Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants

Luk Bettale*, Jean-Charles Faugère, and Ludovic Perret

INRIA, Paris-Rocquencourt Center, SALSA Project
UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France
CNRS, UMR 7606, LIP6, F-75005, Paris, France
luk.bettale@lip6.fr, jean-charles.faugere@inria.fr,
ludovic.perret@lip6.fr

Abstract. We investigate the security of a generalization of HFE (multivariate and odd-characteristic variants). First, we propose an improved version of the basic Kipnis-Shamir key recovery attack against HFE. Second, we generalize the Kipnis-Shamir attack to Multi-HFE. The attack reduces to solve a MinRank problem directly on the public key. This leads to an improvement of a factor corresponding to the square of the degree of the extension field. We used recent results on MinRank to show that our attack is polynomial in the degree of the extension field. It appears that multi-HFE is less secure than original HFE for equal-sized keys. Finally, adaptations of our attack overcome several variants (i.e. minus modifier and embedding). As a proof of concept, we have practically broken the most conservative parameters given by Chen, Chen, Ding, Werner and Yang in 9 days for 256 bits security. All in all, our results give a more precise picture on the (in)security of several variants of HFE proposed these last years.

Keywords: Hidden Field Equations, MinRank, Gröbner bases

1 Introduction

Multivariate Public-Key Cryptography (MPKC) is the set of public-key schemes using multivariate polynomials. The concept of MPKC is very appealing since its security is related to the hardness of a post-quantum problem, namely solving a quadratic system of algebraic equations [23]. In addition, the encryption/decryption procedures are very efficient and can be done in constrained environments [6, 10]. Among these cryptosystems, the Hidden Field Equations cryptosystem (HFE) is probably the most studied one. It has been proposed by Patarin [29] after his cryptanalysis [28] of the historical multivariate scheme C* [27]. In [26] Kipnis and Shamir proposed a key recovery attack on HFE, which reduces to the so-called MinRank [12] problem. Although the attack is not practical for the proposed parameters, it was conjectured to be sub-exponential. Later, Faugère and Joux [17, 19] proposed an efficient message recovery attack based on Gröbner bases. This attack, which is "*quasi-polynomial*" [24], raises serious doubt about the security of HFE. To thwart both attacks on HFE, it has been proposed to use

* Luk Bettale is partially supported by DGA/MRIS (french secretary of defense)

a multivariate system as the secret key [5] or odd-characteristic fields [14] or even both in a recent paper [11]. This new family of schemes is called multi-HFE in the rest of the paper.

Our contributions. We propose here a key recovery attack on HFE, multi-HFE and some of its variants. Our attack is an adaptation and improvement of the Kipnis-Shamir attack [26]. Precisely, we reduce the attack to the problem of finding a linear combination of the public quadratic forms of low rank. This problem is known as the MinRank (MR) problem (MR is usually defined for matrices, but the problem can be defined equivalently on quadratic forms). The coefficients in the linear relation that we are looking for are strongly related to one of the affine transforms used to hide the (multi-)HFE structure. We show that the MinRank can be expressed in the small field, which allows to considerably speed-up solving by approximately a factor corresponding to the square of the degree of the extension field. Thanks to recent results on MinRank [20, 21] and bilinear systems [22], we conjecture that the attack is polynomial in the degree of the extension. Using this complexity analysis, we can prove that, for the same size of keys (a precise definition of this notion is given in Sect. 3.6), multi-HFE is always less secure than HFE. In addition, the large number of equivalent keys allows to attack the minus variant (this amounts to remove some equations in the public key) using the induced degrees of freedom of the MinRank. Finally, we present an attack on the embedding variant of (multi-)HFE. This variant consists in instantiating some variables of the public system. However, a low rank linear combination of the quadratic forms can still be found. In this case, solving the corresponding MinRank on truncated quadratic forms allows us to recover only a rectangular sub matrix of the linear transform; to overcome this difficulty we need to extend this matrix in a special way (details can be found in Sect. 5) to make it invertible. As a proof of concept, we practically broke several parameters proposed in [11], supposed to have up to 256 bits security (experiments are given in Sect. 6). We also mention that the second part of the attack of Kipnis and Shamir as presented in [26] does not apply in characteristic 2. It is possible to overcome this problem but due to space limitation, this will be presented in an extended version of this paper. Consequently, we assume in the rest of the paper that q (the size of the small field) is odd.

2 Multivariate HFE

Throughout this paper, we use the following conventions: an underlined letter denotes a vector, e.g. $\underline{v} = (v_1, \ldots, v_n)$. A capital bold font letter denotes a matrix, e.g. $\mathbf{M} = [m_{i,j}]$. A calligraphic capital letter denotes a general mapping, e.g. $\mathcal{F}$.

For Multi-HFE, the parameters considered are $(q, N, d, D) \in \mathbb{N}^4$. Here, q (odd) denotes the size of the ground field $\mathbb{F}_q$, d is the degree of the extension field $\mathbb{F}_{q^d}$, N is the number of variables and equations of the secret polynomials in the ring $\mathbb{F}_{q^d}[X_1, \ldots, X_N]$, and D their degree. Throughout the paper, we use capital letters for elements relative to the big field $\mathbb{F}_{q^d}$ (e.g. $V_i \in \mathbb{F}_{q^d}$, $F_i \in \mathbb{F}_{q^d}[X_1, \ldots, X_N]$), and small letters for elements relative to $\mathbb{F}_q$ (e.g. $v_i \in \mathbb{F}_q$, $f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$). The secret internal transformation is $\mathcal{F}^* : (V_1, \ldots, V_N) \in (\mathbb{F}_{q^d})^N \mapsto \big(F_1(V_1, \ldots, V_N), \ldots, F_N(V_1, \ldots, V_N)\big) \in (\mathbb{F}_{q^d})^N$ with $\deg(F_i) \leqslant D$. The degree D is chosen such that $\mathcal{F}^*$ is easy to invert. In addition, the

polynomials $F_1, \ldots, F_N$ are constructed in a specific way:

$$F_k = \sum_{1 \leqslant i \leqslant j \leqslant N} \sum_{\substack{0 \leqslant u,v < d \\ q^u + q^v \leqslant D}} A_{k,i,u,j,v} X_i^{q^u} X_j^{q^v} + \sum_{1 \leqslant i \leqslant N} \sum_{\substack{0 \leqslant u < d \\ q^u \leqslant D}} B_{k,i,u} X_i^{q^u} + C_k.$$

From now on, we say that such systems have (multi-)HFE-shape. For convenience, we denote $n = Nd$. Let φ_N be the natural morphism $(\mathbb{F}_{q^d})^N \mapsto (\mathbb{F}_q)^n$ and $\mathscr{F}$ be the small field representation of the secret polynomials $\mathscr{F} = \varphi_N \circ \mathscr{F}^* \circ \varphi_N^{-1}$ with $\mathscr{F} : (v_1, \ldots, v_n) \in (\mathbb{F}_q)^n \mapsto (f_1(v_1, \ldots, v_n), \ldots, f_n(v_1, \ldots, v_n)) \in (\mathbb{F}_q)^n$. Due to the HFE-shape, each polynomial f_i has total degree 2. For the secret key, the mapping $\mathscr{F}^*$ is supplemented by two affine maps $\mathscr{S}, \mathscr{T} \in \mathrm{Aff}(n, \mathbb{F}_q)$ represented by matrices $\mathbf{S}$ and $\mathbf{T}$ which hide the internal structure. The public key $\mathscr{G} = \mathscr{T} \circ \mathscr{F} \circ \mathscr{S} : (v_1, \ldots, v_n) \in (\mathbb{F}_q)^n \mapsto (g_1(v_1, \ldots, v_n), \ldots, g_n(v_1, \ldots, v_n)) \in (\mathbb{F}_q)^n$ is then composed of polynomials $g_1, \ldots, g_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ of total degree 2.

To encrypt, we evaluate $g_1, \ldots, g_n$ in the message $\underline{m} = (m_1, \ldots, m_n) \in (\mathbb{F}_q)^n$. With the knowledge of the private key, the decryption of a ciphertext $\underline{c} = (c_1, \ldots, c_n) \in (\mathbb{F}_q)^n$ is done by computing $\mathscr{S}^{-1} \circ \varphi_N \circ \mathscr{F}^{*-1} \circ \varphi_N^{-1} \circ \mathscr{T}^{-1}(\underline{c})$. As each part can be inverted efficiently, the decryption is done efficiently.

The original HFE scheme [29] is mostly used over $\mathbb{F}_2$ with a single univariate polynomial as a secret map. It is then an instantiation of multi-HFE with $q = 2$ and $N = 1$. The construction PHFE (for projected HFE) of [14] is an odd characteristic univariate HFE that uses the embedding modifier (see Sect. 5). The scheme IFS (for Intermediate Field System) from [5] is a multi-HFE in characteristic 2 and THFE from [11] is a multi-HFE in odd characteristic (possibly with embedding modifier). To make the decryption efficient, all instances of multi-HFE with $N > 1$ use quadratic polynomials as internal secret transformations. Parameters examples from the literature are given in the tables below.

	q	N	d	D	security
HFE [29]	2	1	128	513	128
PHFE [14]	7	1	67	56	201

	q	N	d	D	security
IFS [5]	2	8	16	2	128
THFE [11]	31	3	10	2	150

We now review two attacks on the original HFE: the direct algebraic attack (message recovery) of [19] and the key recovery attack of [26].

2.1 Direct Algebraic Attack

Let $(c_1, \ldots, c_n) \in (\mathbb{F}_q)^n$ be a ciphertext, a message-recovery reduces to solve a system of quadratic equations, i.e. $\{g_1 - c_1 = 0, \ldots, g_n - c_n = 0\}$. A classical method to solve algebraic systems is to compute a Gröbner basis [8, 1, 13]. The historical method for computing Gröbner bases has been proposed by Buchberger in his PhD thesis [8]. The algorithms F_4 [15] and F_5 [16] by Faugère permit to improve the basic Buchberger's algorithm. A good measure of the complexity for Gröbner bases is the so-called "*degree of regularity*" of a system. This is the maximum degree of the polynomials appearing during the computation (see [2, 3]).

It appeared [17, 19] that inverting the public key of the original HFE is much easier than expected (i.e. in comparison to a random system of the same size). For original

HFE, the degree of regularity has been experimentally shown to be roughly $\log_q(D)$ (see [19]). This makes the attack sub-exponential in the number of variables. Further analysis of the Gröbner basis approach [24] confirmed this result. Note that the field equations (i.e. $x_1^q - x_1 = \ldots = x_n^q - x_n = 0$) are mandatory to achieve this complexity. Their role is to force the solutions to be only in the base field $\mathbb{F}_q$. To prevent a direct algebraic attack, it has been proposed [14] to use a field with a bigger characteristic. Field equations only intervene in degree at least q. Typically, a HFE system with $q > n$ seems very hard to solve with a direct approach (for n sufficiently big). Note that the hybrid approach described in [4] has been designed to solve such systems. However, for $n = 28$ and $q = 31$ the complexity of the hybrid approach is 2^{82}. It is better than a direct solving (2^{115}) but the attack remains exponential. For multi-HFE, the situation is almost similar. On characteristic 2, multi-HFE can still be attacked similarly. This confirms that the algebraic attack is somehow "optimal" over $\mathbb{F}_2$. However, the direct algebraic attack does not affect instantiations of multi-HFE with bigger odd characteristic as adding the field equations would not be useful.

2.2 Original Kipnis-Shamir (KS) Attack

We now describe the key recovery attack proposed in [26] for the original HFE scheme ($N = 1, n = d$). The starting idea is to remark that polynomials of the public key – as well as the transformations $\mathscr{S}, \mathscr{T}$ – can be viewed as mappings $\mathscr{G}^*, \mathscr{S}^*, \mathscr{T}^* : \mathbb{F}_{q^n} \mapsto \mathbb{F}_{q^n}$ and represented by the univariate polynomials $G, S, T \in \mathbb{F}_{q^n}[X]$. The public key relation then becomes $G = \mathscr{G}^*(X) = \mathscr{T}^*(\mathscr{F}^*(\mathscr{S}^*(X)))$. Kipnis and Shamir [26] proposed interpolation to recover a univariate representation of the public key. We present a more efficient and simpler way in Sect. 3 to perform this step.

Kipnis and Shamir [26] also showed that the univariate polynomials can be written as a "*non-standard quadratic form*". For instance, we have:

$$G = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} g_{i,j} X^{q^i+q^j} = \underline{X}\mathbf{G}\underline{X}^t, \text{ where } \underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$$

and $\mathbf{G} = [g_{i,j}]$ is a symmetric matrix. Similarly, we define $\mathbf{F} = [f_{i,j}]$ the symmetric matrix representation of the secret univariate polynomial.

The Kipnis-Shamir attack is based on the remark that $\text{Rank}\left(\mathbf{F}\right) \leqslant \log_q(D)$. Indeed, the degree of the secret polynomial is smaller than D and the only non-zero entries in $\mathbf{F}$ are $f_{i,j}$, if $i, j \leqslant \log_q(D)$. In addition, if we write $\mathscr{T}^{*-1}(X) = \sum_{k=0}^{n-1} t_k X^{q^i}$ and $\mathscr{S}^*(X) = \sum_{k=0}^{n-1} s_k X^{q^i}$ the equation $\mathscr{G}^*(X) = \mathscr{T}^*(\mathscr{F}^*(\mathscr{S}^*(X)))$ implies this so-called "*Fundamental Equation*" (see [26] for the proof).

$$\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k} = \mathbf{G}' = \widetilde{\mathbf{W}}\mathbf{F}\widetilde{\mathbf{W}}^t \tag{1}$$

where $\widetilde{\mathbf{W}} = [\widetilde{w}_{i,j}]$ is a specified invertible matrix (with $\widetilde{w}_{i,j} = s_{j-i}^{q^i}$) and $\mathbf{G}^{*k}$ the matrix such that its (i, j)-th entry is $g_{i-k,j-k}^{q^k}$. As the rank of $\mathbf{F}$ is bounded, so is the rank of $\mathbf{G}'$. Recovering the t_k's reduces to solve a MinRank problem:

MinRank (MR) in a finite field $\mathbb{K}$
Input: $n, r, k \in \mathbb{N}$ and matrices $\mathbf{M_1}, \ldots, \mathbf{M_k} \in \mathbb{K}^{n \times n}$.
Question: is there a k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$ such that Rank $\left(\sum_{i=1}^{k} \lambda_i \mathbf{M_i}\right) \leqslant r$.
The MinRank problem is NP-complete [9]. From an algorithmic point of view, Kipnis and Shamir proposed to model the problem as a system of overdetermined quadratic equations and then to solve it with the so-called relinearization method [26]. This Kipnis-Shamir modeling – which turns to be a set of bilinear equations [21] – as well as the so-called Minors modeling have been further studied and improved in [20, 21]. In both modelings, solving MinRank reduces to compute the solutions of a system of structured algebraic equations.

Once the t_k's of equation (1) are known, the s_k's are recovered by solving a linear system. From (1), we see that $\ker(\mathbf{G}') = \ker(\widetilde{\mathbf{W}}\mathbf{F})$ and thus $\ker(\mathbf{G}')\widetilde{\mathbf{W}} = \ker(\mathbf{F})$. Due to the special shape of $\mathbf{F}$, the first $\ell = \log_q(D)$ columns of its left kernel are 0. This gives rise to a linear system of equations of $\ell(n-\ell)$ equations in n^2 variables. Since $w_{i+1,j+1} = w_{i,j}^q$, Kipnis and Shamir proposed to reinterpret the equations over $\mathbb{F}_q$. This gives $n\ell(n-\ell)$ equations in n^2 variables over $\mathbb{F}_q$. Solving this overdetermined system completes the key recovery.

3 Improvement and Generalization of KS Attack

3.1 Improving the Univariate Case

To generalize the KS attack, it is convenient to interpret it as vector/matrix operations. In this paper, we denote by $\mathrm{Frob_k}$ the function raising all the components of a vector or a matrix to the power q^k in any field $\mathbb{K}$ of characteristic q. For example $\mathrm{Frob_k}(\underline{v}) = (v_1^{q^k}, \ldots, v_m^{q^k})$, for a vector $\underline{v} = (v_1, \ldots, v_m) \in \mathbb{K}^m$ and $\mathrm{Frob_k}(\mathbf{A}) = [a_{i,j}^{q^k}]$, for a matrix $\mathbf{A} = [a_{i,j}]$.

Proposition 1. *Let $(\theta_1, \ldots, \theta_n) \in (\mathbb{F}_{q^n})^n$ be a vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\mathbf{M}_n$ be the $n \times n$ matrix whose columns are the Frobenius powers of the basis:*

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

We can express the morphism $\varphi_1 : \mathbb{F}_{q^n} \mapsto (\mathbb{F}_q)^n$ as

$$V \mapsto (V, V^q, \ldots, V^{q^{n-1}})\,\mathbf{M}_n^{-1}$$

and its inverse $\varphi_1^{-1} : (\mathbb{F}_q)^n \mapsto \mathbb{F}_{q^n}$ as

$$(v_1, \ldots, v_n) \mapsto V_1, \text{ with } (V_1, \ldots, V_n) = (v_1, \ldots, v_n)\,\mathbf{M}_n.$$

Furthermore, we have that $V_{(i \mod n)+1}^q = V_{(i+1 \mod n)+1}$.

Proof. The i-th entry of $(v_1,\ldots,v_n)\mathbf{M}_n$ is $(\sum_{j=1}^{n} v_j\theta_j)^{q^i}$, the q^i-th power of the representation of $(v_1,\ldots,v_n)$ in $\mathbb{F}_{q^n}$ with respect to the basis $(\theta_1,\ldots,\theta_n)$. □

The matrix $\mathbf{M}_n$ allows to go back and forth from the big ($\mathbb{F}_{q^n}$) to the small field ($\mathbb{F}_q$). It can be used to have the univariate representation of the public key in a simpler way than in [26]; we replace interpolation by matrix multiplication. For the sake of simplicity, from now on, we consider only linear transformations and homogeneous polynomials. What follows can easily be adapted to the affine case (as pointed in [26]).

Let $\mathbf{F}^{*k}$ be the matrix such that its (i,j)-th entry is $f_{i-k,j-k}^{q^k}$. The matrix $\mathbf{F}^{*k}$ is the "matrix representation" of the q^k-th power of the univariate polynomial F. Indeed, since $F=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{i,j}X^{q^i+q^j}$, we have

$$\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{i-k,j-k}^{q^k}X^{q^i+q^j}=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{i,j}^{q^k}X^{q^{i+k}+q^{j+k}}=F^{q^k}.$$

Then, $F^{q^k}=\underline{X}\mathbf{F}^{*k}\underline{X}^t$.

Consider now the symmetric matrices $(\mathbf{G_1},\ldots,\mathbf{G_n})$ such that $g_i=\underline{x}\mathbf{G_i}\underline{x}^t$ for all $i, 1\leqslant i\leqslant n$, where $\underline{x}=(x_1,\ldots,x_n)$. Using the definition of φ_1 with the matrix $\mathbf{M}_n$, the equation $\mathscr{G}=\mathscr{T}\circ\mathscr{F}\circ\mathscr{S}$ becomes

$$(\mathbf{G_1},\ldots,\mathbf{G_n})=(\mathbf{S}\mathbf{M}_n\mathbf{F}^{*0}\mathbf{M}_n^t\mathbf{S}^t,\ldots,\mathbf{S}\mathbf{M}_n\mathbf{F}^{*n-1}\mathbf{M}_n^t\mathbf{S}^t)\mathbf{M}_n^{-1}\mathbf{T}.$$

As $\mathbf{T}$ and $\mathbf{M}_n$ are invertible, we have

$$(\mathbf{G_1},\ldots,\mathbf{G_n})\mathbf{T}^{-1}\mathbf{M}_n=(\mathbf{S}\mathbf{M}_n\mathbf{F}^{*0}\mathbf{M}_n^t\mathbf{S}^t,\ldots,\mathbf{S}\mathbf{M}_n\mathbf{F}^{*n-1}\mathbf{M}_n^t\mathbf{S}^t). \tag{2}$$

In other words, we have a direct relation between the polynomials of the public key written as quadratic forms and the secret polynomial F or more precisely its matrices $\mathbf{F}^{*i}$. From now on, we denote by $\mathbf{U}$ the matrix $\mathbf{T}^{-1}\mathbf{M}_n$ and $\mathbf{W}$ the matrix $\mathbf{S}\mathbf{M}_n$ and rewrite (2) as

$$(\mathbf{G_1},\ldots,\mathbf{G_n})\mathbf{U}=(\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t,\ldots,\mathbf{W}\mathbf{F}^{*n-1}\mathbf{W}^t). \tag{3}$$

By construction, $u_{i,j+1}=u_{i,j}^q$ and $w_{i,j+1}=w_{i,j}^q$. Thus, we only need to know one column of $\mathbf{U}$ to recover the whole matrix. By considering $(u_{0,0},\ldots,u_{n-1,0})^t$, the first column of $\mathbf{U}$, we have

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}=\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t=\mathbf{W}\mathbf{F}\mathbf{W}^t. \tag{4}$$

The equation is similar to (1), but we have not used the univariate representation of $\mathscr{G}$. Here again, as the rank of $\mathbf{F}$ is $\log_q(D)$, so is the rank of $\mathbf{W}\mathbf{F}\mathbf{W}^t$. Contrarily to the initial attack, $\mathbf{G_i}$ are the public matrices and not matrices with coefficients in the big field. This leads to the following theorem.

Theorem 1. *For HFE, recovering* $\mathbf{U}$ *reduce to solve a MinRank with* $k=n$ *and* $r=\log_q(D)$ *on the public matrices* $\mathbf{G_1},\ldots,\mathbf{G_n}$ *whose entries are in* $\mathbb{F}_q$.

Computing a Gröbner basis of a system over a smaller field ($\mathbb{F}_q$ instead of $\mathbb{F}_{q^n}$ is faster as the cost of arithmetic operations is decreased. The expected gain is a factor $\mathrm{M}(n)$ (the cost of the multiplication of two univariate polynomials of degree n) over the KS attack. In the table below, we compare the original KS Minrank attack and the new MinRank attack on HFE ($N = 1$) with parameters $q = 31$, $D = 31^2 + 31 = 992$. The implementation used is the same as in Sect. 6.

n	8	9	10	11	12	13	14	15	16
KS attack (in s.)	15.3	20.4	76.9	391	680	1969	2439	3197	13407
new attack (in s.)	0.75	1.25	2.05	4.45	8.80	16.9	30.2	68.5	103
ratio	20.4	16.3	37.5	87.9	77.3	117	80.8	46.7	130

3.2 Attacking Multi-HFE

The Kipnis-Shamir attack uses the univariate representation of the public key. In multi-HFE the degree of the univariate representation of the secret key is not bounded. This was in fact the initial motivation for the design of IFS [5]. As a consequence, there is no linear combination of the $\mathbf{G}^{*k}$ leading to a small rank, making the MinRank attack impossible. The hidden field structure exists but it can only be unveiled by working in the right field. To have the correct analogy with the univariate case, we introduce a new change of basis between the small field vector space $(\mathbb{F}_q)^n$ and the big field vector space $(\mathbb{F}_{q^d})^N$.

Proposition 2. *Let $(\theta_1,\ldots,\theta_d) \in (\mathbb{F}_{q^d})^d$ be a vector basis of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$. Let $\mathbf{M}_{N,d}$ be the $(n \times n)$-matrix such that $\mathbf{M}_{N,d} = \mathrm{Diag}(\underbrace{\mathbf{M}_d,\ldots,\mathbf{M}_d}_{N})$. We can express the morphism $\varphi_N : (\mathbb{F}_{q^d})^N \mapsto (\mathbb{F}_q)^n$ as*

$$(V_1,\ldots,V_N) \mapsto (V_1,V_1^q,\ldots,V_1^{q^{d-1}},\ldots\ldots,V_N,V_N^q,\ldots,V_N^{q^{d-1}})\,\mathbf{M}_{N,d}^{-1}$$

and its inverse $\varphi_N^{-1} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_{q^d})^N$ as

$$(v_1,\ldots,v_n) \mapsto (V_1,V_{d+1},\ldots,V_{d(N-1)+1}) \text{ with } (V_1,\ldots,V_n) = (v_1,\ldots,v_n)\,\mathbf{M}_{N,d}.$$

Furthermore, we have that $V_{id+(j \mod d)+1}^q = V_{id+(j+1 \mod d)+1}$.

Proof. The $(d(i-1)+j)$-th entry of $(v_1,\ldots,v_n)\,\mathbf{M}_{N,d}$ is $\left(\sum_{\ell=1}^{d} v_{d(i-1)+\ell}\theta_\ell\right)^{q^j}$. Each N block of d values represents the vector $(V_i,V_i^q,\ldots,V_i^{q^{d-1}})$, for all $i, 1 \leqslant i \leqslant N$. Thus $(v_1,\ldots,v_n)\,\mathbf{M}_{N,d}$ is $(V_1,V_1^q,\ldots,V_1^{q^{d-1}},\ldots,V_N,V_N^q,\ldots,V_N^{q^{d-1}})$ with respect to the basis $(\theta_1,\ldots,\theta_d)$. □

Note that $\mathbf{M}_{1,d} = \mathbf{M}_d$ which generalizes Proposition 1. When $N > 1$, the q^k-th power of a polynomial $F_i \in \mathbb{F}_{q^d}[X_1,\ldots,X_N]$ is represented by the matrix $\mathbf{F_i}^{*d,k} = [f^{q^k}_{d\lfloor i/d\rfloor+(i-1 \mod d),d\lfloor j/d\rfloor+(j-1 \mod d)}]$

(this definition matches the case $N = 1$). Equation (3) can be generalized for multi-HFE. Let $\mathbf{F_i}^{(j)} = \mathbf{W}{\mathbf{F_i}}^{*d,j}\mathbf{W}^t$, with $i, 1 \leqslant i \leqslant N$, and $j, 0 \leqslant j < d$. We have the relation:

$$(\mathbf{G_1}, \ldots, \mathbf{G_n})\,\mathbf{U} = (\mathbf{F_1}^{(0)}, \ldots, \mathbf{F_1}^{(d-1)}, \ldots\ldots, \mathbf{F_N}^{(0)}, \ldots, \mathbf{F_N}^{(d-1)}).$$

Similarly to (4), as ${\mathbf{F_i}}^{*d,0} = \mathbf{F_i}$, when we consider the $(i\,d)$-th columns of $\mathbf{U}$ for $0 \leqslant i < N$ we have

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_1}\mathbf{W}^t, \ldots, \sum_{k=0}^{n-1} u_{k,Nd}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F_N}\mathbf{W}^t. \tag{5}$$

As in the univariate case, the problem of finding correct values for $\mathbf{U}$ turns to be a simultaneous MinRank problem.

Theorem 2. *For multi-HFE, recovering* $\mathbf{U}$ *reduce to simultaneously solve N MinRank problems with* $k = n$ *and* $r = N\log_q(D)$ *on the public matrices* $\mathbf{G_1}, \ldots, \mathbf{G_n}$ *whose entries are in* $\mathbb{F}_q$.

Proof. Each polynomial F_i has degree bounded by D, thus each variable X_i has at most degree D. By construction of the matrix $\mathbf{M}$ of Proposition 2, the only non-zero entries of the matrix $\mathbf{F_i} = {\mathbf{F_i}}^{*d,0}$ are the ones in the upper-left $\log_q(D)$ square of each N diagonal $(d \times d)$ block. The rank of $\mathbf{F_i}$ is then $N\log_q(D)$. By construction, the rank of ${\mathbf{F_i}}^{*d,j}$ is left unchanged. □

Before discussing of the complexity of the MinRank attack for Multi-HFE, we introduce equivalent keys.

3.3 About Equivalent Keys and Induced Degrees of Freedom

Two keys are equivalent if they have the same public key. The subject has already been treated for original HFE [31, 30]. It has been shown to have (at least) $(nq^{2n}(q^n-1)^2)$ equivalent keys. A larger number of equivalent keys in multi-HFE induces a degree of freedom when solving the MinRank that can be used to attack the minus variant. Due to space limitations, proofs of Propositions 3, 4, and 5 will be given in an extended version of this paper.

Definition 1. *Let* $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ *be a multi-HFE private key with parameters* (q, N, d, D). *We say that* $(\mathscr{F}^{*\prime}, \mathscr{S}', \mathscr{T}')$ *is an equivalent key iff* $\mathscr{F}^{*\prime}$ *has a HFE-shape, and* $\mathscr{T}' \circ \varphi_N \circ \mathscr{F}^{*\prime} \circ \varphi_N^{-1} \circ \mathscr{S}' = \mathscr{G} = \mathscr{T} \circ \varphi_N \circ \mathscr{F}^* \circ \varphi_N^{-1} \circ \mathscr{S}$ *(same public key).*

Wolf and Preneel [31] introduced the notion of sustaining transformations which is a couple of affine transformations $(\mathscr{A}^*, \mathscr{B}^*)$ such that $\mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^*$ preserves the "shape" of $\mathscr{F}^*$. For HFE, the "big sustainer" (multiplication in the big field), the "additive sustainer" and the "Frobenius sustainer" keep the HFE-shape unchanged. In multi-HFE, not only multiplication keeps the HFE-shape. We also have any affine transformation on the N variables. Thus, the two first sustainers can be generalized as follows.

Lemma 1. *Let* $(q, N, d, D) \in \mathbb{N}^4$ *and* $\mathscr{F}^* : (\mathbb{F}_{q^d})^N \mapsto (\mathbb{F}_{q^d})^N$ *a mapping with HFE-shape. Let* $\mathscr{A}^*, \mathscr{B}^*$ *be invertible affine transformations over* $(\mathbb{F}_{q^d})^N$. *Then* $\mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^*$ *has the HFE-shape.*

Proof. The only exponents occurring in a single variable X_i is a power of q. The transformation $\mathscr{A}^*$ mixes the variables $X_1,\dots,X_N$ by affine combinations. Thus by linearity of the Frobenius, we know that no other exponents can appear and the system keeps its HFE-shape. Trivially, as $\mathscr{B}^*$ only performs affine combinations of the polynomials $F_1,\dots,F_N$ the shape is also unchanged. □

With lemma 1, we can produce HFE internal maps while keeping the same property. To build equivalent keys, we look at these affine transformations in the small field $\mathbb{F}_q$.

Proposition 3. *Let $(\mathscr{F}^*,\mathscr{S},\mathscr{T})$ be a multi-HFE private key with parameters (q,N,d,D). For any invertible affine transformations $\mathscr{A}^*,\mathscr{B}^*$ over $(\mathbb{F}_{q^d})^N$, let $\mathscr{A}=\varphi_N\circ\mathscr{A}^*\circ\varphi_N^{-1}$ and $\mathscr{B}=\varphi_N\circ\mathscr{B}^*\circ\varphi_N^{-1}$, then $\left(\mathscr{B}^*\circ\mathscr{F}^*\circ\mathscr{A}^*,\mathscr{A}^{-1}\circ\mathscr{S},\mathscr{T}\circ\mathscr{B}^{-1}\right)$ is an equivalent key.*

The following proposition gives the structure of one of these transformations in the linear case. It has to be slightly adapted in the affine case.

Proposition 4. *Let $\mathbf{A}^*=[a_{i,j}]$ be the matrix representing a linear transformation $\mathscr{A}^*$ over $(\mathbb{F}_{q^d})^N$. $\mathscr{A}^*$ can be represented in the field $\mathbb{F}_q$ as $\mathbf{A}=\mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{M}_{N,d}^{-1}$ where $\mathbf{M}_{N,d}$ is the matrix of Proposition 2 and $\widetilde{\mathbf{A}^*}$ is a matrix of $N\times N$ blocks of Frobenius powers of elements of $\mathbf{A}^*$, i.e.*

$$\widetilde{\mathbf{A}^*}=\begin{pmatrix}
\begin{vmatrix} a_{0,0} & & \\ & a_{0,0}^q & \\ & & \ddots \\ & & & a_{0,0}^{q^{d-1}} \end{vmatrix} & \cdots & \begin{vmatrix} a_{0,N-1} & & \\ & a_{0,N-1}^q & \\ & & \ddots \\ & & & a_{0,N-1}^{q^{d-1}} \end{vmatrix} \\
\vdots & & \vdots \\
\begin{vmatrix} a_{N-1,0} & & \\ & a_{N-1,0}^q & \\ & & \ddots \\ & & & a_{N-1,0}^{q^{d-1}} \end{vmatrix} & \cdots & \begin{vmatrix} a_{N-1,N-1} & & \\ & a_{N-1,N-1}^q & \\ & & \ddots \\ & & & a_{N-1,N-1}^{q^{d-1}} \end{vmatrix}
\end{pmatrix}$$

In addition, for any k, $0\leqslant k<d$, the components polynomials of $(\mathrm{Frob_k}\circ\mathscr{F}^*\circ\mathrm{Frob_{d\text{-}k}})(X_1,\dots,X_N)=\left(\mathscr{F}^*(X_1^{q^{d-k}},\dots,X_N^{q^{d-k}})\right)^{q^k}$ have the same monomials as $\mathscr{F}^*(X_1,\dots,X_N)$ but their coefficients are raised to the power of q^k. That is, if $\mathscr{F}^*(X_1,\dots,X_N)$ has HFE-shape, so is $(\mathrm{Frob_k}\circ\mathscr{F}^*\circ\mathrm{Frob_{d\text{-}k}})(X_1,\dots,X_N)$.

Proposition 5. *Let $(\mathscr{F}^*,\mathscr{S},\mathscr{T})$ be a multi-HFE private key with parameters $(q,N,d,D)\in\mathbb{N}^4$. For all $k,0\leqslant k<d$,*

$$\left(\mathrm{Frob_k}\circ\mathscr{F}^*\circ\mathrm{Frob_{d\text{-}k}},\varphi_N\circ\mathrm{Frob_k}\circ\varphi_N^{-1}\circ\mathscr{S},\mathscr{T}\circ\varphi_N\circ\mathrm{Frob_{d\text{-}k}}\circ\varphi_N^{-1}\right)$$

is an equivalent key.

According to Proposition 5, we can derive $(d-1)$ other equivalent keys from any valid private key. This refers to the so-called Frobenius sustainer of [31]. We can count the number of equivalent keys.

Theorem 3. *For any multi-HFE private key* $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ *with given parameters* $(q, N, d, D) \in \mathbb{N}^4$*, there are at least* $\left(q^{dN} \prod_{i=0}^{N-1} (q^{dN} - q^{di})\right)^2$ *equivalent keys coming from affine transformations in* $\mathrm{Aff}(N, \mathbb{F}_{q^d})$.

Proof. There are exactly $\prod_{i=0}^{N-1} \left((q^d)^N - (q^d)^i\right)$ invertible $(N \times N)$-matrices over $\mathbb{F}_{q^d}$. We have to multiply this by $(q^d)^N$ to include the affine transformations. From Proposition 3, one can choose 2 invertible affine transformations over the big field to build an equivalent key, thus the previous value is squared. □

This number may actually be bigger (at most d times) using the Frobenius sustainer. An interesting particularity of the MinRank arising in HFE/multi-HFE is that the kernel of the matrices in (5) is independent on which equivalent key is used up to Frobenius transforms.

Theorem 4. *Let* $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ *and* $(\mathscr{F}^{*\prime}, \mathscr{S}', \mathscr{T}')$ *be equivalent multi-HFE private keys and* $(\mathbf{G_1} \dots \mathbf{G_n})$ *be the matrices of their associated public key. Let* $\mathbf{S}$, $\mathbf{T}$, $\mathbf{S}'$, *and* $\mathbf{T}'$ *be the matrix representation of respectively* $\mathscr{S}$, $\mathscr{T}$, $\mathscr{S}'$, *and* $\mathscr{T}'$. *Let* $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_{N,d} = [u_{i,j}]$, $\mathbf{K} = \ker(\sum_{i=0}^{n} u_{i,0}\mathbf{G_i})$, $\mathbf{U}' = \mathbf{T}'^{-1}\mathbf{M}_{N,d} = [u'_{i,j}]$ *and* $\mathbf{K}' = \ker(\sum_{i=0}^{n} u'_{i,0}\mathbf{G_i})$, *then* $\exists k, 0 \leqslant k < d, \mathbf{K}' = \mathrm{Frob_k}(\mathbf{K})$.

Proof. By construction of equivalent keys, $u'_{i,j}$ are linear combinations of the $u_{i,\ell}^{q^k}$ for a given k. Linear combinations of $u_{i,j}$ do not change the kernel. By linearity, $u'_{i,j} = \sum_\ell \alpha_\ell u_{i,\ell}^{q^k} = \left(\sum_\ell \alpha_\ell u_{i,\ell}\right)^{q^k}$. Consequently, $\mathbf{K}' = \mathrm{Frob_k}(\mathbf{K})$. □

We discuss the complexity of our attack in the next section.

3.4 Complexity analysis of the attack

In this section, we study the particularities of the MinRank problems coming from (5). Here again we consider only linear maps and homogeneous polynomials for the sake of simplicity.

Let an instance of HFE with parameters $(q, N, d, D) \in \mathbb{N}^4$, and $\ell = \lceil \log D \rceil$. We have to solve the MinRank problem on the $(n \times n)$-matrices $\mathbf{G_1} \dots \mathbf{G_n}$ whose entries lie in $\mathbb{F}_q$ with target rank $N\ell$. Using the Kipnis-Shamir modeling described in [26, 20, 21], it is equivalent to solve the algebraic system of the $(n(n - N\ell))$ bilinear equations in $(N\ell(n - N\ell) + n)$ variables given by the entries of the matrix

$$\begin{pmatrix} 1 & & x_{1,1} & \dots & x_{1,N\ell} \\ & \ddots & \vdots & & \vdots \\ & & 1 & x_{n-N\ell,1} & \dots & x_{n-N\ell,N\ell} \end{pmatrix} \cdot \left(\sum_{i=1}^{n} \lambda_i \mathbf{G_i}\right). \tag{6}$$

Note that we are looking for solutions in the field $\mathbb{F}_{q^d}$ rather than in $\mathbb{F}_q$.

From now on, and similarly to [20], these equations are called the KS (Kipnis-Shamir) equations. We denote by $\mathscr{I}_{\mathrm{KS}}$ the ideal generated by the KS equations and $\mathscr{V}_{\mathrm{KS}} \subset \mathbb{F}_{q^d}$ its associated variety.

Theorem 5. *The MinRank problem associated to HFE (resp. multi-HFE) can be solved by fixing one (resp. N) coefficients to random values. That is, the dimension of* $\mathscr{I}_{\mathrm{KS}} \cap \mathbb{F}_q[\lambda_1, \ldots, \lambda_n]$ *is at least one (resp. N).*

Proof. We know that any column of $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_{N,d}$ is a solution of MinRank for $(\lambda_1, \ldots, \lambda_n)$. From Proposition 3, for any invertible matrix $\mathbf{A}^*$, the columns of the matrix $\mathbf{U}\widetilde{\mathbf{A}^*}$ give a solution $(\lambda_1, \ldots, \lambda_n)$ for the MinRank. As each column of $\widetilde{\mathbf{A}^*}$ has N non-zero entries, this allows to choose N coefficients λ_i arbitrarily. □

This means that for valid values $x_{i,j}$, there are $(q^d)^N$ possible vectors $(\lambda_1, \ldots, \lambda_n)$ such that the kernel of $\left(\sum_{i=1}^n \lambda_i \mathbf{G_i}\right)$ is the one induced by the $x_{i,j}$'s. Therefore, the values of N components (say $\lambda_1, \ldots, \lambda_N$) can be randomly chosen. The new system still has $(n(n - N\ell))$ equations but only $(N\ell(n - N\ell) + n - N)$ variables. As described in Sect. 3.1, the coefficients are in the small field $\mathbb{F}_q$. To keep this property, we fix variables with values over the small field. Experimentally, fixing one variable to 1 (or any value from $\mathbb{F}_q$) and the $(N-1)$ others to 0 gives the best results. After N variables $(\lambda_1, \ldots, \lambda_N)$ have been fixed, $\mathscr{V}_{\mathrm{KS}}$ has at least d elements. This property already noticed in [25] for HFE is a direct consequence of theorem 4. Once $\mathbf{K} = \ker\left(\sum_{k=1}^n \lambda_k \mathbf{G_k}\right)$ is recovered, finding a valid transformation $\mathbf{U}'$ is done by solving a linear system as entries of (6) become linear. Some experimental results of our attack are presented in Sect. 6.

It is interesting to remark that the degree of regularity experimentally observed seems to be constant when d grows. This behavior can be explained theoretically using the bound on the degree of regularity of MinRank given in [21].

Proposition 6 (Faugère, Safey El Din, Spaenlehauer [21]). *Let* (n, r, k) *be the parameters of a MinRank instance. Let* $\mathbf{A} = [a_{i,j}]$ *be the* $(r \times r)$*-matrix defined by* $a_{i,j}(t) = \sum_{\ell=0}^{n-\max(i,j)} \binom{n-i}{\ell}\binom{n-j}{\ell} t^\ell$. *The degree of regularity of the system associated to MinRank instance is bounded from above by* $1 + \deg(\mathrm{HS}(t))$ *where* $\mathrm{HS}(t)$ *is the polynomial obtained from the first positive terms of the series* $(1-t)^{(n-r)^2-k} \frac{\det \mathbf{A}(t)}{t^{\binom{r}{2}}}$.

Back to our specific MinRank problem, we have instantiate this theoretical bound with multi-HFE parameters for values of $N \leqslant 20$ and $\ell \leqslant 10$. When d, is sufficiently bigger than ℓ, we always obtain $(N\ell + 1)$ (verified for $N\,d$ up to 500). Since the parameter d is not involved we state the following conjecture.

Conjecture 1. The degree of regularity of the MinRank problem associated to a multi-HFE instance does not depend on d. When d grows to infinity, it is bounded from above by $(N\ell + 1)$.

The degree of regularity depends only in the number N of secret variables and the degree D of the secret polynomials. This is consistent with the observations on simple HFE where d_{reg} was observed to be $\log(D)$. We have the necessary material to evaluate the difficulty of MinRank involved in HFE/multi-HFE.

Proposition 7. *Assuming Conjecture 1, for N and* ℓ *fixed, the complexity of solving the multi-HFE MinRank problem is* $\mathscr{O}\left(d^{(N\ell+1)\,\omega}\right)$ $\left(2 \leqslant \omega < 3 \text{ being the linear algebra constant}\right)$ *and thus polynomial in d.*

Proof. According to Conjecture 1, the degree of regularity is $(N\ell+1)$ and thus independent of the degree of the extension d. When d grows to infinity, the complexity of the Gröbner basis computation [2, 3] is $\mathscr{O}\left(\binom{Nd+N\ell+1}{N\ell+1}^{\omega}\right) \sim \mathscr{O}\left((Nd)^{(N\ell+1)\,\omega}\right) \sim \mathscr{O}\left(d^{(N\ell+1)\,\omega}\right)$. □

Once the matrix $\mathbf{U}$ has been found with the MinRank attack, we need to recover the matrix $\mathbf{W}$.

3.5 Recovering the transformation on the variables

Kipnis and Shamir [26] originally proposed a method for this step by solving an overdetermined system of $(n\ell(n-\ell))$ linear equations in n^2 variables over $\mathbb{F}_q$. Applied to multi-HFE, it would give $(n\ell(n-N\ell))$ equations in n^2 variables over $\mathbb{F}_q$. We propose here an alternative method which reduces the number of variables and equations by a factor d while it is done over the big field.

Lemma 2. *Let $(\mathbf{G_1},\ldots,\mathbf{G_n})$ be a multi-HFE public key and $\ell = \lceil \log_q(D) \rceil$. Suppose that the matrix $\mathbf{K} = \ker(\sum_{k=1}^{n} \lambda_k \mathbf{G_k})$ has $\mathrm{Rank}(\sum_{k=1}^{n} \lambda_k \mathbf{G_k}) = N\ell$. Once $\mathbf{K}$ is known, then we can recover a matrix $\mathbf{W}' = \mathbf{S}'\mathbf{M}_{N,d}$ such that $\mathbf{S}'$ is a valid matrix for the private key by solving a linear system of $(N\ell(n-N\ell))$ equations in $(N(n-N))$ variables.*

Proof. To find the coefficients $w_{i,j}$, it is enough to remark that from (5) one has $\mathbf{KW}' = \ker(\mathbf{F_i})$. We know by construction of the private key that $\ker(\mathbf{F_i})$ has $N\ell$ columns set to zero. By construction of $\mathbf{W}'$, N columns are needed to build the whole matrix. We build the corresponding linear system of $\left(N(n-N\ell)\right)$ equations in Nn variables. Proposition 3 tells us that one can randomly fix N variables on each of the N columns which gives $(N(n-N))$ variables left. If $\ell > 1$, the system is underdetermined. To find the matrix, we have to add the $\left((\ell-1)N(n-N\ell)\right)$ equations coming from $\mathrm{Frob_j}(\mathbf{K})\mathbf{W}' = \ker(\mathbf{F_i}^{*d,j})$. For $j, (d-\ell+1) \leqslant j < d$, it can be verified that $\ker(\mathbf{F_i}^{*d,j})$ has also $N\ell$ columns set to zero. The system has $\left(N\ell(n-N\ell)\right)$ linear equations. □

Recovering the polynomial system. Once the matrices $\mathbf{T}' = \mathbf{M}_{N,d}\mathbf{U}'^{-1}$ and $\mathbf{S}' = \mathbf{W}'\mathbf{M}_{N,d}^{-1}$ are recovered, we only need to reconstruct a private transformation. It is done simply by computing $\mathscr{F}^{*\prime} = \varphi_N^{-1} \circ \mathscr{T}'^{-1} \circ \mathscr{G} \circ \mathscr{S}'^{-1} \circ \varphi_N$. By construction of its components, the transformation $\mathscr{F}$ respects the HFE-shape.

3.6 Weaknesses of Multi-HFE Relative to the Original HFE

In order to compare instances of HFE/multi-HFE, we introduce the notion of "similarity" between instances. Two similar instances share the same size of public key and private key.

Definition 2. *Two (multi-)HFE instances of resp. parameters (q_1,N_1,d_1,D_1) and (q_2,N_2,d_2,D_2) are* similar *iff $q_1 = q_2$ and $N_1 d_1 = N_2 d_2$ and $N_1 \log_{q_1}(D_1) = N_2 \log_{q_2}(D_2)$ holds.*

The KS equations of two similar instances have the same number of variables and equations as the target rank is the same $N\log_q(D)$. According to the complexity of the MinRank given in Proposition 7, the bigger is d, the harder it is to mount our attack. In particular, the case $N=1$ (original HFE) is the more resistant. This behavior has been verified experimentally. For similar keys, choosing $N=1$ seems to be the optimal value for security. With respect to our attack, multi-HFE is then less secure than HFE.

As a side remark, speed of decryption has to be taken into account when designing a scheme. Choosing $N=1$ and a big degree D of the inner univariate polynomial can sometimes dramatically slow down the decryption process for similar keys. Multi-HFE construction could still be competitive if a modification can prevent attacks. To this end, the minus modifier and the embedding modifier have been proposed. We study these variants in the next sections.

4 Multivariate HFE$^-$

In this section, we study a classical variant of multivariate schemes, the so-called "minus" modifier. It consists in removing some polynomials from the public key. This construction is only suitable for signature as the decryption (signature generation) is not unique.

Description. Let $(\mathscr{F}^*,\mathscr{S},\mathscr{T})$ be a multi-HFE private key as defined in Sect. 2 with parameters $(q,N,d,D)\in\mathbb{N}^4$. We define the parameter $s\in\mathbb{N}$ and the projection $\pi:(\mathbb{F}_q)^n\mapsto(\mathbb{F}_q)^{n-s}$. The public key is the mapping $\mathscr{G}=\pi\circ\mathscr{T}\circ\varphi_N^{-1}\circ\mathscr{F}^*\circ\varphi_N\circ\mathscr{S}$ viewed as $(n-s)$ polynomials in n variables. To sign, s random values from $\mathbb{F}_q$ are appended to a message $\underline{m}=(m_1,\ldots,m_{n-s})$ before applying the basic decryption process. Verifying a signature consists in its evaluation in $\mathscr{G}$.

Attack. The goal is to find a valid private key with only $(n-s)$ public polynomials. Usually the minus modification is enough to prevent classical attacks as some information is missing. In particular it is the case for basic HFE ($N=1$). In Sect. 3.4, we have shown that the problem has N degrees of freedom. Indeed, only $(n-N+1)$ matrices are needed to recover the kernel. This means that if $s<N$, the kernel matrix $\mathbf{K}$ can still be found with no additional cost. Still, the recovering step has to be adapted. We know that there exists a vector $(\lambda_1,\ldots,\lambda_n)$ and symmetric $(n\times n)$-matrices $(\blacksquare_1,\ldots,\blacksquare_s)$ such that

$$\ker\left(\sum_{i=1}^{n-s}\lambda_i\mathbf{G_i}+\sum_{i=1}^{s}\lambda_{n-s+i}\blacksquare_\mathbf{i}\right)=\mathbf{K}.$$

The $\blacksquare_\mathbf{i}$'s matrices are unknown and correspond to the removed polynomials. If we fix N values λ_i, we still have solutions to our system. For instance, let $(\lambda_{n-N+1},\ldots,\lambda_n)=(\ell_1,\ldots,\ell_N)$. We write

$$\mathbf{K}\cdot\left(\sum_{i=1}^{n-N}\lambda_i\mathbf{G_i}+\sum_{i=1}^{N-s}\ell_i\mathbf{G_{n-N+i}}+\sum_{i=1}^{s}\ell_{N-s+i}\blacksquare_\mathbf{i}\right)=\mathbf{0}. \tag{7}$$

The resulting system has $n(n-N\ell)$ *linear* equations in $\left((n-N)+s\frac{n(n+1)}{2}\right)$ variables. The system is greatly underdetermined and hence have many solutions. To find the correct entries, we use the following remark:

Proposition 8. *For any* $j, 0 \leqslant j < d$, *we have* $\mathrm{Frob_j}(\mathbf{K}) \cdot \left(\sum_{i=1}^{n} \lambda_i^{q^j} \mathbf{G_i}\right) = \mathbf{0}$.

Proof. By definition, $\mathrm{Frob_j}\left(\mathbf{K} \cdot \left(\sum_{i=1}^{n} \lambda_i \mathbf{G_i}\right)\right) = \mathbf{0}$. By linearity of the Frobenius, this is equal to $\mathrm{Frob_j}(\mathbf{K}) \cdot \left(\sum_{i=1}^{n} \lambda_i^{q^j} \mathrm{Frob_j}(\mathbf{G_i})\right)$. As $\mathbf{G_i}$ has its entries in $\mathbb{F}_q$, we also have that $\mathrm{Frob_j}(\mathbf{G_i}) = \mathbf{G_i}$. □

Solving together equations (7) and their Frobenius images forces the entries of $\blacksquare_\mathbf{i}$ to be in $\mathbb{F}_q$. To avoid carrying equations of degree q^j (coming from $\lambda_i^{q^j}$), we add $(d-1)(n-N)$ new variables $(\lambda_1^{(1)}, \ldots, \lambda_{n-N}^{(1)}, \ldots, \lambda_1^{(d-1)}, \ldots, \lambda_{n-N}^{(d-1)})$. The new system then becomes:

$$\mathrm{Frob_j}(\mathbf{K}) \cdot \left(\sum_{i=1}^{n-N} \lambda_i^{(j)} \mathbf{G_i} + \sum_{i=1}^{N-s} \ell_i^{q^j} \mathbf{G_{n-N+i}} + \sum_{i=1}^{s} \ell_{N-s+i}^{q^j} \blacksquare_\mathbf{i} \right) = \mathbf{0},$$

for all $j, 0 \leqslant j < d$. The resulting system is overdetermined and has a solution if $(\ell_1, \ldots, \ell_N) \neq (0, \ldots, 0)$. We have to solve N times this linear system with different values for $(\ell_1, \ldots, \ell_N)$ to get a valid matrix $\mathbf{U}$. With this technique, the private key of a multi-HFE$^-$ can be recovered almost as efficiently as the standard construction if the number of withdrawn equations is less than $(N-1)$. Experimental results are presented in Sect. 6.

5 Multivariate HFE with Embedding

In [14], it has been proposed to use a variant of HFE with embedding. This so-called PHFE construction consists in removing few variables of the public key and is claimed to resist Kipnis-Shamir's attack. The authors of [11] use the same modification on multi-HFE and claim that it prevents a possible "big-field" based attack. Still, for both PHFE and its multivariate version a key recovery attack is possible.

Description. Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key as defined in Sect. 2 with parameters $(q, N, d, D) \in \mathbb{N}^4$. We define a new parameter $r \in \mathbb{N}$ and the embedding $\rho : (\mathbb{F}_q)^{n-r} \mapsto (\mathbb{F}_q)^n$ which is part of the private key. Then the public key is the mapping $\mathscr{G} = \mathscr{T} \circ \varphi_N^{-1} \circ \mathscr{F}^* \circ \varphi_N \circ \mathscr{S} \circ \rho$. To encrypt a plaintext, we still evaluate $\mathscr{G}$. To decrypt, as in the standard scheme, one inverts each component separately. To simplify, we can assume w.lo.g. that the embedding is always $\rho_0 : (x_1, \ldots, x_{n-r}) \in (\mathbb{F}_q)^{n-r} \mapsto (x_1, \ldots, x_{n-r}, 0, \ldots, 0) \in (\mathbb{F}_q)^n$. Indeed, from any embedding ρ and any invertible transformation $\mathscr{S}$, one can find an invertible transformation $\mathscr{S}'$ such that $\mathscr{S} \circ \rho = \mathscr{S}' \circ \rho_0$; this gives equivalent keys.

Attack. The matrix representation $\mathbf{G_i}$ of the public key polynomials have $(n-r)$ rows and columns. However, the rank of $\sum_{i=0}^{n} u_{i,0} \mathbf{G_{i+1}}$ remains bounded by $N \log_q(D)$ (i.e. removing rows or columns does not increase the rank).

Let $\mathbf{K} = \ker\left(\sum_{i=0}^{n} u_{i,0} \mathbf{G_{i+1}}\right)$. As usual a matrix $\mathbf{U}'$ can still be recovered by solving a MinRank as soon as $\mathbf{K}$ is known. The problem appears when trying to recover the matrix $\mathbf{W}' = \mathbf{S}' \mathbf{M}_{N,d}$ where $\mathbf{S}'$ is an equivalent matrix for the private key. By following the method described in Sect. 3.5, we get a system having $N\ell(n-r-N\ell)$ equations

with only $N(n-r-N)$ variables. Let the following matrix be a solution of this linear system

$$\mathbf{W}' = \begin{pmatrix} w_{0,0} & w_{0,0}^q & \dots & w_{0,0}^{q^{d-1}} & \dots\dots & w_{0,N-1} & w_{0,N-1}^q & \dots & w_{0,N-1}^{q^{d-1}} \\ \vdots & \vdots & \dots & \vdots & \dots\dots & \vdots & \vdots & \dots & \vdots \\ w_{n-r,0} & w_{n-r,0}^q & \dots & w_{n-r,0}^{q^{d-1}} & \dots\dots & w_{n-r,N-1} & w_{n-r,N-1}^q & \dots & w_{n-r,N-1}^{q^{d-1}} \end{pmatrix}.$$

The matrix $\mathbf{W}'$ has $(n-r)$ rows and thus is not invertible. However, such $\mathbf{W}'$ needs to be inverted in order to compute a full private key.

The first idea is to build a new invertible matrix $\mathbf{W_r}$ by appending to $\mathbf{W}'$ a $(r \times n)$-matrix $\mathbf{V} = [v_{i,j}]$ such that $v_{i,j}^q = v_{i,j+1}$. The secret transformation is reconstructed by computing $\mathbf{G_i}' = \mathbf{W_r}^{-1}\mathbf{G_i}\mathbf{W_r}^{-t}$. As the matrix $\mathbf{W_r}^{-1}$ has non-zero coefficients in its r last rows, so is $\mathbf{G}_i'$. Since the MinRank was done over $(n-r \times n-r)$-matrices, when we finally compute $\sum_{i=0}^{n} u_{i,0}\mathbf{G_{i+1}}'$, monomials in the last variables $(x_{n-r+1},\dots,x_n)$ are mixed with the other monomials, which eventually leads to polynomials that are not in HFE-shape (and then hard to invert). To circumvent this issue, we no longer append a random matrix to $\mathbf{W}'$, we construct an invertible matrix $\mathbf{W_z}$ by appending vertically to $\mathbf{W}'$ the matrix

$$\mathbf{Z} = \begin{pmatrix} 0 \dots\dots\dots\dots 0\ 1 \\ \vdots \qquad\qquad\quad \vdots \quad \ddots \\ 0 \dots\dots\dots\dots 0 \qquad 1 \end{pmatrix}.$$

We ensure the property that $\mathbf{W_z}$ is invertible. The variables $(x_{n-r+1},\dots,x_n)$ do not appear when we build $\mathbf{G_i}' = \mathbf{W_z}^{-1}\mathbf{G_i}\mathbf{W_z}^{-t}$, and the rank property is preserved. The only difference is that the relation $w_{i,j}^q = w_{i,j+1}$ only holds for all $i, 0 \leqslant i < n-r$. The consequence is that $\mathbf{S}' = \mathbf{W_z}\mathbf{M}_{N,d}^{-1}$ has coefficients in the big field $\mathbb{F}_{q^d}$. Still, $\mathbf{S}'$ can be inverted and a mapping $\mathscr{F}^*$ with HFE-shape can be recovered. Experimental results are given in Sect. 6.

6 Experimental results

We present some experimental results for our attacks implemented in MAGMA [7] (V2.16-10). All the timings have been obtained on a 2.93 GHz Intel® Xeon® CPU. The MinRank's have been solved using the Kipnis-Shamir modeling.

The degree of regularity experimentally observed is noted d_{reg}. The theoretical degree of regularity is denoted by $d_{\text{reg}}^{\text{theo}}$. We applied our attack to the real-scale parameters proposed in [10] (multi-HFE with embedding). They are not secure since they are practically broken (9 days for the most conservative, i.e. 256 bits claimed security). One may get even better results using the minors modeling of MinRank and the F_5 implementation available in the FGb software [18]. The following results are obtained on the same computer.

q	N	d	D	security	$d_{\text{reg}}^{\text{theo}}$	time MAGMA	mem MAGMA	time FGb	d_{reg}
31	2	15	2	150 bits	3	2 min 27 s	434 MB	21.1 s	3
31	3	10	2	150 bits	4	1 h 38 min	1500 MB	24 min 56 s	3
31	3	15	2	192 bits	4	2 days 1 h	12 GB		3
31	3	18	2	256 bits	4	9 days 16 h	33 GB		3

We also compare the different steps of our attack to the minus and the embedding variants for multi-HFE with parameters $q = 31, N = 3, d = 8, D = 2$ (≈ 120 bits security). The minus modifier does not change the time of the MinRank attack but recovering **W** will be slower. In practice, multi-HFE with the embedding takes more time to break but the degree of regularity is the same.

	MR time	MR d_{reg}	Finding **U**	Finding **W**
No variant (ref. time)	23.3 s	3	0.01 s	7.29 s
Minus ($s = 1$)	23.2 s	3	0.01 s	16.71 s
Minus ($s = 2$)	23.4 s	3	0.01 s	35.24 s
Minus ($s = 3$)	Not possible			
Embedding ($r = 1$)	788 s	3	0.01 s	6.14 s
Embedding ($r = 2$)	2811 s	3	0.01 s	5.25 s
Embedding ($r = 3$)	401 s	3	0.01 s	4.44 s

7 Conclusion

Multi-HFE over an odd-characteristic field seems to fix the weaknesses of HFE. The embedding modifier was also proposed to better hide the big field structure in the public key. These properties turn out to be weaknesses. Not only does our attack allow to do a complete key recovery in polynomial time, it is also more efficient on multi-HFE than on original HFE. On multi-HFE, key recovery on real-size parameters becomes practical. We broke parameter sets from [11] up to claimed 256 bits security. It is therefore insecure to use multi-HFE. Increasing the number N of secret variables/equations or their degree D may lead to a set of parameters out of reach of our attack but then, the rightful decryption would be very slow or infeasible. With respect to our attacks, among the studied constructions, only the minus variants of HFE/multi-HFE are secure if the removed equations is bigger than $(N-1)$. Note that vinegar variants of HFE are not concerned.

Acknowledgments. We would like to thank C. Wolf for his helpful comments which helped to improve the paper. The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II. The authors were also supported in part by the french ANR under the Computer Algebra and Cryptography (CAC) project ANR-09- JCJCJ-0064-01.

References

1. Adams, W.W., Loustaunau, P.: An Introduction to Gröbner Bases, Graduate Studies in Mahematics, vol. 3. AMS (1994)
2. Bardet, M., Faugère, J.C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proc. International Conference on Polynomial System Solving (ICPSS). pp. 71–75 (2004)
3. Bardet, M., Faugère, J.C., Salvy, B., Yang, B.Y.: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry (2005)
4. Bettale, L., Faugère, J.C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology pp. 177–197 (2009)
5. Billet, O., Patarin, J., Seurin, Y.: Analysis of Intermediate Field Systems. In: SCC 2008 (2008)
6. Bogdanov, A., Eisenbarth, T., Rupp, A., Wolf, C.: Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves? In: Cryptographic Hardware and Embedded Systems – CHES '08. pp. 45–61. LNCS (2008)
7. Bosma, W., Cannon, J.J., Playoust, C.: The Magma algebra system I: The user language. Journal of Symbolic Computation 24(3-4), 235–265 (1997)
8. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. thesis, University of Innsbruck (1965)
9. Buss, W., Frandsen, G., Shallit, J.: The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences (1999)
10. Chen, A.I.T., Chen, M.S., Chen, T.R., Cheng, C.M., Ding, J., Kuo, E.L.H., Lee, F.Y.S., Yang, B.Y.: SSE implementation of multivariate PKCs on modern x86 CPUs. In: Cryptographic Hardware and Embedded Systems – CHES 2009. LNCS, vol. 5747, pp. 33–48. Springer (2009)
11. Chen, C.H.O., Chen, M.S., Ding, J., Werner, F., Yang, B.Y.: Odd-char multivariate Hidden Field Equations. Cryptology ePrint Archive (2008), http://eprint.iacr.org/2008/543
12. Courtois, N.T.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in Cryptology – ASIACRYPT 2001. LNCS, vol. 2248, pp. 402–421. Springer (2001)
13. Cox, D.A., Little, J.B., O'Shea, D.: Ideals, Varieties and Algorithms. Springer (2005)
14. Ding, J., Schmidt, D., Werner, F.: Algebraic attack on HFE revisited. In: Information Security. LNCS, vol. 5222, pp. 215–227. Springer (2008)
15. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139, 61–88 (June 1999)
16. Faugère, J.C.: 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 ISSAC. pp. 75–83. ACM Press (2002)
17. Faugère, J.C.: Algebraic cryptanalysis of HFE using Gröbner bases. Reasearch report RR-4738, INRIA (2003), http://hal.inria.fr/inria-00071849/PDF/RR-4738.pdf
18. Faugère, J.C.: FGb: A Library for Computing Gröbner Bases. In: Fukuda, K., Hoeven, J., Joswig, M., Takayama, N. (eds.) Mathematical Software – ICMS 2010. Lecture Notes in Computer Science, vol. 6327, pp. 84–87. Springer Berlin / Heidelberg, Berlin, Heidelberg (September 2010), http://www-salsa.lip6.fr/ jcf/Papers/ICMS.pdf
19. Faugère, J.C., Joux, A.: Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In: Advances in Cryptology – CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer (2003)

20. Faugère, J.C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Advances in Cryptology – CRYPTO 2008. LNCS, vol. 5157, pp. 280–296. Springer (2008)
21. Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation 2010 – ISSAC 2010 (2010)
22. Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J.: Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity. Journal of Symbolic Computation pp. 1–39 (2010)
23. Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman (1979)
24. Granboulan, L., Joux, A., Stern, J.: Inverting HFE is quasipolynomial. In: Advances in Cryptology – CRYPTO 2006. LNCS, vol. 4117, pp. 345–356. Springer (2006)
25. Jiang, X., Ding, J., Hu, L.: Kipnis-Shamir attack on HFE revisited. In: Information Security and Cryptology. LNCS, vol. 4990, pp. 399–411. Springer (2007)
26. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Advances in Cryptology – CRYPTO '99. LNCS, vol. 1666, pp. 19–30. Springer (1999)
27. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Advances in Cryptology – EUROCRYPT '88. LNCS, vol. 330, pp. 419–453. Springer (1988)
28. Patarin, J.: Cryptoanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88. In: Advances in Cryptology – CRYPTO '95. pp. 248–261 (1995)
29. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In: Advances in Cryptology – EUROCRYPT '96. LNCS, vol. 1070, pp. 33–48. Springer (1996)
30. Wolf, C., Preneel, B.: Equivalent keys in HFE, C^*, and variations. In: Progress in Cryptology – Mycrypt 2005. LNCS, vol. 3715, pp. 33–49. Springer (2005)
31. Wolf, C., Preneel, B.: Large superfluous keys in multivariate quadratic asymmetric systems. In: Public Key Cryptography – PKC 2005. LNCS, vol. 3386, pp. 275–287. Springer (2005)