Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions

JAYASHREE DEY and RATNA DUTTA, Indian Institute of Technology Kharagpur

Multivariate Public Key Cryptosystem (MPKC) seem to be promising toward future digital security even in the presence of quantum adversaries. MPKCs derive their security from the difficulty of solving a random system of multivariate polynomial equations over a finite field, which is known to be an NP-hard problem. This article aims at presenting a comprehensive survey that covers multivariate public key encryption and signature schemes specifically targeting toward security, efficiency, and parameter choice. The survey starts by giving an overview of the existing security challenges which include structural attacks such as MinRank attack, *differential attack*, and finding Gröbner basis for *direct attack*, and so on. Additionally, it discusses the necessary algorithms for the implementation of the multivariate schemes. This study also compares the promising multivariate encryption and signature schemes. The critical open challenges that are reviewed in this survey will serve as a single comprehensive source of information on multivariate encryption and signature schemes and a ready reference for researchers working in this rising area of public key cryptography.

CCS Concepts: • **Security and privacy → Public key (asymmetric) techniques;**

Additional Key Words and Phrases: Post-quantum cryptography, multivariate polynomials, HFE polynomials, diophantine equations, MQ problem

ACM Reference format:
Jayashree Dey and Ratna Dutta. 2023. Progress in Multivariate Cryptography: Systematic Review, Challenges, and Research Directions. *ACM Comput. Surv.* 55, 12, Article 246 (March 2023), 34 pages.
https://doi.org/10.1145/3571071

1 INTRODUCTION

Towards meeting the growing demand for security in advanced computational scenarios, it is a continuous endeavor to formulate and develop cost-effective strong security primitives. Multivariate public key cryptography is one of the main approaches to ensure safe communication in a post-quantum world. In the last few years, ***Multivariate Public Key Cryptosystems*** **(MPKCs)** have been seen to be considered as a possible alternative to the public key cryptosystems like RSA, Diffie-Hellman key exchange, DSA, elliptic curve algorithms, and so on. which are secure under number theoretic assumptions. In 1994, Shor [102] showed that quantum computers can break each of these systems in polynomial time. As soon as large quantum computers become a reality, the security of cryptosystems based on number theoretic assumptions will be questionable. The modern idea to design a multivariate cryptographic scheme was introduced by Matsumoto and Imai [78] in

Authors' address: J. Dey (corresponding author) and R. Dutta, Indian Institute of Technology Kharagpur, Kharagpur, West Bengal 721302, India; emails: deyjayashree@iitkgp.ac.in, ratna@maths.iitkgp.ernet.in.

0360-0300/2023/03-ART246 $15.00
https://doi.org/10.1145/3571071

Eurocrypt 1988. Multivariate cryptography is the generic term for the asymmetric cryptographic primitives based on multivariate polynomials over a finite field. The security relies on solving a set of multivariable polynomial equations over a finite field which is NP-hard in general. So far quantum computers have not yet been able to solve a set of multivariate polynomial equations efficiently and are unlikely to provide any advantage against such a problem. The ***National Institute of Standards and Technology*** (**NIST**) announced a call for ideas for quantum-resistant algorithms in December 2016. Besides, government organizations like the *European Commission* and the *Japanese Society* promoted science finance research programs to enhance post-quantum cryptography research.

Most of the MPKCs do not have a formal security proof. The security is analyzed theoretically and experimentally based on selected parameters. In a multivariate public key encryption scheme, an encryptor encrypts a message $\mathbf{x}$ using his public key P which is an injective map, and outputs the ciphertext $P(\mathbf{x})$. The public key P consists of a composition of certain multivariate affine maps and a central map which is MQ polynomials in general. The corresponding secret key consists of the central map and the affine maps used in P. On the contrary, in a multivariate signature scheme, a signature is generated using the secret key and is verified using the public key. To generate a signature for a message $\mathbf{x}$, the signer computes $\mathbf{z}$ utilizing his secret key information in constructing the public map P. The verifier, having the public key P, checks the validity of the signature $\mathbf{z}$ where $\mathbf{x}$ is the corresponding message. In direct attacks, an adversary tries to solve the public system $P(\mathbf{x}) = \mathbf{y}$ for $\mathbf{x}$ directly by finding Gröbner basis using various algorithms such as F4 of Faugère [50] and F5 of Faugère [51]. *Structural attacks* such as *rank attacks* and *differential attacks* utilize the structure of the central map of a multivariate scheme to recover the composition of the public key. In MinRank attack [72], the adversary finds a linear combination of the quadratic forms associated with the public key polynomials of low rank and is able to recover the secret key of multivariate scheme. A differential attack [55] searches for symmetries or invariants of the differential $G(\mathbf{x}, \mathbf{y}) = P(\mathbf{x} + \mathbf{y}) - P(\mathbf{x}) - P(\mathbf{y}) + P(\mathbf{0})$ of the public key P which are then used to analyze the structure of the scheme and recovers the central map.

One of the main advantages of MPKCs is the speed of encryption and signature verification. For a multivariate encryption scheme, an encryption algorithm is easy and efficient as it is a simple computation of $P(\mathbf{x})$ for plaintext $\mathbf{x}$ using a public map P. On the other hand, the decryption algorithm is comparatively slower and costly as it involves solving system of linear equations and finding pre-image under MQ polynomials. This requires the use of heavy computational algorithms like *Gaussian elimination*, *Berlekamp algorithm*, and so on. It is hard to invert the public map P and recover the message without knowing the secret key. In case of signature schemes, the inversion of public map P is required to generate a signature corresponding to a message whereas verification needs a simple computation of $P(\mathbf{x})$ for message $\mathbf{x}$ using a public map P. Multivariate schemes are in general very fast and efficient and look attractive for signatures on low-cost devices like ***Radio Frequency IDentifications*** (**RFIDs**) or *smart cards* [29].

Although MPKCs have been very productive in designing quantum-safe cryptographic protocols, they have public keys much larger than lattice-based cryptosystems and classical schemes based on number theoretic assumptions. Furthermore, most of the multivariate public key schemes do not have formal security proofs.

This article focuses on providing a rather complete relevant literature survey on multivariate public key encryption schemes and signature schemes. Different aspects are presented on the most promising multivariate public key encryption and signature schemes together with an overview on the suggested practical parameters and discussion on their security and efficiency.

1.1 Contribution

Efficiency and security are the two main issues of any cryptographic primitive. Achieving both simultaneously is a challenging task and has been the priority of the research community even since the birth of applied cryptography. In 2017, Ding and Petzoldt [39] provided a review on promising multivariate encryption and signature schemes. The review was mainly focused on conveying the status of MPKC along with a preliminary sketch of the security, efficiency, and limitations rather than concentrating on giving a description of existing attacks and necessary algorithms for the schemes. Later, Hashimoto ([62], [63]) presents surveys on MPKC that provide an idea of some schemes with security analysis and discuss some open problems in that area. But those lack a complete discussion of the promising constructions that have enriched the area. In 2020, Ding, Petzoldt, and Schmidt [40] published a book (second edition) that contains more fresh new ideas and research results on multivariate cryptography in detail besides demonstrating the basic essential ideas, methods, and examples. We emphasize that our article will help the researchers to get an immediate idea of the present scenario in this area. Moreover, in the last two years, more research was done on MPKC due to the development of new attack strategies. Hence, we strongly believe that a comprehensive survey is essential for interested readers who are planning to initiate research in this area.

The primary focus of this survey is to provide a systematic review on the multivariate encryption and signature schemes covering the security, and efficiency aspects. We omit some earlier multivariate encryption schemes like MI [78], basic HFE [84] and some of their variants due to the lack of security as well as efficiency. We have described the Simple Matrix [107], ZHFE [98], HFERP [69], and EFLASH [17] scheme in this survey. Although most of the above-mentioned schemes are not fully secure, those seem to be promising candidates to design new multivariate schemes in upcoming days. Almost all the signature schemes are mainly encouraged by the idea of Oil Vinegar, Rainbow, and HFE equation-based schemes. Also, schemes like **Unbalanced Oil Vinegar** (**UOV**) and Rainbow are useful in designing some other primitives like identity-based signatures and ring signatures and may be effective in devising further constructions in the future. We have tried to give a description of the schemes like Oil Vinegar [85], Rainbow [42], HFEv- [95], and HMFEv [94]. We discuss state-of-the-art security challenges, their countermeasures, and necessary algorithms that are useful for cryptanalysis as well as for designing secure multivariate cryptosystems. This article does not attempt to solve any new challenge. We investigate the critical open challenges and suggest directions for future research toward provisioning efficient and secure solutions for multivariate cryptosystems.

In particular, the principal contributions of our work are as follows:

- We present the essential background knowledge for MPKCs, its functionalities, and its related concepts. The goal is to enable the new readers to get the required familiarity with the multivariate cryptography and its relevant definitions. It is notably needed to understand the methodology, advantages, and challenges affiliated with the MPKCs.
- We also discuss the essential algorithms for the implementation of the multivariate schemes. In multivariate cryptography, decryption or signature generation requires the use of costly algorithms like Gaussian elimination, Berlekamp algorithm, and *Relinearization* technique. It is necessary to know the algorithms so that a clear scenario can be viewed by a new reader regarding the utilization of those procedures in MPKCs.
- We present and discuss the existing attacks associated with MPKCs such as direct attacks, rank attacks, differential attacks, and so on. We also describe the necessary algorithms which an adversary can exploit to launch an attack on a scheme.

— We systematically present an overview of some promising encryption schemes and signature schemes with the parameters that were suggested to avoid existing attacks. We also discuss the efficiency and limitations of the schemes besides discussing the attack possibilities on those designs. Furthermore, we present a summary of the NIST candidates in all the three rounds of the prestigious competition. Finally, we furnish the list of lessons learned, open problems, and future directions based on our survey.

To the best of our knowledge, this survey explores nearly all primitives and aspects of the multivariate cryptography, discusses the most promising encryption and signature schemes in detail along with a brief description of the existing attacks and heavy computational algorithms used during decryption procedure or signature generation and highlights the advantages and limitations of the schemes. The article intends to support the enthusiastic readers to understand the scope of MPKCs, to learn the impact of possible attacks on the schemes and to indicate the possible directions to design more efficient and secure multivariate schemes. We believe that some characteristics of multivariate schemes make these attacks practical. These characteristics include the low rank property of the central map, the low rank of the affine maps, and some other structural weakness. Hence, the purpose of our work is to promote the MPKC research on the earnest requirement to prevent various attacks.

Organization of Article: The rest of this article is organized as follows. The preliminary background on multivariate cryptography are presented in Section 2 to make the survey self-contained. In Section 3, we discuss some structural attacks on MPKCs. Then we illustrate the designs of some promising multivariate public key encryption schemes in Section 4 and the constructions of some signature schemes in Section 5. We present an overview of the submissions in NIST competition in Section 6. In Section 7, some observations on MPKCs are outlined and a few possible directions are indicated. Finally, we conclude in Section 8.

2 PRELIMINARIES

The one-wayness of multivariate polynomial maps depends on the difficulty of finding solutions to a system of multivariate polynomial equations. This problem is referred to as the MP problem. In particular, if the multivariate polynomials involved in the MP problem consist only of quadratic polynomials, the problem is called the MQ problem.

Definition 2.1 (MQ Problem). Consider a system of m multivariate quadratic polynomials $f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_m(\mathbf{x})$ in n variables $x_1, x_2, \ldots, x_n$ defined as

$$
\begin{aligned}
f_1(x_1, x_2, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} f_i^{(1)} \cdot x_i + f_0^{(1)} \\
f_2(x_1, x_2, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} f_i^{(2)} \cdot x_i + f_0^{(2)}, \\
&\vdots \\
f_m(x_1, x_2, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} f_i^{(m)} \cdot x_i + f_0^{(m)},
\end{aligned}
$$

with coefficients $f_{ij}^{(k)}, f_l^{(k)}$, $1 \le i, j \le n$, $1 \le k \le m$, $0 \le l \le n$ and the variables x_i, $1 \le i \le n$ are elements of a finite field $\mathbb{F}$. The MQ problem is to find a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ such that $f_1(\mathbf{x}) = f_2(\mathbf{x}) = \cdots = f_m(\mathbf{x}) = 0$.

The MQ problem is proven to be NP-hard even for quadratic polynomials over the field GF(2) ([58]).

A public key encryption scheme consists of four **probabilistic polynomial time algorithms** (**PPT**) Setup, KeyGen, Encrypt, and Decrypt where

$$\text{Setup}(1^\lambda) \to \text{pp}, \text{KeyGen}(\text{pp}) \to (\text{pk}, \text{sk}), \text{Encrypt}(\text{pp}, \text{pk}, \mathbf{x}) \to \mathbf{c}, \text{Decrypt}(\text{pp}, \text{sk}, \mathbf{c}) \to \mathbf{x}.$$

Here λ is the security parameter, pp is the set of global public parameters, pk and sk are respectively public key and secret key, $\mathbf{x}$ is a plaintext and $\mathbf{c}$ is the corresponding ciphertext. To construct a public key encryption scheme whose security is based on the MQ problem, pp is generated and published by running Setup algorithm where λ is the security parameter. The algorithm KeyGen(pp) is invoked by a user who selects an easily invertible quadratic map $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ and composes it with two invertible maps $S : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ and $T : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ to hide the structure of F. The algorithm outputs the public key $\text{pk} = P = S \circ F \circ T$ and the secret key consists of S, F and T. The encryptor uses his public key $\text{pk} = P$ and encrypts a message $\mathbf{x} \in \mathbb{F}^n$ by computing the ciphertext $\mathbf{c} = P(\mathbf{x})$ in $\mathbb{F}^m$ by running Encrypt(pp, pk, $\mathbf{x}$). To decrypt the ciphertext $\mathbf{c} \in \mathbb{F}^m$, the decryptor uses his secret key $\text{sk} = (S, F, T)$, runs Decrypt(pp, sk, $\mathbf{c}$) to compute $\mathbf{y} = S^{-1}(\mathbf{c})$, $\mathbf{u} = F^{-1}(\mathbf{y})$ and recovers the corresponding plaintext $\mathbf{x} = T^{-1}(\mathbf{u})$.

On the other hand, a signature scheme is a tuple of four PPT algorithms Setup, KeyGen, Sign and Verify where

$$\text{Setup}(1^\lambda) \to \text{pp}, \text{KeyGen}(\text{pp}) \to (\text{pk}, \text{sk}), \text{Sign}(\text{pp}, \text{sk}, \mathbf{d}) \to \mathbf{z}, \text{Verify}(\text{pp}, \text{pk}, \mathbf{d}, \mathbf{z}) \to 0/1.$$

Here λ is the security parameter, pp is the set of global public parameters, pk is the public key, sk is the secret key, $\mathbf{d}$ is a document and $\mathbf{z}$ is the corresponding signature to the message $\mathbf{d}$. To build a signature scheme that relies on MQ problem, pp is generated and published in Setup phase taking the security parameter λ as input. In key generation phase, a user runs KeyGen(pp) that chooses an invertible quadratic map $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ and composes it with another two invertible maps $S : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ and $T : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ to mask the structure of F. The algorithm outputs the public key $\text{pk} = P = S \circ F \circ T$ and the secret key sk consists of the maps S, F and T. To generate the signature $\mathbf{z} \in \mathbb{F}^n$ for a document $\mathbf{d} \in \mathbb{F}^m$, the signer uses his secret key $\text{sk} = (S, F, T)$, runs Sign(pp, sk, $\mathbf{d}$) to compute $\mathbf{y} = S^{-1}(\mathbf{d})$, $\mathbf{w} = F^{-1}(\mathbf{y})$ and $\mathbf{z} = T^{-1}(\mathbf{w})$. To check the authenticity of the signature $\mathbf{z} \in \mathbb{F}^n$ for the document $\mathbf{d} \in \mathbb{F}^m$, the verifier uses the public key $\text{pk} = P$, executes Verify(pp, pk, d, z) and checks whether $\mathbf{d} = P(\mathbf{z})$ or not. If $\mathbf{d} = P(\mathbf{z})$ holds, the signature is accepted, otherwise rejected.

2.1 HFE Polynomial [84]

Let $\mathbb{F}$ be a finite field of size q, n be a positive integer, $g(y) \in \mathbb{F}[y]$ be an irreducible polynomial of degree n and $K = \mathbb{F}[y]/(g(y))$ be the extension field. Let $\phi : K \to \mathbb{F}^n$ be an isomorphism defined by $\phi(u_1 + u_2 y + \cdots + u_n y_{n-1}) = (u_1, u_2, \ldots, u_n)$.

A polynomial is said to have Hamming weight W if the maximum of the q-Hamming weights of all its exponents is W. Here the q-Hamming weight of a non-negative integer is defined as the sum of the q-digits of its q-nary expansion.

Definition 2.2 (Hidden Field Equations (HFE)). An HFE polynomial $F : K \to K$ is a polynomial of the form

$$F(X) = \sum_{0 \le j \le i}^{n-1} a_{ij} X^{q^i + q^j} + \sum_{i=0}^{n-1} b_i X^{q^i} + c,$$

with Hamming weight two where the coefficients $a_{ij}, b_i, c \in K$.

If $\deg(F(X)) \leq d$ holds for a fixed positive integer d, $F(X)$ is said to be an *HFE polynomial with bound d*.

2.2 Polynomials of Degree Increasing Type [81]

Let $\mathbb{Z}[\underline{x}] = \mathbb{Z}[x_1, x_2, \ldots, x_n]$ denote the polynomial ring with n variables and $\mathbb{Z}_{\geq 0}$ be the set of non-negative integers. For a vector $\underline{i} = (i_1, i_2, \ldots, i_n) \in (\mathbb{Z}_{\geq 0})^n$, we define $\underline{x}^{\underline{i}} = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ and $\sum \underline{i} = \sum_{1 \leq j \leq n} i_j \in \mathbb{Z}_{\geq 0}$. Let X be a multivariate polynomial of degree w_X defined by

$$X(\underline{x}) = \sum_{(i_1, i_2, \ldots, i_n) \in \Lambda} X_{i_1 i_2 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} = \sum_{\underline{i} \in \Lambda} X_{\underline{i}}\, \underline{x}^{\underline{i}} \in \mathbb{Z}[\underline{x}],$$

where $\Lambda \subset (\mathbb{Z}_{\geq 0})^n$. The degree of a multivariate polynomial refers to the maximal of the sums of all the powers of the variables in each term. We consider the support of X defined by $\Lambda_X = \{\underline{i} \in (\mathbb{Z}_{\geq 0})^n | X_{\underline{i}} \neq 0\}$.

Definition 2.3 (Polynomials of Degree Increasing Type [81]). Let $\sigma : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ be a map defined by $\sigma(\underline{i}) = \sum \underline{i}$. A polynomial $X \in \mathbb{Z}[\underline{x}]$ is said to be a polynomial of degree increasing type if $\sigma|_{\Lambda_X}$ is injective where $\sigma|_{\Lambda_X}$ is the restriction of σ to Λ_X. In other words, X is said to be a polynomial of degree increasing type if and only if X has at most one term of degree k for each $k \in \mathbb{Z}$.

For example $X(x, y) = 9x^4y^2 + xy^2 + 3xy + 2x + 7$ is a polynomial of degree increasing type.

2.3 Eulerian Equation and Eulerian Map [108]

Let q be a prime, $\mathbb{F}$ be a finite field with cardinality q and $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

Definition 2.4 (Eulerian Equation). An equation of the form $x^\alpha = b$, $b \in \mathbb{F}, \alpha \in \mathbb{Z}$, is said to be Eulerian equation over the field $\mathbb{F}$ if $\gcd(\alpha, q-1) = 1$. This equation has a unique solution in $\mathbb{F}$.

Definition 2.5 (Eulerian Map). A multivariate map $f : \mathbb{F}^n \to \mathbb{F}^n$ is said to be an Eulerian map over the field $\mathbb{F}$ if it is an injection into $(\mathbb{F}^*)^n$ when restricted to $(\mathbb{F}^*)^n$. The equation $f(\mathbf{x}) = \mathbf{b}$, $\mathbf{b} \in (\mathbb{F}^*)^n$ has a unique solution $\mathbf{x} \in (\mathbb{F}^*)^n$.

2.4 Berlekamp Factorization [5]

Given a monic univariate polynomial $f \in \mathbb{F}[x]$ where $\mathbb{F}$ is a finite field, the Berlekamp factorization algorithm aims at finding distinct irreducible factors of f. Consider the theorem stated below.

Theorem 2.6. *Let $\mathbb{F}$ be a finite field. If $f \in \mathbb{F}[x]$ is a monic polynomial and a polynomial $h \in \mathbb{F}[x]$ satisfies $h^q = h \mod f$, then $f(x) = \prod_{c \in \mathbb{F}} gcd(f(x), h(x) - c)$.*

The polynomial f can be expressed as a product of k irreducible factors $f_1, f_2, \ldots, f_k$ as follows.

- Step 1. Make f square-free.
- Step 2. Construct the matrix of transformation B corresponding to the map $h \mapsto h^q - h$. Note that the polynomial h satisfies $h^q = h \mod f_i$ for $1 \leq i \leq k$. The kernel of this map $h \mapsto h^q - h$ asks for all vectors $\mathbf{v}$ such that $\mathbf{v}B = 0$. The dimension of B is k which is the number of distinct monic irreducible factors of $f(x)$. If rank of B is r, the number of distinct monic irreducible factors is $k = n - r$.
- Step 3. Find a basis $\{h_1, h_2, \ldots, h_k\}$ of the null space of B.
- Step 4. If $k = 1$, f is irreducible and the procedure will be terminated. If $k \geq 2$, a non trivial factorization of $f(x)$ will be $\gcd(f(x), h_2(x) - c)$ for all $c \in \mathbb{F}$ by Theorem 2.6. If k factors of f are not obtained using $h_2(x)$, then $\gcd(f(x), h_3(x) - c)$ will be computed for all $c \in \mathbb{F}$. The process will continue until the computation of all k factors of $f(x)$.

2.5 Relinearization Technique [71]

The Relinearization technique solves a overdetermined system of multivariate quadratic equations. Suppose a system consists of m quadratic equations in the n variables $x_1, x_2, \ldots, x_n$. Then one proceed as follows:

- Introduce a new variable y_{ij} for each quadratic monomial $x_i x_j$ for $i, j \in \{1, 2, \ldots, n\}$ to obtain a system of linear equations.
- Solve the system using Gaussian elimination.

3 ATTACKS ON MULTIVARIATE CRYPTOSYSTEMS

The purpose of an attack on any cryptosystem is to recover plaintext $\mathbf{x}$ from a given ciphertext $\mathbf{c}$ which is equivalent to solving an instance of the MQ problem over a finite field. Although the MQ problem is NP-hard, some techniques are helpful in practice. In this section, we give a rough idea of some significant attacks on MPKCs such as direct attack, MinRank attacks, and differential attacks.

3.1 Direct Attack

— **Gröbner bases**. One significant way to execute the direct attack on MPKCs is by finding Gröbner bases. In 1965, Buchberger [12] presented the Buchberger algorithm to calculate them. The concept behind the attack is to consider a ciphertext $\mathbf{c}$ and solve the system $P(\mathbf{x}) - \mathbf{c} = 0$ for the plaintext $\mathbf{x}$ by searching a Gröbner basis of the ideal generated by the polynomials $P(\mathbf{x}) - \mathbf{c}$. The main cost of the Gröbner basis attack lies on the computation of the Gröbner basis.

Definition 3.1 (Gröbner Basis). A subset G of the polynomial ring $\mathbb{F}[x_1, x_2, \ldots, x_n]$ over a field $\mathbb{F}$ is said to be a Gröbner basis with respect to the term order $\leq$ if it is finite, $0 \notin G$, and $f \xrightarrow[G]{*} 0$ holds for all $f \in \mathsf{Id(G)}$ where $f \xrightarrow[G]{*} 0$ indicates that the remainder of division f by G is zero and $\mathsf{Id(G)}$ denotes the ideal generated by G. If I is an ideal of $\mathbb{F}[x_1, x_2, \ldots, x_n]$, then a Gröbner basis of I is a Gröbner basis G such that $\mathsf{Id}(G) = I$.

Note that, a solution of all the polynomials of G must also be a solution of all polynomials of $P(\mathbf{x}) - \mathbf{c}$ as $P(\mathbf{x}) - \mathbf{c}$ and G both generate I. In [15], the efficiency of multivariate quadratic public key operation against its direct attack is precisely analysed to understand the role of the field equations in the attack besides optimizing implementations for those operations on various finite fields.

— **XL algorithm**. In 2000, Courtois et al. [25] proposed the ***eXtended Linearization*** **(XL)** algorithm which is useful for direct/algebraic attacks. The XL algorithm is used to solve a system of quadratic equations.

Let $\mathbb{F}$ be a finite field and consider a system of multivariate equations $p_j = 0$ for $1 \leq j \leq m$ where each p_j represents multivariate polynomial in the form $f_j(x_1, x_2, \ldots, x_n) - b_j$ for $f_j \in \mathbb{F}[X] = \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $b_j \in \mathbb{F}$.

Now we consider all the polynomials of the form $\prod_{j=1}^{r} x_{i_j} \cdot p_j$ of total degree $\leq d$ where d is a positive integer. Let S_d be the linear space spanned by the polynomials.

XL algorithm follows the steps described below.

- Step 1. Compute all the products in the form $\prod_{j=1}^{r} x_{i_j} \cdot p_j \in S_d$ of total degree $\leq d$ where $r \leq d - 2$.
- Step 2. Execute Gaussian elimination on the equations derived in Step 1 considering each monomial in the x_i having degree $\leq d$ as a new variable. The monomial ordering must be done in such a way that all the terms with one variable (say x_1) are eliminated at the last.

— Step 3. Suppose Step 2 produces at least one univariate equation in the powers of x_1. Solve the equation using Berlekamp's algorithm to get x_1.
— Step 4. After getting x_1, simplify the equations and repeat the process to get the values of the other variables $x_2, x_3, \ldots, x_n$.

There are several variants of XL that have been proposed, such as FXL, XL2, and MutantXL. FXL is generally used to find a solution to a system at a lower degree. It fixes the values of some variables before involving the XL algorithm. The variant XL2 is helpful for use over the field GF(2). The primary concept of MutantXL is to privilege some polynomials of a lower degree during the elimination process of XL.

3.2 MinRank Attacks

Another attack on MQ-based encryption schemes is by solving instances of the MinRank problem. Precisely, the aim of such attack is to split the public key $P = S \circ F \circ T$ into the private key (S, F, T). The MinRank problem is NP-complete and firstly introduced by Buss et al. [13]. The *minors method* by Bettale et al. [6], the ***Kipnis-Shamir (KS)*** *method* by Kipnis and Shamir [72] and the *linear algebra search* by Goubin and Courtois [59] are familiar techniques to solve a MinRank problem.

Definition 3.2 (MinRank Problem [59]). Let $\mathbb{F}$ be a field and r be a positive integer. Then MinRank(r) problem asks to find a non-zero l-tuple $(\lambda_1, \lambda_2, \ldots \lambda_l) \in \mathbb{F}^l$ such that Rank$(\sum_{i=1}^{l} \lambda_i M_i) \leq r$ holds for a given set $\{M_1, M_2, \ldots, M_l\} \in \mathbb{F}^{n \times n}$.

The purpose of MinRank attack is to get the knowledge of the private key (S, F, T), starting with the function S. After that, the attack continues to reveal the quadratic coefficients of F and the function T. Once those are recognized, one can determine the constant and linear coefficients of F by gaussian elimination.

The work of Verbel et al. [110] reconsiders the KS approach to solve MinRank problem focusing on a precise set of instances that induce an extremely overdetermined system called "superdetermined". More interestingly, for such instances, the complexities of the approach for some multivariate schemes are carefully analysed. Another considerable improvement in algebraic techniques for solving the MinRank problem was suggested by Bardet et al. [4]. It is built on top of a breakthrough work of [3] demonstrating an improvement over Gröbner basis computation for solving a system of equations. In [4], Gröbner bases computations for specific parameters were thoroughly bypassed while possessing only linear systems.

3.3 Differential Cryptanalysis

In 2005, Fouque et al. [55] suggested an attack using differential cryptanalysis to PMI [31] encryption scheme by producing practical decryption functions. More precisely, for any given ciphertext $\mathbf{c}$, the associated plaintext $\mathbf{x}$ can be found using a calculated function rather than solving a system for ciphertext $\mathbf{c}$. The main technique involved to determine such a function is the use of differential and the bilinear function. For a public key function $P : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ and $k \in \mathbb{F}^n$ where $\mathbb{F}$ is a field, the differential of P with respect to k is $dP_k(\mathbf{x}) = P(\mathbf{x} + k) - P(\mathbf{x})$ and the bilinear function is $B(\mathbf{x}, k) = dP_k(\mathbf{x}) - dP_k(0)$. Using differentials of quadratic functions P to get bilinear functions is the main idea of the attack. The attack uses the fact that the differential of the public key in a multivariate quadratic system is a linear map and encloses invariants like the dimension of the kernel from which data of the secret key can be acquired. In case of the PMI scheme, the dimension of the kernel helps to revoke the perturbation by recognizing the suitable components. The work in [55] presents two algorithms to rebuild the kernel. The key point is to establish a bilinear relation between the ciphertext and the kernel whereby one can retrieve the plaintext by solving a linear

system. More precisely, the bilinear maps yield a bilinear system in terms of the plaintext **x** and the ciphertext **c**.

4 MULTIVARIATE PUBLIC KEY ENCRYPTION SCHEMES

Related works. Designing efficient and secure multivariate encryption scheme is a challenging task. Research on MPKCs were not very successful in the mid 1980s. In Eurocrypt 1988, Matsumoto and Imai [78] proposed C* cryptosystem which is also referred as MI cryptosystem. This was the first multivariate encryption scheme based on the idea of a BigField families of multivariate encryption schemes where the central map is defined over an extension field. The cryptosystem C* was defeated in 1995 by Patarin's algebraic attack via linearization equations [83]. In 1996, Patarin [84] designed the ***Hidden Field Equation*** (**HFE**) cryptosystem. But, Kipnis and Shamir [73] found a way of recovering the secret key of HFE cryptosystem and proposed MinRank attack in 1999. Later in 2001, Courtois [26] improved the Kipnis-Shamir MinRank attack. Following this work, multivariate encryption schemes like ***Perturbed Matsumoto-Imai with Plus*** (**PMI+**) by Ding [31] in 2004 and ***Internally Perturbed HFE with Plus*** (**IPHFE+**) by Ding and Schmidt [41] in 2005 were proposed using perturbation from the Big Field families of multivariate encryption schemes. These designs are not efficient in terms of key storage and speed. The scheme ***HFE with Minus*** (**HFE-**) has been considered as a candidate of HFE schemes. However, HFE- is not efficienct in terms of speed similar to IPHFE+ and PMI+. Furthermore, the security of HFE- seems to be questionable due to an attack by Vates and Smith-tone [109] in 2017. In 2008, Chen et al. [19] suggested a multivariate encryption scheme MultiHFE, a multivariate version of HFE. Although the scheme was very efficient, it was broken by Bettale et al. [6] in 2013 using a generalization of the Kipnis-Shamir attack against HFE construction that exploits the low rank property of the system. In 2013, Tao et al. [105] came up with a new and efficient multivariate encryption scheme Simple Matrix that uses a large matrix algebra structure. The idea was improved later in 2015 by Tao et al. [107]. The security of Simple Matrix encryption scheme has been studied carefully by Moody et al. [80] in 2014. In 2014, Porras et al. [98] proposed ZHFE which is an interesting construction of multivariate encryption scheme that overcomes the security weakness of HFE-based multivariate encryption schemes. The idea of the construction is inspired by the first steps of the *Zhuang-Zi* algorithm by Ding et al. [33]. In 2017, Ikematsu et al. [67] presented a new efficient algorithm for the secret key generation for ZHFE that avoids slow key generation of the original ZHFE. However, ZHFE seems to be vulnerable due to a key recovery attack by Cabarcas et al. [14] in 2017. In 2015, a new encryption scheme SRP (*Square, Rainbow, and Plus*) by Yasuda and Sakurai [114] came up using the stucture of Square encryption scheme [23], Rainbow signature scheme [42], and Plus technique [34]. The scheme SRP fails to be an ambitious encryption scheme due to an attack by Perlner et al. [89] in 2017. The encryption scheme HFERP (*HFE, Rainbow and Plus*), introduced by Ikematsu et al. [69] in 2018, utilizes a similar construction as SRP with an HFE primitive replacing the Square polynomial and seems to be secure against all existing attacks. In 2015, Okumura [81] presented a completely new method of building a public key encryption scheme *Diophantine Equations Cryptosystem* (DEC) based on Diophantine equations of degree increasing type. He used an analogous method to the ***Algebraic Surface Cryptosystem*** (**ASC**) proposed by Akiyama et al. [1] in 2009. DEC also could not survive due to a polynomial time attack by Ding et al. [37] in 2016. In 2017, Ustimenko [108] proposed a new construction based on Eulerian equation without giving any security analysis. In the same year, the multivariate encryption scheme EFLASH was proposed by Cartor and Smith-Tone [17] that uses the central map of MI cryptosystem. The crypanalysis of Oygarden [82] in 2020 shows that EFLASH does not offer the desired level of security. In 2018, Yasuda [113] introduced a new mathematical problem, constrained MQ problem, obtained from the MQ problem and proposed an encryption technique using *pq*-method

Table 1. Comparison of Multivariate Encryption Schemes

Scheme	Advantages	Disadvantages	Proposed Attacks
MI [78]	first multivariate scheme	not secure	algebraic attack [83]
HFE [84]	efficient than MI	not secure	MinRank attacks ([73], [26])
MultiHFE [19]	multivariate version of HFE	weak security	MinRank attack [6]
Simple Matrix [105]	no low rank property of the central map, fast decryption	non-negligible decryption failure probability	structural attack [80]
Improved Simple Matrix [107]	negligible decryption failure probability, fast decryption	weak security	combinatorial rank attack [2]
ZHFE [98]	Efficient than basic HFE variants	slow key generation	MinRank attack [14]
SRP [114]	small blow up factor between plaintext and ciphertext space	minrank weakness	MinRank attack [89]
HFERP [69]	small blow up factor between plaintext and ciphertext space, no minrank weakness	decryption is slower than SRP	–
DEC [81]	efficient, short key sizes	can be broken with high probability under some assumptions	attack via weighted LLL reduction [37]
EFLASH [17]	efficient decryption strategy	decryption failure possibility	algebraic cryptanalysis [82]
[20]	new central trapdoor	weak security	algebraic Attack [68]
[113]	enhances the security of any weak scheme	comparatively large key sizes	–

whose security relies on the hardness of solving the constrained MQ problem. For prime numbers p, q with $p < q$, the pq-method transforms an encryption scheme in MPKC over a field $\mathbb{F}$ having cardinality p, to an encryption scheme over the field $\mathbb{E}$ having cardinality q. Later in 2020, another encryption scheme was proposed by Yasuda et al. [115] exploiting polynomial equations over real numbers. In the same year, Chen et al. [20] proposed a new encryption scheme for multivariate quadratic systems. Later, Ikematsu et al. [68] showed that even if the minus and plus modifiers are used to prevent known attacks like linear equations attack, MinRank attack, and algebraic attack, an attack exploiting linear algebra is applicable for this scheme. Very recently, Smith-Tone [103] came up with a new approach to design a multivariate encryption scheme inspired by the concept of random linear codes.

Multivariate public key encryption is an active area of research nowadays. Table 1 shows a rough comparison of the advantages and disadvantages of promising multivariate public key encryption schemes. We provide below a description of some selected multivariate encryption schemes to illustrate the difference of the procedures among the several variants of multivariate public key encryption schemes.

4.1 Simple Matrix ([107])

In 2015, Tao et al. [107] suggested Simple Matrix scheme using a large matrix algebra structure. The scheme is an improvement of the construction by Tao et al. [105]. The protocol executes the following steps.

Description of the scheme

— Setup$(1^\lambda) \rightarrow$ pp: On input a security parameter λ, a trusted authority chooses a finite field $\mathbb{F}$ having q elements and positive integers r, s, u, v, m, n where $m = s(u + v)$, $s \geq r$ and $(n - r(u + v - s))(n - r(u + v - s) + 1) \leq 2m$. The user publishes the public parameters $\text{pp} = (\mathbb{F}, q, r, s, u, v, m, n)$.

— KeyGen(pp) $\rightarrow$ (pk, sk): A user takes public parameter pp as input and executes the following steps.

(i) Consider three matrices $A = A(\mathbf{z}) = (a_{i,j})_{s\times r}$, $B = B(\mathbf{z}) = (b_{i,j})_{r\times u}$ and $C = C(\mathbf{z}) = (c_{i,j})_{r\times v}$ where $a_{i,j}$ are chosen randomly from the set $\{z_1, z_2, \ldots, z_n\}$, $\mathbf{z}$ represents the vector $(z_1, z_2, \ldots, z_n)$, $b_{i,j}$ and $c_{i,j}$ are randomly chosen linear combinations of the elements from $\{z_1, z_2, \ldots, z_n\}$. Then set $D = AB = (d_{i,j})_{s\times u}$, $E = AC = (e_{i,j})_{s\times v}$ and construct the central map $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ defined as $F(\mathbf{z}) = (D(\mathbf{z}), E(\mathbf{z}))$ consisting of $m = s(u + v)$ components of the matrices $D = D(\mathbf{z})$ and $E = E(\mathbf{z})$. Note that,

$$F = (d_{1,1}, d_{1,2}, \ldots, d_{1,u}; d_{2,1}, d_{2,2}, \ldots, d_{2,u}; \ldots; d_{s,1}, d_{s,2}, \ldots, d_{s,u}; e_{1,1}, e_{1,2}, \ldots, e_{1,v};$$
$$e_{2,1}, e_{2,2}, \ldots, e_{2,v}; \ldots; e_{s,1}, e_{s,2}, \ldots, e_{s,v}).$$

(ii) Select two invertible linear maps $S : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ and $T : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ and finally compute the map $P = S \circ F \circ T : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ where $\circ$ stands for map composition.

(iii) Set the public key $\mathsf{pk} = P$ and secret key $\mathsf{sk} = (S, T, A, B, C)$. The public key pk is made public while the secret key sk is kept secret to the user.

— Encrypt$(\mathsf{pp}, \mathsf{pk}, \mathbf{x}) \rightarrow \mathbf{c}$: An encryptor uses public parameter pp and his public key $\mathsf{pk} = P$ and produces a ciphertext $\mathbf{c} \in \mathbb{F}^m$ for a message $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ by generating $\mathbf{c} = P(\mathbf{x})$ and sends $\mathbf{c}$ through a public channel.

— Decrypt$(\mathsf{pp}, \mathsf{sk}, \mathbf{c}) \rightarrow \mathbf{x}$: A decryptor, having secret key $\mathsf{sk} = (S, T, A, B, C)$, performs the following steps to recover the plaintext $\mathbf{x}$ from the ciphertext $\mathbf{c} = P(\mathbf{x})$:

(i) Compute $\mathbf{y} = (y_1, y_2, \ldots, y_m) = S^{-1}(\mathbf{c})$ where $m = s(u + v)$ and set two matrices $\overline{D}$ and $\overline{E}$ where

$$\overline{D} = \begin{pmatrix} y_1 & y_2 & \cdots & y_u \\ y_{u+1} & y_{u+2} & \cdots & y_{2u} \\ & \cdots & & \\ y_{(s-1)u+1} & y_{(s-1)u+2} & \cdots & y_{su} \end{pmatrix}, \overline{E} = \begin{pmatrix} y_{su+1} & y_{su+2} & \cdots & y_{su+v} \\ y_{su+v+1} & y_{su+v+2} & \cdots & y_{su+2v} \\ & \cdots & & \\ y_{su+(s-1)v+1} & y_{su+(s-1)v+2} & \cdots & y_{su+sv} \end{pmatrix}.$$

(ii) Find a vector $\mathbf{z} \in \mathbb{F}^n$ satisfying $F(\mathbf{z}) = \mathbf{y}$ as follows.

(a) Let $\overline{A} = A(\mathbf{z})$, $\overline{B} = B(\mathbf{z})$ and $\overline{C} = C(\mathbf{z})$. If the rank of the matrix $\overline{A}$ is r, then an $r \times s$ matrix W (left inverse of $\overline{A}$) exists and satisfies $W\overline{A} = I$ where I is the $r \times r$ identity matrix. Also compute $\overline{D} = \overline{D}(\mathbf{z})$ and $\overline{E} = \overline{E}(\mathbf{z})$ from $\mathbf{y} = S^{-1}(\mathbf{c})$ satisfying $\overline{D} = \overline{A}\,\overline{B}$ and $\overline{E} = \overline{A}\,\overline{C}$.

(b) Construct the equations $W\overline{D} = \overline{B}$, $W\overline{E} = \overline{C}$ as $W\overline{A} = I$. By interpreting the elements of W as new variables, obtain $r(u + v)$ linear equations in $sr + n$ unknowns corresponding to sr variables for W and n variables $z_1, z_2, \ldots, z_n$.

(c) Eliminate the sr elements of W from these equations and solve the system of $r(u + v - s)$ linear equations in the n variables $z_1, z_2, \ldots, z_n$. The dimension of the solution space of this system is very small. Let *Gaussian elimination* eliminates U unknown variables. By writing these U variables as linear combinations of the remaining unknown variables and substituting these equations into the central polynomials of $F(\mathbf{z}) = \mathbf{y}$, obtain a new system of $m = s(u + v)$ quadratic equations in the remaining $n - U$ unknown variables. When the number $n - U$ is small enough, the system can be solved efficiently by Relinearization technique of Kipnis et al. [71]. Note that the condition $(n - r(u + v - s))(n - r(u + v - s) + 1) \leq 2m$ is required to apply the Relinearization technique for solving the system.

(iii) Finally, recover the plaintext $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ by computing $T^{-1}(\mathbf{z})$.

We note that, $T^{-1}(\mathbf{z}) = T^{-1}(F^{-1}(\mathbf{y})) = T^{-1}(F^{-1}(S^{-1}(\mathbf{c})) = T^{-1} \circ F^{-1} \circ S^{-1}(\mathbf{c}) = (S \circ F \circ T)^{-1}(\mathbf{c}) = P^{-1}(\mathbf{c}) = \mathbf{x}$ where $\mathbf{c} = P(\mathbf{x})$.

Security analysis: Smaller fields are not appropriate to avoid the larger size public keys. Tao et al. [107] recommended that the field $\mathsf{GF}(2^{32})$ is most suitable for the scheme Simple Matrix. For field $\mathsf{GF}(2^{32})$, the probability of decryption failure is about 2^{-64} which is less than the probability of decryption failures for smaller fields $\mathsf{GF}(2^{16})$ or $\mathsf{GF}(2^8)$. The other parameters are set as $s = r + 1$, $u = r$, $v = r$, $m = 2r(r + 1)$, $n = r(r + 1)$. Tao et al. [107] analyzed the security of Simple Matrix for all known attacks against multivariate public key encryption schemes including (high order) *linearization equation* attacks, *rank* attacks, *direct/algebraic* attacks. The linearization equation attack was introduced by Patarin [83]. The high order linearization equation attack was proposed by Ding et al. [35]. For reasonably chosen parameters, high order linearization attacks against Simple Matrix are shown to be completely impractical. There are two different types of

rank attacks - MinRank attack/LowRank attack [59] and HighRank attack [24]. The complexity of the MinRank attack against Simple Matrix is $O(q^{4r}r^6)$ while the complexity of the HighRank attack is $O(q^{2r}r^{12})$ where q is the number of elements in the field $\mathbb{F}$ and the parameter r is the number of columns of the matrix A. In the HighRank attack, an adversary randomly chooses linear combinations of the public polynomials intending to select a polynomial whose rank is significantly less than full rank. The rank attacks against Simple Matrix are shown to be infeasible with a proper choice of the parameters. A careful complexity estimation of direct attacks was also provided by Tao et al. [107]. Later in the year 2014, a key recovery attack on Simple Matrix scheme by Moody et al. [80] using a differential invariant property of the core map is shown. More interestingly, from an analysis on a MinRank attack method by Apon et al. [2], it is evident that the security of this improved version that uses rectangular matrices is quite weak than that of the square version, although the strategy of using rectangular matrices lowers the decryption failure rate. Surprisingly, the decryption failures can still be exploited in a concrete reaction attack [2] that diminishes security. The complexity of the MinRank method is $O(n^\omega q^{2s+1-r})$ while it is $O(n^\omega q^{2s-r})$ in case of reaction attack where ω is a linear algebra constant. Therefore, this encryption technique using matrices needs significant attention.

Efficiency: The key generation algorithm needs two matrix multiplications over $\mathbb{F}$ while the encryption is a simple evaluation of the quadratic map P at $\mathbf{x} \in \mathbb{F}^n$. The decryption requires solving a system of $r(u+v)$ linear equations in $sr+n$ unknowns by Gaussian elimination and Relinearization technique which is costly. The size of the secret key sk is large as sk contains three large matrices along with two linear transformations.

Remark 1 (Decryption Fails when Rank($\overline{A}$) $< r$). The probability of decryption failures is approximately $\frac{1}{q^{s-r+1}}$. By an appropriate choice of the parameters s and r, the probability of decryption failure can be reduced to a negligible value. However, finding a general solution is still an open problem.

4.2 ZHFE ([98])

In 2014, Porras et al. [98] presented ZHFE employing a new strategy to use HFE polynomials in order to recover low rank weakness of basic HFE schemes. The formal description of the protocol is given below.

Description of the scheme

- Setup$(1^\lambda) \rightarrow$ pp: On input a security parameter λ, a trusted authority selects a finite field $\mathbb{F}$ having q elements, fixes a positive integers n, d_0 and considers the field extension $K = \mathbb{F}[y]/(g(y))$ where $g(y) \in \mathbb{F}[y]$ is an irreducible polynomial of degree n. The trusted authority publishes the public parameters pp $= (\mathbb{F}, q, K, n, d_0)$.
- KeyGen(pp) $\rightarrow$ (pk, sk): A user takes public parameter pp as input and performs the following steps.
  (i) Select two high degree HFE polynomials $F, \tilde{F}$ and construct a low degree polynomial Ψ from F and $\tilde{F}$ as follows adapting the technique of Porras et al. ([97]).
  (a) Let $F(X) = \sum_{0\le j\le i}^{n-1} a_{i,j}X^{q^i+q^j} + \sum_{i=0}^{n-1} b_iX^{q^i} + c$, $\widetilde{F}(X) = \sum_{0\le j\le i}^{n-1} \tilde{a}_{i,j}X^{q^i+q^j} + \sum_{i=0}^{n-1} \tilde{b}_iX^{q^i} + \tilde{c}$ be two HFE polynomials over K where the coefficients $a_{i,j}, b_i, c, \tilde{a}_{i,j}, \tilde{b}_i, \tilde{c} \in K$ are to be determined.
  (b) Construct a low degree polynomial

$$\Psi = X(\alpha_1F_0 + \cdots + \alpha_nF_{n-1} + \beta_1\widetilde{F}_0 + \cdots + \beta_n\widetilde{F}_{n-1}) + X^q(\alpha_{n+1}F_0 + \cdots + \alpha_{2n}F_{n-1} + \beta_{n+1}\widetilde{F}_0 + \cdots + \beta_{2n}\widetilde{F}_{n-1}),$$

of Hamming weight three with $F_i(X) = [F(X)]^{q^i}$, $\widetilde{F}_i(X) = [\widetilde{F}(X)]^{q^i}$, $i = 0, 1, \ldots, n-1$. The coefficients $a_{ij}, b_i, c, \tilde{a}_{ij}, \tilde{b}_i, \tilde{c} \in K$ in F and $\tilde{F}$ as well as the scalars $\alpha_j, \beta_j \in K$, $j = 1, 2, \ldots, 2n$ are determined in such a way that makes the $\deg(\Psi) \leq d_0$ and Ψ can be easily inverted using Berlekamp algorithm.

(c) Select scalars α_j and β_j randomly to produce a linear system whose solution provides the coefficients of F and $\widetilde{F}$. The linear system, obtained by equating coefficients of X^d in Ψ equal to zero for $d > d_0$, has more variables than equations. Thus nontrivial solutions can be obtained.

(ii) Choose two invertible affine transformations $S : \mathbb{F}^n \to \mathbb{F}^n$ and $T : \mathbb{F}^{2n} \to \mathbb{F}^{2n}$ and finally construct a map defined by $P = T \circ (\phi \times \phi) \circ G \circ \phi^{-1} \circ S$: $\mathbb{F}^n$ to $\mathbb{F}^{2n}$ where $G = (F, \widetilde{F})$ is the core map, $\phi : K \to \mathbb{F}^n$ is the isomorphism defined by $\phi(u_1 + u_2 y + \cdots + u_n y^{n-1}) = (u_1, u_2, \ldots, u_n)$ and $\circ$ is the map composition.

(iii) Set the public key as $\mathsf{pk} = P$ and secret key as $\mathsf{sk} = (S, T, \Psi, \{(\alpha_j, \beta_j), j = 1, 2, \ldots 2n\})$. The public key pk is made public while the secret key sk is kept secret to the user.

— $\mathsf{Encrypt}(\mathsf{pp}, \mathsf{pk}, \mathbf{x}) \to \mathbf{c}$: On input the public parameter pp, public key pk and the message $\mathbf{x}$, the encryptor computes the ciphertext $\mathbf{c} = (c_1, c_2, \ldots, c_{2n}) = P(\mathbf{x}) \in \mathbb{F}^{2n}$ for a plaintext $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ using his public key pk and sends the ciphertext $\mathbf{c}$ through a public channel.

— $\mathsf{Decrypt}(\mathsf{pp}, \mathsf{sk}, \mathbf{c}) \to \mathbf{x}$: The decryptor, having public parameter pp, secret key $\mathsf{sk} = (S, T, \Psi, \{(\alpha_j, \beta_j), j = 1, 2, \ldots 2n\})$ and the ciphertext $\mathbf{c}$, performs the following steps to recover the message $\mathbf{x}$.

(i) Compute $(w_1, w_2, \ldots, w_{2n}) = T^{-1}(\mathbf{c}) = T^{-1}(c_1, c_2, \ldots, c_{2n})$ and calculate $(Y_1, Y_2) = (\phi^{-1}(w_1, w_2, \ldots, w_n), \phi^{-1}(w_{n+1}, w_{n+2}, \ldots, w_{2n}))$.

(ii) Invert the core map $G = (F, \widetilde{F})$ by solving the equation $G(X) = (Y_1, Y_2)$. The solutions of the equation are part of the roots of the low degree polynomial Ψ', obtained from Ψ and (Y_1, Y_2) as in the following proposition.

Proposition 4.1 ([97]). *The set of pre-images of (Y_1, Y_2) under the map $G = (F, \widetilde{F})$ is a subset of the roots of the low degree polynomial*

$$\Psi' = \Psi - \sum_{j=1}^{2} X^{q^{j-1}} \sum_{i=1}^{n} \alpha_{i+n(j-1)} Y_1^{q^{i-1}} + \beta_{i+n(j-1)} Y_2^{q^{i-1}}$$

where (Y_1, Y_2) be an element in $Im(G) \subseteq K \times K$.

Determine the set $\mathcal{U} = \{X \in K | \Psi'(X) = 0\}$ consisting of the solutions of $G(X) = (Y_1, Y_2)$. For each $X \in \mathcal{U}$, compute $\phi(X) \in \mathbb{F}^n$ and perform the transformation $S^{-1}(\phi(X))$ $\forall X \in \mathcal{U}$.

(iv) Finally, using the public key P as redundancy information, find the original plaintext. Note that P is an injective mapping. Using ciphertext $\mathbf{c}$ and the candidate plaintext $\mathbf{x} = S^{-1}(\phi(X))$, $X \in \mathcal{U}$, check whether $P(\mathbf{x}) = \mathbf{c}$ or not and recover the correct plaintext.

We note that, $S^{-1}(\phi(X)) = S^{-1}(\phi(G^{-1}(Y_1, Y_2))) = S^{-1}(\phi(G^{-1} \circ \phi^{-1} \times \phi^{-1}(T^{-1}(\mathbf{c})))) = (S^{-1} \circ \phi \circ G^{-1} \circ \phi^{-1} \times \phi^{-1} \circ T^{-1})(\mathbf{c}) = P^{-1}(\mathbf{c}) = \mathbf{x}$.

Security analysis: The practical parameters for ZHFE were suggested as $(q, n, d_0) = (7, 55, 105)$ by Porras et al. [98]. *Direct algebraic* attack by Faugere and Joux [52] and the KS MinRank attack by Kipnis, and Shamir [73] are two attacks that have broken the security of multivariate public key encryption schemes based on HFE polynomials. Although ZHFE belongs to the same family, it overcomes the weakness against direct algebraic attack. Porras et al. [98] claimed that KS MinRank attack does not succeed for ZHFE due to the use of two high degree HFE polynomials in constructing the core map. An improved security estimate is provided by Zhang et al. [118] for the original parameters of ZHFE. In 2016, Perlner and Smith-Tone [90] studied the rank structure of ZHFE,

discussed parameters for ZHFE against rank and direct attacks and investigated the security against differential adversaries. Moreover, the work presents a modification of ZHFE engaging the minus modifier which optimizes the key size while maintaining the security and performance properties as ZHFE. Later in the year 2017, Cabarcas et al. [14] showed that although the core map in ZHFE uses two HFE polynomials of high degree, their low rank property makes ZHFE vulnerable to KS MinRank attack whereby they recovered a secret key for ZHFE with $(q, n, d_0) = (7, 55, 105)$ in approximately 2^{64} operations. The expected complexity of the attack is $O(n^{(\lceil \log_q(d_0) \rceil + 2)\omega})$ where d_0 is the degree bound for ZHFE and $2 < \omega \leq 3$ is a linear algebra constant.

Efficiency: The key generation algorithm is time consuming as the secret key computation involves constructing a low degree polynomial Ψ from two high degree HFE polynomials. The encryption process is just an evaluation of the map P at $\mathbf{x} \in \mathbb{F}^n$. The decryption needs invocation of Berlekamp algorithm which is much faster for ZHFE compared to other HFE-based schemes. Note that ZHFE requires solution of a low degree polynomial Ψ for decryption while other HFE based schemes needs solution of higher degree polynomial.

4.3 HFERP ([69])

HFERP is introduced by Ikematsu et al. [69] in the year 2018 using HFE polynomial, Rainbow signature scheme and Plus technique. This scheme is an improvement of the SRP encryption scheme proposed by Yasuda and Sakurai [114]. The scheme is described below.

Description of the scheme

— Setup$(1^\lambda) \rightarrow$ pp: Taking input the security parameter λ, a trusted authority executes the following steps to output public parameters pp.

(i) Fix a finite field $\mathbb{F}$ having q elements and degree of extension d of K, an extension field over $\mathbb{F}$.

(ii) Choose h positive integers $o_1, o_2, \ldots, o_h$ and set
$$n = d + o_1 + \cdots + o_h - l,\ m = d + o_1 + \cdots + o_h + hr + s,\ n' = d + o_1 + \cdots + o_h$$
where r, s, l are three positive integers and h is referred as the number of layers.

(iii) Publish the public parameters pp $= (\mathbb{F}, d, K, o_1, o_2, \ldots, o_h, h, r, s, n, n', m)$.

— KeyGen(pp) $\rightarrow$ (pk, sk): On input public parameter pp, a user performs the following steps and outputs public-secret key pair (pk, sk).

(i) Choose an HFE polynomial f with high rank. Note that $f(X) \in K$ for $X \in K$. Let π_d be the projection onto the first d coordinates defined by $\pi_d(a_1, a_2, \ldots, a_{n'}) = (a_1, a_2, \ldots, a_d)$ and $\phi : K \rightarrow \mathbb{F}^d$ be a linear isomorphism over $\mathbb{F}$. Then construct a multivariate quadratic map $G_H : \mathbb{F}^{n'} \rightarrow \mathbb{F}^d$ using π_d , ϕ and f as $G_H : \mathbb{F}^{n'} \xrightarrow{\pi_d} \mathbb{F}^d \xrightarrow{\phi^{-1}} K \xrightarrow{f} K \xrightarrow{\phi} \mathbb{F}^d$.

(ii) For each layer $1 \leq k \leq h$, set $v_k = d + o_1 + \cdots + o_{k-1}$, $V_k = \{1, 2, \ldots, v_k\}$, $O_k = \{v_k + 1, v_k + 2, \ldots, v_k + o_k\}$ and construct a multivariate quadratic map $G_{R,k} : \mathbb{F}^{n'} \rightarrow \mathbb{F}^{o_k + r}$ by choosing $o_k + r$ multivariate quadratic polynomials of the form
$$g(x_1, x_2, \ldots, x_{n'}) = \sum_{i \in O_k, j \in V_k} \alpha_{i,j} x_i x_j + \sum_{i,j \in V_k, i \leq j} \beta_{i,j} x_i x_j + \sum_{i \in V_k \cup O_k} \gamma_i x_i + \eta,$$
where $\alpha_{i,j}, \beta_{i,j}, \gamma_i, \eta$ are randomly chosen from $\mathbb{F}$. Define a multivariate map $G_R : \mathbb{F}^{n'} \rightarrow \mathbb{F}^{o_1 + \cdots + o_h + hr}$ by setting $G_R = G_{R,1} || G_{R,2} || \cdots || G_{R,h}$.

(iii) Generate another multivariate quadratic map $G_P : \mathbb{F}^{n'} \rightarrow \mathbb{F}^s$ which consists of s random multivariate quadratic polynomials of the form
$$g'(x_1, x_2, \ldots, x_{n'}) = \sum_{1 \leq i \leq j \leq n'} \alpha'_{i,j} x_i x_j + \sum_{1 \leq i \leq n'} \beta'_i x_i + \eta',$$

where $\alpha_{i,j}^{'}, \beta_i^{'}, \eta^{'}$ are randomly chosen from $\mathbb{F}$. Form the central map $G : \mathbb{F}^{n^{'}} \rightarrow \mathbb{F}^m$ by setting $G = G_H||G_R||G_P$.

(iv) Select an affine embedding map $S : \mathbb{F}^n \rightarrow \mathbb{F}^{n^{'}}$ and an affine isomorphism $T : \mathbb{F}^m \rightarrow \mathbb{F}^m$ and finally compute $F = T \circ G \circ S : \mathbb{F}^n \rightarrow \mathbb{F}^m$ where $\circ$ stands for map composition.

(v) Set the public key $\mathsf{pk} = F$ which is made public whereas the secret key $\mathsf{sk} = (G, S, T)$ is kept secret to the user. Note that the component G_H of G contains the information of the HFE polynomial f.

— $\mathsf{Encrypt}(\mathsf{pp}, \mathsf{pk}, \mathbf{x}) \rightarrow \mathbf{c}$: For a plaintext $\mathbf{x} \in \mathbb{F}^n$, the encryptor computes the ciphertext as $\mathbf{c} = F(\mathbf{x}) \in \mathbb{F}^m$ using the public key $\mathsf{pk} = F$ and sends $\mathbf{c}$ over a public channel.

— $\mathsf{Decrypt}(\mathsf{pp}, \mathsf{sk}, \mathbf{c}) \rightarrow \mathbf{x}$: For a ciphertext $\mathbf{c} = (c_1, c_2, \ldots, c_m) \in \mathbb{F}^m$, the decryptor uses his secret key $\mathsf{sk} = (G, S, T)$ where $S : \mathbb{F}^n \rightarrow \mathbb{F}^{n^{'}}$ and $T : \mathbb{F}^m \rightarrow \mathbb{F}^m$ are affine maps and $G : \mathbb{F}^{n^{'}} \rightarrow \mathbb{F}^m$ is the central map parsed as $G = G_H||G_R||G_P$ where $G_H : \mathbb{F}^{n^{'}} \rightarrow \mathbb{F}^d$, $G_R : \mathbb{F}^{n^{'}} \rightarrow \mathbb{F}^{o_1+\cdots+o_h+hr}$ and $G_P : \mathbb{F}^{n'} \rightarrow \mathbb{F}^s$ and proceeds as follows.

(i) Compute $B = (b_1, b_2, \ldots, b_m) = T^{-1}(\mathbf{c})$, set $B_d = (b_1, b_2, \ldots, b_d)$ and finds $B_0 = \phi^{-1}(B_d)$ where $\phi : K \rightarrow \mathbb{F}^d$ is a linear isomorphism over $\mathbb{F}$. Then extract f from the component G_H of G in the secret key sk, invert f using the Berlekamp algorithm to find the pre-image $R = f^{-1}(B_0)$ of B_0 and compute $D_0 = \phi(R) \in \mathbb{F}^d$.

(ii) For each $k = 1, 2, \ldots, h$, set $B_k = (b_{m_k+1}, b_{m_k+2}, \ldots, b_{m_k+o_k+r})$ where $m_k = v_k + (k-1)r$, construct a set of linear equations $G_{R,k}(D_{k-1}, X_k) = B_k$ with respect to $X_k = (x_{v_k+1}, x_{v_k+2}, \ldots, x_{v_k+o_k})$ and solve this system of o_k variables to get the solution D_k. Note that D_{k-1} and B_k are known and X_k is unknown.

For instance, let $k = 1$. Then $v_1 = d$, $V_1 = \{1, 2, \ldots, d\}$, $O_1 = \{d+1, d+2, \ldots, d+o_1\}$, $m_1 = v_1 = d$. Using the values of $D_0 = \{x_1, x_2, \ldots, x_d\}$, solve the system of $o_1 + r$ linear equations in the o_1 variables $x_{d+1}, \ldots, x_{d+o_1}$ given by $G_{R,1}(D_0, X_1) = B_1$ i.e., $G_{R,1}(x_1, x_2, \ldots, x_d, x_{d+1}, \ldots, x_{d+o_1}) = (b_{d+1}, b_{d+2}, \ldots, b_{d+o_1+r})$. Note that the multivariate polynomials used for defining the map $G_{R,1}$ forms a system of linear equations as the vinegar variables $x_j,\ j \in V_1 = \{1, 2, \ldots, d\}$ are known. Then the system can be solved by gaussian elimination.

(iii) Finally compute $D = D_0||D_1||\cdots||D_h$ and recover the plaintext $\mathbf{x}$ by calculating $S^{-1}(D)$.

We note that, $S^{-1}(D) = S^{-1}(G^{-1}(B)) = S^{-1}(G^{-1}(T^{-1}(\mathbf{c}))) = (S^{-1} \circ G^{-1} \circ T^{-1})(\mathbf{c}) = F^{-1}(\mathbf{c}) = \mathbf{x}$ as $\mathbf{c} = F(\mathbf{x})$.

Security analysis. Ikematsu et al. [69] proposed the following single-layer parameters for 80-bit security $q = 3, d = 42, o = 21, r = 15, s = 17, l = 0, D = 3^7 + 1; q = 3, d = 63, o = 21, r = 11, s = 10, l = 0, D = 3^7 + 1$ and the following double-layer parameters for 128-bit security $q = 3, d = 85, o_1 = o_2 = 70, r = 89, s = 61, l = 0, D = 3^7 + 1; q = 3, d = 60, o_1 = o_2 = 40, r = 23, s = 40, l = 0, D = 3^9 + 1$ where D is the bound of the HFE polynomial.

The scheme is proven to be secure against direct attack by Faugere et al. [52], MinRank attack by Perlner et al. [89], rank attacks by Goubin et al. [59] and UOV invariant attack by Kipnis et al. [71]. The detailed complexity estimation of those attacks is illustrated in [69]. Ikematsu et al. [69] provided a concrete bound of the degree of regularity of public key of HFERP. The complexity of the algebraic attack against HFERP is $O(n^{2\lceil \log_q D \rceil + 6})$ when the degree of regularity is at least $\lceil \log_q D \rceil + 2$ for sufficiently large n and small odd q. The system of multivariate quadratic equations obtained from any ciphertext in HFERP behave like a system of random quadratic equations with respect to direct attacks. When minors modeling method is applied to HFERP, the estimated complexity of the MinRank attack is $O(m^{2\lceil \log_q D \rceil + 2})$.

Efficiency. The key generation involves composition of certain maps whereas encryption requires evaluation of central core map $F = T \circ G \circ S : \mathbb{F}^n \rightarrow \mathbb{F}^m$ at $\mathbf{x} \in \mathbb{F}^n$. Decryption needs execution of Berlekamp algorithm to find the preimage under an HFE polynomial which is utilized in solving system of linear equations in each layer. As the secret key contains the data used in constructing the central map G together with two affine maps, the size of the secret key is large.

4.4 EFLASH ([17])

The scheme EFLASH is presented by Cartor et al. [17] in 2017. The protocol executes the following steps.

Description of the scheme

- Setup$(1^\lambda) \rightarrow$ pp: A trusted authority takes security parameter λ as input, selects n, m, d such that $m \geq n$ and $m < d$ and chooses a finite field $\mathbb{F}$ having q elements. Here $d(> n)$ is the degree of the extension field K over $\mathbb{F}$. It publishes the public parameter pp $= (\mathbb{F}, q, n, d, m, K)$.
- KeyGen(pp) $\rightarrow$ (pk, sk): On input public parameter pp, a user performs the following steps and outputs, public-secret key pair (pk, sk).
  (i) Set the map $f : K \longrightarrow K$ defined by $f(x) = x^{q^\theta+1}$ for an integer θ, select two affine maps $S : \mathbb{F}^d \rightarrow \mathbb{F}^d$ and $T : \mathbb{F}^d \rightarrow \mathbb{F}^d$ and finally compute $P = \pi \circ T \circ \phi^{-1} \circ f \circ \phi \circ S \circ \tau$: $\mathbb{F}^n \rightarrow \mathbb{F}^m$ where $\phi : \mathbb{F}^d \rightarrow K$ be a linear isomorphism, τ is a linear embedding from $\mathbb{F}^n \rightarrow \mathbb{F}^d$, $\pi : \mathbb{F}^d \rightarrow \mathbb{F}^m$ be a linear projection and $\circ$ is the map composition.
  (ii) Set the public key pk $= P$ which is made public whereas the secret key is set as sk $= (S, T, f, \tau)$ which is kept secret to the user.
- Encrypt(pp, pk, $\mathbf{x}$) $\rightarrow \mathbf{c}$: To encrypt a message $\mathbf{x} \in \mathbb{F}^n$, the encryptor computes the ciphertext $\mathbf{c} = P(\mathbf{x}) \in \mathbb{F}^m$ using his public key pk $= P$ and sends $\mathbf{c}$ over a public channel.
- Decrypt(pp, sk, $\mathbf{c}$) $\rightarrow \mathbf{x}$: Having secret key sk $= (S, T, f, \tau)$ and a ciphertext $\mathbf{c}$, the decryptor proceed as follows to recover the message.
  (i) Generate $\mathbf{c}^{'} = \mathbf{c}||\mathbf{c}_a \in \mathbb{F}^d$ appending every possible $\mathbf{c}_a \in \mathbb{F}^{d-m}$ to $\mathbf{c}$ where $a = d - m$ and compute $\mathbf{v}$=$T^{-1}(\mathbf{c}^{'})$. Here the plaintext $\mathbf{x}$ and the output $\mathbf{v}$ of $T^{-1}(\mathbf{c}^{'}) = \phi^{-1} \circ f \circ \phi \circ S \circ \tau$ are related by linearization equations, $\mathbf{u} = \phi \circ U(\mathbf{x})$, $\mathbf{v}^{'} = \phi(\mathbf{v})$ where $U = S \circ \tau$ (technique similar to that used in Patarin et al. [83]). Observe that $\mathbf{v} = T^{-1}(\mathbf{c}') = \phi^{-1} \circ f \circ \phi \circ S \circ \tau(\mathbf{x}) = \phi^{-1} \circ f \circ \phi \circ U(\mathbf{x})$ and $\mathbf{v}^{'} = \phi(\mathbf{v}) = f \circ \phi \circ U(\mathbf{x}) = f(\mathbf{u})$ as $\mathbf{u} = \phi(U(\mathbf{x}))$.
  (ii) Solve the linear system defined by the linearization equations. If the linear system gives a solution $\mathbf{x}$ satisfying $\mathbf{c} = P(\mathbf{x})$, the process stops.

Security analysis. Cartor and Smith-Tone [17] suggested the parameters of EFLASH as (q, n, d, m) $=(2, 80, 101, 96)$ for 80-bit and $(q, n, d, m) = (2, 134, 159, 150)$ for 128-bit classical security levels. They also suggested $(q, n, d, m) = (2, 160, 181, 176)$ for 80-bit and $(q, n, d, m) = (2, 256, 279, 272)$ for 128-bit quantum security levels. The scheme EFLASH is shown to resist three known attacks including direct algebraic attack by Faugere et al. [52], MinRank attack by Bettale et al. [6] and discrete differential attack Dubois et al. [47]. They have estimated the complexity of direct attack and MinRank attack. An algebraic cryptanalysis is shown by Oygarden et al. [82] against EFLASH. They developed a way to measure the degree for the systems of equations arising from the scheme EFLASH. Their estimation shows that the 80-bit security parameters of EFLASH can provide at most 69-bit security.

Efficiency. The public key generation includes composition of maps S, T, f, τ whereas encryption is simply computation of the public map P at $\mathbf{x} \in \mathbb{F}^n$. Decryption needs to solve a linear system of equations defined by the linearization equations at most q^a times as the decryptor appends every possible $\mathbf{c}_a$ to $\mathbf{c}$ to generate $\mathbf{c}^{'} = \mathbf{c}||\mathbf{c}_a \in \mathbb{F}^d$ for the ciphertext $\mathbf{c}$ and proceeds to find the plaintext until he gets the original one.

4.5 Other Constructions

— DEC ([81]): The **Diophantine Equation Cryptosystem** (**DEC**) was proposed by Okumura [81] in 2015. DEC is a public key encryption scheme hath is based on the difficulty of solving diophantine equations of degree increasing type.

The key generation of DEC needs only integer additions and multiplications whereas the encryption algorithm executes moduler exponentiation, polynomial multiplications, and additions. More interestingly, the secret key contains only an integer vector. However, the decryption process is comparatively slower due to the execution of Extended Euclidean algorithm for finding gcd and modular multiplicative inverse calculation.

The scheme DEC was proposed as an analogue of the ***Algebraic Surface Cryptosystem*** (**ASC**) of Akiyama et al. [1]. Okumura discussed the security of DEC by reduction to a multivariate equation system against *rational point attack* of Ivanov et al. [70], *ideal decomposition attack* of Faugere et al. [54] which break the one-wayness of ASC. Despite its efficiency in terms of storage, DEC seems unfortunate due to a polynomial time attack of Ding et al. [37] that employs weighted LLL reduction against DEC by showing that the security of DEC cryptosystem relies on searching comparatively short vectors in some lattices derived from a ciphertext and a public key. In three steps the attack transforms the one-wayness of DEC into locating proper solutions of linear systems obtained from public information utilizing a linearization technique that is enabled from the three ciphertext polynomials. In each step, a linear system is obtained which possesses a proper solution, i.e., a suitable lattice point in the lattice which is the solution space of that linear system. The solution acquired in the first step is used to form a linear system in the second step and the solution received from the second step leads to the construction of a linear system in the third step. In this way, the message is retrieved with sufficiently high probability by involving some modular arithmetic technique and the Babai nearest plane algorithm. Locating a correct solution in the first step and consequently in subsequent steps is essential for the attack. The thorough experiments in [37] exhibit that DEC with 128-bit security is vulnerable due to the attack.

— New Multivariate Cryptosystems Based on Hidden Eulerian Equations over Finite Fields ([108]): Ustimenko [108] proposed a multivariate public key encryption scheme in the year 2017 based on Eulerian equations over finite field. The author of [108] has not discussed the security and efficiency of the scheme. The idea of using Eulerian equations over a finite field requires a prudent analysis. However, the decryption includes inversion of some certain maps and solving triangular system of equation multiple times. The size of the secret key is large as the decryptor must have knowledge of the large data to recover the plaintext.

5 MULTIVARIATE PUBLIC KEY SIGNATURE SCHEMES

Related works. It is generally agreed that multivariate cryptography turned out to be more prosperous as an approach for building signature schemes as those provide the shortest signature among post-quantum algorithms. In the last few years, a huge variety of multivariate signature schemes have been proposed.

In 1997, Patarin [85] introduced *Oil Vinegar* signature scheme where the idea behind the scheme is that certain solvable quadratic equations can be generated if random values are assigned to some variables. Later in 1999, Kipnis et al. [71] proposed UOV scheme by modifying the original Oil Vinegar scheme as the security of original Oil Vinegar scheme is questionable due to the attack by Kipnis and Shamir [72]. In 2001, Patarin and Courtois [87] proposed a multivariate signature scheme QUARTZ based on the concept of HFE constructions. While QUARTZ produces very short signatures, the signature generation process is very slow. In the same year, a signature scheme SFLASH was proposed by Patarin et al. [86] that follows a earlier design of Patarin et al. [88] introduced

in 1998. Although both the signaure generation and verification of SFLASH are fast, making the scheme applicable in low cost smart cards, unfortunately SFLASH could not survive due to an attack by Dubois et al. [47] in 2007. Later in 2015, Chen et al. [22] developed an asymmetric digital signature scheme PFLASH which can be seen as a direct descendent of the scheme SFLASH. In that year, Zhang and Tan [117] proposed a new signature protocol MI-T-HFE as a competitor of QUARTZ. The core map used in MI-T-HFE is similar to that of HFEv type construction. The scheme is efficient in terms of public key size while its signature size is twice than that of QUARTZ. In 2005, Ding and Schmidt [42] suggested a new signature scheme Rainbow improving the efficiency of the UOV signature scheme. Although the balanced Oil Vinegar scheme was broken by Kipnis and Shamir [72] in 1998, both the schemes Rainbow and UOV seems to continue to offer promise for post quantum cryptography. In 2010, Petzoldt et al. [92] presented an idea to reduce the public key size of the UOV signature scheme significantly. Furthermore, in 2010, Petzoldt et al. [91] extended the idea to get smaller public key than that of Rainbow. In 2017, ***Lifted Unbalanced Oil Vinegar*** (**LUOV**) was introduced by Beullens et al. [10] to achieve better key sizes, signature sizes, and speed. LUOV is another modifiaction of the UOV signature scheme. Apart from LUOV, there are several improvements on UOV which are discussed in Subsection 5.1. The scenario of UOV and Rainbow has been changed due to two efficient attacks of Beullens [7] – the intersection attack is effective to both UOV and Rainbow and the rectangular MinRank attack is applicable only on Rainbow. Both the attacks reduce the key recovery cost compared to existing attacks. In 2017, Casanova et al. [18] suggested a ***Great Multivariate Short Signature*** (**G*e*MSS**) having benefits of small signatures and fast verification process. G*e*MSS can be seen as an immediate lineage from QUARTZ and adopts some design techniques of the multivariate signature scheme Gui of petzoldt et al. [95] introduced in 2015. Although GeMSS has been selected for the third round of the NIST Project, recently an efficient key recovery attack by Tao et al. [106] makes the scheme vulnerable indicating that both the Minus and the Vinegar modification fail to enhance the security of the basic HFE. In 2017, Petzoldt et al. [94] proposed a efficient signature scheme HMFEv which is a modification of the encryption scheme MultiHFE [19]. In 2018, the first provably secure MQ signature scheme SOFIA was proposed by Chen et al. [21] where the construction utilizes an extension of Unruh's transform for 5-pass identification schemes. In 2020, Kundu et al. [75] designed a digital signature protocol providing short signature based on the Multivariate Cubic problem using the central map of HFE and the idea of Rainbow. Recently, a study on a new perturbation was introduced in [53] that claims to strengthen the security of some well-known multivariate families like HFE and UOV.

In 2011, Sakumoto et al. [99] suggested public key identification protocols by constructing statistical zero-knowledge argument of knowledge based on the MQ problem, assuming the existence of a non-interactive statistically-hiding and computationally-binding commitment scheme. In 2016, Chen et al. [66] introduced the first provably secure signature scheme MQDSS based on the MQ problem. The fundamental concept behind the scheme is to involve Fiat-Shamir transform to the 5-pass multivariate identification scheme of Sakumoto et al. [99]. MQDSS is also a part of the first and second rounds of the NIST competition. Later in 2020, Beullens came up with an efficient signature scheme, ***MUltivariate quaDratic FIat-SHamir*** (**MUDFISH**), having security proof in the quantum random oracle model. In his work, Beullens first presented a Sigma protocol for the MQ relation and then employed the Fiat-Shamir transform to obtain the signature scheme. He also claimed that MUDFISH is better than MQDSS in terms of efficiency, especially from the aspect of signature size and speed on the NIST platform.

In 2013, Shen et al. [101] introduced the first identity-based multivariate signature scheme ***Identity Based Unbalanced Oil Vinegar*** (**IBUOV**) from UOV signature scheme. Later in 2019, Luyen [76] proposed a method to design an EU-CMA secure identity-based signature scheme

Table 2. Comparison of Multivariate Signature Schemes

Scheme	Advantages	Disadvantages	Proposed attacks
Oil Vinegar [85]	requires very little RAM in smartcard implementations	not secure	algebraic attack [72]
UOV [71]	efficient and secure than Oil Vinegar	parameters must be chosen carefully to avoid attacks	intersection attack [7]
QUARTZ [87]	produces short signatures, no practical attack	slow signature generation	-
HFEv- [95]	faster than QUARTZ, short signatures	restricted to the field GF(2)	attack using projection [38], Minrank attack [106]
SFLASH [86]	fast decryption, smaller public key, useful on low cost smart cards	not secure	differential attack [47]
PFLASH [22]	strong security and easier to implement, on a smart card without an arithmetic coprocessor	slower than Sflash	-
MI-T-HFE [117]	smaller public key than QUARTZ	larger signature size than QUARTZ	-
Rainbow [42]	efficient than UOV and Sflash in terms of speed, better choice for practical application	parameters must be chosen carefully to avoid attacks	Minrank attack ([11],[4]), Rainbow-Band-Separation attack [44], intersection attack and rectangular MinRank attack [7], differential attack [9]
GeMSS [18]	short signatures, faster than quartz	large public key	Minrank attacks ([106], [4])
HMFEv [94]	efficient in terms of performance and memory requirements, smaller key size and signature size than Gui and Rainbow	costly decryption	HighRank attack [61]

IBS-Rainbow from Rainbow construction. Another multivariate identity-based signature scheme based on the hardness of the isomorphism of polynomials problem was proposed in [49] which is efficient in terms of storage.

In 2011, Wang et al. [111] introduced an idea to design a multivariate ring signature scheme with a security model. Later in 2017, Mohamed et al. [79] suggested an efficient method that extends multivariate signature schemes to ring signature schemes and applied the technique to the Rainbow construction. A *Ring signature* scheme allows a member of a group of users (named ring) to sign a document anonymously so that no one receives information of which member has signed the document except the actual signer. The signer members, who have their own signing keys, can generate signature for the document on behalf of the ring. The above-mentioned scheme grants perfect anonymity for the signer (as member of a group) as well as shorter ring signatures than all previously suggested post-quantum ring signature schemes. Earlier in 2015, Zhang et al. [116] proposed a threshold ring signature scheme based on the MQ problem by improving the scheme of Petzoldt et al. [93]. In a t-out-of-N *threshold ring signature*, t users can sign a document jointly and anonymously for a group of N users. Recently in 2021, Duong et al. [48] proposed a new and improved technique to design multivariate threshold ring signature scheme where the signature length is shorter than that of Zhang et al. [116].

In 2011, Yang et al. [112] introduced the first multivariate group signature scheme based on **Isomorphism of Polynomials** (**IP**) Problem. The signature size of the protocol is independent of the number of group members while the manager's public key remains linear to the number of group users. Last year, a secure multivariate group signature scheme was suggested by Kundu et al. [74] employing a 5-pass identification protocol and multivariate signature scheme as its building blocks where signature size, manager's public key size, and signer's secret key size do no rely on the number of group users.

In 2017, Petzoldt et al. [96] introduced a method to construct an efficient blind signature scheme from Rainbow multivariate signature scheme. A *Blind signature* scheme permits a user, who has no access to the secret signing key, to get a signature for a document on behalf of the owner of the secret key (the signer). The key point is that the signer gains no knowledge about the content of the message nor the signature, generated during interaction. The above-mentioned blind signature scheme satisfies the usual blindness criterion and unforgeability criterion adapted to multivariate quadratic signatures and produces short blind signatures. In 2020, Duong et al. [64] came up with a new idea to design multivariate blind ring signature scheme by combining the concept of blind and ring signature to increase flexibility in real life aspects, e.g., e-banking.

In the area of digital signatures, a large number of practical and well-understood multivariate schemes exist. Table 2 shows a rough comparison of advantages and disadvantages of promising multivariate public key signature schemes. There are mainly two types of existing signature

designs- SingleField schemes like UOV and Rainbow and Big Field schemes like HFEv- and HMFEv. The schemes UOV and Rainbow follow a similar design strategy employing Oil Vinegar polynomials whereas HFEv- links the HFE design with the Minus and Vinegar modifiers and HMFEv combines the Vinegar modification to MultiHFE construction. We present those signature schemes below to show the concept behind their constructions.

5.1 Oil and Vinegar ([71])

In 1999, Kipnis et al. [71] proposed Unbalanced Oil and Vinegar scheme. This can be seen as a secure variant of original Oil and Vinegar scheme which was broken by Kipnis and Shamir [72] in 1998.

Description of the scheme

— Setup$(1^\lambda) \rightarrow$ pp: On input a security parameter λ, a trusted authority selects a finite field $\mathbb{F}$ having q elements, chooses positive integers n, o, v such that $n = o + v, V = \{1, 2, \ldots, v\}$ and $O = \{v + 1, v + 2, \ldots, n\}$ and a hash function $H : \{0,1\}^* \longrightarrow \mathbb{F}^o$. It publishes the public parameter pp $= (\mathbb{F}, o, v, V, O, n, H)$.

— KeyGen(pp) $\rightarrow$ (pk, sk): A user inputs public parameter pp and proceeds as follows.

(i) Choose a central map $F : \mathbb{F}^n \longrightarrow \mathbb{F}^o$ that consists of multivariate quadratic polynomials $f^1, f^2, \ldots, f^o$ where

$$f^k(x_1, x_2, \ldots, x_n) = \sum_{i \in V} \sum_{j \in V} a^k_{i,j} x_i x_j + \sum_{i \in V} \sum_{j \in O} b^k_{i,j} x_i x_j + \sum_{i \in V \cup O} c^k_i x_i + d^k,$$

with randomly chosen coefficients $a^k_{i,j}, b^k_{i,j}, c^k_i, d^k \in \mathbb{F}, k = 1, 2, \ldots, o$. Here, first v variable $x_1, x_2, \ldots, x_v$ are vinegar variables and last $n - v = o$ variables $x_{v+1}, x_{v+2}, \ldots, x_n$ are oil variables.

(ii) Select an invertible affine map $T : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ and compute $P : \mathbb{F}^n \longrightarrow \mathbb{F}^o$ by setting $P = F \circ T$.

(iii) Set the public key pk $= P$ which is made public whereas the secret key is set as sk $= (F, T)$ which is kept secret to the user.

— Sign(pp, sk, $\mathbf{d}$) $\rightarrow \mathbf{z}$: The signer uses the hash function $H : \{0,1\}^* \longrightarrow \mathbb{F}^o$ to compute $\mathbf{w} = H(\mathbf{d}) \in \mathbb{F}^o$, generates a signature $\mathbf{z} \in \mathbb{F}^n$ for a document $\mathbf{d}$ and performs the following steps.

(i) Compute a pre-image $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ of $\mathbf{w} = (w_1, w_2, \ldots, w_o) \in \mathbb{F}^o$ under the central map F as follows.

(a) Choose the values of the vinegar variables $x_1, x_2, \ldots, x_v$ randomly.

(b) Substitute the values of the vinegar variables $x_1, x_2, \ldots, x_v$ into the polynomials $f^1, f^2, \ldots, f^o$. Due to the structure of the central polynomials $f^1, f^2, \ldots, f^o$, o linear polynomials $\widetilde{f}^1, \widetilde{f}^2, \ldots, \widetilde{f}^o$ in the o oil variables $x_{v+1}, x_{v+2}, \ldots, x_n$ are obtained.

(c) Solve the resulting linear system $\widetilde{f}^k(x_{v+1}, x_{v+2}, \ldots, x_n) = w_k$ by Gaussian elimination where $k = 1, 2, \ldots, o$.

(d) If the system has no solution, choose another set of values of the vinegar variables $x_1, x_2, \ldots, x_v$ and repeat the steps.

(ii) Compute the signature $\mathbf{z} \in \mathbb{F}^n$ of the document $\mathbf{d}$ by $\mathbf{z} = T^{-1}(\mathbf{x})$.

— Verify(pp, pk, $\mathbf{d}, \mathbf{z}$) $\rightarrow$ 0/1: To verify the authenticity of the signature $\mathbf{z} \in \mathbb{F}^n$, the verifier finds $\mathbf{w} = H(\mathbf{d}) \in \mathbb{F}^o$ and computes $\mathbf{w}' = P(\mathbf{z})$ utilizing the public key pk $= P$ and public parameter pp. If $\mathbf{w}' = \mathbf{w}$ holds, verifier accepts the signature; otherwise, rejects.

Correctness follows from the fact that $\mathbf{w}' = P(\mathbf{z}) = F \circ T(\mathbf{z}) = F \circ T(T^{-1}(\mathbf{x})) = F \circ T \circ (T^{-1}(F^{-1}(\mathbf{w}))) = F \circ (T \circ T^{-1})(F^{-1}(\mathbf{w})) = (F \circ F^{-1})(\mathbf{w}) = \mathbf{w}$.

For $o = v$, the scheme is called balanced **Oil Vinegar** (**OV**) while for $v > o$, the scheme is called UOV signature scheme.

Security analysis: In 1998, original Oil and Vinegar scheme or balanced Oil Vinegar scheme was broken by Kipnis and Shamir [72]. The cryptanalysis of [72] also works for $v < o$. In the attack of [72], one looks at the quadratic forms of the o public equations to separate the oil variables and the vinegar variables. On the other hand, the cases $v > o$ are much more complex. The suggested practical parameters $(\mathbb{F}, o, v)$ for UOV scheme are $(\mathrm{GF}(2^8), 28, 56)$ for 80-bit security, $(\mathrm{GF}(2^8), 35, 70)$ for 100-bit security and $(\mathrm{GF}(2^8), 45, 90)$ for 128- bit security. Note that, choosing variables o and v using $v \geq 2o$ is preferable to avoid the attack [72]. In 2021, Beullens [7] proposed the intersection attack, an improved key recovery attack, that downsizes the key recovery cost compared to existing attacks. It follows the concept behind the Kipnis-Shamir attack along with a system-solving strategy like the reconciliation attack [44].

Efficiency: The key generation involves the composition of several maps. The signature generation is comparatively fast as it requires to solve a system of linear equations using Gaussian elimination and matrix inversion over a small finite field. The verification algorithm needs evaluation of the central core map P for a signature $\mathbf{z} \in \mathbb{F}^n$. The secret key needs to store the data of the polynomials in central map F and the affine map T which are necessary in constructing P.

Variants of UOV: As UOV needs to use a large public key, several methods have been proposed to address the issue.

- *Lifted Unbalanced Oil and Vinegar (LUOV)* [10]: This proposal chooses the UOV keys over the smallest field $\mathbb{F}$ of cardinality 2 and lifts those to a larger field, resulting a remarkable reduction of the public key size of UOV. Also, the scheme works favourably in terms of signature sizes, key sizes and speed with existing signature schemes.
- *Block-Anti-Circulant Unbalanced Oil and Vinegar (BAC-UOV)* [104]: This technique to compress the UOV public keys exploits block-anti-circulant matrices which offer a compact representation as the remaining components can be figured out from the first row of a block.
- *UOV using an arbitrary quotient ring (QR-UOV)* [56]: This work utilizes a public key which is expressed by block matrices whose components are related to an element of a quotient ring $\mathbb{F}[x]/(f)$ using an injective ring homomorphism between the quotient ring $\mathbb{F}[x]/(f)$ to the matrix ring $\mathbb{F}^{l\times l}$ for a polynomial $f \in \mathbb{F}[x]$ of degree l. For NIST recommended security levels, the approach helps to acquire a smaller public key than that of the 3rd round finalist Rainbow while not increasing the signature size significantly.
- *MAYO* [8]: This variant of the UOV scheme employs a UOV map with a small oil space which causes a compact representation of the public key. When the oil space is very small, the complexity of the key recovery attacks increases. The unique technique of MAYO solves the crisis by "whipping up" the UOV map into a larger one having a satisfactorily bigger oil space.
- *UOV-Pepper* [77]: This variant of UOV offers a method to use a new perturbation called "Pepper" and degree 3 UOV to design signature protocol which is claimed to be fast and resist all known attacks, particularly the Gröbner basis attacks and the MinRank attacks. The Pepper perturbation operates for the public key equations with at least degree 3. The authors also claimed that the size of the signatures can be very short while retaining a reasonable public key size.

5.2 Rainbow ([42])

The scheme Rainbow was proposed by Ding and Schmidt [42] in the year 2005. Rainbow can be portrayed as a multi-layer construction of Oil-Vinegar scheme and its generalization.

Description of the scheme

— Setup$(1^\lambda) \rightarrow$ pp: On input a security parameter λ, a trusted authority proceeds as follows to output public parameters pp.

(i) Pick a finite field $\mathbb{F}$ having q elements. Choose a sequence of integers $0 < v_1 < v_2 < \cdots < v_{h+1} = n$. Also let $V_i = \{1, 2, \ldots, v_i\}$, $O_i = \{v_i + 1, v_i + 2, \ldots, v_{i+1}\}$ and $o_i = v_{i+1} - v_i$ for $i = 1, 2, \ldots, h$.

(ii) Select a hash function $H : \{0,1\}^* \longrightarrow \mathbb{F}^{n-v_1}$ and publish public parameters pp $= (\mathbb{F}, (v_1, v_2, \ldots, v_{h+1}), H, o_i, V_i, O_i, i = 1, 2, \ldots h)$.

— KeyGen$(1^\lambda) \rightarrow$ (pk, sk): A user inputs public parameters pp and performs the following steps to output public key pk and secret key sk.

(i) Choose central map $F : \mathbb{F}^n \longrightarrow \mathbb{F}^{n-v_1}$ which consists of $n - v_1$ quadratic polynomials $f^{v_1+1}, f^{v_1+2}, \ldots, f^n$ given by

$$f^k(x_1, x_2, \ldots, x_n) = \sum_{i \in O_l} \sum_{j \in V_l} a^k_{i,j} x_i x_j + \sum_{i,j \in V_l, i \leq j} b^k_{i,j} x_i x_j + \sum_{i \in V_l \cup O_l} c^k_i x_i + d^k,$$

where $k = v_1 + 1, v_1 + 2, \ldots, n$. Here, $a^k_{i,j}, b^k_{i,j}, c^k_i, d^k \in \mathbb{F}$ are randomly chosen coefficients and $l \in \{1, 2, \ldots, h\}$ is the only integer such that $k \in O_l$. Note that these are Oil and Vinegar polynomials with $x_i, i \in V_l$ being the Vinegar variables and $x_j, j \in O_l$ being the Oil variables.

(ii) Select two invertible affine transformations $S : \mathbb{F}^{n-v_1} \longrightarrow \mathbb{F}^{n-v_1}$, $T : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ and compute $P = S \circ F \circ T : \mathbb{F}^n \longrightarrow \mathbb{F}^{n-v_1}$.

(iii) Set the public key pk $= P$ which is made public whereas the secret key is set as sk $= (S, F, T)$ which is kept secret to the user.

— Sign(pp, sk, $\mathbf{d}$) $\rightarrow \mathbf{z}$: To generate a signature $\mathbf{z} \in \mathbb{F}^n$ for a document $\mathbf{d}$, the signer uses the hash function $H : \{0,1\}^* \longrightarrow \mathbb{F}^{n-v_1}$, computes $\mathbf{w} = H(\mathbf{d}) \in \mathbb{F}^{n-v_1}$ and proceeds as follows.

(i) Compute $\mathbf{y} = S^{-1}(\mathbf{w}) \in \mathbb{F}^{n-v_1}$.

(ii) Find a pre-image $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ of $\mathbf{y}$ under the central map F in the following way.

(a) Choose the values of the vinegar variables $x_1, x_2, \ldots, x_{v_1}$ randomly.

(b) Substitute the values of the variables $x_1, x_2, \ldots, x_{v_1}$ into the polynomials $f^{v_1+1}, f^{v_1+2}, \ldots, f^n$.

(c) For $l = 1$ to h, execute Gaussian elimination on the polynomials $f^k (k \in O_l)$ to obtain the values of $x_k (k \in O_l)$. Now put the values of $x_k (k \in O_l)$ into the polynomials $f^k (k > v_{l+1})$.

Suppose $l = 1$. Then, $k \in O_1 = \{v_1 + 1, v_1 + 2, \ldots, v_2\}$. Hence, there will be a system of o_1 linear equations having o_1 unknowns $x_{v_1+1}, x_{v_1+2} \ldots, x_{v_2}$ from $f^{v_1+1}, f^{v_1+2}, \ldots, f^{v_2}$, which can be solved by Gaussian Elimination. The so computed values of $x_{v_1+1}, x_{v_1+2}, \ldots, x_{v_2}$ are put into the polynomials $f^{v_2+1}, f^{v_2+2}, \ldots, f^n$. Next, for $l = 2, k \in O_2 = \{v_2 + 1, v_2 + 2, \ldots, v_3\}$. So, again a system of o_2 linear equations with the o_2 unknowns $x_{v_2+1}, x_{v_2+2} \ldots, x_{v_3}$ can be obtained from $f^{v_2+1}, f^{v_2+2}, \ldots, f^{v_3}$ and then the system can be solved using the method of Gaussian Elimination. Again the computed values of $x_{v_2+1}, x_{v_2+2} \ldots, x_{v_3}$ are put into the polynomials $f^{v_3+1}, f^{v_3+2}, \ldots, f^n$. By repeating this process one can get values for all the variables $x_1, x_2, \ldots, x_n$.

(d) If the system has no solution, choose different values of $x_1, x_2, \ldots, x_{v_1}$ and repeat the steps.

(iii) Compute the signature $\mathbf{z} \in \mathbb{F}^n$ for the document $\mathbf{d}$ by $\mathbf{z} = T^{-1}(\mathbf{x})$.

— Verify(pp, pk, $\mathbf{d}, \mathbf{z}$) $\longrightarrow$ 0/1: To verify the signature $\mathbf{z} \in \mathbb{F}^n$, the verifier uses the hash function H to find $\mathbf{w} = H(\mathbf{d}) \in \mathbb{F}^{n-v_1}$ and computes $\mathbf{w}' = P(\mathbf{z})$ where pk $= P$ is the public key. If $\mathbf{w}^{'} = \mathbf{w}$ holds, the verifier accepts the signature; otherwise rejects.

Correctness follows from the fact that $\mathbf{w}' = P(\mathbf{z}) = S \circ F \circ T(T^{-1}(\mathbf{x})) = S \circ F \circ (T \circ T^{-1})(\mathbf{x}) = S \circ F(F^{-1}(\mathbf{y})) = S \circ (F \circ F^{-1})(S^{-1}(\mathbf{w})) = (S \circ S^{-1})(\mathbf{w}) = \mathbf{w}$.

Security Analysis: The suggested practical parameters $(\mathbb{F}, v_1, o_1, o_2)$ for the Rainbow signature scheme with two layers ($h = 2$) are (GF(2^8), 17, 13, 13) for 80-bit security, (GF(2^8), 26, 17, 16) for 100-bit security and GF(2^8), 36, 22, 21) for 128-bit security. Rainbow signature scheme can be seen as a multilayered version of UOV signature scheme. The scheme seems confident against direct attacks and UOV attacks. The currently-known attacks against Rainbow are Minrank attack of Billet et al. [11] and the Rainbow-Band-Separation attack of Ding et al. [44]. Rainbow-Band-Separation attack attempts to obtain affine maps that convert the public polynomials into the polynomials as in the central map of Rainbow to find an equivalent key for forging a signature. Later in 2021, Rainbow faced the rectangular MinRank attack of Beullens [7] that reduces key recovery cost for the parameters proposed in the NIST competition. Beullens used rectangular matrices in their attack instead of square matrices. He showed the presence of another instance of the MinRank problem within the public keys of Rainbow. Rainbow is also vulnerable to the intersection attack of Beullens [7]. Therefore, a proper selection of Rainbow parameters is essential due to these attack possibilities.

Efficiency: The Key generation involves the composition of several maps while the signature generation requires solving linear systems of equations using Gaussian elimination method and matrix inversions over a finite field. Rainbow reduces the number of variables in the system which leads to better performance along with short key sizes and signatures. The verification algorithm needs evaluation of central core map P at the signature $\mathbf{z} \in \mathbb{F}^n$. The secret key contains the data used in constructing P which is needed to sign a message. The scheme is very easy to execute and can be used on embedded devices.

5.3 HFEv- ([95])

In 2015, petzoldt et al. [95] proposed HFEv- based multivariate signature scheme, Gui, which can be seen as an extension of HFEv- signature protocols. HFEv- variants are very attractive for multivariate digital signatures. Here, we describe the technique behind the construction of HFEv- signature schemes.

Description of the scheme

— Setup(1^λ) $\rightarrow$ pp: A trusted authority takes a security parameter λ as input, selects a finite field $\mathbb{F}$ with q elements and chooses positive integers D, a, v and n such that n be the degree of the extension field K of $\mathbb{F}$. The trusted authority publishes public parameters pp $= \{D, a, v, n, \mathbb{F}, K\}$.

— KeyGen(pp) $\rightarrow$ (pk, sk): Taking public parameters pp as input, the user proceeds as follows.

(i) Select a central map $f : K \times \mathbb{F}^v \longrightarrow K$ of the form

$$f(X, u_1, u_2, \ldots, u_v) = \sum_{0 \le i \le j}^{q^i + q^j \le D} a_{ij} \cdot X^{q^i + q^j} + \sum_{i=0}^{q^i \le D} b_i(u_1, u_2, \ldots, u_v) \cdot X^{q^i} + c(u_1, u_2, \ldots, u_v),$$

where $a_{ij} \in K$, $b_i : \mathbb{F}^v \longrightarrow K$ is a linear function, $c : \mathbb{F}^v \longrightarrow K$ is a quadratic function and $u_1, u_2, \ldots, u_v$ are vinegar variables. Let, $\bar{f} = \phi^{-1} \circ f \circ (\phi \times i_v) : \mathbb{F}^{n+v} \longrightarrow \mathbb{F}^n$ is a quadratic

polynomial map where $\phi : \mathbb{F}^n \longrightarrow K$ be the canonical isomorphism between defined by $\phi(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i \cdot X^{i-1}$ and i_v is the identity map from $\mathbb{F}^v \longrightarrow \mathbb{F}^v$.

(ii) Choose two affine transformations $S : \mathbb{F}^n \longrightarrow \mathbb{F}^{n-a}$ and $T : \mathbb{F}^{n+v} \longrightarrow \mathbb{F}^{n+v}$ and compute $P = S \circ \bar{f} \circ T : \mathbb{F}^{n+v} \longrightarrow \mathbb{F}^{n-a}$.

(iii) Set the public key as $\mathsf{pk} = P$ which is made public and the secret key as $\mathsf{sk} = (S, f, T)$ which is kept secret to the user.

— Sign(pp, sk, $\mathbf{d}$) $\rightarrow \mathbf{z}$: On input the public parameters pp, secret key sk and a document $\mathbf{d}$, the signer generates a signature $\mathbf{z}$ for the document $\mathbf{d} \in \mathbb{F}^{n-a}$ by performing the steps below.

(i) Compute $\mathbf{y} = S^{-1}(\mathbf{d}) \in \mathbb{F}^n$ and $Y = \phi(\mathbf{y}) \in K$.

(ii) Choose random values for the vinegar variables $u_1, u_2, \ldots, u_v \in \mathbb{F}$ and substitute them in the polynomial f to find f_u.

(iii) Find preimage X of Y under f_u by solving the univariate polynomial equation $f_u(X) = Y$ using Berlekamp's algorithm and compute $\mathbf{x}^{'} = \phi^{-1}(X) \in \mathbb{F}^n$. Set $\mathbf{x} = (\mathbf{x}^{'}||u_1||u_2|| \cdots ||u_v)$.

(iv) Generate the signature $\mathbf{z} \in \mathbb{F}^{n+v}$ for the document $\mathbf{d}$ by $\mathbf{z} = T^{-1}(\mathbf{x}) \in \mathbb{F}^{n+v}$.

— Verify(pp, pk, $\mathbf{d}, \mathbf{z}$) $\longrightarrow$ 0/1: To verify a signature $\mathbf{z} \in \mathbb{F}^{n+v}$ for the document $\mathbf{d}$, the verifier computes $\mathbf{d}^{'} = P(\mathbf{z}) \in \mathbb{F}^{n-a}$ and compares it with $\mathbf{d}$. If $\mathbf{d}^{'} = \mathbf{d}$ holds, the signature is accepted, otherwise rejected.

Correctness follows from the fact that $\mathbf{d}' = P(\mathbf{z}) = S \circ \bar{f} \circ T(T^{-1}(\mathbf{x})) = S \circ \bar{f} \circ (T \circ T^{-1})(\mathbf{x}) = S \circ \bar{f}(\bar{f}^{-1}(\mathbf{y})) = S \circ (\bar{f} \circ \bar{f}^{-1})(S^{-1}(\mathbf{d})) = (S \circ S^{-1})(\mathbf{d}) = \mathbf{d}$.

Security analysis: The suggested practical parameters $(\mathbb{F}, n, D, a, v)$ for HFEv- signature scheme are $(\mathrm{GF}(7), 62, 8, 2, 2)$ for 80-bit security, $(\mathrm{GF}(7), 78, 8, 3, 3)$ for 100-bit security and $(\mathrm{GF}(7), 100, 8, 4, 4)$ for 128-bit security. The possible attacks on HFEv- based signature schemes are the MinRank attack of Kipnis and Shamir [73], direct algebraic attack [27] and differential attack [16]. A rough complexity estimation of the MinRank attack on HFEv- based constructions is given roughly by $O(q^{n(r+v+a-1)} \cdot (n-a)^3)$ where r is a parameter that depends on D and q. Also, Ding and Yang [43] estimated an upper bound for the degree of regularity of direct attack using Gröbner basis against HFEv- constructions. However, in 2018, Ding et al. [38] proposed new attack strategies against the scheme HFEv- by employing the idea of projection. In 2021, Tao et al. [106] suggested an improved MinRank based attack on HFEv- signature scheme showing that the present approaches are incapable to provide a secure and efficient signature scheme from the HFE construction. By employing the minors modeling method, the estimated complexity of the attack on HFEv- is $O\left(\binom{n+v+d+1}{d+1}^{\omega}\right)$ where $d = \log_q(D)$ and $2 < \omega \leq 3$ is a linear algebra constant. This ascertains that the Minus and Vinegar modification do not provide an extra advantage in the security of HFE constructions as the complexity does not depend on the number a used for Minus modification and polynomial both in n and the number of Vinegar variables v. Therefore, all HFE signature variants including HFEv- face a polynomial time attack for a fixed D. Taking a very large value of D is highly required to encounter the security requirements, but it causes a slow and inefficient signature generation.

Efficiency: The key generation includes the composition of certain maps. The signature generation is costly for HFEv- as it needs the invocation of the Berlekamp algorithm for the inversion of a univariate polynomial equation over an extension field. The signature verification is simply an evaluation of the quadratic map P at $\mathbf{z} \in \mathbb{F}^{n+v}$. In the signature generation of Gui, one needs to invert the HFEv- polynomial k times resulting k times slower signature generation than that of HFEv- and also a considerably slower signature generation than that of UOV and Rainbow although Gui furnishes the shortest signatures among all existing schemes.

5.4 HMFEv ([94])

In 2017, Petzoldt et al. [94] suggested a signature scheme **Hidden Medium Field Equations with a Vinegar variation** (**HMFEv**), more specifically, a Vinegar variation of MultiHFE encryption by Chen et al. [19].

Description of the scheme

— Setup$(1^\lambda) \rightarrow$ pp: On input a security parameter λ, a trusted authority chooses a finite field $\mathbb{F}$ of cardinality q and an irreducible polynomial $g(x) \in \mathbb{F}[x]$ of degree l. Let $K = \mathbb{F}[x]/g(x)$ be the extension field over $\mathbb{F}$. The trusted authority also selects positive integers m, n, v such that $n = m.l$, a hash function $H : \{0,1\}^* \longrightarrow \mathbb{F}^n$ and publishes public parameter pp $= \{\mathbb{F}, q, l, H, K, n, m, v\}$.

— KeyGen(pp) $\rightarrow$ (pk, sk): Taking public parameters pp as input, a user executes the following steps to output public key and secret key.

(i) Select a central map $f : K^m \times \mathbb{F}^v \longrightarrow K^m$ that consists of m components $f^1, f^2, \ldots, f^m$ given by

$$f^i(X_1, X_2, \ldots, X_m, u_1, u_2, \ldots, u_v) = \sum_{r=1}^{m}\sum_{s=r}^{m} a_{r,s}^{(i)} X_r X_s + \sum_{r=1}^{m} b_r^{(i)}(u_1, u_2, \ldots, u_v) \cdot X_r + c^{(i)}(u_1, u_2, \ldots, u_v),$$

where $a_{r,s}^{(i)} \in K$, linear functions $b_r^{(i)} : \mathbb{F}^v \longrightarrow K$ and quadratic maps $c^{(i)} : F^v \longrightarrow K$ for $i = 1, 2, \ldots, m$.

(ii) Choose two invertible affine maps $S : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ and $T : \mathbb{F}^{n+v} \longrightarrow F^{n+v}$ and compute $P = S \circ \bar{f} \circ T : \mathbb{F}^{n+v} \longrightarrow \mathbb{F}^n$ where $\phi : \mathbb{F}^l \longrightarrow K$ is an isomorphism defined by $\phi(y_1, y_2, \ldots, y_l) = \sum_{i=1}^{l} y_i x^{i-1}$ and $\bar{f} = (\underbrace{\phi^{-1} \times \phi^{-1} \times \cdots \times \phi^{-1}}_{m \text{ times}}) \circ f \circ (\underbrace{\phi \times \phi \times \cdots \times \phi}_{m \text{ times}}) \circ \mathrm{i}_v) : \mathbb{F}^{n+v} \longrightarrow \mathbb{F}^n$ is a multivariate quadratic map. Here, i_v is the identity map from $\mathbb{F}^v \longrightarrow \mathbb{F}^v$ and $n = m \cdot l$.

(iii) Set public key pk $= P$ which is made public whereas the secret key is set as sk $= (S, T, f)$ which is kept secret to the user.

— Sign(pp, sk, $\mathbf{d}$) $\rightarrow \mathbf{z}$: On input public parameters pp, secret key sk, the signer generates a signature for a document $\mathbf{d}$ by computing the hash value $\mathbf{w} = H(\mathbf{d}) \in \mathbb{F}^n$ first and then performing as follows.

(i) Compute $\mathbf{y} = (y_1, y_2, \ldots, y_n) = S^{-1}(\mathbf{w}) \in \mathbb{F}^n$ where $n = ml$.

(ii) Now compute $Y_i = \phi(y_{(i-1).l+1}, \ldots, y_{i.l}) \in K$ for $i = 1, 2, \ldots, m$.

(iii) Choose random values of the Vinegar variables $u_1, u_2, \ldots, u_v \in \mathbb{F}$ and substitute them into the central map components $f^1, f^2, \ldots, f^m$ to obtain $f_u^1, f_u^2, \ldots, f_u^m$ where

$$f^i(X_1, X_2, \ldots, X_m, u_1, u_2, \ldots, u_v) = \sum_{r=1}^{m}\sum_{s=r}^{m} a_{r,s}^{(i)} X_r X_s + \sum_{r=1}^{m} b_r^{(i)}(u_1, u_2, \ldots, u_v) \cdot X_r + c^{(i)}(u_1, u_2, \ldots, u_v).$$

(iv) Use the XL algorithm or a Gröbner basis method to compute $X_1, X_2, \ldots, X_m$ such that $f_u^i(X_1, X_2, \ldots, X_m) = Y_i$, $i = 1, 2, \ldots, m$.

(v) Compute $\mathbf{x} = (\phi^{-1}(X_1), \phi^{-1}(X_2), \ldots, \phi^{-1}(X_m), u_1, u_2, \ldots, u_v) \in \mathbb{F}^{n+v}$.

(vi) Generate the signature $\mathbf{z} \in \mathbb{F}^{n+v}$ by $\mathbf{z} = T^{-1}(\mathbf{x})$.

— Verify(pp, pk, $\mathbf{d}, \mathbf{z}$) $\longrightarrow$ 0/1: The verifier, on input public parameters pp, public key pk, a document $\mathbf{d}$ and the signature $\mathbf{z}$, checks the validity of the signature $\mathbf{z} \in \mathbb{F}^{n+v}$ for the document $\mathbf{d}$ by computing $\mathbf{w} = H(\mathbf{d})$ and $\mathbf{w}' = P(\mathbf{z})$. If $\mathbf{w} = \mathbf{w}'$ holds, verifier accepts the signature, otherwise rejects.

Correctness follows from the fact that $\mathbf{w}' = P(\mathbf{z}) = S \circ \bar{f} \circ T(T^{-1}(\mathbf{x})) = S \circ \bar{f} \circ (T \circ T^{-1})(\mathbf{x}) = S \circ \bar{f}(\bar{f}^{-1}(\mathbf{y})) = S \circ (\bar{f} \circ \bar{f}^{-1})(S^{-1}(\mathbf{w})) = (S \circ S^{-1})(\mathbf{w}) = \mathbf{w}$.

Security analysis: Petzoldt et al. [94] suggests the parameters $(\mathbb{F}, m, l, v)$ of HMFEv as $(GF(31), 2, 28, 12)$ and $(GF(256), 3, 15, 16)$ for 128-bit security, $(GF(31), 2, 40, 17)$ and $(GF(256), 3, 23, 21)$ for 192-bit security, $(GF(31), 2, 55, 21)$ and $(GF(256), 3, 31, 26)$ for 256-bit security. The authors also have analyzed that HMFEv is resistant to attacks like direct algebraic attack of Huang et al. [65], MinRank attack of Bettale et al. [6] and Quantum attacks of Schwabe et al. [100], differential attack of Daniels et al. [30] and an attack against the original MultiHFE encryption scheme of Hashimoto [60]. They have estimated complexity of direct attack and MinRank attack. The complexity of direct algebraic attack depends on the degree of regularity ([36]). From their experiments it is clear that the upper bound of the degree of regularity of a direct attack against HMFEv is relatively tight. Besides, the MinRank attack and differential attack seems infeasible to this scheme. The complexity of the MinRank attack is estimated as $O\left(\binom{n+m+v+1}{m+v+1}^{\omega}\right)$ for a linear algebra constant ω. HMFEv is more secure against the MinRank attack for a larger vinegar parameter v. Also the Vinegar variables can cleverly remove all the differential symmetries. A careful study on the structure of HMFEv and its security against the HighRank attack is discussed by Hashimoto [61] who exhibits that the vinegar modifier is not enough to ensure security against HighRank attack having complexity $O\left(\binom{n+v+1}{m}^{\omega}\right)$.

Efficiency: The key generation includes the composition of some maps. In the signature generation procedure, the most costly part is the execution of the XL algorithm or the Gröbner Basis method. The signature verification is simply an evaluation using the quadratic map P at $\mathbf{z} \in \mathbb{F}^{n+v}$ and a hash computation.

6 NIST SUBMISSIONS

Post-Quantum Cryptography Standardization is a competition and program declared by NIST to develop standards to include post-quantum cryptography. Several attempts have been made to design and standardize fresh quantum-safe protocols in the competition which is now in its third round. Table 3 presents a summary of the multivariate candidates submitted in the three rounds where most of the submissions are signature schemes. The details of all the potential candidates are available in [28]. Although Himq-3 guarantees a fast signing process, its security becomes questionable due to the singularity attack method of Ding et al. [46] that performs a signature forgery. Also, a modification of parameters of LUOV for the second round occurred as Ding et al. [45] introduced the *Subfield Differential Attack*. Later Ding et al. [32] shows that the *Nested Subset Differential Attack*, a modification to the Subfield Differential Attack, can practically break the level I security parameters of LUOV under 210 min only. The security of Gui is also at stake due to [106]. The schemes GeMSS and Rainbow in the second round are greatly affected by the attack in [4]. Rainbow reaches the third round of the competition as a finalist along with one alternate candidate GeMSS which strongly follows the idea of HFEv- signature scheme. Last year the security of both candidates face questions due to the attacks ([7], [106]). The attack on Rainbow in [7] lowers the key recovery cost by $2^{17}, 2^{53}, 2^{73}$ factors for the parameter sets offered to the second round of the competition targeting the security levels I, III, and V respectively whereby reducing the same by $2^{20}, 2^{40}, 2^{55}$ factors respectively for the third round parameters. The latest approach of key recovery attacks against Rainbow by Beullens [9] seems the most efficient. The key recovery is very much practical for the NIST security level I parameters. On a standard laptop, the secret key can be recovered after nearly 53 hours of computing time, especially for the second round parameters of security level I. The rank attack in [106] breaks all the recommended parameters against GeMSS, especially for the higher security categories. A very large value of D (degree of the HFE polynomial) is required to fulfill the security requirements of NIST, yielding an inefficient

Table 3. Multivariate Schemes Submitted in NIST

Rounds	Encryption schemes	Signature schemes
1st	CFPKM, Giophantus	DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow
2nd	–	GeMSS, LUOV, MQDSS, Rainbow
3rd	–	Rainbow (finalist), GeMSS (alternate candidate)

Table 4. Key and Ciphertext Sizes of Multivariate Encryption Schemes based on MQ Problem

Scheme	Public key (Field elements)	Secret key (Field elements)	Ciphertext (Field elements)
Improved Simple Matrix [107]	$\frac{m}{2}(n+1)(n+2)$	$m(m+1)+n(n+1)+(sr+ru+rv)n$	m
ZHFE [98]	$n(n+1)(n+2)$	$n(5n+3+d_0)+4n^2$	$2n$
HFERP [69]	$\frac{m}{2}(n+1)(n+2)$	$n'(n+1)+m(m+1)+\frac{m-m_2}{2}(n'+1)(n'+2)+d_1m_1$	m
EFLASH [17]	$\frac{m}{2}(n+1)(n+2)$	$2m_1(m_1+1)+m_1(n+1)+m_1$	m

n, m, n', m_1, m_2, d_0, d_1 are positive integers, $n < m$, $n' > n$, $m < m_1$, $d_1 > d_0$, $m_2 < m$.

Table 5. Key and Signature Sizes of Multivariate Signature Schemes based on MQ Problem

Scheme	Public key (Field elements)	Secret key (Field elements)	Signature (Field elements)
Oil Vinegar [85]	$\frac{n-v}{2}(n+1)(n+2)$	$\frac{n-v}{2}(n+1)(n+2)+n(n+1)$	n
HFEv- [95]	$\frac{n-a}{2}(n+v+1)(n+v+2)$	$(n-a)(n+1)+(n+v)(n+v+1)+(2d+1)n$	$(n+v)$
Rainbow [42]	$\frac{n-v}{2}(n+1)(n+2)$	$(n-v)(n-v+1)+n(n+1)+\frac{n-v}{2}(n+1)(n+2)$	n
HMFEv [94]	$\frac{n}{2}(n+v+1)(n+v+2)$	$n(n+1)+(n+v)(n+v+1)+n+\frac{n^2}{l}+\frac{n^2}{2l}(\frac{n}{l}+1)$	$(n+v)$

n, a, v, d, l are positive integers $n > a$, $l|n$.

signature generation process. Hence, the strategies in GeMSS are not adequate to acquire high security levels while maintaining efficiency.

7 SUMMARY OF OBSERVATIONS AND FUTURE RESEARCH DIRECTIONS

After our extensive study on the MPKCs and their security and efficiency related aspects, we now summarize our lessons learned, before presenting the probable future challenges and research directions. Some of those are already discussed in earlier sections. In Tables 4 and 5, a theoretical comparison of some promising encryption and signature schemes based on MQ problem is given, focusing on the key sizes, ciphertext size, and signature size. However, remaining challenges and open research concerns are outlined in this section. With the use of multivariate polynomials over a finite field, MPKCs provide a practical solution to ensure safety in communicating information in presence of post-quantum adversaries. However, most of the multivariate public key cryptosystems analyze their security theoretically and experimentally based on the selected parameters as those do not have security proofs. Nevertheless, MPKCs provide faster encryption and signature verification. The research community is putting a lot of effort to design schemes with enhanced security and devise new techniques to make the primitives more practical. Despite the fact that the authors of [108] have not discussed the security and efficiency, the strategy to use hidden Eulerian equations over finite fields may be useful in the future to devise new multivariate schemes. The encryption scheme EFLASH is a projected C^{*-} scheme [88] with a parameterization that follows the conception of expanding the size of the codomain to avoid ciphertext collision and eliminates decryption failures with a much smaller blow-up factor. Although the scheme ZHFE seems to be a better way to design a multivariate encryption scheme, it can not survive due to a practical key recovery attack that exploits the low rank property of ZHFE by adapting the minors modeling approach to the KS attack. HFERP covers the weaknesses of SRP by substituting the weaker Square

layer with a higher rank HFE polynomial to avoid MinRank attack and holds the comparatively small blow-up factor between the plaintext space and ciphertext space without an essential doubling the size between plaintext and ciphertext. The Rainbow signature scheme is one of the fastest available signature schemes and requires simple linear algebra operations like matrix-vector multiplication and solving linear systems over small finite fields in signature generation. Rainbow does not need a cryptographic coprocessor and can be implemented on low-cost devices. The approaches to address the issue of the large public key of UOV are quite interesting, although there is a practical attack on LUOV by Ding et al. [32] as well as a structural attack on BAC-UOV by Furue et al. [57]. The signature scheme HMFEv is the Vinegar modification to the MultiHFE scheme where the number of components in the central map is reduced to enhance efficiency. Both the schemes Gui and QUARTZ utilizes the concept of HFEv- type protocols. Besides, Gui and QUARTZ signature scheme are mainly limited to the field GF(2) while HMFEv uses larger fields which allows reducing the number of variables and consequently the public key size in the system. Also for high levels of (quantum) security, HMFEv provides shorter keys than that of Gui and Rainbow.

Although most of the schemes have large secret key as it needs to store several maps that are required in the multivariate trapdoor, DEC only needs to store a vector of length n over $\mathbb{Z}$. MQ cryptography has a terrible track record as most of the ideas have been broken. Indeed, an attack on DEC, which is supposed to be a candidate of PQC, shows the significance of thoroughly investigating this cryptosystem further. Hence, more careful design strategies are required for building MQ trapdoors. From the improvement perspective, MPKC seems to be a good promise toward future digital security in the post-quantum era. In the recent future, the area will constantly be developing. Hence, we now discuss a few research directions that could be exploited in the upcoming days.

— In the last few years, several encryption schemes have been proposed using MQ polynomials. No MQ encryption scheme has withstood the test of time, while several MQ signature schemes have. Although there has been quite a bit of progress, there are various major challenges left in this area. Solving some of these numerous rather exciting challenges that remained unattempted could reveal new tracks both from theoretical and practical points of view. Simple Matrix scheme for encryption uses a large matrix algebra structure which leads to a large public key and secret key. In the basic version, three square matrices have been used while the scheme has been generalized by utilizing non-square matrices instead of using square matrices in the improved version. The decryption procedure is a little expensive here. During the inversion of the trapdoor, a decryption failure occurs for a particular case. So finding a general solution is required. Besides, a recent attack [2] shows that the technique used in Simple Matrix might be able to reduce the decryption failure rate than that of the basic version, but actually, it weakens the security. Employing matrix structure in a different approach may help to remove the problems.
— Several constructions have been proposed using the rainbow polynomials that make the scheme simple and easy to implement while their practical security is well understood. But the recent attack strategies in [7], [4], and [9] are a major setback for Rainbow. Therefore, a fresh and concrete idea to use the rainbow polynomials is highly required to design multivariate trapdoors.
— Recently an attack in [106] causes a great defeat for all HFE signature variants like HFEv-. Therefore, searching for new techniques to employ the HFE polynomials in designing protocols is essential. Also, a study on the situation on HFERP and EFLASH is quite required as the support minors modeling method [4] and the new MinRank type attack [106] have entered into the scenario of MPKC.

— The security of MPKCs relies on the MQ problem which is mathematical in nature. Recently, a new mathematical problem called the constrained MQ problem [113], which originated from the original MQ problem, is introduced along with a thorough analysis of the difficulty level of solving the problem. The authors of [113] also suggested a new method, named *pq*-method, to design encryption schemes based on the difficulty of solving the constrained MQ problem. The *pq*-method intends to convert a multivariate encryption scheme over a smaller field to a multivariate encryption scheme over a larger field, which helps to enhance security. Therefore, a careful investigation on the constrained MQ problem is needed as the problem is very much attractive and expected to be studied by numerous strategies to design new schemes.
— Recently, a multivariate encryption scheme [103] has been proposed by employing the idea of linear codes. The concept of combining the multivariate construction with linear codes is impressive. Therefore, a thorough study on the construction is required to explore the direction.
— Many application-specific variants of signature schemes with security reduction from MQ problems have remained largely unexplored. We concentrate our main focus on designing secure and efficient ring signature, blind signature, and proxy signature. Ring signature has potential applications in e-voting, anonymous authentication for ad-hoc groups, whistle blow, and so on. Blind signature is a crucial technique to provide anonymity in many information systems such as e-cash, e-voting, sensor networks, power industry, and smart grid systems. Proxy signatures have found numerous practical applications where the delegation of rights is quite common, particularly in distributed systems, Grid Computing, mobile agent applications, distributed shared object systems and mobile communications. Therefore, one may investigate whether the HFE central map can be employed in designing efficient constructions for the above variants of signature schemes and raise their profile with security reduction from MQ problems which have not drawn much attention despite their importance.

8 CONCLUSION

Several promising multivariate public key encryption and signature schemes have been described in this survey which can be used for constructing more efficient and secure schemes in the future. Description of some earlier schemes have been left out. The area is still growing and seems to have a bright future in the post quantum world. This survey is addressed mainly to researchers already having a solid background in cryptography and basic algebra. The multivariate public key schemes described here are summarized and might lack some details that can be found in the original articles.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable suggestions and comments which greatly improved the quality of the article.

REFERENCES

[1] Koichiro Akiyama, Yasuhiro Goto, and Hideyuki Miyake. 2009. An algebraic surface cryptosystem. In *Proceedings of the International Workshop on Public Key Cryptography.* Springer, 425–442.
[2] Daniel Apon, Dustin Moody, Ray Perlner, Daniel Smith-Tone, and Javier Verbel. 2020. Combinatorial rank attacks against the rectangular simple matrix encryption scheme. In *Proceedings of the International Conference on Post-Quantum Cryptography*. Springer, 307–322.
[3] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, and Jean-Pierre Tillich. 2020. An algebraic attack on rank metric code-based cryptosystems. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 64–93.

[4] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. 2020. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 507–536.
[5] Elwyn R. Berlekamp. 1967. Factoring polynomials over finite fields. *Bell System Technical Journal* 46, 8 (1967), 1853–1859.
[6] Luk Bettale, Jean-Charles Faugere, and Ludovic Perret. 2013. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography* 69, 1 (2013), 1–52.
[7] Ward Beullens. 2021. Improved cryptanalysis of UOV and rainbow. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 348–373.
[8] Ward Beullens. 2021. MAYO: Practical post-quantum signatures from oil-and-vinegar maps. *Cryptology ePrint Archive* (2021).
[9] Ward Beullens. 2022. Breaking rainbow takes a weekend on a laptop. *Cryptology ePrint Archive* (2022).
[10] Ward Beullens, Alan Szepieniec, Frederik Vercauteren, and Bart Preneel. 2017. LUOV: Signature scheme proposal for NIST PQC project. (2017).
[11] Olivier Billet and Henri Gilbert. 2006. Cryptanalysis of rainbow. In *Proceedings of the International Conference on Security and Cryptography for Networks*. Springer, 336–347.
[12] Bruno Buchberger. 1965. Ein algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. *PhD Thesis, Universitat Insbruck* (1965).
[13] Jonathan F. Buss, Gudmund S. Frandsen, and Jeffrey O. Shallit. 1999. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences* 58, 3 (1999), 572–596.
[14] Daniel Cabarcas, Daniel Smith-Tone, and Javier A. Verbel. 2017. Key recovery attack for ZHFE. In *International Workshop on Post-Quantum Cryptography*. Springer, 289–308.
[15] Felipe Cabarcas, Daniel Cabarcas, and John Baena. 2019. Efficient public-key operation in multivariate schemes. *Advances in Mathematics of Communications* 13, 2 (2019), 343.
[16] Ryann Cartor, Ryan Gipson, Daniel Smith-Tone, and Jeremy Vates. 2016. On the differential security of the HFEv-signature primitive. In *Proceedings of the Post-Quantum Cryptography*. Springer, 162–181.
[17] Ryann Cartor and Daniel Smith-Tone. 2018. EFLASH: A new multivariate encryption scheme. In *Proceedings of the International Conference on Selected Areas in Cryptography*. Springer, 281–299.
[18] Antoine Casanova, Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. 2017. Gemss: A great multivariate short signature. *Submission to NIST* (2017).
[19] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang. 2008. Odd-char multivariate hidden field equations. *IACR Cryptology ePrint Archive* 2008 (2008), 543.
[20] Jiahui Chen, Jianting Ning, Jie Ling, Terry Shue Chien Lau, and Yacheng Wang. 2020. A new encryption scheme for multivariate quadratic systems. *Theoretical Computer Science* 809 (2020), 372–383.
[21] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. 2018. SOFIA: MQ-based signatures in the QROM. In *Proceedings of the IACR International Workshop on Public Key Cryptography*. Springer, 3–33.
[22] Ming-Shing Chen, Bo-Yin Yang, and Daniel Smith-Tone. 2015. PFLASH-secure asymmetric signatures on smart cards. In *Proceedings of the Lightweight Cryptography Workshop*.
[23] Crystal Clough, John Baena, Jintai Ding, Bo-Yin Yang, and Ming-Shing Chen. 2009. Square, a new multivariate encryption scheme. In *Proceedings of the Cryptographers' Track at the RSA Conference*. Springer, 252–264.
[24] Don Coppersmith, Jacques Stern, and Serge Vaudenay. 1994. Attacks on the birational permutation signature schemes. In *Proceedings of the Advances in Cryptology–CRYPTO'93*. Springer, 435–443.
[25] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. 2000. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 392–407.
[26] Nicolas T. Courtois. 2001. The security of hidden field equations (HFE). In *Proceedings of the Cryptographers' Track at the RSA Conference*. Springer, 266–281.
[27] Nicolas T. Courtois, Magnus Daum, and Patrick Felke. 2003. On the security of HFE, HFEv-and Quartz. In *Proceedings of the International Workshop on Public Key Cryptography*. Springer, 337–350.
[28] NIST CSRC. 2017. Post-quantum Cryptography Standardization–Post-quantum Cryptography.
[29] Peter Czypek, Stefan Heyse, and Enrico Thomae. 2012. Efficient implementations of MQPKS on constrained devices. In *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 374–389.
[30] Taylor Daniels and Daniel Smith-Tone. 2014. Differential properties of the HFE cryptosystem. In *Proceedings of the International Workshop on Post-Quantum Cryptography*. Springer, 59–75.

[31] Jintai Ding. 2004. A new variant of the Matsumoto-Imai cryptosystem through perturbation. In *Proceedings of the International Workshop on Public Key Cryptography*. Springer, 305–318.
[32] Jintai Ding, Joshua Deaton, Vishakha, and Bo-Yin Yang. 2021. The nested subset differential attack. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 329–347.
[33] Jintai Ding, Jason E. Gower, and Dieter Schmidt. 2006. Zhuang-Zi: A new algorithm for solving multivariate polynomial equations over a finite field. *IACR Cryptology ePrint Archive* 2006 (2006), 38.
[34] Jintai Ding, Jason E. Gower, and Dieter S. Schmidt. 2006. *Multivariate Public Key Cryptosystems, Advances in Information Security*. Springer Science & Business Media.
[35] Jintai Ding, Lei Hu, Xuyun Nie, Jianyu Li, and John Wagner. 2007. High order linearization equation (hole) attack on multivariate public key cryptosystems. In *Proceedings of the International Workshop on Public Key Cryptography*. Springer, 233–248.
[36] Jintai Ding and Thorsten Kleinjung. 2011. Degree of regularity for HFE-. *IACR Cryptology ePrint Archive* 2011 (2011), 570.
[37] Jintai Ding, Momonari Kudo, Shinya Okumura, Tsuyoshi Takagi, and Chengdong Tao. 2016. Cryptanalysis of a public key cryptosystem based on diophantine equations via weighted LLL reduction (short paper). In *Proceedings of the International Workshop on Security*. Springer, 305–315.
[38] Jintai Ding, Ray Perlner, Albrecht Petzoldt, and Daniel Smith-Tone. 2018. Improved cryptanalysis of hfev-via projection. In *Proceedings of the International Conference on Post-Quantum Cryptography*. Springer, 375–395.
[39] Jintai Ding and Albrecht Petzoldt. 2017. Current state of multivariate cryptography. *IEEE Security & Privacy* 15, 4 (2017), 28–36.
[40] Jintai Ding, Albrecht Petzoldt, and Dieter S. Schmidt. 2020. *Multivariate Public Key Cryptosystems, Second Edition*. Advances in Information Security. Springer.
[41] Jintai Ding and Dieter Schmidt. 2005. Cryptanalysis of HFEv and internal perturbation of HFE. In *Proceedings of the International Workshop on Public Key Cryptography*. Springer, 288–301.
[42] Jintai Ding and Dieter Schmidt. 2005. Rainbow, a new multivariable polynomial signature scheme. In *Proceedings of the International Conference on Applied Cryptography and Network Security*. Springer, 164–175.
[43] Jintai Ding and Bo-Yin Yang. 2013. Degree of regularity for HFEv and HFEv. In *Proceedings of the International Workshop on Post-Quantum Cryptography*. Springer, 52–66.
[44] Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng. 2008. New differential-algebraic attacks and reparametrization of rainbow. In *Proceedings of the International Conference on Applied Cryptography and Network Security*. Springer, 242–257.
[45] Jintai Ding, Zheng Zhang, Joshua Deaton, Kurt Schmidt, and F. Vishakha. 2019. New attacks on lifted unbalanced oil vinegar. In *Proceedings of the 2nd NIST PQC Standardization Conference*.
[46] Jintai Ding, Zheng Zhang, Joshua Deaton, and Lih-Chung Wang. 2020. A complete cryptanalysis of the post-quantum multivariate signature scheme Himq-3. In *Proceedings of the International Conference on Information and Communications Security*. Springer, 422–440.
[47] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern. 2007. Practical cryptanalysis of SFLASH. In *Annual International Cryptology Conference*. Springer, 1–12.
[48] Dung H. Duong, Ha T. N. Tran, Willy Susilo, and Le Van Luyen. 2021. An efficient multivariate threshold ring signature scheme. *Computer Standards & Interfaces* 74 (2021), 103489.
[49] Ratna Dutta, Sumit Kumar Debnath, and Chinmoy Biswas. 2021. Storage friendly provably secure multivariate identity-based signature from isomorphism of polynomials problem. In *Proceedings of the 18th International Conference on Security and Cryptography*. SCITEPRESS, 595–602.
[50] Jean-Charles Faugere. 1999. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra* 139, 1–3 (1999), 61–88.
[51] Jean Charles Faugère. 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. ACM, 75–83.
[52] Jean-Charles Faugere and Antoine Joux. 2003. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *Proceedings of the Annual International Cryptology Conference*. Springer, 44–60.
[53] Jean-Charles Faugère, Gilles macario-Rat, Jacques Patarin, and Ludovic Perret. 2022. A new perturbation for multivariate public key schemes such as HFE and UOV. *Cryptology ePrint Archive* (2022).
[54] Jean-Charles Faugere and Pierre-Jean Spaenlehauer. 2010. Algebraic cryptanalysis of the PKC'2009 algebraic surface cryptosystem. In *Proceedings of the International Workshop on Public Key Cryptography*. Springer, 35–52.
[55] Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern. 2005. Differential cryptanalysis for multivariate schemes. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 341–353.

[56] Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, and Tsuyoshi Takagi. 2021. A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 187–217.
[57] Hiroki Furue, Koha Kinjo, Yasuhiko Ikematsu, Yacheng Wang, and Tsuyoshi Takagi. 2020. A structural attack on block-anti-circulant UOV at SAC 2019. In *Proceedings of the International Conference on Post-Quantum Cryptography*. Springer, 323–339.
[58] Michael R. Garey and David S. Johnson. 1979. Computers and intractability. *A Guide to the Theory of NP-Completeness* (1979).
[59] Louis Goubin and Nicolas T. Courtois. 2000. Cryptanalysis of the TTM cryptosystem. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 44–57.
[60] Yasufumi Hashimoto. 2015. Cryptanalysis of multi-HFE. *IACR Cryptology ePrint Archive* 2015 (2015), 1160.
[61] Yasufumi Hashimoto. 2018. High-rank attack on HMFEv. *JSIAM Letters* 10 (2018), 21–24.
[62] Yasufumi Hashimoto. 2018. Multivariate public key cryptosystems. In *Proceedings of the Mathematical Modelling for Next-Generation Cryptography*. Springer, 17–42.
[63] Yasufumi Hashimoto. 2021. Recent developments in multivariate public key cryptosystems. In *Proceedings of the International Symposium on Mathematics, Quantum Theory, and Cryptography*. Springer, Singapore, 209–229.
[64] Dung Hoang Duong, Willy Susilo, and Ha Thanh Nguyen Tran. 2020. A multivariate blind ring signature scheme. *The Computer Journal* 63, 8 (2020), 1194–1202.
[65] Ming-Deh A Huang, Michiel Kosters, Yun Yang, and Sze Ling Yeo. 2018. On the last fall degree of zero-dimensional Weil descent systems. *Journal of Symbolic Computation* 87 (2018), 207–226.
[66] Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. 2016. From 5-pass MQ-based identification to MQ-based signatures. *IACR Cryptol. ePrint Arch.* 2016 (2016), 708.
[67] Yasuhiko Ikematsu, Dung H. Duong, Albrecht Petzoldt, and Tsuyoshi Takagi. 2017. Revisiting the efficient key generation of ZHFE. In *Proceedings of the International Conference on Codes, Cryptology, and Information Security*. Springer, 195–212.
[68] Yasuhiko Ikematsu and Shuhei Nakamura. 2020. Security analysis against "A new encryption scheme for multivariate quadratic systems". *Cryptology ePrint Archive* (2020).
[69] Yasuhiko Ikematsu, Ray Perlner, Daniel Smith-Tone, Tsuyoshi Takagi, and Jeremy Vates. 2018. HFERP-a new multivariate encryption scheme. In *Proceedings of the International Conference on Post-Quantum Cryptography*. Springer, 396–416.
[70] Petar Ivanov and José Felipe Voloch. 2009. Breaking the Akiyama-Goto cryptosystem. *Contemporary Mathematics* 487 (2009), 113.
[71] Aviad Kipnis, Jacques Patarin, and Louis Goubin. 1999. Unbalanced oil and vinegar signature schemes. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 206–222.
[72] Aviad Kipnis and Adi Shamir. 1998. Cryptanalysis of the oil and vinegar signature scheme. In *Proceedings of the Annual International Cryptology Conference*. Springer, 257–266.
[73] Aviad Kipnis and Adi Shamir. 1999. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Proceedings of the Annual International Cryptology Conference*. Springer, 19–30.
[74] Nibedita Kundu, Sumit Kumar Debnath, and Dheerendra Mishra. 2021. A secure and efficient group signature scheme based on multivariate public key cryptography. *Journal of Information Security and Applications* 58 (2021), 102776.
[75] Nibedita Kundu, Sumit Kumar Debnath, Dheerendra Mishra, and Tanmay Choudhury. 2020. Post-quantum digital signature scheme based on multivariate cubic problem. *Journal of Information Security and Applications* 53 (2020), 102512.
[76] Le Van Luyen. 2019. An improved identity-based multivariate signature scheme based on rainbow. *Cryptography* 3, 1 (2019), 8.
[77] Gilles Macario-Rat and Jacques Patarin. 2021. UOV-pepper: New public key short signature in degree 3. *Cryptology ePrint Archive* (2021).
[78] Tsutomu Matsumoto and Hideki Imai. 1988. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 419–453.
[79] Mohamed Saied Emam Mohamed and Albrecht Petzoldt. 2017. RingRainbow–an efficient multivariate ring signature scheme. In *Proceedings of the International Conference on Cryptology in Africa*. Springer, 3–20.
[80] Dustin Moody, Ray Perlner, and Daniel Smith-Tone. 2014. An asymptotically optimal structural attack on the ABC multivariate encryption scheme. In *Proceedings of the International Workshop on Post-Quantum Cryptography*. Springer, 180–196.
[81] Shinya Okumura. 2015. A public key cryptosystem based on diophantine equations of degree increasing type. *Pacific Journal of Mathematics for Industry* 7, 1 (2015), 4.

[82] Morten Øygarden, Patrick Felke, Håvard Raddum, and Carlos Cid. 2020. Cryptanalysis of the multivariate encryption scheme EFLASH. In *Proceedings of the Cryptographers' Track at the RSA Conference*. Springer, 85–105.
[83] Jacques Patarin. 1995. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In *Proceedings of the Annual International Cryptology Conference*. Springer, 248–261.
[84] Jacques Patarin. 1996. 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*. Springer, 33–48.
[85] Jacques Patarin. 1997. The oil and vinegar algorithm for signatures. In *Proceedings of the Dagstuhl Workshop on Cryptography, 1997*.
[86] Jacques Patarin, Nicolas Courtois, and Louis Goubin. 2001. Flash, a fast multivariate signature algorithm. In *Proceedings of the Cryptographers' Track at the RSA Conference*. Springer, 298–307.
[87] Jacques Patarin, Nicolas Courtois, and Louis Goubin. 2001. Quartz, 128-bit long digital signatures. In *Proceedings of the Cryptographers' Track at the RSA Conference*. Springer, 282–297.
[88] Jacques Patarin, Louis Goubin, and Nicolas Courtois. 1998. C-+* and HM: Variations around two schemes of T. Matsumoto and H. Imai. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 35–50.
[89] Ray Perlner, Albrecht Petzoldt, and Daniel Smith-Tone. 2017. Total break of the SRP encryption scheme. In *Proceedings of the International Conference on Selected Areas in Cryptography*. Springer, 355–373.
[90] Ray Perlner and Daniel Smith-Tone. 2016. Security analysis and key modification for ZHFE. In *Proceedings of the Post-Quantum Cryptography*. Springer, 197–212.
[91] Albrechtc Petzoldt, Stanislav Bulygin, and Johannes Buchmann. 2010. CyclicRainbow-a multivariate signature scheme with a partially cyclic public key. In *Proceedings of the International Conference on Cryptology in India*. Springer, 33–48.
[92] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann. 2010. A multivariate signature scheme with a partially cyclic public key. In *Proceedings of the SCC 2010*. 229–235.
[93] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann. 2013. A multivariate based threshold ring signature scheme. *Applicable Algebra in Engineering, Communication and Computing* 24, 3–4 (2013), 255–275.
[94] Albrecht Petzoldt, Ming-Shing Chen, Jintai Ding, and Bo-Yin Yang. 2017. HMFEv-an efficient multivariate signature scheme. In *Proceedings of the International Workshop on Post-quantum Cryptography*. Springer, 205–223.
[95] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. 2015. Design principles for HFEv-based multivariate signature schemes. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 311–334.
[96] Albrecht Petzoldt, Alan Szepieniec, and Mohamed Saied Emam Mohamed. 2017. A practical multivariate blind signature scheme. In *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, 437–454.
[97] Jaiberth Porras, John Baena, and Jintai Ding. 2014. New candidates for multivariate trapdoor functions. *IACR Cryptology ePrint Archive* 2014 (2014), 387.
[98] Jaiberth Porras, John Baena, and Jintai Ding. 2014. ZHFE, a new multivariate public key encryption scheme. In *Proceedings of the International Workshop on Post-quantum Cryptography*. Springer, 229–245.
[99] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. 2011. Public-key identification schemes based on multivariate quadratic polynomials. In *Proceedings of the Annual Cryptology Conference*. Springer, 706–723.
[100] Peter Schwabe and Bas Westerbaan. 2016. Solving binary MQ with Grover's algorithm. In *Proceedings of the International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer, 303–322.
[101] Wuqiang Shen, Shaohua Tang, and Lingling Xu. 2013. IBUOV, A provably secure identity-based UOV signature scheme. In *Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering*. IEEE, 388–395.
[102] Peter W. Shor. 1994. Polynomial-time algorithms for prime factorization and discrete logarithms. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. 124–134.
[103] Daniel Smith-Tone and Cristina Tone. 2021. A multivariate cryptosystem inspired by random linear codes. *Finite Fields and Their Applications* 69 (2021), 101778.
[104] Alan Szepieniec and Bart Preneel. 2019. Block-anti-circulant unbalanced oil and vinegar. In *Proceedings of the International Conference on Selected Areas in Cryptography*. Springer, 574–588.
[105] Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding. 2013. Simple matrix scheme for encryption. In *Proceedings of the International Workshop on Post-Quantum Cryptography*. Springer, 231–242.
[106] Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. 2021. Efficient key recovery for all HFE signature variants. In *Proceedings of the Annual International Cryptology Conference*. Springer, 70–93.

[107] Chengdong Tao, Hong Xiang, Albrecht Petzoldt, and Jintai Ding. 2015. Simple matrix–a multivariate public key cryptosystem (MPKC) for encryption. *Finite Fields and Their Applications* 35 (2015), 352–368.
[108] Vasyl Ustimenko. 2017. On new multivariate cryptosystems based on hidden Eulerian equations over finite fields. *IACR Cryptology ePrint Archive* 2017 (2017), 93.
[109] Jeremy Vates and Daniel Smith-Tone. 2017. Key recovery attack for all parameters of HFE. In *Proceedings of the International Workshop on Post-Quantum Cryptography.* Springer, 272–288.
[110] Javier Verbel, John Baena, Daniel Cabarcas, Ray Perlner, and Daniel Smith-Tone. 2019. On the complexity of "superdetermined" Minrank instances. In *Proceedings of the International Conference on Post-Quantum Cryptography*. Springer, 167–186.
[111] Shangping Wang, Rui Ma, Yaling Zhang, and Xiaofeng Wang. 2011. Ring signature scheme based on multivariate public key cryptosystems. *Computers & Mathematics with Applications* 62, 10 (2011), 3973–3979.
[112] Guangdong Yang, Shaohua Tang, and Li Yang. 2011. A novel group signature scheme based on mpkc. In *Proceedings of the International Conference on Information Security Practice and Experience*. Springer, 181–195.
[113] Takanori Yasuda. 2018. Multivariate encryption schemes based on the constrained MQ problem. In *Proceedings of the International Conference on Provable Security*. Springer, 129–146.
[114] Takanori Yasuda and Kouichi Sakurai. 2015. A multivariate encryption scheme with rainbow. In *Proceedings of the International Conference on Information and Communications Security.* Springer, 236–251.
[115] Takanori Yasuda, Yacheng Wang, and Tsuyoshi Takagi. 2020. Multivariate encryption schemes based on polynomial equations over real numbers. In *Proceedings of the International Conference on Post-Quantum Cryptography*. Springer, 402–421.
[116] Jingwan Zhang and Yiming Zhao. 2015. A new multivariate based threshold ring signature scheme. In *Proceedings of the International Conference on Network and System Security*. Springer, 526–533.
[117] Wenbin Zhang and Chik How Tan. 2015. MI-T-HFE, a new multivariate signature scheme. In *Proceedings of the IMA International Conference on Cryptography and Coding*. Springer, 43–56.
[118] Wenbin Zhang and Chik How Tan. 2016. On the security and key generation of the ZHFE encryption scheme. In *Proceedings of the International Workshop on Security.* Springer, 289–304.

Received 28 June 2021; revised 25 September 2022; accepted 2 November 2022