate, and code-based cryptographic methods, which are designed to withstand quantum attacks. Lattice-based cryptography relies on the hardness of problems like the Learning With Errors (LWE) problem, making it resistant to quantum decryption. Hash-based cryptography ensures security through one-way hash functions, often used in digital signatures. Multivariate cryptography leverages the difficulty of solving systems of nonlinear equations, while code-based cryptography relies on the complexity of decoding random error-correcting codes, as seen in the McEliece cryptosystem. The quantum key distribution (QKD) illustrated here shares a fundamental goal with these cryptographic techniques: ensuring secure communication in a future where quantum computers threaten classical encryption.

➢ *Implementation Challenges and Standardization Efforts*

The transition to post-quantum cryptography (PQC) presents a multitude of implementation challenges, necessitating coordinated standardization efforts to ensure robust and interoperable security solutions. One primary challenge lies in the integration of PQC algorithms into existing systems. Many current infrastructures are deeply rooted in classical cryptographic schemes, and replacing these with quantum-resistant alternatives requires significant modifications. This process involves not only updating algorithms but also ensuring compatibility with existing protocols and hardware, which can be both complex and resource-intensive (Dziechciarz, et al.,2024) as presented in table 3. Another critical concern is the performance of PQC algorithms. Some quantum-resistant schemes demand greater computational resources, potentially leading to increased latency and reduced efficiency. For instance, certain lattice-based algorithms, while secure, may require larger key sizes, impacting storage and transmission efficiency. Balancing security with performance is essential, especially for applications with stringent speed and resource constraints ((Igb a, et al.,2025). Standardization plays a pivotal role in addressing these challenges. The National Institute of Standards and Technology (NIST) has been at the forefront of this effort, initiating a comprehensive process to evaluate and standardize PQC algorithms. In August 2024, NIST finalized three algorithms designed to resist attacks from both classical and quantum computers, marking a significant milestone in the journey toward quantum-resistant cryptographic standards (NIST, 2024). These algorithms are based on mathematical problems distinct from those used in classical cryptography, ensuring resilience against quantum attacks (Bavdekar, et al.,2022) Despite these advancements, the path to widespread adoption of PQC is fraught with obstacles. Organizations must undertake extensive testing to validate the security and performance of new algorithms within their specific operational contexts. Additionally, the global nature of digital communications necessitates international collaboration to develop universally accepted standards, ensuring seamless interoperability across borders. The urgency of these efforts is underscored by the rapid progression of quantum computing technologies, which threaten to outpace the deployment of quantum-resistant solutions (Ayoola, et al., 2024).

In conclusion, while significant strides have been made in the standardization of post-quantum cryptography, the implementation of these standards presents complex challenges. A concerted effort involving rigorous testing, international cooperation, and a balance between security and performance is essential to safeguard information in the impending quantum era (Igb a, et al.,2025).

Table 3 Implementation Challenges and Standardization Efforts

Challenge/ Standardization Effort	**Description**	**Impact on Security**	**Proposed Solutions & Best Practices**
Scalability of Post-Quantum Cryptography (PQC) Algorithms	Transitioning from classical cryptographic systems to PQC faces computational overhead and hardware limitations.	Increased processing power requirements may slow down encryption and authentication processes.	Optimize algorithm efficiency, implement hybrid cryptographic approaches, and upgrade hardware for quantum-resistant encryption.
Interoperability Between Security Protocols	Inconsistent cryptographic standards across industries create compatibility issues in multi-platform security frameworks.	Weak integrations can result in security gaps, making systems vulnerable to cyberattacks.	Develop unified encryption frameworks, promote cross-industry collaboration, and adopt NIST-approved PQC standards.
Regulatory and Compliance Adaptation	Existing legal frameworks, such as GDPR and HIPAA, lack specific guidelines for post-quantum security transitions.	Ambiguity in compliance regulations may lead to non-standardized security implementations.	Establish updated compliance policies, encourage global regulatory cooperation, and integrate quantum-safe encryption mandates.
Resource Constraints in Small and Medium Enterprises (SMEs)	SMEs struggle to adopt advanced encryption methods due to high costs and lack of expertise.	Limited security budgets increase exposure to cyber threats, including post-quantum attacks.	Provide government incentives for PQC adoption, develop cost-effective cryptographic solutions, and offer cybersecurity training programs.

V. ZERO TRUST SECURITY AS A CYBER DEFENSE STRATEGY

➢ *Core Principles of Zero Trust Security*

Zero Trust Security is a cybersecurity paradigm that fundamentally challenges the traditional notion of trust within network architectures. Operating on the principle of "never trust, always verify," it posits that no entity—whether inside or outside the network perimeter—should be granted access without stringent authentication and continuous validation (CrowdStrike, 2024) (Ayoola, et al., 2024). A cornerstone of Zero Trust is the assumption that threats can originate from anywhere, necessitating a shift from perimeter-based defenses to a more granular, identity-centric approach. This involves implementing robust identity and access management (IAM) protocols, ensuring that users and devices are authenticated and authorized based on dynamic policies before accessing resources (CrowdStrike, 2024). Another critical principle is the enforcement of least privilege access. By granting users and devices only the permissions necessary for their specific functions, organizations can minimize potential attack surfaces and limit the impact of security breaches. This approach requires continuous monitoring and adjustment of access rights to align with evolving roles and responsibilities (CrowdStrike, 2024). Micro-segmentation further enhances security by dividing networks into isolated segments, each protected by its own set of access controls. This containment strategy ensures that even if a breach occurs, its impact is confined to a limited segment, preventing lateral movement across the network (CrowdStrike, 2024). Continuous monitoring and validation are imperative in a Zero Trust framework. By persistently analyzing user activities, device health, and network traffic, organizations can detect anomalies in real-time, enabling prompt responses to potential threats. This proactive stance is essential for maintaining a robust security posture in the face of sophisticated cyberattacks (CrowdStrike, 2024). The dynamic nature of modern cloud networks presents unique challenges to traditional Zero Trust models, which often rely on static policies and rigid access controls. To address this, a conceptual shift towards more granular and dynamic security measures is necessary. This involves adapting Zero Trust principles to accommodate the fluidity of cloud environments, ensuring that security measures are as agile and scalable as the networks they protect (Enyejo et al., 2021).

In summary, the core principles of Zero Trust Security—comprising strict identity verification, least privilege access, micro-segmentation, and continuous monitoring—collectively fortify an organization's defenses against both external and internal threats. By adopting a "never trust, always verify" stance, organizations can enhance their resilience in an increasingly complex and hostile cyber landscape (Ayoola, et al.,2024).

➢ *Integration of Zero Trust with Post-Quantum Cryptographic Models*

The convergence of Zero Trust Architecture (ZTA) and Post-Quantum Cryptography (PQC) represents a strategic advancement in fortifying cybersecurity frameworks against emerging threats. Zero Trust operates on the principle of "never trust, always verify," enforcing strict identity verification and continuous monitoring to mitigate risks associated with both internal and external actors. PQC, on the other hand, involves the development and implementation of cryptographic algorithms resistant to the computational capabilities of quantum computers, thereby safeguarding data against future decryption attempts by quantum adversaries (Raheman, F. et al., 2024) Integrating PQC into a Zero Trust framework enhances the security posture by ensuring that all data transmissions and storage are protected with quantum-resistant encryption, effectively addressing the "harvest now, decrypt later" threat scenario. In this context, even if an attacker intercepts encrypted data today, the use of PQC ensures that the data remains secure against future quantum decryption capabilities. This integration necessitates a comprehensive assessment of existing cryptographic protocols and a systematic migration to PQC algorithms, ensuring that all components of the network adhere to quantum-resistant standards (Gharib, et al.,2023) The National Institute of Standards and Technology (NIST) has been at the forefront of standardizing PQC algorithms, selecting multiple standards to enhance security and resilience against technological advancements. This proactive approach aims to provide organizations with a robust set of tools to defend against the impending quantum threat. The implementation of these standards is a long-term project that will significantly influence global cryptographic practices. Organizations are encouraged to begin the transition to post-quantum cryptography to protect sensitive information from future quantum-enabled threats (Ezeh, et al., 2024) Incorporating PQC into a Zero Trust model also involves adopting a crypto-agile posture, enabling organizations to swiftly update cryptographic algorithms and protocols in response to emerging vulnerabilities or advancements in quantum computing. This agility is crucial in maintaining a resilient security infrastructure capable of adapting to the rapidly evolving threat landscape. By unifying the principles of Zero Trust with the protective measures offered by PQC, organizations can establish a fortified defense mechanism that addresses both current and foreseeable cybersecurity challenges (Ezeh, et al., 2024).

➢ *Benefits and Challenges of a Zero Trust Architecture*

Zero Trust Architecture (ZTA) has emerged as a transformative approach in cybersecurity, fundamentally redefining how organizations protect their digital assets. By operating on the principle of "never trust, always verify," ZTA enforces continuous authentication and strict access controls, thereby minimizing the risk of unauthorized access and lateral movement within networks. This paradigm shift enhances an organization's ability to protect sensitive data, maintain operational integrity, and respond swiftly to emerging threats (Ezeh, et al., 2024) as presented in table 4. One of the primary benefits of ZTA is its robust defense against internal and external threats. By eliminating implicit trust and requiring verification for every access request, ZTA significantly reduces the attack surface. This approach is particularly effective in mitigating risks associated with insider threats and compromised credentials, as it ensures that access privileges are continuously evaluated and adjusted based on real-time assessments of user behavior and context. Moreover, ZTA's emphasis on least privilege access ensures that users and devices have only the permissions necessary to perform their functions, thereby limiting potential damage from security breaches (Joshi, 2024). However, implementing a Zero Trust Architecture presents several challenges. One significant hurdle is the complexity involved in overhauling existing legacy systems to align with ZTA principles. Many organizations operate on traditional perimeter-based security models, and transitioning to a Zero Trust framework requires a comprehensive assessment and restructuring of network infrastructures. This process can be resource-intensive, necessitating significant investments in time, technology, and personnel training. Additionally, the continuous monitoring and verification processes integral to ZTA can introduce latency and impact system performance if not properly managed. Organizations must balance the need for stringent security measures with the imperative of maintaining operational efficiency (Dziechciarz, et al., 2024).

Another challenge lies in the integration of ZTA with diverse cloud services and third-party applications. As enterprises increasingly adopt multi-cloud environments, ensuring consistent application of Zero Trust policies across various platforms becomes complex. Each cloud provider may have unique security protocols, and harmonizing these with an organization's ZTA requires meticulous planning and coordination. Furthermore, the dynamic nature of modern workforces, characterized by remote work and the proliferation of personal devices accessing corporate networks, complicates the enforcement of Zero Trust principles. Ensuring secure access in such fluid environments demands advanced identity management solutions and adaptive security policies. In conclusion, while Zero Trust Architecture offers a robust framework for enhancing cybersecurity by addressing both external and internal threats, its implementation is not without challenges. Organizations must navigate the complexities of system integration, performance considerations, and policy enforcement to fully realize the benefits of a Zero Trust model. A strategic, well-planned approach that includes stakeholder engagement, investment in appropriate technologies, and ongoing evaluation is essential for the successful adoption of ZTA.

Table 4 Benefits and Challenges of a Zero Trust Architecture

Aspect	Description	Impact on Security	Proposed Solutions & Best Practices
Enhanced Access Control	Zero Trust enforces strict identity verification and least privilege access to reduce unauthorized access.	Minimizes insider threats and unauthorized lateral movement within networks.	Implement multi-factor authentication (MFA), continuous monitoring, and role-based access controls.
Improved Threat Detection & Response	Continuous authentication and real-time monitoring help detect anomalies early.	Reduces dwell time of attackers and prevents data breaches.	Deploy AI-driven security analytics and automated response mechanisms.
Implementation Complexity	Zero Trust requires a complete overhaul of traditional network security models.	Initial deployment may introduce operational inefficiencies and increased workload for IT teams.	Adopt a phased implementation approach, provide staff training, and leverage cloud-native security tools.
Scalability and Cost Concerns	Adopting Zero Trust can be expensive, requiring significant investment in infrastructure and security policies.	High costs may deter small and medium enterprises (SMEs) from full implementation.	Utilize cost-effective Zero Trust solutions, prioritize critical assets, and seek cybersecurity funding programs.

VI. CASE STUDIES AND REAL-WORLD APPLICATIONS

➢ *Analysis of Organizations Implementing PQC and Zero Trust*

The integration of Post-Quantum Cryptography (PQC) and Zero Trust Architecture (ZTA) represents a strategic response by organizations aiming to fortify their cybersecurity frameworks against emerging threats. This dual implementation addresses vulnerabilities posed by advancements in quantum computing and the evolving landscape of cyber threats (Ayoola, et al., 2024). In the realm of PQC, several organizations have proactively initiated transitions to quantum-resistant cryptographic protocols. The National Institute of Standards and Technology (NIST) has been at the forefront, collaborating with industry leaders such as Microsoft, Amazon Web Services (AWS), VMware, Cisco Systems, and Samsung. These collaborations focus on guiding the nation's migration to cryptographic standards resilient to quantum computing capabilities, ensuring that data remains secure against potential future quantum attacks (Dziechciarz, et al., 2024).

This concerted effort underscores the importance of public-private partnerships in addressing complex cybersecurity challenges (Ayoola, et al., 2024). Concurrently, the adoption of Zero Trust principles has gained significant momentum across various sectors. A report indicates that nearly 90% of organizations worldwide have begun embracing Zero Trust security models.

This widespread adoption reflects a paradigm shift from traditional perimeter-based defenses to a model that assumes potential threats both inside and outside the network, thereby enforcing strict verification for every access request (CSO Online, 2023).

This approach enhances security by minimizing implicit trust and continuously validating user identities and device integrity (Ijiga, et al., 2024). The convergence of PQC and ZTA within organizational strategies offers a comprehensive defense mechanism. By implementing PQC, organizations safeguard their cryptographic infrastructure against the prospective decryption capabilities of quantum computers. Simultaneously, Zero Trust frameworks ensure that access controls are stringent and continuously monitored, reducing the risk of unauthorized data exposure. This integrated approach not only addresses future quantum threats but also fortifies defenses against current cyber vulnerabilities (Ijiga, et al., 2024). However, the dual implementation of PQC and ZTA is not without challenges. Organizations must navigate the complexities of overhauling existing systems, which often involves significant resource allocation and meticulous planning.

The transition to PQC requires updating cryptographic algorithms across various platforms, while adopting Zero Trust necessitates a cultural shift towards continuous verification and monitoring. Despite these challenges, the proactive steps taken by leading organizations demonstrate a commitment to enhancing cybersecurity resilience in an era of rapid technological evolution (Ijiga, et al., 2024).

➢ *Lessons Learned and Best Practices*

The integration of Post-Quantum Cryptography (PQC) and Zero Trust Architecture (ZTA) presents organizations with a multifaceted challenge, necessitating a strategic approach to enhance cybersecurity resilience. Insights from early adopters reveal critical lessons and best practices essential for a successful transition (Ijiga, et al., 2024) as represented in figure 5.

- *Comprehensive Cryptographic Inventory*

A fundamental step in preparing for PQC involves conducting a thorough inventory of existing cryptographic assets. Understanding the current deployment of cryptographic algorithms, keys, and certificates is imperative for assessing vulnerabilities and planning the migration to quantum-resistant alternatives. This process, often referred to as achieving "crypto-agility," enables organizations to adapt swiftly to new cryptographic standards and ensures that all assets are accounted for during the transition (Kunde, et al., 2024).

- *Phased and Prioritized Implementation*

Transitioning to PQC and implementing ZTA should be approached in a phased manner. Prioritizing critical systems and data for early adoption allows organizations to manage resources effectively and address potential issues on a manageable scale. This strategy not only mitigates risks associated with large-scale overhauls but also provides a framework for iterative learning and improvement throughout the implementation process (Ijiga, et al., 2024).

- *Stakeholder Engagement and Training*

Engaging stakeholders across all levels of the organization is vital. Awareness programs and specialized training ensure that employees understand the importance of the transition and are equipped to operate within the new security paradigms. Such initiatives foster a culture of security and compliance, which is essential for the successful adoption of PQC and ZTA (Enyejo, et al.,2024)

- *Collaboration with Industry and Government Bodies*

Collaborating with industry peers and government agencies provides access to shared knowledge, resources, and guidance. For instance, the National Institute of Standards and Technology (NIST) offers frameworks and standards that can assist organizations in navigating the complexities of implementing PQC within a Zero Trust framework (Dziechciarz, et al., 2024). Leveraging such resources ensures alignment with best practices and facilitates a more seamless integration (Enyejo, et al.,2024).

- *Continuous Monitoring and Adaptation*

The cybersecurity landscape is dynamic, with threats and technologies evolving rapidly. Continuous monitoring of systems and regular updates to security protocols are essential to maintain robust defenses. Organizations must remain vigilant and adaptable, ensuring that their security measures evolve in tandem with emerging threats and technological advancements.

In summary, the successful integration of PQC and ZTA requires a strategic, informed, and collaborative approach. By conducting comprehensive assessments, engaging stakeholders, collaborating with authoritative bodies, and maintaining adaptability, organizations can enhance their cybersecurity posture in the face of evolving challenges (Enyejo, et al.,2024)

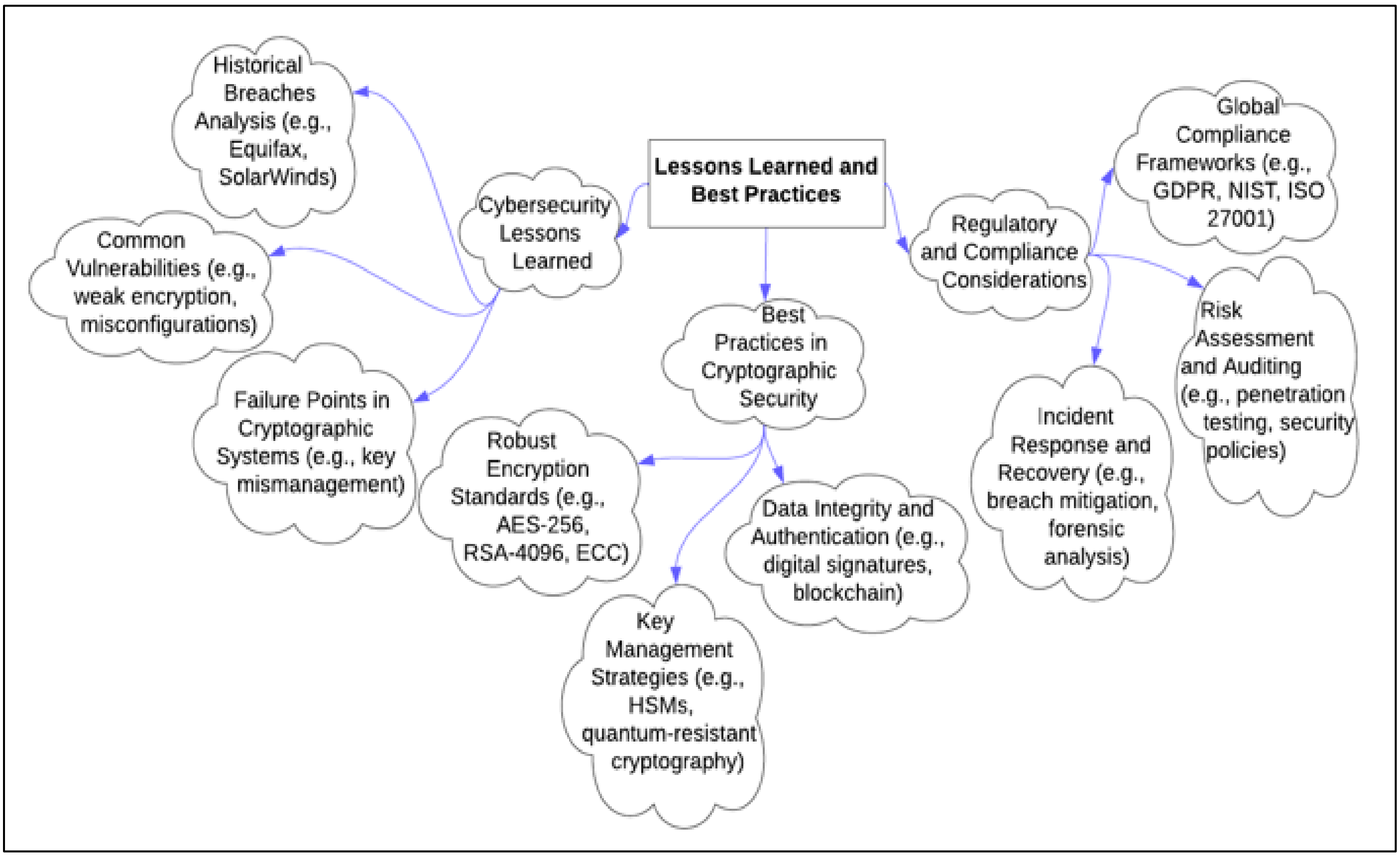
Lessons Learned and Best Practices
Cybersecurity Lessons Learned
Historical Breaches Analysis (e.g., Equifax, SolarWinds)
Common Vulnerabilities (e.g., weak encryption, misconfigurations)
Failure Points in Cryptographic Systems (e.g., key mismanagement)
Best Practices in Cryptographic Security
Robust Encryption Standards (e.g., AES-256, RSA-4096, ECC)
Key Management Strategies (e.g., HSMs, quantum-resistant cryptography)
Data Integrity and Authentication (e.g., digital signatures, blockchain)
Regulatory and Compliance Considerations
Global Compliance Frameworks (e.g., GDPR, NIST, ISO 27001)
Risk Assessment and Auditing (e.g., penetration testing, security policies)
Incident Response and Recovery (e.g., breach mitigation, forensic analysis)

Fig 5 Analysis of Organizations Implementing PQC and Zero Trust

Figure 5 provides a structured overview of key lessons learned and best practices in cryptographic security, divided into three primary branches. The first branch, Cybersecurity Lessons Learned, examines past security breaches, highlighting vulnerabilities such as weak encryption, misconfigurations, and poor key management that have led to major cyber incidents. The second branch, Best Practices in Cryptographic Security, outlines essential measures like adopting robust encryption standards (AES-256, RSA-4096, ECC), implementing secure key management techniques (HSMs, quantum-resistant cryptography), and ensuring data integrity through authentication methods like digital signatures and blockchain technology. The third branch, Regulatory and Compliance Considerations, focuses on the importance of aligning security strategies with global frameworks such as GDPR, NIST, and ISO 27001, emphasizing risk assessment, penetration testing, and incident response protocols. By integrating these components, the diagram presents a holistic approach to strengthening cryptographic implementations, enabling organizations to mitigate security risks while maintaining compliance and resilience against evolving cyber threats.

➢ *Regulatory and Compliance Considerations*

The integration of Post-Quantum Cryptography (PQC) and Zero Trust Architecture (ZTA) necessitates a thorough understanding of evolving regulatory and compliance landscapes. Organizations must proactively adapt to new standards and frameworks to ensure robust security and compliance (Enyejo, et al.,2024) as presented in table 5.

- *Post-Quantum Cryptography Standards*

The National Institute of Standards and Technology (NIST) has been at the forefront of developing PQC standards to counteract potential threats posed by quantum computing. In August 2024, NIST finalized its initial set of quantum-resistant encryption algorithms, marking a significant milestone in cryptographic standardization (Dziechciarz, et al., 2024). These standards are designed to secure a wide range of electronic information, from confidential communications to financial transactions, against the anticipated capabilities of quantum computers. Organizations are encouraged to transition to these NIST-approved algorithms to maintain compliance and protect sensitive data (Enyejo, et al.,2024)

- *Zero Trust Architecture and Regulatory Alignment*

Zero Trust Architecture emphasizes strict access controls and continuous verification, aligning closely with various regulatory requirements. For instance, implementing ZTA can aid in meeting the stringent data protection mandates of regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). By enforcing robust authentication and authorization protocols, ZTA helps ensure that only authorized individuals access sensitive information, thereby supporting compliance efforts (Akamai, 2023).

- *Challenges in Certification and Compliance*

Despite advancements, integrating PQC into existing systems presents challenges, particularly concerning certification and compliance. Current certification frameworks, such as Common Criteria (CC) and Commercial Solutions for Classified (CSfC), have yet to fully incorporate PQC algorithms. This gap means that products utilizing the latest quantum-resistant encryption may face hurdles in achieving necessary certifications for government use (Cisco, 2024). Organizations must stay informed about updates to these certification processes to ensure that their security implementations remain compliant as standards evolve (Enyejo, et al.,2024)

- *Proactive Measures for Compliance*

To navigate the complexities of regulatory compliance in the context of PQC and ZTA, organizations should:

- Stay Informed: Regularly monitor updates from standardization bodies like NIST to remain abreast of new cryptographic standards and compliance requirements (Ayoola, et al.,2024).
- Engage in Planning: Develop comprehensive migration strategies that address the integration of PQC and ZTA, considering potential impacts on existing compliance statuses.
- Collaborate with Authorities: Work closely with regulatory agencies and industry groups to understand evolving requirements and contribute to the development of practical compliance frameworks (Ayoola, et al.,2024).

By adopting these proactive measures, organizations can effectively manage the regulatory and compliance challenges associated with implementing Post-Quantum Cryptography and Zero Trust Architectures.

Table 5 Lessons Learned and Best Practices

Regulatory Frameworks	Compliance Requirements	Challenges in Implementation	Proposed Strategies
General Data Protection Regulation (GDPR)	Requires strict data privacy, user consent, and breach notification within 72 hours.	Ensuring full compliance across decentralized systems is complex.	Implement strong encryption, data anonymization, and automated compliance monitoring.
National Institute of Standards and Technology (NIST) Guidelines	Provides cybersecurity best practices, including Zero Trust and Post-Quantum Cryptography (PQC) adoption.	Organizations may struggle with adapting legacy systems to align with new security standards.	Gradual integration of NIST-recommended security controls and workforce training.
Financial Industry Regulatory Authority (FINRA) & Banking Regulations	Mandates risk assessments, transaction monitoring, and fraud prevention in financial systems.	Compliance with evolving financial security laws can be costly and resource-intensive.	Leverage AI-driven compliance tools, blockchain auditing, and automated reporting.
Sector-Specific Regulations (e.g., HIPAA, PCI-DSS)	Requires strict access controls, data encryption, and security audits in healthcare, finance, and critical infrastructure.	Achieving interoperability between regulatory requirements and emerging security technologies is challenging.	Adopt a unified compliance framework, real-time monitoring, and Zero Trust policies to ensure adherence.

VII. CONCLUSION AND FUTURE DIRECTIONS

➤ *Summary of Key Findings*

The study explored the intersection of Post-Quantum Cryptography (PQC) and Zero Trust Architecture (ZTA), emphasizing their collective role in fortifying cybersecurity frameworks against evolving threats. The findings highlight the increasing urgency for organizations to transition toward quantum-resistant encryption mechanisms while simultaneously adopting a Zero Trust model to enhance security posture and mitigate unauthorized access risks. The integration of PQC within existing cryptographic infrastructures poses both technical and operational challenges, necessitating extensive research, standardization, and strategic planning. As quantum computing capabilities advance, the vulnerabilities of classical encryption protocols become more pronounced, necessitating a proactive approach to cryptographic agility and resilience. Zero Trust Architecture, which operates on the principles of continuous verification, least privilege access, and micro-segmentation, aligns closely with regulatory and compliance requirements. Organizations implementing ZTA benefit from enhanced visibility, reduced attack surfaces, and improved threat detection. However, challenges such as legacy system compatibility, policy enforcement complexity, and increased authentication overhead remain key concerns. The necessity of real-time identity verification and access control mechanisms underscores the criticality of ZTA adoption in securing decentralized financial ecosystems and enterprise infrastructures. The study also examined regulatory considerations surrounding PQC and ZTA, particularly in the context of compliance frameworks such as GDPR and NIST's post-quantum cryptography standardization efforts. While regulatory bodies have taken significant steps in developing guidelines, organizations face hurdles in achieving certification for emerging cryptographic solutions. Compliance strategies must be adaptive, requiring collaboration between enterprises, government agencies, and cybersecurity experts to establish practical and enforceable standards.

Key lessons from early adopters of PQC and ZTA highlight best practices such as phased implementation, risk-based approaches to cryptographic migration, and the importance of stakeholder education. By addressing adoption challenges and aligning with regulatory expectations, organizations can effectively future-proof their security frameworks, ensuring resilience in an era of rapid technological advancement.

- *Emerging Trends in Quantum Security and Cyber Resilience*

The evolution of quantum computing has necessitated a paradigm shift in cybersecurity strategies, with emerging trends in quantum security and cyber resilience becoming a focal point for organizations worldwide. The rapid advancements in quantum algorithms pose a significant threat to classical cryptographic systems, leading to an accelerated global effort toward the adoption of Post-Quantum Cryptography (PQC). One key trend is the development and standardization of quantum-resistant cryptographic algorithms, as spearheaded by initiatives such as NIST’s PQC competition. These algorithms aim to replace vulnerable encryption protocols and ensure long-term data security against quantum-enabled attacks. Another critical trend is the integration of Zero Trust Architecture (ZTA) with quantum security measures to enhance cyber resilience. As organizations shift toward decentralized security models, incorporating quantum-resistant authentication mechanisms and encryption layers within Zero Trust frameworks is essential. This approach ensures that even in post-quantum environments, access control, identity verification, and network segmentation remain robust against advanced cyber threats. The convergence of PQC and ZTA reflects a broader industry movement toward dynamic security models that rely on continuous verification rather than perimeter-based defenses. Organizations are also exploring hybrid cryptographic approaches that combine classical and quantum-resistant encryption methods. This transitional strategy mitigates risks associated with the abrupt obsolescence of traditional cryptographic protocols while providing a scalable pathway for post-quantum migration. Additionally, the rise of quantum key distribution (QKD) and quantum-safe communication networks highlights a growing interest in leveraging quantum mechanics for secure key exchange, eliminating vulnerabilities associated with conventional asymmetric encryption. Cyber resilience frameworks are evolving to incorporate quantum security measures into risk management and compliance strategies. Governments and regulatory bodies are actively drafting policies to address the quantum threat, encouraging enterprises to invest in quantum-readiness assessments. By proactively adopting PQC solutions, integrating Zero Trust principles, and refining regulatory frameworks, organizations can ensure long-term security and resilience in the face of quantum-driven cyber risks.

- *Recommendations for Future Research and Security Implementations*

As quantum computing capabilities continue to advance, future research must prioritize the development of scalable and efficient post-quantum cryptographic (PQC) models that ensure long-term data security and cyber resilience. A key area of focus should be refining quantum-resistant encryption schemes to optimize performance and interoperability across diverse digital infrastructures. Research efforts should explore the integration of PQC with existing cybersecurity frameworks, ensuring seamless deployment in both legacy and modernized systems without compromising efficiency. Additionally, continuous evaluation of hybrid cryptographic models that combine classical and post-quantum encryption methods will be essential to facilitate a smooth transition and mitigate the risks associated with the eventual obsolescence of traditional cryptographic standards.

Future research should also expand on the role of Zero Trust Architecture (ZTA) in a post-quantum security environment. Investigating the implementation of quantum-resistant identity verification mechanisms within ZTA can enhance the effectiveness of access control policies, reducing the likelihood of credential-based cyberattacks. Furthermore, leveraging artificial intelligence and machine learning to automate threat detection and response in quantum-secure environments presents a promising avenue for strengthening cyber resilience. AI-driven anomaly detection models, combined with Zero Trust principles, can significantly improve an organization's ability to mitigate evolving quantum threats in real time. In addition to technical advancements, regulatory and compliance considerations must be further explored to establish globally accepted standards for quantum-secure implementations. Policymakers and industry stakeholders should collaborate on frameworks that promote transparency, interoperability, and enforceable guidelines for quantum-resistant security adoption. Future studies should examine the economic and operational challenges of large-scale PQC deployment, identifying cost-effective solutions to ensure broad accessibility. To maintain a proactive stance against quantum-enabled cyber threats, interdisciplinary collaboration between cryptographers, security analysts, and regulatory bodies is crucial. By fostering innovation in quantum security research, refining ZTA models, and aligning policy developments with technological advancements, organizations can achieve robust, future-proof cybersecurity infrastructures that withstand the evolving quantum landscape.

REFERENCES

[1]. Afrose, S., Xiao, Y., Rahaman, S., Miller, B. P., & Yao, D. (2021). Evaluation of Static Vulnerability Detection Tools with Java Cryptographic API Benchmarks. *arXiv preprint arXiv:2112.04037*. https://arxiv.org/abs/2112.04037

[2]. Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Quantum Cryptography and Blockchain-Based Social Media Platforms as a Dual Approach to Securing Financial Transactions in CBDCs and Combating Misinformation in U.S. Elections. *International Journal of Innovative Science and Research Technology*, 9(10). https://doi.org/10.38124/ijisrt/IJISRT24OCT1697

[3]. Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Quantum Cryptography and Blockchain-Based Social Media Platforms as a Dual Approach to Securing Financial Transactions in CBDCs and

Combating Misinformation in U.S. Elections. *International Journal of Innovative Science and Research Technology*, 9(10). https://doi.org/10.38124/ijisrt/IJISRT24OCT1697

[4]. Akindotei, O., Igba E., Awotiwon, B. O., & Otakwu, A (2024). Blockchain Integration in Critical Systems Enhancing Transparency, Efficiency, and Real-Time Data Security in Agile Project Management, Decentralized Finance (DeFi), and Cold Chain Management. *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 3, Issue 11, 2024. DOI: 10.38124/ijsrmt.v3i11.107.

[5]. Alvarado, M., Gayler, L., Seals, A., Wang, T., & Hou, T. (2023). A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges. *arXiv preprint arXiv:2312.10430*. https://arxiv.org/abs/2312.10430

[6]. Alvarado, M., Gayler, L., Seals, A., Wang, T., & Hou, T. (2023). A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges. *arXiv preprint arXiv:2312.10430*. https://arxiv.org/abs/2312.10430

[7]. Ayoola, V. B., Audu, B. A., Boms, J. C., Ifoga, S. M., Mbanugo, O. J., & Ugochukwu, U. N. (2024). Integrating Industrial Hygiene in Hospice and Home Based Palliative Care to Enhance Quality of Life for Respiratory and Immunocompromised Patients. NOV 2024 | *IRE Journals* | Volume 8 Issue 5 | ISSN: 2456-8880.

[8]. Ayoola, V. B., Idoko, P. I., Danquah, E. O., Ukpoju, E. A., Obasa, J., Otakwu, A. & Enyejo, J. O. (2024). Optimizing Construction Management and Workflow Integration through Autonomous Robotics for Enhanced Productivity Safety and Precision on Modern Construction Sites. *International Journal of Scientific Research and Modern Technology (IJSRMT)*. Vol 3, Issue 10, 2024. https://www.ijsrmt.com/index.php/ijsrmt/article/view/56

[9]. Ayoola, V. B., Ugochukwu, U. N., Adeleke, I., Michael, C. I. Adewoye, M. B., & Adeyeye, Y. (2024). Generative AI-Driven Fraud Detection in Health Care Enhancing Data Loss Prevention and Cybersecurity Analytics for Real-Time Protection of Patient Records. *International Journal of Scientific Research and Modern Technology (IJSRMT)*, Volume 3, Issue 11, 2024.https://www.ijsrmt.com/index.php/ijsrmt/article/view/112

[10]. Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., Daniel, S. J., & Atul. (2022). Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. *arXiv preprint arXiv:2202.02826*.

[11]. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2008). *Post-Quantum Cryptography*. Springer.

[12]. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2008). *Post-Quantum Cryptography*. Springer.

[13]. Bernstein, E., Vazirani, U., & Bennett, C. H. (1997). The strengths and weaknesses of quantum computation. *SIAM Journal on Computing*, 26(5), 1510-1523.

[14]. Cem Dilmegani (2025) **Quantum Cryptography/Encryption** https://research.aimultiple.com/quantum-cryptography/

[15]. Cintas Canto, A., Kaur, J., Mozaffari Kermani, M., & Azarderakhsh, R. (2023). Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security. *arXiv preprint arXiv:2305.13544*. https://arxiv.org/abs/2305.13544

[16]. Cintas Canto, A., Kaur, J., Mozaffari Kermani, M., & Azarderakhsh, R. (2023). Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security. *arXiv preprint arXiv:2305.13544*. https://arxiv.org/abs/2305.13544

[17]. CrowdStrike. (2024). *What is Zero Trust Security? Principles of the Zero Trust Model*. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/

[18]. Ding, J., & Petzoldt, A. (2017). Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4), 28-36.

[19]. Dziechciarz, D., & Niemiec, M. (2024). Efficiency Analysis of NIST-Standardized Post-Quantum Cryptographic Algorithms for Digital Signatures in Various Environments. *Electronics*, *14*(1), 70.

[20]. Dziechciarz, D., & Niemiec, M. (2024). Efficiency Analysis of NIST-Standardized Post-Quantum Cryptographic Algorithms for Digital Signatures in Various Environments. *Electronics*, *14*(1), 70.

[21]. Dziechciarz, D., & Niemiec, M. (2024). Efficiency Analysis of NIST-Standardized Post-Quantum Cryptographic Algorithms for Digital Signatures in Various Environments. *Electronics*, *14*(1), 70.

[22]. Enyejo, J. O., Fajana, O. P., Jok, I. S., Ihejirika, C. J., Awotiwon, B. O., & Olola, T. M. (2024). Digital Twin Technology, Predictive Analytics, and Sustainable Project Management in Global Supply Chains for Risk Mitigation, Optimization, and Carbon Footprint Reduction through Green Initiatives. *International Journal of Innovative Science and Research Technology*, Volume 9, Issue 11, November– 2024. ISSN No:-2456-2165. https://doi.org/10.38124/ijisrt/IJISRT24NOV1344

[23]. Enyejo, J. O., Fajana, O. P., Jok, I. S., Ihejirika, C. J., Awotiwon, B. O., & Olola, T. M. (2024). Digital Twin Technology, Predictive Analytics, and Sustainable Project Management in Global Supply Chains for Risk Mitigation, Optimization, and Carbon Footprint Reduction through Green Initiatives. *International Journal of Innovative Science and Research Technology*, Volume 9, Issue 11, November– 2024. ISSN No:-2456-2165. https://doi.org/10.38124/ijisrt/IJISRT24NOV1344

[24]. Enyejo, J. O., Obani, O. Q., Afolabi, O., Igba, E., & Ibokette, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular and dynamic security models.

Magna Scientia Advanced Research and Reviews, 2021, 11(02), 132–150. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2021-0032.pdf

[25]. Enyejo, L. A., Adewoye, M. B. & Ugochukwu, U. N. (2024). Interpreting Federated Learning (FL) Models on Edge Devices by Enhancing Model Explainability with Computational Geometry and Advanced Database Architectures. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. Vol. 10 No. 6 (2024): November-December doi : https://doi.org/10.32628/CSEIT24106185

[26]. Ezeh, N. V., Batur, D. S., Oluhaiyero, S. Y., Kehinde, A., Chukwunweike, C. N., Ali, O. E., & Igba, E. (2024). Blockchain Driven Cold Chain Logistics and Decentralized Inventory Systems for Managing Post-Harvest Losses and Improving Financial Sustainability in Regional Food Hubs. *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 3, Issue 9, 2024 DOI:https://doi.org/10.5281/zenodo.14874303

[27]. Ezeh, N. V., Batur, S. D., Oluhaiyero, Shade. Y., Abiodun, K., Nwobi, C. C., Ali, O. E., & Igba, E. (2024). Blockchain Driven Cold Chain Logistics and Decentralized Inventory Systems for Managing Post-Harvest Losses and Improving Financial Sustainability in Regional Food Hubs. *International Journal of Scientific Research and Modern Technology (IJSRMT)*. Volume 3, Issue 9, 2024. DOI: https://doi.org/10.5281/zenodo.14874303

[28]. Gaudry, P., & Golovnev, A. (2019). Breaking the encryption scheme of the Moscow Internet voting system. *arXiv preprint arXiv:1908.05127*. https://arxiv.org/abs/1908.05127

[29]. Igba E., Ihimoyan, M. K., Awotinwo, B., & Apampa, A. K. (2024). Integrating BERT, GPT, Prophet Algorithm, and Finance Investment Strategies for Enhanced Predictive Modeling and Trend Analysis in Blockchain Technology. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.,* November-December-2024, 10 (6) : 1620-1645.https://doi.org/10.32628/CSEIT241061214

[30]. Igba, E., Abiodun, K. & Ali, E. O. (2025). Building the Backbone of the Digital Economy and Financial Innovation through Strategic Investments in Data Centers. International Journal of Innovative Science and Research Technology, ISSN No:-2456-2165. https://doi.org/10.5281/zenodo.14651210

[31]. Igba, E., Danquah, E. O., Ukpoju, E. A., Obasa, J., Olola, T. M., & Enyejo, J. O. (2024). Use of Building Information Modeling (BIM) to Improve Construction Management in the USA. *World Journal of Advanced Research and Reviews*, 2024, 23(03), 1799–1813. https://wjarr.com/content/use-building-information-modeling-bim-improve-construction-management-usa

[32]. Ijiga, A. C., Igbede, M. A., Ukaegbu, C., Olatunde, T. I., Olajide, F. I. & Enyejo, L. A. (2024). Precision healthcare analytics: Integrating ML for automated image interpretation, disease detection, and prognosis prediction. *World Journal of Biology Pharmacy and Health Sciences*, 2024, 18(01), 336–354. https://wjbphs.com/sites/default/files/WJBPHS-2024-0214.pdf

[33]. Ijiga. A. C., Eguagie, M. O. & Tokowa, A. (2025). Mineralization Potential of the Lithium-Bearing Micas in the St Austell Granite, SW England. *International Journal of Innovative Science and Research Technology*. ISSN No:-2456-2165, https://doi.org/10.5281/zenodo.14709730

[34]. Joshi, H. (2024). Emerging Technologies Driving Zero Trust Maturity Across Industries. *IEEE Open Journal of the Computer Society*.

[35]. Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., & Schimmler, M. (2006). Breaking ciphers with COPACOBANA–a cost-optimized parallel code breaker. In *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8* (pp. 101-118). Springer Berlin Heidelberg.

[36]. Kunde, V., Nold, J. M., & Hielscher, J. (2024, September). " Everything We Encrypt Today Could Be Cracked"—Exploring (Post) Quantum Cryptography Misconceptions. In *Proceedings of the 2024 European Symposium on Usable Security* (pp. 125-136).

[37]. M. Jarjar, Abid Abdellah (2024) Multiple image encryption acting at the RNA level https://www.semanticscholar.org/paper/Multiple-image-encryption-acting-at-the-RNA-level-Jarjar-Abdellah/21f689ed2100e1898bf28f25691790e2fb30c594

[38]. Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *arXiv preprint* arXiv:1804.00200. https://arxiv.org/abs/1804.00200

[39]. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

[40]. National Institute of Standards and Technology (NIST). (2016). *Post-Quantum Cryptography: NIST's Plan for the Future*. Retrieved from https://csrc.nist.gov/publications/detail/nistir/8105/final

[41]. Rahaman, S., Xiao, Y., Afrose, S., Shaon, F., Tian, K., Frantz, M., Yao, D., & Kantarcioglu, M. (2018). CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects. *arXiv preprint arXiv:1806.06881*. https://arxiv.org/abs/1806.06881

[42]. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6), 1-40.

[43]. Saxena, A., Mancilla, J., Montalban, I., & Pere, C. (2023). *Financial Modeling Using Quantum Computing: Design and manage quantum machine learning solutions for financial analysis and decision making*. Packt Publishing Ltd.

[44]. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In

Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124-134). IEEE.

[45]. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134.

[46]. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

[47]. Shor's algorithm. (2023, October 1). In *Wikipedia*. https://en.wikipedia.org/wiki/Shor%27s_algorithm

[48]. Tiamiyu, D., Aremu, S. O., Igba, E., Ihejirika, C. J., Adewoye, M. B., & Ajayi, A. A. (2024). Interpretable Data Analytics in Blockchain Networks Using Variational Autoencoders and Model-Agnostic Explanation Techniques for Enhanced Anomaly Detection. *International Journal of Scientific Research in Science and Technology*, 11(6), 152–183. https://doi.org/10.32628/IJSRST24116170

[49]. Tiamiyu, D., Aremu, S. O., Igba, E., Ihejirika, C. J., Adewoye, M. B. & Ajayi, A. A. (2024). Interpretable Data Analytics in Blockchain Networks Using Variational Autoencoders and Model-Agnostic Explanation Techniques for Enhanced Anomaly Detection. *International Journal of Scientific Research in Science and Technology*. Volume 11, Issue 6 November-December-2024. 152-183. https://doi.org/10.32628/IJSRST24116170