Efficient Key Recovery for all HFE Signature Variants

Chengdong Tao[2], Albrecht Petzoldt[3], Jintai Ding[1,2†]

[1] Yau Mathematical Center, Tsinghua University, Beijing, China
[2] Ding Lab, Beijing Institute of Mathematical Sci. and Applications, Beijing, China
[3] FAU Erlangen-Nuremberg, Nuremberg, Germany

†: corresponding author: Jintai Ding (jintai.ding@gmail.com)

Abstract. The HFE cryptosystem is one of the most popular multivariate schemes. Especially in the area of digital signatures, the HFEv- variant offers short signatures and high performance. Recently, an instance of the HFEv- signature scheme called GeMSS was selected as one of the alternative candidates for signature schemes in the third round of the NIST Post-Quantum Crypto (PQC) Standardization Project.
In this paper, we propose a new key recovery attack on the HFEv- signature scheme. Our attack shows that both the Minus and the Vinegar modification do not enhance the security of the basic HFE scheme significantly. This shows that it is very difficult to build a secure and efficient signature scheme on the basis of HFE. In particular, we use our attack to show that the proposed parameters of the GeMSS scheme are not as secure as claimed.

Keywords: Multivariate Cryptography · HFEv- · Key Recovery · MinRank · NIST Standardization Process

1 Introduction

Cryptographic techniques such as encryption and digital signatures are an indispensable part of modern communication systems. However, the currently used schemes RSA and ECDSA become insecure as soon as large quantum computers arrive. Due to recent progress in the development of such computers, there is an urgent need for alternatives to these classical schemes which are resistant against attacks with quantum computers. These are known as post-quantum cryptosystems [4, 6].

One of the main candidates for such schemes are multivariate public key cryptosystems [15]. Especially in the area of digital signatures, there exist many promising multivariate schemes. In fact, the multivariate signature scheme Rainbow is among the three signature schemes in the third round of the NIST standardization process of post-quantum cryptosystems [8]. Another multivariate signature scheme, GeMMS, is one of the alternative candidates. GeMMS is a special instance of

the well known HFEv- signature scheme, which was first proposed by Patarin et al. in [26]. The principle idea of HFEv- is to combine the Minus and the Vinegar modifications with the HFE cryptosystem of [25]. Since the resulting multivariate quadratic system contains more variables than equations, HFEv- can only be used for digital signatures.

Attacks against HFEv- and Related Work. There exist many attack methods on HFEv-, such as the direct attack [9][27], the distinguishing attack [13], the differential attack [7], and the MinRank attack [13]. The most studied attack against HFEv- is the MinRank attack, which was first proposed by Kipnis and Shamir in [23]. Later, many variants of this technique have been proposed to increase its efficiency. The most prominent examples of this are the minors modeling of Bettale, Faugére and Perret [3] as well as the support minors modelling of Bardet, Bros, Cabarcas, Gaborit, Perlner, Smith-Tone, Tillich and Verbel [1]. Another recent paper closely related to our work is that of Beullens [2]. The main difference to our paper is that Beullens studies MinRank type attacks against SingleField schemes such as Rainbow, while we are interested in applying this attack to BigField schemes.
In this paper, we mainly consider the MinRank attack using minors modeling as a reference. According to [3], the complexity of this attack is given as

$$\mathcal{O}\left(\binom{n+d+a+v+1}{d+a+v+1}^{\omega}\right),$$

where n is the degree of the field extension, $d = \lceil \log_q(D) \rceil$, where D is the degree bound on the HFE central polynomial, a is the number of Minus equations, v is the number of Vinegar variables and $2 < \omega \leq 3$ is the linear algebra constant. More information about the different strategies to solve the MinRank problem can be found in Section 3.2.

Our Contribution. In this paper, we present an improved MinRank type key recovery attack on the HFEv- signature scheme. The complexity of our new attack on HFEv- using minors modeling is

$$\mathcal{O}\left(\binom{n+d+v+1}{d+1}^{\omega}\right).$$

This shows that the Minus modification does not enhance the security of HFE type cryptosystems, while the Vinegar modification increases the complexity of our attack only by a polynomial factor. This shows that the currently used techniques are insufficient to transform HFE into a secure signature scheme. In particular, we use our attack to show that the parameters of GeMSS which were submitted to the NIST Post-Quantum Crypto Standardization Project are not as secure as claimed.
The remainder of this paper is organized as follows. Section 2 gives a short introduction into multivariate cryptography and introduces the HFEv- signature scheme, while Section 3 repeats some cryptanalytic concepts used in the further

parts of the paper. In Section 4 we present our attack against the HFEv- signature scheme and analyze its complexity. Section 5 discusses a possible speed up of our attack by solving the MinRank problem using the support minors modeling and Section 6 analyzes the importance of our attack on the NIST alternative candidate GeMMS. Finally, Section 7 concludes the paper.

2 Multivariate Cryptography

The public key of a multivariate public key cryptosystem is a system of quadratic polynomials in several variables over a finite field $\mathbb{F}_q$ of q elements, i.e.

$$\begin{aligned} p^{(1)}(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} \alpha_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} \beta_i^{(1)} x_i + \gamma^{(1)}, \\ &\vdots \\ p^{(m)}(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} \alpha_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} \beta_i^{(m)} x_i + \gamma^{(m)}. \end{aligned}$$

The problem of inverting such a system is known as the MQ problem and was proven to be NP hard [20].

In order to construct a digital signature scheme on the basis of the MQ problem, one starts with an easily invertible quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ (central map). To hide the structure of this map in the public key, one combines $\mathcal{F}$ with two randomly chosen invertible affine maps $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The public key of a multivariate signature scheme is therefore given as

$$\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^m,$$

the private key of the scheme consists of the three maps $\mathcal{T}$, $\mathcal{F}$ and $\mathcal{S}$.

In order to generate a signature for a document $d \in \{0,1\}^\star$, the owner of the private key performs the following steps.

1. Use a hash function $\mathcal{H}$ to compute the hash value $\mathbf{h} = \mathcal{H}(d) \in \mathbb{F}_q^m$.
2. Compute $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{h}) \in \mathbb{F}_q^m$.
3. Find a pre-image $\mathbf{y} \in \mathbb{F}_q^n$ of $\mathbf{x}$ under the central map $\mathcal{F}$.
4. Compute the signature $\mathbf{z} \in \mathbb{F}_q^n$ of the document d as $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{y})$.

To check the corrrectness of a message/signature pair $(d, \mathbf{z})$, one simply computes $\mathbf{h} = \mathcal{H}(d)$ and $\mathbf{h}' = \mathcal{P}(\mathbf{z})$. The signature is accepted, if and only if $\mathbf{h} = \mathbf{h}'$ holds. The process of signature generation and verification is illustrated by Figure 1.

2.1 The HFEv- Signature Scheme

The HFEv- signature scheme is an example of a multivariate BigField scheme. In such a scheme, the central map $\mathcal{F}$ is a univariate map over a degree n extension

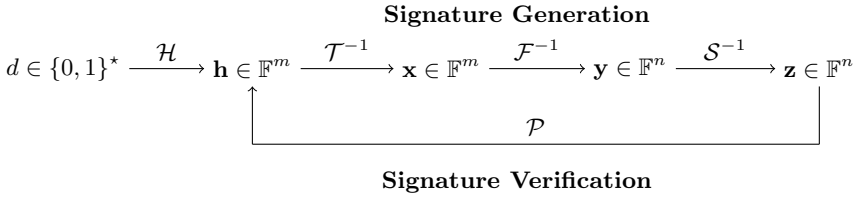

Fig. 1. Signature Generation and Verification Process for Multivariate Signature Schemes

field $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. Using an isomorphism ϕ between the field $\mathbb{F}_{q^n}$ and the vector space $\mathbb{F}_q^n$, we can transform the univariate polynomial map $\mathcal{F}$ into a quadratic map $\bar{\mathcal{F}} = \phi \circ \mathcal{F} \circ \phi^{-1}$ over the vector space $\mathbb{F}_q^n$ (see Figure 2).

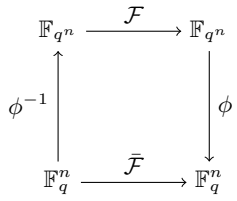

Fig. 2. Construction of the Central Map for Multivariate BigField Schemes

The HFEv- signature scheme uses three integer parameters D, a and v. The three algorithms for key generation, signature generation and signature verification can be described as follows.

Key Generation. In order to generate a key pair for the HFEv- signature scheme, one randomly generates a polynomial (the central map) of the form

$$\mathcal{F}(X, x_{n+1}, \ldots, x_{n+v}) = \sum_{i,j \in \mathbb{N}}^{q^i+q^j \leq D} \alpha_{ij} X^{q^i+q^j} + \sum_{i \in \mathbb{N}}^{q^i \leq D} \beta_i(x_{n+1}, \ldots, x_{n+v}) X^{q^i} + \gamma(x_{n+1}, \ldots, x_{n+v}).$$

So, $\mathcal{F}$ is a map from $\mathbb{F}_{q^n} \times \mathbb{F}_q^v$ to $\mathbb{F}_{q^n}$, where the $\alpha_{i,j}$ are randomly chosen elements of the field $\mathbb{F}_{q^n}$, the $\beta_i : \mathbb{F}_q^v \to \mathbb{F}_{q^n}$ are linear maps from the vector space $\mathbb{F}_q^v$ to the field $\mathbb{F}_{q^n}$ and $\gamma : \mathbb{F}_q^v \to \mathbb{F}_{q^n}$ is a quadratic map in the Vinegar variables $x_{n+1}, x_{n+2}, \ldots, x_{n+v}$.
Due to the special structure of it, the central map $\mathcal{F}$ corresponds to a quadratic map $\bar{\mathcal{F}} = \phi \circ \mathcal{F} \circ \phi^{-1} : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^n$. Furthermore, in order to hide the structure of the central map $\mathcal{F}$ in the public key, one randomly chooses two affine transfor-

mations $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-a}$ and $\mathcal{S} : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n+v}$ of maximal rank.
Therefore, the public key of the scheme is the quadratic map

$$\mathcal{P} = \mathcal{T} \circ \bar{\mathcal{F}} \circ \mathcal{S} = \mathcal{T} \circ \phi \circ \mathcal{F} \circ (\phi^{-1} \times id_v) \circ \mathcal{S} : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n-a}.$$

The *private key* of the HFEv- scheme consists of the three maps $\mathcal{T}$, $\mathcal{F}$ and $\mathcal{S}$, the *public key* is given by $\mathcal{P}$.

Signature Generation. Let $d \in \{0,1\}^\star$ be a document to be signed. The process of signature generation works as follows:

1. Use a hash function $\mathcal{H} : \{0,1\}^\star \to \mathbb{F}_q^{n-a}$ to compute the hash value $\mathbf{h} = (h_1, \ldots, h_{n-a}) \in \mathbb{F}_q^{n-a}$ of the document d.
2. Compute a pre-image $\mathbf{x} \in \mathbb{F}_q^n$ of $\mathbf{h}$ under the affine transformation $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-a}$ and lift it to the extension field, obtaining $X = \phi^{-1}(\mathbf{x}) \in \mathbb{F}_{q^n}$.
3. Choose random values for the Vinegar variables $(y_{n+1}, \ldots, y_{n+v}) \in \mathbb{F}_q^v$ and substitute them into the central map $\mathcal{F}$ to obtain a univariate polynomial map $\mathcal{F}_V(Z) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$.
4. Find a solution to the equation $\mathcal{F}_V(Z) = X$ using Berlekamps algorithm. If this equation has no solution, go back to step 2, and randomly choose another vector $(y_{n+1}, \ldots, y_{n+v}) \in \mathbb{F}_q^v$ until we can find a solution. Let $Y \in \mathbb{F}_{q^n}$ be one of the solutions and set $\mathbf{y}' = \phi(Y) = (y_1, \cdots, y_n) \in \mathbb{F}_q^n$. Append the Vinegar variables of step 2 to it, obtaining $\mathbf{y} = (\mathbf{y}', y_{n+1}, \cdots, y_{n+v}) \in \mathbb{F}_q^{n+v}$.
5. Compute $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{y})$. Then $\mathbf{z} \in \mathbb{F}_q^{n+v}$ is the signature of the document d.

Signature Verification. To check if $\mathbf{z} \in \mathbb{F}_q^{n+v}$ is indeed a valid signature for the document $d \in \{0,1\}^\star$, the receiver simply computes

- $\mathbf{h} = \mathcal{H}(d) \in \mathbb{F}_q^{n-a}$ and
- $\mathbf{h}' = \mathcal{P}(\mathbf{z})$.

If $\mathbf{h}' = \mathbf{h}$ holds, the signature is accepted, otherwise it is rejected.

Efficiency. The most costly step during the signature generation of HFEv- is the solution of the polynomial equation $\mathcal{F}_V(Z) = X$ by Berlekamps algorithm. The complexity of this algorithm is given as

$$O(D^\omega + Dn(log(D)log(log(D))log(q))),$$

(see [15]) where D is the degree of the HFE polynomial, n is the degree of the extension field $\mathbb{F}_{q^n}$ and q is the cardinality of the base field.
A higher value of D therefore slows down the signature generation process of HFEv- drastically.
One important strategy for the design of HFE based signature schemes was therefore to choose D small and to compensate for this fact by increasing a and v.

2.2 Previous Attacks on HFE

Historically, the most efficient attacks against signature schemes of the HFE type are the direct and the MinRank attack. With regard to the direct attack, it was discovered that the public systems of HFE and its variants can be solved much more efficiently than random systems. This phenomenon was analyzed in a series of papers [11, 12, 16]. The authors of these papers found that the degree of regularity of a public HFEv- system is bounded from above by

$$\begin{cases} \frac{(q-1)(d+v+a-1)}{2}+2 & \text{if } q \text{ is even and } d+a \text{ is odd,} \\ \frac{(q-1)(d+v+a)}{2}+2 & \text{otherwise.} \end{cases}$$

Regarding attacks of the MinRank type, many researchers considered the so called min-Q-rank of the HFE system, which can be seen as the rank of the quadratic form $\mathcal{P}$ lifted to the extension field $\mathbb{F}_{q^n}$. Similar to the degree of regularity, the min-Q-rank of the HFE system is bounded by the HFE parameters. However, in our attack, we don't consider the min-Q-rank of the HFE system, but perform a MinRank attack over the base field $\mathbb{F}_q$. While it is clear that the complexity of a direct attack on a system of the HFE type is exponential in d, a and v [10], our attack shows that this is not the case for MinRank. We take a closer look at the MinRank problem and different strategies to solve it in Section 3.2.

3 Preliminaries

For simplification, in the following sections of this paper, we assume that $\mathcal{T}$ and $\mathcal{S}$ are linear transformations and q is an odd prime. Our attack method can be easily extended to the case of affine maps $\mathcal{T}$ and $\mathcal{S}$ and even characteristic.

3.1 Equivalent Keys

An important notion in this paper is that of equivalent keys. For a multivariate public key cryptosystem, the concept of equivalent keys is defined as follows.

Definition 1. *Let $((\mathcal{T},\mathcal{F},\mathcal{S}),\mathcal{P})$ be a key pair of a multivariate public key cryptosystem. A tuple $(\mathcal{T}',\mathcal{F}',\mathcal{S}')$ is called an equivalent private key if and only if*

$$\mathcal{P}=\mathcal{T}\circ\mathcal{F}\circ\mathcal{S}=\mathcal{T}'\circ\mathcal{F}'\circ\mathcal{S}'$$

and $\mathcal{F}'$ is a valid central map of the cryptosystem, i.e. $\mathcal{F}'$ has the same algebraic structure as $\mathcal{F}$.

We have

Theorem 1 (Theorem 4.13 in [28]). *Let $\mathcal{P}$ be a public key of the HFEv- scheme over $\mathbb{F}_q$. Let v be the number of Vinegar variables, a be the number of Minus equations and n be the degree of the field extension. Then there exist*

$$nq^{a+2n+vn}(q^n-1)^2\prod_{i=0}^{v-1}(q^v-q^i)\prod_{i=n-a-1}^{n-1}(q^n-q^i)$$

equivalent private keys for the public key $\mathcal{P}$.

Given an HFEv- public key $\mathcal{P}$, our attack finds one of the equivalent private keys.

3.2 The MinRank Problem

The search version of the MinRank problem is defined as follows.

Definition 2 (MinRank problem). *Given a positive number r and n_x matrices $M_1, M_2, \ldots, M_{n_x}$ with m rows and n columns over a field $\mathbb{F}_q$, find a nonzero vector $(x_1, x_2, \ldots, x_{n_x}) \in \mathbb{F}_q^{n_x}$, such that the linear combination $M = \sum_{i=1}^{n_x} x_i M_i$ has rank at most r.*

The MinRank problem is an NP-complete problem [5]. The main methods for solving the MinRank problem are linear algebra search [21], Kipnis-Shamir modeling [23], minors modeling [19] and support minors modeling [1].

In this paper, we mostly consider the minors modeling of the MinRank attack. The main idea of this modeling is that the $r+1$ minors of the low rank matrix M are all zero. Since there are $\binom{n}{r+1}$ minors and n_x variables $x_1, \ldots, x_{n_x}$, this gives us a highly overdetermined system of equations of degree $r+1$, which can be solved by e.g. Gröbner basis techniques. The complexity of this process can be estimated as

$$\text{complexity}_{\text{minors modelling}} = \mathcal{O}\left(\binom{n+r+1}{r+1}^{\omega}\right),$$

where, for previous attacks against HFEv-, r was given as $d+v+a$. We show, how this value can be dropped to d.

In Section 5 of this paper we show how our attack might be sped up using the support minors modeling approach. However, since we don't have a full theoretical understanding of the outcome of our experiments yet, we leave a complete analysis of our attack using support minors modeling as a future work.

3.3 Matrix Representation of HFEv- Keys

Similar to [3], we represent the HFEv- central map in matrix form.

Proposition 1. *Let*

$$F^{*0} = \begin{pmatrix} \alpha_{00} & \alpha_{01} & \cdots & \alpha_{0,n-1} & \gamma_{00} & \gamma_{01} & \cdots & \gamma_{0,v-1} \\ \alpha_{10} & \alpha_{11} & \cdots & \alpha_{1,n-1} & \gamma_{10} & \gamma_{11} & \cdots & \gamma_{1,v-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1,0} & \alpha_{n-1,1} & \cdots & \alpha_{n-1,n-1} & \gamma_{n-1,0} & \gamma_{n-1,1} & \cdots & \gamma_{n-1,v-1} \\ \beta_{00} & \beta_{01} & \cdots & \beta_{0,n-1} & \delta_{00} & \delta_{01} & \cdots & \delta_{0,v-1} \\ \beta_{10} & \beta_{11} & \cdots & \beta_{1,n-1} & \delta_{10} & \delta_{11} & \cdots & \delta_{1,v-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{v-1,0} & \beta_{v-1,1} & \cdots & \beta_{v-1,n-1} & \delta_{v-1,0} & \delta_{v-1,1} & \cdots & \delta_{v-1,v-1} \end{pmatrix}$$

be an $(n+v)\times(n+v)$ *matrix over the field* $\mathbb{F}_{q^n}$ *and*

$$F(X, x_1, \ldots, x_v) = (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v) F^{*0} (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v)^t$$

be a polynomial in the quotient ring $\mathbb{F}_{q^n}[X, x_1, \ldots, x_v]/\langle x_1^q - x_1, \ldots, x_v^q - x_v\rangle$. *Then we have for all* $0 \le k < n$

$$F^{q^k}(X, x_1, \ldots, x_v) = (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v) F^{*k} (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v)^t,$$

where $F^{*k} \in \mathcal{M}_{(n+v)\times(n+v)}(\mathbb{F}_{q^n})$, *the* (i,j)*-th entry of* F^{*k} *is* $\alpha_{i-k,j-k}^{q^k}$ *for all* $0 \le i,j,k < n$, *the* $(i, n+j)$*-th entry of* F^{*k} *is* $\gamma_{j-k,i}^{q^k}$ *for all* $0 \le j,k < n$, $0 \le i < v$, *the* $(n+i, j)$*-th entry of* F^{*k} *is* $\beta_{i,j-k}^{q^k}$ *for all* $0 \le i < v, 0 \le j,k < n$, *and the* $(n+i, n+j)$*-th entry is* $\delta_{ij}^{q^k}$ *for all* $0 \le i < v, 0 \le j < v, 0 \le k < n$.

Proof. If $k = 0$, we have obviously $F^{q^k}(X, x_1, \cdots, x_v) = F(X, x_1, \cdots, x_v)$. Now we consider the case of $1 \le k < n$. Since $x_i^{q^k} = x_i$ for all $1 \le i \le v$, we have

$$\begin{aligned} F^{q^k} &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \alpha_{ij}^{q^k} X^{q^{i+k}+q^{j+k}} + \sum_{i=0}^{v-1}\sum_{j=0}^{n-1} (\beta_{ij}^{q^k} + \gamma_{ji}^{q^k}) x_i X^{q^{j+k}} + \sum_{i=0}^{v-1}\sum_{j=0}^{v-1} \delta_{ij}^{q^k} x_i x_j \\ &= \sum_{i=k}^{n-1+k}\sum_{j=k}^{n-1+k} \alpha_{i-k,j-k}^{q^k} X^{q^i+q^j} + \sum_{i=0}^{v-1}\sum_{j=k}^{n-1+k} (\beta_{i,j-k}^{q^k} + \gamma_{j-k,i}^{q^k}) x_i X^{q^j} + \sum_{i=0}^{v-1}\sum_{j=0}^{v-1} \delta_{ij}^{q^k} x_i x_j \end{aligned}$$

Then it can be divided as follows

$$\begin{aligned} F^{q^k} = &\sum_{i=k}^{n-1} \left(\sum_{j=k}^{n-1+k} \alpha_{i-k,j-k}^{q^k} X^{q^i+q^j} \right) + \sum_{i=n}^{n-1+k} \left(\sum_{j=k}^{n-1+k} \alpha_{i-k,j-k}^{q^k} X^{q^i+q^j} \right) \\ &+ \sum_{i=0}^{v-1}\sum_{j=k}^{n-1} (\beta_{i,j-k}^{q^k} + \gamma_{j-k,i}^{q^k}) x_i X^{q^j} + \sum_{i=0}^{v-1}\sum_{j=n}^{n-1+k} (\beta_{i,j-k}^{q^k} + \gamma_{j-k,i}^{q^k}) x_i X^{q^j} + \sum_{i=0}^{v-1}\sum_{j=0}^{v-1} \delta_{ij}^{q^k} x_i x_j. \end{aligned}$$

That is

$$\begin{aligned}F^{q^k} &= \sum_{i=k}^{n-1}\left(\sum_{j=k}^{n-1}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}+\sum_{j=n}^{n-1+k}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}\right)\\ &+\sum_{i=n}^{n-1+k}\left(\sum_{j=k}^{n-1}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}+\sum_{j=n}^{n-1+k}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}\right)\\ &+\sum_{i=0}^{v-1}\sum_{j=k}^{n-1}(\beta_{i,j-k}^{q^k}+\gamma_{j-k,i}^{q^k})x_iX^{q^j}+\sum_{i=0}^{v-1}\sum_{j=n}^{n-1+k}(\beta_{i,j-k}^{q^k}+\gamma_{j-k,i}^{q^k})x_iX^{q^j}+\sum_{i=0}^{v-1}\sum_{j=0}^{v-1}\delta_{ij}^{q^k}x_ix_j.\end{aligned}$$

Thus we have

$$\begin{aligned}F^{q^k} &= \sum_{i=k}^{n-1}\left(\sum_{j=k}^{n-1}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}+\sum_{j=0}^{k-1}\alpha_{i-k,j-k+n}^{q^k}X^{q^i+q^{j+n}}\right)\\ &+\sum_{i=0}^{k-1}\left(\sum_{j=k}^{n-1}\alpha_{i-k+n,j-k}^{q^k}X^{q^{i+n}+q^j}+\sum_{j=0}^{k-1}\alpha_{i-k+n,j-k+n}^{q^k}X^{q^{i+n}+q^{j+n}}\right)\\ &+\sum_{i=0}^{v-1}\sum_{j=k}^{n-1}(\beta_{i,j-k}^{q^k}+\gamma_{j-k,i}^{q^k})x_iX^{q^j}+\sum_{i=0}^{v-1}\sum_{j=0}^{k-1}(\beta_{i,j-k+n}^{q^k}+\gamma_{j-k+n,i}^{q^k})x_iX^{q^{j+n}}+\sum_{i=0}^{v-1}\sum_{j=0}^{v-1}\delta_{ij}^{q^k}x_ix_j.\end{aligned}$$

Since $X^{q^n}=X$ we obtain by reducing the index of coefficients modulo n

$$\begin{aligned}F^{q^k} &= \sum_{i=k}^{n-1}\left(\sum_{j=k}^{n-1}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}+\sum_{j=0}^{k-1}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}\right)\\ &+\sum_{i=0}^{k-1}\left(\sum_{j=k}^{n-1}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}+\sum_{j=0}^{k-1}\alpha_{i-k,j-k}^{q^k}X^{q^i+q^j}\right)\\ &+\sum_{i=0}^{v-1}\sum_{j=k}^{n-1}(\beta_{i,j-k}^{q^k}+\gamma_{j-k,i}^{q^k})x_iX^{q^j}+\sum_{i=0}^{v-1}\sum_{j=0}^{k-1}(\beta_{i,j-k}^{q^k}+\gamma_{j-k,i}^{q^k})x_iX^{q^j}+\sum_{i=0}^{v-1}\sum_{j=0}^{v-1}\delta_{ij}^{q^k}x_ix_j.\end{aligned}$$

Grouping the sums back together, we get

$$\begin{aligned}F^{q^k} &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}a_{i-k,j-k}^{q^k}X^{q^i+q^j}+\sum_{i=0}^{v-1}\sum_{j=0}^{n-1}(\beta_{i,j-k}^{q^k}+\gamma_{j-k,i}^{q^k})x_iX^{q^j}+\sum_{i=0}^{v-1}\sum_{j=0}^{v-1}\delta_{ij}^{q^k}x_ix_j\\ &= (X,X^q,\cdots,X^{q^{n-1}},x_1,\cdots,x_v)F^{*k}(X,X^q,\cdots,X^{q^{n-1}},x_1,\cdots,x_v)^t,\end{aligned}$$

where $F^{*k}\in\mathcal{M}_{(n+v)\times(n+v)}(\mathbb{F}_{q^n})$, the (i,j)-th entry of F^{*k} is $\alpha_{i-k,j-k}^{q^k}$ for all $0\le i,j,k<n$, the $(i,n+j)$-th entry of F^{*k} is $\gamma_{j-k,i}^{q^k}$ for all $0\le j,k<n, 0\le i<v$, the $(n+i,j)$-th entry of F^{*k} is $\beta_{i,j-k}^{q^k}$ for all $0\le i<v, 0\le j,k<n$, and the $(n+i,n+j)$-th entry is $\delta_{ij}^{q^k}$ for all $0\le i<v, 0\le j<v, 0\le k<n$. □

Proposition 2 (Proposition 2.1 in [3]). *Let $(\theta_1,\theta_2,\cdots,\theta_n)\in\mathbb{F}_{q^n}^n$ be a vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and*

$$M=\begin{pmatrix}\theta_1 & \theta_1^q & \cdots & \theta_1^{q^{n-1}}\\ \theta_2 & \theta_2^q & \cdots & \theta_2^{q^{n-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \theta_n & \theta_n^q & \cdots & \theta_n^{q^{n-1}}\end{pmatrix}$$

be the matrix whose columns are the Frobenius powers of the basis elements. We can express the morphism $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ *as*

$$V \mapsto (V, V^q, \cdots, V^{q^{n-1}})M^{-1}.$$

Its inverse $\phi^{-1} : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ *is given as*

$$(v_1, v_2, \cdots, v_n) \mapsto V,$$

where V *is the first component of the vector* $(v_1, v_2, \cdots, v_n)M$*. More generally, we have*

$$(v_1, v_2, \cdots, v_n) \cdot M = (V, V^q, \cdots, V^{q^{n-1}}).$$

In this paper, we choose

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^q & \cdots & \theta^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1} & (\theta^{n-1})^q & \cdots & (\theta^{n-1})^{q^{n-1}} \end{pmatrix}, \tag{1}$$

where θ is a generator of $\mathbb{F}_{q^n}$. Define

$$\widetilde{M} = \begin{pmatrix} M & 0 \\ 0 & I_v \end{pmatrix} \in \mathcal{M}_{(n+v)\times(n+v)}(\mathbb{F}_{q^n}), \tag{2}$$

where I_v is the $v \times v$ identity matrix. According to Proposition 2, we have

$$(v_1, v_2, \cdots, v_n, x_1, \cdots, x_v) \cdot \widetilde{M} = (V, V^q, \cdots, V^{q^{n-1}}, x_1, \cdots, x_v),$$

where $v_i, x_j \in \mathbb{F}_q, 1 \le i \le n, 1 \le j \le v$ and $V \in \mathbb{F}_{q^n}$.

Proposition 3. *Let* $p_i \in \mathbb{F}_q[x_1, x_2, \cdots, x_{n+v}]$ *be the public key polynomials of HFEv- and* P_i *be the matrix representing the quadratic form of* p_i*,* $0 \le i < n-a$*. Let the central map of HFEv- be*

$$F = (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v)F^{*0}(X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v)^t,$$

where $F^{*0} \in \mathcal{M}_{(n+v)\times(n+v)}(\mathbb{F}_{q^n})$*. Let* $S \in \mathcal{M}_{(n+v)\times(n+v)}(\mathbb{F}_q)$ *and* $T \in \mathcal{M}_{n\times(n-a)}(\mathbb{F}_q)$ *be the matrices representing the linear parts of* $\mathcal{S}$ *and* $\mathcal{T}$*. Then*

$$\begin{aligned} &\left(\widetilde{M}^{-1}S^{-1}P_0(S^{-1})^t(\widetilde{M}^{-1})^t, \cdots, \widetilde{M}^{-1}S^{-1}P_{n-a-1}(S^{-1})^t(\widetilde{M}^{-1})^t\right) \\ &= \left(F^{*0}, \cdots, F^{*n-1}\right) M^{-1}T \end{aligned} \tag{3}$$

Proof. Similar to Lemma 2 in [3].

Denote $U = \widetilde{M}^{-1}S^{-1} \in \mathcal{M}_{(n+v)\times(n+v)}(\mathbb{F}_{q^n})$ and $W = M^{-1}T \in \mathcal{M}_{n\times(n-a)}(\mathbb{F}_{q^n})$, then Equation (3) can be rewritten as

$$\left(UP_0U^t, \cdots, UP_{n-a-1}U^t\right) = \left(F^{*0}, \cdots, F^{*n-1}\right) W. \tag{4}$$

4 Our Key Recovery Attack on HFEv-

In this section we describe our key recovery attack on the HFEv- signature scheme. Our attack is very much motivated by the basic idea that the best attack on any cryptosystem should make full use of information available for attack. In this sense, our attack follows a current trend in the cryptanalysis of multivariate schemes, namely to utilize information provided by certain rows of the public matrices (see also [1, 2]).

Let q, n, v, D, a be the parameters of HFEv- and denote $d = \lceil \log_q(D) \rceil$. In this paper, we assume that $0 \leq a < n - 2d - 1$. Note that this condition is fulfilled for all practical parameter sets for HFEv-.[4]
Our attack consists of two steps. In the first step, we recover an equivalent linear transformation $\mathcal{S}$ by solving a MinRank problem over the base field $\mathbb{F}_q$. In the second step, we use this equivalent linear map to recover equivalent maps $\mathcal{F}$ and $\mathcal{T}$. By doing so, we obtain an equivalent HFEv- private key which allows us to generate signatures for arbitrary messages.

4.1 Recovering an Equivalent Linear Transformation $\mathcal{S}$

In this subsection, we will present our technique of finding an equivalent map S. We first show that the right hand side of (4) is a matrix of rank $\leq d$ and then show how to recover $\mathcal{S}$ by solving a MinRank problem.

Proposition 4. *Let $F^{*0}, \cdots, F^{*n-1}$ and $W = [w_{ij}]$ be the matrices of Equation (4) and $\mathbf{a}_i$ be the first row of matrix F^{*i} $(i = 0, 1, \ldots, n-1)$. Let Q be the matrix given as $Q = W^t \cdot \begin{pmatrix} \mathbf{a}_0 \\ \vdots \\ \mathbf{a}_{n-1} \end{pmatrix}$. Then the rank of Q is at most $d = \lceil \log_q(D) \rceil$.*

Proof. We have

$$Q = \begin{pmatrix} w_{11}\mathbf{a}_0 + w_{21}\mathbf{a}_1 + \cdots + w_{n1}\mathbf{a}_{n-1} \\ w_{12}\mathbf{a}_0 + w_{22}\mathbf{a}_1 + \cdots + w_{n2}\mathbf{a}_{n-1} \\ \cdots \\ w_{1,n-a}\mathbf{a}_0 + w_{2,n-a}\mathbf{a}_1 + \cdots + w_{n,n-a}\mathbf{a}_{n-1} \end{pmatrix} = W^t \cdot \begin{pmatrix} \mathbf{a}_0 \\ \mathbf{a}_1 \\ \cdots \\ \mathbf{a}_{n-1} \end{pmatrix}$$

Due to the construction of the matrices $F^{*i} (i = 0, 1, \ldots, n-1)$, we have

$$\begin{pmatrix} \mathbf{a}_0 \\ \mathbf{a}_1 \\ \cdots \\ \mathbf{a}_{n-1} \end{pmatrix} = \begin{pmatrix} A_1 \\ 0 \\ A_2 \end{pmatrix},$$

[4] Indeed, $a \geq n-2d+1$ implies that the number $n-a$ of equations in the public system is bounded from above by $2d+1$. Defending the scheme against brute force attacks would therefore require a high value of d which would make the scheme completely impractical.

where A_1 is an $1 \times (n+v)$ matrix and A_2 is a $(d-1) \times (n+v)$ matrix. That is, this matrix has only d non-zero rows, therefore its rank is at most d. Therefore the rank of Q is at most d. $\square$

Theorem 2. *Let $P_0, P_1, \ldots, P_{n-a-1}$ and U be the matrices of Equation (4), the vector $\mathbf{u} = (u_0, u_1, \cdots, u_{n+v-1})$ be the first row of U and $\mathbf{b}_i = (u_0, u_1, \ldots, u_{n+v-1})P_i$, $(i = 0, 1, \ldots, n-a)$. Define $Z \in \mathcal{M}_{(n-a)\times(n+v)}(\mathbb{F}_{q^n})$ as the matrix whose row vectors are the $\mathbf{b}_i$. Then the rank of Z is at most d.*

Proof. From Equation (4) and Proposition 4, we know that the rank of ZU^t is not more than d. Thus the rank of Z is at most d. $\square$

Proposition 5. *Let $A = [a_{ij}]$ be an $n \times m$ matrix over $\mathbb{F}_q$, $B = M^{-1}A = [b_{ij}] \in \mathcal{M}_{n\times m}(\mathbb{F}_{q^n})$. Then*

$$b_{ij} = b_{i-1,j}^q, \quad \text{for all } i, j, \text{ with } 0 \leq i < n, 0 \leq j < m.$$

That is, each row is obtained from the previous one using a Frobenius application. Therefore, the whole matrix B is completely defined by any of its rows.

Proof. Let $(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$ be a dual basis of $(\theta_1, \theta_2, \cdots, \theta_n)$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then we have

$$M^{-1} = \begin{pmatrix} \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_n \\ \varepsilon_1^q & \varepsilon_2^q & \cdots & \varepsilon_n^q \\ \vdots & \vdots & \ddots & \vdots \\ \varepsilon_1^{q^{n-1}} & \varepsilon_2^{q^{n-1}} & \cdots & \varepsilon_n^{q^{n-1}} \end{pmatrix}.$$

Thus $b_{ij} = \sum_{k=0}^{n-1} a_{kj}\varepsilon_{k+1}^{q^i}$ for all $i, j, 0 \leq i < n, 0 \leq j < m$. Since $a_{ij}^q = a_{ij}$ and the linearity of Frobenius, we have

$$b_{i-1,j}^q = \left(\sum_{k=0}^{n-1} a_{kj}\varepsilon_{k+1}^{q^{i-1}}\right)^q = \sum_{k=0}^{n-1} a_{kj}^q (\varepsilon_{k+1}^{q^{i-1}})^q = \sum_{k=0}^{n-1} a_{kj}\varepsilon_{k+1}^{q^i} = b_{ij}$$

for all $i, j, 0 < i \leq n, 0 \leq j < m$. $\square$

Proposition 5 implies that we only need to find one row of matrix $U = \widetilde{M}^{-1}S^{-1}$ to recover the first n rows of U. Let $u_0, u_1, \cdots, u_{n+v-1}$ be the first row of U. We assume that $u_0, u_1, \cdots, u_{n+v-1}$ are unknowns. Since we need to find only one of the equivalent HFEv- private keys, we can fix $u_0 = 1$ [22]. Since the rank of Z is at most d, we can find the u_i $(i = 1, \ldots, n+v-1)$ by soving a MinRank Problem over the base field. This can be done by using any of the methods presented in Section 3. Our method to recover $\mathcal{S}$ can be summarized as shown in Algorithm 1.

Algorithm 1 Recovering an Equivalent Linear Transformation S

Input: HFEv- parameters (q, n, v, D, a), matrices $(P_0, \cdots, P_{n-a-1})$ representing the quadratic forms of the public key polynomials, matrix $\widetilde{M}$ (see Equation (2)).

Output: Equivalent linear transformation S.

1. Set $\mathbf{b}_i = (1, u_1, \cdots, u_{n+v-1})P_i$, $0 \leq i < n-a$, where $(u_1, \cdots, u_{n+v-1})$ are unknowns.
2. Construct a matrix Z whose row vectors are $\mathbf{b}_i$, $0 \leq i < n-a$. According to Theorem 2, the rank of Z is at most d.
3. Solve the MinRank Problem with matrix Z using one of the methods described in Section 3. Denote the solution by $u_0, u_1, \cdots, u_{n+v-1}$.
4. Set $U = \begin{pmatrix} u_0 & u_1 & \cdots & u_{n+v-1} \\ u_0^q & u_1^q & \cdots & u_{n+v-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ u_0^{q^{n-1}} & u_1^{q^{n-1}} & \cdots & u_{n+v-1}^{q^{n-1}} \\ r_{00} & r_{01} & \cdots & r_{0,n+v-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{v-1,0} & r_{v-1,1} & \cdots & r_{v-1,n+v-1} \end{pmatrix}$, where $r_{ij}, 0 \leq i < v, 0 \leq j < n+v$ are randomly chosen from the finite field $\mathbb{F}_q$ such that U is invertible.
5. Compute $S' = (\widetilde{M}U)^{-1}$.
6. Return S'.

4.2 Recovering Equivalent Maps $\mathcal{F}$ and $\mathcal{T}$

In this subsection we show how, having found an equivalent linear transformation $\mathcal{S}$, we can recover equivalent maps $\mathcal{F}$ and $\mathcal{T}$ by solving several systems of (non)linear equations.

Proposition 6. *Let (q, n, v, D, a) be the parameters of HFEv-, P_i $(0 \leq i < n-a), M$, $U, W, F^{*j} (0 \leq j < n)$ be the matrices of Equation (4). We set $d = \lceil \log_2 D \rceil$. Assume that U is known, then F^{*0} can be recovered by solving a linear system with $n-a-1$ variables, $(d+a)\cdot(n+v)$ additional linear equations in at most $d+v$ variables, and $\binom{v+1}{2}$ univariate polynomial equations of degree q^d.*

Proof. From Equation (4) we know that $W = M^{-1}T \in \mathcal{M}_{n\times(n-a)}(\mathbb{F}_{q^n})$. Let $W = \begin{pmatrix} W_1 \\ W_2 \end{pmatrix}$, where $W_1 \in \mathcal{M}_{a\times(n-a)}(\mathbb{F}_{q^n})$ and $W_2 \in \mathcal{M}_{(n-a)\times(n-a)}(\mathbb{F}_{q^n})$. Since M is invertible and the entries of T are randomly chosen from $\mathbb{F}_q$, the probability of W_2 being singular is $1 - \prod_{i=1}^{n-a}(1 - \frac{1}{q^i})$. According to Theorem 1, there are at least q^n equivalent maps T, thus the probability that all matrices W_2 associated to the equivalent maps T are singular is approximately $(1 - \prod_{i=1}^{n-a}(1 - \frac{1}{q^i}))^{q^n}$. Therefore we find an invertible matrix W_2 with overwhelming probability. We

multiply both sides of Equation (4) by W_2^{-1}, obtaining

$$\left(UP_0U^t, \cdots, UP_{n-a-1}U^t\right) W_2^{-1} = \left(F^{*0}, \cdots, F^{*n-1}\right) \begin{pmatrix} W_1W_2^{-1} \\ I_{n-a} \end{pmatrix}, \quad (5)$$

where I_{n-a} is the $(n-a)\times(n-a)$ identity matrix. Let $(\widetilde{w}_0, \widetilde{w}_1, \ldots, \widetilde{w}_{n-a-1})$ be the first column of W_2^{-1} and $(\widetilde{l}_0, \widetilde{l}_1, \ldots, \widetilde{l}_{a-1}, 1, 0, \ldots, 0)$ be the first column of $\begin{pmatrix} W_1W_2^{-1} \\ I_{n-a} \end{pmatrix}$, then Equation (5) yields

$$\sum_{k=0}^{n-a-1} \widetilde{w}_k UP_kU^t = \sum_{i=0}^{a-1} \widetilde{l}_i F^{*k} + F^{*a}.$$

We multiply both sides by $\widetilde{l}_0^{-1}$, obtaining

$$\sum_{k=0}^{n-a-1} \widetilde{l}_0^{-1}\widetilde{w}_k UP_kU^t = F^{*0} + \sum_{i=1}^{a-1} \widetilde{l}_0^{-1}\widetilde{l}_i F^{*i} + \widetilde{l}_0^{-1}F^{*a}.$$

Denoting $w_k = \widetilde{l}_0^{-1}\widetilde{w}_k$, $(k = 0, 1, \cdots, n-a-1)$, and $l_i = \widetilde{l}_0^{-1}\widetilde{l}_i$, $(i = 1, 2, \cdots, a-1)$, $l_a = \widetilde{l}_0^{-1}$ yields

$$\sum_{k=0}^{n-a-1} w_k UP_kU^t = \sum_{i=1}^{a} l_i F^{*i} + F^{*0}. \quad (6)$$

Note that $\sum_{i=1}^{a} l_i F^{*i} + F^{*0} = \begin{pmatrix} F_0' & 0 & F_1' \\ 0 & 0 & 0 \\ F_1'^t & 0 & F_2' \end{pmatrix} \in \mathcal{M}_{(n+v)\times(n+v)}(\mathbb{F}_{q^n})$, where $F_0' = [f_{ij}']$ is a $(d+a)\times(d+a)$ diagonal band symmetric matrix of width $2d-1$, that is $f_{ij}' = 0$, if $|i-j| \geq d$, $F_1' \in \mathcal{M}_{(d+a)\times v}(\mathbb{F}_{q^n})$, $F_1'^t \in \mathcal{M}_{v\times(d+a)}(\mathbb{F}_{q^n})$ is the transpose of F_1' , $F_2' \in \mathcal{M}_{v\times v}(\mathbb{F}_{q^n})$ is a symmetric matrix .
Assume that $w_0, w_1, \ldots, w_{n-a-1}$ are unknowns. Since we need to find only one of the equivalent HFEv- private keys, we can fix $w_0 = 1$ [28]. Due to the fact that U is known and the special structure of the matrix $\sum_{i=1}^{a} l_i F^{*i} + F^{*0}$, we obtain from Equation (6) $d(n-a-d)$ linear equations in the $n-a-1$ variables $w_1, w_2, \cdots, w_{n-a-1}$. Since $0 < a < n-2d-1$, we have $d(n-a-d) \geq n-a-1$. Therefore, by solving these linear equations, we get a solution $(w_0', w_1', w_2', \cdots, w_{n-a-1}')$ with $w_0' = 1$. Thus Equation (6) can be rewritten as

$$\sum_{k=0}^{n-a-1} w_k' UP_kU^t = \sum_{i=1}^{a} l_i F^{*i} + F^{*0}. \quad (7)$$

Now we will find $l_1, \cdots, l_a$ and F^{*0} from Equation (7). We know that F^{*0} has the form

$$F^{*0} = \begin{pmatrix} F_0 & 0 & F_1 \\ 0 & 0 & 0 \\ F_1^t & 0 & F_2 \end{pmatrix},$$

where $F_0 = [\alpha_{ij}] \in \mathcal{M}_{d\times d}(\mathbb{F}_{q^n})$ is a symmetric matrix, $F_1 = [\gamma_{ij}] \in \mathcal{M}_{d\times v}(\mathbb{F}_{q^n})$, $F_1^t \in \mathcal{M}_{v\times d}(\mathbb{F}_{q^n})$ is the transpose of F_1 and $F_2 = [\delta_{ij}] \in \mathcal{M}_{v\times v}(\mathbb{F}_{q^n})$ is a symmetric matrix . According to Proposition 1 we can represent F^{*k} $(1 \le k \le n-1)$ by the entries of F^{*0}.

Assume that $l_1, \ldots, l_a$, α_{ij} $(0 \le i \le j < d)$, $\gamma_{ij}(0 \le i < d, 0 \le j < v)$, $\delta_{ij}(0 \le i \le j < v)$ are unknowns. Then we can recover F^{*0} as follows.

- From the first row of matrix equation (7), we can find a linear system in the variables α_{0j} $(0 \le j < d)$ and γ_{0j} $(0 \le j < v)$ of the form

  $$\alpha_{00}+\theta_{00} = 0, \cdots, \alpha_{0,d-1}+\theta_{0,d-1} = 0, \gamma_{00}+\theta_{0,d} = 0, \cdots, \gamma_{0,v-1}+\theta_{0,d+v-1} = 0.$$

  Thus we can obtain the first row of F^{*0} by solving this linear system.
- Once the first row of F^{*0} is known, we can obtain from the second row of matrix equation (7) a linear system in the variables l_1 and $\alpha_{1j}(1 \le j < d)$ and $\gamma_{1j}(0 \le j < v)$. By solving this linear system we can obtain the second row of F^{*0} and l_1.
- Similarly, if $a \le d$, we can obtain $l_1, \cdots, l_a$, F_0 and F_1 using the first d rows of matrix equation (7). If $a > d$, we can obtain $l_1, \cdots, l_d$, F_0 and F_1 by using the first d rows of matrix equation (7) and $l_{d+k}(1 \le k \le a-d)$ by using the $(d+k)$-th row of matrix equation (7). Thus we obtain $l_1, \cdots, l_a$, F_0 and F_1.
- Once $l_1, \cdots, l_a$, F_0 and F_1 are known, we get from the last v rows of matrix equation (7), $\binom{v+1}{2}$ univariate polynomial equations of the form

  $$\sum_{k=0}^{d} \lambda_{ijk} \delta_{ij}^{q^k} + \eta_{ij} = 0,$$

  where $\lambda_{ijk}, \eta_{ij} \in \mathbb{F}_{q^n}, 0 \le i \le j < v$. Solving these equations we obtain δ_{ij} and then recover F^{*0}.
- Once F^{*0} is known, we can obtain an equivalent central map as

  $$\begin{aligned} &F'(X, x_1, \ldots, x_v) \\ &= (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v) F^{*0} (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v)^t. \end{aligned}$$

□

Proposition 7. *Let (q, n, v, D, a) be the parameters of HFEv-, P_i $(0 \le i < n-a), S, T, M$, F^{*j} $(0 \le j < n)$ be the matrices of Equation (3). Assume that $S, P_i(0 \le i < n-a), M, F^{*j}(0 \le j < n)$ are known, then T can be recovered by solving $n-a$ linear systems in n variables.*

Proof. Equation (3) can be rewritten as

$$(P_0, \cdots, P_{n-a}) = \left(SMF^{*0}M^tS^t, \cdots, SMF^{*n-1}M^tS^t\right) M^{-1}T. \tag{8}$$

Let $(t_{1k}, t_{2k}, \cdots, t_{nk})$ be the entries of the k-th $(k = 1, 2, \cdots, n-a)$ column of T. Since S, P_i $(0 \le i < n-a), M, F^{*j}(0 \le j < n)$ are known, we obtain

from Equation (8) a linear system with $\frac{n(n+1)}{2}$ equations in the n variables $(t_{1k}, t_{2k}, \cdots, t_{nk})$ for all $(k = 1, 2, \cdots, n-a)$. We can recover T by solving $(n-a)$ of these linear systems. $\square$

The process of recovering the maps $\mathcal{F}$ and $\mathcal{T}$ of our equivalent HFEv- key is summarized in Algorithm 2 .

Algorithm 2 Recovering Equivalent Maps $\mathcal{F}$ and $\mathcal{T}$

Input: HFEv- parameters (q, n, v, D, a), Frobenius matrix M (see (1)), matrices $(P_0, \cdots, P_{n-a-1})$ representing the quadratic forms of the public key polynomials, recovered linear map S.

Output: Equivalent private maps F and T.

1. Let $w_0, w_1, \cdots, w_{n-a-1}$ be unknowns and $w_0 = 1$. Get a linear system with $d(n-d-a)$ equations in the $n-a-1$ variables $w_i, (1 \leq i < n-a-1)$ from matrix equation (6). as shown in the proof of Proposition 6. By solving this linear system we obtain a solution $w'_0, w'_1, \cdots, w'_{n-a-1}$ with $w'_0 = 1$.
2. Let $l_1, \cdots, l_a$ and the nonzero entries of F^{*0} be unknowns in matrix equation (7). We get $(d+a) \cdot (n+v)$ bilinear equations from the first $d+a$ rows of matrix equation (7) and $\binom{v+1}{2}$ univariate polynomial equations from the last v rows of matrix equation (7). By solving these linear systems and univariate polynomial equations we recover F^{*0} (see Proposition 6). Then we can obtain an equivalent central map as

$$F' = (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v) F^{*0} (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v)^t.$$

3. Compute F^{*k} $1 \leq k < n$ according to Proposition 1.
4. Let $(t_{1k}, t_{2k}, \cdots, t_{nk})$ be the (unknown) entries of the k-th $(k = 1, 2, \cdots, n-r)$ column of T. Get $n-r$ linear systems from matrix equation (8) as shown in Proposition 7. By solving these linear systems we can recover an equivalent map T.
5. Return F', T.

4.3 Complexity of the Attack

The most complex step of our attack is step 3 of Algorithm 1. That is the step of solving the MinRank problem on the matrix Z, which has rank at most d. For this step, we can use the methods discussed in Section 3.2, in particular the minors modeling or the support minors modeling.

If we solve the MinRank problem using minors modeling, the degree of regularity of solving the public system using the F4 algorithm is given as $d+1$ (c.f. [3]).

Therefore, the complexity of our attack using minors modeling is

$$\mathcal{O}\left(\binom{n+v+d+1}{d+1}^{\omega}\right),$$

where $2 < \omega \leq 3$ is the linear algebra constant.

4.4 Discussion

The complexity of our attack is independent of the number a of Minus Equations and polynomial both in the parameter n and the number v of Vinegar variables. So, for a fixed parameter D, we obtain a polynomial time attack on all HFE signature variants. Therefore, the only way of enhancing the security of the HFEv- scheme is by increasing the parameter d (i.e. the degree D of the HFE polynomial). However, during the signature generation process, we have to invert the HFE polynomial using for example Berlekamps algorithm. Since the complexity of this algorithm grows with D^{ω} or $2^{d\omega}$, this slows down the scheme drastically. Our attack therefore raises the question if it is possible at all to construct a secure and efficient signature scheme on the basis of the HFE cryptosystem. An alternative might be to use polynomials of degree > 2 (see for example [24]).

5 Possible Speed Up using Support Minus Modeling

In [1] Bardet et al. proposed a new modeling for the MinRank attack called support minors modeling. The main idea of this modeling is to write the low rank matrix M as a product $M = AC$, where A is an $m \times r$ matrix and C is an $r \times n$ matrix. For $i = 1, 2, \ldots, m$ we define matrices of the form $\widetilde{C_i} = \begin{pmatrix} \mathbf{r}_i \\ C \end{pmatrix}$, where $\mathbf{r}_i$ is the i-th row of M. Since $\mathbf{r}_i$ lies in the space spanned by the rows of C, the rank of the matrix $\widetilde{C_i}$ $(i = 1, 2, \ldots, m)$ is at most r. This implies that all $(r+1)\times(r+1)$ minors of the matrices $\widetilde{C_i}$ $(i = 1, 2, \ldots, m)$ are 0. We view the $r \times r$ minors of the matrix C as new variables which are called kernel variables and are denoted as $y_1, y_2, \ldots, y_{n_y}$, where $n_y = \binom{n}{r}$. The $(r+1)\times(r+1)$ minors of the matrices $\widetilde{C}_i$ are therefore given as bilinear equations in the variables $x_1, \ldots, x_{n_x}$ and $y_1, \ldots, y_{n_y}$. Altogether, we obtain $m\binom{n}{r+1}$ of these bilinear equations. The total number of monomials of degree 2 in these bilinear equations is at most $n_x\binom{n}{r}$. If

$$m\binom{n}{r+1} \geq n_x\binom{n}{r} - 1,$$

holds, we can solve this system of bilinear equations using relinearization.

In practical applications, we can assume that C has the form (I_r, C_0), where I_r is an $r \times r$ identity matrix and C_0 is an $r \times (n-r)$ matrix. Moreover, instead

of using all $r \times r$ minors of the matrix C as variables, we choose a positive integer $n' \leq n$ such that

$$m\binom{n'}{r+1} \geq n_x\binom{n'}{r} - 1 \tag{9}$$

holds and restrict the computation of minors to the first n' rows of the matrices $\tilde{C}_i$.

If the MinRank problem has only one solution, the resulting linear system is sparse, and we can solve it using the Wiedemann algorithm. The complexity of solving this linear system is

$$\mathcal{O}\left(\left(n_x\binom{n'}{r}\right)^2 \cdot n_x(r+1)\right)$$

field operations. If the MinRank problem has no unique solution and $\mathbb{F}_q$ is a small finite field, we can guess the values of some variables such that the resulting linear system has a unique solution, and then solve it using the Wiedemann algorithm. Otherwise, we solve the bilinear system using a Gröbner basis algorithm such as F_4 or F_5 [17].

When applying the support minors modeling to our attack, we obtain an overdetermined bilinear system of $n_x + n_y$ variables and $\frac{(n_x+n_y)(n_x+n_y+1)}{2}$ equations, where $n_x = n + v$ and $n_y = \binom{n'}{d}$, $n' = \lceil \frac{(n-a)(d+1)}{n+v} \rceil + d + 1$, $n' < 2d + 2$. This bilinear system has at least n solutions. In fact, if $(u_0, u_1, \ldots, u_{n+v-1})$ is a solution of this bilinear system, $(u_0^{q^{i-1}}, u_1^{q^{i-1}}, \ldots, u_{n+v-1}^{q^{i-1}})$ for all $1 \leq i \leq n$ are also solutions of the bilinear system (see [22] for more details). Therefore, we don't longer have a unique solution as in the case of e.g. Rainbow, which makes the use of the Wiedemann algorithm inefficient. Thus we use a Gröbner basis technique such as the F_4 or F_5 algorithm to solve the system instead of using the relinearization method and Wiedemann.

To estimate the complexity of our attack using the support minors modeling, we carried out a large number of experiments using the F_4 algorithm included in MAGMA. For these experiments, we created HFEv- public keys over base fields of size $q \in \{2, 3, 5, 7\}$ using the HFEv- parameters $n \in \{20, 30, 40\}$, $a \in \{0, 2, 4\}$, $v \in \{0, 2, 4, 6\}$ and $d \in \{4, 5, 6\}$. We applied our attack on these instances solving the MinRank problem for the matrix Z with target rank d using the support minors modeling. The resulting bilinear system was solved using the F_4 algorithm included in MAGMA. We found that, independently of the HFEv- parameters used in the experiments, the first degree fall occurs at degree 3. Therefore we come up with the following

Conjecture: Independently of the HFEv- parameters, the bilinear systems obtained by our attack and the support minors modeling, can be solved at degree 3.

However, so far, we do not have theoretical arguments for the correctness of our conjecture and therefore leave a proof of the conjecture as future work.

Since the total number of monomials in the bilinear system generated by the support minors modeling is $n_x n_y + n_x + n_y + 1$, the total number of monomials of degree at most 3 is given as $\mathcal{O}(n_x^2 n_y + n_x n_y^2)$. Thus, assuming the correctness of our conjecture, the complexity of our attack on HFEv- using support minors modeling is $\mathcal{O}\left(n_x^2 n_y + n_x n_y^2\right)^\omega$ or $\mathcal{O}\left((n+v)^2\binom{2d+2}{d} + (n+v)\binom{2d+2}{d}^2\right)^\omega$. Here, $2 < \omega \leq 3$ is again the linear algebra constant. However we note again that this formula only holds assuming the correctness of our conjecture about the first fall degree.

6 Application to GeMSS

GeMSS is an HFEv- type signature scheme which is one of the alternative candidates in the third round of the NIST Post Quantum Crypto Standardization Project [8]. The attack complexity on GeMSS using our key recovery attack method can be estimated as shown in Table 1. The table shows:

Table 1. Complexity of our Attack on GeMMS (# of gates)

NIST security category		parameters (q, n, v, D, a)	required security level	our attack using minors modeling	our attack using support minors modeling
I	GeMSS128	(2,174,12,513,12)	143	139	118
	BlueGeMSS128	(2,175,14,129,13)		119	99
	RedGeMSS128	(2,177,15,17,15)		86	72
II	GeMSS192	(2,265,20,513,22)	207	154	120
	BlueGeMSS192	(2,265,23,129,22)		132	101
	RedGeMSS192	(2,266,25,17,23)		95	75
III	GeMSS256	(2,354,33,513,30)	272	166	121
	BlueGeMSS256	(2,358,32,129,34)		141	103
	RedGeMSS256	(2,358,35,17,34)		101	76

1. Especially for the higher security categories (NIST category II and III), the proposed parameters for GeMMS don't reach the required security levels.
2. Speeding up the signature generation process of GeMSS by decreasing D while increasing a and v is, with regard to the security of the scheme, not possible. This forbids the GeMSS variants BlueGeMMS and RedGeMMS.
3. In order to meet NIST security level III (272 gates), we would need an HFE parameter d of at least 20, which corresponds to a degree D of the HFE polynomial of at least $2^{19} + 1 = 524.289$. This would lead to a slow down of the signature generation process by a factor of $1.4 \cdot 10^7$. Therefore, the techniques used in GeMMS don't suffice to reach high levels of security while keeping the scheme efficient.

7 Conclusion

In this paper we proposed a new key recovery attack on the HFEv- signature scheme. While most of the cryptanalysts tried to attack the HFEv- scheme by solving a MinRank attack over the extension field $\mathbb{F}_{q^n}$, our attack works completely over the base field. The complexity of the attack is exponential in the parameter $d = \lceil \log_q(D) \rceil$, but polynomial in n. Therefore, the complexity of our attack behaves assymptotically exactly as the complexity of the signing process of HFEv-. Our attack shows that the Minus modifications does not enhance the security of the HFEv- scheme, while the Vinegar modification only adds a polynomial factor. Therefore, in order to meet the NIST security requirements, a very large value of D is needed. However, this makes the signature generation process of HFEv- very inefficient. We therefore conclude that the currently existing techniques are not sufficient to transform the HFE scheme into a secure and efficient signature scheme.

Acknowledgements

Parts of the work were done while the third author was at Cincinnati. We thank CCB Fintech Co. Ltd for partially sponsoring the work of the first and the last author with No. KT2000040. Furthermore we thank NFS for partially sponsoring this work and the anonymous reviewers of CRYPTO 2021 for their valuable comments which helped to improve the paper.

References

1. M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.P. Tillich, J. Verbel: Improvements of algebraic attacks for solving the rank decoding and MinRank problems. International Conference on the Theory and Application of Cryptology and Information Security, 2020.
2. W. Beullens: Improved Attacks on UOV and Rainbow. IACR eprint 2020/1343.
3. L. Bettale, J.C. Faugere, L. Perret: Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. Designs, Codes and Cryptography, 69(1), pp. 1-52 (2013).
4. D. Bernstein, J. Buchmann, E. Dahmen (eds.): Post Quantum Cryptography. Springer 2009.
5. J. F. Buss, G. S. Frandsen, J. O. Shallit: The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences, 58(3), pp. 572-596 (1999).
6. M. Campagna, K. Chen, Ö. Dagdelen, J. Ding, J.K. Ferrick, N. Gisin et al.: Quantum safe cryptography and security. ETSI White paper 8. Available at https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf (June 2015)
7. R. Cartor, R. Gipson, D. Smith-Tone, J. Vates: On the differential security of the HFEv-signature primitive. PQCrypto 2016, LNCS vol. 9606, pp. 162-181.

8. A. Casanova, J. C. Faugere, G. Macario Rat, J. Patarin, L. Perret, J. Ryckegem: GeMSS: a great multivariate short signature (2019). Submission to NIST PQC competition Round-3.
9. N. Courtois, M. Daum, P. Felke: On the security of HFE, HFEv-and Quartz. PQCrypto 2003, LNCS vol. 2567, pp. 337 - 350.
10. J. Ding, C. Clough, R. Araujo: Inverting square systems algebraically is exponential. Finite Fields and Their Applications 26, pp. 32-46.
11. J. Ding, T.J. Hodges: Inverting HFE systems is quasipolynomial for all fields. CRYPTO 2011, LNCS vol. 6841, pp. 724 - 742.
12. J. Ding, T. Kleinjung: Degree of regularity for HFE Minus (HFE-). Journal of Math for Industry 4, pp. 97 - 104.
13. J. Ding, R. Perlner, A. Petzoldt, D. Smith-Tone: Improved cryptanalysis of hfev-via projection. PQCrypto 2018, LNCS vol. 10786, pp. 375-395.
14. J. Ding, A. Petzoldt: Current state of multivariate cryptography. IEEE Security and Privacy 15 (4), pp. 28-36.
15. J. Ding, A. Petzoldt, D. Schmidt: Multivariate Public Key Cryptosystems - Second Edition. ISBN 978-1-0716-0985-9. Springer, 2020.
16. J. Ding, B.Y. Yang: Degree of regularity for HFEv and HFEv-. PQCrypto 2013, LNCS vol. 7932, pp 52 - 66.
17. J.C. Faugère: A new efficient algorithm for computing Gröbner bases (F4): Journal of pure and applied algebra, 139(1-3), pp. 61-88 (1999).
18. J.C. Faugère, M.S. El Din, P.J. Spaenlehauer: Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. Proceedings of the International Symposium on Symbolic and Algebraic Computation, pp. 257-264 (2010).
19. P. Gaborit, O. Ruatta, J. Schrek: On the complexity of the rank syndrome decoding problem. IEEE Transactions on Information Theory, 62(2), pp. 1006-1019, 2016.
20. M. R. Garey and D. S. Johnson. Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company 1979.
21. L. Goubin, N. Courtois: Cryptanalysis of the TTM Cryptosystem. ASIACRYPT 2000, LNCS vol. 1976, pp. 44-57.
22. X. Jiang, J. Ding, L. Hu: Kipnis-Shamir attack on HFE revisited. Inscrypt 2007, LNCS vol. 4990, pp. 399-411.
23. A. Kipnis, A. Shamir A. Cryptanalysis of the HFE public key cryptosystem by relinearization. CRYPTO 99, LNCS vol. 1666, pp. 19-30.
24. G. Macario-Rat, J. Patarin: Ariadne Thread and Salt: New Multivariate Cryptographic Schemes with Public Keys in Degree 3. Available at https://eprint.iacr.org/2021/084.pdf
25. J. Patarin: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. EUROCRYPT 1996, LNCS vol. 1070, pp. 33-48.
26. J. Patarin, N. Courtois, L. Goubin: Quartz, 128-bit long digital signatures. Cryptographers Track at the RSA Conference, LNCS vol. 2020, pp. 282-297.
27. A. Petzoldt, M.S. Chen, B.Y. Yang, C. Tao, J. Ding: Design principles for HFEv-based multivariate signature schemes. ASIACRYPT 2015(1), LNCS vol. 9452, pp. 311-334.
28. C. Wolf, B. Preneel: Equivalent keys in multivariate quadratic public key systems. Journal of Mathematical Cryptology 4(4), pp. 375-415 (2011).

A Example of the Attack

To illustrate our new attack method, we present a complete key recovery for a toy example of the HFEv- scheme over a small field. Let the parameters of our HFEv- instance be $(q, n, v, D, a) = (7, 7, 2, 14, 2)$. Then we have $d = \lceil \log_q(D) \rceil = 2$. We construct the degree n extension field $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/\langle x^7 + 6x + 4 \rangle$. Let θ be a primitive root of the irreducible polynomial $p(x) = x^7 + 6x + 4$.

We randomly generate central map $F = \theta^{176932}X^{14} + \theta^{461287}X^8 + \theta^{199902}X^2 + (\theta^{270502}x_1 + \theta^{358630}x_2)X + (\theta^{65557}x_1 + \theta^{2597}x_2)X^7 + \theta^{811326}x_1^2 + \theta^{14415}x_1x_2 + \theta^{151050}x_2^2$. The linear transformations $\mathcal{S}$ and $\mathcal{T}$ are given by the matrices

$$S = \begin{pmatrix} 3&1&1&6&4&2&0&1&6 \\ 6&2&4&5&3&3&2&6&0 \\ 6&1&3&4&4&2&4&5&3 \\ 0&1&4&6&4&2&2&3&1 \\ 2&0&0&5&2&4&2&1&3 \\ 0&5&1&2&4&2&1&4&3 \\ 3&3&5&0&2&6&4&6&6 \\ 5&2&0&2&5&6&3&1&2 \\ 6&2&5&5&5&4&3&6&1 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1&4&4&6&5 \\ 0&6&5&3&2 \\ 0&2&0&2&2 \\ 1&3&1&0&1 \\ 2&4&2&5&3 \\ 3&4&1&0&6 \\ 6&5&6&5&0 \end{pmatrix}.$$

We compute the public key as $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$. The quadratic forms representing the public key polynomials are given as

$$P_0 = \begin{pmatrix} 1&2&0&3&3&6&1&3&3 \\ 2&6&0&4&4&3&4&4&3 \\ 0&0&3&5&4&4&4&5&3 \\ 3&4&5&2&1&1&3&2&1 \\ 3&4&4&1&0&2&1&6&2 \\ 6&3&4&1&2&5&0&5&1 \\ 1&4&4&3&1&0&6&0&0 \\ 3&4&5&2&6&5&0&3&2 \\ 3&3&3&1&2&1&0&2&1 \end{pmatrix}, P_1 = \begin{pmatrix} 4&0&3&3&5&6&6&3&2 \\ 0&3&0&6&1&1&0&4&4 \\ 3&0&3&3&5&4&5&5&4 \\ 3&6&3&1&6&6&2&3&5 \\ 5&1&5&6&1&6&3&6&4 \\ 6&1&4&6&6&5&3&3&1 \\ 6&0&5&2&3&3&0&0&5 \\ 3&4&5&3&6&3&0&2&1 \\ 2&4&4&5&4&1&5&1&6 \end{pmatrix}, P_2 = \begin{pmatrix} 3&2&6&4&5&2&6&6&2 \\ 2&5&1&0&6&4&1&5&4 \\ 6&1&6&0&0&5&0&3&3 \\ 4&0&0&5&5&5&5&2&2 \\ 5&6&0&5&1&2&1&6&0 \\ 2&4&5&5&2&4&1&5&0 \\ 6&1&0&5&1&1&4&4&5 \\ 6&5&3&2&6&5&4&4&4 \\ 2&4&3&2&0&0&5&4&0 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 2&6&4&5&4&1&6&0&1 \\ 6&6&6&1&2&1&0&6&3 \\ 4&6&2&6&1&5&0&4&6 \\ 5&1&6&0&0&0&0&3&5 \\ 4&2&1&0&6&1&6&0&4 \\ 1&1&5&0&1&2&6&3&5 \\ 6&0&0&0&6&6&5&6&1 \\ 0&6&4&3&0&3&6&2&0 \\ 1&3&6&5&4&5&1&0&1 \end{pmatrix} P_4 = \begin{pmatrix} 3&0&5&4&5&6&0&5&2 \\ 0&3&0&3&3&5&4&2&2 \\ 5&0&4&2&4&6&1&1&3 \\ 4&3&2&3&4&3&2&6&1 \\ 5&3&4&4&1&2&3&3&6 \\ 6&5&6&3&2&4&0&0&2 \\ 0&4&1&2&3&0&6&5&1 \\ 5&2&1&6&3&0&5&5&0 \\ 2&2&3&1&6&2&1&0&3 \end{pmatrix},$$

Let $M = \begin{pmatrix} 1&1&1&1&1&1&1 \\ \theta&\theta^7&\theta^{49}&\theta^{343}&\theta^{2401}&\theta^{16807}&\theta^{117649} \\ \theta^2&\theta^{14}&\theta^{98}&\theta^{686}&\theta^{4802}&\theta^{33614}&\theta^{235298} \\ \theta^3&\theta^{21}&\theta^{147}&\theta^{1029}&\theta^{7203}&\theta^{50421}&\theta^{352947} \\ \theta^4&\theta^{28}&\theta^{196}&\theta^{1372}&\theta^{9604}&\theta^{67228}&\theta^{470596} \\ \theta^5&\theta^{35}&\theta^{245}&\theta^{1715}&\theta^{12005}&\theta^{84035}&\theta^{588245} \\ \theta^6&\theta^{42}&\theta^{294}&\theta^{2058}&\theta^{14406}&\theta^{100842}&\theta^{705894} \end{pmatrix}$ and $\widetilde{M} = \begin{pmatrix} M&0 \\ 0&I_v \end{pmatrix}$ In the following we demonstrate our method to recover the private key from $\mathcal{P}$.

A.1 Recovering $\mathcal{S}$

Let the first row of matrix $U = \widetilde{M}^{-1}S^{-1}$ be $(u_0, u_1, \cdots, u_{n+v-1})$. Fix $u_0 = 1$ and let $u_1, \cdots, u_{n+v-1}$ be unknowns. Set $\mathbf{b}_i = (1, u_1, \cdots, u_{n+v-1})P_i, i = 0, 1, \cdots, n-a-1$. Let $\mathbf{b}_i$ be the i-th row of the matrix Z. Then the rank of Z is 2. This implies that all minors of order 3 are 0. Solving the MinRank Problem for

matrix Z gives us a solution $\mathbf{u} = (1, \theta^{2689}, \theta^{240750}, \theta^{393451}, \theta^{682468}, \theta^{184068}, \theta^{218176}, \theta^{85224}, \theta^{760002})$. Then we have

$$U = \begin{pmatrix} 1 & \theta^{2689} & \theta^{240750} & \theta^{393451} & \theta^{682468} & \theta^{184068} & \theta^{218176} & \theta^{85224} & \theta^{760002} \\ 1 & \theta^{18823} & \theta^{38166} & \theta^{283531} & \theta^{659566} & \theta^{464934} & \theta^{703690} & \theta^{596568} & \theta^{378762} \\ 1 & \theta^{131761} & \theta^{267162} & \theta^{337633} & \theta^{499252} & \theta^{783912} & \theta^{808120} & \theta^{58266} & \theta^{180708} \\ 1 & \theta^{98785} & \theta^{223050} & \theta^{716347} & \theta^{200596} & \theta^{546132} & \theta^{715588} & \theta^{407862} & \theta^{441414} \\ 1 & \theta^{691495} & \theta^{737808} & \theta^{73177} & \theta^{580630} & \theta^{528756} & \theta^{67864} & \theta^{384408} & \theta^{619272} \\ 1 & \theta^{722755} & \theta^{223404} & \theta^{512239} & \theta^{770242} & \theta^{407124} & \theta^{475048} & \theta^{220230} & \theta^{217194} \\ 1 & \theta^{118033} & \theta^{740286} & \theta^{291505} & \theta^{450442} & \theta^{379242} & \theta^{31168} & \theta^{718068} & \theta^{696816} \\ 1 & 5 & 1 & 0 & 1 & 3 & 0 & 3 & 2 \\ 4 & 6 & 1 & 5 & 4 & 5 & 5 & 6 & 6 \end{pmatrix},$$

where the last v rows of U are randomly chosen from $\mathbb{F}_q$, such that U is invertible.

Thus we can recover an equivalent linear transformation $\mathcal{S}$ as

$$S' = U^{-1}\widetilde{M}^{-1} = \begin{pmatrix} 0 & 1 & 1 & 2 & 3 & 6 & 6 & 0 & 6 \\ 1 & 4 & 5 & 3 & 1 & 6 & 0 & 4 & 6 \\ 4 & 5 & 3 & 1 & 5 & 6 & 0 & 6 & 4 \\ 5 & 0 & 1 & 2 & 5 & 6 & 0 & 2 & 0 \\ 2 & 3 & 1 & 3 & 5 & 6 & 0 & 3 & 1 \\ 1 & 6 & 5 & 0 & 4 & 1 & 0 & 4 & 1 \\ 0 & 4 & 6 & 4 & 2 & 2 & 0 & 6 & 2 \\ 2 & 1 & 5 & 2 & 5 & 1 & 2 & 1 & 2 \\ 6 & 0 & 2 & 6 & 4 & 6 & 1 & 5 & 6 \end{pmatrix}.$$

Recovering $\mathcal{F}$ and $\mathcal{T}$ Step 1. Once $\mathcal{S}$ is known, let $w_0, w_1, \cdots, w_{n-a-1}$ be unknowns and $w_0 = 1$. We generate a linear system with $d(n-d-a)$ equations in the $n-a-1$ variables $w_i, (1 \le i < n-a-1)$ using the matrix equation (6). By solving this linear system we obtain a solution $(1, \theta^{558954}, \theta^{326166}, \theta^{142979}, \theta^{806014})$.

Step 2. Let $l_1, \cdots, l_a$ and the nonzero entries of F^{*0} be variables in matrix equation (7). By using the first $d+a$ rows of matrix equation (7) we get $(d+a)\cdot(n+v)$ bilinear equations as follows:

$$\begin{pmatrix} \alpha_{00}+\theta^{599798} & \alpha_{01}+\theta^{499519} & 0 & 0 & 0\ 0\ 0 & \gamma_{00}+\theta^{424284} & \gamma_{01}+\theta^{665059} \\ \alpha_{10}+\theta^{499519} & \alpha_{00}^7 l_1+\alpha_{11}+\theta^{381840} & \alpha_{01}^7 l_1+\theta^{349085} & 0 & 0\ 0\ 0 & \gamma_{00}^7 l_1+\gamma_{10}+\theta^{228693} & \gamma_{01}^7 l_1+\gamma_{11}+\theta^{396254} \\ 0 & \alpha_{10}^7 l_1+\theta^{349085} & \alpha_{00}^{49} l_2+\alpha_{11}^7 l_1+\theta^{622586} & \alpha_{01}^{49} l_2+\theta^{524551} & 0\ 0\ 0 & \gamma_{00}^{49} l_2+\gamma_{10}^7 l_1+\theta^{475138} & \gamma_{01}^{49} l_2+\gamma_{11}^7 l_1+\theta^{2659} \\ 0 & 0 & \alpha_{10}^{49} l_2+\theta^{524551} & \alpha_{11}^{49} l_2+\theta^{32832} & 0\ 0\ 0 & \gamma_{10}^{49} l_2+\theta^{9738} & \gamma_{11}^{49} l_2+\theta^{392135} \end{pmatrix}$$

$= 0_{(d+a)\times(n+v)}$.

From the first row, we obtain $\alpha_{00} = \theta^{188027}, \alpha_{01} = \theta^{87748}, \gamma_{00} = \theta^{12513}, \gamma_{01} = \theta^{253288}$. Once α_{00}, α_{01} are known, we get from the second row $\alpha_{10} = \theta^{87748}, \alpha_{11} = \theta^{10485}, \gamma_{10} = \theta^{581451}, \gamma_{11} = \theta^{606062}, l_1 = \theta^{146620}$. From the third row we can obtain $l_2 = \theta^{754380}$.

Once l_1, l_2 are known, we get from the last v rows of matrix equation (7), $\binom{v+1}{2}$ univariate polynomial equations as follows:

$$\begin{aligned} \theta^{754380}\delta_{00}^{49} + \theta^{146620}\delta_{00}^{7} + \delta_{00} + \theta^{81317} &= 0, \\ \theta^{754380}\delta_{01}^{49} + \theta^{146620}\delta_{01}^{7} + \delta_{01} + \theta^{689914} &= 0, \\ \theta^{754380}\delta_{11}^{49} + \theta^{146620}\delta_{11}^{7} + \delta_{11} + \theta^{162754} &= 0. \end{aligned}$$

Each of these equations has 49 solutions. We choose one of them as the value of δ_{ij}. Thus we have $\delta_{00} = \theta^{27191}, \delta_{01} = \delta_{10} = \theta^{19044}, \delta_{11} = \theta^{9718}$ and

$$F^{*0} = \begin{pmatrix} \theta^{188027} & \theta^{87748} & 0\ 0\ 0\ 0\ 0 & \theta^{12513} & \theta^{253288} \\ \theta^{87748} & \theta^{10485} & 0\ 0\ 0\ 0\ 0 & \theta^{581451} & \theta^{606062} \\ 0 & 0 & 0\ 0\ 0\ 0\ 0 & 0 & 0 \\ 0 & 0 & 0\ 0\ 0\ 0\ 0 & 0 & 0 \\ 0 & 0 & 0\ 0\ 0\ 0\ 0 & 0 & 0 \\ 0 & 0 & 0\ 0\ 0\ 0\ 0 & 0 & 0 \\ 0 & 0 & 0\ 0\ 0\ 0\ 0 & 0 & 0 \\ \theta^{12513} & \theta^{581451} & 0\ 0\ 0\ 0\ 0 & \theta^{27191} & \theta^{19044} \\ \theta^{253288} & \theta^{606062} & 0\ 0\ 0\ 0\ 0 & \theta^{19044} & \theta^{9718} \end{pmatrix}$$

Therefore we get an equivalent central map as $F' = \theta^{10485}X^{14} + \theta^{362262}X^8 + \theta^{188027}X^2 + (\theta^{287027}x_1 + \theta^{527802}x_2)X + (\theta^{32423}x_1 + \theta^{57034}x_2)X^7 + \theta^{27191}x_1^2 + \theta^{293558}x_1x_2 + \theta^{9718}x_2^2$ for F.

Let $(t_{1k}, t_{2k}, \cdots, t_{nk})$ be entries of the k-th $(k = 1, 2, \cdots, n-a)$ column of T. Get $n-a$ linear systems from matrix equation (8) as shown by Proposition 7. By solving these linear systems we can recover a equivalent key of T as follows

$$T' = \begin{pmatrix} 1 & 1 & 6 & 0 & 5 \\ 3 & 3 & 2 & 0 & 2 \\ 1 & 3 & 2 & 5 & 6 \\ 6 & 6 & 6 & 0 & 2 \\ 2 & 2 & 3 & 3 & 6 \\ 2 & 2 & 1 & 0 & 5 \\ 0 & 5 & 1 & 3 & 0 \end{pmatrix}.$$

It is easy to check that $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} = \mathcal{T}' \circ \mathcal{F}' \circ \mathcal{S}'$. Therefore the adversary can use the three maps $\mathcal{T}'$, $\mathcal{F}'$ and $\mathcal{S}'$ to forge signatures for arbitrary messages.