Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic

Luk Bettale, Jean-Charles Faugère, Ludovic Perret

Designs, Codes and Cryptography manuscript No.
(will be inserted by the editor)

Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic

Luk Bettale · **Jean-Charles Faugère** · **Ludovic Perret**

Received: date/ Accepted: Jan 23, 2012

Abstract We investigate in this paper the security of HFE and Multi-HFE schemes as well as their minus and embedding variants. Multi-HFE is a generalization of the well-known HFE schemes. The idea is to use a multivariate quadratic system – instead of a univariate polynomial in HFE – over an extension field as a private key. According to the authors, this should make the classical direct algebraic (message-recovery) attack proposed by Faugère and Joux on HFE no longer efficient against Multi-HFE. We consider here the hardness of the key-recovery in Multi-HFE and its variants, but also in HFE (both for odd and even characteristic). We first improve and generalize the basic key recovery proposed by Kipnis and Shamir on HFE. To do so, we express this attack as matrix/vector operations. In one hand, this permits to improve the basic Kipnis-Shamir (KS) attack on HFE. On the other hand, this allows to generalize the attack on Multi-HFE. Due to its structure, we prove that a Multi-HFE scheme has much more equivalent keys than a basic HFE. This induces a structural weakness which can be exploited to adapt the KS attack against classical modifiers of multivariate schemes such as minus and embedding. Along the way, we discovered that the KS attack as initially described cannot be applied against HFE in characteristic 2. We have then strongly revised KS in characteristic 2 to make it work. In all cases, the cost of our attacks is related to the complexity of solving MinRank. Thanks to recent complexity results on this problem, we prove that our attack is polynomial in the degree of the extension field for all possible practical settings used in HFE and Multi-HFE. This makes then Multi-HFE less secure than basic HFE for equally-sized keys. As a proof of concept, we have been able to practically break the most conservative proposed parameters of multi-HFE in few days (256 bits security broken in 9 days).

Keywords Hidden Field Equations, MinRank, Gröbner bases

1 Introduction

The problem of finding a low rank linear combination of matrices is a basic linear algebra problem [12] known as MinRank in cryptography [16]. This problem is NP-hard [12] and was used to design a zero-knowledge authentication scheme [16]. More generally, it appears that MinRank is underlying the security of several cryptographic schemes [35, 15]. A well known example is the key recovery attack of the multivariate scheme HFE [41] (Hidden Field Equations) proposed by Kipnis and Shamir [35] who showed that the security of HFE can be reduced to the difficulty of MinRank. Their technique is usually called Kipnis-Shamir's attack, or KS attack. They also proposed a general algorithm to solve MinRank. The idea is to map an instance of MinRank to an algebraic system. They then proposed an "ad-hoc" technique to solve such polynomial systems.

Later, Faugère, Levy-dit-Vehel and Perret [27] improve Kipnis-Shamir's attack by using Gröbner bases [9, 10, 11] techniques. In particular, they noticed that the system arising in Kipnis-Shamir's attack has a very specific structure: it is "*bilinear*". This means that each equation of the system is the product of linear forms with distinct

Luk Bettale was partially supported by DGA/MRIS (french secretary of defense).

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
E-mail: l.bettale@oberthur.com, jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr

variables. Soon after, Faugère, Safey El Din and Spaenlehauer [29] presented a detailed study of the complexity of solving bilinear systems with Gröbner bases. In particular, [29] proved that (generic or random) bilinear systems are much easier to solve than (generic) algebraic systems of the same size.

However, it seems reasonable to believe that polynomial systems occurring in cryptographic applications (such as in MinRank) are likely not generic; motivating then a dedicated analysis for important cases. In [28], MinRank instances occurring in authentication schemes have been further studied. In this paper, we consider instances of MinRank occurring in the cryptanalysis of multivariate public-key schemes.

Multivariate Public-Key Cryptography (MPKC) is the set of asymmetric schemes using the NP-hardness of solving a quadratic system of multivariate algebraic equations [32]. Multivariate schemes are often considered as possible "low-cost" alternatives [39] to number theory based public key schemes. Their encryption/decryption procedures are very efficient and can be done in constrained environments [7, 13]. The main drawback is that the public key is rather large. Indeed, the one-way function is defined by a set of m quadratic polynomials $(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n)) \in \mathbb{K}[x_1,\ldots,x_n]^m$. Namely, the public operation is the application

$$\mathscr{G} : (v_1,\ldots,v_n) \in \mathbb{K}^n \mapsto (g_1(v_1,\ldots,v_n),\ldots,g_m(v_1,\ldots,v_n)) \in \mathbb{K}^m.$$

To introduce a trapdoor, we choose a transformation $\mathscr{F}$ given by a system of algebraic equations $(f_1,\ldots,f_m) \in \mathbb{K}[x_1,\ldots,x_n]^m$. Thanks to a well chosen structure, the system is easy to solve. Let $\mathrm{GL_n}(\mathbb{K})$ be the group of invertible linear transformations and let $\mathrm{Aff}_n(\mathbb{K}) \simeq \mathrm{GL_n}(\mathbb{K}) \times \mathbb{K}^n$ be the group of invertible affine transformations. This structure is hidden by two affine transformations $\mathscr{S} \in \mathrm{Aff}_n(\mathbb{K})$ and $\mathscr{T} \in \mathrm{Aff}_m(\mathbb{K})$ represented by matrices $\mathbf{S}$ and $\mathbf{T}$. The public key is then:

$$\begin{aligned} \mathscr{G} &= \mathscr{T} \circ \mathscr{F} \circ \mathscr{S} \\ (g_1,\ldots,g_m) &= (f_1((x_1,\ldots,x_n)\,\mathbf{S}),\ldots,f_m((x_1,\ldots,x_n)\,\mathbf{S}))\,\mathbf{T}. \end{aligned}$$

In such schemes, the transformations $\mathscr{S}$, $\mathscr{T}$ and (usually) $\mathscr{F}$ are kept secret and $\mathscr{G}$ is made public.

To encrypt a message $\underline{m} = (m_1,\ldots,m_n) \in \mathbb{K}^n$, we compute:

$$\underline{c} = (c_1,\ldots,c_m) = (g_1(m_1,\ldots,m_n),\ldots,g_m(m_1,\ldots,m_n)) \in \mathbb{K}^m.$$

To decrypt, the owner of the secret key inverts separately each component. As $\mathscr{S}$, $\mathscr{T}$ and $\mathscr{F}$ are easy to invert, this is done efficiently. The first multivariate scheme C* was introduced by Matsumoto and Imai [37] and broken by Patarin [40]. After that, several trapdoor functions were proposed in this framework [41, 36, 38, 44]. HFE probably remains the most famous one. In this paper we focus on the HFE and Multi-HFE structure introduced in [41, 6, 14].

In the original HFE [41], the secret inner system is the representation of a univariate polynomial over some extension of degree $n \in \mathbb{N}$ of a finite field $\mathbb{F}_q$. This polynomial is chosen to be easy to solve (low degree) and has a special structure that allows to have only quadratic polynomials in its (multivariate) small field representation. A practical message recovery attack [24, 26] and a theoretical key recovery [35] undermined the security of this scheme. To tackle these attacks, a generalization of HFE that uses a system of N equations in N variables (instead of one univariate polynomial) in an extension field of degree d has been proposed in [6] and in [13]. In this paper, we call this construction Multi-HFE. The basic HFE scheme is then an instantiation of Multi-HFE with $N = 1, d = n$.

1.1 Main results

First, we propose an improved key recovery attack against HFE in odd-characteristic. To do so, we have improved and adapted the "classical" Kipnis-Shamir (KS) attack [35]. The KS attack reduces to a MinRank over $\mathbb{F}_{q^n}$ related to the public key. In contrast to the KS attack, we show that the MinRank can be expressed in the small field and directly on the quadratic forms of the public key $(g_1,\ldots,g_n) \in \mathbb{F}_q[x_1,\ldots,x_n]^n$. This allows to considerably speed up the solving step (for instance we have a speedup factor of 424 for $q = 31$ and $n = 19$) and also simplifies the KS attack. Due to its simpler description, we are able to generalize our attack to Multi-HFE ($N > 1$) in odd-characteristic. These results were first published in [5] and concern only odd-characteristic fields. In characteristic 2, there is no symmetric quadratic form representing a quadratic polynomial, and contrary to what was stated in [35], the KS attack does not work as initially described (more specifically the second part of the attack given in [35]). Using the specificity of the problem in characteristic 2 and the possibility to add the field equations, we give two methods for adapting our attack in characteristic 2 depending on the parity of the target rank of the MinRank. Note that our adaptation applies to both for HFE and Multi-HFE.

The MinRank problems which occur here are very specific. First, a certain degree of freedom is left for its solving. This is related to a large amount of equivalent keys in HFE/Multi-HFE. We isolated two kind of transformations allowing to build equivalent keys. These transformations generalize those given in [46, 47] for HFE. We show that an equivalent key has a canonical representation in terms of these transformations. As a direct consequence, we give a lower bound on the number of equivalent keys for Multi-HFE, more precise than the one given in [5]. Second, the MinRank considered are greatly over-determined. Thanks to recent results on MinRank [27, 28], bilinear systems [29] and a new expression of the Hilbert function using orthogonal polynomials, we provide a precise complexity analysis of our attack. For all proposed parameter sets, we prove that the attack is polynomial in d, the degree of the extension and linear in $\log(q)$, just as we conjectured in [5].

Another consequence of equivalent keys is the possibility to attack two variants of Multi-HFE, namely Multi-HFE$^-$ and Multi-HFE with embedding. In Multi-HFE$^-$, several polynomials are removed from the public keys. We show that only $(n-N)$ matrices are needed to solve the MinRank problem instead of n. These N degrees of freedom in the MinRank problem allow to perform our key recovery with no additional cost as the rank property still holds as long as the number of removed equations does not exceed N. For the embedding variant, the public polynomials have less variables leading to matrices with fewer rows and columns. However, a low rank linear combination of the quadratic forms can still be found. In this case, the matrix $\mathbf{S}$ (corresponding to the change of variable) recovered is rectangular. In order to make it invertible, we need to extend this matrix in a special way to keep the shape of $\mathscr{F}$ unchanged.

All in all, for the same size of keys, the Multi-HFE family seems to be less secure than the original HFE ($N=1$). As a proof of concept, we provide a practical key recovery on the most conservative parameters (256-bit security) proposed in [14] in less than 10 days.

1.2 Organization of the Paper

The paper is organized as follows. After this introduction, we present in Sect. 2 the necessary material regarding the MinRank problem and the algorithmic tools to solve it. We also review previous known attacks against HFE, and more particularly the KS attack on which ours is based. Section 3 is devoted to the presentation of our key recovery attack on both HFE and Multi-HFE. Equivalent keys are an important feature for our attack. They are discussed in Sect. 4 and the consequences are presented in Sect. 5. We use the degrees of freedom induced by equivalent keys to enhance the solving step by fixing some variables. After that, we unroll our attack on an example in Sect. 6. In this section, we also describe how to adapt our attack in characteristic 2. The complexity analysis of our attack is given in Sect. 7, and in Sect. 8 we devise how to extend our attack for the minus and the embedding variants of HFE/Multi-HFE. Finally, as a conclusion we show in Sect. 9 that Multi-HFE is less secure than HFE.

2 Preliminaries

Let $\mathbb{K}$ be a field. Throughout this paper, we use the following conventions: an underlined letter denotes a vector, e.g. $\underline{v}=(v_1,\ldots,v_n)\in\mathbb{K}^n$. A capital bold font letter denotes a matrix, e.g. $\mathbf{M}\in\mathscr{M}_{n\times n}(\mathbb{K})$ where $\mathscr{M}_{n\times n}(\mathbb{K})$ denotes the set of $n\times n$ matrices whose entries lie in $\mathbb{K}$. We also write $\mathbf{M}=[m_{i,j}]$ to denote that the (i,j)-th coefficient of the matrix $\mathbf{M}$ is $m_{i,j}\in\mathbb{K}$ for $0\leqslant i,j<n$. We will also indifferently use $\ker(\mathbf{M})$ to denote the left kernel of $\mathbf{M}$ or (more often) a matrix whose rows form a basis of its left kernel. A calligraphic capital letter denotes a general mapping, e.g. $\mathscr{F}$. The set of invertible matrices of $\mathscr{M}_{n\times n}(\mathbb{K})$ is denoted by $\mathrm{GL_n}(\mathbb{K})$. The group of affine invertible transformations is denoted by $\mathrm{Aff}_n(\mathbb{K})\simeq\mathrm{GL_n}(\mathbb{K})\times\mathbb{K}^n$.

2.1 Multi-HFE

The parameters considered are $(q,N,d,D)\in\mathbb{N}^4$. Here, q 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. In the rest of the paper, we use capital letters for elements relative to the extension $\mathbb{F}_{q^d}$ (a.k.a. "big field" in this paper), 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 $\mathbb{F}_q$ (a.k.a. "small field"), e.g. $v_i \in \mathbb{F}_q,\ f_i \in \mathbb{F}_q[x_1,\ldots,x_n]$. To build the trapdoor function $\mathscr{F}$, we use the following transformation over the big field

$$\mathscr{F}^* : (V_1,\ldots,V_N) \in (\mathbb{F}_{q^d})^N \mapsto (F_1(V_1,\ldots,V_N),\ldots,F_N(V_1,\ldots,V_N)) \in (\mathbb{F}_{q^d})^N$$

with $F_k \in \mathbb{F}_{q^d}[X_1,\ldots,X_N], \forall k, 1 \leqslant k \leqslant N$, and $\deg(F_i) \leqslant D$. In addition, the polynomials $F_1,\ldots,F_N$ are constructed in a specific way. For all $k, 1 \leqslant k \leqslant N$:

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

where $A_{\substack{k,i,u,\\ j,v}}, B_{k,i,u}, C_k \in \mathbb{F}_{q^d}, \forall i,j, 1 \leqslant i,j \leqslant N, \forall u,v, 0 \leqslant u,v < d$. From now on, we say that such systems have (multi-)HFE-shape. For convenience, we denote $n = N\,d$. Let φ_N be a morphism from $(\mathbb{F}_{q^d})^N$ to $\mathbb{F}_q^n$. The transformation $\mathscr{F}$ uses the small field representation of the secret polynomials, $\mathscr{F} = \varphi_N \circ \mathscr{F}^* \circ \varphi_N^{-1}$ with

$$\mathscr{F} : (v_1,\ldots,v_n) \in \mathbb{F}_q^n \mapsto (h_1(v_1,\ldots,v_n),\ldots,h_n(v_1,\ldots,v_n)) \in \mathbb{F}_q^n.$$

Due to the HFE-shape, each polynomial h_i, for $i, 1 \leqslant i \leqslant n$ has total degree 2.

The original HFE scheme [41] is mostly used over $\mathbb{F}_2$ and always 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 [20] (for projected HFE) is an odd characteristic univariate HFE that uses the embedding modifier (see Sect. 8.2). The scheme IFS [6] (for Intermediate Field System) is a multi-HFE in characteristic 2 and THFE [14] 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. In Table 1, we provide sample of parameters from the literature.

Table 1 Parameters of various Multi-HFE instances found in several papers.

	q	N	d	D	security
HFE [41]	2	1	128	513	128
PHFE [20]	7	1	67	56	201
IFS [6]	2	8	16	2	128
THFE [14]	31	3	10	2	150

We briefly review known attacks against HFE/multi-HFE.

2.2 Direct Algebraic Attack

Let $(c_1,\ldots,c_n) \in \mathbb{F}_q^n$ be a ciphertext. A message-recovery attack in a multivariate scheme reduces to solving a system of quadratic equations, i.e. $\{g_1 - c_1 = 0,\ldots,g_n - c_n = 0\}$, where the g_i's are the public polynomials. A classical way to solve algebraic systems is to compute a Gröbner basis [9, 10, 11, 1, 17]. The historical method for computing such bases has been proposed by Buchberger in his PhD thesis [9]. The algorithms F_4 [22] and F_5 [23] 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 can be viewed as the maximum degree of the polynomials appearing during the computation (see [2, 3]).

It appeared [24, 26] 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 [26]). This makes the attack sub-exponential in the number of variables. Further analysis [33] 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 [20] to use a field with a bigger characteristic. During the Gröbner basis computation, field equations only intervene in degree at least q. Note that the hybrid approach described in [4] has been especially designed to solve such systems (for "intermediate" fields). As an example, 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 impractical.

More specifically, a HFE system with $q > n$ is very hard to solve with a direct approach such as in [26] (for n sufficiently big). This intuition has been recently confirmed in [21] where the authors extend the analysis of [33] for all fields. After this, [19] produces an explicit bound on the degree of regularity which is

$$\frac{(q-1)\lceil \log(D) \rceil}{2} + 2.$$

We remark that this bound is linear in q. This makes the cost of a direct Gröbner basis computation exponential in q and then useless for a big enough field. For example, HFE with parameters $q = 23$, $D = 1058$ and $n = 120$, the (upper) bound on the degree of regularity according to [19] is 35. The corresponding cost for mounting a direct message-recovery attack is then 2^{242} operations. For a comparison, the key-recovery attack presented in this paper will need 2^{28} operations for the same parameters.

For multi-HFE, there are less results. In characteristic 2, multi-HFE can still be attacked similarly to HFE as pointed in [6]. This confirms that the algebraic attack is somehow "optimal" over $\mathbb{F}_2$. However, as for basic HFE, the direct algebraic attack does not affect instantiations of multi-HFE with bigger odd characteristic.

2.3 Original Kipnis-Shamir Attack

We now describe the key recovery attack proposed in [35] against the original HFE scheme ($N = 1, n = d$). The starting idea is to remark that the 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 $G, S, T \in \mathbb{F}_{q^n}[X]$ respectively. The public key relation then becomes

$$G = \mathscr{G}^*(X) = \mathscr{T}^*(\mathscr{F}^*(\mathscr{S}^*(X))).$$

Kipnis and Shamir [35] 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 [35] also showed that the univariate polynomials can be written as "*non-standard quadratic forms*". 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 $\mathbf{G} = [g_{i,j}] \in \mathscr{M}_{n \times n}(\mathbb{F}_{q^n})$. Note that this representation does not work in characteristic 2. In this section and in Sect. 3, we assume then that q is odd. The characteristic 2 case is addressed in Sect. 6.3. Similarly, we define $\mathbf{F} = [f_{i,j}] \in \mathscr{M}_{n \times n}(\mathbb{F}_{q^n})$ as the symmetric matrix representation of the secret univariate polynomial.

The Kipnis-Shamir attack is based on the remark that the rank of $\mathbf{F}$ is bounded, namely Rank $(\mathbf{F}) \leqslant \log_q(D)$. Indeed, the degree of the secret polynomial is smaller than D and the entries $f_{i,j}$ in $\mathbf{F}$ are non-zero only if $i, j \leqslant \log_q(D)$. In addition, we write $\mathscr{T}^{*-1}(X) = \sum_{k=0}^{n-1} t_k X^{q^k}$ and $\mathscr{S}^*(X) = \sum_{k=0}^{n-1} s_k X^{q^k}$.

The equation $\mathscr{G}^*(X) = \mathscr{T}^*(\mathscr{F}^*(\mathscr{S}^*(X)))$ implies the so-called "*Fundamental Equation*" (see [35] 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 $\widetilde{\mathbf{W}} = [\widetilde{w}_{i,j}] \in \mathscr{M}_{n \times n}(\mathbb{F}_{q^n})$ is a specified invertible matrix such that $\widetilde{w}_{i,j} = s_{(j-i) \bmod n}^{q^i}$, for all $i, j, 0 \leqslant i, j < n$. Finally, for a given $k, 0 \leqslant k < n$, $\mathbf{G}^{*k}$ is the matrix whose (i,j)-th entry is $g_{(i-k) \bmod n, (j-k) \bmod n}^{q^k}$, for all $i, j, 0 \leqslant i, j < n$. 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.

Once the t_k's of (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 $\ker(\mathbf{G}')\widetilde{\mathbf{W}} = \ker(\mathbf{F})$. Let $\ell = \lceil \log_q(D) \rceil$, we recall that only the upper left $\ell \times \ell$ submatrix of $\mathbf{F}$ has non-zero coefficients. Thus, any $(n - \ell) \times n$ matrix $\mathbf{K}$ whose first ℓ columns are 0 ensures $\mathbf{KF} = \mathbf{0}$. Furthermore, if $\text{Rank}(\mathbf{F}) = \ell$ and the rows of $\mathbf{K}$ are chosen linearly independent, then their rows form a basis of $\ker(\mathbf{F})$.

In any case, this is enough to ensure that the ℓ first columns of $\ker(\mathbf{G}')\,\widetilde{\mathbf{W}}$ are zero. This gives rise to a linear system over $\mathbb{F}_{q^n}$ of $\ell\,(n-\ell)$ equations in the n^2 coefficients of $\widetilde{\mathbf{W}}$. In addition, $\widetilde{\mathbf{W}}$ has the following shape:

$$\widetilde{\mathbf{W}} = \begin{pmatrix} \widetilde{w}_{0,0} & \widetilde{w}_{0,1} & \cdots & \cdots & \widetilde{w}_{0,n-2} & \widetilde{w}_{0,n-1} \\ \widetilde{w}_{0,n-1}^{q} & \widetilde{w}_{0,0}^{q} & \widetilde{w}_{0,1}^{q} & \cdots & \cdots & \widetilde{w}_{0,n-2}^{q} \\ & \ddots & \ddots & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ \cdots & \cdots & \widetilde{w}_{0,n-2}^{q^{n-2}} & \widetilde{w}_{0,n-1}^{q^{n-2}} & \widetilde{w}_{0,0}^{q^{n-2}} & \widetilde{w}_{0,1}^{q^{n-2}} \\ \widetilde{w}_{0,1}^{q^{n-1}} & \cdots & \cdots & \widetilde{w}_{0,n-2}^{q^{n-1}} & \widetilde{w}_{0,n-1}^{q^{n-1}} & \widetilde{w}_{0,0}^{q^{n-1}} \end{pmatrix}.$$

This is due to the fact that $\widetilde{w}_{i+1,j+1} = s^{q^{i+1}}_{(j+1)-(i+1)} = \left(s^{q^i}_{(j-i)}\right)^q = \widetilde{w}^q_{i,j}$. Thus, Kipnis and Shamir proposed to reinterpret the equations over $\mathbb{F}_q$. This gives $n\,\ell\,(n-\ell)$ equations in only n^2 variables over $\mathbb{F}_q$. Solving this overdetermined system completes the key recovery. The main (and more difficult) part of the attack is to solve the so-called MinRank problem. In the next section, we present the problem as well as the tools to solve it.

2.4 The MinRank Problem

The (square) MinRank problem over a finite field $\mathbb{K}$ is defined as follows:
MinRank (MR)
Input: $n,r,k \in \mathbb{N}$ and $\mathbf{M_0},\mathbf{M_1},\ldots,\mathbf{M_k} \in \mathscr{M}_{n\times n}(\mathbb{K})$.
Question: Find – if any – a k-tuple $(\lambda_1,\ldots,\lambda_k) \in \mathbb{K}^k$ such that:

$$\operatorname{Rank}\left(\sum_{i=1}^{k}\lambda_i\,\mathbf{M_i} - \mathbf{M_0}\right) \leqslant r.$$

We review below known algebraic techniques to solve this problem.

2.4.1 Kipnis-Shamir Modeling

Kipnis and Shamir [35] proposed to formulate MinRank as a multivariate polynomial system of equations. With the previous notations, solving MinRank over a finite field $\mathbb{K}$ is equivalent to solving the algebraic system of $n\,(n-r)$ equations in $r\,(n-r)+k$ variables given by the entries of the matrix

$$\begin{pmatrix} 1 & & & x_{1,1} & \cdots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{n-r,1} & \cdots & x_{n-r,r} \end{pmatrix} \cdot \left(\sum_{i=1}^{k}\lambda_i\,\mathbf{M_i} - \mathbf{M_0}\right).$$

Solving this system is equivalent to find a left kernel (in echelon form) of $\left(\sum_{i=1}^{k}\lambda_i\,\mathbf{M_i} - \mathbf{M_0}\right)$. This left kernel can be written in such a systematic form with high probability over a finite field. Initially, relinearization [35] has been used to solve this algebraic system. The authors of [27] proposed instead to use Gröbner bases tools to solve this system. In addition, [27] noticed that the system has a specific structure: it is formed by bilinear equations [29].

2.4.2 Minors Modeling

Alternatively, MinRank is equivalent to finding a vector $(\lambda_1,\ldots,\lambda_k) \in \mathbb{K}^k$ vanishing on all the minors of size $r+1$ of the matrix $\left(\sum_{i=1}^{k}\lambda_i\,\mathbf{M_i} - \mathbf{M_0}\right)$ are zero. We have then to solve a multivariate polynomial system of $\binom{n}{r+1}^2$ equations in k variables as pointed in [27, 28]. The system has more equations and less variables than the Kipnis-Shamir modeling but the degree of the equations is r. However, it seems that this approach is more efficient [28] (at least for MinRank instances used in the authentication scheme [16]). In addition, precise complexity bounds can be derived for this modeling [28].

2.4.3 Complexity.

We recall the complexity of the F_5 algorithm as given in [2, 3].

Theorem 1 *The complexity of computing a Gröbner basis of a zero-dimensional (i.e. with a finite number of solutions in the algebraic closure of the coefficient field) polynomial system of m equations in n variables with F_5 is*

$$\mathscr{O}\left(\binom{n+d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^{\omega}\right),$$

where d_{reg} is the degree of regularity of the ideal and $2 \leqslant \omega \leqslant 3$ the linear algebra constant.

Informally, d_{reg} is the maximum degree reached during a Gröbner basis computation. For random instances of square $(m = n)$ quadratic systems, it holds that $d_{\mathrm{reg}} = n+1$ (see [2]). It has to be noticed that if the degree of regularity does not depend on the number of variables, the complexity then becomes polynomial in n.

We consider now MinRank systems obtained by the minors modeling. Corollary 3 of [28] gives a bound on the degree of regularity of these particular systems.

Proposition 1 (Faugère, Safey El Din, Spaenlehauer [28]) *Let (n,r,k) be the parameters of a MinRank instance. Let $\mathbf{A}(t) = [a_{i,j}(t)]$ 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 MinRank polynomial systems 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*

$$(1-t)^{(n-r)^2-k}\ \frac{\det \mathbf{A}(t)}{t^{\binom{r}{2}}}.$$

As explained in [28], the proof is valid under the assumption that a variant of the Fröberg conjecture [31] is true. More recently [30], the same result was proved when $k \geq (n-r)^2$ without using any variant of Fröberg's conjecture. However, in the overdetermined case (that is to say when $k < (n-r)^2$) the conjecture is still needed. The Fröberg conjecture states that some property (the rank of some linear map is maximal) holds on a Zariski open subset $\mathscr{O}$ when the characteristic of $\mathbb{K}$ is 0. Hence, we can find a polynomial $h(\mathbf{a})$ in $\mathbb{Z}[\mathbf{a}]$ which does not depend on the field $\mathbb{K}$ such that $h(\mathbf{a}) \neq 0 \Rightarrow \mathbf{a} \in \mathscr{O}$. When $\mathbb{K}$ is a finite field the notion of Zariski open set is meaningless but the following lemma can be used:

Lemma 1 (Schwartz, Zippel, DeMillo, Lipton [18, 48, 42]) *Let $\mathbb{K}$ be a field and $P \in \mathbb{K}[x_1,\ldots,x_n]$ be a non-zero polynomial. Select $r_1,\ldots,r_n$ uniformly at random from a finite subset $\mathscr{X}$ of $\mathbb{K}$. Then, the probability that $P(r_1,\ldots,r_n) = 0$ is less than $\deg(P)/|\mathscr{X}|$.*

The lemma states that if we choose uniformly at random in $\mathbb{F}_q$ the coefficient of the polynomials occuring in the Fröberg conjecture then the probability that $h(\mathbf{a}) = 0$ is upper bounded by $\deg(h)/q$ and therefore tends to 0 when q goes to infinity. This means that if the Fröberg conjecture is true in characteristic 0 then it is also true over $\mathbb{F}_q$ with a good probability when q is big enough. In addition, the Fröberg conjecture (even over $\mathbb{F}_2$) is well supported by computer experiments.

Note that the bound given by Proposition 1 is also an upper bound for the degree of regularity of the Kipnis-Shamir modeling [28]. In Sect. 7, we will see that Proposition 1 is useful to bound the complexity of MinRank problems coming from HFE/multi-HFE.

3 Improvement and Generalization of the MinRank Attack

To generalize the MinRank attack proposed by Kipnis and Shamir [35], it is convenient to interpret it as matrix/vector operations. In what follows, 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, for a vector $\underline{v} = (v_1,\ldots,v_m) \in \mathbb{K}^m$, we have $\mathrm{Frob_k}(\underline{v}) = (v_1^{q^k},\ldots,v_m^{q^k}) \in \mathbb{K}^m$. For a matrix $\mathbf{A} = [a_{i,j}] \in \mathscr{M}_{n\times n}(\mathbb{K})$, we have $\mathrm{Frob_k}(\mathbf{A}) = [a_{i,j}^{q^k}] \in \mathscr{M}_{n\times n}(\mathbb{K})$. In this section, we will suppose that the characteristic of the field $\mathbb{F}_q$ is different than two. This particular case is addressed in Sect. 6.3.

3.1 Improving the Univariate Case

To express the KS attack as matrix/vector operation, we introduce the following change of basis matrix.

Proposition 2 *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 $\mathbf{M}_n \in \mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$ be the matrix whose columns are the Frobenius powers of the basis elements, i.e.:*

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

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

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

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

$$(v_1,\ldots,v_n) \mapsto \big((v_1,\ldots,v_n)\,\mathbf{M}_n\big)[1],$$

$\big((v_1,\ldots,v_n)\,\mathbf{M}_n\big)[1]$ *denoting the first component of the vector $(v_1,\ldots,v_n)\,\mathbf{M}_n$. More generally, we have*

$$(v_1,\ldots,v_n)\,\mathbf{M}_n = (V, V^q, \ldots, V^{q^{n-1}}).$$

Proof Let $(v_1,\ldots,v_n) \in \mathbb{F}_q^n$ be the decomposition of $V \in \mathbb{F}_{q^n}$ as a vector in $\mathbb{F}_q^n$. That is, $V = \sum_{i=1}^n v_i\theta_i \in \mathbb{F}_{q^n}$. By construction:

$$\begin{aligned}(v_1,\ldots,v_n)\,\mathbf{M}_n &= \left(\sum_{i=1}^n v_i\theta_i^{q^0},\ldots,\sum_{i=1}^n v_i\theta_i^{q^{n-1}}\right) = \left(\left(\sum_{i=1}^n v_i\theta_i\right)^{q^0},\ldots,\left(\sum_{i=1}^n v_i\theta_i\right)^{q^{n-1}}\right)\\ &= \left(V^{q^0},\ldots,V^{q^{n-1}}\right).\end{aligned}$$

As a consequence:

$$\varphi_1^{-1}(v_1,\ldots,v_n) = \big((v_1,\ldots,v_n)\,\mathbf{M}_n\big)[1] = V.$$

$\mathbf{M}_n$ being invertible, we have for φ_1:

$$\begin{aligned}\left(V^{q^0},\ldots,V^{q^{n-1}}\right) &= (v_1,\ldots,v_n)\,\mathbf{M}_n\\ \left(V^{q^0},\ldots,V^{q^{n-1}}\right)\mathbf{M}_n^{-1} &= (v_1,\ldots,v_n) = \varphi_1(V).\end{aligned}$$

□

The matrix $\mathbf{M}_n$ allows to go back and forth from the big field $\mathbb{F}_{q^n}$ to the vector-space $\mathbb{F}_q^n$. It can be used to compute the univariate representation of the public key in a simpler way than in [35]. Namely, we replace interpolation by a matrix multiplication. For the sake of simplicity, we consider from now on only linear transformations and homogeneous polynomials. This is not a restriction since what follows can easily be adapted to the affine case (as already pointed in [35]).

Let $\mathbf{F}^{*k} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ be the matrix whose (i,j)-th entry is $f_{i-k,j-k}^{q^k}$ (indexes are modulo n). The matrix $\mathbf{F}^{*k}$ is in fact 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

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

The sums can be divided as follows:

$$
\begin{aligned}
F^{q^k} &= \sum_{i=k}^{n-1}\left(\sum_{j=k}^{n-1+k} f_{i-k,j-k}^{q^k} X^{q^i+q^j}\right) + \sum_{i=n-1+1}^{n-1+k}\left(\sum_{j=k}^{n-1+k} f_{i-k,j-k}^{q^k} X^{q^i+q^j}\right)\\
F^{q^k} &= \sum_{i=k}^{n-1}\left(\sum_{j=k}^{n-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j} + \sum_{j=n-1+1}^{n-1+k} f_{i-k,j-k}^{q^k} X^{q^i+q^j}\right)\\
&\quad + \sum_{i=n-1+1}^{n-1+k}\left(\sum_{j=k}^{n-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j} + \sum_{j=n-1+1}^{n-1+k} f_{i-k,j-k}^{q^k} X^{q^i+q^j}\right)\\
F^{q^k} &= \sum_{i=k}^{n-1}\left(\sum_{j=k}^{n-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j} + \sum_{j=0}^{k-1} f_{i-k,n+j-k}^{q^k} X^{q^i+q^{n+j}}\right)\\
&\quad + \sum_{i=0}^{k-1}\left(\sum_{j=k}^{n-1} f_{n+i-k,j-k}^{q^k} X^{q^{n+i}+q^j} + \sum_{j=0}^{k-1} f_{n+i-k,n+j-k}^{q^k} X^{q^{n+i}+q^{n+j}}\right).
\end{aligned}
$$

Remark that $X^{q^n} = X$. By reducing the indexes of $f_{i,j}$ modulo n, we get:

$$
\begin{aligned}
F^{q^k} &= \sum_{i=k}^{n-1}\left(\sum_{j=k}^{n-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j} + \sum_{j=0}^{k-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j}\right)\\
&\quad + \sum_{i=0}^{k-1}\left(\sum_{j=k}^{n-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j} + \sum_{j=0}^{k-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j}\right).
\end{aligned}
$$

Grouping the sums back together, we obtain

$$
F^{q^k} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{i-k,j-k}^{q^k} X^{q^i+q^j} \quad = \underline{X}\mathbf{F}^{*k}\underline{X}^t. \tag{2}
$$

Thanks to Proposition 2, we deduce a useful property on these matrices.

Lemma 2 *Let $\mathbf{M}_n \in \mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$ be the matrix defined in Proposition 2. We consider also the symmetric matrices $(\mathbf{H_1},\ldots,\mathbf{H_n}) \in (\mathscr{M}_{n\times n}(\mathbb{F}_q))^n$ associated to the secret quadratic polynomials in the small field $(h_1,\ldots,h_n) \in \left(\mathbb{F}_q[x_1,\ldots,x_n]\right)^n$, i.e. $h_i = \underline{x}\mathbf{H_i}\underline{x}^t$ for all i, $1 \leqslant i \leqslant n$. It holds that:*

$$
(\mathbf{H_1},\ldots,\mathbf{H_n}) = \left(\mathbf{M}_n\,\mathbf{F}^{*0}\,\mathbf{M}_n^t,\ldots,\mathbf{M}_n\mathbf{F}^{*n-1}\,\mathbf{M}_n^t\right)\mathbf{M}_n^{-1}.
$$

Proof By construction, for all $\underline{v} = (v_1,\ldots,v_n) \in \mathbb{F}_q^n$:

$$
\left(h_1(\underline{v}),\ldots,h_n(\underline{v})\right) = \varphi_1\left(F\left(\varphi_1^{-1}(\underline{v})\right)\right).
$$

Using the matrix definition of φ_1, we express this relation as follows:

$$
\left(h_1(\underline{v}),\ldots,h_n(\underline{v})\right) = \varphi_1\left(F(\underline{v}\mathbf{M}_n)\right) = \left(F^{q^0}(\underline{v}\mathbf{M}_n),\ldots,F^{q^{n-1}}(\underline{v}\mathbf{M}_n)\right)\mathbf{M}_n^{-1}.
$$

We recall that the matrix representation of F^{q^k} is $\mathbf{F}^{*k}$. Thus for all $\underline{v} \in \mathbb{F}_q^n$:

$$
\begin{aligned}
\left(\underline{v}\,\mathbf{H_1}\,\underline{v}^t,\ldots,\underline{v}\,\mathbf{H_n}\,\underline{v}^t\right) &= \left(\underline{v}\,\mathbf{M}_n\,\mathbf{F}^{*0}\,\mathbf{M_n}^t\,\underline{v}^t,\ldots,\underline{v}\,\mathbf{M}_n\,\mathbf{F}^{*n-1}\,\mathbf{M}_n^t\,\underline{v}^t\right)\mathbf{M}_n^{-1}\\
(\mathbf{H_1},\ldots,\mathbf{H_n}) &= \left(\mathbf{M}_n\,\mathbf{F}^{*0}\,\mathbf{M_n}^t,\ldots,\mathbf{M}_n\,\mathbf{F}^{*n-1}\,\mathbf{M}_n^t\right)\mathbf{M}_n^{-1}.
\end{aligned}
$$

□

We consider now the symmetric matrices $(\mathbf{G_1},\ldots,\mathbf{G_n}) \in (\mathscr{M}_{n\times n}(\mathbb{F}_q))^n$ associated to the public polynomials $(g_1,\ldots,g_n) \in \left(\mathbb{F}_q[x_1,\ldots,x_n]\right)^n$, i.e. $g_i = \underline{x}\mathbf{G_i}\underline{x}^t$ for all i, $1 \leqslant i \leqslant n$. We want to bind the public matrices $\mathbf{G_i}$ in the small field to the secret matrix $\mathbf{F}$ in the big field. To do that, the equation $\mathscr{G} = \mathscr{T} \circ \mathscr{F} \circ \mathscr{S}$ can also be interpreted as matrix/vector operations.

$$\begin{aligned}
\mathscr{G}(\underline{x}) &= \mathscr{T} \circ \mathscr{F} \circ \mathscr{S}(\underline{x}) \\
(g_1(\underline{x}), \ldots, g_n(\underline{x})) &= \big(h_1(\underline{x}\mathbf{S}), \ldots, h_n(\underline{x}\mathbf{S})\big)\,\mathbf{T} \\
\big(\underline{x}\,\mathbf{G_1}\,\underline{x}^t, \ldots, \underline{x}\,\mathbf{G_n}\,\underline{x}^t\big) &= \big(\underline{x}\,\mathbf{S}\,\mathbf{H_1}\,\mathbf{S}^t\,\underline{x}^t, \ldots, \underline{x}\,\mathbf{S}\,\mathbf{H_n}\,\mathbf{S}^t\,\underline{x}^t\big)\,\mathbf{T} \\
(\mathbf{G_1}, \ldots, \mathbf{G_n}) &= \big(\mathbf{S}\,\mathbf{H_1}\,\mathbf{S}^t, \ldots, \mathbf{S}\,\mathbf{H_n}\,\mathbf{S}^t\big)\,\mathbf{T}.
\end{aligned}$$

Thanks to Lemma 2:

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

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

$$(\mathbf{G_1}, \ldots, \mathbf{G_n})\,\mathbf{T}^{-1}\mathbf{M}_n = (\mathbf{S}\mathbf{M}_n\mathbf{F}^{*0}\mathbf{M}_n^t\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{M}_n\mathbf{F}^{*n-1}\mathbf{M}_n^t\mathbf{S}^t). \tag{3}$$

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 $\mathbf{F}^{*i}$, for all $i, 0 \leqslant i < n$.

Notice that Equation (3) involves left products of a matrix with $\mathbf{M}_n$. This product has an interesting property.

Proposition 3 *Let $\mathbf{A} = [a_{i,j}] \in \mathscr{M}_{n\times n}(\mathbb{F}_q)$, and $\mathbf{B} = [b_{i,j}] = \mathbf{A}\mathbf{M}_n \in \mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$. We have:*

$$b_{i,j} = b_{i,j-1}^q, \text{ for all } i, j, 0 \leqslant i, j < n.$$

That is, each column is obtained from the previous one using a Frobenius application. As a consequence, the whole matrix $\mathbf{B} = [b_{i,j}] = \mathbf{A}\mathbf{M}_n$ can be defined with any of its columns.

Proof Due to the definition of $\mathbf{M}_n$ in Proposition 2, $b_{i,j} = \sum_{k=0}^{n-1} a_{i,k}\,\theta_{k+1}^{q^j}$, for all i, j, $0 \leqslant i, j < n$. Consequently:

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

As $a_{i,j} \in \mathbb{F}_q$ (i.e. $a_{i,j}^q = a_{i,j}$) and since the Frobenius is linear, we get:

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

□

From now on, we will write $\mathbf{T}^{-1}\,\mathbf{M}_n = \mathbf{U} = [u_{i,j}] \in \mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$ and $\mathbf{S}\,\mathbf{M}_n = \mathbf{W} = [w_{i,j}] \in \mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$. We then rewrite (3) as follows:

$$(\mathbf{G_1}, \ldots, \mathbf{G_n})\,\mathbf{U} = (\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\mathbf{F}^{*n-1}\mathbf{W}^t). \tag{4}$$

According to Proposition 3, $u_{i,j+1} = u_{i,j}^q$ and $w_{i,j+1} = w_{i,j}^q$, for all $i, j, 0 \leqslant i, j < n$. Thus, we only need to know one column of $\mathbf{U}$ (resp. $\mathbf{W}$) to recover the whole matrix. Let then $(u_{0,0}, \ldots, u_{n-1,0}) \in (\mathbb{F}_{q^n})^n$ be the components of the first column of $\mathbf{U}$. We have:

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t = \mathbf{W}\mathbf{F}\mathbf{W}^t. \tag{5}$$

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 $\mathbf{W}\mathbf{F}\mathbf{W}^t$. In contrast to the initial attack, the $\mathbf{G_i}$'s are the public matrices and not matrices whose coefficients are in the big field. In the other hand, the solution of such MinRank lies in $(\mathbb{F}_{q^n})^n$. This leads to the following theorem.

Theorem 2 *For HFE, recovering $\mathbf{U} = \mathbf{T}^{-1}\,\mathbf{M}_n \in \mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$ reduces to solve a MinRank with $k = n$ and $r = \lceil \log_q(D) \rceil$ on the public matrices $(\mathbf{G_1}, \ldots, \mathbf{G_n}) \in \mathscr{M}_{n\times n}(\mathbb{F}_q)^n$ whose entries are in $\mathbb{F}_q$. The solutions (i.e. the linear combinations) of this MinRank are in $(\mathbb{F}_{q^n})^n$.*

Computing a Gröbner basis of a polynomial system whose coefficients are 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 Table 2, we compare the original KS MinRank attack and the new MinRank attack on HFE ($N = 1$) with parameters $q = 31$, $D = 31^2 + 31 = 992$.

Our attack allows a considerable speedup over the original KS attack. It makes it practical for a wide range of parameter whereas the original KS attack was considered theoretical. Another advantage of this new formulation is that it can be easily extended to Multi-HFE.

Table 2 Comparison between the original KS attack and the new attack on HFE ($N=1$) with parameters $q=31$, $D=31^2+31=992$ using MAGMA [8] (V2.17-1) on a 2.93 GHz Intel® Xeon® CPU. The gain (ratio) is expected to be between $n\log n$ and n^2.

n	12	13	14	15	16	17	18	19
KS attack (in s.)	390	1325	1796	2754	14434	38996	30064	138656
new attack (in s.)	3.3	6.7	12.6	25.7	54.3	107	196	327
ratio	120	197	143	107	266	366	153	424

3.2 Generalization to 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 [6]. As a consequence, there is no linear combination of the $\mathbf{G}^{*k}$ (notation as in (2)) leading to a small rank, making the MinRank attack impossible at first glance. 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 $(\mathbb{F}_{q^d})^N$.

The whole idea of our generalization is to "*expand*" the concepts of Sect. 3.1 to N variables. We recall that $n=Nd$. Hence, a n dimensional vector over the small field can be divided in N blocks of size d. Each such block represents an element in the big field (i.e $\mathbb{F}_{q^d}$) and has to be processed as in Sect. 3.1. The process is applied N times, once for each block. This leads to consider N different solutions of a MinRank problem. To this end, the matrix defined in Proposition 2 has to be expanded. Precisely, we consider block diagonal matrices as in the next proposition.

Proposition 4 *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 $\mathbf{M}_d\in\mathscr{M}_{d\times d}\left(\mathbb{F}_{q^d}\right)$ be the matrix as defined in Proposition 2. We construct the matrix $\mathbf{M}_{N,d}=\mathrm{Diag}(\underbrace{\mathbf{M}_d,\ldots,\mathbf{M}_d}_{N})\in\mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$, namely*

$$\mathbf{M}_{N,d}=\begin{pmatrix}
\begin{matrix}\theta_1 & \theta_1^q & \ldots & \theta_1^{q^{d-1}}\\ \theta_2 & \theta_2^q & \ldots & \theta_2^{q^{d-1}}\\ \vdots & \vdots & \ldots & \vdots\\ \theta_d & \theta_d^q & \ldots & \theta_d^{q^{d-1}}\end{matrix} & & 0\\
& \ddots & \\
0 & & \begin{matrix}\theta_1 & \theta_1^q & \ldots & \theta_1^{q^{d-1}}\\ \theta_2 & \theta_2^q & \ldots & \theta_2^{q^{d-1}}\\ \vdots & \vdots & \ldots & \vdots\\ \theta_d & \theta_d^q & \ldots & \theta_d^{q^{d-1}}\end{matrix}
\end{pmatrix}.$$

We can express the morphism $\varphi_N:(\mathbb{F}_{q^d})^N\to\mathbb{F}_q^n$ as

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

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

$$(v_1,\ldots,v_n)\mapsto(W_1,W_{d+1},\ldots,W_{d(N-1)+1})$$

where $(W_1,\ldots,W_n)=(v_1,\ldots,v_n)\,\mathbf{M}_{N,d}$.

Proof Once again, we recall that $n=Nd$. Hence, a n dimensional vector $(v_1,\ldots,v_n)\in\mathbb{F}_q^n$ can be divided in N blocks of size d. Due to the construction of $\mathbf{M}_{N,d}$, each block of d elements in $(v_1,\ldots,v_n)$ is multiplied by the matrix $\mathbf{M}_d$. Eventually, the matrix acts just as if we apply Proposition 2 to each of the N blocks of d elements. This is then a multi-dimensional extension of Proposition 2.

More formally, we define $V_k = \sum_{i=1}^{d} v_{(k-1)d+i}\theta_i$ for all $k, 1 \leqslant k \leqslant N$. That is, the k-th block of d components in $(v_1,\ldots,v_n) \in \mathbb{F}_q^n$ represents the k-th component of $(V_1,\ldots,V_N) \in (\mathbb{F}_{q^d})^N$, for all $k, 1 \leqslant k \leqslant N$, i.e. $\varphi_N(V_1,\ldots,V_N) = (\varphi_1(V_1),\ldots,\varphi_1(V_N)) = (v_1,\ldots,v_n)$.

Let $(W_1,\ldots,W_n) = (v_1,\ldots,v_n)\,\mathbf{M}_{N,d}$. We point out that the k-th block of d components of the vector $(W_1,\ldots,W_n)$ $\big($resp. $(v_1,\ldots,v_n))$ is $\big(W_{(k-1)d+1},\ldots,W_{kd}\big)$ $\big($resp. $(v_{(k-1)d+1},\ldots,v_{kd})\big)$. Then, by construction of $\mathbf{M}_{N,d}$:

$$(W_{(k-1)d+1},\ldots,W_{kd}) = (v_{(k-1)d+1},\ldots,v_{kd})\,\mathbf{M}_d, \forall k, 1 \leqslant k \leqslant N.$$

From Proposition 2:

$$(v_{(k-1)d+1},\ldots,v_{kd})\,\mathbf{M}_d = (V_k^{q^0},\ldots,V_k^{q^{d-1}}), \forall k, 1 \leqslant k \leqslant N.$$

By gathering all N blocks:

$$\begin{aligned}(W_1,\ldots,W_n) &= (V_1^{q^0},\ldots,V_1^{q^{d-1}},\ldots,V_N^{q^0},\ldots,V_N^{q^{d-1}})\\ (v_1,\ldots,v_n)\,\mathbf{M}_{N,d} &= (V_1^{q^0},\ldots,V_1^{q^{d-1}},\ldots,V_N^{q^0},\ldots,V_N^{q^{d-1}})\,.\end{aligned}$$

This proves the proposition for φ_N^{-1}. As $\mathbf{M}_{N,d}$ is invertible, it also holds that

$$(V_1^{q^0},\ldots,V_1^{q^{d-1}},\ldots,V_N^{q^0},\ldots,V_N^{q^{d-1}})\,\mathbf{M}_{N,d}^{-1} = (v_1,\ldots,v_n),$$

which proves the proposition for φ_N. □

Note that Proposition 4 indeed generalizes Proposition 2 since $\mathbf{M}_{1,d} = \mathbf{M}_d$. Using this definition for φ_N, a non-standard representation of the secret polynomials – similar to the one of Kipnis-Shamir – can be introduced. For a multi-HFE shaped polynomial $F \in F_{q^d}[X_1,\ldots,X_N]$, this corresponds to the matrix $\mathbf{F} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ such that $F = \underline{\widetilde{X}}\mathbf{F}\underline{\widetilde{X}}^t$ where $\underline{\widetilde{X}} = (X_1, X_1^q,\ldots,X_1^{q^{d-1}},\ldots,X_N,X_N^q,\ldots,X_N^{q^{d-1}})$. We need now to generalize the $\mathbf{F}^{*k}$ matrices used in Sect. 2.3.

Definition 1 Let $\mathbf{F} = [f_{i,j}] \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ be the non-standard matrix representation of a HFE-shaped polynomial $F \in \mathbb{F}_{q^d}[X_1,\ldots,X_N]$. We have $n = Nd$, and the matrix $\mathbf{F}$ can be divided in $N\times N$ blocks of size $d\times d$. We denote then by $\mathbf{F}^{*d,k} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ the matrix obtained from $\mathbf{F}$ by rotating the rows and columns of each $d\times d$ blocks from k positions and raising each components to the power q^k. That is, if we denote by $\mathbf{F}_{i,j}$ the $d\times d$ block of $\mathbf{F}$ located at position (i,j), $0 \leqslant i,j < N$, we have:

$$\mathbf{F}^{*d,k} = \begin{pmatrix} \mathbf{F}_{0,0}^{*k} & \ldots & \mathbf{F}_{0,N-1}^{*k} \\ \vdots & & \vdots \\ \mathbf{F}_{N-1,0}^{*k} & \ldots & \mathbf{F}_{N-1,N-1}^{*k}\end{pmatrix}.$$

The definition generalizes the one of $\mathbf{F}^{*k}$. As in the univariate case the matrix $\mathbf{F}^{*d,k}$ indeed represents the q^k-th power of a polynomial in $\mathbb{F}_{q^d}[X_1,\ldots,X_N]$.

Proposition 5 *Let $F \in \mathbb{F}_{q^d}[X_1,\ldots,X_N]$ be a HFE-shaped polynomial and $\mathbf{F} = [f_{i,j}] \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ be its non-standard matrix representation. $\mathbf{F}^{*d,k}$ is the non-standard matrix representation of F^{q^k}.*

To prove Proposition 5, one can remark that the block $\mathbf{F}_{i,j}$ of the matrix $\mathbf{F}$ operates only on the variables X_{i+1} and X_{j+1}. To apply the Frobenius action to the whole polynomial F, it has to be applied to each of these blocks, leading to the shape of $\mathbf{F}^{*d,k}$. The precise proof can be found in Appendix B.

Thanks to Proposition 5, equation (4) can be generalized for multi-HFE. To this end, we propose a multivariate version of Lemma 2. Namely:

Lemma 3 *Let $\mathbf{M}_{N,d} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ be the matrix defined in Proposition 4. Let $\mathbf{F_1},\ldots,\mathbf{F_N}$ be the non-standard symmetric matrices representing the secret polynomials $F_1,\ldots,F_N$, and $\mathbf{F_i}^{*d,k}$ be the matrices defined in Definition 1. Finally, we consider the symmetric matrices $(\mathbf{H_1},\ldots,\mathbf{H_n}) \in \left(\mathscr{M}_{n\times n}(\mathbb{F}_q)\right)^n$ associated to the secret quadratic polynomials in the small field $(h_1,\ldots,h_n) \in \left(\mathbb{F}_q[x_1,\ldots,x_n]\right)^n$, i.e. $h_i = \underline{x}\mathbf{H_i}\underline{x}^t$ for all i, $1 \leqslant i \leqslant n$. It holds that:*

$$\begin{aligned}(\mathbf{H_1},\ldots,\mathbf{H_n}) = \big(\mathbf{M}_{N,d}\,\mathbf{F_1}^{*d,0}\,\mathbf{M}_{N,d}^t,\ldots,\mathbf{M}_{N,d}\,\mathbf{F_1}^{*d,d-1}\,\mathbf{M}_{N,d}^t,\ldots\\ \ldots,\mathbf{M}_{N,d}\mathbf{F_N}^{*d,0}\,\mathbf{M}_{N,d}^t,\ldots,\mathbf{M}_{N,d}\mathbf{F_N}^{*d,d-1}\,\mathbf{M}_{N,d}^t\big)\,\mathbf{M}_{N,d}^{-1}.\end{aligned}$$

Proof The proof is very similar to the proof of Lemma 2. We start from the definition of the small field polynomials $h_1,\ldots,h_n$. For all $\underline{v}\in\mathbb{F}_q^n$,

$$(h_1(\underline{v}),\ldots,h_n(\underline{v}))=\varphi_N\left(F_1\left(\varphi_N^{-1}(\underline{v})\right),\ldots,F_N\left(\varphi_N^{-1}(\underline{v})\right)\right).$$

Similarly, we need to express the above equation by matrix operations. We use then the definition of φ_N and its inverse using the matrix $\mathbf{M}_{N,d}$ of Proposition 4, $(h_1(\underline{v}),\ldots,h_n(\underline{v}))=$

$$\left(F_1^{q^0}\left(\underline{v}\mathbf{M}_{N,d}\right),\ldots,F_1^{q^{d-1}}\left(\underline{v}\mathbf{M}_{N,d}\right),\ldots,F_N^{q^0}\left(\underline{v}\mathbf{M}_{N,d}\right),\ldots,F_N^{q^{d-1}}\left(\underline{v}\mathbf{M}_{N,d}\right)\right)\mathbf{M}_{N,d}^{-1}.$$

Recall from Proposition 5 that $\mathbf{F_i}^{*d,j}$ is the matrix representation of $F_i^{q^j}$, $\forall i, 1\leqslant i\leqslant N$ and $\forall j, 0\leqslant j<d$. We replace the polynomials by their matrix expression and we get for all $\underline{v}\in\mathbb{F}_q^n$:

$$\begin{aligned}(\underline{v}\mathbf{H_1}\underline{v}^t,\ldots,\underline{v}\mathbf{H_n}\underline{v}^t)=\big(&\underline{v}\mathbf{M}_{N,d}\mathbf{F_1}^{*d,0}\mathbf{M}_{N,d}^t\underline{v}^t,\ldots,\underline{v}\mathbf{M}_{N,d}\mathbf{F_1}^{*d,d-1}\mathbf{M}_{N,d}^t\underline{v}^t,\ldots\\&\ldots,\underline{v}\mathbf{M}_{N,d}\mathbf{F_N}^{*d,0}\mathbf{M}_{N,d}^t\underline{v}^t,\ldots,\underline{v}\mathbf{M}_{N,d}\mathbf{F_N}^{*d,d-1}\mathbf{M}_{N,d}^t\underline{v}^t\big)\mathbf{M}_{N,d}^{-1},\end{aligned}$$

which concludes the proof. □

Now, let $\mathbf{U}=\mathbf{T}^{-1}\mathbf{M}_{N,d}\in\mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$, $\mathbf{W}=\mathbf{S}\mathbf{M}_{N,d}\in\mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ and $\mathbf{F_i}^{(j)}=\mathbf{W}\mathbf{F_i}^{*d,j}\mathbf{W}^t$, with i, $1\leqslant i\leqslant N$, and j, $0\leqslant j<d$. We have the relation:

$$\begin{aligned}\mathscr{G}(\underline{x})&=\mathscr{T}\circ\mathscr{F}\circ\mathscr{S}(\underline{x}),\\(g_1(\underline{x}),\ldots,g_n(\underline{x}))&=\big(h_1(\underline{x}\mathbf{S}),\ldots,h_n(\underline{x}\mathbf{S})\big)\mathbf{T},\\\left(\underline{x}\mathbf{G_1}\underline{x}^t,\ldots,\underline{x}\mathbf{G_n}\underline{x}^t\right)&=\left(\underline{x}\mathbf{S}\mathbf{H_1}\mathbf{S}^t\underline{x}^t,\ldots,\underline{x}\mathbf{S}\mathbf{H_n}\mathbf{S}^t\underline{x}^t\right)\mathbf{T},\\(\mathbf{G_1},\ldots,\mathbf{G_n})&=\left(\mathbf{S}\mathbf{H_1}\mathbf{S}^t,\ldots,\mathbf{S}\mathbf{H_n}\mathbf{S}^t\right)\mathbf{T}.\end{aligned}$$

Using Lemma 3:

$$\begin{aligned}(\mathbf{G_1},\ldots,\mathbf{G_n})=\big(&\mathbf{S}\mathbf{M}_{N,d}\mathbf{F_1}^{*d,0}\mathbf{M}_{N,d}^t\mathbf{S}^t,\ldots,\mathbf{S}\mathbf{M}_{N,d}\mathbf{F_1}^{*d,d-1}\mathbf{M}_{N,d}^t\mathbf{S}^t,\ldots\\&\ldots,\mathbf{S}\mathbf{M}_{N,d}\mathbf{F_N}^{*d,0}\mathbf{M}_{N,d}^t\mathbf{S}^t,\ldots,\mathbf{S}\mathbf{M}_{N,d}\mathbf{F_N}^{*d,d-1}\mathbf{M}_{N,d}^t\mathbf{S}^t\big)\mathbf{M}_{N,d}^{-1}\mathbf{T}.\end{aligned}\tag{6}$$

Matrices $\mathbf{T}$ and $\mathbf{M}_{N,d}$ being invertible, we obtain:

$$\begin{aligned}(\mathbf{G_1},\ldots,\mathbf{G_n})\,\mathbf{T}^{-1}\mathbf{M}_{N,d}&=(\mathbf{F_1}^{(0)},\ldots,\mathbf{F_1}^{(d-1)},\ldots\ldots,\mathbf{F_N}^{(0)},\ldots,\mathbf{F_N}^{(d-1)}),\\(\mathbf{G_1},\ldots,\mathbf{G_n})\,\mathbf{U}&=(\mathbf{F_1}^{(0)},\ldots,\mathbf{F_1}^{(d-1)},\ldots\ldots,\mathbf{F_N}^{(0)},\ldots,\mathbf{F_N}^{(d-1)}).\end{aligned}\tag{7}$$

As in the univariate case, matrices $\mathbf{U}$ and $\mathbf{W}$ have a useful property.

Proposition 6 *Let $\mathbf{A}=[a_{i,j}]\in\mathscr{M}_{n\times n}(\mathbb{F}_q)$, and $\mathbf{B}=[b_{i,j}]=\mathbf{A}\mathbf{M}_{N,d}\in\mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$. For all $i, 0\leqslant i<n$, $k, 0\leqslant k<N$ and $j, 0\leqslant j<d$, we have:*

$$b_{i,kd+j}=b_{i,kd+((j-1)\bmod d)}^q.$$

That is, for each group of d columns, one column is obtained from the previous one using a Frobenius application. Each group of d columns is defined by one of them, and consequently, the whole matrix is defined by N columns, one in each group.

The proof of Proposition 6 is similar to the proof of Proposition 3. The property comes from the fact that each group of d columns is processed by a matrix $\mathbf{M}_d$ leading to a similar property as Proposition 3 for each group. The precise proof can be found in Appendix B.

To get the analogy with the MinRank in the univariate case, we remark that $\mathbf{F_i}^{*d,0}=\mathbf{F_i}$. By considering the (id)-th columns of $\mathbf{U}$ for all $i, 0\leqslant i<N$ we have

$$\sum_{k=0}^{n-1}u_{k,0}\mathbf{G_{k+1}}=\mathbf{W}\mathbf{F_1}\mathbf{W}^t,\ldots,\sum_{k=0}^{n-1}u_{k,(N-1)d}\mathbf{G_{k+1}}=\mathbf{W}\mathbf{F_N}\mathbf{W}^t.\tag{8}$$

The following lemma allows to bind (8) to a MinRank problem.

Lemma 4 *Let* $(F_1,\ldots,F_N)\in(\mathbb{F}_{q^d}[X_1,\ldots,X_N])^N$ *be polynomials having Multi-HFE shape. For all* $k, 1\leqslant k\leqslant N$, *let* $\mathbf{F_k}\in\mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ *be their non-standard symmetric matrix representation. Let* D *be the degree of each polynomial* F_k *and* $\ell=\lceil\log_q D\rceil$. *For all* $k, 1\leqslant k\leqslant N$

$$\operatorname{Rank}(\mathbf{F_k})\leqslant N\ell.$$

Furthermore, let

$$\mathbf{K}_{N,d,\ell}=\begin{pmatrix} \left|\mathbf{0}_{d-\ell,\ell}\ \mathbf{I}_{d-\ell}\right| & \mathbf{0}_{d-\ell,d} & \ldots & \mathbf{0}_{d-\ell,d} \\ \mathbf{0}_{d-\ell,d} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0}_{d-\ell,d} \\ \mathbf{0}_{d-\ell,d} & \ldots & \mathbf{0}_{d-\ell,d} & \left|\mathbf{0}_{d-\ell,\ell}\ \mathbf{I}_{d-\ell}\right| \end{pmatrix}\in\mathscr{M}_{n-N\ell,n}\left(\mathbb{F}_{q^d}\right)$$

where $\mathbf{0}_{d-\ell,\ell}$ *(resp.* $\mathbf{0}_{d-\ell,d}$*) is the zero matrix with* $(d-\ell)$ *rows and* ℓ *(resp. d) columns, and* $\mathbf{I}_{d-\ell}$ *is the identity matrix with* $(d-\ell)$ *rows and columns. Then, the rows of the matrix* $\mathbf{K}_{N,d,\ell}$ *are a basis of the left kernel of* $\mathbf{F_k}$ *with high probability and does not depend on the entries of* $\mathbf{F_k}$.

Proof Each polynomial F_k has degree bounded by D, for k, $1\leqslant k\leqslant N$, thus each variable X_i has at most degree D, for all $i, 1\leqslant i\leqslant N$. The only non-zero entries of the matrix $\mathbf{F_k}$ are the ones in the upper-left $\log_q(D)$ square of each $N\times N$ block of size $(d\times d)$. Thus, $\mathbf{F_k}$ has at most $N\ell$ non-zero rows and columns and has the following structure

$$\mathbf{F_k}=\begin{pmatrix} \mathbf{A_k}^{0,0} & \ldots & \mathbf{A_k}^{0,N-1} \\ \vdots & & \vdots \\ \mathbf{A_k}^{N-1,0} & \ldots & \mathbf{A_k}^{N-1,N-1} \end{pmatrix}$$

where each block $\mathbf{A_k}^{i,j}$ is a $d\times d$ matrix

$$\mathbf{A_k}^{i,j}=\begin{pmatrix} A^{i,j}_{k,0,0} & \ldots & A^{i,j}_{k,0,\ell} & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ A^{i,j}_{k,\ell,0} & \ldots & A^{i,j}_{k,\ell,\ell} & \vdots & & \vdots \\ 0 & \ldots & \ldots & 0 & & \vdots \\ \vdots & & & & \ddots & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \end{pmatrix}$$

for i,j, $0\leqslant i,j<N$. As the consequence, the rank of such matrix $\mathbf{F_k}$ is at most $N\ell$.

From the construction of $\mathbf{K}_{N,d,\ell}$, it is clear that $\mathbf{K}_{N,d,\ell}\mathbf{F_k}=\mathbf{0}$. As $\mathbf{K}_{N,d,\ell}$ has exactly $N(d-\ell)=(n-N\ell)$ linearly independent rows, if $\operatorname{Rank}(\mathbf{F_k})$ is exactly $N\ell$, which is the case with high probability, then $\mathbf{K}_{N,d,\ell}$ is a basis of the left kernel of $\mathbf{F_k}$. □

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

Theorem 3 *For multi-HFE, recovering* $\mathbf{U}=\mathbf{T}^{-1}\mathbf{M}_{N,d}\in\mathscr{M}_{n\times n}(\mathbb{F}_{q^n})$ *reduces to solve* N *times a MinRank problem with* $k=n$ *and* $r=N\log_q(D)$ *on the public matrices* $(\mathbf{G_1},\ldots,\mathbf{G_n})\in\mathscr{M}_{n\times n}(\mathbb{F}_q)^n$. *On the other hand, the solutions (i.e. the linear combinations) of each MinRank are in* $\mathbb{F}_{q^d}$.

Proof The N MinRank solutions come from (8). From Lemma 4, the rank of $\mathbf{F_k}$ is bounded by $r=N\lceil\log_q(D)\rceil$. Since $\mathbf{W}$ is invertible, the rank of $\mathbf{W}\mathbf{F_k}\mathbf{W}^t$ is equal to the rank of $\mathbf{F_k}$ for all $k, 1\leqslant k\leqslant N$. From Proposition 6, knowing one column in each of the N sequences of d columns in $\mathbf{U}$ is enough to recover the whole matrix $\mathbf{U}$. This allows to conclude the proof. □

Recovering the transformation $\mathscr{T}$ reduces to solving a MinRank problem. Recovering the other parts of a secret key reduces to solving linear systems. This will be discussed in Sect. 6. Before that, we study the effects of equivalent keys. This allows to better understand the MinRank arising in HFE/Multi-HFE as well as the other parts of the attack.

4 About Equivalent Keys and Induced Degrees of Freedom

Two secret keys are equivalent if they lead to the the same public key. The subject has already been treated for the original HFE [46, 45, 47]. It has been shown that $n\,q^{2n}(q^n-1)^2$ equivalent keys exist for HFE. This phenomena is even amplified for multi-HFE. In this section, we exploit this fact.

Definition 2 Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key with parameters $(q, N, d, D) \in \mathbb{N}^4$. We say that the key $(\mathscr{F}^{*\prime}, \mathscr{S}', \mathscr{T}')$ is an equivalent key if and only if $\mathscr{F}^{*\prime}$ has HFE-shape, and

$$\mathscr{T}' \circ \varphi_N \circ \mathscr{F}^{*\prime} \circ \varphi_N^{-1} \circ \mathscr{S}' = \mathscr{G} = \mathscr{T} \circ \varphi_N \circ \mathscr{F}^* \circ \varphi_N^{-1} \circ \mathscr{S} \text{ (same public key).}$$

Wolf and Preneel [46, 47] 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, multiplication keeps the HFE-shape. But, we also have any affine transformation on the N variables. Thus, the two first sustainers can be generalized as follows.

Proposition 7 *Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key with parameters (q, N, d, D). For any invertible affine transformations $(\mathscr{A}^*, \mathscr{B}^*) \in \mathrm{Aff}_N(\mathbb{F}_{q^d}) \times \mathrm{Aff}_N(\mathbb{F}_{q^d})$, we set $\mathscr{A} = \varphi_N \circ \mathscr{A}^* \circ \varphi_N^{-1}$ and $\mathscr{B} = \varphi_N \circ \mathscr{B}^* \circ \varphi_N^{-1}$. Then*

$$\left(\mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^*, \quad \mathscr{A}^{-1} \circ \mathscr{S}, \quad \mathscr{T} \circ \mathscr{B}^{-1}\right)$$

is an equivalent key.

Proof First, we show that $\mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^*$ has HFE-shape. This is due to the fact that the only exponents occurring in a variable X_i is a power of q. The transformation $\mathscr{A}^*$ mixes the variables $X_1, \ldots, X_N$ by affine combinations. By linearity of the Frobenius, no other exponents can appear and the system keeps its HFE-shape. Trivially, as $\mathscr{B}^*$ only performs affine combinations of the polynomials $F_1, \ldots, F_N$ the shape is also unchanged. To conclude, we notice that

$$\begin{aligned}
&\mathscr{G} = \mathscr{T} \circ \varphi_N \circ \mathscr{F}^* \circ \varphi_N^{-1} \circ \mathscr{S} \\
&\mathscr{G} = \left(\mathscr{T} \circ \varphi_N \circ \mathscr{B}^{*-1} \circ \varphi_N^{-1}\right) \circ \varphi_N \circ \left(\mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^*\right) \circ \varphi_N^{-1} \circ \left(\varphi_N \circ \mathscr{A}^{*-1} \circ \varphi_N^{-1} \circ \mathscr{S}\right) \\
&\mathscr{G} = \left(\mathscr{T} \circ \mathscr{B}^{-1}\right) \circ \varphi_N \circ \left(\mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^*\right) \circ \varphi_N^{-1} \circ \left(\mathscr{A}^{-1} \circ \mathscr{S}\right).
\end{aligned}$$

□

The following proposition provides the structure of a transformation used in Proposition 7 in the linear case (it has to be slightly adapted in the affine case).

Proposition 8 *Let $\mathbf{A}^* = [a_{i,j}] \in \mathscr{M}_{N\times N}\left(\mathbb{F}_{q^d}\right)$ be the matrix associated to a linear transformation $\mathscr{A}^*$ over $(\mathbb{F}_{q^d})^N$. The transformation $\mathscr{A}^*$ can be represented in the field $\mathbb{F}_q$ as:*

$$\mathbf{A} = \mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{M}_{N,d}^{-1} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_q\right),$$

where $\mathbf{M}_{N,d} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ is the matrix of Proposition 4 and $\widetilde{\mathbf{A}^*} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ is a matrix composed of $N\times N$ blocks of Frobenius powers of elements of $\mathbf{A}^*$, i.e.

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

Proof Let $(V_1,\ldots,V_N) \in (\mathbb{F}_{q^d})^N$. We set:

$$(Z_1,\ldots,Z_N) = \mathscr{A}^*(V_1,\ldots,V_N) = \left(\sum_{i=0}^{N-1} a_{i,0}V_{i+1},\ldots,\sum_{i=0}^{N-1} a_{i,N-1}V_{i+1}\right).$$

According to Proposition 4, we need to compute the Frobenius images of $(Z_1,\ldots,Z_N)$ to split it to the small field. For all $k, 0 \leqslant k < d$, we have:

$$(Z_1^{q^k},\ldots,Z_N^{q^k}) = \left(\sum_{i=0}^{N-1} a_{i,0}^{q^k}V_{i+1}^{q^k},\ldots,\sum_{i=0}^{N-1} a_{i,N-1}^{q^k}V_{i+1}^{q^k}\right).$$

We notice that $Z_i^{q^k}$ is obtained only from the $V_j^{q^k}$'s for j, $1 \leqslant j \leqslant N$. This explains intuitively the shape of $\widetilde{\mathbf{A}^*}$ We constructed the matrix $\widetilde{\mathbf{A}^*}$ such that:

$$(V_1,V_1^q,\ldots,V_1^{q^{d-1}},\ldots,V_N,V_N^q,\ldots,V_N^{q^{d-1}})\,\widetilde{\mathbf{A}^*} = (Z_1,Z_1^q,\ldots,Z_1^{q^{d-1}},\ldots,Z_N,Z_N^q,\ldots,Z_N^{q^{d-1}}). \tag{9}$$

Let $\mathbf{A} \in \mathscr{M}_{n\times n}(\mathbb{F}_q)$ be the small field representation of $\mathscr{A}^*$, we now prove that $\mathbf{A} = \mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{M}_{N,d}^{-1}$.

First, let $(v_1,\ldots,v_n) \in \mathbb{F}_q^n$ $\big($resp. $(z_1,\ldots,z_n) \in \mathbb{F}_q^n\big)$ be the small field representation of $(V_1,\ldots,V_N)$ (resp. $(Z_1,\ldots,Z_N)$). It holds that

$$(v_1,\ldots,v_n)\mathbf{A} = (z_1,\ldots,z_n).$$

From Proposition 4, we know that

$$\begin{aligned}(v_1,\ldots,v_n)\,\mathbf{M}_{N,d} &= (V_1,V_1^q,\ldots,V_1^{q^{d-1}},\ldots,V_N,V_N^q,\ldots,V_N^{q^{d-1}}),\\ (z_1,\ldots,z_n)\,\mathbf{M}_{N,d} &= (Z_1,Z_1^q,\ldots,Z_1^{q^{d-1}},\ldots,Z_N,Z_N^q,\ldots,Z_N^{q^{d-1}}).\end{aligned}$$

By replacing in (9), we get

$$\begin{aligned}(v_1,\ldots,v_m)\,\mathbf{M}_{N,d}\,\widetilde{\mathbf{A}^*} &= (z_1,\ldots,z_m)\mathbf{M}_{N,d}\\ (v_1,\ldots,v_m)\,\mathbf{M}_{N,d}\,\widetilde{\mathbf{A}^*}\,\mathbf{M}_{N,d}^{-1} &= (z_1,\ldots,z_m).\end{aligned}$$

Then, $\mathbf{A} = \mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{M}_{N,d}^{-1}$ is the small field representation of $\mathscr{A}^*$. □

We consider now the Frobenius transformation.

Proposition 9 *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 $k, 0 \leqslant k < d$:*

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

is an equivalent key.

Proof For any $k, 0 \leqslant k < d$, the polynomials of

$$(\mathrm{Frob_k} \circ \mathscr{F}^* \circ \mathrm{Frob_{d\text{-}k}})(X_1,\ldots,X_N) = \left(\mathscr{F}^*(X_1^{q^{d-k}},\ldots,X_N^{q^{d-k}})\right)^{q^k}$$

have the same monomials as $\mathscr{F}^*(X_1,\ldots,X_N)$ but their coefficients are raised to the power of q^k. This is explained in (2). As a consequence, if $\mathscr{F}^*(X_1,\ldots,X_N)$ has HFE-shape, so is $(\mathrm{Frob_k} \circ \mathscr{F}^* \circ \mathrm{Frob_{d\text{-}k}})(X_1,\ldots,X_N)$. In addition:

$$\begin{aligned}\mathscr{G} &= \mathscr{T} \circ \varphi_N \circ \mathscr{F}^* \circ \varphi_N^{-1} \circ \mathscr{S}\\ \mathscr{G} &= \left(\mathscr{T} \circ \varphi_N \circ \mathrm{Frob_{d\text{-}k}} \circ \varphi_N^{-1}\right) \circ \left(\varphi_N \circ \mathrm{Frob_k} \circ \mathscr{F}^* \circ \mathrm{Frob_{d\text{-}k}} \circ \varphi_N^{-1}\right) \circ \left(\varphi_N \circ \mathrm{Frob_k} \circ \varphi_N^{-1} \circ \mathscr{S}\right).\end{aligned}$$

As the Frobenius application is linear in $\mathbb{F}_q$, the transformations $\mathscr{T} \circ \varphi_N \circ \mathrm{Frob_{d\text{-}k}} \circ \varphi_N^{-1}$ and $\varphi_N \circ \mathrm{Frob_k} \circ \varphi_N^{-1} \circ \mathscr{S}$ remain affine. Finally, $\mathrm{Frob_k} \circ \mathscr{F}^* \circ \mathrm{Frob_{d\text{-}k}}$ has HFE-shape, proving Proposition 9. □

We introduce also the matrix representation of a Frobenius application.

Proposition 10 *Let* $\mathbf{Frob_k} \in \mathscr{M}_{n\times n}(\mathbb{F}_q)$ *be the matrix representing the linear transformation* $\varphi_N \circ \mathrm{Frob_k} \circ \varphi_N^{-1}$ *over* $\mathbb{F}_q$. *Then*

$$\mathbf{Frob_k} = \mathbf{M}_{N,d}\mathbf{P}_{N,d,k}\mathbf{M}_{N,d}^{-1}$$

where $\mathbf{P}_{N,d,k} = \mathrm{Diag}(\underbrace{\mathbf{R}_{d,k},\dots,\mathbf{R}_{d,k}}_{N})$ *and* $\mathbf{R}_{d,k}$ *is the* $d\times d$ *matrix of a* k *positions left-rotation, that is*

$$\mathbf{R}_{d,k} = \begin{pmatrix} \mathbf{0}_{k,d-k} & \mathbf{I}_k \\ \mathbf{I}_{d-k} & \mathbf{0}_{d-k,k} \end{pmatrix}.$$

Proof Let $(V_1,\dots,V_N) \in (\mathbb{F}_{q^d})^N$. We set

$$\mathrm{Frob_k}(V_1,\dots,V_N) = (V_1^{q^k},\dots,V_N^{q^k}) = (Z_1,\dots,Z_N).$$

In the big field, a left k-rotation of $(V,V^q,\dots,V^{q^{d-1}})$ is the application of $\mathrm{Frob_k}$ to such vector. Indeed, $\mathrm{Frob_k}(V,V^q,\dots,V^{q^{d-1}}) = (V^{q^k},\dots,V^{q^{d-1}},V,\dots,V^{q^{k-1}})$. More generally, the matrix $\mathbf{P}_{N,d,k}$ makes this rotation on each N components in the big field. That is

$$(V_1^{q^0},\dots,V_1^{q^{d-1}},\dots,V_N^{q^0},\dots,V_N^{q^{d-1}})\,\mathbf{P}_{N,d,k} = \\ (V_1^{q^k},\dots,V_1^{q^{d-1}},V_1^{q^0},\dots,V_1^{q^{k-1}},\dots,V_N^{q^k},\dots,V_N^{q^{d-1}},V_N^{q^0},\dots,V_N^{q^{k-1}}).$$

We have then:

$$(V_1^{q^0},\dots,V_1^{q^{d-1}},\dots,V_N^{q^0},\dots,V_N^{q^{d-1}})\,\mathbf{P}_{N,d,k} = (Z_1^{q^0},\dots,Z_1^{q^{d-1}},\dots,Z_N^{q^k},\dots,Z_N^{q^{d-1}}). \tag{10}$$

As in the proof of Proposition 8, let $(v_1,\dots,v_n)\in\mathbb{F}_q^n$ $\big($resp. $(z_1,\dots,z_n)\in\mathbb{F}_q^n\big)$ be the small field representation of $(V_1,\dots,V_N)$ (resp. $(Z_1,\dots,Z_N)$). According to Proposition 4, it holds that

$$(v_1,\dots,v_n)\,\mathbf{M}_{N,d} = (V_1,V_1^q,\dots,V_1^{q^{d-1}},\dots,V_N,V_N^q,\dots,V_N^{q^{d-1}}),$$
$$(z_1,\dots,z_n)\,\mathbf{M}_{N,d} = (Z_1,Z_1^q,\dots,Z_1^{q^{d-1}},\dots,Z_N,Z_N^q,\dots,Z_N^{q^{d-1}}).$$

By replacing in (10):

$$(v_1,\dots,v_m)\,\mathbf{M}_{N,d}\,\mathbf{P_{N,d,k}} = (z_1,\dots,z_m)\mathbf{M}_{N,d}$$
$$(v_1,\dots,v_m)\,\mathbf{M}_{N,d}\,\mathbf{P_{N,d,k}}\,\mathbf{M}_{N,d}^{-1} = (z_1,\dots,z_m).$$

Then, $\mathbf{M}_{N,d}\,\mathbf{P_{N,d,k}}\,\mathbf{M}_{N,d}^{-1}$ is indeed the small field representation of $\mathrm{Frob_k}$. □

According to Proposition 9, we can derive $(d-1)$ other equivalent keys from any valid private key. This refers to the so-called Frobenius sustainer of [46, 47]. To count the number of equivalent keys introduced by Proposition 7 and 9, we need to know how many different keys they generate. To do that, we will show that any equivalent key obtained from the Frobenius and affine sustainers has a unique representation.

Lemma 5 *Let* $\mathscr{A}^* \in \mathrm{Aff}_N(\mathbb{F}_{q^d})$. *For all* k, $0 \leqslant k < d$, *there exists* $\mathscr{A}^{*\prime} \in \mathrm{Aff}_N(\mathbb{F}_{q^d})$ *such that* $\mathrm{Frob_k} \circ \mathscr{A}^* = \mathscr{A}^{*\prime} \circ \mathrm{Frob_k}$.

Proof As $\mathrm{Frob_{d\text{-}k}} \circ \mathrm{Frob_k}$ is the identity, it holds that

$$\mathrm{Frob_k} \circ \mathscr{A}^* = \mathrm{Frob_k} \circ \mathscr{A}^* \circ \mathrm{Frob_{d\text{-}k}} \circ \mathrm{Frob_k}.$$

Now we prove that $\mathscr{A}^{*\prime} = \mathrm{Frob_k} \circ \mathscr{A}^* \circ \mathrm{Frob_{d\text{-}k}}$ is an affine transformation. Let $(X_1,\dots,X_N) \in (\mathbb{F}_{q^d})^N$:

$$\mathscr{A}^{*\prime}(X_1,\dots,X_N) = \mathrm{Frob_k} \circ \mathscr{A}^* \circ \mathrm{Frob_{d\text{-}k}}(X_1,\dots,X_N) = \mathrm{Frob_k} \circ \mathscr{A}^*\left(X_1^{q^{d-k}},\dots,X_N^{q^{d-k}}\right)$$
$$\mathscr{A}^{*\prime}(X_1,\dots,X_N) = \mathrm{Frob_k}\left(\textstyle\sum_{i=0}^{N-1} A_{i,0}X_{i+1}^{q^{d-k}} + A_0,\dots,\sum_{i=0}^{N-1} A_{i,N-1}X_{i+1}^{q^{d-k}} + A_N\right)$$
$$\mathscr{A}^{*\prime}(X_1,\dots,X_N) = \left(\left(\textstyle\sum_{i=0}^{N-1} A_{i,0}X_{i+1}^{q^{d-k}} + A_0\right)^{q^k},\dots,\left(\sum_{i=0}^{N-1} A_{i,N-1}X_{i+1}^{q^{d-k}} + A_N\right)^{q^k}\right)$$
$$\mathscr{A}^{*\prime}(X_1,\dots,X_N) = \left(\textstyle\sum_{i=0}^{N-1} A_{i,0}^{q^k}X_{i+1}^{q^d} + A_N^{q^k},\dots,\sum_{i=0}^{N-1} A_{i,N-1}^{q^k}X_{i+1}^{q^d} + A_N^{q^k}\right)$$
$$\mathscr{A}^{*\prime}(X_1,\dots,X_N) = \left(\textstyle\sum_{i=0}^{N-1} A_{i,0}^{q^k}X_{i+1} + A_N^{q^k},\dots,\sum_{i=0}^{N-1} A_{i,N-1}^{q^k}X_{i+1} + A_N^{q^k}\right).$$

The transformation $\mathscr{A}^{*\prime}$ is indeed an affine transformation with the same coefficients as $\mathscr{A}^*$ raised to the power q^k. □

Lemma 5 shows that the Frobenius and the affine transformation somehow commute. This will be useful to write uniquely an equivalent key.

Lemma 6 *Let* $(\mathscr{A}^*, \mathscr{A}^{*\prime}) \in \mathrm{Aff}_N(\mathbb{F}_{q^d}) \times \mathrm{Aff}_N(\mathbb{F}_{q^d})$ *be two invertible affine transformations. If* $\mathrm{Frob_k} \circ \mathscr{A}^* = \mathrm{Frob_{k'}} \circ \mathscr{A}^{*\prime}$*, for* $k, k', 0 \leqslant k, k' < d$*, then* $\mathscr{A}^{*\prime} = \mathscr{A}^*$ *and* $k' = k$.

Proof First, it is straightforward to see that if $k = k'$, then

$$\mathrm{Frob_k} \circ \mathscr{A}^* = \mathrm{Frob_k} \circ \mathscr{A}^{*\prime} \Leftrightarrow \mathrm{Frob_{d\text{-}k}} \circ \mathrm{Frob_k} \circ \mathscr{A}^* = \mathrm{Frob_{d\text{-}k}} \circ \mathrm{Frob_k} \circ \mathscr{A}^{*\prime} \Leftrightarrow \mathscr{A}^* = \mathscr{A}^{*\prime}.$$

Then, we have only to prove that $\mathrm{Frob_k} \circ \mathscr{A}^* = \mathrm{Frob_{k'}} \circ \mathscr{A}^{*\prime} \Rightarrow k = k'$. Assume for a contradiction that there exists k and k' such that $\mathrm{Frob_k} \circ \mathscr{A}^* = \mathrm{Frob_{k'}} \circ \mathscr{A}^{*\prime}$ and $k' \neq k$. Then, we can write $k' = k + \ell$, with $\ell \neq 0$:

$$\begin{aligned} \mathrm{Frob_k} \circ \mathscr{A}^* &= \mathrm{Frob_{k'}} \circ \mathscr{A}^{*\prime} \\ \mathrm{Frob_k} \circ \mathscr{A}^* \circ \mathrm{Frob_{d\text{-}k}} &= \mathrm{Frob_{k+\ell}} \circ \mathscr{A}^{*\prime} \circ \mathrm{Frob_{d\text{-}k}} \\ \mathrm{Frob_k} \circ \mathscr{A}^* \circ \mathrm{Frob_{d\text{-}k}} &= \mathrm{Frob}_\ell \circ \mathrm{Frob_k} \circ \mathscr{A}^{*\prime} \circ \mathrm{Frob_{d\text{-}k}}. \end{aligned}$$

According to Lemma 5, $\widetilde{\mathscr{A}^*} = \mathrm{Frob_k} \circ \mathscr{A} \circ \mathrm{Frob_{d\text{-}k}}$ and $\widetilde{\mathscr{A}^{*\prime}} = \mathrm{Frob_k} \circ \mathscr{A}^{*\prime} \circ \mathrm{Frob_{d\text{-}k}}$ are also affine transformations. We write:

$$\widetilde{\mathscr{A}^*} = \mathrm{Frob}_\ell \circ \widetilde{\mathscr{A}^{*\prime}}.$$

As $\ell \neq 0$, the transformation $\mathrm{Frob}_\ell \circ \widetilde{\mathscr{A}^{*\prime}}$ has degree q^ℓ. That is, each polynomial in the representation of $\mathrm{Frob}_\ell \circ \widetilde{\mathscr{A}^{*\prime}}$ has the form $\left(\sum_{i=1}^N A_i^{q^\ell} X_i^{q^\ell} + A_0^{q^\ell}\right)$, with $A_i \in \mathbb{F}_{q^d}$. As $\widetilde{\mathscr{A}^{*\prime}}$ is invertible, at least one term of degree q^ℓ is non-zero. Thus, $\mathrm{Frob}_\ell \circ \widetilde{\mathscr{A}^{*\prime}}$ cannot be equal to $\widetilde{\mathscr{A}^*}$ which is an affine transformation and has maximal degree 1. This proves that $\mathrm{Frob_k} \circ \mathscr{A}^* = \mathrm{Frob_{k'}} \circ \mathscr{A}^{*\prime} \Rightarrow k = k'$ and $\mathscr{A}^* = \mathscr{A}^{*\prime}$. □

Together with Lemma 5, Lemma 6 is used to derive a canonical representation of equivalent keys.

Theorem 4 *Let* $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ *be a multi-HFE private key with parameters* $(q, N, d, D) \in \mathbb{N}^4$. *Let* $\mathscr{A}^*, \mathscr{B}^* \in \mathrm{Aff}_N(\mathbb{F}_{q^d})$ *be affine transformations in the big field and* $k, 0 \leqslant k < d$ *be an integer. Each Multi-HFE equivalent key* $(\mathscr{F}', \mathscr{S}', \mathscr{T}')$ *obtained using Proposition 7 and 9 can be written uniquely*

$$\begin{aligned} \mathscr{F}' &= \mathrm{Frob_k} \circ \mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^* \circ \mathrm{Frob_{d\text{-}k}} \\ \mathscr{S}' &= \varphi_N \circ \mathrm{Frob_k} \circ \mathscr{A}^{*-1} \circ \varphi_N^{-1} \circ \mathscr{S} \\ \mathscr{T}' &= \mathscr{T} \circ \varphi_N \circ \mathscr{B}^{*-1} \circ \mathrm{Frob_{d\text{-}k}} \circ \varphi_N^{-1}. \end{aligned}$$

Proof Let $(\mathscr{F}', \mathscr{S}', \mathscr{T}')$ and $(\mathscr{F}, \mathscr{S}, \mathscr{T})$ be equivalent keys. By hypothesis, a equivalent key has been obtained by composition of several Frobenius and affine transformations. According to Lemma 5, the transformations can be reordered. Hence, any equivalent key can then be written as

$$\begin{aligned} \mathscr{F}' &= \mathrm{Frob_{k_1}} \circ \cdots \circ \mathrm{Frob_{k_r}} \circ \mathscr{B}_1^* \circ \cdots \circ \mathscr{B}_{n_b}^* \circ \mathscr{F}^* \circ \mathscr{A}_{n_a}^* \circ \cdots \circ \mathscr{A}_1^* \circ \mathrm{Frob_{d\text{-}k_r}} \circ \cdots \circ \mathrm{Frob_{d\text{-}k_1}} \\ \mathscr{S}' &= \varphi_N \circ \mathrm{Frob_{k_1}} \circ \cdots \circ \mathrm{Frob_{k_r}} \circ \mathscr{A}_1^{*-1} \circ \cdots \circ \mathscr{A}_{n_a}^{*-1} \circ \varphi_N^{-1} \circ \mathscr{S} \\ \mathscr{T}' &= \mathscr{T} \circ \varphi_N \circ \mathscr{B}_{n_b}^{*-1} \circ \cdots \circ \mathscr{B}_1^{*-1} \circ \mathrm{Frob_{d\text{-}k_r}} \circ \cdots \circ \mathrm{Frob_{d\text{-}k_1}} \circ \varphi_N^{-1}. \end{aligned}$$

The composition of two affine transformations is an affine transformation, and the composition of two Frobenius transformations is a Frobenius transformation. This can then be simplified as

$$\begin{aligned} \mathscr{F}' &= \mathrm{Frob_k} \circ \mathscr{B}^* \circ \mathscr{F}^* \circ \mathscr{A}^* \circ \mathrm{Frob_{d\text{-}k}} \\ \mathscr{S}' &= \varphi_N \circ \mathrm{Frob_k} \circ \mathscr{A}^{*-1} \circ \varphi_N^{-1} \circ \mathscr{S} \\ \mathscr{T}' &= \mathscr{T} \circ \varphi_N \circ \mathscr{B}^{*-1} \circ \mathrm{Frob_{d\text{-}k}} \circ \varphi_N^{-1}. \end{aligned}$$

To show the uniqueness of this representation, suppose that there exists $\mathscr{A}^{*\prime}, \mathscr{B}^{*\prime} \in \mathrm{Aff}_N(\mathbb{F}_{q^d})$ and $k' \in \mathbb{N}, 0 \leqslant k < d$ leading to the same equivalent key. Then, by considering $\mathscr{S}'$, we get:

$$\begin{aligned} \varphi_N \circ \mathrm{Frob_k} \circ \mathscr{A}^{*-1} \circ \varphi_N^{-1} \circ \mathscr{S} &= \varphi_N \circ \mathrm{Frob_{k'}} \circ \mathscr{A}^{*\prime-1} \circ \varphi_N^{-1} \circ \mathscr{S} \\ \mathrm{Frob_k} \circ \mathscr{A}^{*-1} &= \mathrm{Frob_{k'}} \circ \mathscr{A}^{*\prime-1}. \end{aligned}$$

According to Lemma 6, this implies that $k' = k$ and $\mathscr{A}^{*\prime-1} = \mathscr{A}^{*-1}$. Similarly for $\mathscr{T}'$, we show that $\mathscr{B}^{*\prime-1} = \mathscr{B}^{*-1}$, i.e. the representation is unique, proving the theorem. □

We are finally able to count the total number of equivalent keys coming from Proposition 7 and Proposition 9.

Theorem 5 *Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key with parameters $(q,N,d,D) \in \mathbb{N}^4$. There are exactly*

$$d\left(q^{dN}\prod_{i=0}^{N-1}(q^{dN}-q^{d\,i})\right)^2$$

equivalent keys coming from affine transformations and Frobenius transformations.

Proof According to Theorem 4, each equivalent key is uniquely defined by two invertible affine transformations $(\mathscr{A}^*, \mathscr{B}^*) \in \mathrm{Aff}_N(\mathbb{F}_{q^d}) \times \mathrm{Aff}_N(\mathbb{F}_{q^d})$ and an integer $k, 0 \leqslant k < d$. The number of equivalent keys is the number of elements in

$$\mathrm{GL_N}(\mathbb{F}_{q^d}) \times (\mathbb{F}_{q^d})^N \times \mathrm{GL_N}(\mathbb{F}_{q^d}) \times (\mathbb{F}_{q^d})^N \times \mathbb{Z}/d\,\mathbb{Z}.$$

There are exactly $\prod_{i=0}^{N-1}\left((q^d)^N-(q^d)^i\right)$ invertible matrices in $\mathscr{M}_{N\times N}\left(\mathbb{F}_{q^d}\right)$. Thus, we obtain the expected number of keys. $\square$

5 Weaknesses of HFE/multi-HFE Induced by Equivalent Keys

We show here that the high number of equivalent keys turns out to be a weakness for HFE/Multi-HFE schemes. For example, an interesting property of the MinRank arising in HFE/Multi-HFE is that the kernel of the matrices in (8) is independent of the equivalent key used up to Frobenius transforms. To show this result (Theorem 6), we first need to prove the property for a single private key.

Lemma 7 *Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key with parameters $(q,N,d,D) \in \mathbb{N}^4$. We denote by $(\mathbf{G_1},\ldots,\mathbf{G_n}) \in (\mathscr{M}_{n\times n}(\mathbb{F}_q))^n$ the matrices associated to the public key $\mathscr{G} = \mathscr{T}\circ\mathscr{F}\circ\mathscr{S}$. Let $\mathbf{S} \in \mathscr{M}_{n\times n}(\mathbb{F}_q)$ and $\mathbf{T} \in \mathscr{M}_{n\times n}(\mathbb{F}_q)$ be the matrix representation of $\mathscr{S}$ and $\mathscr{T}$, respectively. Finally, let $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_{N,d} = [u_{i,j}] \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$, and $\mathbf{K} = \ker(\sum_{i=0}^{n-1} u_{i,0}\mathbf{G_{i+1}})$. Then $\forall t,k, 0 \leqslant t < N$, $0 \leqslant k < d$,*

$$\ker\left(\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) = \mathrm{Frob_k}\left(\mathbf{K}\right).$$

Proof Let $t, 0 \leqslant t < N$ and k, $0 \leqslant k < d$ be two integers. Using equation (6) it holds that $\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}} = \mathbf{S}\mathbf{M}_{N,d}\mathbf{F_t}^{*d,k}\mathbf{M}_{N,d}^t\mathbf{S}^t$. As $\mathbf{S}$ and $\mathbf{M}_{N,d}$ are invertible, we have that

$$\begin{aligned}
\ker\left(\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) &= \ker\left(\mathbf{S}\mathbf{M}_{N,d}\mathbf{F_t}^{*d,k}\right)\\
\ker\left(\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right)\mathbf{S}\mathbf{M}_{N,d} &= \ker\left(\mathbf{F_t}^{*d,k}\right)\\
\ker\left(\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) &= \ker\left(\mathbf{F_t}^{*d,k}\right)\mathbf{M}_{N,d}^{-1}\mathbf{S}^{-1}.
\end{aligned}$$

Recall that $\ell = \lceil \log_q(D)\rceil$. With high probability, $\ker(\mathbf{F_t}) = \ker(\mathbf{F_1}) = \mathbf{K}_{N,d,N\ell}$, $\forall t, 1 \leqslant t \leqslant N$ (see Lemma 4). From Definition 1, the non-zero columns of $\mathbf{F_t}^{*d,k}$ are the ones of $\mathbf{F_t}$ after rotating the columns of each $d\times d$ blocks from k positions. Then, rotating accordingly the columns of $\mathbf{K}_{N,d,N\ell}$ leads to a basis of $\ker(\mathbf{F_t}^{*d,k})$. This rotation is exactly the one performed by the matrix $\mathbf{P}_{N,d,-k}$ defined in Proposition 10. Then, $\ker(\mathbf{F_t}^{*d,k}) = \mathbf{K}_{N,d,N\ell}\mathbf{P}_{N,d,-k}$. As $\mathbf{P}_{N,d,-k}$ is a permutation matrix, its inverse is simply $\mathbf{P}_{N,d,k}$ (the rotation is done the other way). Finally we obtain

$$\begin{aligned}
\ker\left(\textstyle\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) &= \mathbf{K}_{N,d,N\ell}\mathbf{P}_{N,d,-k}\mathbf{M}_{N,d}^{-1}\mathbf{S}^{-1}\\
\ker\left(\textstyle\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) &= \mathbf{K}_{N,d,N\ell}\left(\mathbf{M}_{N,d}\mathbf{P}_{N,d,-k}^{-1}\right)^{-1}\mathbf{S}^{-1}\\
\ker\left(\textstyle\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) &= \mathbf{K}_{N,d,N\ell}\left(\mathbf{M}_{N,d}\mathbf{P}_{N,d,k}\right)^{-1}\mathbf{S}^{-1}.
\end{aligned}$$

The matrix $\mathbf{M}_{N,d}\mathbf{P}_{N,d,k}$ is obtained from $\mathbf{M}_{N,d}$ by rotating the columns of each $d \times d$ block to the left. Due to the construction of $\mathbf{M}_{N,d}$, this is equal to $\mathrm{Frob}_{\mathrm{k}}(\mathbf{M}_{N,d})$. Then:

$$\ker\left(\textstyle\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) = \mathbf{K}_{N,d,N\ell}\,\mathrm{Frob}_{\mathrm{k}}\left(\mathbf{M}_{N,d}\right)^{-1}\mathbf{S}^{-1}$$
$$\ker\left(\textstyle\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) = \mathbf{K}_{N,d,N\ell}\,\mathrm{Frob}_{\mathrm{k}}\left(\mathbf{M}_{N,d}^{-1}\right)\mathbf{S}^{-1}.$$

As the coefficients of $\mathbf{S}$ and $\mathbf{K}_{N,d,N\ell}$ lie in the field $\mathbb{F}_q$, this is equal to

$$\ker\left(\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) = \mathrm{Frob}_{\mathrm{k}}\left(\mathbf{K}_{N,d,N\ell}\mathbf{M}_{N,d}^{-1}\mathbf{S}^{-1}\right).$$

Finally, as $\mathbf{K}_{N,d,N\ell} = \ker(\mathbf{F_1}) = \ker(\mathbf{F_1}^{*d,0})$, we conclude:

$$\ker\left(\sum_{i=0}^{n-1} u_{i,t\,d+k}\mathbf{G_{i+1}}\right) = \mathrm{Frob}_{\mathrm{k}}\left(\ker(\mathbf{F_1}^{*d,0})\mathbf{M}_{N,d}^{-1}\mathbf{S}^{-1}\right) = \mathrm{Frob}_{\mathrm{k}}\left(\ker\left(\sum_{i=0}^{n-1} u_{i,0}\mathbf{G_{i+1}}\right)\right) = \mathrm{Frob}_{\mathrm{k}}\left(\mathbf{K}\right).$$

This proves the lemma. □

In other words, the kernel is unique up to Frobenius transformation. This property is used to prove the following theorem for any equivalent key.

Theorem 6 *Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ and $(\mathscr{F}^{*\prime}, \mathscr{S}', \mathscr{T}')$ be equivalent multi-HFE private keys and $(\mathbf{G_1}, \ldots, \mathbf{G_n}) \in \left(\mathscr{M}_{n\times n}(\mathbb{F}_q)\right)^n$ be the matrices of their associated public key. Let $(\mathbf{S}, \mathbf{T}) \in \mathscr{M}_{n\times n}(\mathbb{F}_q) \times \mathscr{M}_{n\times n}(\mathbb{F}_q)$, and $(\mathbf{S}', \mathbf{T}') \in \mathscr{M}_{n\times n}(\mathbb{F}_q) \times \mathscr{M}_{n\times n}(\mathbb{F}_q)$ be the matrix representation of $(\mathscr{S}, \mathscr{T})$, and $(\mathscr{S}', \mathscr{T}')$ respectively. Let $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_{N,d} = [u_{i,j}] \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$, and $\mathbf{K} = \ker(\sum_{i=0}^{n-1} u_{i,0}\mathbf{G_{i+1}})$. Similarly, let $\mathbf{U}' = \mathbf{T}'^{-1}\mathbf{M}_{N,d} = [u'_{i,j}] \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ and $\mathbf{K}' = \ker(\sum_{i=0}^{n-1} u'_{i,0}\mathbf{G_{i+1}})$. Then $\exists k$, $0 \leqslant k < d$, such that:*

$$\mathbf{K}' = \mathrm{Frob}_{\mathrm{k}}\left(\mathbf{K}\right).$$

Proof From Theorem 4, we can write $\mathscr{T}' = \mathscr{T} \circ \varphi_N \circ \mathscr{A}^{*-1} \circ \mathrm{Frob}_{\text{d-k}} \circ \varphi_N^{-1}$. Each of these application has a matrix representation (see Proposition 4, 8 and 10). The matrix corresponding to $\mathscr{T}'$ is then $\mathbf{T}' = \mathbf{M}_{N,d}\mathbf{P}_{N,d,d-k}\widetilde{\mathbf{A}^*}^{-1}\mathbf{M}_{N,d}^{-1}\mathbf{T}$, where $\widetilde{\mathbf{A}^*}$ has the shape of Proposition 8. Its inverse is the matrix $\mathbf{T}'^{-1} = \mathbf{T}^{-1}\mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{P}_{N,d,d-k}^{-1}\mathbf{M}_{N,d}^{-1}$. We have

$$\mathbf{U}' = \mathbf{T}'^{-1}\mathbf{M}_{N,d} = \mathbf{T}^{-1}\mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{P}_{N,d,d-k}^{-1}\mathbf{M}_{N,d}^{-1}\mathbf{M}_{N,d} = \mathbf{U}\widetilde{\mathbf{A}^*}\mathbf{P}_{N,d,k}.$$

Let $\widetilde{\mathbf{A}^*}\mathbf{P}_{N,d,k} = [a_{i,j}] \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$, we have:

$$u'_{i,j} = \sum_{t=0}^{n-1} u_{i,t}a_{t,j}, \forall i,j, 0 \leqslant i,j < n.$$

Due to the shape of $\widetilde{\mathbf{A}^*}$ and $\mathbf{P}_{N,d,k}$, $a_{t,j}$ is non-zero if and only if $t \equiv j-k \bmod d$. Then, we have $u'_{i,j} = \sum_{t=0}^{N-1} u_{i,t\,d+(j-k \bmod d)}a_{t\,d+(j-k \text{ m}}$ for all $i,j, 0 \leqslant i,j < n$. Therefore

$$\begin{aligned}\sum_{i=0}^{n-1} u'_{i,0}\mathbf{G_{i+1}} &= \sum_{i=0}^{n-1}\left(\sum_{t=0}^{N-1} u_{i,t\,d+(-k \bmod d)}a_{t\,d+(-k \bmod d),0}\right)\mathbf{G_{i+1}} \\ &= \sum_{t=0}^{N-1} a_{t\,d+(-k \bmod d),0}\left(\sum_{i=0}^{n-1} u_{i,t\,d+(-k \bmod d)}\mathbf{G_{i+1}}\right).\end{aligned}$$

We denote by $\blacksquare_{t,-k}$ the matrix $\left(\sum_{i=0}^{n-1} u_{i,t\,d+(-k \bmod d)}\mathbf{G_{i+1}}\right)$. One can see that the kernel of this matrix is the same for all $t, 0 \leqslant t < N$. Indeed, according to Lemma 7:

$$\ker\left(\blacksquare_{t,-k}\right) = \mathrm{Frob}_{\text{t d+(-k mod d) mod d}}(\mathbf{K}) = \mathrm{Frob}_{\text{-k mod d}}(\mathbf{K})\ \forall t, 0 \leqslant t < N.$$

As

$$\sum_{i=0}^{n-1} u'_{i,0}\mathbf{G_{i+1}} = \sum_{t=0}^{N-1} a_{t\,d+(-k \bmod d),0}\blacksquare_{t,-k}$$

is a linear combination of $\blacksquare_{t,-k}$ for $t, 0 \leqslant t < N$, then $\ker\left(\blacksquare_{t,-k}\right) \subseteq \ker\left(\sum_{i=0}^{n-1} u'_{i,0}\, \mathbf{G_{i+1}}\right)$. As $\mathbf{U}'$ is an equivalent key, there exists – according to (8) – a matrix $\mathbf{W}'$ such that

$$\sum_{i=0}^{n-1} u'_{i,0} \mathbf{G_{i+1}} = \mathbf{W}' \mathbf{F_1} \mathbf{W}'^t,$$

so that the rank of $\sum_{i=0}^{n-1} u'_{i,0} \mathbf{G_{i+1}}$ is $\operatorname{Rank}(\mathbf{F_1})$.

Similarly from (7), we get $\blacksquare_{t,-k} = \sum_{i=0}^{n-1} u_{i,t\,d+(-k \bmod d)} \mathbf{G_{i+1}} = \mathbf{W} \mathbf{F_{t+1}}^{*d,-k} \mathbf{W}^t$, where $\mathbf{W}$ is invertible. As rotating rows and columns of a matrix does not change its rank, it holds that

$$\operatorname{Rank}\left(\blacksquare_{t,-k}\right) = \operatorname{Rank}\left(\mathbf{F_{t+1}}^{*d,-k}\right) = \operatorname{Rank}\left(\mathbf{F_{t+1}}\right) = \operatorname{Rank}\left(\mathbf{F_1}\right) = \operatorname{Rank}\left(\sum_{i=0}^{n-1} u'_{i,0} \mathbf{G_{i+1}}\right).$$

Thus, we get $\ker\left(\blacksquare_{t,-k}\right) = \ker\left(\sum_{i=0}^{n-1} u'_{i,0} \mathbf{G_{i+1}}\right) = \mathbf{K}'$. Finally, $\mathbf{K}' = \mathrm{Frob}_{\text{-k mod d}}(\mathbf{K})$, proving the theorem. □

With Theorem 6, we know that the matrices of (8) have the same kernel (up to Frobenius transform), independently on the equivalent key chosen.

Equivalent keys allow also to further slightly improve the MinRank attack. We consider 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 $\mathbf{G_1}, \ldots, \mathbf{G_n}$ whose entries lie in $\mathbb{F}_q$ with target rank $N\ell$. Using the Kipnis-Shamir modeling described in [35, 27, 28], we have to solve the algebraic system of the $(n\,(n - N\ell))$ quadratic equations in $(N\ell\,(n-N\ell)+n)$ variables given by the entries of the matrix

$$\begin{pmatrix} 1 & & & x_{1,1} & \ldots & x_{1,N\ell} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{n-N\ell,1} & \ldots & x_{n-N\ell,N\ell} \end{pmatrix} \cdot \left(\sum_{i=1}^{n} \lambda_i \mathbf{G_i}\right). \tag{11}$$

Note that we are looking for solutions in $\mathbb{F}_{q^d}$ rather than in $\mathbb{F}_q$. From now on, and similarly to [27], these equations are called the KS (Kipnis-Shamir) equations. We denote by

$$\mathscr{I}_{\mathrm{KS}} \in \mathbb{F}_q[\{x_{i,j}\}_{1\leq i\leq n-N\ell}^{1\leq j\leq N\ell}, \lambda_1, \ldots, \lambda_n]$$

the ideal generated by the KS equations and $\mathscr{V}_{\mathrm{KS}} \subset \left(\mathbb{F}_{q^d}\right)^{N\ell(n-N\ell)+n}$ the corresponding variety.

Theorem 7 *The MinRank problem associated to HFE (resp. multi-HFE) can be solved by fixing one (resp. N) coefficient(s) to a random non-zero value (resp. to random non all zero values) in $\mathbb{F}_{q^d}$. That is, the variety $\mathscr{V}_{\mathrm{KS}}$ has at least $q^d - 1$ (resp. $q^{dN} - 1$) solutions.*

Proof We know that the first column of $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_{N,d} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ is in $\mathscr{V}_{\mathrm{KS}}$. Let $\widetilde{\mathbf{A}^*} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ be an invertible matrix as described in Proposition 8 and $\mathscr{A}^* \in \mathrm{GL_N}(\mathbb{F}_{q^d})$ be the induced transformation. According to Proposition 7, $\mathscr{A}^*$ can be used to build an equivalent key. Let then $(\mathscr{F}^{*\prime}, \mathscr{S}', \mathscr{T}')$ be an equivalent key such that $\mathscr{T}'^{-1} = \mathscr{A} \circ \mathscr{T}^{-1}$ with $\mathscr{A} = \varphi_N \circ \mathscr{A}^* \circ \varphi_N^{-1}$. Consider now the matrix representation $\mathbf{T}'^{-1}$ of $\mathscr{T}'^{-1}$. It holds that $\mathbf{T}'^{-1} = \mathbf{T}^{-1}\mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{M}_{N,d}^{-1}$. Being an equivalent key, the first column of $\mathbf{U}' = \mathbf{T}'\mathbf{M}_{N,d} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ is also in $\mathscr{V}_{\mathrm{KS}}$. Using the construction of $\mathbf{T}^{-1}$, $\mathbf{U}' = \mathbf{T}^{-1}\mathbf{M}_{N,d}\widetilde{\mathbf{A}^*}\mathbf{M}_{N,d}^{-1}\mathbf{M}_{N,d} = \mathbf{U}\widetilde{\mathbf{A}^*}$. Each column of $\widetilde{\mathbf{A}^*}$ can have at most N non-zero entries. The N non-zero entries of the first column of $\widetilde{\mathbf{A}^*}$ are $a_{0,0}, a_{d,0}, \ldots, a_{(N-1)\,d,0}$. The first column of $\mathbf{U}\widetilde{\mathbf{A}^*}$ is then

$$\underline{\lambda} = (\lambda_1, \ldots, \lambda_n) = \left(\sum_{k=0}^{n-1} u_{0,k}a_{k,0}, \ldots \sum_{k=0}^{n-1} u_{n-1,k}a_{k,0}\right)$$

$$\underline{\lambda} = \left(\sum_{k=0}^{N-1} u_{0,kd}a_{kd,0}, \ldots \sum_{k=0}^{n-1} u_{n-1,kd}a_{kd,0}\right).$$

Consider the first N components of $\underline{\lambda}$. This gives rise to a linear system of N equations:

$$\lambda_1 = \sum_{k=0}^{N-1} u_{0,kd} a_{kd,0}, \ \ldots \ , \lambda_N = \sum_{k=0}^{N-1} u_{N,kd} a_{kd,0} \, .$$

For any fixed $\lambda_1, \ldots, \lambda_N$ not all zero, this linear system has then one solution for $a_{0,0}, \ldots, a_{(N-1)d,0}$ with high probability. This allows to choose N coefficients λ_i arbitrarily and still obtain a valid solution (equivalent key). The variety $\mathscr{V}_{\mathrm{KS}}$ has then at least $q^{dN}-1$ solutions. $\square$

This means that for valid values $\{x_{i,j}\}_{1\le i\le n-N\ell}^{1\le j\le N\ell}$ in (11), there are $(q^d)^N$ 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 of the polynomial system 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 [34] for HFE is a direct consequence of Theorem 6, i.e. Frobenius images of the kernel are also valid.

The MinRank allows to recover a kernel that is central to our attack. Once $\mathbf{K} = \ker(\sum_{k=1}^n \lambda_k \mathbf{G_k})$, it is used to recover the different parts of the private key as described in the next section.

6 Full Key Recovery

In this part, we detail all the steps of a key-recovery attack against multi-HFE.

6.1 Roadmap of the attack

Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key with parameters $(q, N, d, D) \in \mathbb{N}^4$ (as defined in Sect. 2.1). The attack is divided in 3 steps.

6.1.1 Recovering the Transformation on the Polynomials

This part of the key-recovery corresponds to the MinRank problem described in Sect. 3. Solving the MinRanks of (8) allow to recover a kernel matrix $\mathbf{K}$ related to the private key and consequently the transformation $\mathscr{T}$. There are N MinRanks to be solved but we show that this has to be done only once to recover $\mathscr{T}$.

Theorem 8 *For multi-HFE, recovering $\mathbf{U} = [u_{i,j}] = \mathbf{T^{-1}} \mathbf{M}_{N,d} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ reduces to solving $N-1$ linear systems of $(n(n-N\ell))$ equations in $(n-N)$ variables in $\mathbb{F}_{q^d}$ once one column of $\mathbf{U}$ is known.*

Proof Assume w.l.o.g. that the first column of $\mathbf{U}$ is known i.e. after solving one of the MinRank of (8). We can compute the matrix $\mathbf{K} = \ker\left(\sum_{i=0}^{n-1} u_{i,0} \mathbf{G_{i+1}}\right)$. According to Lemma 7, we also have that $\mathbf{K} = \ker\left(\sum_{i=0}^{n-1} u_{i,t\,d+0} \mathbf{G_{i+1}}\right)$, $\forall t, 0 \leqslant t < N$. Thus, for all $t, 0 \leqslant t < N$, it holds that

$$\mathbf{K} \cdot \left(\textstyle\sum_{i=0}^{n-1} u_{i,t\,d+0} \mathbf{G_{i+1}}\right) = \mathbf{0}.$$

This is a linear system where the $u_{i,t\,d+0}$'s are unknown. Solving this system gives another column of the matrix $\mathbf{U}$. This has to be done $N-1$ times in order to recover $N-1$ other columns of $\mathbf{U}$. According to Proposition 6, this is enough to recover the entire matrix $\mathbf{U}$. $\square$

6.1.2 Recovering the Transformation on the Variables

Kipnis and Shamir [35] originally proposed a method for recovering the transformation on the variables by solving an overdetermined system of $(n\ell(n-\ell))$ linear equations in n^2 variables over $\mathbb{F}_q$ with $\ell = \lceil \log_q(D) \rceil$. Applied to multi-HFE, this 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. On the other hand, it operates on the big field.

Theorem 9 *For multi-HFE, recovering* $\mathbf{W} = [w_{i,j}] = \mathbf{S}\mathbf{M}_{N,d} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ *reduces to solve a linear system of* $(N\ell(n-N\ell))$ *equations in* (Nn) *variables in* $\mathbb{F}_{q^d}$ *once* $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_{N,d} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ *is known.*

Proof Let $\mathbf{K} = \ker\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}\right)$. To find the coefficients $w_{i,j}$ of $\mathbf{W}$, it is enough to remark that according to (8), $\mathbf{KW} = \ker(\mathbf{F_i})$ for all $i, 1 \leqslant i \leqslant n$. According to Lemma 4, we know that $\ker(\mathbf{F_i})$ has $N\ell$ columns set to zero. Moreover, we know that only N columns are needed to build the whole matrix $\mathbf{W}$ (see Proposition 6). We construct the corresponding linear system of $\left(N(n-N\ell)\right)$ equations in Nn variables. However, If $\ell > 1$, the system is underdetermined. To circumvent this issue, we will use Lemma 7: $\mathrm{Frob_j}(\mathbf{K}) = \ker\left(\sum_{k=0}^{n-1} u_{k,id+j}\mathbf{G_{k+1}}\right) = \ker\left(\mathbf{W}\mathbf{F_i}^{*d,j}\mathbf{W}^t\right) = \ker\left(\mathbf{W}\mathbf{F_i}^{*d,j}\right)$. Finally:

$$\ker\left(\mathbf{F_i}^{*d,j}\right) = \mathrm{Frob_j}(\mathbf{K})\mathbf{W}. \tag{12}$$

For all j, $0 \leqslant j < d$, $\ker(\mathbf{F_i}^{*d,j})$ has $N\ell$ columns set to zero (see Lemma 4). Moreover, for j, $(d-\ell+1) \leqslant j < d$, each matrix $\ker(\mathbf{F_i}^{*d,j})$ has N common zero-columns with $\ker(\mathbf{F_i}^{*d,0})$. We may then add the $N(n-N\ell)$ equations induced by (12) for each j, $(d-\ell+1) \leqslant j < d$. All in all, the system has $\left(N\ell(n-N\ell)\right)$ linear equations. This allows to recover $\mathbf{W}$ and thus $\mathscr{S}$. $\square$

Recovering $\mathscr{S}$ amounts then to solve the linear system given by the entries of

$$\mathrm{Frob_{(d\text{-}\ell+1)}}(\mathbf{K})\mathbf{W}'_{(N)} = \cdots = \mathrm{Frob_{(d\text{-}1)}}(\mathbf{K})\mathbf{W}'_{(N)} = \mathbf{K}\mathbf{W}'_{(N)} = \mathbf{0}, \tag{13}$$

where $\mathbf{W}'$ is unknown and $\mathbf{W}'_{(N)}$ denotes the N columns submatrix of $\mathbf{W}$ corresponding to the common zero columns of $\ker\left(\mathbf{F_i}^{*d,0}\right), \ldots, \ker\left(\mathbf{F_i}^{*d,d-1}\right)$ for any $i, 1 \leqslant i \leqslant N$.

6.1.3 Recovering the Inner Polynomial System

As soon as 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 (inner) transformation. This is done simply by computing $\mathscr{F}^* = \varphi_N^{-1} \circ \mathscr{T}^{-1} \circ \mathscr{G} \circ \mathscr{S}^{-1} \circ \varphi_N$. By construction of its components, the transformation $\mathscr{F}^*$ respects the HFE-shape (as defined in Sect. 2.1).

6.1.4 A Step by Step Example

To illustrate our attack, we consider a small odd characteristic example. For the sake of simplicity, we use homogeneous polynomials and linear transformations. Once again, our attack can be adapted to the affine case as explained in Sect. 6.2.

We consider the parameters $q = 7, N = 2, d = 4$, and $D = 14$. We denote $n = Nd = 8$, and $\ell = \lceil \log_q(D) \rceil = 2$. We consider $\mathbb{F}_{7^4} = \mathbb{F}_7[x]/ < x^4 + 5x^2 + 4x + 3 >$. Finally, let θ be a primitive root of the defining irreducible polynomial.

Key Generation. We choose N random polynomials having a "multi-HFE shape" of degree less than or equal to D as well as two invertible $(n \times n)$ matrices $\mathbf{S}$ and $\mathbf{T}$. To visualize the rank property, we give in Fig. 1 the symmetric matrices $\mathbf{F_i}$ associated to the polynomials F_i, i.e.:

$$F_i = \underline{X}\mathbf{F_i}\underline{X}^t \text{ where } \underline{X} = (X_1, X_1^q, \ldots, X_1^{q^{d-1}}, \ldots, X_N, X_N^q, \ldots, X_N^{q^{d-1}}).$$

The public key of this multi-HFE instance is a set of n quadratic polynomials $(g_1, \ldots, g_n)$. We give in Fig. 2 the symmetric matrix representation $\mathbf{G_i}$ of each g_i, i.e.:

$$g_i = (x_1, \ldots, x_n)\,\mathbf{G_i}\,(x_1, \ldots, x_n)^t.$$

$$
\begin{aligned}
F_1 &= \theta^{2097}X_1^{14} + \theta^{2150}X_1^{8} + \theta^{1623}X_1^{7}X_2^{7} + \theta^{481}X_1^{7}X_2 + \theta^{1131}X_1^{2} \\
&\quad + \theta^{83}X_1X_2^{7} + \theta^{1779}X_1X_2 + \theta^{940}X_2^{14} + \theta^{1075}X_2^{8} + \theta^{1220}X_2^{2}, \\
F_2 &= \theta^{1586}X_1^{14} + \theta^{899}X_1^{8} + \theta^{1078}X_1^{7}X_2^{7} + \theta^{554}X_1^{7}X_2 + \theta^{260}X_1^{2} \\
&\quad + \theta^{1709}X_1X_2^{7} + \theta^{1971}X_1X_2 + \theta^{1090}X_2^{14} + \theta^{287}X_2^{8} + \theta^{179}X_2^{2}.
\end{aligned}
$$

$$
\mathbf{F_1} = \begin{pmatrix}
\theta^{1131} & \theta^{1350} & 0 & 0 & \theta^{979} & \theta^{1683} & 0 & 0 \\
\theta^{1350} & \theta^{2097} & 0 & 0 & \theta^{2081} & \theta^{823} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\theta^{979} & \theta^{2081} & 0 & 0 & \theta^{1220} & \theta^{275} & 0 & 0 \\
\theta^{1683} & \theta^{823} & 0 & 0 & \theta^{275} & \theta^{940} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}, \mathbf{F_2} = \begin{pmatrix}
\theta^{260} & \theta^{99} & 0 & 0 & \theta^{1171} & \theta^{909} & 0 & 0 \\
\theta^{99} & \theta^{1586} & 0 & 0 & \theta^{2154} & \theta^{278} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\theta^{1171} & \theta^{2154} & 0 & 0 & \theta^{179} & \theta^{1887} & 0 & 0 \\
\theta^{909} & \theta^{278} & 0 & 0 & \theta^{1887} & \theta^{1090} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
$$

$$
\mathbf{S} = \begin{pmatrix}
0 & 0 & 5 & 3 & 6 & 4 & 4 & 2 \\
5 & 6 & 2 & 0 & 1 & 6 & 6 & 1 \\
5 & 5 & 1 & 6 & 4 & 5 & 3 & 1 \\
3 & 4 & 1 & 4 & 3 & 5 & 0 & 6 \\
1 & 2 & 2 & 1 & 2 & 2 & 6 & 0 \\
1 & 2 & 3 & 5 & 3 & 0 & 3 & 3 \\
1 & 3 & 3 & 6 & 2 & 1 & 0 & 0 \\
4 & 0 & 3 & 0 & 0 & 0 & 2 & 2
\end{pmatrix}, \qquad \mathbf{T} = \begin{pmatrix}
2 & 2 & 3 & 4 & 6 & 1 & 6 & 0 \\
4 & 6 & 6 & 1 & 3 & 0 & 1 & 4 \\
6 & 0 & 3 & 1 & 1 & 5 & 3 & 6 \\
1 & 0 & 0 & 5 & 1 & 2 & 4 & 3 \\
5 & 0 & 3 & 3 & 6 & 4 & 3 & 3 \\
0 & 6 & 5 & 5 & 0 & 4 & 6 & 0 \\
1 & 5 & 4 & 0 & 6 & 3 & 2 & 3 \\
0 & 2 & 2 & 2 & 2 & 6 & 0 & 5
\end{pmatrix}.
$$

Fig. 1 Private key of the Multi-HFE example with $q = 7$, $N = 2$, $d = 4$, and $D = 14$.

$$
\mathbf{G_1} = \begin{pmatrix}
3 & 0 & 0 & 6 & 5 & 1 & 1 & 1 \\
0 & 3 & 3 & 1 & 4 & 6 & 4 & 4 \\
0 & 3 & 4 & 5 & 3 & 5 & 5 & 4 \\
6 & 1 & 5 & 2 & 2 & 4 & 4 & 2 \\
5 & 4 & 3 & 2 & 1 & 0 & 4 & 4 \\
1 & 6 & 5 & 4 & 0 & 1 & 2 & 2 \\
1 & 4 & 5 & 4 & 4 & 2 & 0 & 1 \\
1 & 4 & 4 & 2 & 4 & 2 & 1 & 2
\end{pmatrix}, \mathbf{G_2} = \begin{pmatrix}
3 & 5 & 6 & 4 & 6 & 6 & 2 & 6 \\
5 & 1 & 6 & 0 & 5 & 4 & 0 & 5 \\
6 & 6 & 6 & 1 & 6 & 3 & 1 & 6 \\
4 & 0 & 1 & 4 & 3 & 0 & 0 & 0 \\
6 & 5 & 6 & 3 & 6 & 2 & 5 & 1 \\
6 & 4 & 3 & 0 & 2 & 5 & 3 & 2 \\
2 & 0 & 1 & 0 & 5 & 3 & 0 & 0 \\
6 & 5 & 6 & 0 & 1 & 2 & 0 & 6
\end{pmatrix}, \mathbf{G_3} = \begin{pmatrix}
3 & 5 & 2 & 4 & 1 & 4 & 2 & 4 \\
5 & 5 & 1 & 3 & 3 & 5 & 5 & 0 \\
2 & 1 & 4 & 4 & 1 & 0 & 4 & 2 \\
4 & 3 & 4 & 6 & 1 & 2 & 4 & 6 \\
1 & 3 & 1 & 1 & 0 & 5 & 4 & 2 \\
4 & 5 & 0 & 2 & 5 & 1 & 4 & 6 \\
2 & 5 & 4 & 4 & 4 & 4 & 4 & 6 \\
4 & 0 & 2 & 6 & 2 & 6 & 6 & 6
\end{pmatrix},
$$

$$
\mathbf{G_4} = \begin{pmatrix}
1 & 5 & 0 & 0 & 3 & 1 & 0 & 6 \\
5 & 5 & 5 & 3 & 2 & 1 & 1 & 4 \\
0 & 5 & 5 & 3 & 3 & 4 & 2 & 0 \\
0 & 3 & 3 & 4 & 3 & 6 & 5 & 5 \\
3 & 2 & 3 & 3 & 3 & 5 & 1 & 4 \\
1 & 1 & 4 & 6 & 5 & 6 & 4 & 0 \\
0 & 1 & 2 & 5 & 1 & 4 & 0 & 3 \\
6 & 4 & 0 & 5 & 4 & 0 & 3 & 5
\end{pmatrix}, \mathbf{G_5} = \begin{pmatrix}
4 & 2 & 6 & 6 & 2 & 6 & 5 & 5 \\
2 & 3 & 4 & 2 & 2 & 5 & 3 & 0 \\
6 & 4 & 6 & 0 & 4 & 3 & 6 & 5 \\
6 & 2 & 0 & 0 & 2 & 5 & 2 & 5 \\
2 & 2 & 4 & 2 & 1 & 4 & 0 & 2 \\
6 & 5 & 3 & 5 & 4 & 0 & 2 & 0 \\
5 & 3 & 6 & 2 & 0 & 2 & 3 & 0 \\
5 & 0 & 5 & 5 & 2 & 0 & 0 & 3
\end{pmatrix}, \mathbf{G_6} = \begin{pmatrix}
2 & 0 & 2 & 6 & 2 & 4 & 2 & 3 \\
0 & 6 & 0 & 2 & 3 & 6 & 1 & 5 \\
2 & 0 & 2 & 4 & 6 & 0 & 6 & 1 \\
6 & 2 & 4 & 0 & 2 & 0 & 0 & 1 \\
2 & 3 & 6 & 2 & 4 & 3 & 1 & 4 \\
4 & 6 & 0 & 0 & 3 & 6 & 4 & 6 \\
2 & 1 & 6 & 0 & 1 & 4 & 5 & 1 \\
3 & 5 & 1 & 1 & 4 & 6 & 1 & 2
\end{pmatrix},
$$

$$
\mathbf{G_7} = \begin{pmatrix}
6 & 2 & 2 & 0 & 4 & 0 & 1 & 4 \\
2 & 4 & 2 & 6 & 3 & 2 & 3 & 1 \\
2 & 2 & 1 & 5 & 1 & 0 & 4 & 4 \\
0 & 6 & 5 & 1 & 5 & 6 & 4 & 5 \\
4 & 3 & 1 & 5 & 1 & 2 & 4 & 4 \\
0 & 2 & 0 & 6 & 2 & 5 & 4 & 6 \\
1 & 3 & 4 & 4 & 4 & 4 & 3 & 5 \\
4 & 1 & 4 & 5 & 4 & 6 & 5 & 6
\end{pmatrix}, \mathbf{G_8} = \begin{pmatrix}
6 & 1 & 3 & 4 & 5 & 4 & 3 & 6 \\
1 & 0 & 1 & 5 & 3 & 6 & 6 & 6 \\
3 & 1 & 3 & 0 & 1 & 0 & 6 & 4 \\
4 & 5 & 0 & 6 & 5 & 0 & 5 & 0 \\
5 & 3 & 1 & 5 & 6 & 6 & 1 & 5 \\
4 & 6 & 0 & 0 & 6 & 2 & 4 & 2 \\
3 & 6 & 6 & 5 & 1 & 4 & 2 & 2 \\
6 & 6 & 4 & 0 & 5 & 2 & 2 & 4
\end{pmatrix}.
$$

Fig. 2 Public key (given as matrices) of the Multi-HFE example considered with $q = 7$, $N = 2$, $d = 4$, and $D = 14$.

Recovering an Equivalent $\mathscr{T}$. The first step is to solve a MinRank problem. By construction, there exists a non-zero vector $(\lambda_1, \ldots, \lambda_n) \in \left(\mathbb{F}_{q^d}\right)^n$ such that $\mathrm{Rank}(\sum_{i=1}^{n} \lambda_i \mathbf{G_i}) = N\ell$ (Theorem 3). According to Sect. 5, we can randomly fix N variables to have a zero-dimensional ideal.

We fix for instance $\lambda_1 = 1$ and $\lambda_2 = 0$. Using the notations of Sect. 2.4, we have to solve a MinRank with $(\mathbf{M_0} = -\mathbf{G_1}, \mathbf{M_1}, \ldots, \mathbf{M_6} = \mathbf{G_3}, \ldots, \mathbf{G_8})$ with $n = Nd = 8, k = n - N = 6$, $r = N\ell = 4$. We have $d = 4$ solutions given by the vector

$$
\underline{\lambda}^{(1)} = (1, 0, \theta^{110}, \theta^{2215}, \theta^{830}, \theta^{1958}, \theta^{1889}, \theta^{2363})
$$

as well as its Frobenius images $\mathrm{Frob_j}(\underline{\lambda}^{(1)})$ for all $j, 0 \leqslant j < d$. This is a direct consequence of Proposition 9 from Sect. 4. The kernel $\mathbf{K}$ of $(\sum_{i=1}^{n} \lambda_i^{(1)} \mathbf{G_i})$ can be computed, and we get the matrix

$$\mathbf{K} = \begin{pmatrix} 1\ 0\ 0\ 0 & \theta^{828} & \theta^{1612} & \theta^{530} & \theta^{1086} \\ 0\ 1\ 0\ 0 & \theta^{502} & \theta^{134} & \theta^{1450} & \theta^{566} \\ 0\ 0\ 1\ 0 & \theta^{1981} & \theta^{1755} & \theta^{1660} & \theta^{2059} \\ 0\ 0\ 0\ 1 & \theta^{870} & \theta^{963} & \theta^{2276} & \theta^{425} \end{pmatrix}.$$

This matrix is then used to recover N columns of $\mathbf{U}' = \mathbf{T}'^{-1}\mathbf{M}_{N,d}$ according to Theorem 8. In our example, we need only one more column as $N = 2$. This amounts to solve the linear system $\mathbf{K}\,(\sum_{i=1}^{n} \lambda_i \mathbf{G_i}) = \mathbf{0}$. As pointed again in Theorem 8, this is enough to recover the whole matrix $\mathbf{U}$. To have independent columns, we fix $\lambda_1 = 0$ and $\lambda_2 = 1$. Solving this linear system gives

$$\underline{\lambda}^{(2)} = (0, 1, \theta^{1587}, \theta^{2150}, \theta^{59}, \theta^{1111}, \theta^{1093}, \theta^{1656}).$$

The matrix $\mathbf{U}'$ is finally reconstructed by taking the Frobenius of these vectors $\underline{\lambda}^{(1)}$ and $\underline{\lambda}^{(2)}$:

$$\mathbf{U}' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \theta^{110} & \theta^{770} & \theta^{590} & \theta^{1730} & \theta^{1587} & \theta^{1509} & \theta^{963} & \theta^{1941} \\ \theta^{2215} & \theta^{1105} & \theta^{535} & \theta^{1345} & \theta^{2150} & \theta^{650} & \theta^{2150} & \theta^{650} \\ \theta^{830} & \theta^{1010} & \theta^{2270} & \theta^{1490} & \theta^{59} & \theta^{413} & \theta^{491} & \theta^{1037} \\ \theta^{1958} & \theta^{1706} & \theta^{2342} & \theta^{1994} & \theta^{1111} & \theta^{577} & \theta^{1639} & \theta^{1873} \\ \theta^{1889} & \theta^{1223} & \theta^{1361} & \theta^{2327} & \theta^{1093} & \theta^{451} & \theta^{757} & \theta^{499} \\ \theta^{2363} & \theta^{2141} & \theta^{587} & \theta^{1709} & \theta^{1656} & \theta^{1992} & \theta^{1944} & \theta^{1608} \end{pmatrix}.$$

The secret matrix $\mathbf{T}' = \mathbf{M}_{N,d}\mathbf{U}'^{-1}$ has been recovered at this step:

$$\mathbf{T}' = \begin{pmatrix} 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ 5\ 5\ 5\ 0\ 3\ 3\ 3\ 1 \\ 6\ 2\ 0\ 5\ 0\ 0\ 5\ 5 \\ 0\ 5\ 6\ 1\ 1\ 2\ 4\ 5 \\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ 1\ 3\ 2\ 4\ 4\ 2\ 6\ 4 \\ 3\ 0\ 1\ 3\ 3\ 5\ 2\ 6 \\ 1\ 6\ 6\ 3\ 5\ 2\ 0\ 3 \end{pmatrix}.$$

Recovering an Equivalent $\mathscr{S}$. We follow the method explained in Sect. 6.1.2 to recover a valid matrix $\mathbf{W}' = \mathbf{S}'\mathbf{M}_{N,d}$. Even if the matrices $\mathbf{F_1}$ and $\mathbf{F_2}$ of the private key are unknown, we know due to the HFE-shape that in echelon form we have for all i, $1 \leqslant i \leqslant N$:

$$\ker(\mathbf{F_i}) = \begin{pmatrix} 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1 \end{pmatrix}, \qquad \ker\left(\mathbf{F_i}^{*d,(d-1)}\right) = \begin{pmatrix} 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0 \end{pmatrix}.$$

These two matrices have both their $(i\,d)$-th columns set to zero for $0 \leqslant i < N$ (i.e. columns 0 and 4). We now construct a linear system of $N\,(n - N\ell)$ equations in the $N\,n$ variables $\gamma_{1,1}, \ldots, \gamma_{1,n}, \ldots, \gamma_{N,1}, \ldots, \gamma_{N,n}$ from

$$\mathbf{K} \cdot \begin{pmatrix} \gamma_{1,1} & \gamma_{2,1} \\ \vdots & \vdots \\ \gamma_{1,n} & \gamma_{2,n} \end{pmatrix} = \mathbf{0}, \qquad \mathrm{Frob_{d\text{-}1}}(\mathbf{K}) \cdot \begin{pmatrix} \gamma_{1,1} & \gamma_{2,1} \\ \vdots & \vdots \\ \gamma_{1,n} & \gamma_{2,n} \end{pmatrix} = \mathbf{0}.$$

The system has $(q^d)^N$ solutions. This is again a consequence of equivalent keys explained in Sect. 4. We then randomly set N variables in each one of the N columns to arbitrary values. For this example, we take $\gamma_{1,1} =$

$1, \gamma_{1,2} = 0, \gamma_{2,1} = 0, \gamma_{2,2} = 1$ (the columns have to be linearly independent). This linear system has one solution providing two vectors:

$$\underline{w}^{(1)} = (1, 0, \theta^{75}, \theta^{66}, \theta^{314}, \theta^{132}, \theta^{1308}, \theta^{2017}),$$
$$\underline{w}^{(2)} = (0, 1, \theta^{505}, \theta^{1673}, \theta^{1960}, \theta^{1947}, \theta^{733}, \theta^{1788}).$$

As for $\mathbf{U}'$, the rest of the matrix is built by raising the first columns to the power of q^j, for all j, $0 < j < d$.

$$\mathbf{W}' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \theta^{75} & \theta^{525} & \theta^{1275} & \theta^{1725} & \theta^{505} & \theta^{1135} & \theta^{745} & \theta^{415} \\ \theta^{66} & \theta^{462} & \theta^{834} & \theta^{1038} & \theta^{1673} & \theta^{2111} & \theta^{377} & \theta^{239} \\ \theta^{314} & \theta^{2198} & \theta^{986} & \theta^{2102} & \theta^{1960} & \theta^{1720} & \theta^{40} & \theta^{280} \\ \theta^{132} & \theta^{924} & \theta^{1668} & \theta^{2076} & \theta^{1947} & \theta^{1629} & \theta^{1803} & \theta^{621} \\ \theta^{1308} & \theta^{1956} & \theta^{1692} & \theta^{2244} & \theta^{733} & \theta^{331} & \theta^{2317} & \theta^{1819} \\ \theta^{2017} & \theta^{2119} & \theta^{433} & \theta^{631} & \theta^{1788} & \theta^{516} & \theta^{1212} & \theta^{1284} \end{pmatrix}.$$

The matrix $\mathbf{S}' = \mathbf{W}'\mathbf{M}_{N,d}^{-1}$, which is part of a private key has been then recovered:

$$\mathbf{S}' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 4 & 1 & 6 & 5 & 2 & 2 & 0 \\ 1 & 6 & 5 & 0 & 5 & 3 & 3 & 0 \\ 0 & 4 & 3 & 0 & 6 & 3 & 5 & 0 \\ 3 & 3 & 5 & 4 & 2 & 3 & 1 & 4 \\ 2 & 0 & 6 & 4 & 0 & 4 & 0 & 3 \\ 6 & 3 & 1 & 2 & 4 & 3 & 0 & 6 \end{pmatrix}.$$

Recovering an Equivalent $\mathscr{F}$. To conclude the attack, we have to recover a valid inner transformation. From the knowledge of $\mathbf{S}'$ and $\mathbf{T}'$, we compute:

$$\mathscr{F}^{*\prime} = \varphi_N^{-1} \circ \mathscr{T}'^{-1} \circ \mathscr{G} \circ \mathscr{S}'^{-1} \circ \varphi_N.$$

In terms of matrix/vector operations, we first compute the small field representation of $\mathscr{F}^{*\prime}$:

$$\mathscr{F}' = \mathscr{T}'^{-1} \circ \mathscr{G} \circ \mathscr{S}'^{-1}$$
$$(\mathbf{H_1}', \ldots, \mathbf{H_n}') = (\mathbf{S}'^{-1}\mathbf{G_1}\mathbf{S}'^{-t}, \ldots, \mathbf{S}'^{-1}\mathbf{G_n}\mathbf{S}'^{-t})\,\mathbf{T}'^{-1}.$$

Then, we recover the transformation on the big field using the matrix $\mathbf{M}_{N,d}$ of Proposition 4.

$$\mathscr{F}^{*\prime} = \varphi_N^{-1} \circ \mathscr{F}' \circ \varphi_N$$
$$(\mathbf{F_1}', \ldots, \mathbf{F_N}') = (\mathbf{P_1}, \mathbf{P_{d+1}}, \ldots, \mathbf{P_{d(N-1)+1}})$$
$$\text{where } (\mathbf{P_1}, \ldots, \mathbf{P_n}) = (\mathbf{M}_{N,d}^{-1}\mathbf{H_1}'\mathbf{M}_{N,d}^{-t}, \ldots, \mathbf{M}_{N,d}^{-1}\mathbf{H_n}'\mathbf{M}_{N,d}^{-t})\,\mathbf{M}_{N,d}.$$

From the definitions of matrices $\mathbf{U}'$ and $\mathbf{W}'$, it is equivalent (and simpler) to directly compute

$$\mathscr{F}^{*\prime} = \varphi_N^{-1} \circ \mathscr{T}'^{-1} \circ \mathscr{G} \circ \mathscr{S}'^{-1} \circ \varphi_N.$$
$$(\mathbf{F_1}', \ldots, \mathbf{F_N}') = (\mathbf{P_1}, \mathbf{P_{d+1}}, \ldots, \mathbf{P_{d(N-1)+1}})$$
$$\text{where } (\mathbf{P_1}, \ldots, \mathbf{P_n}) = (\mathbf{W}'^{-1}\mathbf{G_1}\mathbf{W}'^{-t}, \ldots, \mathbf{W}'^{-1}\mathbf{G_n}\mathbf{W}'^{-t})\,\mathbf{U}'.$$

With the matrices $\mathbf{F_1}', \ldots, \mathbf{F_N}'$, we recover a set of HFE-shaped polynomials. In our example, we obtain

$$\mathbf{F_1}' = \begin{pmatrix} \theta^{784} & \theta^{1599} & 0 & 0 & \theta^{173} & \theta^{2089} & 0 & 0 \\ \theta^{1599} & \theta^{1581} & 0 & 0 & \theta^{59} & \theta^{709} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \theta^{173} & \theta^{59} & 0 & 0 & \theta^{157} & \theta^{1724} & 0 & 0 \\ \theta^{2089} & \theta^{709} & 0 & 0 & \theta^{1724} & \theta^{1791} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$
\mathbf{F_2}' = \begin{pmatrix}
\theta^{2277} & \theta^{375} & 0 & 0 & \theta^{321} & \theta^{1681} & 0 & 0 \\
\theta^{375} & \theta^{749} & 0 & 0 & \theta^{665} & \theta^{227} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\theta^{321} & \theta^{665} & 0 & 0 & \theta^{1384} & \theta^{510} & 0 & 0 \\
\theta^{1681} & \theta^{227} & 0 & 0 & \theta^{510} & \theta^{1556} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
$$

Thus

$$
\begin{aligned}
F_1' &= \theta^{1581}X_1^{14} + \theta^{2399}X_1^{8} + \theta^{1509}X_1^{7}X_2^{7} + \theta^{859}X_1^{7}X_2 + \theta^{784}X_1^{2} \\
&\quad + \theta^{489}X_1X_2^{7} + \theta^{973}X_1X_2 + \theta^{1791}X_2^{14} + \theta^{124}X_2^{8} + \theta^{157}X_2^{2} \\
F_2' &= \theta^{749}X_1^{14} + \theta^{1175}X_1^{8} + \theta^{1027}X_1^{7}X_2^{7} + \theta^{1465}X_1^{7}X_2 + \theta^{2277}X_1^{2} \\
&\quad + \theta^{81}X_1X_2^{7} + \theta^{1121}X_1X_2 + \theta^{1556}X_2^{14} + \theta^{1310}X_2^{8} + \theta^{1384}X_2^{2}.
\end{aligned}
$$

The attack is now complete and a full valid private key has been recovered.

6.2 Affine Transformations

So far, we have only considered linear transformations and homogeneous polynomials. However, HFE or multi-HFE can use affine transformations and non-homogeneous polynomials. We describe here how to generalize our approach to the affine case.

6.2.1 Representation

The starting idea of our attack is to represent the polynomials in a matrix form. If the HFE-shaped polynomial $F_i \in \mathbb{F}_{q^d}[X_1,\ldots,X_N]$ is not homogeneous, then there exists a matrix $\mathbf{F_i} \in \mathscr{M}_{(n+1)\times(n+1)}\left(\mathbb{F}_{q^d}\right)$ such that $F_i = \underline{X}\mathbf{F_i}\underline{X}^t$ where $\mathbf{F_i}$ is symmetric and $\underline{\widetilde{X}} = (X_1, X_1^q, \ldots, X_1^{q^{d-1}}, \ldots, X_N, X_N^q, \ldots, X_N^{q^{d-1}}, 1)$. Similarly, if a quadratic polynomial $g_i \in \mathbb{F}_q[x_1,\ldots,x_n]$ is not homogeneous, then we can write $g_i = \underline{x}\mathbf{G_i}\underline{x}^t$ where $\mathbf{G_i} \in \mathscr{M}_{(n+1)\times(n+1)}(\mathbb{F}_q)$ is symmetric and $\underline{x} = (x_1,\ldots,x_n,1)$.

The matrix $\mathbf{M}_{N,d}$ – allowing to change basis – given in Proposition 4 simply becomes

$$
\begin{pmatrix}
\mathbf{M}_{N,d} & & 0 \\
 & & \vdots \\
0 & \cdots & 1
\end{pmatrix}.
$$

The matrix representations of the secret polynomials $F_1,\ldots,F_N$ have however $(n+1)$ rows and columns instead of n. The rank of such matrices is $(N\ell+1)$ (one row and column have been added). In our attack, we then try to find an affine combination of the public polynomials such that the rank of its corresponding matrix representation is $(N\ell+1)$.

6.2.2 MinRank attack

To adapt the MinRank attack, we remark that it is possible to find a linear combination of the matrices instead of an affine combination. Thanks to equivalent keys (cf. Sect. 4) such linear combination exists. The problem is then to find $(u_{0,0},\ldots,u_{n-1,0}) \in (\mathbb{F}_{q^d})^n$ such that

$$
\operatorname{Rank}\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}\right) = N\ell+1.
$$

We recover in this way a matrix $\mathbf{U} \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ as explained in 6.1. For the second step, the matrix $\mathbf{K} = \ker\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}\right)$ has $(n+1)$ columns. To have an analogous property, the last column of $\mathbf{K}$ is set to zero i.e.

$$\mathbf{K} = \begin{pmatrix} 1 & 0 & \dots\dots & 0 & k_{0,0} & \dots & k_{0,N} & 0 \\ 0 & 1 & & \vdots & \vdots & \dots & \vdots & \vdots \\ \vdots & & \ddots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & \dots\dots & 0 & 1 & k_{n-N,0} & \dots & k_{n-N,N} & 0 \end{pmatrix}$$

The first n columns of $\mathbf{K}$ can be used to perform the second step of the attack just as in Sect. 6.

The method described above is the most straightforward and natural. However, there are at least two other ways of performing the MinRank attack.

Take the homogeneous part. The idea is to ignore the affine part. Namely, we perform the MinRank attack on the homogeneous part of the polynomials. That is, we try to find $(u_{0,0},\dots,u_{n-1,0}) \in (\mathbb{F}_d)^n$ such that

$$\mathrm{Rank}\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}^h\right) = N\ell$$

where $\mathbf{G_i}^h \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ is the matrix of the homogeneous part of g_i (i.e. the matrix $\mathbf{G_i}$ without the last row and column).

Since the rank of $\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}^h\right)$ is $N\ell$, $\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}\right)$ is of rank $N\ell+1$. We added one more row and column. The attack is completed as we have found a linear combination such that the rank is $N\ell+1$. From a practical point of view, this method turns to be less efficient than the first one. This is probably due to the fact that the information coming from the non-homogeneous part is not used.

Add a constant polynomial. We consider a third strategy. We look for a private equivalent key such that $\mathscr{F}$ is homogeneous. This way, the rank of their matrices is $N\ell$ instead of $(N\ell+1)$. We are then looking for an affine combination of the public polynomials. Namely, we compute $(u_{0,0},\dots,u_{n,0}) \in (\mathbb{F}_{q^d})^{n+1}$ such that

$$\mathrm{Rank}\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} + u_{n,0}\mathbf{I}\right) = N\ell$$

where $\mathbf{I}$ is the matrix of the constant polynomial 1 (i.e. $\mathbf{I}[i,j] = 1$ if $i = j = n+1$ and 0 otherwise).

In this case, we try to cancel the affine part of $\left(\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}}\right)$ such that its rank is $N\ell$ instead of $N\ell+1$. Note that in this method, we move the affine part of the inner polynomials to the matrix $\mathbf{U}$ and try to find an homogeneous internal transformation. Note that using only the first n components $(u_{0,0},\dots,u_{n-1,0})$ of the solution leads back to the first method as the linear combination is of rank $(N\ell+1)$ (only one entry is modified).

Experimentally, this method is the most efficient for the non-homogeneous case. This can be explained by the fact that the rank is lower and the affine part is taken into account.

6.3 Key Recovery in Characteristic 2

Our attack uses the matrix representation of the public and secret polynomials. This representation has to be symmetric in order to keep a canonical representation of the quadratic forms. Let $\mathbf{A}$ be a matrix representing some quadratic form. The symmetric representation is obtained by computing $\frac{\mathbf{A}+\mathbf{A}^t}{2}$. In characteristic 2, such a matrix would be zero.

In their original paper, Kipnis and Shamir [35] suggest to use instead $\mathbf{A}+\mathbf{A}^t$. Whilst the first step of the attack (MinRank) works indeed similarly, it appears that the second step of the attack – recovering $\mathscr{S}$ – fails with the method described in Sect. 6.1. In characteristic 2, the two steps are not independent and cannot be treated separately. We now discuss how to adapt our attack in characteristic 2. For reasons which will be explained, our adaptation depends on the parity of the rank. Thus, the section is divided in two parts. From now on, we denote by $r = N\ell$ the target rank of the MinRank. A toy example of our attack is given in Appendix A.

6.3.1 Even Rank.

The first part of the attack is to find a linear combination of the public matrices whose rank is r. For HFE, any solution $(\lambda_1,\ldots,\lambda_n)\in(\mathbb{F}_{q^d})^n$ of the MinRank leads to another solution $\alpha(\lambda_1^{q^i},\ldots,\lambda_n^{q^i})$, for any $\alpha\in\mathbb{F}_{q^d}^*$, and any $i, 0\leqslant i<d$. This is due to equivalent keys as detailed in Sect. 4.

In characteristic 2, it has been noticed [34] that $\forall(\alpha,\beta)\in\mathbb{F}_{q^d}^*\times\mathbb{F}_{q^d}$, a vector $\alpha(\lambda_1^{q^i},\ldots,\lambda_n^{q^i})+\beta(\lambda_1^{q^{i+1}},\ldots,\lambda_n^{q^{i+1}})$ is also solution if r is even. As a consequence, the ideal generated by the MinRank equations when r is even has dimension at least 1 (we can fix any value for β).

Assume then that we fix a random value for λ_1. Even after that, the MinRank problem has q^d-1 solutions (and their Frobenius images). That is $d\,(q^d-1)$ in total. To decrease the number of solutions (i.e. to have only d solutions), we can try to fix one more variable as suggested in [34]. A matrix $\mathbf{T}'$ can be computed, but there is an issue on the second step of the attack (recovering $\mathbf{S}'$). The linear system allowing to recover $\mathbf{S}'$ has no solution, which means that the $\mathbf{T}'$ computed is not valid. This suggests a relation between the different steps of the attack in characteristic 2.

The problem is that only solutions with $\beta=0$ are actually equivalent keys. The solutions coming from $\beta\neq0$ are not equivalent keys obtained from the affine and Frobenius transformations as described in Sect. 4. They appear to be spurious solutions. Thus, if we fix another variable as in [34], it is very likely that the matrix $\mathbf{T}'$ that will be recovered does not lead to an equivalent secret key. In the other hand, not fixing another variable leads to an ideal of dimension at least 1 with an exponential number of solutions. As a consequence, the two parts of the attack cannot be treated separately. Recall that $\ell=\lceil\log_q(D)\rceil$. We need both

$$\mathrm{Rank}\left(\textstyle\sum_{i=1}^n\lambda_i\mathbf{G_i}\right)=N\ell\qquad\text{and}\qquad\ker\left(\textstyle\sum_{i=1}^n\lambda_i\mathbf{G_i}\right)\mathbf{W}'=\ker(\mathbf{F_1}).$$

Let $\mathbf{K}$ be the unknown kernel of $(\sum_{i=1}^n\lambda_i\mathbf{G_i})$, and let $\mathbf{W}'_{(N)}$ be the N columns matrix obtained from $\mathbf{W}'$ according to Sect 6.1.2. Thanks to (13), we have to solve:

$$\mathbf{K}\cdot\left(\textstyle\sum_{i=1}^n\lambda_i\mathbf{G_i}\right)=\mathbf{0}\qquad\text{and}\qquad\begin{cases}\mathrm{Frob}_{(\text{d-}\ell+1)}(\mathbf{K})\mathbf{W}'_{(N)}=\mathbf{0},\\ \vdots\\ \mathrm{Frob}_{(\text{d-1})}(\mathbf{K})\mathbf{W}'_{(N)}=\mathbf{0},\\ \mathbf{K}\mathbf{W}'_{(N)}=\mathbf{0}.\end{cases}$$

In our case $\mathbf{K}$ is unknown, thus the Frobenius transforms add equations of degree up to q^{d-1}. To avoid this, for any $k, 0\leqslant k<d$ we use that

$$\mathrm{Frob}_{\text{d-k}}\left(\mathrm{Frob}_{\text{k}}(\mathbf{K})\mathbf{W}'_{(N)}\right)=\mathrm{Frob}_{\text{d-k}}(\mathrm{Frob}_{\text{k}}(\mathbf{K}))\,\mathrm{Frob}_{\text{d-k}}(\mathbf{W}'_{(N)})=\mathbf{K}\,\mathrm{Frob}_{\text{d-k}}(\mathbf{W}'_{(N)}).$$

As $\mathrm{Frob}_{\text{k}}(\mathbf{K})\mathbf{W}'_{(N)}=\mathbf{0}$, we have $\mathbf{K}\,\mathrm{Frob}_{\text{d-k}}(\mathbf{W}'_{(N)})=\mathrm{Frob}_{\text{d-k}}(\mathbf{0})=\mathbf{0}$. Thus, we use instead the following equations:

$$\mathbf{K}\cdot\left(\textstyle\sum_{i=1}^n\lambda_i\mathbf{G_i}\right)=\mathbf{0}\qquad\text{and}\qquad\begin{cases}\mathbf{K}\,\mathrm{Frob}_{\ell\text{-1}}(\mathbf{W}'_{(N)})=\mathbf{0},\\ \vdots\\ \mathbf{K}\,\mathrm{Frob}_{1}(\mathbf{W}'_{(N)})=\mathbf{0},\\ \mathbf{K}\mathbf{W}'_{(N)}=\mathbf{0}.\end{cases}$$

We use also the representation of the entries of $\mathbf{W}'$ as a vector over $\mathbb{F}_2$ using the mapping φ_N. As $\mathbf{W}'=\mathbf{S}'\mathbf{M}_{N,d}$, we have $w'_{i,j}=\sum_{k=0}^{d-1}\theta^{k(q^j \bmod d)}s'_{i,d\lfloor j/d\rfloor+k}$ with $s'_{i,j}\in\mathbb{F}_2$ for $0\leqslant i,j<n$. Since the Frobenius transform is linear over $\mathbb{F}_2$, the degree does not increase. The field equations $s'^2_{i,j}-s'_{i,j}=0$ can also be added.

Finally, the system to be solved is the union of two overdetermined bi-linear systems [29]. The system has $r\,(n-r)$ variables coming from $\mathbf{K}, n$ coming from the λ_i's, and $d\,N\,n$ coming from $\mathbf{S}'$. There are $n\,(n-r)$ equations coming from $\mathbf{K}\cdot(\sum_{i=1}^n\lambda_i\mathbf{G_i})=0$, $\ell N\,(n-r)$ coming from $\mathbf{K}\,\mathrm{Frob}_{\text{k}}(\mathbf{W}'_{(N)})=0$ and n^2 from the field equations. There is a total of $n\,(n-r)+\ell N\,(n-r)+n^2$ equations in $r\,(n-r)+n+n^2$ variables.

On various small examples, we observed that the degree of regularity of such systems is $(N\ell+1)$ and does not depend on d when growing the size of d. This value matches the degree of regularity of the MinRank attack (see Sect. 7 for the complexity analysis). Hence, our variant seems to have asymptotically the same complexity as the attack in odd characteristic.

6.3.2 Odd Rank.

We now consider the case where the target rank $r = N\ell$ is odd. Here, the first step of the attack can be performed as expected and we recover the matrix $\mathbf{T}'$ (and consequently $\mathbf{U}' = \mathbf{T}'^{-1}\mathbf{M}_{N,d}$), as well as a kernel $\mathbf{K}$. Thus, we can assume now that the matrices $\mathbf{T}'$, $\mathbf{U}'$ and $\mathbf{K}$ are known.

The second step of the attack is to recover $\mathbf{S}'$. To do that in characteristic $\neq 2$, we had to solve the system $\mathbf{K}\,\mathbf{W}' = \ker(\mathbf{F_i})$, where $\mathbf{W}' \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ is unknown. The success of this step is based on the remark that $\ker(\mathbf{F_i})$ is independent of the actual value of $\mathbf{F_i}$ and is equal to $\mathbf{K}_{N,d,\ell}$ as described in Lemma. 4. In characteristic 2, this property does not hold. Recall that the matrix $\mathbf{F_i}$ should be a symmetric matrix of rank $N\ell$. In characteristic 2, this matrix has zero entries in its diagonal by following Kipnis-Shamir. The rank of such symmetric matrix cannot be odd (see for instance [34]. Thus, in characteristic 2, $\ker(\mathbf{F_i}) \neq \mathbf{K}_{N,d,\ell}$ and cannot be used for the second step of our attack. To fix our attack, one shall not consider the symmetric form of $\mathbf{F_i}$. Consider the relation between the components of an equivalent public/private key:

$$\mathscr{T}' \circ \varphi_N \circ \mathscr{F}^{*\prime} \circ \varphi_N^{-1} \circ \mathscr{S}' = \mathscr{G}$$
$$\mathscr{F}^{*\prime} \circ \varphi_N^{-1} \circ \mathscr{S}' = \varphi_N^{-1} \circ \mathscr{T}'^{-1} \circ \mathscr{G}.$$

Recall that $\mathbf{W}' = \mathbf{S}'\,\mathbf{M}_{N,d}$. When we consider the matrix representation, we obtain

$$\left(\mathbf{W}'\mathbf{F_1}'^{*d,0}\mathbf{W}'^t, \ldots, \mathbf{W}'\mathbf{F_1}'^{*d,d-1}\mathbf{W}'^t, \ldots, \mathbf{W}'\mathbf{F_N}'^{*d,d-1}\mathbf{W}'^t, \ldots, \mathbf{W}'\mathbf{F_N}'^{*d,d-1}\mathbf{W}'^t\right) = (\mathbf{G_1}, \ldots, \mathbf{G_n})\,\mathbf{U}'.$$

The matrices $\mathbf{G_i}$ for $i, 1 \leqslant i \leqslant n$ are the public matrices and the matrix $\mathbf{U}'$ has been recovered during the first step of our attack. Hence, the right hand side of this equation is known. Even if we do not know the value of the matrices $\mathbf{F_i}$ for $i, 1 \leqslant i \leqslant N$, we know the "shape" of these matrices. Indeed, only $\lceil \log(D) \rceil \times \lceil \log(D) \rceil$ elements are non-zero, and we know the positions of these elements (see proof of Lemma. 4 for instance). The key is to use the upper triangular matrix representing this quadratic form instead of a symmetric matrix. We will use this knowledge to recover both $\mathbf{W}'$ and $\mathbf{F_i}'$, for $i, 0 \leqslant i < N$.

Let $\underline{u}^{(1)t}$ be the first column $\mathbf{U}$. Recall that $\mathbf{F_1}^{*d,0} = \mathbf{F_1}$, we have for instance

$$\mathbf{W}'\,\mathbf{F_1}'^{*d,0}\,\mathbf{W}'^t = (\mathbf{G_1}, \ldots, \mathbf{G_n})\,\underline{u}^{(1)t}$$
$$\mathbf{F_1}' = \mathbf{W}'^{-1}\left((\mathbf{G_1}, \ldots, \mathbf{G_n})\,\underline{u}^{(1)t}\right)\mathbf{W}'^{-t}.$$

Equivalently, this amounts to solving the equations $\mathbf{F_1}' - \mathbf{W}'^{-1}\left((\mathbf{G_1}, \ldots, \mathbf{G_n})\,\underline{u}^{(1)t}\right)\mathbf{W}'^{-t} = \mathbf{0}$. As in the even rank attack, we interpret the entries of $\mathbf{W}'^{-1}$ as elements in $\mathbb{F}_2$. By doing this, the field equations can be added.

If we gather the equations coming from $\mathbf{F_1}, \ldots, \mathbf{F_N}$, solving this system (one set of equations for each entry) is enough to recover $\mathbf{W}'$ and $\mathbf{F}'_{\mathbf{i}}$ for $i, 1 \leqslant i \leqslant N$. Note that this system is quadratic. It features equations of degree 2 in the variables from $\mathbf{W}'$ and linear in the variables from $\mathbf{F_i}'$. In this case again, the observed degree of regularity is not more than the degree of regularity of the MinRank step. The overall complexity is still bounded by the MinRank step.

7 Complexity Analysis of the MinRank Attack

In this section, we study the peculiarities of the MinRank arising in our attack, i.e. coming from (8). In [35], it is conjectured that the basic Kipnis-Shamir attack against HFE is sub-exponential. The authors remarked that the algebraic system to be solved is greatly overdetermined. Recent results on solving MinRank [28] allow to have a fresher look at the complexity of MinRank-"type" key-recovery attacks against HFE and multi-HFE. For instance, from our experiments (described in the next section), we have remarked that the degree of regularity observed seems to be constant when d grows (d being the degree of the extension field). We explain theoretically this behavior using the formula (recalled in Sect. 2.4) on the degree of regularity of MinRank instances given in [28]. In our case, the MinRank arising involves n matrices of size $n \times n$ and a target rank $r = N\lceil \log_q(D) \rceil$. Thus, the MinRank considered are limited to instances of parameters (n, r, n). In this particular overdetermined case, we can get a precise bound under some conditions.

Proposition 11 *If the variant of the Fröberg Conjecture as defined in [28] is true, then the degree of regularity of the MinRank problem (n, r, n) is exactly $r + 1$ when $r < 4$ and $n \geqslant 6$.*

Proof As in Proposition 1, we introduce the following polynomials:

$$a_{i,j}(t) = \sum_{\ell=0}^{n-\max(i,j)} \binom{n-i}{\ell}\binom{n-j}{\ell} t^{\ell}$$

and the corresponding $r \times r$ matrix $\mathbf{A}_r(t) = [a_{i,j}(t)]$. According to Proposition 1, the index of the first negative coefficient of the power series

$$(1-t)^{(n-r)^2-n} \, \frac{\det \mathbf{A}_r(t)}{t^{\binom{r}{2}}} \tag{14}$$

gives the degree of regularity. To show that the degree of regularity is $r+1$, we need then to show that the coefficient of t^{r+1} in (14) is the first negative coefficient. Equivalently, we show that the coefficient of $t^{r+1+\binom{r}{2}}$ is the first negative coefficient in

$$H_r(t) = (1-t)^{(n-r)^2-n} \, \det \mathbf{A}_r(t)\,. \tag{15}$$

We denote by $F_{n-i}(t)$ the polynomial $a_{i,i}(t)$. It is straightforward to show that:

$$F_k(t) = (1-t)^k L_k\left(\frac{1+t}{1-t}\right)$$

where $L_n(X)$ is the n-th Legendre polynomial [43].

We can compute immediately $\det(\mathbf{A}_1(t)) = F_{n-1}(t)$ so that

$$H_1(t) = 1 + nt - \frac{1}{4} n\left(n^3 - 2n^2 - n - 2\right) t^2 + \mathscr{O}\left(t^3\right).$$

The coefficients of t^0 and t^1 are clearly positive and the coefficient of t^2 is of the opposite sign of n^3-2n^2-n-2; this coefficient is thus <0 as soon as $n > 2.7$.

To compute $H_2(t)$, we need to express $a_{1,2}(t) (= a_{2,1}(t))$ in terms of F_{n-1}.

$$\begin{aligned}
a_{2,1}(t) &= \textstyle\sum_{\ell=0}^{n-2} \binom{n-2}{\ell}\binom{n-1}{\ell} t^{\ell} \\
&= \textstyle\sum_{\ell=0}^{n-2} \frac{n-1-\ell}{n-1}\binom{n-1}{\ell}^2 t^{\ell} \\
&= \textstyle\sum_{\ell=0}^{n-2} \binom{n-1}{\ell}^2 t^{\ell} - \frac{1}{n-1} t \sum_{\ell=0}^{n-2} \binom{n-1}{\ell}^2 \ell t^{\ell-1} \\
&= \left(F_{n-1}(t) - t^{n-1}\right) - \frac{t}{n-1}\frac{\partial}{\partial t}\left(F_{n-1}(t) - t^{n-1}\right) \\
&= F_{n-1}(t) - \frac{t}{n-1} F'_{n-1}(t).
\end{aligned}$$

Hence, we can compute:

$$\begin{aligned}
\det\left(\mathbf{A}_2(t)\right) &= \begin{vmatrix} F_{n-1} & F_{n-1} - \frac{t}{n-1}F'_{n-1} \\ F_{n-1} - \frac{t}{n-1}F'_{n-1} & F_{n-2} \end{vmatrix} = F_{n-1}F_{n-2} - \left(F_{n-1} - \tfrac{t}{n-1}F'_{n-1}\right)^2 \\
&= t + (n-2)^2 t^2 + 1/2\left(n^2 - 4n + 5\right)(n-2)^2 t^3 + \\
&\qquad 1/36\left(5n^2 - 16n + 20\right)(n-2)^2 (n-3)^2 t^4 + \mathscr{O}\left(t^5\right).
\end{aligned}$$

Hence:

$$H_2(t) = t + nt^2 + 1/2\, n(n+1) t^3 - 1/36\, n\left(n^5 - 6n^4 + 13n^3 - 18n^2 - 14n - 12\right) t^4 + \mathscr{O}\left(t^5\right).$$

Clearly all the coefficients of t^1, t^2, t^3 are positive and the coefficient of t^4 is negative as soon as $n > 4.2$.

When $r = 3$, we have

$$\begin{aligned}
a_{2,3}(t) &= F_{n-2} - \frac{t}{n-2} F'_{n-2} \\
a_{1,3}(t) &= F_{n-1} + \frac{t^2 F''_{n-1} + 2(2-n) t F'_{n-1}}{(n-1)(n-2)}
\end{aligned}$$

We can compute explicitly

$$\begin{aligned}
\det\left(\mathbf{A}_3(t)\right) = t^3 + (n-3)^2 t^4 &+ \frac{1}{2}\left(n^2 - 6n + 10\right)(n-3)^2 t^5 \\
&+ \frac{1}{6}\left(n^2 - 6n + 10\right)\left(n^2 - 6n + 11\right)(n-3)^2 t^6 \\
&+ \frac{1}{576}\left(23n^4 - 242n^3 + 1067n^2 - 2268n + 1980\right)(n-3)^2 (n-4)^2 t^7 + \mathscr{O}\left(t^8\right)
\end{aligned}$$

and deduce that

$$H_3(t) = t^3 + nt^4 + \frac{1}{2}\,n\,(n+1)\,t^5 + \frac{1}{6}\,n\,(n+2)\,(n+1)\,t^6 \\ - \frac{1}{576}\,n\left(n^7 - 12\,n^6 + 58\,n^5\; - 144\,n^4 + 169\,n^3 - 276\,n^2 - 228\,n - 144\right)t^7 + \mathscr{O}\left(t^8\right).$$

Again the coefficients of t^3, t^4, t^5 and t^6 are obviously positive. Since the biggest real root of the coefficient of t^7 is ≈ 5.59 then it is negative when $n > 5$ $\square$

Instead of computing all the coefficients H_r given by equation (15), we can simply compute the coefficient of $t^{r+1+\binom{r}{2}}$ in $H_r(t)$.

Proposition 12 *If the variant of the Fröberg Conjecture as defined in [28] is true, then the degree of regularity of the MinRank Problem (n,r,n) is less than $r+1$ when $r \leqslant 10$ and $n \geqslant 6$.*

Proof Let $C_r(n)$ be the coefficient of $t^{r+1+\binom{r}{2}}$ in $H_r(t)$. We have:

$C_{10} = -\frac{1}{1593350922240000}\,(n^{21} - 110\,n^{20} + 5665\,n^{19} - 181500\,n^{18} + 4054446\,n^{17} - 67075140\,n^{16} + 852003130\,n^{15} - 8501266400\,n^{14} + 67608163381\,n^{13} - 432299636670\,n^{12} + 2232012515445\,n^{11} - 9309555172500\,n^{10} + 31264617802396\,n^9 - 84016440120800\,n^8 + 177471642248560\,n^7 - 299981580148800\,n^6 + 330208359091776\,n^5 - 468532034657280\,n^4 - 130151988172800\,n^3 - 586220360140800\,n^2 - 411093107712000\,n - 144850083840000)\,n.$

$C_9 = -\frac{1}{13168189440000}\,(n^{19} - 90\,n^{18} + 3765\,n^{17} - 97200\,n^{16} + 1733946\,n^{15} - 22676220\,n^{14} + 225084130\,n^{13} - 1731961800\,n^{12} + 10460514381\,n^{11} - 49893169050\,n^{10} + 188094067545\,n^9 - 558407719800\,n^8 + 1288998059896\,n^7 - 2330497406880\,n^6 + 2826910578960\,n^5 - 3910275907200\,n^4 - 721132948224\,n^3 - 5000541557760\,n^2 - 3593557094400\,n - 1316818944000)\,n.$

$C_8 = -\frac{1}{131681894400}\,(n^{17} - 72\,n^{16} + 2388\,n^{15} - 48384\,n^{14} + 669606\,n^{13} - 6704208\,n^{12} + 50170300\,n^{11} - 285855552\,n^{10} + 1251320145\,n^9 - 4215469608\,n^8 + 10855779816\,n^7 - 21379728384\,n^6 + 28864042768\,n^5 - 39461075712\,n^4 - 2881845504\,n^3 - 51701690880\,n^2 - 38140139520\,n - 14631321600)\,n.$

$C_7 = -\frac{1}{1625702400}\,(n^{15} - 56\,n^{14} + 1428\,n^{13} - 21952\,n^{12} + 226982\,n^{11} - 1667568\,n^{10} + 8962364\,n^9 - 35733376\,n^8 + 105954513\,n^7 - 233382296\,n^6 + 356137768\,n^5 - 490476672\,n^4 + 30217104\,n^3 - 661207680\,n^2 - 501500160\,n - 203212800)\,n.$

$C_6 = -\frac{1}{25401600}\,(n^{13} - 42\,n^{12} + 791\,n^{11} - 8820\,n^{10} + 64743\,n^9 - 328986\,n^8 + 1184153\,n^7 - 3039960\,n^6 + 5376616\,n^5 - 7669872\,n^4 + 1745856\,n^3 - 10725120\,n^2 - 8372160\,n - 3628800)\,n.$

$C_5 = -\frac{1}{518400}\,(n^{11} - 30\,n^{10} + 395\,n^9 - 3000\,n^8 + 14523\,n^7 - 46710\,n^6 + 100085\,n^5 - 154500\,n^4 + 67876\,n^3 - 227760\,n^2 - 182880\,n - 86400)\,n.$

$C_4 = -\frac{1}{14400}\,\left(n^9 - 20\,n^8 + 170\,n^7 - 800\,n^6 + 2273\,n^5 - 4100\,n^4 + 2980\,n^3 - 6600\,n^2 - 5424\,n - 2880\right)n.$

It is easy to check that the biggest real root of $C_4, C_5, C_6, C_7, C_8, C_9, C_{10}$ are approximately:

$$7.03, 8.45, 9.86, 11.3, 12.7, 14.1, 15.5$$

As a consequence, $C_4, C_5, C_6, C_7, C_8, C_9, C_{10}$ are all negative when $n > 15$. $\square$

From the previous propositions (Proposition 11 and 12) it is natural to make the following conjecture.

Conjecture 1 Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key with parameters $(q, N, d, D) \in \mathbb{N}^4$ and let $\ell = \lceil \log_q(D) \rceil$. The degree of regularity of the associated MinRank instances is bounded from above by $(N\ell + 1)$ when d is big enough.

Note that, by Proposition 11 and 12, the conjecture is proved for all $n > 15$ when $N\ell < 11$, this covers all possible practical settings for HFE and Multi-HFE. To further validate the conjecture, we have instantiated the theoretical bound of Proposition1 with HFE/multi-HFE parameters for values of $N \leqslant 20$ and $\ell \leqslant 10$. When d is sufficiently bigger than ℓ, we always obtain a degree of regularity equals to $(N\ell + 1)$. This has been verified for $n = N\,d$ up to 500.

Interestingly enough, the parameter d is not involved. In our context the degree of regularity depends only on the number N of secret variables and the degree D of the secret polynomials. We have then the necessary material to evaluate the difficulty of the MinRank involved in HFE/multi-HFE.

Proposition 13 *If the variant of the Fröberg Conjecture as defined in [28] is true, when $N\ell < 11$, for N and ℓ fixed, the complexity of solving the MinRank arising in Multi-HFE is $\mathscr{O}\left(d^{(N\ell+1)\,\omega}\right)$ $\left(2 \leqslant \omega < 3\right.$ being the linear algebra constant$\left.\right)$ and thus polynomial in d. Moreover if Conjecture 1, the previous complexity estimate is valid for any value of N and ℓ.*

Proof According to Proposition 12, the degree of regularity is not more than $(N\ell+1)$ and thus independent of the degree of the extension d. When d grows to infinity and according to Theorem 1 the complexity of the Gröbner basis computation is $\mathscr{O}\left(\binom{Nd+N\ell+1}{N\ell+1}^{\omega}\right) \sim \mathscr{O}\left((Nd)^{(N\ell+1)\,\omega}\right) \sim \mathscr{O}\left(d^{(N\ell+1)\,\omega}\right)$. □

This complexity refers to the number of arithmetic operations (in $\mathbb{F}_q$) needed. This makes the binary complexity logarithmic in q. As a comparison, the complexity of a message recovery attack on HFE according to [19] is polynomial in ℓ but exponential in q.

8 Attacks on Multi-HFE Variants

8.1 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. We recall that this construction is only suitable for signature as the decryption is not unique.

8.1.1 Description.

Let $(\mathscr{F}^*, \mathscr{S}, \mathscr{T})$ be a multi-HFE private key with parameters $(q,N,d,D) \in \mathbb{N}^4$ as defined in Sect. 2.1. We introduce a new 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 digest $\underline{m} = (m_1, \ldots, m_{n-s}) \in \mathbb{F}_q^{n-s}$. The signature is generated by applying the basic decryption process to such element. To verify a signature, we evaluate it on $\mathscr{G}$.

8.1.2 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, this is the case for the basic HFE ($N=1$). However we have shown in Sect. 5 that the problem has N degrees of freedom. As a consequence, only $(n-N+1)$ matrices are needed to recover the (secret) kernel. This means that if the number of equation removed s is (strictly) smaller than N, then the kernel matrix $\mathbf{K}$ can be found with no additional cost. Still, the last steps of the attack have to be adapted.

The first step is as follows. We know that there exists a vector $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_q)^n$ and symmetric $(n \times n)$-matrices $(\blacksquare_\mathbf{1}, \ldots, \blacksquare_\mathbf{s})$ 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 are unknown matrices corresponding to the removed polynomials. According to Theorem 7, we can fix N values λ_i and still having solutions to our polynomial system. For instance, let

$$(\lambda_{n-N+1}, \ldots, \lambda_n) = (\ell_1, \ldots, \ell_N).$$

We write

$$\mathbf{K} \cdot \left(\sum_{i=1}^{n-N} \lambda_i \mathbf{G_i} + \sum_{i=1}^{N-s} \ell_i \mathbf{G_{n-N+i}} + \sum_{i=1}^{s} \ell_{N-s+i} \blacksquare_\mathbf{i}\right) = \mathbf{0}. \tag{16}$$

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 entries of $\blacksquare_\mathbf{i}$, we use the following remark:

Proposition 14 *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, $\text{Frob}_\text{j}\left(\mathbf{K}\cdot(\sum_{i=1}^{n}\lambda_i\mathbf{G_i})\right)=\mathbf{0}$. By linearity of the Frobenius, this is equal to:

$$\text{Frob}_\text{j}(\mathbf{K})\cdot\text{Frob}_\text{j}\left(\sum_{i=1}^{n}\lambda_i\mathbf{G_i}\right)=\text{Frob}_\text{j}(\mathbf{K})\cdot\left(\sum_{i=1}^{n}\lambda_i^{q^j}\,\text{Frob}_\text{j}(\mathbf{G_i})\right).$$

As each $\mathbf{G_i}$ has its entries in $\mathbb{F}_q$, we also have that $\text{Frob}_\text{j}(\mathbf{G_i})=\mathbf{G_i}$. □

Solving equations (16) together with their Frobenius images forces the entries of $\blacksquare_\mathbf{i}$ to be in $\mathbb{F}_q$. In order to avoid equations of degree q^j coming from $\lambda_i^{q^j}$, we add $(d-1)(n-N)$ new variables $(\lambda_1^{(1)},\ldots,\lambda_{n-N}^{(1)},\ldots,\lambda_1^{(d-1)},\ldots,\lambda_{n-N}^{(d-1)})$. From Proposition 14, we get that $\forall j, 0\leqslant j<d$:

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

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 $\mathbf{U}$ as explained in Theorem 8.

8.1.3 Experimental Results

We present experimental results for the attack. It has been implemented in MAGMA [8] (V2.16-10). MinRank instances have been solved using the Kipnis-Shamir modeling. Our results are presented in Table 3. We mounted our attack on a basic multi-HFE and on multi-HFE- with the same parameters As predicted, the minus modifier

Table 3 Comparison of each step of our attack on minus variant on multi-HFE with parameters $q=31, N=3, d=8, D=2$ ($\approx$ 120 bits security) using a MAGMA [8] (V2.16-10) implementation on a 2.93 GHz Intel® Xeon® CPU.

	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			

does not change the time of the MinRank attack but recovering **W** is a bit slower. As a conclusion, the private key of a multi-HFE$^-$ can be recovered with this technique almost as efficiently as the standard construction if the number of withdrawn equations is less than $(N-1)$.

8.2 Multivariate-HFE with Embedding

In [20], it has been proposed to use a variant of HFE with embedding. This so-called PHFE construction consists in removing/fixing few variables of the public key. This scheme is claimed to resist Kipnis-Shamir's attack [20]. The authors of [14] 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.

8.2.1 Description.

Let $(\mathscr{F}^*,\mathscr{S},\mathscr{T})$ be a multi-HFE private key with parameters $(q,N,d,D)\in\mathbb{N}^4$ as defined in Sect. 2.1. 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. 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.

8.2.2 Attack.

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

Let $\mathbf{K} = \ker\left(\sum_{i=0}^{n-1} u_{i,0}\mathbf{G_{i+1}}\right)$. As usual a matrix $\mathbf{U}'$ can still be recovered by solving a MinRank. 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. 6.1.2, we get a system having $N\ell(n-r-N\ell)$ equations with only $N(n-r-N)$ variables. Let $\mathbf{W}'$ be a matrix solution of this linear system. This matrix is as follows:

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

This 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 inner mapping 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 $\mathbf{G}_i'$. Recall that the MinRank was done over $(n-r \times n-r)$-matrices. Therefore, when we finally compute $\sum_{i=0}^{n} u_{i,0}\mathbf{G_{i+1}}'$, monomials in the last variables $(x_{n-r+1},\ldots,x_n)$ are mixed with the other monomials. This eventually leads to polynomials that are not in HFE-shape (and then hard to invert).

To circumvent this issue, we no longer append a "quasi" random matrix to $\mathbf{W}'$. Instead, we construct an invertible matrix $\mathbf{W_z}$ by appending vertically to $\mathbf{W}'$ the matrix

$$\mathbf{Z} = \begin{pmatrix} 0 & \cdots\cdots\cdots\cdots & 0 & 1 & & \\ \vdots & & \vdots & & \ddots & \\ 0 & \cdots\cdots\cdots\cdots & 0 & & & 1 \end{pmatrix}.$$

From the way it is constructed, $\mathbf{W_z}$ is indeed invertible. The variables $(x_{n-r+1},\ldots,x_n)$ do not appear in $\mathbf{G_i}' = \mathbf{W_z}^{-1}\mathbf{G_i}\mathbf{W_z}^{-t}$, 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 $\mathbb{F}_{q^d}$. But, this is not an issue; $\mathbf{S}'$ can be inverted and a mapping $\mathscr{F}^*$ with HFE-shape can be recovered.

8.2.3 Experimental Results

Experimental results are given in Table. 4. We compare the different steps of the attack on a basic multi-HFE to the same attack running on multi-HFE with embedding.

Table 4 Comparison of each step of our attack on embedding variant on multi-HFE with parameters $q = 31, N = 3, d = 8, D = 2$ (≈ 120 bits security) using a MAGMA [8] (V2.16-10) implementation on a 2.93 GHz Intel® Xeon® CPU.

	MR time	MR d_{reg}	Finding **U**	Finding **W**
No variant (ref. time)	23.3 s	3	0.01 s	7.29 s
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

In practice, the MinRank occurring in multi-HFE with embedding takes more time to break. However, the degree of regularity remains the same. Thus, there is only a constant factor between the complexity of solving a regular MR occurring in multi-HFE and a MR occurring in multi-HFE with embedding. As a conclusion, the embedding modifier does not add more security to the basic HFE/multi-HFE construction.

To further point out this weakness, we practically broke a 256 bits Multi-HFE scheme using embedding whilst a classical HFE instance with $n = 256$ bits is still intractable. In Table 5, we show our results on the parameters proposed in [13] (multi-HFE with embedding $r = 1$). The degree of regularity experimentally observed is noted

d_{reg}. The theoretical degree of regularity is denoted by $d_{\text{reg}}^{\text{theo}}$. The proposed parameters 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 [25].

Table 5 MinRank attack on real-scale parameters from [13] using a MAGMA [8] (V2.16-10) implementation of Kipnis-Shamir modeling and a FGb [25] implementation of the minors modeling on a 2.93 GHz Intel® Xeon® CPU.

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	1.5 GB	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

9 Weaknesses of Multi-HFE relative to HFE

In light of our results, we conclude the paper by evaluating the real security gain offered by the Multi-HFE construction (w.r.t. basic HFE). In order to compare instances of HFE/multi-HFE with each other, we introduce and formalize the notion of "similarity" between two instances of multi-HFE.

Definition 3 Two multi-HFE instances of respective parameters (q_1, N_1, d_1, D_1) and (q_2, N_2, d_2, D_2) are *similar* iff

i) $q_1 = q_2$ (same base field)
ii) $N_1 d_1 = N_2 d_2$ (same public key size)
iii) $N_1 \log_{q_1}(D_1) = N_2 \log_{q_2}(D_2)$ (same private key size)

This definition is motivated by the following fact.

Property 1 Two similar instances of multi-HFE share the same size of public key and (almost) the same size of private key.

Proof The transformations $\mathscr{S}$ and $\mathscr{T}$ have the same size for two similar multi-HFE instances. Each secret polynomial can be written as a non-standard quadratic form on the q-th powers of the variables. As the degree is bounded by D, we have at most $(N\log_q(D)+1)(N\log_q(D)+2)/2$ monomials in each polynomial. We then have to store $N(N\log_q(D)+1)(N\log_q(D)+2)(d\log_2(q))$ bits. □

This definition includes HFE as it is a particular case of Multi-HFE ($N = 1$) To illustrate the concept of equivalent keys, we provide in Table 6 two multi-HFE parameters proposed by [6] and [14]. The table shows the correspondence between their similar univariate instance, as well as the complexity of solving the MinRank for each set of parameters.

Note that this definition takes into account the size of the private key. The speed of decryption can vary a lot between two similar instances as pointed in Table 6. A different notion of similarity with respect to the speed of decryption could also be considered.

Table 6 Similar univariate HFE parameters for multi-HFE instances. The two sets of parameters in each line provide the same general security (key sizes and message space) but the decryption speed and the complexity of our attack vary a lot.

	q	N	d	D	msg space	pub (bits)	priv (bits)	decr. time	MinRank comp.
IFS	2	8	16	2	128 bits	2130048	39042	0.610 s.	$16^{9\omega} = 2^{36\omega}$
HFE	2	1	128	192	128 bits	2130048	38018	0.120 s.	$128^{9\omega} = 2^{63\omega}$
THFE	31	3	10	2	150 bits	144150	11110	< 0.001 s.	$10^{3\omega} \approx 2^{10\omega}$
HFE	31	1	30	1922	150 bits	144150	11110	≈ 10 s.	$30^{3\omega} \approx 2^{15\omega}$

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 13, 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 also 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.

Acknowledgments

We would like to thank C. Wolf for his comments on a preliminary version of this paper. We also would like to thank the referees for their meaningful comments. The work described in this paper has been supported in part by the European Commission through the ICT program 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 WW, Loustaunau P (1994) An Introduction to Gröbner Bases, Graduate Studies in Mahematics, vol 3. AMS
2. Bardet M, Faugère JC, Salvy B (2004) On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proc. of International Conference on Polynomial System Solving (ICPSS), pp 71–75
3. Bardet M, Faugère JC, Salvy B, Yang BY (2005) 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
4. Bettale L, Faugère JC, Perret L (2009) Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology pp 177–197
5. Bettale L, Faugère JC, Perret L (2011) Cryptanalysis of multivariate and odd-characteristic hfe variants. In: Public Key Cryptography – PKC 2011, Springer, Lecture Notes in Computer Science, vol 6571, pp 441–458
6. Billet O, Patarin J, Seurin Y (2008) Analysis of Intermediate Field Systems. In: SCC 2008
7. Bogdanov A, Eisenbarth T, Rupp A, Wolf C (2008) Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves? In: Cryptographic Hardware and Embedded Systems – CHES ’08, LNCS, pp 45–61
8. Bosma W, Cannon JJ, Playoust C (1997) The Magma algebra system I: The user language. Journal of Symbolic Computation 24(3-4):235–265
9. Buchberger B (1965) Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. PhD thesis, University of Innsbruck
10. Buchberger B (2006) Bruno buchberger’s phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J Symb Comput 41(3-4):475–511
11. Buchberger B (2006) Comments on the translation of my phd thesis. J Symb Comput 41(3-4):471–474
12. Buss W, Frandsen G, Shallit J (1999) The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences
13. Chen AIT, Chen MS, Chen TR, Cheng CM, Ding J, Kuo ELH, Lee FYS, Yang BY (2009) SSE implementation of multivariate PKCs on modern x86 CPUs. In: Cryptographic Hardware and Embedded Systems – CHES 2009, Springer, LNCS, vol 5747, pp 33–48
14. Chen CHO, Chen MS, Ding J, Werner F, Yang BY (2008) Odd-char multivariate Hidden Field Equations. Cryptology ePrint Archive, `http://eprint.iacr.org/2008/543`
15. Courtois N, Goubin L (2000) Cryptanalysis of the TTM cryptosystem. In: Advances in Cryptology – ASIACRYPT ’00, Springer, Lecture Notes in Computer Science, vol 1976, pp 44–57
16. Courtois NT (2001) Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in Cryptology – ASIACRYPT 2001, Springer, LNCS, vol 2248, pp 402–421
17. Cox DA, Little JB, O’Shea D (2005) Ideals, Varieties and Algorithms. Sringer
18. DeMillo R, Lipton R (1978) A probabilistic remark on algebraic program testing. Information Processing Letters 7(4):192–194
19. Ding J, Hodges TJ (2011) Inverting hfe systems is quasi-polynomial for all fields. In: Rogaway P (ed) CRYPTO, Springer, Lecture Notes in Computer Science, vol 6841, pp 724–742
20. Ding J, Schmidt D, Werner F (2008) Algebraic attack on HFE revisited. In: Information Security, Springer, LNCS, vol 5222, pp 215–227

21. Dubois V, Gama N (2011) The degree of regularity of HFE systems. In: Advances in Cryptology – ASIACRYPT 2011, Springer, Lecture Notes in Computer Science, vol 6477, pp 557–576
22. Faugère JC (1999) A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139:61–88
23. Faugère JC (2002) A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC, ACM Press, pp 75–83
24. Faugère JC (2003) Algebraic cryptanalysis of HFE using Gröbner bases. Reasearch report RR-4738, INRIA, URL `http://hal.inria.fr/inria-00071849/PDF/RR-4738.pdf`
25. Faugère JC (2010) FGb: A Library for Computing Gröbner Bases. In: Fukuda K, Hoeven J, Joswig M, Takayama N (eds) Mathematical Software – ICMS 2010, Springer Berlin / Heidelberg, Berlin, Heidelberg, Lecture Notes in Computer Science, vol 6327, pp 84–87, URL `http://www-salsa.lip6.fr/~jcf/Papers/ICMS.pdf`
26. Faugère JC, Joux A (2003) Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In: Advances in Cryptology – CRYPTO 2003, Springer, LNCS, vol 2729, pp 44–60
27. Faugère JC, Levy-dit-Vehel F, Perret L (2008) Cryptanalysis of MinRank. In: Advances in Cryptology – CRYPTO 2008, Springer, LNCS, vol 5157, pp 280–296
28. Faugère JC, Safey El Din M, Spaenlehauer PJ (2010) Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In: Koepf W (ed) ISSAC, ACM, pp 257–264
29. Faugère JC, Safey El Din M, Spaenlehauer PJ (2010) Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity. Journal of Symbolic Computation pp 1–39
30. Faugère JC, Safey El Din M, Spaenlehauer PJ (2011) On the complexity of the generalized minrank problem, preprint
31. Fröberg R (1985) An inequality for Hilbert series of graded algebras. Mathematica Scandinavica 56:117–144
32. Garey MR, Johnson DS (1979) Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman
33. Granboulan L, Joux A, Stern J (2006) Inverting HFE is quasipolynomial. In: Advances in Cryptology – CRYPTO 2006, Springer, LNCS, vol 4117, pp 345–356
34. Jiang X, Ding J, Hu L (2007) Kipnis-Shamir attack on HFE revisited. In: Information Security and Cryptology, Springer, LNCS, vol 4990, pp 399–411
35. Kipnis A, Shamir A (1999) Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Advances in Cryptology – CRYPTO ’99, Springer, LNCS, vol 1666, pp 19–30
36. Kipnis A, Patarin J, Goubin L (1999) Unbalanced oil and vinegar signature schemes. In: Advances in Cryptology – EUROCRYPT ’99, Springer, Lecture Notes in Computer Science, vol 1592, pp 206–222
37. Matsumoto T, Imai H (1988) Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Advances in Cryptology – EUROCRYPT ’88, Springer, LNCS, vol 330, pp 419–453
38. Moh TT (1999) A public key system with signature and master key functions. Communications in Algebra 27(5):2207–2222
39. Nguyen P (2003) New trends in cryptology, european project “stork: Strategic roadmap for advances in cryptology - crypto”, ist-2002-38273. `http://www.di.ens.fr/~pnguyen/pub.html#Ng03`
40. Patarin J (1995) Cryptoanalysis of the Matsumoto and Imai public key scheme of Eurocrypt ’88. In: Advances in Cryptology – CRYPTO ’95, pp 248–261
41. Patarin J (1996) Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In: Advances in Cryptology – EUROCRYPT ’96, Springer, LNCS, vol 1070, pp 33–48
42. Schwartz JT (1980) Fast probabilistic algorithms for verification of polynomial identities. Journal of the ACM 27(4):701–717
43. Szegö G (1939) Orthogonal Polynomials, 4th edn. American Mathematical Society
44. Wang LC, Hu YH, Lai F, yen Chou C, Yang BY (2005) Tractable rational map signature. In: Public Key Cryptography – PKC ’05, Springer, Lecture Notes in Computer Science, vol 3386, pp 244–257
45. Wolf C, Preneel B (2005) Equivalent keys in HFE, C^*, and variations. In: Progress in Cryptology – Mycrypt 2005, Springer, LNCS, vol 3715, pp 33–49
46. Wolf C, Preneel B (2005) Large superfluous keys in multivariate quadratic asymmetric systems. In: Public Key Cryptography – PKC 2005, Springer, LNCS, vol 3386, pp 275–287

47. Wolf C, Preneel B (2011) Equivalent keys in multivariate quadratic public key systems. Journal of Mathematical Cryptology 4(4):375–415
48. Zippel R (1979) Probabilistic algorithms for sparse polynomials. In: Symbolic and algebraic computation (EUROSAM'79), Internat. Sympos., Springer Verlag, Lecture Notes in Computer Science, vol 72, pp 216–226

A Example of Key Recovery in Characteristic 2

A.1 Example for Even Rank

We consider an instance of HFE with the following parameters: $q = 2$, $N = 1$, $d = 6$, $D = (q+1) = 3$, $r = N \lceil \log_q(d) \rceil = 2$. The private key is given in Fig. 3 and the public key in Fig. 4.

$$F_1 = \theta^{30} X_1^3 + \theta^{33} X_1^2.$$

$$\mathbf{S} = \begin{pmatrix} 1&1&1&1&1&1 \\ 0&0&0&0&1&0 \\ 1&0&0&1&1&1 \\ 1&1&0&0&1&0 \\ 1&0&1&0&1&1 \\ 1&0&0&0&1&1 \end{pmatrix}, \mathbf{T} = \begin{pmatrix} 1&0&0&1&0&0 \\ 0&0&0&1&0&0 \\ 1&0&1&0&1&1 \\ 0&1&0&0&1&1 \\ 0&1&0&1&0&1 \\ 1&0&1&0&0&0 \end{pmatrix}.$$

Fig. 3 Private key for a (Multi-)HFE with parameters $q = 2$, $N = 1$, $d = 6$, and $D = 3$.

$$\mathbf{G_1} = \begin{pmatrix} 1&1&1&1&0&1&0 \\ 0&1&1&1&0&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_2} = \begin{pmatrix} 1&1&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_3} = \begin{pmatrix} 1&1&1&0&0&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&0&1&1&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \end{pmatrix},$$

$$\mathbf{G_4} = \begin{pmatrix} 1&0&0&1&1&0&0 \\ 0&1&1&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_5} = \begin{pmatrix} 1&1&0&1&1&1&0 \\ 0&1&1&0&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_6} = \begin{pmatrix} 1&1&0&0&0&0&0 \\ 0&1&1&1&1&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}.$$

Fig. 4 Public key for a (Multi-)HFE with parameters $q = 2$, $N = 1$, $d = 6$, and $D = 3$.

As explained in Sect. 6.1.4, we can fix $\lambda_1 = 1$. However, the MinRank problem has still $d\,(q^d - 1) = 6 \times 63 = 378$ solutions. We can fix one more variable as suggested in [34]. For example, we fix $\lambda_2 = \theta$. We have now only $d = 6$ solutions, i.e.:

$$(1,\theta,\theta^{15},\theta,\theta^{61},\theta^{50}),(1,\theta,\theta^{17},\theta^{41},\theta,\theta^{30}),(1,\theta,\theta^{22},\theta^{43},\theta^{51},\theta^{38}),$$
$$(1,\theta,\theta^{28},\theta^{53},\theta^{24},\theta^{60}),(1,\theta,\theta^{42},\theta^{11},\theta^{9},\theta^{17}),(1,\theta,\theta^{45},\theta^{20},\theta^{32},\theta).$$

We build the corresponding matrices $\mathbf{K}$ and $\mathbf{T}'$. In the second step – recovering $\mathbf{S}'$– the linear system $\mathbf{KW} = \ker(\mathbf{F_i})$ has no solution. The computed $\mathbf{T}'$ is then not valid.

Using the technique described in Sect. 6.3, we have to solve a system of 68 equations in 50 variables. After fixing $\lambda_1 = 1$ and $w'_{0,0} = 1$, the system is of dimension 0 and the solution is:

$$\underline{\lambda} = (1,\theta^{9},\theta^{5},\theta^{28},\theta^{41},\theta^{15}),$$

$$\mathbf{K} = \begin{pmatrix} 1&0&0&0&\theta^{46}&\theta^{32} \\ 0&1&0&0&\theta^{29}&\theta^{41} \\ 0&0&1&0&\theta^{12}&\theta^{39} \\ 0&0&0&1&\theta^{38}&\theta^{21} \end{pmatrix}, \qquad \mathbf{S}' = \begin{pmatrix} 1&0&0&1&0&0 \\ 0&0&0&1&1&1 \\ 0&0&1&0&1&0 \\ 1&1&1&0&1&1 \\ 0&1&1&1&1&0 \\ 0&1&0&1&1&1 \end{pmatrix}.$$

Finally, the matrix $\mathbf{T}'$ can be recovered

$$\mathbf{T}' = \begin{pmatrix} 0&0&1&1&0&0 \\ 0&0&1&0&0&1 \\ 1&1&0&1&0&0 \\ 0&0&0&0&1&1 \\ 1&0&0&0&1&0 \\ 1&0&1&0&1&0 \end{pmatrix}.$$

With the matrices $\mathbf{T}'$ and $\mathbf{S}'$, we recover a secret polynomial $F_1' = \theta^{48} X_1^3 + \theta^{46} X_1^2$ which completes the key recovery.

A.2 Example for Odd Rank

We consider an instance of HFE with the following parameters: $q = 2$, $N = 1$, $d = 6$, $D = (q^2 + 1) = 5$, and $r = N \lceil \log_q(D) \rceil = 3$. The private key is given in Fig. 5 and the public key in Fig. 6.

$$F_1 = \theta^{27} X_1^5 + \theta^{61} X_1^4 + \theta^{36} X_1^3 + \theta^{53} X_1^2.$$

$$\mathbf{S} = \begin{pmatrix} 1&0&0&0&1&1 \\ 0&0&0&1&1&0 \\ 0&0&1&1&1&1 \\ 0&1&0&1&0&0 \\ 1&1&1&1&1&1 \\ 0&0&0&1&0&0 \end{pmatrix}, \mathbf{T} = \begin{pmatrix} 0&0&0&1&1&1 \\ 0&0&1&1&0&1 \\ 1&0&1&0&1&1 \\ 1&0&0&1&0&1 \\ 1&1&1&0&0&1 \\ 0&1&1&0&1&0 \end{pmatrix}.$$

Fig. 5 Private key of a (Multi-)HFE with parameters: $q = 2$, $N = 1$, $d = 6$, and $D = 3$.

$$\mathbf{G_1} = \begin{pmatrix} 0&0&0&0&1&0&0 \\ 0&1&0&0&1&1&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&1&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_2} = \begin{pmatrix} 1&1&1&1&1&0&0 \\ 0&1&1&1&1&1&0 \\ 0&0&0&1&0&1&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_3} = \begin{pmatrix} 0&1&0&1&1&1&0 \\ 0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \end{pmatrix},$$

$$\mathbf{G_4} = \begin{pmatrix} 1&0&1&0&0&0&0 \\ 0&0&0&1&1&0&0 \\ 0&0&1&1&1&1&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_5} = \begin{pmatrix} 0&1&0&1&1&1&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}, \mathbf{G_6} = \begin{pmatrix} 1&1&0&0&0&0&0 \\ 0&0&1&1&1&1&0 \\ 0&0&1&1&1&0&0 \\ 0&0&0&1&0&1&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{pmatrix}.$$

Fig. 6 Public key of a (Multi-)HFE with parameters: $q = 2$, $N = 1$, $d = 6$, and $D = 3$.

After fixing $\lambda_1 = 1$, the MinRank problem has d solutions. The solution are:

$$\underline{\lambda}^{(1)} = (1, \theta^7, \theta^{52}, \theta^4, \theta^{33}, \theta^{36})$$

and all its Frobenius images. The matrix $\mathbf{T}'$ can be recovered normally:

$$\mathbf{T}' = \begin{pmatrix} 0&0&0&1&0&1 \\ 1&1&0&0&0&1 \\ 0&0&0&1&1&0 \\ 0&1&1&0&1&1 \\ 1&1&1&0&1&1 \\ 0&0&1&0&1&1 \end{pmatrix}.$$

The first step of the attack runs pretty well and we are able to compute $\mathbf{K}$. Nevertheless, one can remark that the kernel matrix of $\mathbf{F_1}$ is

$$\ker(\mathbf{F_1}) = \begin{pmatrix} 0&1&\theta^9&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{pmatrix}.$$

The matrix has 1 column set to zero instead of 3 leading to an underdetermined linear system when we consider $\mathbf{KW} = \ker(\mathbf{F_1})$. We can try to fix more variables in such system. For instance:

$$\underline{w}^{(1)} = (1, \theta, \theta^{31}, \theta^{16}, \theta^{50}, \theta^{5})$$

is a possible solution to our system. However, when we use it as in Sect. 6.1.4 to build the matrix $\mathbf{W}'$, $\mathbf{W}'$ is not invertible, making the full key recovery impossible. Another possible solution is

$$\underline{w}^{(1)} = (1, \theta^{5}, \theta^{12}, \theta^{36}, \theta^{34}, \theta^{6}).$$

In this case, $\mathbf{W}'$ is invertible. But, we have:

$$F_1' = \theta^7 X_1^{33} + \theta^5 X_1^{32} + \theta^{55} X_1^{17} + \theta^{23} X_1^{16} + \theta^{50} X_1^{9} + \\ \theta^{61} X_1^{8} + \theta^{26} X_1^{5} + \theta^{18} X_1^{4} + \theta^{59} X_1^{3} + \theta^{61} X_1^{2} + \theta^{31} X_1$$

whose degree is not anymore bounded by D.

Using the method described in Sect. 6.3, we know that:

$$\mathbf{F}_1 = \begin{pmatrix} a_1 & a_2 & a_3 & 0 & 0 & 0 \\ 0 & a_4 & a_5 & 0 & 0 & 0 \\ 0 & 0 & a_6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

for some values $a_1, \ldots, a_6 \in \mathbb{F}_{q^d}$. We have

$$(\mathbf{G_1}, \ldots, \mathbf{G_n})\,\underline{\lambda}^{(1)t} = \begin{pmatrix} \theta^{56} & \theta^{47} & \theta^{50} & \theta^{28} & \theta^{17} & \theta^{58} \\ 0 & \theta^{41} & \theta^{14} & \theta^{39} & \theta^{54} & \theta^{45} \\ 0 & 0 & \theta^{12} & \theta^{56} & \theta^{44} & \theta^{36} \\ 0 & 0 & 0 & \theta^{25} & \theta^{15} & \theta^{4} \\ 0 & 0 & 0 & 0 & \theta^{14} & \theta^{5} \\ 0 & 0 & 0 & 0 & 0 & \theta^{2} \end{pmatrix}$$

using the same notations as in Sect. 6.3. The resulting system

$$\mathbf{F_1} = \mathbf{W}'^{-1}\left((\mathbf{G_1}, \ldots, \mathbf{G_n})\,\underline{\lambda}^{(1)t}\right)\mathbf{W}'^{-t}.$$

has 21 quadratic equations and 36 field equations in 42 variables. After fixing $\mathbf{W}'^{-1}[0,0] = 1$ the system has dimension 0 and it gives

$$\mathbf{F_1}' = \begin{pmatrix} \theta^{41} & \theta^{23} & \theta^{61} & 0 & 0 & 0 \\ 0 & \theta^{26} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad \mathbf{S}' = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

The polynomial $F_1' = \theta^{61} X_1^5 + \theta^{26} X_1^4 + \theta^{23} X_1^3 + \theta^{41} X_1^2$ has HFE-shape and it can be verified that the recovered components are a valid equivalent key.

B Proofs from Section 3.2

Proof (Proposition 5) Let $F = \sum_{r=0,s=0}^{N-1} \sum_{u=0,v=0}^{d-1} A_{r,s,u,v} X_{r+1}^{q^u} X_{s+1}^{q^v}$ be a HFE-shaped polynomial and

$$\underline{\widetilde{X}} = (X_1, X_1^q, \ldots, X_1^{q^{d-1}}, \ldots, X_N, X_N^q, \ldots, X_N^{q^{d-1}}).$$

From the definition of the non-standard matrix representation, we have that $F = \underline{\widetilde{X}}\,\mathbf{F}\,\underline{\widetilde{X}}^t$ with $\mathbf{F} = [f_{i,j}] \in \mathscr{M}_{n\times n}\left(\mathbb{F}_{q^d}\right)$ and then $A_{r,s,u,v} = f_{rd+u,sd+v}$. Assume that $F' = \underline{\widetilde{X}}\,\mathbf{F}^{*d,k}\,\underline{\widetilde{X}}^t$, we will prove that $F' = F^{q^k}$. From Definition 1, each element of $\mathbf{F}^{*d,k}$ can be expressed from the $f_{i,j}$'s. By construction of $\mathbf{F}^{*d,k}$, it is straightforward to show that $\mathbf{F}^{*d,k} = [f^{q^k}_{d\lfloor i/d\rfloor+(i-k \bmod d),d\lfloor j/d\rfloor+(j-k \bmod d)}]$. Then, the polynomial F' is:

$$F' = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f^{q^k}_{d\lfloor i/d\rfloor+(i-k \bmod d),d\lfloor j/d\rfloor+(j-k \bmod d)} X_{\lfloor i/d\rfloor+1}^{q^{i \bmod d}} X_{\lfloor j/d\rfloor+1}^{q^{j \bmod d}}.$$

We do the replacement $i \leftarrow rd+u$ and $j \leftarrow sd+v$.

$$F' = \sum_{r=0}^{N-1}\sum_{u=0}^{d-1}\sum_{s=0}^{N-1}\sum_{v=0}^{d-1} f^{q^k}_{dr+(u-k \bmod d),ds+(v-k \bmod d)} X_{r+1}^{q^u} X_{s+1}^{q^v}$$

$$F' = \sum_{r,s=0}^{N-1}\sum_{u,v=0}^{d-1} f^{q^k}_{dr+(u-k \bmod d),ds+(v-k \bmod d)} X_{r+1}^{q^u} X_{s+1}^{q^v}.$$

We shift the indexes u and v by k (i.e. $u \leftarrow u+k$, $v \leftarrow v+k$). As in (2) – as the indexes being computed $\mod d$ – we have

$$
\begin{aligned}
F' &= \sum_{r,s=0}^{N-1} \sum_{u,v=0}^{d-1} f^{q^k}_{d\,r+(u \bmod d),d\,s+(v \bmod d)} X_{r+1}^{q^{u+k \bmod d}} X_{s+1}^{q^{v+k \bmod d}} \\
F' &= \sum_{r,s=0}^{N-1} \sum_{u,v=0}^{d-1} \left(f_{d\,r+u,d\,s+v} X_{r+1}^{q^u} X_{s+1}^{q^v} \right)^{q^k} \\
F' &= \left(\sum_{r,s=0}^{N-1} \sum_{u,v=0}^{d-1} A_{r,s,u,v} X_{r+1}^{q^u} X_{s+1}^{q^v} \right)^{q^k} \\
F' &= F^{q^k}.
\end{aligned}
$$

This proves the proposition. □

Proof (Proposition 6) The proof is very similar to the proof of Proposition 3. For $i,j, 0 \leqslant i,j < n$, let $m_{i,j}$ be the (i,j)-th element of $\mathbf{M}_{N,d}$. According to the definition of $\mathbf{M}_{N,d}$ in Proposition 4, $m_{i,j} = 0$ if $\lfloor i/d \rfloor \neq \lfloor j/d \rfloor$. For all i, j, $0 \leqslant i,j < n$, an element $b_{i,j}$ of $\mathbf{B}$ is then

$$
b_{i,j} = \sum_{\ell=0}^{n-1} a_{i,\ell} m_{\ell,j} = \sum_{\ell=0}^{d-1} a_{i,\lfloor j/d \rfloor+\ell}\, m_{\lfloor j/d \rfloor+\ell,j} = \sum_{\ell=0}^{d-1} a_{i,\lfloor j/d \rfloor+\ell}\, \theta_{\ell+1}^{j \bmod d}\,.
$$

Thus: $b_{i,k\,d+((j-1) \bmod d)} = \sum_{\ell=0}^{d-1} a_{i,k+\ell}\, \theta_{\ell+1}^{j-1}$. Consequently:

$$
b^q_{i,k\,d+((j-1) \bmod d)} = \left(\sum_{\ell=0}^{d-1} a_{i,k+\ell}\, \theta_{\ell+1}^{j-1} \right)^q.
$$

As $a_{i,j} \in \mathbb{F}_q$ (i.e. $a^q_{i,j} = a_{i,j}$) and since the Frobenius is linear, we get:

$$
b^q_{i,k\,d+((j-1) \bmod d)} = \sum_{\ell=0}^{d-1} a^q_{i,k+\ell} \left(\theta_{\ell+1}^{j-1} \right)^q = \sum_{\ell=0}^{d-1} a_{i,k+\ell}\, \theta_{\ell+1}^{j} = b_{i,k\,d+j}\,.
$$

□