Article

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

Yong Wang , Lingyue Li , Ying Zhou , Huili Zhang *

Posted Date: 24 September 2024

doi: 10.20944/preprints202409.1874.v1

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

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 [2,*]

[1] School of Arts and Science, Guangzhou Maritime University, Guangzhou, 510725, Chin; p117646@siswa.ukm.edu.my; lilingyue17@mails.ucas.ac.cn
[2] Institute of Visual Informatics (IVI), Universiti Kebangsaan Malaysia (UKM); p114383@siswa.ukm.edu.my
* Correspondence: zhang.huili0203@163.com

Abstract: The RSA cryptosystem has long been a fundamental component of contemporary public key infrastructure. However, recent developments in quantum computing and mathematical theory have introduced significant challenges to its security. A fully operational quantum computer would allow for the application of Shor's algorithm, enabling the efficient factoring of large integers, thereby compromising the integrity of RSA and other cryptographic methods dependent on discrete logarithms. Although Grover's algorithm poses a comparatively smaller threat to symmetric encryption systems, it still presents a vulnerability by accelerating key search processes. The looming threat from quantum technologies has driven a surge in research aimed at developing quantum-resistant cryptography. These efforts focus on cryptographic techniques grounded in 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 preserve security in a post-quantum world. This paper reviews the current progress in quantum-resistant encryption methods, particularly emphasizing the role of robust trapdoor functions. Additionally, it provides a comprehensive analysis of critical multivariate cryptosystem frameworks, such as Matsumoto-Imai, Oil and Vinegar, and Polly Cracker schemes. It also examines advances in lattice-based systems like Kyber and Crystals-Dilithium, which are undergoing assessment by NIST for potential standardization. As quantum computing continues to evolve, the demand for cutting-edge cryptographic solutions to safeguard digital communications grows increasingly pressing.

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

1. Introduction

The RSA cryptosystem [1] has been widely recognized as a dominant public key encryption technique in modern public key infrastructure. Its security is primarily based on the presumed computational difficulty of factoring large integers, a challenge deeply intertwined with both elementary and analytic number theory. Over several decades, no highly efficient algorithm has been identified for factoring large integers, reinforcing RSA's role as a cornerstone in cryptographic protection. Nonetheless, the emergence of new advances in computational technologies, especially the development of quantum computing, has begun to cast doubt on this foundational assumption.

If quantum computers become fully functional, they could exploit Shor's algorithm [2] to factor large numbers in polynomial time, which would critically undermine RSA and other cryptographic protocols based on discrete logarithms, such as elliptic curve cryptography (ECC) and the Diffie-Hellman key exchange. The potential threat posed by quantum computing is increasingly pressing, given the accelerating research in this area, driven by innovations in technologies such as superconducting qubits and ion trap systems. Although quantum computers capable of large-scale operations have not yet

 doi:10.20944/preprints202409.1874.v

materialized, significant progress and substantial financial backing suggest their development could be achieved within the next few decades. This creates an immediate necessity for cryptographic solutions that can withstand quantum-based attacks.

To address the threat posed by quantum advancements, researchers are actively developing cryptographic techniques that are resistant to quantum attacks, often referred to as post-quantum cryptography (PQC). Such approaches include cryptographic schemes based on error-correcting codes [3,4], lattice-based systems [5,6], and multivariate public key cryptosystems [7–9]. A notable example of lattice-based cryptography relies on the inherent difficulty of problems like the Learning with Errors (LWE) and the Shortest Vector Problem (SVP), which are resistant to the capabilities of currently known quantum algorithms. Similarly, code-based cryptosystems, such as the McEliece cryptosystem, are based on 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 [7–9], 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. Among the leading candidates in this process are lattice-based protocols like Kyber and Crystals-Dilithium, both of which have demonstrated significant promise during the standardization evaluations. As quantum technology continues to progress, the need for cryptographic systems capable of safeguarding communications against future quantum threats is becoming increasingly critical.

2. Literature Review

With the rapid advancement of quantum computing, the cryptographic community is increasingly pressured to devise secure post-quantum cryptographic solutions. Multivariate public key cryptography (MPKC) has emerged as a notable candidate due to its security foundation rooted in the complexity of solving multivariate quadratic equations, a well-known NP-hard problem. This section presents an in-depth exploration of the theoretical foundations, recent innovations, and challenges in MPKC, with a focus on the Hidden Field Equations (HFE) cryptosystem and its adaptations.

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.

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. However, challenges remain, particularly concerning the often-large public key sizes and the intricate design of secure trapdoors necessary to ensure cryptographic robustness.

 doi:10.20944/preprints202409.1874.v

2.2. HFE Cryptosystem and Its Variants

The Hidden Field Equations (HFE) cryptosystem, introduced by Patarin, 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. To mitigate these weaknesses, variants like HFEv and HFEv- have been developed, incorporating vinegar variables and internal perturbation methods to strengthen security.

Recent advances have sought to improve both the efficiency and resilience of HFE-based systems. For instance, the QUARTZ signature scheme, 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, 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. 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. 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. As quantum computing technology continues to evolve, addressing these vulnerabilities is vital to ensure the long-term security and viability of MPKCs.

2.4. 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. 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.

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.

 doi:10.20944/preprints202409.1874.v

3.1. The Matsumoto-Imai Cryptosystem

The Matsumoto-Imai (MI) cryptosystem, also known as the C^* scheme, is an early example of multivariate public key cryptosystems (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 takes advantage of the computational difficulty of solving multivariate quadratic (MQ) problems over finite fields, which are known to be NP-hard. As a result, MI is resistant to both classical and quantum attacks, including those based on 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, improving the practicality of encryption and decryption processes.

However, the original MI cryptosystem is vulnerable to specific algebraic attacks, such as differential and Gröbner basis attacks. These vulnerabilities have led to numerous proposed modifications and improvements, yet 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:

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

 doi:10.20944/preprints202409.1874.v

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. Security Analysis and Known Attacks

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.

 doi:10.20944/preprints202409.1874.v

3.5. 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.

3.6. Performance and Practical Efficiency

The Matsumoto-Imai 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.

3.7. Real-World Applications and Future Directions

Despite its theoretical advantages, the practical implementation of the Matsumoto-Imai (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.

 doi:10.20944/preprints202409.1874.v

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.

3.8. 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:

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

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:

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

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:

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

 doi:10.20944/preprints202409.1874.v

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.

8. Summary

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.

3.9. Linearization Equation Attack on the MI Scheme

In this section, we explore attacks targeting the C^* scheme, focusing on the use of linearization equations in cryptanalysis.

3.9.1. Linearization Equations in Cryptanalysis

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

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

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

3.9.2. Higher-Order Linearization Equations

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

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

where the degree d of the system is given by:

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

 doi:10.20944/preprints202409.1874.v

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.

3.9.3. 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 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 $x_1, \ldots, x_n$.

3.9.4. Conclusion

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.

 doi:10.20944/preprints202409.1874.v

3.10. 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.

3.10.1. Estimating Attack Complexity

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.

3.10.2. Attack History and Evolution

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.

3.10.3. Conclusion

The estimated complexity of attacking the C^* cryptosystem is approximately $O(n^6)$, largely driven by the inherent difficulty of solving multivariate quadratic systems and the additional overhead of Gröbner basis computations. Despite this complexity, cryptanalysis techniques continue to evolve, pushing cryptographers to develop more secure variants of multivariate cryptosystems. The history of the C^* scheme and its ongoing evolution highlight the constant back-and-forth between cryptographic innovation and cryptanalytic advances, as researchers work to balance security with practicality in post-quantum cryptography.

 doi:10.20944/preprints202409.1874.v

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 multivariate public key cryptosystems (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.

4.1.1. 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.

 doi:10.20944/preprints202409.1874.v

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}:

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

 doi:10.20944/preprints202409.1874.v

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 the 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

 doi:10.20944/preprints202409.1874.v

decryption is dominated by the evaluation of multivariate quadratic polynomials and the inversion of the central map.

Key Size and Computation

A significant challenge 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. Some Attacks on HFE

Although HFE was developed to address vulnerabilities in the C^* cryptosystem, it is not entirely immune to cryptanalysis. Two significant attacks on HFE are the Kipnis-Shamir attack and the MinRank attack.

4.6.1. Kipnis-Shamir Attack

This attack exploits the algebraic structure of HFE's central map by transforming the problem into a linear algebra context. By doing so, it reduces the complexity of solving the multivariate system, making the attack feasible under certain parameter choices. Specifically, it leverages the low rank of the matrix representation of the public key and uses linearization techniques to recover the private key. The attack's complexity is sub-exponential in the number of variables, posing a serious threat to specific HFE instances.

4.6.2. MinRank Attack

The MinRank attack is particularly threatening when the public key has a low rank. It attempts to solve the system of equations by minimizing the rank of a matrix representing the public key. The success of this attack depends on the parameter choices within the HFE system and has proven effective against certain HFE variants.

4.6.3. Countermeasures

To mitigate these attacks, several HFE variants have been proposed:

- **HFEv**: Introduces additional "vinegar" variables to increase system complexity.
- **HFEv-**: A refinement of HFEv that further reduces the public key's rank, enhancing resistance to MinRank attacks.
- **Perturbation Techniques**: Involve adding random noise to the public key to obscure its structure, making it more difficult for attackers to linearize or reduce its rank.

While these countermeasures significantly improve HFE's security, they often come with trade-offs in efficiency. For example, the introduction of vinegar variables increases the size of the public key, which may not be practical for all applications.

4.6.4. Direct Attack

The **direct attack** focuses on solving the system of multivariate quadratic equations defined by the public key map $\Gamma(x) = y$, where x represents the input variables and y is the output (e.g., ciphertext or signature). Although solving such systems is NP-hard, the specific structure of HFE polynomials provides avenues for more efficient attacks compared to generic MQ systems.

 doi:10.20944/preprints202409.1874.v

Algebraic Solving Techniques:

Common methods include the *Extended Linearization (XL) algorithm* and *Gröbner basis methods*, which exploit the algebraic properties of the equations to reduce the number of variables or equations. Experimental analyses indicate that HFE systems, characterized by a relatively low degree of regularity d, are more vulnerable to direct algebraic attacks than random quadratic systems. The degree of regularity d is bounded by:

$$d \leq \frac{(q-1)(r-1)}{2}, \quad \text{if } q \text{ is even and } r \text{ is odd,}$$

or

$$d \leq \frac{(q-1)r}{2} + 2, \quad \text{otherwise,}$$

where $r = \lfloor \log_q D \rfloor + 1$.

Recent Advances in Direct Attacks:

Recent research has focused on hybrid algorithms that combine Gröbner basis computations with lattice-based techniques to accelerate solving MQ systems. Advances in hardware, such as the use of *FPGAs* and *quantum computing*, have also increased the efficiency of direct attacks. As a result, cryptographers are exploring ways to strengthen HFE by increasing the complexity of the central map or introducing random perturbations to reduce the system's regularity.

4.6.5. Rank Attack (Kipnis–Shamir)

The **Kipnis–Shamir Rank Attack** exploits the algebraic structure of HFE's central map by transforming the quadratic map P through isomorphisms. This attack targets the *Q-rank*—the rank of the matrix representation of the quadratic form—simplifying the MQ system into a form more amenable to linear algebra techniques, such as solving the *MinRank Problem*.

MinRank Problem:

This problem involves finding coefficients $\lambda_1, \lambda_2, \ldots, \lambda_k$ such that the rank of the matrix

$$M = \lambda_1 M_1 + \lambda_2 M_2 + \cdots + \lambda_k M_k$$

is minimized, where $M_1, M_2, \ldots, M_k$ are known matrices. Although NP-hard, specialized methods like *Kipnis–Shamir modeling* and *Minors modeling* have been developed to solve it more efficiently.

Recent Developments in Rank Attacks:

Current research aims to improve rank attacks by leveraging *machine learning techniques* to identify low-rank structures more quickly. New algebraic insights into the invariants of HFE's central map under linear transformations have also led to enhanced modeling techniques, further reducing the complexity of solving the MinRank problem. These advancements highlight the need for cryptosystems like HFE to continually adapt to emerging threats.

4.6.6. Attack of Relinearization

The **relinearization attack** takes advantage of the purely quadratic nature of HFE's central map. By replacing each quadratic term $x_i x_j$ with a new variable y_{ij}, the system becomes linear in the y_{ij} variables, making it more tractable.

 doi:10.20944/preprints202409.1874.v

Transformation and Linearization:

The attack begins by substituting quadratic terms with new linear variables, reducing the system to εm^2 linear equations in $\frac{m^2}{2}$ variables. This simplification allows for the application of Gaussian elimination or other linear algebra techniques.

Recursive Relinearization:

Recent advancements have led to *recursive relinearization* methods, which iteratively apply relinearization to further simplify the system. By introducing higher-order constraints involving products of more than two variables, attackers can reduce the number of variables, increasing the attack's efficiency.

4.7. Security Considerations for HFE

The security of HFE is closely linked to the parameter D, which affects both the complexity of the central map and the overall security level. Increasing D enhances resistance to algebraic and rank-based attacks but also increases the computational cost of decryption and signature generation, as complexity scales cubically with D.

Quantum Resilience:

The advent of quantum computing introduces potential quantum attacks that HFE must address. While Grover's algorithm provides a quadratic speed-up for brute-force searches, interest has grown in *post-quantum variants of HFE*, such as incorporating trapdoor functions or using *super-polynomial degree HFE systems*. These approaches aim to mitigate quantum threats while maintaining efficient decryption and signature generation.

In conclusion, HFE remains an active research area, balancing inherent security with the evolving landscape of cryptographic attacks. Continuous advancements in cryptanalysis and algorithmic design are essential for its sustained use in secure communication systems.

5. 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 the advantages HFE holds over earlier systems like C^*, it still faces challenges related to 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.

5.1. 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.

 doi:10.20944/preprints202409.1874.v

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.

5.2. 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.

5.3. Improvements and Future Challenges

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 I, 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.

6. 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

 doi:10.20944/preprints202409.1874.v

(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.

6.1. Comprehensive Analysis and Future Research Directions 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.

6.2. Challenges from Theoretical Design to Practical Application

6.2.1. 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:

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

 doi:10.20944/preprints202409.1874.v

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.

6.2.2. 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.

6.3. Expanded Security Analysis Based on Recent Advances

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

 doi:10.20944/preprints202409.1874.v

6.3.1. Resistance to Lattice-Based and Algebraic Attacks

Lattice-based cryptanalysis, alongside algebraic attacks like 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.

6.3.2. 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.

6.3.3. 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. Below are several key areas for future investigation:

- **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,

 doi:10.20944/preprints202409.1874.v

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:

  $$\text{Key size} \propto q^r \quad \text{(where } q \text{ is the field size and } r \text{ represents the number of perturbation variables).}$$

  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 be extended 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 into hybrid systems combining multivariate public key cryptography (MPKC) with quantum-resistant techniques is essential for ensuring long-term security in the face of 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 explored key areas requiring attention, including susceptibility to lattice-based attacks, quantum threats, and the optimization of key size and efficiency. As a variant of multivariate public key cryptography, IPHFE offers promising avenues 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 ahead, 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

 doi:10.20944/preprints202409.1874.v

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.

7. Conclusion and Outlook

Multivariate cryptosystems, especially those based on multivariate quadratic (MQ) equations like HFE and its variants, have shown considerable potential for post-quantum cryptography. The Internal Perturbation HFE Cryptosystem (IPHFE) introduces perturbation variables to strengthen resistance against rank and relinearization attacks, which enhances security. However, as cryptanalysis techniques and quantum computing capabilities evolve, further research is needed to ensure the robustness of such systems.

Recent advances in cryptanalysis, particularly through techniques such as Gröbner basis methods and Bardet's complexity analysis, have deepened our understanding of the vulnerabilities in multivariate systems. These insights underscore the need for improving system-solving algorithms to strike a balance between security and efficiency. Quantum computing introduces new challenges, particularly through Grover's algorithm, which increases the need for post-quantum cryptographic primitives. Although multivariate schemes show promise, their long-term quantum security remains an open question, with IPHFE being a step toward quantum-resistant cryptography.

Looking ahead, several challenges need to be addressed. First, future cryptographic research must refine the complexity analysis of both classical and quantum-resistant cryptosystems. Understanding the true resilience of multivariate schemes in the face of advanced system-solving techniques remains a key goal. Second, improving the efficiency of cryptanalytic methods without compromising accuracy is crucial for bridging the gap between theoretical advances and practical applications. Lastly, designing new cryptographic constructions that balance classical security with quantum resilience will be essential to securing communications in the quantum era.

Specific areas of future research include:

- **Dynamic Perturbation Structures:** Current IPHFE systems use static perturbations. Dynamic perturbations that change over time or usage could significantly enhance resistance to long-term attacks.
- **Quantum-Resistant Extensions:** Integrating quantum-resistant techniques, such as lattice-based cryptography or hash-based signatures, with multivariate systems like IPHFE can create hybrid systems capable of resisting classical and quantum attacks.
- **Optimization of Cryptosystem Performance:** Further optimization of IPHFE, particularly reducing key size and computational complexity while maintaining security, is essential for real-world deployment.
- **Refined Complexity Analysis:** More precise frameworks are needed to evaluate the resilience of complex cryptosystems, particularly against quantum-based attacks.

In conclusion, multivariate cryptosystems, especially IPHFE, hold great promise in post-quantum cryptography. However, as quantum computing advances and cryptanalysis techniques become more sophisticated, continuous innovation and adaptation will be necessary to ensure these systems remain robust against emerging threats.

References

1. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, vol. 21, no. 2, 1978, pp. 120–126.
2. Shor, Peter W. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM Journal on Computing, vol. 26, no. 5, 1997, pp. 1484–1509.

 doi:10.20944/preprints202409.1874.v

3. McEliece, Robert J. *A public-key cryptosystem based on algebraic coding theory*. DSN Progress Report, vol. 42, no. 44, 1978, pp. 114–116.
4. Niederreiter, Harald. *Knapsack-type cryptosystems and algebraic coding theory*. Problems of Control and Information Theory, vol. 15, no. 2, 1986, pp. 159–166.
5. Regev, Oded. *Lattice-based cryptography*. Proceedings of the 38th Annual ACM Symposium on Theory of Computing, 2006, pp. 84–93.
6. Nguyen, Phong Q., and Jacques Stern. *The two faces of lattices in cryptology*. Proceedings of the 2001 Cryptography and Lattices Conference, Springer, 2001, pp. 146–180.
7. Patarin, Jacques. *Hidden field equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms*. Advances in Cryptology — EUROCRYPT '96, Springer, 1996, pp. 33–48.
8. Kipnis, Aviad, and Adi Shamir. *Cryptanalysis of the HFE public key cryptosystem by relinearization*. Advances in Cryptology — CRYPTO '99, Springer, 1999, pp. 19–30.
9. Courtois, Nicolas T., Matthieu Finiasz, and Nicolas Sendrier. *Quartz, an asymmetric signature scheme based on multivariate quadratic polynomials*. Public Key Cryptography — PKC 2001, Springer, 2001, pp. 291–307.
10. Buchberger, Bruno. *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal*. PhD thesis, University of Innsbruck, 1965.
11. Faugère, Jean-Charles. *A new efficient algorithm for computing Gröbner bases (F4)*. Journal of Pure and Applied Algebra, vol. 139, no. 1-3, 1999, pp. 61–88.
12. Faugère, Jean-Charles. *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*. Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, 2002, pp. 75–83.
13. Bardet, Magali. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, Université Paris 6, 2004.
14. Fraenkel, Aviezri S., and Yossi Yesha. *Complexity of problems in games, graphs, and algebraic equations*. Discrete Applied Mathematics, vol. 2, no. 3, 1980, pp. 195–214.
15. Matsumoto, Tsutomu, and Hideki Imai. *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*. Advances in Cryptology — EUROCRYPT '88, Springer, 1988, pp. 419–453.
16. Kipnis, Aviad, Adi Shamir, and Jacques Patarin. *Unbalanced oil and vinegar signature schemes*. Advances in Cryptology — EUROCRYPT '99, Springer, 1999, pp. 206–222.
17. Kipnis, Aviad, and Adi Shamir. *Cryptanalysis of the oil and vinegar signature scheme*. Advances in Cryptology — CRYPTO '98, Springer, 1998, pp. 257–266.
18. Arora, Sanjeev, and Rong Ge. *New Algorithms for Learning in Presence of Errors*. Proceedings of the 43rd annual ACM Symposium on Theory of Computing, ACM, 2011, pp. 405–414.
19. Fellows, Michael R., and Neal Koblitz. *Polly Cracker: A new way to break codes*. Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, Springer-Verlag, 1994, pp. 397–408.
20. Chen, Chengdong, et al. *Internal perturbation of HFE*. Information Security and Cryptology, Springer, 2008, pp. 274–287.
21. Ding, Jintai, and Dieter Schmidt. *Cryptanalysis of HFEv and internal perturbation of HFE*. Post-Quantum Cryptography, Springer, 2004, pp. 24–29.
22. Ding, Jintai, Andreas Petzoldt, and Dieter Schmidt. *Selecting the right parameters for HFEv-variants*. Post-Quantum Cryptography, Springer, 2011, pp. 252–272.
23. Courtois, Nicolas T., Matthieu Finiasz, and Nicolas Sendrier. *Quartz, 128-bit long digital signatures*. Proceedings of the 4th International Conference on Information Security and Cryptology, Springer, 2001, pp. 282–297.
24. Tang, Shanxiang, Zhicong Chen, and Chengdong Chen. *The GUI public key cryptosystem*. Information Security and Cryptology, Springer, 2008, pp. 173–186.
25. Petzoldt, Albrecht, Ming-Shing Chen, Jintai Ding, Dieter Schmidt, and Bo-Yin Yang. *Gui: A Simple and Efficient Post-Quantum Signature Scheme*. NIST PQC Standardization Workshop, 2018.
26. Koblitz, Neal. *Elliptic curve cryptosystems*. Mathematics of Computation, vol. 48, no. 177, 1987, pp. 203–209.

 doi:10.20944/preprints202409.1874.v

27. Courtois, Nicolas T., Alex Klimov, Jacques Patarin, and Adi Shamir. *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*. Advances in Cryptology — EUROCRYPT 2000, Springer, 2000, pp. 392–407.
28. Courtois, Nicolas T. *Efficient zero-knowledge authentication based on a linear algebra problem MinRank*. Advances in Cryptology — ASIACRYPT 2001, Springer, 2001, pp. 402–421.