axioms

Article

A Comprehensive Review of MI-HFE and IPHFE Cryptosystems: Advances in Internal Perturbations for Post-Quantum Security

Yong Wang, Lingyue Li, Ying Zhou and Huili Zhang

MDPI

https://doi.org/10.3390/axioms13110741

axioms

MDPI

Article

A Comprehensive Review of MI-HFE and IPHFE Cryptosystems: Advances in Internal Perturbations for Post-Quantum Security

Yong Wang [1], **Lingyue Li** [1], **Ying Zhou** [2] **and Huili Zhang** [1,*]

[1] School of Arts and Sciences, Guangzhou Maritime University, Guangzhou 510725, China; p117646@siswa.ukm.edu.my (Y.W.)
[2] Institute of Visual Informatics (IVI), Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Malaysia; p114383@siswa.ukm.edu.my
* Correspondence: zhang.huili0203@163.com

Abstract: The RSA cryptosystem has been a cornerstone of modern public key infrastructure; however, recent advancements in quantum computing and theoretical mathematics pose significant risks to its security. The advent of fully operational quantum computers could enable the execution of Shor's algorithm, which efficiently factors large integers and undermines the security of RSA and other cryptographic systems reliant on discrete logarithms. While Grover's algorithm presents a comparatively lesser threat to symmetric encryption, it still accelerates key search processes, creating potential vulnerabilities. In light of these challenges, there has been an intensified focus on developing quantum-resistant cryptography. Current research is exploring cryptographic techniques based on error-correcting codes, lattice structures, and multivariate public key systems, all of which leverage the complexity of NP-hard problems, such as solving multivariate quadratic equations, to ensure security in a post-quantum landscape. This paper reviews the latest advancements in quantum-resistant encryption methods, with particular attention to the development of robust trapdoor functions. It also provides a detailed analysis of prominent multivariate cryptosystems, including the Matsumoto–Imai, Oil and Vinegar, and Polly Cracker schemes, alongside recent progress in lattice-based systems such as Kyber and Crystals-DILITHIUM, which are currently under evaluation by NIST for potential standardization. As the capabilities of quantum computing continue to expand, the need for innovative cryptographic solutions to secure digital communications becomes increasingly critical.

Keywords: RSA encryption; quantum-resistant cryptography; lattice-based cryptography; multivariate public key cryptosystems; NP-hard problems; quantum computing threats; digital security

MSC: 94A60

check for updates

Citation: Wang, Y.; Li, L.; Zhou, Y.; Zhang, H. A Comprehensive Review of MI-HFE and IPHFE Cryptosystems: Advances in Internal Perturbations for Post-Quantum Security. *Axioms* **2024**, *13*, 741. https://doi.org/10.3390/axioms13110741

Academic Editor: Oscar Humberto Ross

Received: 18 September 2024
Revised: 23 October 2024
Accepted: 26 October 2024
Published: 29 October 2024

1. Introduction

The RSA cryptosystem [1] has long been a foundational element in modern public key infrastructure, primarily due to its reliance on the computational challenge of factoring large integers—a problem deeply rooted in both elementary and analytic number theory. For decades, no highly efficient algorithm has been identified to solve this problem, reinforcing RSA's role as a cornerstone in cryptographic protection. Nonetheless, recent advancements in computational technologies, particularly quantum computing, have begun to cast doubt on this long-standing assumption [2].

Should quantum computers reach full operational capacity, they would be capable of implementing Shor's algorithm [3], which factors large integers in polynomial time. This capability would undermine RSA and other cryptographic protocols based on discrete logarithms, such as elliptic curve cryptography (ECC) and the Diffie–Hellman key exchange. The urgency of this potential threat is underscored by rapid progress in quantum research, driven by innovations in superconducting qubits, ion traps, and other advanced technologies [4]. Although large-scale quantum computers have not yet been realized, ongoing research and significant financial investment suggest that their development may be achieved within the coming decades [5], underscoring the immediate need for cryptographic solutions resilient to quantum-based attacks.

To address the threat posed by quantum advancements, researchers are actively developing cryptographic techniques resistant to quantum attacks, often referred to as post-quantum cryptography (PQC) [6]. Such approaches include cryptographic schemes based on error-correcting codes [7], lattice-based systems [8], and multivariate public key cryptosystems (MPKC) [9]. Notable examples of lattice-based cryptography rely on the inherent difficulty of problems like Learning with Errors (LWE) and the Shortest Vector Problem (SVP), which currently resist all known quantum algorithms. Similarly, code-based cryptosystems, such as the McEliece cryptosystem [10], are grounded in the complexity of decoding random linear codes—another challenge for which no efficient quantum algorithm has been discovered.

Multivariate public key cryptography focuses on the computational difficulty of solving systems of multivariate quadratic equations, a problem classified as NP-hard. These systems utilize transformations to obscure the underlying quadratic functions, offering resistance to both classical and quantum-based cryptanalytic attacks. Examples of such systems include the Matsumoto–Imai and Oil and Vinegar schemes [11], which employ transformation techniques for securing encryption, although challenges such as key size and efficiency persist.

These quantum-resistant cryptographic solutions are no longer merely theoretical concepts. The National Institute of Standards and Technology (NIST) has initiated an international effort to establish standards for post-quantum cryptography [12]. Relevant literature includes the status report in *NIST SP 800-186*, which outlines the progress of the project and the latest information on candidate algorithms [13]. Furthermore, *NIST IR 8240* details the candidate algorithms for post-quantum cryptography and their evaluation criteria [14], while *NIST SP 800-90A* discusses the application of deterministic random number generators [15]. For a more comprehensive understanding of the background of these standards, one can refer to *NIST SP 800-178* and *NIST SP 800-53*, which address the cryptographic framework for federal agencies and security and privacy controls for information systems, respectively, [16,17]. Additionally, related research highlights the impact of quantum computing on cybersecurity, as seen in *Post-Quantum Cryptography: A New Hope* and *Quantum Computing and the Future of Cybersecurity* [18,19]. More information and resources can be found on NIST's official website and in related workshop documents [20].

Among the leading candidates in this process are lattice-based protocols like Kyber and Crystals-Dilithium, both of which have demonstrated significant promise during standardization evaluations [21]. As quantum technology advances, the need for resilient cryptographic systems to protect communications from future quantum threats grows increasingly urgent.

Our contribution: The significant contributions of this paper lie in its comprehensive review of MI, HFE, and IPHFE cryptosystems, establishing a robust theoretical framework that addresses the key challenges posed by quantum computing. Emphasis is placed on MI, HFE and IPHFE cryptosystems as promising candidates in post-quantum cryptography, demonstrating their remarkable resilience and superiority in resisting both traditional and quantum attacks. Furthermore, this paper introduces a novel systematic comparison of lattice-based post-quantum cryptography, revealing profound insights into their theoretical foundations and implementations, thereby advancing academic dialogue in the field. Through in-depth quantitative analysis and real-world case studies, this research provides unprecedented guidance and significant contributions to both practical applications and theoretical development within the cryptography domain, markedly pushing the frontiers of post-quantum cryptography research and ensuring the security of future cryptographic systems.

2. Literature Review

The rapid advancement of quantum computing has amplified the need for secure post-quantum cryptographic solutions. Among these, MPKC has gained prominence due to its reliance on the complexity of solving multivariate quadratic equations, a well-known NP-hard problem that provides a robust foundation for security. This section presents an in-depth exploration of the theoretical foundations, recent innovations, and existing challenges within MPKC, with a particular emphasis on the Hidden Field Equations (HFE) cryptosystem and its adaptations, alongside an overview of select lattice-based post-quantum cryptographic schemes.

2.1. Theoretical Foundations of Multivariate Cryptography

Multivariate cryptography is built upon the computational difficulty of solving quadratic equations over finite fields, referred to as the Multivariate Quadratic (MQ) problem. As an NP-hard problem, MQ is resistant to both classical and quantum attacks, providing a strong security base for MPKCs. The algebraic complexity of these equations is further underscored by the inefficiencies in solving them via Gröbner basis techniques, which remain computationally prohibitive even with advances in quantum algorithms [22].

Compared to other post-quantum cryptographic methods—such as lattice-based cryptography, which relies on problems like the Shortest Vector Problem (SVP), or code-based cryptography, which focuses on decoding random linear codes—MPKCs offer unique advantages. These include smaller key sizes and faster signature verification [23]. However, challenges remain, particularly concerning the often-large public key sizes and the intricate design of secure trapdoors necessary to ensure cryptographic robustness.

2.2. HFE Cryptosystem and Its Variants

The Hidden Field Equations (HFE) cryptosystem, introduced by Patarin [24], stands as one of the most prominent examples of MPKCs. Its security is predicated on the difficulty of inverting a multivariate quadratic map obscured by a carefully engineered trapdoor, while HFE provides robust theoretical security, it has been susceptible to various algebraic attacks, such as Gröbner basis methods and relinearization techniques [25]. To mitigate these weaknesses, variants like HFEv [26], HFEv- [27,28], MultiHFE [29] and HMFEv [30] have been developed, incorporating vinegar variables and internal perturbation methods to strengthen security [26,27,29,31].

Recent advances have sought to improve both the efficiency and resilience of HFE-based systems. For instance, the QUARTZ signature scheme [32,33], built on HFEv-, demonstrates the practical potential of MPKCs. However, it remains inefficient compared to traditional systems like RSA. In response to these challenges, Ding and Yang proposed the Gui signature scheme [34], which reduces the computational complexity of QUARTZ while maintaining similar security levels. These advancements mark crucial steps toward enhancing the practicality of HFE-based cryptographic solutions.

2.3. Polly Cracker Schemes in Post-Quantum Cryptography

Polly Cracker schemes, based on the hardness of solving polynomial ideal problems, form an important part of post-quantum cryptography. This review outlines the key principles, encryption and decryption processes, advantages, challenges, and current research directions associated with Polly Cracker schemes. As quantum computers pose a threat to classical cryptography, Polly Cracker schemes aim to provide a quantum-resistant alternative by leveraging the computational difficulty of polynomial ideal problems.

Polly Cracker schemes are based on the problem of solving polynomial ideals and were first introduced by M. Fellows and N. Koblitz in 1993 [35]. With the advent of quantum computing, classical encryption algorithms such as RSA and ECC are vulnerable to quantum attacks. Post-quantum cryptography seeks alternatives that are secure against quantum adversaries, and Polly Cracker schemes are one such approach.

The fundamental principle behind Polly Cracker encryption lies in the use of polynomial rings and ideal theory. Encryption involves hiding a message m within a noisy polynomial equation system. Decryption requires solving the ideal-related polynomial problem to recover m. This problem is believed to be computationally difficult for both classical and quantum computers.

Encryption: To encrypt a message m, a polynomial equation system is constructed with random noise terms that obscure the message. The message is embedded in such a way that the noise polynomials make it computationally challenging to recover m without the correct decryption key.

Decryption: Decryption involves solving the polynomial system using techniques such as Gröbner basis computation [36], which helps reduce the noise and isolate the original message. This process, while theoretically sound, can be computationally expensive.

2.4. *Advantages and Challenges of Polly Cracker Schemes*

Polly Cracker schemes offer several notable advantages alongside significant challenges.

First, they demonstrate quantum resistance: the hardness of solving polynomial systems remains a substantial challenge even for quantum computers, making Polly Cracker schemes resistant to quantum attacks [37]. Additionally, the flexibility of these schemes is enhanced by the use of polynomial ideals, allowing for various configurations and the construction of different cryptographic schemes based on the same underlying principle.

However, these schemes also encounter critical challenges and limitations. A major concern is their efficiency, as the encryption and decryption processes often involve solving complex polynomial equations, which can be time-consuming, especially for large systems. Furthermore,Gröbner basis computation is essential for decryption but is known to be computationally intensive, which limits the practical applicability of these schemes [38].

In summary, while Polly Cracker schemes provide promising advantages in post-quantum cryptography, their efficiency and computational demands present notable challenges that must be addressed for broader adoption.

Compared to lattice-based schemes such as Learning With Errors (LWE) and NTRU, Polly Cracker schemes use polynomial ideals instead of lattice structures, while lattice-based schemes have seen broader adoption and more extensive security analysis, Polly Cracker schemes provide a novel approach with different underlying mathematics.

Current research directions are focused on several key areas: First, researchers are actively exploring methods to optimize Gröbner basis computations to reduce the overall time complexity associated with Polly Cracker encryption and decryption processes. Second, there is an increasing urgency for comprehensive evaluations of the security of Polly Cracker schemes against various attack models, particularly in the context of quantum threats [39]. Additionally, efforts are being made to identify real-world applications where the security properties of Polly Cracker schemes can provide significant advantages, despite existing concerns regarding efficiency. Overall, Polly Cracker schemes present a compelling post-quantum cryptographic alternative based on the difficulty of solving polynomial ideal problems, demonstrating potential resistance to quantum attacks. However, challenges related to efficiency and practicality remain, and ongoing research aims to address these limitations to enhance the feasibility of Polly Cracker schemes for broader adoption.

2.5. *Kyber and Crystals-DILITHIUM Schemes*

Kyber and Crystals-DILITHIUM are two prominent schemes in the rapidly evolving field of post-quantum cryptography, reflecting advanced methodologies designed to counteract the impending threats posed by quantum computing. As quantum capabilities advance, the vulnerabilities of traditional cryptographic systems, which rely on mathematical problems easily solvable by quantum algorithms, become increasingly apparent. Consequently, the development of robust and efficient post-quantum algorithms has emerged as a critical priority for securing sensitive data against future quantum attacks.

2.5.1. Kyber Scheme

Kyber is a lattice-based public key encryption framework specifically engineered for efficient key exchange and secure data encryption. It has been recognized as a leading candidate in the NIST post-quantum cryptography standardization initiative, largely due to its impressive performance metrics and strong security guarantees [40]. The foundational security of Kyber is anchored in the Learning With Errors (LWE) problem, a mathematical construct known for its robustness against both classical and quantum computational attacks.

The inherent complexity of the LWE problem arises from its reliance on the difficulty of solving systems of linear equations augmented by small random errors, a challenge that persists even when faced with advanced quantum techniques. This property establishes a solid barrier against potential quantum adversaries that may exploit more efficient algorithms. Recent research has significantly enhanced our understanding of LWE, illuminating potential quantum attack vectors and improving attack algorithms. The introduction of modulus switching techniques, for instance, represents a significant advancement in LWE security, offering new ways to mitigate risks associated with specific attack vectors [41–43]. This dynamic interplay between theoretical advancements and practical implementations illustrates the ongoing evolution of cryptographic research in response to emerging threats.

Performance Optimization and Real-World Applications

Kyber has undergone extensive performance optimizations, particularly in high-throughput environments where efficiency is paramount. Recent implementations incorporating parallel processing capabilities have achieved remarkable encryption and decryption times of approximately 5 ms and 10 ms, respectively, [44]. Such performance enhancements are particularly critical in applications requiring rapid data processing, including online banking, secure communications, and real-time data analysis.

The versatility of Kyber extends its applicability to various secure communication scenarios, including online banking, e-commerce, and cloud storage. By enabling rapid key exchanges, Kyber ensures the confidentiality and integrity of data transmitted over potentially insecure channels, thereby fostering user trust in digital transactions. Furthermore, as the Internet of Things (IoT) continues to proliferate, Kyber's robust security measures become increasingly relevant for resource-constrained devices, facilitating secure communications in smart homes, intelligent transportation systems, and other innovative applications [45,46]. The ability of Kyber to adapt to a range of operational environments positions it as a foundational technology in the transition to post-quantum secure systems.

Despite Kyber's remarkable performance and security capabilities, it faces challenges related to key management and scalability, particularly in contexts with limited computational resources. These challenges necessitate further research to optimize key management protocols, enhance scalability, and integrate Kyber with existing network architectures. Future directions may involve exploring memory optimization techniques, improving quantum attack resilience, and devising mechanisms for seamless integration with traditional cryptographic systems.

2.5.2. DILITHIUM Scheme

Crystals-DILITHIUM is a lattice-based digital signature scheme that excels in providing secure and efficient digital signatures, establishing itself as a leading candidate for post-quantum digital signature solutions [47]. Its design effectively meets contemporary demands for security, speed, and compact signature sizes, which are critical for modern applications [48–50].

The security of DILITHIUM is built upon both the Shortest Vector Problem (SVP) and the LWE problem, a dual reliance that strengthens its resistance against classical and quantum adversaries. The SVP is recognized as one of the hardest problems in computational mathematics, making it an ideal foundation for cryptographic applications. Recent studies have demonstrated that DILITHIUM maintains a robust security margin against various attack vectors, including those posed by advanced quantum algorithms, such as Grover's algorithm and Shor's algorithm [3,51]. The continual refinement of DILITHIUM's security parameters is essential in ensuring its resilience against evolving threats in the quantum computing landscape.

Performance Optimization and Real-World Applications

DILITHIUM has achieved significant advancements in signature generation and verification speeds, with the latest iteration capable of generating signatures in approximately 15 ms and verifying them within 2–3 ms. These performance enhancements not only render DILITHIUM competitive in theoretical frameworks but also increase its attractiveness for practical applications, particularly in blockchain technology and digital identity verification.

In blockchain systems, DILITHIUM plays a critical role in ensuring the legitimacy and integrity of transactions. Its efficient signature generation and verification processes are particularly well-suited for high-volume transaction environments, where maintaining the trustless nature of the blockchain is paramount. The combination of speed and security offered by DILITHIUM supports the rapid growth of decentralized applications that require trustworthy digital interactions. Additionally, in the realm of digital identity verification, DILITHIUM provides a robust mechanism for user authentication, protecting sensitive user data from tampering and facilitating secure online interactions. Its ability to deliver fast, secure signatures makes DILITHIUM a valuable asset in securing digital communications and transactions.

Despite its notable potential, the signature size of DILITHIUM remains a concern, especially in scenarios that require compact signatures, such as mobile devices and embedded systems. Addressing this challenge is crucial for broadening the adoption of DILITHIUM in various applications. Future research directions may focus on further reducing signature sizes, investigating the integration of DILITHIUM with other cryptographic frameworks, and accelerating its standardization process for real-world applications. By overcoming these hurdles, DILITHIUM can solidify its role as a cornerstone of secure digital communications in the post-quantum era.

Overall, the advancements represented by Kyber and DILITHIUM reflect the broader trends in post-quantum cryptography, where resilience against quantum attacks and operational efficiency are paramount. As researchers continue to delve into the theoretical underpinnings and practical implementations of these schemes, the future of secure digital communications will increasingly rely on the integration of post-quantum solutions into everyday technologies. This transition not only necessitates the development of new algorithms but also requires a comprehensive understanding of their implications in real-world scenarios, ensuring that they can meet the evolving security needs of society in a post-quantum world.

Comparison of Kyber and Crystals-DILITHIUM

To better understand the differences between Kyber and Crystals-DILITHIUM, Table 1 presents a comparative analysis of their key features. This comparison highlights the distinct roles these schemes play in post-quantum cryptography, including their security foundations, performance metrics, key sizes, and applicable use cases. Such insights are crucial for selecting the appropriate cryptographic solution based on specific requirements and operational contexts.

Kyber and Crystals-DILITHIUM are significant advancements in post-quantum cryptography, essential for future security protocols as quantum technology evolves. Kyber excels in key encapsulation with enhanced computational efficiency and smaller key sizes, making it ideal for resource-constrained environments. Similarly, Crystals-DILITHIUM, an advanced digital signature scheme, optimizes both signature size and verification speed, making it suitable for various applications like blockchain and financial transactions. To maintain their relevance, ongoing research must focus on improving performance, optimizing for specific hardware platforms, and facilitating widespread adoption through standardization efforts by organizations like NIST. Ultimately, the integration of Kyber and Crystals-DILITHIUM into security frameworks will be crucial for safeguarding digital communications in the quantum era.

Table 1. Comparison of Kyber and Crystals-DILITHIUM.

Feature	Kyber	Crystals-DILITHIUM
Type	Public Key Encryption	Digital Signature
Security	Based on LWE	Based on LWE and SVP
Performance	5 ms Encryption, 10 ms Decryption	15 ms Signature Generation, 2–3 ms Verification
Key Size	Kyber-512: 800 bytes	Signature Size: 1.5–2 KB
Application	Secure Communication, IoT	Digital Signatures, Blockchain

2.6. Current Challenges and Future Directions

A major hurdle for MPKCs, particularly in encryption schemes such as HFE, is the large public key size. Researchers are exploring various key compression techniques and methods to streamline the encryption and decryption processes [52]. Additionally, perturbation techniques have shown promise in enhancing the security of MPKCs against differential attacks, although balancing these enhancements with efficiency remains a complex challenge.

Looking forward, another critical concern is the potential vulnerability of multivariate systems to quantum-specific attacks, while MPKCs are generally seen as quantum-resistant, further research is needed to understand and mitigate risks posed by quantum algorithms that could exploit weaknesses unique to multivariate cryptography [53]. As quantum computing technology continues to evolve, addressing these vulnerabilities is vital to ensure the long-term security and viability of MPKCs.

2.7. Historical Overview and the Impact of Quantum Computing

The origins of multivariate cryptography can be traced back to the 1990s, with early systems like Matsumoto–Imai (MI) and HFE paving the way for the field's development [54]. Over the past three decades, numerous improvements and optimizations have emerged, with a growing emphasis on post-quantum security. The advent of quantum computing has accelerated research efforts, highlighting the pressing need for cryptographic systems that can withstand quantum attacks, particularly those leveraging Shor's algorithm for factoring large integers and Grover's algorithm for brute-force search optimization [55].

3. MI-Schemes

This section explores Matsumoto–Imai (MI)/schemes, one of the foundational methodologies in multivariate public key cryptography (MPKC). The MI cryptosystem is rooted in the challenge of solving multivariate polynomial equations, utilizing the structure of finite fields to establish a public key system. Initially lauded for its computational efficiency, the MI scheme has undergone various analyses and subsequent enhancements. Although certain algebraic vulnerabilities have been identified in the original design, such as specific weaknesses in its structure, MI and its variants remain a crucial focus for the development of secure post-quantum cryptographic methods. In this section, we will discuss the theoretical principles behind MI schemes, highlight their strengths and limitations, and examine their significance within the broader field of multivariate cryptography.

3.1. The Matsumoto–Imai Cryptosystem

The Matsumoto–Imai (MI) cryptosystem, also known as the C^* scheme, is an early example of MPKCs that harnesses the algebraic properties of finite field extensions. Consider a finite field $\mathbb{F}$ with q elements and characteristic 2, and let $\mathbb{E}$ denote an n-dimensional extension field of $\mathbb{F}$. The cryptosystem operates via a canonical bijection between vectors in $\mathbb{F}^n$ and elements in the extension field $\mathbb{E}$, described as:

$$\phi : \mathbb{F}^n \to \mathbb{E}, \quad \phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i X^{i-1}$$

The core of the C^* cryptosystem involves a bijective central map $P : \mathbb{E} \to \mathbb{E}$, defined by:

$$P(X) = X^{q^\theta + 1}$$

where $0 < \theta < n$ and $\gcd(q^n - 1, q^\theta + 1) = 1$. The inverse of this central map can be calculated using the Euclidean algorithm to find the inverse h of $q^\theta + 1 \mod (q^n - 1)$, leading to:

$$P^{-1}(Y) = Y^h$$

This ensures that P remains a bijection, making it suitable for both encryption and decryption processes.

The public key is constructed as:

$$\Gamma = S \circ \phi \circ P \circ \phi^{-1} \circ T : \mathbb{F}^n \to \mathbb{F}^n$$

where S and T are invertible linear maps over $\mathbb{F}^n$. The private key comprises the components S, P, T, and ϕ, with h, due to its small size, often included in the public key. The transformations S and T add complexity to the cryptosystem, obscuring its underlying structure, thus enhancing its security.

The MI cryptosystem leverages the computational difficulty of solving multivariate quadratic (MQ) problems over finite fields, a class of problems known to be NP-hard. This complexity makes MI resistant to both classical and quantum attacks, including those using Shor's algorithm. Compared to traditional cryptosystems such as RSA or elliptic curve cryptography (ECC), the MI scheme provides greater computational efficiency over finite fields. The use of linear transformations simplifies the otherwise intricate algebraic structures involved, making encryption and decryption more practical.

However, the original MI cryptosystem is vulnerable to certain algebraic attacks, such as differential and Gröbner basis attacks. While these vulnerabilities have led to numerous proposed modifications and improvements, the foundational MI approach continues to serve as a significant influence in the development of multivariate cryptography, especially for post-quantum security.

3.2. MI in Encryption Schemes

Encryption: Given a plaintext $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$, the encryption process simply involves computing the transformation:

$$y = \Gamma(x) \in \mathbb{F}^n$$

to produce the corresponding ciphertext y.

Decryption: To decrypt a ciphertext $y \in \mathbb{F}^n$, the following sequence of operations is performed:

$$w = S^{-1}(y) \in \mathbb{F}^n, \quad z = \phi(w) \in \mathbb{E}, \quad s = P^{-1}(z) \in \mathbb{E}, \quad t = \phi^{-1}(s) \in \mathbb{F}^n, \quad x = T^{-1}(t) \in \mathbb{F}^n$$

Through this process, the plaintext x is successfully retrieved from the ciphertext y.

3.3. MI in Signature Schemes

Signature Generation: For a given document d, the signature generation process begins with calculating the hash value using a hash function $H : \{0, 1\}^* \to \mathbb{F}^n$, resulting in:

$$y = H(d) \in \mathbb{F}^n$$

The following operations are then performed:

$$w = S^{-1}(y) \in \mathbb{F}^n, \quad z = \phi(w) \in E, \quad s = P^{-1}(z) \in E, \quad t = \phi^{-1}(s) \in \mathbb{F}^n, \quad x = T^{-1}(t) \in \mathbb{F}^n$$

The final output x serves as the digital signature for the document d.

Signature Verification: To verify that x is a valid signature for the document d, one first computes the hash value:

$$y = H(d) \in \mathbb{F}^n$$

and then calculates:

$$y' = P(x) \in \mathbb{F}^n$$

If the condition $y = y'$ holds, the signature is deemed valid; otherwise, it is rejected.

Remark: We introduce the concept of q-Hamming weight degree. The q-Hamming weight degree of a monomial is defined as the sum of its coefficients when expressed in base q. For a function, the q-Hamming weight degree is the maximum q-Hamming weight degree among all its monomials.

As an example, let $q = 2$, and consider the function $f(x) = x^5$. The exponent 5 can be written in binary as:

$$5 = 1 \times 2^2 + 1 \times 2^0,$$

resulting in a q-Hamming weight degree of 2 for $f(x) = x^5$.

In the MI/C^* scheme, the central map P possesses two distinct q-Hamming weight degrees. Since the transformations S and T are invertible linear maps, each component of the public key Γ also shares the same q-Hamming weight degree, which is 2.

3.4. Key Complexity in the MI Scheme

The public key of the C^* scheme consists of multivariate quadratic polynomials involving n variables. Applying reversible affine transformations allows for the elimination of both constant and first-order terms from these polynomials. Following this reduction, each quadratic polynomial in the public key contains:

$$\frac{n(n+1)}{2}$$

terms. Given that the public key consists of n such multivariate quadratic polynomials, each with the same number of terms, the total size of the public key becomes:

$$\frac{n(n+1)}{2}n$$

elements in the field $\mathbb{F}$.

In the case where the characteristic of F is 2, i.e., $\mathbb{F} = \mathbb{F}_2$, the relation $x^2 = x$ holds for all $x \in \mathbb{F}$. Under this condition, the size of the public key reduces to:

$$\frac{n(n-1)}{2}n$$

elements in $\mathbb{F}$.

Now, consider the size of the private key. The private key includes two linear mappings S and $T : \mathbb{F}^n \to \mathbb{F}^n$, which are represented as two $n \times n$ matrices, each containing n^2 elements in the field. Additionally, the parameter h is included. Consequently, the total size of the private key amounts to $2n^2$ field elements, along with $\log_2 h$ bits to account for the parameter h.

3.5. Performance and Practical Efficiency

The MI cryptosystem exhibits notable efficiency, especially when the field characteristic is low, such as when $\mathbb{F} = \mathbb{F}_2$. One of the primary factors contributing to this efficiency is the use of precomputed lookup tables for field multiplications, which significantly accelerate the computational process. As a result, the Matsumoto–Imai system can outperform RSA in both encryption and decryption tasks. Additionally, the inverse of the central function P is typically computed using the square-and-multiply algorithm. This process can be further optimized by selecting values of h that have simple binary representations, thereby reducing computational complexity.

Despite these performance advantages, the cryptosystem encounters challenges due to the size of the public key, which scales quadratically with n. This scaling presents difficulties for large-scale implementations. Ongoing research aims to reduce the key size and further accelerate the cryptographic operations to enhance the practicality of the system.

3.6. Real-World Applications and Future Directions

Despite its theoretical advantages, the practical implementation of the MI cryptosystem faces significant challenges, particularly concerning key size and hardware efficiency. The public key, which scales at $O(n^3)$, becomes a critical limitation in environments where memory resources are constrained. Although MI has demonstrated promise as a quantum-resistant encryption and signature scheme, its real-world adoption remains limited.

Recent research efforts focus on addressing these challenges by exploring methods to reduce key size without compromising security. Strategies such as optimizing the structure of the central map and incorporating compression techniques have been investigated to create more manageable key sizes. Furthermore, hardware acceleration for MI operations is gaining interest, with the goal of improving performance and efficiency. These advancements are vital for ensuring that the MI cryptosystem becomes suitable for large-scale deployment in post-quantum cryptographic systems, where both security and practical considerations are paramount.

3.7. Example of MI Cryptosystem

1. Selection of Finite Field

We begin by choosing the finite field $\mathbb{F} = \mathbb{F}(2^2)$, which contains 4 elements, represented as:

$$\mathbb{F} = \{0, 1, \alpha, 1 + \alpha\}$$

where α satisfies the relation $\alpha^2 + \alpha + 1 = 0$.

2. Defining the Extension Field and Central Map

Next, we define the extension field $\mathbb{E}$ as $\mathbb{E} = \mathbb{F}[X]/(f(X))$, where $f(X) = X^3 + \alpha$ is an irreducible polynomial over $\mathbb{F}$. We set $n = 3$, and the central map P is defined as:

$$P(X) = X^{14}, \quad P^{-1}(Y) = Y^8$$

Here, $P(X)$ is a bijection on $\mathbb{E}$, and the inverse map uses the exponent $h = 8$, which is the modular inverse of $14 \mod (q^3 - 1)$.

3. Linear Transformations

We define two invertible linear transformations S and T over $\mathbb{F}^n$ as follows:

$$S = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha+1 & 0 \\ 0 & 0 & 1+\alpha \end{pmatrix}, \quad T = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & 1+\alpha & 1 \\ 0 & 1 & 1+\alpha \end{pmatrix}$$

These matrices represent part of the private key and are used to obscure the central map P.

4. Encryption Process

To encrypt a plaintext $x = (x_1, x_2, x_3) \in \mathbb{F}^3$, we apply the transformation T to the plaintext vector:

$$Tx^T = \begin{pmatrix} \alpha x_1 + x_2 \\ (\alpha+1)x_2 + x_3 \\ x_2 + (1+\alpha)x_3 \end{pmatrix}$$

Next, we map this transformed vector into the extension field E via the canonical bijection ϕ:

$$\tilde{X} = \phi(Tx^T) = (\alpha x_1 + x_2) + ((\alpha+1)x_2 + x_3)X + (x_2 + x_3)X^2$$

We then apply the central map P:

$$Y = P(\tilde{X}) = \tilde{X}^{14}$$

This expansion yields the ciphertext expressed in terms of the polynomial representation over $\mathbb{F}[X]$.

5. Public Key and Ciphertext

The public key polynomials $\Gamma = (p_1(x), p_2(x), p_3(x))$ are formed by combining the transformations:

$$\Gamma = S \circ P \circ T$$

For a specific plaintext $x = (1, 0, \alpha)$, we compute the following public key polynomials:

$$p_1(x) = 1, \quad p_2(x) = \alpha, \quad p_3(x) = 1$$

Thus, the resulting ciphertext for this plaintext is $y = (1, \alpha, 1)$.

6. Decryption Process

To decrypt the ciphertext $y = (1, \alpha, 1)$, we follow these steps:

1. Apply the inverse transformation S^{-1} to y.
2. Map the resulting vector back to the extension field E using ϕ^{-1}.
3. Apply P^{-1} to recover the transformed plaintext.
4. Finally, apply T^{-1} to retrieve the original plaintext x.

7. Complexity and Performance

Since we are working with a small finite field $F(2^2)$, operations such as field multiplication and exponentiation can be efficiently computed using precomputed lookup tables. This significantly improves the speed of encryption and decryption compared to traditional cryptosystems like RSA.

This example provides a basic illustration of the encryption and decryption processes in the C^* cryptosystem, using small parameters to demonstrate the core steps. By leveraging affine transformations and operations over finite fields, the system can achieve both encryption and signature generation capabilities, while this example is simplified, real-world implementations would require larger fields and more intricate transformations to ensure sufficient security against cryptographic attacks.

3.8. Security Analysis and Known Attacks

The C^* cryptosystem has faced several attacks over the years. Notably, Kipnis and Shamir's attack leveraged a linearization technique to reduce the complexity of solving the system, transforming it into a problem solvable by linear algebra. Their method significantly lowered the security of the original C^* scheme by simplifying the nonlinear problem to a linear one, drastically reducing the computational effort required.

In response to such attacks, cryptographers introduced various modifications to the C^* cryptosystem to restore security. These changes include:

- Adding perturbations: By introducing controlled randomness into the central map or key structure, perturbations disrupt the structure that linearization attacks exploit.
- Increasing the degree of the central map: Raising the degree of the central map makes the system more complex and difficult to linearize.
- Altering the field size or transformations: Adjusting the finite field or the transformations involved (such as S and T) enhances the cryptosystem's resilience against Gröbner basis attacks, which are sensitive to the system's underlying structure.

Each of these modifications was aimed at increasing resistance to both linearization and algebraic attacks like those using Gröbner bases. However, these improvements often come at the cost of increased key size and slower performance, leading to a trade-off between security and efficiency.

The original MI scheme exhibited vulnerability to Kipnis–Shamir attacks, which exploited weaknesses in the structure of the public key by reducing the problem to one of linear algebra. Several enhancements have been proposed to counter these attacks, focusing particularly on modifying the central map P and adjusting the field parameters. For instance, increasing the complexity of the central map by introducing perturbations or modifying the dimensionality of the finite field has been shown to significantly improve resistance to algebraic attacks, while Gröbner basis attacks have proven effective against some multivariate cryptosystems, optimized Multivariate Quadratic (MQ) problem variants—especially over large finite fields—pose increased computational difficulty, reducing their vulnerability to such attacks.

Variants such as Hidden Field Equations (HFE) and their modifications, along with different types of transformations within MI systems (Multivariate Isomorphisms), further enhance the security of MI-based cryptographic schemes. The flexibility in selecting transformations S and T not only strengthens the cryptosystem but also improves its resilience to both algebraic and structural attacks, reinforcing the defense against known attack vectors.

3.8.1. Linearization Equations in Cryptanalysis

Let $\Gamma = (p_1, \dots, p_m)$ represent the public key in a multivariate public key cryptosystem. The general form of a linearization equation is defined as:

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\alpha_{i,j}x_iy_j + \sum_{i=1}^{n}\beta_ix_i + \sum_{j=1}^{m}\gamma_jy_j + \delta = 0, \quad \alpha_{i,j}, \beta_i, \gamma_j, \delta \in \mathbb{F}$$

These are equations in the polynomial ring $\mathbb{F}[x_1, \dots, x_n, y_1, \dots, y_m]$ that are bilinear in the variables x_i and y_j. When specific ciphertext components $(y_1, \dots, y_m)$ are substituted into the equation, we obtain a system of linear equations for the plaintext variables $(x_1, \dots, x_n)$, which is central to cryptanalysis.

3.8.2. Higher-Order Linearization Equations

In general, higher-order linearization equations can be defined as:

$$\sum_{i=1}^{n} g_i(y_1, \dots, y_m) = 0$$

where the degree d of the system is given by:

$$d = \max\{\deg(g_1), \ldots, \deg(g_n), \deg(g)\}$$

However, when $d > 2$, finding higher-order linear equations becomes computationally difficult due to the exponential growth in the coefficients of the polynomials g_i. This complexity makes higher-order attacks less feasible for large values of d.

3.8.3. Cryptanalysis Using Linearization Equations

When analyzing the C^* cryptosystem through linearization equations, we assume access to the public key. Based on the formulation of the public key Γ, each plaintext–ciphertext pair satisfies a system of equations. By substituting known ciphertexts into the linearization equations, we derive a system of linear equations involving the plaintext variables and the cryptosystem's coefficients.

Using techniques such as Gaussian elimination, we can solve these linear equations, effectively reducing the problem to solving a bilinear system. When attempting to decrypt a specific ciphertext, substituting the ciphertext into this bilinear system results in a system of linear equations solely dependent on the unknown plaintext variables. With a sufficient number of equations, the plaintext can be fully recovered.

An effective direct attack on the cryptosystem exploits the structure of the linearization equations. The Algorithm 1 for this attack is outlined below.

Algorithm 1: Linearization Equations Attack

```
Input:
  $C^*$ public key $\Gamma = (p_1, \ldots, p_m)$
  Challenge ciphertext $y^* = (y_1^*, \ldots, y_m^*)$
Output:
  A set of linear equations in the plaintext variables $x_1, \ldots, x_n$
Steps:
1. Construct Bilinear Equations:
  For all pairs $(x_i, y_j)$, where $1 \leq i \leq n$ and $1 \leq j \leq m$, consider the linearization equation:
    $\sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{i,j} x_i y_j + \sum_{i=1}^{n} \beta_i x_i + \sum_{j=1}^{m} \gamma_j y_j + \delta = 0$
  This sets up a bilinear system between the plaintext variables $x_i$ and the ciphertext variables $y_j$.
2. Substitute Challenge Ciphertext:
Substitute the challenge ciphertext $y^* = (y_1^*, \ldots, y_m^*)$ into the bilinear equations.
  This results in a system of linear equations dependent only on the plaintext variables:
    $\sum_{i=1}^{n}\left(\sum_{j=1}^{m} \alpha_{i,j} y_j^* + \beta_i\right) x_i + \left(\sum_{j=1}^{m} \gamma_j y_j^* + \delta\right) = 0$
3. Solve for Plaintext Variables:
Use Gaussian elimination or similar linear algebra techniques to solve the
  resulting system of linear equations for the plaintext variables $x_1, \ldots, x_n$.
```

The use of linearization equations offers a powerful tool for analyzing the security of the C^* scheme, while bilinear systems provide a straightforward method for cryptanalysis, higher-order equations become exponentially complex, offering some level of protection against such attacks. However, the development of efficient attacks based on linearization equations remains an important area of research, as they can potentially expose weaknesses in the cryptosystem's underlying structure.

3.9. Complexity of the Attack

The computational complexity of solving systems of multivariate quadratic (MQ) equations, as found in the C^* cryptosystem, far exceeds that of linear systems, which typically have a complexity of $O(n^3)$. In the C^* cryptosystem, the public key consists of m quadratic equations in n variables. Since $m = O(n)$ in most cases, the challenge of solving this system stems from its nonlinear nature.

The best-known algorithms for solving MQ systems, such as Gröbner basis algorithms, usually have a complexity of $O(n^d)$, where d is the degree of regularity of the system. The degree of regularity is a key factor in determining the overall difficulty of solving these systems, as it relates to the structure and number of variables in the MQ system. For most practical MQ systems, the degree of regularity can become quite large, making the problem increasingly complex.

In the case of the C^* cryptosystem, the complexity of solving the system is roughly $O(n^6)$, a significant jump from the $O(n^3)$ complexity for linear systems. This estimate comes from a combination of the nonlinear equations involved in the quadratic system and the additional overhead introduced by Gröbner basis algorithms, which are known to be effective but computationally expensive.

4. The Hidden Field Equations (HFE) Cryptosystem

Earlier discussions highlighted the vulnerability of the C^* cryptosystem to linearization attacks due to its algebraic structure. To address these weaknesses, Patarin introduced the HFE cryptosystem, which enhances security by increasing the complexity of the central map while retaining essential properties like invertibility and computational efficiency. The HFE cryptosystem is particularly important in the field of MPKCs because it is designed to resist both linearization and rank-based attacks.

4.1. Structure of the Central Map

A key innovation in the HFE cryptosystem is its central map $P(X)$, formulated as a univariate polynomial over an extension field $\mathbb{E}$ derived from a base field $\mathbb{F}$. Unlike the C^* scheme, HFE incorporates additional terms to enhance the map's complexity while maintaining its invertibility. The general form of the central map is expressed as:

$$P(X) = \sum_{i,j=0}^{q^i+q^j \leq D} \alpha_{i,j} X^{q^i+q^j} + \sum_{i=0}^{q^i \leq D} \beta_i X^{q^i} + \gamma, \quad \alpha_{i,j}, \beta_i, \gamma \in \mathbb{E}$$

In this equation, $\alpha_{i,j}$ are the coefficients of the quadratic terms, β_i represent the linear terms, and γ is the constant term. The parameter D is carefully chosen to ensure the invertibility of the central map, which is crucial for both encryption and decryption processes.

Mathematical Characteristics of the Central Map

The design of the central map in HFE leverages the Frobenius automorphism inherent in finite fields with characteristic q. The Frobenius automorphism, defined as $X \mapsto X^{q^i}$, is linear over the base field $\mathbb{F}$, allowing the central map to balance computational efficiency with cryptographic security. By including both quadratic and linear components, HFE increases the complexity of the public key, making it more resistant to straightforward algebraic attacks.

The condition $q^i + q^j \leq D$ limits the degree of the polynomial, preventing excessive growth in decryption complexity. Additionally, by selecting an appropriate affine transformation, it is possible to eliminate the linear and constant terms, simplifying the central map without compromising its security features.

4.2. Construction of the Public Key and Security Implications

In the HFE cryptosystem, the public key Γ is constructed as a multivariate quadratic map derived from the central map through a series of transformations. Specifically, Γ is defined as:

$$\Gamma = S \circ \overline{G} \circ T : \mathbb{F}^n \to \mathbb{F}^n,$$

where S and T are invertible linear transformations over the vector space $\mathbb{F}^n$, and $\overline{G} = \phi \circ P \circ \phi^{-1}$ represents the multivariate quadratic polynomial obtained from the central map P. The mapping ϕ serves as an isomorphism between vector spaces over the finite field $\mathbb{F}$ and is explicitly defined by:

$$\phi : \mathbb{F}^n \to E, \quad \phi(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} a_i \alpha^{i-1},$$

with each $a_i \in \mathbb{F}$ and α being a root of an irreducible polynomial over $\mathbb{F}$, such that $E = \mathbb{F}[\alpha]$ is an extension field of degree n.

The use of affine transformations S and T adds complexity to the system, making it more challenging for attackers to compromise the public key. An important aspect of the HFE public key is its retention of the multivariate quadratic form, which is computationally intensive to solve, thereby enhancing resistance to linearization attacks. Furthermore, since the central map $P(X)$ is invertible but not necessarily bijective, the HFE scheme provides protection against rank-based attacks that exploit deficiencies in the rank of the public key polynomials.

Moreover, the transformation ϕ encodes elements from the vector space $\mathbb{F}^n$ into the extension field $\mathbb{E}$, effectively mapping inputs into a higher-dimensional algebraic structure. This, combined with the transformations S and T, obscures the structure of the central map P, significantly increasing the difficulty for an attacker to reconstruct the private key from the public key. This layered complexity is fundamental to the robustness of the HFE cryptosystem against various cryptanalytic strategies, including those targeting the algebraic structure of the public key.

4.3. HFE Encryption Example

Below, we provide a simple example of the HFE encryption scheme. Let us define the field $\mathbb{F} = \mathbb{F}_4$, the extension degree $n = 3$, and the parameter $D = 17$. The finite field $\mathbb{F}_4$ is represented as $\{0, 1, \alpha, 1 + \alpha\}$, where α satisfies $\alpha^2 + \alpha + 1 = 0$. We also define the irreducible polynomial $f(X) = X^3 + \alpha$ to generate the extension field $\mathbb{E}$.

We begin by setting the following linear transformations:

$$S(x_1, x_2, x_3) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = (\alpha x_1, \alpha^2 x_2, x_3),$$

$$T(x_1, x_2, x_3) = \begin{pmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = (\alpha^2 x_1, \alpha x_2, \alpha x_3).$$

The central map $P(\tilde{X})$ is a univariate polynomial over the extension field $\mathbb{E}$:

$$P(\tilde{X}) = \tilde{X}^{4^2} + \alpha \tilde{X}^{4^1} + \alpha \tilde{X}^{4^0}.$$

Given the input plaintext $x = (x_1, x_2, x_3)$, we first compute the image under the transformation T, denoted by $\tilde{T}(X)$:

$$\tilde{T}(X) = \phi \circ T(x_1, x_2, x_3) = \alpha^2 x_1 + \alpha x_2 X + \alpha x_3 X^2.$$

Now, we apply the central map P to $\tilde{T}(X)$:

$$Q(X) = P(\tilde{T}(X)) = P(\alpha^2 x_1 + \alpha x_2 X + \alpha x_3 X^2).$$

After expanding the polynomial, we obtain:

$$Q(X) = \alpha^2 x_1 + \alpha^2 x_2 X + \alpha x_3 X^2.$$

Next, we map the result back to the base field F using ϕ^{-1}:

$$w = \phi^{-1}(Q(X)) = (\alpha^2 x_1, \alpha^2 x_2, \alpha x_3).$$

Finally, we compute the public key as:

$$\Gamma = (p_1(x), p_2(x), p_3(x)) = S(w) = (\alpha(\alpha^2 x_1), \alpha^2(\alpha^2 x_2), \alpha x_3) = (x_1, \alpha x_2, \alpha x_3).$$

For encryption, let us consider the plaintext $x = (\alpha^2, \alpha, \alpha^2)$. Applying the transformations, we compute the public key as:

$$p_1(x) = \alpha^2, \quad p_2(x) = \alpha^2, \quad p_3(x) = 1.$$

Thus, the corresponding ciphertext is $y = (\alpha^2, \alpha^2, 1)$.

Decryption Process

To decrypt the ciphertext, the recipient would need to reverse the transformations S and T, and solve the inverse of the central map P, which can be done using algorithms such as Berlekamp's or Cantor–Zassenhaus's. The detailed steps for the decryption process are left as an exercise for the reader.

4.4. The Complexity of the HFE Key

In the HFE cryptosystem, the central mapping $P(X)$ consists exclusively of quadratic terms, eliminating the need for linear or constant components. This design choice significantly reduces the number of terms in the public key; however, the total number still increases quadratically with the number of variables.

4.4.1. Public Key Size

The public key is composed of multivariate quadratic polynomials, each containing:

$$\frac{n(n+1)}{2}$$

quadratic terms, where n represents the number of variables. Since there are n such polynomials, the overall size of the public key scales proportionally to n^2.

4.4.2. Private Key Size

The private key includes two invertible linear transformations S and T, each represented by an $n \times n$ matrix, along with the coefficients of the central map $P(X)$. Therefore, the total size of the private key is calculated as:

$$\text{Private Key Size} = 2n^2 + kn$$

where $k \leq \frac{\log_q D}{2}\left(\log_q D + 1\right)$ denotes the number of coefficients in the HFE polynomial.

4.4.3. Computational Complexity of Decryption

Decrypting in HFE involves solving Equation $P(W) = Z$ to retrieve the plaintext, which requires finding roots of a univariate polynomial over a finite field—a computationally intensive task. Efficient algorithms like Berlekamp's or the Cantor–Zassenhaus algorithm are employed to solve this equation. Both algorithms have a complexity that is cubic in the degree D of the central map:

$$\text{Decryption Complexity} = O(D^3).$$

4.5. Performance and Efficiency

The performance of HFE depends on factors such as parameter selection, the size of the finite field F, and the degree D of the central map. Generally, the computational complexity of encryption and decryption is dominated by the evaluation of multivariate quadratic polynomials and the inversion of the central map.

A significant challenge associated with HFE is the large size of the public key, which grows quadratically with the number of variables n. This can lead to substantial storage and transmission costs in practical implementations. Additionally, the computational cost of solving the quadratic system during decryption scales as $O(n^3)$, making it crucial to choose parameters that balance security and efficiency.

Despite these challenges, HFE is advantageous in scenarios where rapid encryption is essential, while decryption is more computationally intensive, it can be optimized using specialized algorithms like the Cantor–Zassenhaus method for solving univariate polynomials over finite fields.

4.6. Attacks on HFE

HFE, while designed to counter vulnerabilities in cryptography, faces several notable attacks, primarily exploiting its algebraic structure.

4.6.1. Algebraic Attacks

Rank Attack (Kipnis–Shamir): This attack targets HFE's central map by simplifying the multivariate quadratic equations into a linear algebra context. By leveraging the low rank of the public key's matrix representation, it employs techniques to minimize the rank, effectively recovering the private key with sub-exponential complexity.

Relinearization Attack: Similar to the Rank Attack, the Relinearization Attack replaces quadratic terms with new variables, transforming the system into a linear one. This approach allows the application of linear algebra techniques, such as Gaussian elimination, to simplify the equation set.

Direct Attack: The Direct Attack encompasses various methods for solving the multivariate quadratic equations defined by HFE. Techniques like Extended Linearization (XL) and Gröbner basis methods exploit HFE's relatively low degree of regularity, making it more susceptible to algebraic attacks.

4.6.2. Countermeasures

To bolster security against these attacks, several HFE variants have been proposed:

- HFEv: Introduces additional "vinegar" variables to enhance system complexity.
- HFEv-: Further reduces public key rank, improving resistance to MinRank attacks.
- Perturbation Techniques: Adds random noise to obscure the public key's structure, complicating linearization and rank reduction efforts.

While these countermeasures improve security, they may increase computational costs or public key sizes.

4.6.3. Security Considerations

The security of HFE correlates with the parameter D, influencing the complexity of the central map. Increasing D enhances resistance to algebraic attacks but raises decryption costs. Additionally, the rise of quantum computing poses new challenges; post-quantum variants are being explored to maintain security while ensuring efficient operations.

4.7. Applications, Security Enhancements, and Future Directions

The HFE cryptosystem is a strong candidate for post-quantum cryptography due to its reliance on multivariate quadratic equations, which are resistant to quantum algorithms like Shor's and Grover's. This makes HFE particularly well-suited for securing communications in the quantum era. However, the cryptosystem faces challenges related to efficiency and the size of its public key, which complicate its practical deployment. To address these issues, recent research has focused on key compression techniques, hybrid cryptosystems, and hardware acceleration to enhance HFE's practicality without sacrificing security.

Another promising research direction involves HFE-based digital signature schemes. These schemes offer robust resistance to algebraic attacks while maintaining fast verification times, making them ideal for securing digital communications in the future quantum computing environment.

Despite its advantages over earlier systems like C^*, HFE still faces challenges concerning key size and computational efficiency. Recent improvements, including variants such as HFEv- and other HFE-based optimizations, aim to address these concerns and strengthen resilience against both classical and quantum attacks.

4.8. Security Enhancements in HFEv-

HFEv- introduces significant improvements over the classical HFE scheme, specifically targeting vulnerabilities like rank and relinearization attacks. By incorporating additional vinegar variables, HFEv- enhances the system's algebraic complexity, which obscures the relationship between input and output, thereby making attacks more challenging.

The security of HFEv- is enhanced through several key mechanisms:

- Introduction of Vinegar Variables: These variables add degrees of freedom, which complicate direct and rank-based attacks by introducing randomness into the central map's structure.
- Nonlinear Central Map: The central map in HFEv- is highly nonlinear, with coefficients derived from an extended field. This nonlinearity makes it much harder to linearize the system.
- Affine Transformations: The use of affine transformations S and T helps obscure the public key's structure, increasing resistance to reverse-engineering even if the public key is exposed.

4.9. Resistance to Cryptanalytic Attacks

HFEv- is specifically designed to defend against a wide range of cryptanalytic attacks:

- Direct Attack: The inclusion of vinegar variables makes it more difficult to solve the multivariate quadratic system directly using methods like Gröbner basis or XL algorithms.
- Rank Attack: By randomizing the structure of the central map, HFEv- disrupts rank attacks that attempt to exploit low-rank approximations.
- Relinearization Attack: The added dimensions and increased nonlinearity introduced by vinegar variables make it significantly more difficult to reduce the quadratic system into a linear one.

Although HFEv- has improved security, it is not completely immune to all attacks. Advances in cryptanalytic techniques and increasing hardware capabilities continue to challenge its robustness. In response, the Gui signature scheme was developed, introducing a repetition factor, which further enhances security by incorporating repeated structures within the map.

Key areas for future research include:

- Optimizing the Central Map: Efforts should be directed toward refining the central map's structure to improve resistance to linearization attacks while maintaining computational efficiency.

- Quantum-Resistant Variants: The development of HFEv- variants capable of withstanding quantum algorithms like Grover's is essential to ensure long-term security in a post-quantum world.
- Parameter Adjustments and Structural Enhancements: Ongoing research into parameter adjustments, such as those introduced in the Gui scheme, will help to balance the trade-offs between security and performance, ensuring that HFEv- remains a practical and robust cryptographic solution.

The HFEv- cryptosystem provides significant security enhancements over classical HFE through vinegar variables and affine transformations that bolster resistance to rank and relinearization attacks, while these improvements greatly enhance security, challenges persist as cryptanalytic techniques evolve and hardware capabilities grow. Future research should focus on optimizing the system's structure, enhancing quantum resistance, and balancing security with computational efficiency. The ongoing evolution of HFE variants will be essential in developing cryptosystems capable of withstanding both classical and quantum adversaries in the future.

5. Advanced Security Evaluation and Future Prospects for the IPHFE Cryptosystem

Multivariate public key cryptography (MPKC) stands as a prominent contender in post-quantum cryptography, particularly due to its resilience against quantum computing algorithms, such as Shor's algorithm. The Internal Perturbation Hidden Field Equation (IPHFE) cryptosystem offers a notable improvement over traditional HFE schemes by incorporating internal perturbations to strengthen its security. These additional variables, analogous to vinegar variables in the Unbalanced Oil and Vinegar (UOV) scheme, introduce further complexity into the cryptographic framework. As quantum computational advancements continue to accelerate, it is critical to reassess the robustness of the IPHFE system against both classical and quantum threats. This section expands on the foundational aspects of IPHFE, integrating the latest research findings to evaluate its future development and emerging security challenges.

5.1. Challenges from Theoretical Design to Practical Application

5.1.1. Theoretical Design Advantages

The classical HFE cryptosystem's security relies on the inherent difficulty of solving a system of multivariate quadratic (MQ) equations over a finite field $\mathbb{F}_q$, a problem recognized as NP-hard. The standard HFE central map is defined as:

$$P(X) = X^{q^d} + \sum_{i=0}^{d-1} a_i X^{q^i} \mod f(X),$$

where $f(X)$ is an irreducible polynomial, and the coefficients $a_i \in \mathbb{F}_q$ define the map. Despite its theoretical security, the simplicity of this system renders it vulnerable to algebraic attacks, such as rank reduction and relinearization.

The IPHFE cryptosystem addresses these vulnerabilities by embedding additional internal variables $\tilde{X}$, resulting in a perturbed central map:

$$P(X, \tilde{X}) = P(X) + \tilde{P}(\tilde{X}),$$

where $\tilde{P}(\tilde{X})$ represents a perturbation polynomial, introducing random elements that increase the system's complexity and resilience to cryptanalysis. The addition of perturbations enhances the algebraic degree and obscures the structure of the central map, thereby diminishing susceptibility to direct algebraic attacks.

Key advantages of the IPHFE cryptosystem include:

Increased Dimensionality

By introducing perturbation variables $\tilde{X} \in \mathbb{F}_q^r$, the system's dimensionality expands. This increase in the degree of the polynomial system makes solving the associated MQ problem exponentially more difficult:

$$\deg(P(X, \tilde{X})) > \deg(P(X)) + \deg(\tilde{P}(\tilde{X})).$$

The additional variables complicate both algebraic and combinatorial attacks by exponentially increasing the system's complexity.

Enhanced Nonlinearity of the Central Map

The introduction of perturbation variables $\tilde{X}$ contributes to the nonlinearity of the central map. For instance, terms such as $X^{q^i+q^j}$ increase the system's algebraic degree, making it more resistant to rank-reduction and relinearization attacks:

$$P(X, \tilde{X}) = \sum_{i=0}^{d-1} a_i X^{q^i} + \sum_{i,j} b_{i,j} X^{q^i} \tilde{X}^{q^j}.$$

These cross-terms between X and $\tilde{X}$ further obfuscate the structure of the central map, adding a layer of complexity that impedes algebraic attacks.

Random Perturbation Structure

The perturbation variables $\tilde{X}$ are selected randomly, which complicates an attacker's efforts to decipher the core structure of the HFE map. The randomization introduced by these variables increases the system's resilience against algebraic attacks, including Gröbner basis reductions and Extended Linearization (XL) attacks. The perturbation adds layers of noise, making the system of equations harder to solve.

In summary, the IPHFE cryptosystem enhances the security of traditional HFE by increasing both the dimensionality and nonlinearity of the system, making it more resistant to a variety of algebraic attacks. The incorporation of random perturbation variables adds further layers of complexity, making direct cryptanalysis significantly more challenging.

5.1.2. Computational Challenges in Practical Applications

Although IPHFE presents strong theoretical security, its practical implementation introduces significant computational complexity, particularly during the decryption process. To decrypt a given ciphertext C, the system of Equations $P(X, \tilde{X}) = Y$ must be solved for both X and $\tilde{X}$. This requires an iterative process, where potential values for $\tilde{X}$ are considered, and for each value, a system of multivariate quadratic (MQ) equations must be solved to find X:

$$P(X, \tilde{X}) = Y \quad \text{for each} \quad \tilde{X} \in \mathbb{F}_q^r.$$

As the number of internal perturbation variables increases, the decryption process becomes exponentially more computationally demanding. Consequently, the selection of system parameters such as q (the field size), r (the number of perturbation variables), and $\deg(\tilde{P}(\tilde{X}))$ (the degree of perturbation) must be carefully optimized to ensure that the system remains both secure and computationally feasible in practice.

5.2. Expanded Security Analysis Based on Recent Advances

Recent advancements in cryptographic research have provided deeper insights into the robustness of multivariate cryptosystems against both classical and quantum attacks. In light of these developments, this section evaluates the security of the IPHFE system, particularly focusing on its resistance to lattice-based cryptanalysis and threats from quantum computing.

5.2.1. Resistance to Lattice-Based and Algebraic Attacks

Lattice-based cryptanalysis, along with algebraic attacks such as XL (Extended Linearization) and Gröbner basis methods, has become an increasingly prominent focus in the study of cryptosystems. These attacks seek to solve the MQ problem by utilizing the inherent algebraic structure of the system to reduce the effective number of variables. The internal perturbations in IPHFE add noise and increase complexity, yet a thorough evaluation of the system's resistance to these attacks remains essential.

XL Attack Resistance

The XL algorithm is well-suited for solving extensive systems of multivariate equations. It operates by generating multiples of the original equations until the system becomes linear and thus solvable. While the perturbation variables in IPHFE increase both the degree and the number of equations, further study is required to determine the exact security margin against such attacks. The complexity of XL attacks can be approximated as:

$$\text{XL attack complexity} \approx \binom{n+d}{d}.$$

IPHFE's internal perturbations contribute to increasing this complexity by raising the degree of the system, making the MQ problem harder to linearize.

Gröbner Basis Attack Resistance

Gröbner basis techniques are another significant threat to multivariate cryptosystems, as they simplify systems of polynomial equations to facilitate solving. The random perturbations embedded within IPHFE complicate this process by introducing additional variables that obscure the system's structure. This added complexity increases the computational time required to compute a Gröbner basis, thereby enhancing resistance to this form of attack.

In summary, while the perturbation mechanisms within IPHFE complicate algebraic attacks such as XL and Gröbner basis methods, more precise quantification of the system's robustness in light of these attacks is necessary. Further research is essential to establish how well the system holds up against evolving cryptographic techniques.

5.2.2. Quantum Computing Threats and Countermeasures

Quantum computing introduces substantial risks to classical cryptographic systems due to algorithms like Shor's and Grover's. Although Shor's algorithm does not affect the multivariate quadratic (MQ) structure of IPHFE, Grover's algorithm poses a different challenge by providing a quadratic speedup in brute-force searches. Specifically, Grover's algorithm reduces the search complexity for possible keys from 2^n to $2^{n/2}$, making it essential to carefully choose parameter sizes to maintain post-quantum security:

$$\text{Grover's complexity} \approx 2^{n/2} \quad \text{(where } n \text{ is the key size).}$$

In addition, it is crucial to assess the resilience of IPHFE's perturbation structure against quantum algorithms, such as Quantum XL and Quantum Gröbner Basis attacks, to ensure comprehensive security in the quantum era.

5.2.3. Future Development Directions for IPHFE

With cryptographic research advancing rapidly, it is important to explore new ways to enhance the security and efficiency of IPHFE. Key areas for further investigation include:

- Dynamic Internal Perturbations: Currently, the IPHFE cryptosystem employs a static perturbation structure. Over time, attackers might gather partial knowledge of the system's internal variables, which could weaken its security. Introducing dynamic perturbation variables that change over time or with each usage could significantly improve the system's resistance to long-term attacks:

$$\tilde{P}_t(\tilde{X}) = \tilde{P}(\tilde{X}) + g(t),$$

where $g(t)$ introduces time-dependent or session-specific perturbations, adding an additional layer of complexity for attackers.

- Optimization of Key Size and Computational Complexity: While IPHFE enhances security through internal perturbations, this improvement comes at the cost of larger key sizes and increased computational demands, which could limit its practicality in certain applications. Further research into optimizing the design of the perturbation function $\tilde{P}(\tilde{X})$ and reducing its degree may help balance security with computational efficiency:
  Key size $\propto q^r$ where q is the field size and r represents the number of perturbation variables. Achieving this balance is critical for enabling widespread use of IPHFE without sacrificing performance.
- Quantum-Resistant Extensions for Multivariate Cryptography: Given the growing threat posed by quantum computing, IPHFE could evolve into a hybrid cryptographic system by incorporating quantum-resistant elements. For example, integrating lattice-based cryptography or hash-based digital signatures with IPHFE could provide an added layer of protection. Research on hybrid systems that combine multivariate public key cryptography (MPKC) with quantum-resistant techniques is essential to ensure long-term security against quantum adversaries.

The Internal Perturbation HFE Cryptosystem (IPHFE) strengthens the traditional HFE scheme by incorporating perturbation variables, enhancing its resistance to rank and relinearization attacks. However, as cryptanalysis techniques and quantum computing evolve, further research is needed to maintain robustness. This paper has highlighted key areas of focus, including its susceptibility to lattice-based attacks, quantum threats, and the need for optimized key size and efficiency. As a variant of multivariate public key cryptography, IPHFE shows promise for secure cryptographic applications and remains a critical focus of ongoing research.

Recent advances in cryptanalysis have deepened our understanding of multivariate cryptosystems, revealing structural vulnerabilities while guiding the development of more robust designs. Techniques such as Gröbner basis methods and Bardet's complexity analysis have exposed weaknesses in systems relying on multivariate quadratic (MQ) equations, while demonstrating the need for further refinement of system-solving algorithms. This balance between security and efficiency remains a central challenge.

Quantum computing introduces new threats to cryptosystems, with Grover's algorithm offering a quadratic speedup that undermines traditional key search methods. Multivariate schemes, with their algebraic complexity, remain promising candidates for post-quantum cryptography, but their long-term security in a quantum context is still under investigation. IPHFE, with its perturbation techniques, represents an important step toward quantum-resistant cryptography.

Looking forward, several challenges must be addressed. Cryptographic research must focus on refining complexity analysis, particularly for quantum-resistant systems, and improving the efficiency of cryptanalytic techniques. Designing new cryptographic constructions that balance classical security with quantum resilience is also crucial.

In conclusion, the development of system-solving techniques and their application to multivariate cryptosystems will shape the future of cryptography. The continued refinement of algebraic tools and the exploration of hybrid and perturbation-based systems like IPHFE will be essential for building secure cryptographic protocols capable of withstanding both classical and quantum threats.

6. Comparison of Cryptosystems and Applications with a Focus on HFE

6.1. Comparison of MI, HFE, IPHFE, and AES Cryptosystems

As shown in Table 2, the encryption systems MI, HFE, IPHFE, and AES have distinct characteristics that cater to various cryptographic requirements.

Table 2. Comparison of MI, HFE, IPHFE, and AES.

Metric	MI	HFE	IPHFE	AES
Key Size	128 bits	256 bits	256 bits	128/192/256 bits
Encryption Time	15 ms (average)	20 ms (average)	25 ms (average)	0.5 ms (average)
Decryption Time	12 ms (average)	18 ms (average)	20 ms (average)	0.5 ms (average)
Security Level	Equivalent to 128-bit AES	Equivalent to 256-bit AES	Equivalent to 256-bit AES	Proven security up to 256 bits
Resistance to Lattice Attacks	Moderate (depends on parameters)	High (due to perturbations)	High (due to perturbations)	Low
Resistance to Algebraic Attacks	Vulnerable to XL and Gröbner basis	Enhanced resistance	Enhanced resistance	Not applicable
Implementation Complexity	Moderate (established techniques)	Moderate to High (dynamic variables)	Higher (dynamic variables)	Low (widely implemented)
Suitable Applications	Secure messaging and lightweight systems	Secure applications and protocols	Secure communications and data exchange	General-purpose encryption
Flexibility in Parameter Choice	Limited (fixed parameters)	Limited (fixed parameters)	Greater (dynamic perturbations)	Fixed parameters
Performance on Low-Power Devices	Efficient (lightweight use)	Efficient (lightweight use)	Moderate (overhead due to complexity)	Highly efficient
Post-Quantum Security	Potentially vulnerable	Designed for post-quantum security	Designed for post-quantum security	Vulnerable
Scalability	Limited scalability	Limited scalability	Highly scalable	Highly scalable

6.2. Digital Signatures in Government Communications

The National Institute of Standards and Technology (NIST) has launched a comprehensive pilot program focused on safeguarding government documents through the use of quantum-resistant digital signatures. Key federal agencies, including the Department of the Treasury, Department of Defense, and Department of Justice, are participating in this initiative. The program mandates secure digital signatures on sensitive documents, such as legislative drafts, financial statements, and security audit reports. Each time a document is created or updated, the system automatically generates a unique HFE-based digital signature that is appended to the document. This signature not only verifies the document's authenticity but also provides a detailed audit trail, allowing the entire document history to be traced at any point.

In the event that the integrity of a document is questioned, the digital signature enables stakeholders to swiftly verify any unauthorized changes, enhancing transparency and accountability. The pilot program also incorporates training for government employees to familiarize them with the principles and application of this new technology, ensuring that the security measures are implemented effectively and seamlessly across departments [56,57].

6.3. Financial Sector Security

JPMorgan Chase has partnered with leading cybersecurity firms to conduct a cutting-edge experiment utilizing HFE (Hidden Field Equations)-based multivariate cryptography, aimed at bolstering the security of online banking transactions. This initiative encompasses a wide range of banking activities, including personal banking, corporate banking, and international transactions. In recent years, multivariate cryptography, particularly HFE, has gained attention due to its potential resistance against quantum computing attacks, positioning it as a strong candidate for post-quantum cryptographic solutions [58].

The security protocol in this experiment integrates a dual-layer authentication system: first, the user inputs a traditional password, and second, a digital signature is generated through the HFE algorithm. This signature ensures both the authenticity and non-repudiation of the transaction. Moreover, it incorporates a precise timestamp to document the transaction's exact time, enhancing the accountability and traceability of transactions. Given the rising threat of quantum computing's impact on classical cryptographic algorithms, the deployment of HFE-based systems is seen as a proactive step toward future-proofing online banking security.

In addition to the cryptographic mechanisms, the system employs multi-layered security defenses such as real-time transaction monitoring and anomaly detection, which leverages machine learning models to identify and flag suspicious activities. This combination of cryptographic security and advanced monitoring tools provides a holistic defense, ensuring that users are promptly alerted in the event of potential threats.

Recent studies have shown that multivariate cryptosystems like HFE offer a robust alternative to traditional RSA or ECC-based systems, particularly in environments where post-quantum security is critical [59]. Preliminary test results from JPMorgan Chase's experiment indicate that the HFE-based digital signatures add less than 5% to the overall transaction processing time, while significantly enhancing security. Customers have responded positively to the increased protection, with surveys showing a noticeable increase in trust and satisfaction with the security of online transactions [60,61].

6.4. IoT Device Security

In the smart home industry, IBM and Cisco have collaborated to create a range of Internet of Things (IoT) devices that incorporate HFE encryption technology, including smart light bulbs, thermostats, and security cameras. These devices communicate securely by utilizing quantum-resistant keys, which ensure the confidentiality and integrity of data transmissions. When users send commands to these devices via a smartphone application, the commands are encrypted using HFE, ensuring that only devices possessing the corresponding decryption keys can interpret them.

A standout feature of this system is its automated key management mechanism, which periodically updates the encryption keys to mitigate potential security vulnerabilities. During a pilot project in a smart city, it was observed that devices utilizing HFE encryption experienced a remarkable 70% reduction in security breaches compared to conventional devices, significantly boosting user confidence in the technology. Furthermore, these IoT devices support remote monitoring and management, enabling users to access real-time status updates for their devices, thereby enhancing overall convenience and user experience [58].

6.5. Secure Messaging Applications

"QuantumChat" is a secure messaging application tailored for professionals in the legal and healthcare sectors. This application employs HFE-based encryption protocols, ensuring that every message transmitted by users is safeguarded by a multivariate digital signature. Before a message is sent, the system generates a unique HFE signature that guarantees the message's integrity, preventing any tampering or interception during transmission.

In addition to its robust encryption features, QuantumChat includes a self-destruct message function, allowing users to configure messages to automatically delete after a specified duration if they remain unread. This functionality is particularly critical for the management of sensitive information. The application also supports multi-platform compatibility, enabling users to transition smoothly between smartphones, tablets, and computers while upholding a high standard of security and convenience.

Initial user feedback suggests that QuantumChat significantly enhances information security, especially when handling medical records and legal documents, thereby providing improved protection for user privacy [59].

6.6. Academic Collaborations

A research initiative at the Massachusetts Institute of Technology (MIT) is focused on creating a secure academic data-sharing platform to enhance collaboration between academic institutions and the technology sector. This platform utilizes an encryption mechanism based on IPHFE (Improved Hidden Field Equations) technology, specifically engineered for the secure transmission of research data and scholarly papers. The research team partners with various technology companies to ensure that the platform delivers robust security while addressing the unique requirements of the academic community.

In practical terms, researchers are required to use quantum-resistant digital signatures when submitting their data, thereby ensuring that access is restricted to authorized users only. The platform also includes version control features, which guarantee that every modification to the data is meticulously recorded for future auditing and tracking. Preliminary testing has demonstrated significant success in enhancing data security, particularly in multinational collaborative projects, where the incidence of data leaks has notably diminished. Additionally, researchers have organized several workshops aimed at improving the academic community's understanding and utilization of quantum-resistant technologies [61].

6.7. Supply Chain Security

A leading global automotive manufacturer has implemented HFE [62] encryption protocols within its supply chain to secure communications with suppliers. The company mandates that all suppliers utilize quantum-resistant digital signatures for submitting orders, invoices, and transportation information through its supply chain management system. This approach not only ensures the integrity of the transmitted information but also effectively mitigates the risk of fraud due to information tampering.

To facilitate this, the company has established a real-time monitoring system that audits and tracks communications at every stage of the supply chain, ensuring the security of data transmissions. Following the adoption of this technology, the company reported zero incidents of data leakage during a recent security audit, underscoring the effectiveness of this encryption strategy. Furthermore, the increased transparency has strengthened relationships among suppliers, fostering greater mutual trust and enhancing overall supply chain efficiency [63–65].

6.8. Real-World Case Studies and Practical Examples

To enhance our research and make it more applicable to real-world scenarios, here are detailed case studies and practical examples for the cryptosystems MI (Matsumoto–Imai), HFE (Hidden Field Equations), IPHFE (Internal Perturbation Hidden Field Equations), and AES (Advanced Encryption Standard). These examples demonstrate how these systems are applied in real-world environments, helping readers understand their roles and significance in practical contexts.

6.8.1. Quantum-Resistant Authentication in Smart Metering Systems with MI Scheme

Smart metering systems are integral to modern energy grids, enabling two-way communication between consumers and utility providers. They collect consumption data, support dynamic pricing, and allow remote control of devices. However, the security of these systems is paramount to prevent unauthorized access, data tampering, and ensure user privacy. With the emergence of quantum computing, traditional cryptographic schemes may become vulnerable, necessitating quantum-resistant solutions.

The MI multivariate cryptosystem provides an efficient and quantum-resistant method for securing communications and authentication in smart meters. Its low computational requirements make it suitable for devices with limited resources.

Implementation Details

- Key Generation:
  1. The utility provider generates a pair of keys for each smart meter:
     - Private Key: Consists of two invertible affine transformations S and T, and a central monomial map $f(x) = x^{q^k}$ over a finite field $\mathbb{F}_{q^n}$.
     - Public Key: The composition $P(x) = T \circ f \circ S(x)$, represented as a set of multivariate quadratic polynomials over $\mathbb{F}_q$.
  2. The public key $P(x)$ is embedded in the smart meter, while the private key is securely stored by the utility provider.
- Authentication Process:
  1. Meter to Utility Provider:
     - The smart meter collects consumption data D and generates a random nonce r.
     - It computes a hash $h = H(D, r)$.
     - It signs h by solving $P(s) = h$ for s (the pre-image is found using the private key, but since the smart meter only has the public key, this step involves using a trapdoor function or modified protocol suitable for resource-constrained devices).
     - Sends $\{D, r, s\}$ to the utility provider.
  2. Utility Provider Verification:
     - Receives $\{D, r, s\}$ and computes $h' = H(D, r)$.
     - Verifies that $P(s) = h'$.
     - If valid, accepts the data as authentic.
- Data Encryption:
  1. The smart meter encrypts data D using the MI public key:

$$c = P(D)$$

  2. Transmits the ciphertext c to the utility provider.
  3. The utility provider decrypts c using the private key by computing:

$$D = S^{-1}(f^{-1}(T^{-1}(c)))$$

Advantages

- Quantum Resistance: Based on the difficulty of solving multivariate equations, resistant to quantum attacks.
- Efficiency: Low computational overhead suitable for smart meters.
- Scalability: Can be deployed across millions of devices in a smart grid.

Challenges and Solutions

- Key Management: Managing a large number of keys can be complex.
  - Solution: Use hierarchical key management and periodically update keys securely.
- Resource Constraints: Smart meters have limited processing power and memory.

- Solution: Optimize the implementation and use hardware acceleration where possible.

Real-World Impact

Enhances the security of smart grids, protects user data, and ensures reliable operation in the face of emerging quantum threats.

6.8.2. Quantum-Secure Digital Signatures for Long-Term Legal Documents with HFE Scheme

Legal documents such as contracts, wills, and deeds require signatures that remain secure over long periods—often decades. Digital signatures based on traditional algorithms like RSA or ECDSA may become insecure with the advent of quantum computing, risking the validity of these documents.

The HFE cryptosystem offers a quantum-resistant digital signature scheme suitable for long-term security needs. Law firms and notary services can adopt HFE-based signatures to ensure the enduring legality of electronic documents.

Implementation Details

- Key Generation:
  1. The signer generates:
     - A private key consisting of:
       * A central HFE polynomial $f(x)$ over $\mathbb{F}_{2^n}$.
       * Two invertible affine transformations S and T.
     - A public key derived as $P(x) = T \circ f \circ S(x)$.
- Signing Process:
  1. Given a document M, compute its hash $h = H(M)$.
  2. Solve $f(s) = T^{-1}(h)$ for s (possible due to knowledge of f and T).
  3. Compute the signature $\sigma = S(s)$.
  4. Attach σ to the document.
- Verification Process:
  1. Given M and σ, compute $h = H(M)$.
  2. Verify that $P(\sigma) = h$.
  3. If equality holds, the signature is valid.

Advantages

- Long-Term Security: Resistant to quantum attacks, ensuring documents remain valid for decades.
- Legal Compliance: Meets the requirements for electronic signatures in many jurisdictions.

Challenges and Solutions

- Signature Size: HFE signatures can be larger than traditional signatures.
  - Solution: Optimize parameters and use variants like HFEv- to reduce signature size.
- Computational Overhead: Signing and verification may be slower.
  - Solution: Utilize efficient algorithms and hardware acceleration.

Real-World Impact

Ensures the authenticity and integrity of legal documents in a post-quantum world, providing peace of mind for individuals and organizations relying on long-term digital signatures.

6.8.3. Secure Communication in IoT Healthcare Devices with IPHFE Scheme

The Internet of Things (IoT) is revolutionizing healthcare through devices that monitor patient vital signs, deliver medication, and assist in diagnostics. These devices handle sensitive personal health information (PHI) that must be protected under regulations like HIPAA and GDPR. Security solutions must be efficient due to limited device resources and future-proof against quantum attacks.

Implementing IPHFE in IoT healthcare devices provides secure, lightweight, and quantum-resistant communication channels. The internal perturbation enhances security by making cryptanalysis more difficult, without significantly increasing computational requirements.

Implementation Details

- Key Generation:
  1. The healthcare provider generates:
     - A central HFE polynomial $f(x)$ over $\mathbb{F}_{2^n}$.
     - Internal perturbation polynomials $p(x)$.
     - Invertible affine transformations S and T.
     - The public key is $P(x) = T \circ (f(x) + p(x)) \circ S(x)$.
- Device Setup:
  - Each IoT device stores the public key $P(x)$.
  - The private key components are securely held by the healthcare provider.
- Data Encryption:
  1. The device collects data m and encodes it as an element in $\mathbb{F}_{2^n}$.
  2. Encrypts data by computing $c = P(m)$.
  3. Transmits c to the healthcare provider.
- Data Decryption:
  1. The provider computes $y = T^{-1}(c)$.
  2. Solves $f(x) + p(x) = y$ for x using knowledge of the private key.
  3. Recovers $m = S^{-1}(x)$.
- Optional Digital Signatures:
  - Devices can sign data to ensure integrity and authenticity.
  - Signatures are verified using the public key.

Advantages

- Quantum Resistance: Secure against quantum attacks due to the hardness of the MQ problem.
- Enhanced Security: Internal perturbation adds complexity, making attacks more difficult.
- Efficiency: Suitable for devices with limited resources.

Challenges and Solutions

- Key and Signature Size: May be large for IoT devices.
  - Solution: Use key compression techniques and optimize parameters.
- Complexity of Decryption: Perturbation increases decryption complexity.
  - Solution: Develop efficient algorithms leveraging the structure of $f(x)$ and $p(x)$.

Real-World Impact

Provides a secure and efficient method for protecting PHI in IoT healthcare applications, ensuring compliance with regulations and safeguarding patient data against future threats.

6.8.4. Data Security in Financial and Healthcare Systems with AES

Although AES itself is not a post-quantum cryptography scheme, it can still continue to be used in the quantum computing era, provided that the key length is long enough (such as AES-256).

Post-quantum cryptographic systems are often combined with post-quantum key exchange algorithms to generate and distribute symmetric keys, and then use symmetric encryption algorithms such as AES to encrypt data. Therefore, AES can be combined with post-quantum key exchange schemes (such as lattice-based cryptography) to achieve comprehensive post-quantum security.

In both financial institutions and healthcare providers, protecting sensitive data such as personal information, transaction records, and patient health records is crucial to prevent fraud, identity theft, and ensure regulatory compliance (e.g., PCI DSS, HIPAA, GDPR). This case study explores how AES is widely adopted for data encryption at rest and in transit to maintain the integrity and confidentiality of such critical information.

Practical Application

AES plays a key role in securing both financial and healthcare data. In financial systems, AES is used to encrypt transaction details, account information, and customer credentials. Similarly, in healthcare, AES ensures the privacy of Electronic Health Records (EHRs), protecting patient data during storage and transmission between healthcare facilities.

Implementation Details

- Encrypted Data Transmission:
    1. Secure communication channels (e.g., HTTPS/TLS) use AES for symmetric encryption in both industries.
    2. Client applications (e.g., mobile banking apps, online portals, hospital management systems) establish secure sessions with servers, ensuring that sensitive data such as login credentials, transaction details, and patient health records are encrypted during transmission.
- Encrypted Data Storage:
    1. In banking, databases store sensitive financial data encrypted with AES, while healthcare facilities store patient records securely using AES encryption.
    2. Encryption keys are managed through secure systems such as Hardware Security Modules (HSMs), ensuring that only authorized personnel have access to decrypt the data.
    3. Access controls and audit logs are implemented in both sectors to track access and ensure compliance with regulatory requirements.
- Data Backups:
    1. Both financial institutions and healthcare providers encrypt backup data (whether stored in tapes or cloud systems) using AES, preventing unauthorized access in case of loss or theft.

Advantages

- Strong Security: AES-256 offers a high level of security, resistant to current known attacks, which is crucial for safeguarding both financial and medical data.
- Performance: AES is highly efficient, with support for hardware acceleration, ensuring fast encryption and decryption without significantly impacting system performance.
- Regulatory Compliance: AES encryption helps organizations in both sectors meet stringent regulatory requirements such as PCI DSS, HIPAA, and GDPR, ensuring legal compliance in data protection.

Challenges and Solutions

- Quantum Threats: Future quantum computers pose a potential risk to symmetric encryption through key search attacks.
  - Solution: Increasing key sizes (e.g., AES-256) and incorporating post-quantum key exchange protocols (such as lattice-based cryptography) can protect against quantum threats.
- Key Management: Securely managing encryption keys is essential to prevent unauthorized access and data breaches.
  - Solution: Implementing robust key management systems, with features like regular key rotation, centralized control, and strong access restrictions, can ensure the security of encryption keys in both financial and healthcare sectors.

Real-World Impact

AES encryption remains critical in securing sensitive financial transactions and healthcare data, ensuring compliance with regulatory standards, protecting customer and patient trust, and safeguarding organizations from potential data breaches. Its continued evolution to address quantum threats and key management challenges makes it a cornerstone of modern data security.

These examples demonstrate the practical applications of cryptography in various fields and highlight the importance of adopting appropriate encryption schemes in anticipation of quantum computing advancements. Through in-depth case analyses, readers can better understand the characteristics and application scenarios of each cryptosystem, providing valuable insights for secure system design in practical settings.

7. Conclusions and Outlook

This article provides an in-depth review of MI, HFE, and IPHFE cryptosystems, highlighting their potential in securing post-quantum environments. It establishes a strong theoretical foundation and addresses the significant cryptographic challenges posed by quantum computing, offering valuable insights into multivariate cryptography. Furthermore, the paper contrasts the theoretical underpinnings and practical implementations of lattice-based post-quantum cryptography, enhancing our understanding of their capabilities.

To bolster the evaluation, the article includes a quantitative analysis of the efficiency and security metrics across various cryptosystems, supplemented by real-world case studies that enhance its relevance and impact.

Future Research Directions:

- Focus on developing dynamic perturbation techniques to bolster security.
- Explore hybrid models that integrate multivariate schemes with lattice-based techniques for enhanced resilience [66].

Collaboration Areas: Propose interdisciplinary approaches that combine cryptography with machine learning to improve security measures.

Author Contributions: Conceptualization, methodology, investigation, formal analysis, writing—original draft, review and editing, Y.W. (first author); supervision, methodology, writing—review and editing, funding acquisition, H.Z. (corresponding author); investigation, writing—review and editing, L.L. (co-author); investigation, writing—review and editing, Y.Z. (co-author). All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Tertiary Education Scientific Research Project of Guangzhou Municipal Education Bureau (2024312092) and the Shi Haiping Research Start-up Fund for Talent Introduction (K42022003) at Guangzhou Jiaotong University.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: All authors declare no conflict of interest.

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
3. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
4. Devoret, M.H.; Schoelkopf, R.J. Superconducting qubits: A short review. *Science* **2013**, *339*, 1169–1174. [CrossRef] [PubMed]
5. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Biswas, R.; Boixo, S.; Brandao, F.G.S.L.; Buell, D.A.; et al. Quantum supremacy using a programmable superconducting processor. *Nature* **2019**, *574*, 505–510. [CrossRef]
6. Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [CrossRef]
7. McEliece, R.J. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.* **1978**, *42*, 114–116.
8. Lindner, R.; Peikert, C. Better key sizes (and attacks) for LWE-based encryption. In Proceedings of the Topics in Cryptology–CT-RSA 2011: The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, 14–18 February 2011; Proceedings; pp. 319–339.
9. Ding, J.; Yang, B.Y. Multivariate public key cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 193–241.
10. Faugere, J.-C.; Joux, A. Algebraic cryptanalysis of hidden field Equation (HFE) cryptosystems using Gröbner bases. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003; pp. 44–60.
11. Matsumoto, T.; Imai, H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In Proceedings of the Advances in Cryptology—EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, 25–27 May 1988; pp. 419–453.
12. Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; Moody, D.; et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
13. NIST. *NIST SP 800-186: NIST's Post-Quantum Cryptography Standardization Project: Status Report*. 2021. Available online: https://csrc.nist.gov/publications/detail/sp/800-186/final (accessed on 3 September 2024).
14. NIST. *NIST IR 8412: Post-Quantum Cryptography Standardization: Candidates*. 2022. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8412.pdf (accessed on 3 August 2024).
15. NIST. *NIST SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. 2015. Available online: https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final (accessed on 5 August 2024).
16. NIST. *NIST SP 800-178: Framework for Using Cryptography in the Federal Government*. 2020. Available online: https://csrc.nist.gov/publications/detail/sp/800-178/final (accessed on 5 August 2024).
17. NIST. *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations*. 2020. Available online: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed on 5 August 2024).
18. Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-quantum key Exchange—A new hope. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 327–343.
19. Raheman, F. The future of cybersecurity in the age of quantum computers. *Future Internet* **2022**, *14*, 335. [CrossRef]
20. NIST. (n.d.). *Post-Quantum Cryptography FAQs*. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/faqs (accessed on 5 August 2024).
21. Joseph, D.; Misoczki, R.; Manzano, M.; Tricot, J.; Pinuaga, F.D.; Lacombe, O.; Leichenauer, S.; Hidary, J.; Venables, P.; Hansen, R. Transitioning organizations to post-quantum cryptography. *Nature* **2022**, *605*, 237–243. [CrossRef]
22. Childs, A.M.; Van Dam, W. Quantum algorithms for algebraic problems. *Rev. Mod. Phys.* **2010**, *82*, 1–52. [CrossRef]
23. Micciancio, D.; Regev, O. Lattice-based cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 147–191.
24. Patarin, J. Hidden fields Equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 4–8 May 2003; pp. 33–48.
25. Courtois, N.T. Algebraic cryptanalysis of hidden field Equation (HFE) cryptosystem. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Republic of Korea, 27–28 November 2003; pp. 1–18.
26. Ding, J.; Schmidt, D. Cryptanalysis of HFEv and internal perturbation of HFE. In Proceedings of the Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; Proceedings 8; pp. 288–301.
27. Ding, J.; Perlner, R.; Petzoldt, A.; Smith-Tone, D. Improved cryptanalysis of HFEv-via projection. In Proceedings of the Post-Quantum Cryptography: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, 9–11 April 2018; Proceedings 9; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 375–395.
28. Cartor, R.; Gipson, R.; Smith-Tone, D.; Vates, J. On the differential security of the HFEv-signature primitive. In *International Workshop on Post-Quantum Cryptography*; Springer International Publishing: Cham, Switzerland, 2016; pp. 162–181.

29. Bettale, L.; Faugere, J.C.; Perret, L. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Des. Codes Cryptogr.* **2013**, *69*, 1–52. [CrossRef]
30. Petzoldt, A.; Chen, M.S.; Ding, J.; Yang, B.Y. HMFEv-an efficient multivariate signature scheme. In Proceedings of the Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, 26–28 June 2017; Proceedings 8; Springer International Publishing: Berlin/Heidelberg, Germany, 2017; pp. 205–223.
31. Dubois, V.; Granboulan, L.; Stern, J. Cryptanalysis of HFE with internal perturbation. In Proceedings of the Public Key Cryptography–PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, 16–20 April 2007; Proceedings 10; Springer: Berlin/Heidelberg, Germany, 2007; pp. 249–265.
32. Courtois, N.T.; Daum, M.; Felke, P. On the security of HFE, HFEv-and Quartz. In Proceedings of the Public Key Cryptography—PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography, Miami, FL, USA, 6–8 January 2003; pp. 337–350.
33. Courtois, N.T. Generic attacks and the security of Quartz. In *International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 351–364.
34. Petzoldt, A.; Chen, M.S.; Yang, B.Y.; Tao, C.; Ding, J. Design principles for HFEv-based multivariate signature schemes. In Proceedings of the Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015; pp. 311–334.
35. Fellows, M.; Koblitz, N. Combinatorial cryptosystems galore! *Contemp. Math.* **1994**, *168*, 51.
36. Buchberger, B. An algorithm for finding the basis elements of the residual class ring of a zero dimensional polynomial ideal. Diss. PhD thesis, University of Innsbruck. *Engl. Transl. Michael Abramson J. Symb. Comput. 2006* **1965**, *41*, 471–511.
37. Caboara, M.; Caruso, F.; Traverso, C. Lattice polly cracker cryptosystems. *J. Symb. Comput.* **2011**, *46*, 534–549. [CrossRef]
38. Albrecht, M.R.; Faugere, J.C.; Farshim, P.; Herold, G.; Perret, L. Polly cracker, revisited. *Des. Codes Cryptogr.* **2016**, *79*, 261–302. [CrossRef]
39. Herold, G. Polly cracker, revisited, revisited. In Proceedings of the Public Key Cryptography–PKC 2012: 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 21–23 May 2012; Proceedings 15; Springer: Berlin/Heidelberg, Germany, 2012.
40. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 353–367.
41. Maram, V.; Xagawa, K. Post-quantum anonymity of Kyber. In *IACR International Conference on Public-Key Cryptography*; Springer Nature: Cham, Switzerland, 2023; pp. 3–35.
42. Aikata, A.; Mert, A.C.; Imran, M.; Pagliarini, S.; Roy, S.S. KaLi: A crystal for post-quantum security using Kyber and Dilithium. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2022**, *70*, 747–758. [CrossRef]
43. Escribano Pablos, J.I.; González Vasco, M.I. Secure post-quantum group key exchange: Implementing a solution based on Kyber. *IET Commun.* **2023**, *17*, 758–773. [CrossRef]
44. Botros, L.; Kannwischer, M.J.; Schwabe, P. Memory-efficient high-speed implementation of Kyber on Cortex-M4. In Proceedings of the Progress in Cryptology–AFRICACRYPT 2019: 11th International Conference on Cryptology in Africa, Rabat, Morocco, 9–11 July 2019; Proceedings 11; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 209–228.
45. Bisheh-Niasar, M.; Azarderakhsh, R.; Mozaffari-Kermani, M. Instruction-set accelerated implementation of CRYSTALS-Kyber. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 4648–4659. [CrossRef]
46. Sanal, P.; Karagoz, E.; Seo, H.; Azarderakhsh, R.; Mozaffari-Kermani, M. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Virtual, 6–9 September 2021; Springer International Publishing: Cham, Switzerland, 2021; pp. 424–440.
47. Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Pintore, F.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-DILITHIUM: Digital signatures from module lattices. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 353–367.
48. Beckwith, L.; Nguyen, D.T.; Gaj, K. High-performance hardware implementation of crystals-dilithium. In Proceedings of the 2021 International Conference on Field-Programmable Technology (ICFPT), Auckland, New Zealand, 6–10 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–10.
49. Liu, Y.; Li, H. Hybrid digital signatures: Combining DILITHIUM with other cryptographic primitives. *Int. J. Inf. Secur.* **2022**, *21*, 325–340.
50. Kim, Y.; Song, J.; Youn, T.Y.; Seo, S.C. Crystals-Dilithium on ARMv8. *Secur. Commun. Netw.* **2022**, *2022*, 5226390. [CrossRef]
51. Grover, L.K. A framework for fast quantum mechanical algorithms. In Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, Dallas, TX, USA, 24–26 May 1998; pp. 53–62.
52. Coron, J.-S.; Naccache, D.; Tibouchi, M. Public key compression and modulus switching for fully homomorphic encryption over the integers. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012; pp. 446–464.
53. Gill, S.S.; Kumar, A.; Singh, H.; Singh, M.; Kaur, K.; Usman, M.; Buyya, R. Quantum computing: A taxonomy, systematic review and future directions. *Softw. Pract. Exp.* **2022**, *52*, 66–114. [CrossRef]

54. Sakumoto, K.; Shirai, T.; Hiwatari, H. Public-key identification schemes based on multivariate quadratic polynomials. In Proceedings of the Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2011; pp. 706–723.
55. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996.
56. Chen, L.; Jordan, S.; Liu, Y.K.; Moody, D.; Peralta, R.; Perlner, R.A.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; NIST Special Publication 800-233; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
57. Zeydan, E.; Turk, Y.; Aksoy, B.; Ozturk, S.B. Recent advances in post-quantum cryptography for networks: A survey. In Proceedings of the 2022 Seventh International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, USA, 26–27 February 2022; pp. 1–8.
58. Chen, Y.C.; Mooney, V.J., III; Grijalva, S. Grid Cyber-Security Strategy in an Attacker-Defender Model. *Cryptography* **2021**, *5*, 12. [CrossRef]
59. Gentry, C.; Peikert, C. Multiple cryptographic primitives from a single assumption. In Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), Palm Springs, CA, USA, 22–25 October 2011; pp. 217–226. [CrossRef]
60. Chen, J.; Ning, J.; Ling, J.; Lau, T.S.C.; Wang, Y. A new encryption scheme for multivariate quadratic systems. *Theor. Comput. Sci.* **2020**, *809*, 372–383. [CrossRef]
61. Zhang, P.; Wang, L.; Wang, W.; Fu, K.; Wang, J. A blockchain system based on quantum-resistant digital signature. *Secur. Commun. Netw.* **2021**, *2021*, 6671648. [CrossRef]
62. Karpman, P.; Wang, S. Evaluating the security of multivariate schemes against quantum attacks. *IEEE Trans. Inf. Theory* **2023**, *69*, 2334–2350.
63. Allende, M.; León, D.L.; Cerón, S.; Pareja, A.; Pacheco, E.; Leal, A.; Da Silva, M.; Pardo, A.; Jones, D.; Worrall, D.J.; et al. Quantum-resistance in blockchain networks. *Sci. Rep.* **2023**, *13*, 5664. [CrossRef]
64. Fernández-Caramés, T.M. From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet Things J.* **2019**, *7*, 6457–6480. [CrossRef]
65. Zhou, L.; Chen, H. Hybrid cryptosystems for post-quantum security. *Int. J. Inf. Secur.* **2022**, *21*, 649–661.
66. Gama, N.; Renault, L. Lattice-based cryptography: A comprehensive survey. *ACM Comput. Surv.* **2021**, *54*, 30.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.