State of the art of HFE variants Is it possible to repair HFE with appropriate modifiers? (HFE IP -)

Benoît Cogliati¹, Gilles Macariot-Rat², Jacques Patarin¹, and Pierre Varjabedian¹

¹ THALES, Meudon, France,

 $\{\texttt{benoit-michel.cogliati,jacques.patarin,pierre.varjabedian}\} \texttt{Othalesgroup.com}^2 \ \text{Orange, Chatillon, France, gilles.macariorat@orange.com}$

Keywords: Multivariate Cryptography \cdot Short Signature \cdot HFE \cdot HFE variants \cdot MinRank attacks

Abstract. HFE (that stands for Hidden Field Equations) belongs to multivariate cryptography and was designed by Jacques Patarin in 1996 as a public key trapdoor suitable for encryption or signature. This original basic version is unfortunately known to have a super-polynomial attack, but as imagined since the beginning, it comes with various variants, one can describe as combinations of "modifiers".

In this work, we first present the state of the art of these HFE modifiers, along with their effect on the complexity of the main cryptanalysis techniques against HFE-based schemes. This allows us, in a second time, to identify a combination of two modifiers that has not yet been explored and may still be secure with efficient parameters. Based on our analysis, we propose a new signature scheme that offers extremely short signature sizes, with reasonable public key sizes and performance. In particular, we rely on the classical Feistel-Patarin technique to reduce signature sizes below two times the security parameter.

1 Introduction

The cryptosystem and signature scheme HFE was created in 1996 by Jacques Patarin [Pat96b] in order to repair the Matsumoto-Imai cypher [MI88]. In this initial paper, it was already mentioned that many variants of HFE exist since many "modifiers" can be added to the scheme. We will call "unmodified" HFE the simplest variant, i.e HFE with no additional modifiers. In [Pat96b] it was mentioned that when the degree d of the hidden polynomial is fixed, some polynomial attacks are possible, but at that time the scheme was nevertheless efficient even with small parameters. Since 1996 many other papers have been published, with the discovery of many more variants, along with many more possible attacks. On "unmodified" HFE for example, super-polynomial attacks were published in [FJ03] even when the degree d increases. Therefore "unmodified" HFE is at present only interesting for very specific needs: very short public signatures and a security level of only about 80 bits (see [PMBK20]), since for larger security the size of the public key becomes too large.

The two main families of attacks on HFE and HFE variants are direct attacks using Gröbner bases [FJ03], and full key recovery attacks using MinRank problem. The first MinRank attack was published in [KS99]. Recently great improvements have been done on these MinRank attacks. In fact many different MinRank attacks exist: some that first target the secret matrix **T** of HFE [BFP11] and some that will first attack the secret matrix **S** of HFE. Improvements have also been made in the resolution of the MinRank problem. The first methods were the use of the so called minor modelling, while today we are using an improved version called the Support minor modelling [BBB⁺22].

It is relatively easy to add a simple modifier to resist one of these attacks, but, as we will see in this paper, it is difficult to resist all of them. In fact, the most impressive recent cryptanalysis result on HFE variants was the cryptanalysis of GeMSS done in [TPD21], [BBC⁺22] by a MinRank attack (following the idea of Beullens [Beu21] on the rainbow scheme). GeMSS is a HFEv- signature scheme i.e HFE with modifier v and - (these modifiers will be defined later) submitted to the NIST-PQ competition. The scheme was broken due to these attacks. The aim of this paper will be to see if some combination of two HFE variants can resist all known attacks (Gröbner basis attack, all the MinRank attack variants, differential attacks etc...). We think that it is also interesting to have a general view of the state of the art on this subject because there are so many papers on HFE that the situation may look confusing. As we will see, in encryption we did not find any solution from the known modifiers. However in signature, one of the variants, called HFEIP- (for HFE with the Internal Perturbation and the minus modifier) may still be secure with efficient parameters. Of course, since the analysis of this design is recent, and since many HFE variants have been broken, we do not recommend to use it yet for critical application, but rather to continue the theoretical analysis to see if this variant can really be secure and resist the test of time.

In this paper we provide a summary of the situation of the research on HFE variants. We are making in the first part a cryptanalysis on every variant found on HFE with the most modern attacks available. Hence, we provide cryptanalysis that were not made on certain variants such a "plus" or "internal perturbation". In this section we focus on MinRank attacks and give a slight insight on Gröbner bases attacks or attacks specific to a said variant. In the second part we propose a new scheme based on HFE, we also give a set of parameters for this scheme.

2 Preliminary

2.1 Notations

For our notations, the set of all integers between integers a, b (a and b included) is $\{a \dots b\}$. Row vectors and matrices will be written in **bold**. On this paper we will sometimes switch to a polynomial notation or a function notation so the

function represented by the matrix will sometimes be implicitly called by the same letter that was used for the matrix. For example the function H will be associated with the matrix \mathbf{H} . We denote by v_i the *i*-th component of a vector \mathbf{v} , and the entries of a matrix \mathbf{M} of size $n_r \times n_c$ will be denoted by $\mathbf{M}_{i,j}$, where i (resp. j) is an integer in $\{1..n_r\}$ (resp. $\{1..n_c\}$). If one consider the subsets $I \subset \{1..n_r\}$ and $J \subset \{1..n_c\}$, we use the notation $\mathbf{M}_{I,J}$ for the submatrix of \mathbf{M} formed by its rows (resp. columns) with indexes in I (resp. J), and we adopt the shorthand notation $\mathbf{M}_{*,J} = \mathbf{M}_{\{1..n_r\},J}$ and $\mathbf{M}_{I,*} = \mathbf{M}_{I,\{1..n_c\}}$. We also denote by $|\mathbf{M}|$ the determinant of \mathbf{M} . Finally, we use #I to denote the number of elements of a set I.

A field with q elements is denoted \mathbb{F}_q .

For $X \in \mathbb{F}_{q^n}$, we define $X^{[]} := (X^{q^0}, \ldots, X^{q^{n-1}})$, that is the vector of the conjugates of X.

We note \mathbf{I}_n the identity matrix of size n.

Finally we note Tr_n the well known linear mapping trace defined by $\mathrm{Tr}_n:\mathbb{F}_{q^n}\to\mathbb{F}_q,x\mapsto\sum_{i=0}^{n-1}x^{q^i}$

2.2 Univariate and multivariate representations

An extension \mathbb{F}_{q^n} of \mathbb{F}_q can be classically defined as $\mathbb{F}_q[\alpha]$ where α is a primitive element of degree n. \mathbb{F}_{q^n} can be then considered as a vector space over \mathbb{F}_q with basis $(1, \alpha, \ldots, \alpha^{n-1})$. So let X be an element of \mathbb{F}_{q^n} and (x_1, \ldots, x_n) its coordinates over this basis, such that $X = \sum_{i=1}^n x_i \alpha^{i-1}$. Let \mathbf{M}_n be the matrix of $\mathcal{M}_{n \times n}(\mathbb{F}_{q^n})$ whose (i, j)-coefficient is $\alpha^{(i-1)q^{j-1}}$. One can see that the *i*th row of \mathbf{M}_n is $(\alpha^{i-1})^{[l]}$. By construction of \mathbf{M}_n , we have $(x_1, \ldots, x_n)\mathbf{M}_n = X^{[l]}$ and therefore also $(x_1, \ldots, x_n) = X^{[l]}\mathbf{M}_n^{-1}$. So if we define $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$, $X \mapsto X^{[l]}\mathbf{M}_n^{-1}$, then ϕ converts X to its coordinates, and vice-versa for ϕ^{-1} . Additionally, $\phi^{-1}(x_1, \ldots, x_n) = \sum_{i=1}^n x_i \alpha^{i-1}$ can also be seen as the first component of $(x_1, \ldots, x_n)\mathbf{M}_n$.

Linear mappings and matrices: The \mathbb{F}_q -linear polynomial $\mathbf{T}(X) = \sum_{i=0}^{n-1} t_i X^{q^i}$ over \mathbb{F}_{q^n} , can be represented by the matrix T given by:

$$T = (t_{i,j})_{i,j} = \mathbf{M}_n \begin{pmatrix} t_0^{\parallel} \\ \vdots \\ t_{n-1}^{\parallel} \end{pmatrix} \mathbf{M}_n^{-1}.$$

Proof. Let's write $\mathbf{T}(X) = \sum_{j=1}^{n} (\sum_{i=1}^{n} x_i t_{i,j}) \alpha^{j-1}$ using the coordinates over \mathbb{F}_q of T(X). In one hand we have:

$$\mathbf{T}(X)^{[]} = X^{[]} \begin{pmatrix} t_0^{[]} \\ \vdots \\ t_{n-1}^{[]} \end{pmatrix}.$$

On the other hand, $\mathbf{T}(X)^{[]}\mathbf{M}_n^{-1} = (x_1, \ldots, x_n)(t_{i,j})$. Replacing (x_1, \ldots, x_n) by $X^{[]}\mathbf{M}_n^{-1}$ gives

$$X^{[]}\mathbf{M}_{n}^{-1}(t_{i,j}) = X^{[]} \begin{pmatrix} t_{0}^{[]} \\ \vdots \\ t_{n-1}^{[]} \end{pmatrix} \mathbf{M}_{n}^{-1}.$$

Identifying and multiplying by \mathbf{M}_n on the left gives the result.

2.3 The HFE Cryptosystem

We describe here the HFE cryptosystem mostly as in [Pat96a]: the secret trapdoor is a univariate polynomial over a finite field \mathbb{F}_{q^n} :

$$H(X) = \sum_{0 \le i,j \le d} \alpha_{i,j} X^{q^i + q^j}.$$
(1)

There are two reasons for this special form. First d and mostly $D = q^d$ are chosen not too big so that any equation H(X) = h can be solved efficiently³, and second the polynomial H has only monomials of degrees that are sum of two powers of q, so that it has a multivariate representation over \mathbb{F}_q that is quadratic.

There are two more elements in the secret key, they are bijective linear mappings, that can be represented as univariate polynomials over \mathbb{F}_{q^n} : $S(X) = \sum_{0 \leq i < n} s_i X^{q^i}$ and $T(X) = \sum_{0 \leq i < n} t_i X^{q^i}$.

Finally, the public key is the composition

$$P = T \circ H \circ S,\tag{2}$$

where the structure of H is supposed to be hidden by S and T, and therefore P is deemed to be hard to invert without the knowledge of S and T. Equivalently, $\phi \circ P \circ \phi^{-1}$ can be used to describe the public key as a multivariate quadratic system of n equations in n variables.

The HFE polynomial can be used as a trapdoor function both for encryption and signature. The reason is that it is an almost bijective function: for a random h, the equation H(X) = h has only one⁴ solution with probability around e^{-1} .

Encryption: HFE can be used in encryption in the following way. Let a be the sender and b the receiver. a only has the public key P in its possession and wants to send the message $\mathbf{x} = \{x_1, \ldots, x_n\}$. b has the secret key. To encrypt a computes the vector $P(\mathbf{x}) = \{P_1(x_1, \ldots, x_n), \ldots, P_n(x_1, \ldots, x_n)\}$ and sends it to b. To decrypt

1. b inverts the linear map and T and uses the natural morphism to obtain $H(\phi(S(\mathbf{x})))$

³ We assume simply here that the effective degree of H is between $q^d + 1$ and $2q^d$.

⁴ When q is odd, an homogeneous equation has a even number of non zero solutions since H(-X) = H(X).

- 2. b then uses an algorithm like Berlekamp to find $\phi(S(\mathbf{x}))$ (there may be an ambiguity in the value of $\phi(\mathbf{x})$ as H got several roots but a sends a small vector as well to help b decide which root is the right one).
- 3. Finally b invert S and ϕ to obtain the value of **x**

Signature: HFE can be used in signature in the following way. Let a be the signing party and b be the verifier. b only have the public key P in its possession a has the secret key and wants to sign a message y.

At first a wants to sign the message $\mathbf{y} = \{y_1, \dots, y_n\}$ to b

1. *a* must send a vector $\mathbf{x} = \{x_1, \ldots, x_n\}$ that verifies the property

$$\{P_1(x_1,\ldots,x_n)=y_1,\ldots,P_n(x_1,\ldots,x_n)=y_n\}$$

- 2. *a* uses the private key obtain the problem $H(\phi(S(\mathbf{x}))) = \phi^{-1}(T^{-1}(\mathbf{y}))$, and then uses a root finding algorithm (such as Berlekamp algorithm) to find a solution \mathbf{x} .
- 3. a inverts S and ϕ to obtain a message **x** that verifies the property.
- 4. $a \text{ send } \mathbf{x} \text{ to } b \text{ and } b \text{ uses the public key to check if}$

$$\{P_1(x_1,\ldots,x_n)=y_1,\ldots,P_n(x_1,\ldots,x_n)=y_n\}$$

3 Full key recovery attack on HFE

The attacks described in this section aim to find an equivalent secret key for HFE. The goal is to exploit a rank defect in the HFE structure. Usually, the tool used is the resolution of a MinRank problem. Hence, we will make a full introduction of this problem and a way to solve it. In the rest of the paper, we will call this attack MinRank attack instead of Full key recovery attack by abuse of language.

3.1 Introduction to the MinRank problem

Being one of the main tool used to attack HFE it is important to make a quick introduction to the MinRank problem. This problem was first introduced in [BFS99], the authors proved in this paper the NP-completeness of the problem. Then it was used by Kipnis and Shamir in [KS99] in order to attack "unmodified HFE". Since then, it remained a keystone in the Multivariate Quadratic (MQ) cryptography. It is a linear algebra problem that involves minimizing the rank of a linear combination of matrices.

The MinRank problem can be expressed this way:

Definition 1. Let $n, m, r, k \in \mathbb{N}$ and let $\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_k$ $n \times m$ matrices over the field \mathbb{F} . The MinRank problem consists to find u_1, u_2, \dots, u_k over \mathbb{F} such that $\operatorname{rank}(\sum_{i=1}^k u_i \mathbf{M}_i) \leq r$.

3.2 Resolution of the MinRank problem

We will present here a quick explanation on the method used to solve the Min-Rank problem. We will only introduce the support-minors method as it is the one used nowadays. This technique was first introduced by Bardet *et al.* [BBB⁺22].

Let $n, m, r, k \in \mathbb{N}$ and let $\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_k$ be $n \times m$ matrices over the field \mathbb{F} . Let $\mathbf{M} = \sum_{i=1}^k u_i \mathbf{M}_i$ such that rank $(\mathbf{M}) \leq r$ then there exist \mathbf{S} and \mathbf{C} respectively of size $n \times r$ and $r \times m$ such that $\mathbf{M} = \mathbf{SC}$. If one considers \mathbf{r}_j the *j*-th row of the matrix \mathbf{M} , then the rank of the matrix $\mathbf{R}_j = \begin{pmatrix} \mathbf{r}_j \\ \mathbf{C} \end{pmatrix}$ is at most r. Therefore, all maximum minors of \mathbf{R}_j all null, hence we have a new system where the unknown values are the u_i and the maximal minors of \mathbf{C} . The system is nonlinear but can be solved through linearization.

3.3 Application to HFE

First of all we will write the polynomial central map h in a matrix form, using the Macaulay writing meaning that we write $h(X) = \underline{X}\mathbf{H}\underline{X}^t$ where $\underline{X} = (X, X^q, \dots, X^{q^{n-1}})$.

Lemma 1. Let $\mathbf{S}, \mathbf{T} \in M_{n \times n}(\mathbb{F}_q)$ then the public key P can be written

$$P = (\mathbf{P}_1, \dots, \mathbf{P}_n) = (\mathbf{S}\mathbf{M}_n \mathbf{H}^{*0} \mathbf{M}_n^t \mathbf{S}^t, \dots, \mathbf{S}\mathbf{M}_n \mathbf{H}^{*n} \mathbf{M}_n^t \mathbf{S}^t) \mathbf{M}_n^{-1} \mathbf{T}$$

where \mathbf{H}^{*i} is the matrix representation of the q^i th power of the secret polynomial h.

A detailed proof of this lemma can be found in [BFP11], it is essentially based on the formula of ϕ and ϕ^{-1} . The main problem in order to recover the secret key is to find either **T** or **S**, once it is done it is relatively easy to find an equivalent key [BFP11], [TPD21]. We can then extract two different MinRank problems on HFE, one attacking **S** the other attacking **T**.

1. Attack on T. We will first show how to attack T [BFP11].

Let q, n, D be standard HFE parameters, $(\mathbf{P}_1, \dots, \mathbf{P}_n)$ the public key and $\mathbf{T}, \mathbf{S}, \mathbf{H}$ the secret key as defined earlier. Then we have

$$(\mathbf{P}_1,\ldots,\mathbf{P}_n) = (\mathbf{S}\mathbf{M}_n\mathbf{H}^{*0}\mathbf{M}_n^t\mathbf{S}^t,\ldots,\mathbf{S}\mathbf{M}_n\mathbf{H}^{*n}\mathbf{M}_n^t\mathbf{S}^t)\mathbf{M}_n^{-1}\mathbf{T}_n$$

So we can write

$$(\mathbf{P}_1,\ldots,\mathbf{P}_n)\mathbf{T}^{-1}\mathbf{M}_n = (\mathbf{S}\mathbf{M}_n\mathbf{H}^{*0}\mathbf{M}_n^t\mathbf{S}^t,\ldots,\mathbf{S}\mathbf{M}_n\mathbf{H}^{*n-1}\mathbf{M}_n^t\mathbf{S}^t).$$

We will write $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_n$ and $\mathbf{W} = \mathbf{S}\mathbf{M}_n$. Then we have

$$(\mathbf{P}_1,\ldots,\mathbf{P}_n)\mathbf{U} = (\mathbf{W}\mathbf{H}^{*0}\mathbf{W}^t,\ldots,\mathbf{W}\mathbf{H}^{*n}\mathbf{W}^t).$$

Let $(u_{0,0}, u_{1,0}, \ldots, u_{n-1,0})$ be the first column of **U** then we have

$$\sum_{i=0}^{n-1} u_{0,i} \mathbf{P}_i = \mathbf{W} \mathbf{H} \mathbf{W}^t.$$

 $6~{\rm of}~24$

Recall that

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & 0 \\ 0 & 0 \end{pmatrix}$$

where **A** is a matrix of size $d = \log_{q}(D)$. Hence

$$\operatorname{rank}(\sum_{i=0}^{n-1} u_{0,i} \mathbf{P}_i) = \log_q(D)$$

which is small so finding the first column of **U** reduces to solve a MinRank instance with k = n and $r = \log_a(D)$ on the matrices $\mathbf{P}_1, \ldots, \mathbf{P}_n$.

Remark that the matrix product $\mathbf{T}^{-1}\mathbf{M}_n$ is special as finding the first column means finding the whole matrix because one has

$$\forall (i,j) \in \{0 \dots n-1\} \times \{1 \dots n-1\} u_{i,j} = u_{i,j-1}^q$$

Hence, we are able to find \mathbf{T} by solving the previous MinRank instance.

2. Attack on S. Now we can do a similar thing in order to attack S. It was first proposed by Ward Beullens and by Tao *et al.* [TPD21].

Proposition 1. Retaining the notations U and W from the previous attack, we have $(\mathbf{P}_1, \dots, \mathbf{P}_{n-1}) = (\mathbf{W}\mathbf{H}^{*0}\mathbf{W}^t, \dots, \mathbf{W}\mathbf{H}^{*n-1}\mathbf{W}^t)\mathbf{U}^{-1}$. Then we obtain

$$(\mathbf{W}^{-1}\mathbf{P}_{1}\mathbf{W}^{-1,t},\ldots,\mathbf{W}^{-1}\mathbf{P}_{n-1}\mathbf{W}^{-1,t}) = (\mathbf{H}^{*0},\ldots,\mathbf{H}^{*n-1})\mathbf{U}^{-1}.$$

If one notes $\mathbf{Q} = (\mathbf{U}^{-1})^{t} \begin{pmatrix} a_{0} \\ \vdots \\ a_{n} \end{pmatrix}$ where a_{i} is the first row of the matrix \mathbf{H}^{*t}

then $\mathbf{Q} = (\mathbf{U}^{-1})^t \begin{pmatrix} \mathbf{A}_1 \\ 0 \\ \mathbf{A}_2 \end{pmatrix}$ where \mathbf{A}_1 is an $1 \times n$ matrix, and \mathbf{A}_2 is a $(d-1) \times n$

matrix and rank(\mathbf{Q}) $\leq d$ where $d = \log_q(D)$.

Furthermore, using the proposition above and the matrix equation of HFE:

Theorem 1. Let $\mathbf{P}_1, \ldots, \mathbf{P}_n$ matrices of the public key and \mathbf{W} the matrix previously defined. If one notes $(w_0^{-1}, w_1^{-1}, \ldots, w_{n-1}^{-1})$ the first row of the matrix \mathbf{W}^{-1} , and $b_i = (w_0^{-1}, w_1^{-1}, \ldots, w_{n-1}^{-1})\mathbf{P}_i$, then the matrix \mathbf{Z} whose rows are the b_i has a rank at most d.

Proof. From the previous proposition we know that the rank of \mathbf{ZW}^{-1^t} is bounded by d, hence the rank of \mathbf{Z} is bounded by d

We then have a MinRank attack on **S** with \mathbf{P}_i as the matrices, d as the rank and w_i^{-1} as the target vector. Just like for **T**, once we have the first row of \mathbf{W}^{-1} we have the whole matrix. Hence, we can recover **S**.

We will not describe how we recover the whole key once \mathbf{T} or \mathbf{S} is discovered as the complexity of the attack is mainly the complexity of solving the MinRank problem. For more details for the recovery of the totality of the key please refer to [BFP11], [TPD21]. **3. Complexity of the Attacks.** The complexity of these attacks is the same, as they both only involve solving a MinRank problem. We have a complexity of $\mathcal{O}\left(d(n-1)^4 \binom{2d+1}{d}^2\right)$ [BBC⁺22]. One may note that at first glance the two attacks are extremely similar, and it seems that there is no point having two of them. In fact, this is true for plain HFE, however when we consider variants of HFE we will see that there is often an attack that is more efficient than the other. It is also important to note that it is possible to use two or more variants at the same time, indeed published scheme like GeMSS were using two variants (vinegar and minus). Nevertheless in Section 5 we will only consider variants used alone.

3.4 About characteristic 2

The MinRank attack requires a discussion on the characteristic on the field and on the parity of the rank of the HFE central map. Indeed, when used on characteristic 2, the resolution of the MinRank instance may yield too many solutions if the targeted rank is even. Then some of the solutions must be discarded as they do not yield an equivalent key. However, previous work on HFE like the paper [BFP11] found a variant of the attack that has the same complexity that we mentioned. So in the rest of the paper, we will not mention the special case of characteristic 2 as it will not change the complexity of the cryptanalysis.

4 Direct attacks on HFE

In this section we will discuss direct attacks on HFE. The aim is not to find an equivalent key but rather to invert the system in order to find the original message or forge a signature. Many tools can be used like XL or Gröbner basis, but we will focus on the Gröbner basis approach. Usually instead of direct attack we call this attack Gröbner basis attack by abuse of language. We will not describe the main algorithms used nowadays (F4, F5 [Fau99][Fau02]) rather present the general ideas on Gröbner basis. Let I be an ideal of $\mathbb{F}[X_1, X_2, \dots, X_n]$ where \mathbb{F} is a field. Basically a Gröbner basis is a set of polynomials G that are generator of I. We add a few properties to make this set G unique for each ideal I. The set G depends on the order you take on the monomials. For our purpose the important order will be the lexicographic order. Indeed this order gives the property that the set G forms a triangular system, in other words if one considers a set of polynomials $\{P_1(x_1,\ldots,x_n),\ldots,P_k(x_1,\ldots,x_n)\}$ then the lexicographic Gröbner basis of the ideal generated by the P_i will be of the form: $G = \{G_1(x_1), G_2(x_1, x_2), \dots, G_m(x_1, \dots, x_n)\}$. Hence it can be used to find a solution (x_1, \ldots, x_n) of a system

$$P_1(x_1, \dots, x_n) = y_1$$
$$P_2(x_1, \dots, x_n) = y_2$$
$$\vdots$$
$$P_k(x_1, \dots, x_n) = y_k.$$

Indeed let $G = \{G_1(X_1), G_2(X_1, X_2), \dots, G_m(X_1, \dots, X_n)\}$ be the Gröbner basis of the ideal generated by $P_1(X_1, \dots, X_n) - y_1, \dots, P_k(X_1, \dots, X_n) - y_k$. We then have an equivalent system of equation:

$$G_1(x_1) = 0$$

$$G_2(x_1, x_2) = 0$$

$$\vdots$$

$$G_m(x_1, \dots, x_n) = 0.$$

So the resolution is simply to find first x_1 as root of $G_1(X)$ (with an algorithm like Cantor-Zassenhauss for finite fields [CZ81]), then the roots of the polynomial $G_2(x_1, X)$ and so on. In other words, Gröbner bases can be used to solve multivariate systems of polynomials. We can then use Gröbner bases to attack HFE and its variants. It will not be a full key recovery like MinRank attacks but rather a forgery tool in the case of signature or a plain text recovery in the case of encryption.

The complexity of the computation of a Gröbner basis is hard to determine. Indeed we can write the complexity as $\mathcal{O}\binom{n+d_{reg}}{n}^{\omega}$, (ω is the linear algebra constant, usually we consider $\omega \approx 2.81$). The problem is to determine the value of d_{reg} or "degree of regularity".

Definition 2. [DS13] We define $B = \mathbb{F}[X_1, \ldots, X_n]/\langle X_1^q, \ldots, X_n^q \rangle$ and B_d it's degree d subspace. Let P be a set of homogeneous polynomial $P = \{P_1, \ldots, P_m\} \subset B_2^m$.

Let ψ_d be the map $\psi_d: B^m_d \to B_{d+2}$ defined as

$$\psi(b_1,\ldots,b_m)=\sum_{i=1}^m b_i P_i$$

Then

$$R_d(P_1,\ldots,P_m) := \ker(\psi_d).$$

Further let $T_d(P_1, \ldots, P_m)$ be the subspace of trivial relations generated by the elements

$$\{b(P_i e_j - P_j e_i) | 1 \le i < j \le m, b \in B_{d-2}\},\$$

and

$$\{b(P_i^{q-1})e_i | 1 \le i \le m, b \in B_{d-2(q-1)}\}.$$

Here e_i means the *i*-th unit vector consisting of all zeros except 1 at the *i*-th position $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. The degree of regularity of a homogeneous quadratic set is then

$$Dreg(P_1, \ldots, P_m) := min\{d | R_{d-2}(P_1, \ldots, P_m) / T_{d-2}(P_1, \ldots, P_m) \neq \{0\}\}.$$

For a general system of polynomial, it is not possible to compute the degree of regularity without computing the Gröbner basis. However in the case of HFE, it is possible to find an upper bound for the degree of regularity [DY13]. The upper bound Ding and Yang have found is: $\frac{(q-1)(d-1)}{2} + 2$ if q is even and d is odd, $\frac{(q-1)d}{2} + 2$ otherwise $(d = \log_q(D))$. This upper bound is close to real values of degree of regularity. Although this upper bound is as tight as possible, Petzoldt [Pet17] has found a lower bound allowing us to have a more precise idea on the value of the degree of regularity. Indeed for q = 2 we have $d_{reg} \ge \lfloor \frac{d}{3} \rfloor + 2$. We will keep this value for the rest of the paper.

5 Variants of HFE

5.1 Vinegar (v) variant

The first modifier that we will consider is v. It adds variables y_i into the system. The v stands for vinegar, in an analogue to the scheme UOV (Unbalanced Oil and Vinegar). To decipher one will fix the vinegar variables and solve the system. We can define this modifier that way:

Definition 3. Let $v \in \mathbb{N}$ and $y = (y_1, \ldots, y_v)$, then the new secret polynomial $f : \mathbb{F}_{q^n} \times \mathbb{F}_q^v \to \mathbb{F}_{q^n}$ is of the form:

$$\sum_{j \in \mathbb{N}, q^i + q^j \le D} \alpha_i X^{q^i + q^j} + \sum_{i, q^i \le D} \beta_i(y) X^{q^i} + \gamma(y)$$

where $\beta_i : \mathbb{F}_q^v \to \mathbb{F}_{q^n}$ are linear maps and $\gamma : \mathbb{F}_q^v \to \mathbb{F}_{q^n}$ is a quadratic map. So the central map becomes $\tilde{\mathbf{H}} = \begin{pmatrix} \mathbf{H} & A \\ B & C \end{pmatrix}$. where \mathbf{A} , \mathbf{B} , \mathbf{C} are random matrices. remark however that $\mathbf{A} = \begin{pmatrix} 0 & 0 \\ \mathbf{A}' & 0 \end{pmatrix}$ where \mathbf{A} is a block of size $d \times v$, $\mathbf{B} = \begin{pmatrix} 0 & \mathbf{B}' \\ 0 & 0 \end{pmatrix}$ where \mathbf{B} is a block of size $v \times d$ and \mathbf{C} a matrix of size $v \times v$

hence the rank of the matrix \mathbf{H} is d + v.

Furthermore, the linear transformations must also change accordingly. Indeed **S** is now a full rank linear map $\mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n+v}$. **T** remains unchanged. If we use the previous notation **U** and **W** recall that $\mathbf{W} = \mathbf{SM}_n$ and $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_n$. Obviously as **S** is no more of size n, \mathbf{M}_n in **W** must change. So **W** becomes $\mathbf{W} = \mathbf{S}\tilde{\mathbf{M}}_n$ where $\tilde{\mathbf{M}}_n = \begin{pmatrix} \mathbf{M}_n & 0 \\ 0 & \mathbf{I}_v \end{pmatrix}$.

We can note that $\mathbf{\hat{U}}$ remains unchanged.

This variant has negligible cost when used in signature as the signer only needs to solve a system $z = H_v(x)$ where H_v is the central map of a HFEv. In order to do so he simply fixes randomly the variable v until he is able to find a solution to the rest of the system.

However, this variant is costly in encryption. In order to decrypt the system, one must find the exact x that works hence he needs to do a exhaustive search on the y_i which means a cost of q^v times the complexity of HFE it means that it is extremely costly in encryption.

To make a cryptanalysis of this variant we can do an attack on **S**. We use the equation we wrote in the previous section 3 but with the new $\mathbf{W} = \mathbf{S}\tilde{\mathbf{M}}_n$:

$$(\mathbf{W}^{-1}\mathbf{P}_{1}\mathbf{W}^{-1,t},\ldots,\mathbf{W}^{-1}\mathbf{P}_{n-1}\mathbf{W}^{-1,t}) = (\mathbf{H}^{*0},\ldots,\mathbf{H}^{*n-1})\mathbf{U}^{-1}$$

However the matrix **Q** previously defined is still of the form: $\mathbf{Q} = (\mathbf{U}^{-1})^t \begin{pmatrix} \mathbf{A}_1 \\ 0 \\ \mathbf{A}_2 \end{pmatrix}$,

thus the rank has not changed (r = d). The only difference is the number of equations we get, indeed we now have $(n + v)\binom{2d+1}{d}$ equations. It leads to a slight increase in complexity, which is now $\mathcal{O}\left(dn(n + v - 1)^3\binom{2d+1}{d}^2\right)$.

If we had done the attack on the other way meaning that we try to break **T** we would have had: $(\mathbf{P}_0, \ldots, \mathbf{P}_{n-1})\mathbf{U} = (\mathbf{W}\tilde{\mathbf{H}}^{*0}\mathbf{W}^t, \ldots, \mathbf{W}\tilde{\mathbf{H}}^{*n}\mathbf{W}^t)$. As stated earlier the rank of the matrix $\tilde{\mathbf{H}}^{*0}$ is now r = d + v. Which means we now have a complexity of $\mathcal{O}\left((d+v)(n-1)^4 {\binom{2(d+v)+1}{d+v}}^2\right)$.

If we look at the direct attack (Gröbner basis), it seems that the result resembles what was found for the MinRank attack on **T**. Indeed one should replace d by d + v in the formula we introduced in section $4 \frac{(q-1)(d+v-1)}{2} + 2$ if q is even and d is odd, $\frac{(q-1)(d+v)}{2} + 2$ otherwise. The lower bound becomes for q = 2, $d_{reg} \ge \lfloor \frac{d+v}{3} \rfloor + 2$.

5.2 Minus

The variant – is simply a suppression of some polynomials of the public key of a unmodified HFE. For example if the public key of a HFE is $P = (\mathbf{P}_0, \dots, \mathbf{P}_{n-1})$ then the public key a HFE– will be $P_- = (\mathbf{P}_0, \mathbf{P}_1, \dots, \mathbf{P}_{n-1-a})$ where *a* is the number of equations that were suppressed. If we rewrite it in a matrix form it simply means that *T* is a full rank linear map $\mathbb{F}_q^n \to \mathbb{F}_q^{n-a}$. **S** and \mathbf{M}_n remains unchanged.

This variant cost is almost negligible when using HFE in signature as the signer can randomly complete the matrix \mathbf{T} to make it invertible and solve it like a unmodified HFE. Indeed, this variant does not change the central map.

However, this variant is costly in encryption. In order to decrypt the system, one must find the exact x that works hence he needs to do a exhaustive search on the missing polynomials it means a cost of q^a times the complexity of HFE it means that it is extremely costly in encryption.

We can try an attack on \mathbf{T} : we however cannot write

$$(\mathbf{P}_0,\ldots,\mathbf{P}_{n-1})\mathbf{U} = (\mathbf{W}\mathbf{H}^{*0}\mathbf{W}^t,\ldots,\mathbf{W}\mathbf{H}^{*n}\mathbf{W}^t)$$

as **U** is not invertible any more we can however rewrite $T = T^+ \circ L_a$ where $T^+ : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a bijective extension of T and L_a is a linear polynomial of degree q^a . It means that our central map is equivalent to a standard HFE with $D' = q^a D$ [VS17]. We note $\tilde{H} = L_a \circ H$. So we now have

$$(\mathbf{P}_0,\ldots,\mathbf{P}_{n-1})\mathbf{T}^{+^{-1}}\mathbf{M}_n = (\mathbf{W}\tilde{\mathbf{H}}^{*0}\mathbf{W}^t,\ldots,\mathbf{W}\tilde{\mathbf{H}}^{*n}\mathbf{W}^t).$$

We have now the same equation as in Proposition 2 but with a target rank of r = d + a. So the complexity is now: $\mathcal{O}\left((d+a)(n-1)^4 \binom{2(d+a)+1}{d+a}^2\right)$.

We can also try an attack on S: as in [BBC⁺22] we can write

$$(\mathbf{W}^{-1}\mathbf{P}_1\mathbf{W}^{-1,t},\ldots,\mathbf{W}^{-1}\mathbf{P}_{n-1}\mathbf{W}^{-1,t}) = (\mathbf{H}^{*0},\ldots,\mathbf{H}^{*n-1})\mathbf{U}^{-1}.$$

However this time the rank on the right has not changed (r = d) so we have the exact same attack so the complexity is still

$$\mathcal{O}\left(d(n-1)^4 \binom{2d+1}{d}^2\right).$$

If we look at the direct attack (Gröbner), it seems that the result resembles what was found for the MinRank attack on **T**. Indeed one should replace d by d+a in the upper bound we introduced in section $4 \frac{(q-1)(d+a-1)}{2} + 2$ if q is even and d+a is odd, $\frac{(q+a)(d)}{2} + 2$ otherwise. The lower bound becomes for q = 2, $d_{reg} \ge \lfloor \frac{d+a}{3} \rfloor + 2$.

5.3 Plus

The variant + adds random equations on the public key. This means that if $P = (\mathbf{P}_0, \dots, \mathbf{P}_{n-1})$ is the public key then the public key of HFE+ is $P_+ = (\mathbf{P}_0, \dots, \mathbf{P}_{n-1}, \mathbf{P}_n, \dots, \mathbf{P}_{n-1+k})$ where $P_i, n < i : \mathbb{F}_q \to \mathbb{F}_q$ and k the number of added equations. Note that the equations of the public key are then linearly mixed.

This variant has a negligible cost in encryption, as to decipher one can ignore the added equations. So, it can be inverted. However, it costs q^k in signature because one must first solve the system ignoring the added polynomials and then check if it is compatible with the added polynomials. Obviously as the *n* first polynomials remain untouched by the modifiers we can still find a linear combination of the *n* first polynomials of small rank. Hence, we can find a combination of all the polynomials of small rank.

5.4 Projection

The variant p or projection [CS17] consists in replacing the map $S : \mathbb{F}_q^n \to \mathbb{F}_q^n$ by $S = L \circ S' : \mathbb{F}_q^{n-p} \to \mathbb{F}_q^n$ where $S' : \mathbb{F}_q^{n-p} \to \mathbb{F}_q^{n-p}$ is full rank and $L : \mathbb{F}_q^{n-p} \to \mathbb{F}_q^n$ is a linear polynomial of degree p that is also full rank. This time $\mathbf{W} = \mathbf{S'}\mathbf{M}_n$.

The complexity of this variant in encryption, is almost the same as a plain HFE as to decipher one can ignore the modifier because it is an injective linear map. So it can be inverted. However it costs a factor q^p in signature because one must first solve the system ignoring the projection and then check if it is compatible with the projection.

We can try an attack on S: we can write

 $(\mathbf{W}^{-1}\mathbf{P}_1\mathbf{W}^{-1,t},\ldots,\mathbf{W}^{-1}\mathbf{P}_{n-1}\mathbf{W}^{-1,t}) = (\mathbf{L}\mathbf{H}^{*0}\mathbf{L}^t,\ldots,\mathbf{L}\mathbf{H}^{*n-1}\mathbf{L}^t)\mathbf{U}^{-1}.$

Indeed, taking the first row of each matrix on the right, we have now the same equation as in Proposition 3 but with a target rank of r = d+p. So the complexity is now: $\mathcal{O}\left((d+p)(n-1)^4 \binom{2(d+p)+1}{d+p}^2\right)$ [BBC+22]. However, if we do an attack on **T**, the equation becomes $(\mathbf{P}_0, \ldots, \mathbf{P}_{n-1})\mathbf{U} = (\mathbf{WLH}^{*0}\mathbf{L}^t\mathbf{W}^t, \ldots, \mathbf{WLH}^{*n}\mathbf{L}^t\mathbf{W}^t)$ and the targeted rank is the rank of the matrix $\mathbf{WLH}^{*0}\mathbf{L}^t\mathbf{W}^t$. However, the p modifier does not change the rank of the central map. Indeed the rank of **H** is at most d so the rank of $\mathbf{WLH}^{*0}\mathbf{L}^t\mathbf{W}^t$ is at most r = d because it is a matrix product. So the complexity is $\mathcal{O}\left(d(n-1)^4\binom{2d+1}{d}^2\right)$. The article [CS17] made an analysis of the degree of regularity and found that projection had $d_{reg} = \frac{(q-1)(d+p)}{2} + 2$

5.5 Internal plus $(\hat{+})$

In this section we are going to describe the internal plus $(\hat{+})$ variant as introduced in the paper [FmRPP22]. It adds new equations internally in order to increase the rank of the central map. By "internally" we mean two things:

- The final number of public equation is the same as initially (unlike the + perturbation above)
- The linear transformations S and T are done after the addition of these new equations

. Formally, let t be the parameter of the modifier, let $\beta_i \in \mathbb{F}_{q^n}$ for $i \in \{1 \dots t\}$ be random elements, and $\hat{p}_i(x) = \operatorname{Tr}_n\left(\sum_{j,k} \alpha_{i,j,k} x^{q^j + q^k}\right)$ where $\alpha_{i,j,k}$ are random element of \mathbb{F}_{q^n} and let $Q(x) = \sum_i \beta_i \hat{p}_i(x)$. The central map of the modifier is F(x) = H(x) + Q(x) where H(x) is the central map of a "unmodified HFE" and Q(x) the polynomial previously defined.

The degree of F(x) is much greater than the degree of H(x). Due to the presence of Q(x) it will be q^{n-1} . It means that direct methods of resolution such as Berlekamp algorithm are no longer possible. We can however use the fact that $\hat{p}_i(x)$ is a polynomial in \mathbb{F}_q so we can make an exhaustive search of the value of each $\hat{p}_i(x)$ which means that Q(x) can take at most q^t possibilities. Thus we end up with a variant q^t times slower in decryption or signature than a "unmodified" HFE.

It is important to note that the rank of the central map is very likely to be maximal even with a small t since β_i are chosen randomly hence the polynomial F(x) can have a very high degree. However, it does not mean that MinRank attacks will not work. We have:

$$(\mathbf{P}_1,\ldots,\mathbf{P}_n) = (\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^t,\ldots,\mathbf{W}\mathbf{F}^{*n-1}\mathbf{W}^t)\mathbf{U}^{-1},$$

which gives

$$(\mathbf{W}^{-1}\mathbf{P}_1\mathbf{W}^{-1,t},\ldots,\mathbf{W}^{-1}\mathbf{P}_n\mathbf{W}^{-1,t}) = (\mathbf{F}^{*0},\ldots,\mathbf{F}^{*n-1})\mathbf{U}^{-1}.$$

Let us note $\mathbf{Z} = (\mathbf{U}^{-1})^t \begin{pmatrix} \mathbf{a}_0 \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$ where \mathbf{a}_i is the first row of the matrix \mathbf{F}^{*i} . Recall that for previous attacks on \mathbf{S} we had:

 $\mathbf{Z} = (\mathbf{U}^{-1})^t \begin{pmatrix} \mathbf{A}_1 \\ 0 \\ \mathbf{A}_2 \end{pmatrix}$. Unfortunately, it is no longer the case. Indeed, the matrix that represents \mathbf{F} is now full. However, we can decompose $\mathbf{F} = \mathbf{H} + \mathbf{Q}$. Then

$$\mathbf{Z} = \left(\mathbf{U}^{-1}\right)^t \times \left(\begin{pmatrix} \mathbf{A}_1 \\ 0 \\ \mathbf{A}_2 \end{pmatrix} + \begin{pmatrix} \mathbf{q}_0 \\ \vdots \\ \mathbf{q}_n \end{pmatrix} \right).$$

The Froebenius operation being linear we will study the matrix $\begin{pmatrix} \mathbf{q}_0 \\ \vdots \\ \mathbf{q}_n \end{pmatrix}$ sep-

arately.

We can write that \mathbf{q}_i is the first row of the matrix $\sum_{i=0}^t \beta_i^{q^i} \mathbf{Q}_i$. Indeed \mathbf{Q}_i is the representative matrix of the polynomial $\hat{p}_i(x)$ whose image is in \mathbb{F}_q . Hence the polynomial is unchanged by the Froebenius.

It means that the rank of the matrix **Q** is at most t and thus the rank of the (\mathbf{A}_1) (\mathbf{q}_0)

matrix
$$\begin{pmatrix} \mathbf{A}_1 \\ 0 \\ \mathbf{A}_2 \end{pmatrix} + \begin{pmatrix} \mathbf{q}_0 \\ \vdots \\ \mathbf{q}_n \end{pmatrix}$$
 is at most $r = d + t$.

So the complexity of the attack is the complexity of a MinRank whose target rank is r = d + t: $\mathcal{O}\left((d + t)(n - 1)^4 {\binom{2(d+t)+1}{d+t}}^2\right)$

The attack on **T** r the rank of the central map **H** is now most likely maximal. However, an better attack is still possible as it is possible to find a projection Π such that $\Pi(\beta_i) = 0$ then by composing on left and right we obtain a central whose rank is r = d + t so we obtain the same complexity as the attack on **S**: $\mathcal{O}\left((d+t)(n-1)^4 {\binom{2(d+t)+1}{d+t}}^2\right).$

According [FmRPP22] to the article the degree of regularity is $d_{reg} = \frac{(q-1)(d+p)}{2} + 2$

5.6 Internal perturbation (IP)

The idea of this modifier is similar to the vinegar modifier, it was first introduced in [DS05]. We add a variable Y that is linear combination of X variable, that combination should be of small rank to be able to invert the system. So we have a linear map $Z : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ of low rank π . Then the central map $f : \mathbb{F}_{q^n} \to$ \mathbb{F}_{q^n} is of the form: $\sum_{i,j\in\mathbb{N},q^i+q^j\leq D} \alpha_i X^{q^i+q^j} + \sum_{i,q^i\leq D} \beta_i(Y) X^{q^i} + \bar{P}(Y)$ where $\beta_i : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ are linear maps and $\bar{P} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is a quadratic map and Y = Z(X). A description of this modifier can be found in [DS05]. To decrypt one must try to solve the system without the modifier and hope it will nullify the modifier as well, meaning an increase of a factor q^{π} times the complexity to decrypt or to sign compared to "unmodified HFE".

In terms of rank, it means that the rank of the central map has increased by π . It means that when attacking **T** the target rank will be the one of the central maps. It means that the attack the complexity will be:

$$\mathcal{O}\left((d+\pi)(n-1)^4\binom{2(d+\pi)+1}{d+\pi}^2\right).$$

However, the effect is drastically different when attacking via **S**. Indeed, recall that when attacking S one consider the rank of the matrix $\mathbf{Q} = (\mathbf{U}^{-1})^t \begin{pmatrix} \mathbf{a}_0 \\ \vdots \\ \mathbf{a} \end{pmatrix}$

where \mathbf{a}_i is the first row of the matrix F^{*i} . Although the rank of the F^{*i} is $d + \pi$ the matrix F^{*i} is full. Indeed, the polynomial F(X) have a degree $q^n - 1$. Thus, one cannot write $\mathbf{Q} = (\mathbf{U}^{-1})^t \begin{pmatrix} \mathbf{A}_1 \\ 0 \\ \mathbf{A}_2 \end{pmatrix}$.

We cannot evaluate easily the rank of \mathbf{Q} , but we have observed that for small values of $\pi = (1, 2, 3, 4, 5)$ the rank of \mathbf{Q} is far greater than $d + \pi$. For example, for $n = 20, q = 2, D = 9, \pi = 1$ we observe that the rank of \mathbf{Q} is between 11 and 15 far greater than $d + \pi = 5$. Overall, we have observed that for $1 < \pi$ the rank of the matrix \mathbf{Q} is above n/2. It is the rank we will retain for our complexity evaluation (when π grows the rank quickly becomes far above n/2).

It is important to note that there is another type of attack specific to this variant. Dubois *et al.* [DGS07] have found a differential attack on this variant. They can make a recovery of the kernel of the linear map Z. Once the linear map is discovered, the internal perturbation can be negated. In the following section we will note $DP_{\mathbf{y}}(x) = P(a+x) - P(x) - P(a) + P(0)$ as the discrete differential of P in the vector \mathbf{y} The key to this attack is the following observation:

- If **a** is a vector that is not in the kernel of Z then the differential of the public key in **a** will be written with the form: $D\tilde{P}_{\mathbf{a}}(x) = DP_{\mathbf{a}}(x) + M(x, Z(\mathbf{a})) + M(\mathbf{a}, Z(x)) + D\bar{P}_{Z(\mathbf{a})}(Z(x))$, where \tilde{P} is the public key, P is the public key without the internal perturbation, M the mixing part and \bar{P} the polynomial in y.
- However when **a** is in ker(Z) then $D\tilde{P}_{\mathbf{a}}(x) = DP_{\mathbf{a}}(x) + M(\mathbf{a}, Z(x)).$

Clearly the two forms are quite different. Hence the authors are using these differences to create a non-deterministic distinguisher that can detect whether or not an element **a** is in ker(Z). In order to make a recovery of the kernel to obtain n distinct element of ker(Z), and the number of element that are in ker(Z) is $q^{n-\pi}$ so the number of utilisation of the distinguisher is about $n \times q^{\pi+1}$. The complexity of the attack is then $n \times q^{\pi+1}N$, where N is the complexity of the distinguisher.

The complexity of the distinguisher is difficult to describe briefly. Indeed its calculation is not given by a simple direct formula but requires to solve linear systems. Nonetheless our tests showed that on modern parameters the complexity is high. More details on this matter can be found on the paper [DGS07]. We have computed the complexity of the attack and found that for parameters of HFE with q = 2, n = 177, D = 17 (one can note we used red-GeMSS-128 parameters where we got rid of the modifiers used in GeMSS) with a rank of the internal perturbation of (1,2,3,4,5). Our results are recapped in Table 1

| | IP | complexity |
|---|----|------------|
| [| 1 | 106.26 |
| | 2 | 130.92 |
| | 3 | 150.20 |
| | 4 | 173.58 |
| ſ | 5 | 196.70 |

Table 1. Complexity of the attack from [DGS07] on HFEIP with q = 2, n = 177, D = 17, the complexity are given in \log_2 .

It means that with few of these modifiers we have attacks less effective than MinRank attacks.

We can also look at a Gröbner basis perspective. This variant is very similar to the v variant so the degree of regularity is the same. Indeed one should replace d + v by $d + \pi$ in the formula we introduced in Section 4: $\frac{(q-1)(d+\pi-1)}{2} + 2$ if q is even and d is odd, $\frac{(q-1)(d+\pi)}{2} + 2$ otherwise [DY13]. Although the lower bound was not computed in [Pet17] we can easily conjecture that it will be for q = 2, $d_{req} \geq \lfloor \frac{r+\pi}{3} \rfloor + 2$ due to the similarities with v variant.

6 Summaries of the complexities

In Table 2, 3 we have recapped all complexity results.

Table 2 also shows the cost to sign/decrypt of every variant. These costs do limit the combinations we are able to use without making the scheme too slow. We see from these Tables that it is relatively easy to avoid a specific attack, the problem is to avoid all of them.

For example, in order to avoid Gröbner Basis attacks (i.e direct attacks) we can have d large or, q large, or v large, or a large, or π large. In signature, v large or a large, or q large seems to be good solutions since their cost are negligible. In encryption q large also has small cost with HFE, but the other perturbations have a non negligible cost.

In order to avoid MinRank **T** we can have d large, or v large, or a large, or t large, or π large. In signature v large, or a large have a very small cost.

| | MinRank \mathbf{T} | MinRank \mathbf{S} | | Signature cost | Decryption cost |
|---------|----------------------|----------------------|------------------------------|------------------------|------------------------|
| vanilla | | d | $\frac{(q-1)(d)}{2} + 2$ | | |
| v | d+v | Little effect | $\frac{(q-1)(d+v)}{2} + 2$ | Negligible | $\mathcal{O}(q^v)$ |
| + | | Little effect | | $\mathcal{O}(q^t)$ | Negligible |
| - | d+a | Little effect | $\frac{(q-1)(d+a)}{2} + 2$ | Negligible | $\mathcal{O}(q^a)$ |
| р | Little effect | d+p | Little effect | $\mathcal{O}(q^p)$ | Negligible |
| Ĥ | d+t | d+t | Little effect | $\mathcal{O}(q^t)$ | $\mathcal{O}(q^t)$ |
| IP | $d + \pi$ | $\geq n/2$ | $\frac{(q-1)(d+\pi)}{2} + 2$ | $\mathcal{O}(q^{\pi})$ | $\mathcal{O}(q^{\pi})$ |

Table 2. Simplified Table of the effect of each variants on the complexity of the attacks and their respective cost depending on the mode used. For MinRank we show here the target rank and for Gröbner Basis the degree of regularity (c.f Table 3 for the complexities). Here little effect means the same as in vanilla HFE, so rank = d and degree of regularity $deg = \frac{(q-1)(d)}{2} + 2$. The blank in the vanilla HFE cost is here because the cost should be read in comparison to a vanilla HFE with similar parameters

However in this table we cannot find an effective (i.e not too costly) perturbation against this attack. We can notice that in MinRank \mathbf{T} we will need almost all the equations of the public key for the attack (it explains why – and indirectly v is so efficient).

In order to avoid MinRank **S** we can have d large, or p large, or t large. A very small π is also sufficient (against MinRank **S** it seems that even $\pi = 1$ is sufficient, however due to [DGS07] we need at least $\pi = 3$). In signature all of these perturbations have a cost. However IP (π) seems to be the best solution. Indeed the IP perturbation increases the rank much faster than it's counterpart. In encryption p (projection) seems to be the best solution as it does not cost much, and IP is also a reasonable good solution due to the rapid increase of the rank. We can notice that according to [BBC⁺22], the MinRank **S** only require at least 2d + 1 of the public key equations (i.e only a small number of the public equation, unlike MinRank **T**).

7 On the security of pHFEv-

The HFEv- combination has already been explored for signature schemes, for example in the GeMSS NIST-PQ submission [CFMR⁺20]. This scheme has later been broken in [BBC⁺22]. The projection variant that we introduced earlier was quite recently used to try to repair HFEv- and GeMSS [CFMR⁺20]. This reparation was first mentioned in [ØSV21]. The new scheme would have been called pHFEv-. The reason for this scheme was to counter attacks on **S** because both variant v and minus don't have any effect on this attack. However, with the projection modifier the rank of the matrix we were attacking is increased by p (projection parameter). Nonetheless as GeMSS is a signature scheme, the use of the projection variant induces an increase of the complexity of the signature by a factor q^p . Hence in order to have an efficient scheme, p must remain small. But improvement of **S** attacks discovered by [BBC⁺22] made pHFEv- again

| | Mi | nRank T | Mi | nRank S | Gröbner basis |
|---------|-----------------------------|---|----------|--|------------------------------|
| Vanilla | 0 (| $\left(d(n-1)^4 \binom{2d+1}{d}^2\right)$ | 0 (| $\left(d(n-1)^4 \binom{2d+1}{d}^2\right)$ | $\frac{(q-1)(d)}{2} + 2$ |
| v | 0 (| $((d+v)(n-1)^4 {\binom{2(d+v)+1}{d}}^2)$ | 0 (| $\left(d(n-1+v)^4 \binom{2d+1}{d}^2\right)$ | $\frac{(q-1)(d+v)}{2} + 2$ |
| + | 0 (| $\left(d(n-1)^4 \binom{2d+1}{d}^2\right)$ | 0 (| $\left(d(n-1)^4 \binom{2d+1}{d}^2\right)$ | Little effect |
| - | 0 (| $\left((d+a)(n-1)^4 {\binom{2(d+a)+1}{d+a}}^2 \right)$ | 0 (| $\left(d(n-1)^4 \binom{2d+1}{d}^2\right)$ | $\frac{(q-1)(d+a)}{2} + 2$ |
| р | 0 (| $\left(\frac{d(n-1)^4 \binom{2d+1}{d}^2}{2}\right)$ | 0 (| $\left((d_p)(n-1)^4 \binom{2(d_p)+1}{d_p}^2 \right)$ | $\frac{(q-1)(d+p)}{2} + 2$ |
| Ĥ. | 0 (| $\left((d+t)(n-1)^4 {\binom{2(d+t)+1}{d+t}}^2 \right)$ | 0 (| $\left((d_p)(n-1)^4 {\binom{2(d+t)+1}{d+t}}^2 \right)$ | $\frac{(q-1)(d+t)}{2} + 2$ |
| IP | $\mathcal{O}\left(\right)$ | $((d+\pi)(n-1)^4 {\binom{2(d+\pi)+1}{d+\pi}}^2$ | ≥ 0 | $\mathcal{O}\left((n/2)(n-1)^4 \binom{2(n/2)+1}{n/2}^2\right)$ | $\frac{(q-1)(d+\pi)}{2} + 2$ |

Table 3. Table of the complexity of each attack on each variant, for the Gröbner Basis column we have not written the complexity but the upper bound of the degree of regularity so the real complexity is $\mathcal{O}(\binom{n+d_{reg}}{n}^{\omega})$. The mention Little effect means that the degree of regularity should not change from a vanilla HFE.

The complexity of MinRank ${\bf S}$ on IP is likely far above the complexity we wrote, c.f explanations in the text.

vulnerable. For example, for GeMSS-128 parameters we would require p = 15 to be again above 128 bits of security. It means a signature 2^{15} slower than GeMSS. With GeMSS specification we can make the estimation that it would require 24576000*M* of cycles to sign ($M = 10^6$). Obviously, these times are completely unrealistic. Hence pHFEv- was discarded.

8 New Scheme (HFE IP-)

8.1 Design Rationale

The problem we had with all previous schemes was that either a MinRank attack on **S** or **T** was threatening for their security. Technically for all attacks there exist a countermeasure, but the problem was the cost in complexity of the countermeasure. To be more specific when we use HFE in signature then we can use variants like - (minus) that will easily counter attacks through **T** because - is not costly in signature. However, it is hard to defend from attacks on **S** as we can totally negate - and variants that counter attacks on **S** are very costly in signature. On the other hand, in encryption, we can easily counter attacks on **S** with variants like p however all variants that protect **T** are very costly.

Nevertheless, the internal perturbation variant may lead to a new signature scheme. Indeed, as we have found it is highly effective against attacks on **S** with little modifier required. It means that we can have a small rank π for **Z** between 3 and 5 and avoid all attacks through **S** which means a reasonable increase of the complexity of the signature by a factor q^{π} .

On the other hand, we can avoid attacks on \mathbf{T} by adding a lot of - modifier. Indeed, as we mentioned earlier the - modifier is not costly at all in signature and it is effective against attacks on \mathbf{T} . So our idea is to uses both of these modifiers in order to make a new signature scheme based of HFE.

In order to further reduce the signature size without being vulnerable to a meet in the middle attack, we are using the Feistel-Patarin Technique like, for example, GeMSS. This technique was introduced by Jacques Patarin and can be found in [Cou03] as a solution to obtain short signatures. Its principle is, as the name suggests, inspired from a Feistel Scheme.

Naively the signature of a HFE scheme is built in the following way: given a message \mathbf{y} , one needs to find a vector \mathbf{x} such that $P(\mathbf{x}) = B(\mathbf{y})$, where B is a hash function. In order to avoid generic attacks such as meet-in-the-middle attacks or collision attacks on B, we need to choose n to be at least two times the security parameter. Let us now describe how the 2-round Feistel-Patarin technique can improve signature sizes.

For now, we will consider that m = n. By abuse of language we note $P^{-1}(\mathbf{y})$ a solution \mathbf{x} of the problem $P(\mathbf{x}) = \mathbf{y}$. Dividing the hash of \mathbf{y} in two pieces $B(\mathbf{y}) = (B_1(\mathbf{y}), B_2(\mathbf{y}))$, the signature of \mathbf{y} would be $\mathbf{x} = B_1(\mathbf{y}) \oplus P^{-1}(B_2(\mathbf{y}) \oplus P^{-1}(B_1(\mathbf{y})))$. We can easily see the similarity with a Feistel scheme with two rounds. Hence, this definition can easily be extended to a higher number of rounds.

However in the case of our scheme we have m < n, which creates an issue of dimension in the definition we gave. Indeed, $P^{-1}(B_1(\mathbf{y}))$ has a size of n but $B_2(\mathbf{y})$ is of size m < n due to the use of the minus modifier. It means that it misses some bits, and that we will need to give for each round k the missing bits a_k as part of the signature. We will then obtain $\mathbf{x} = (B_1(\mathbf{y})||a_2) \oplus P^{-1}((B_2(\mathbf{y})||a_1) \oplus P^{-1}(B_1(\mathbf{y})))$. Overall, the signature will be $\mathbf{x}||a_1||a_2||\ldots||a_r$ each a_i has a length of a the number of missing equations. We can then compute the length of the signature in bits by $(n-a) + Nb_{ite} \times a$ where N_{ite} is the number of rounds used in the Feistel-Patarin.

8.2 Parameters

One of the advantages of the scheme HFE is the fact that we can get short signatures. Already in 2020 Bros *et al.* [PMBK20] tried to optimize HFE and variants parameters in order to get the shortest possible signatures.

We propose 8 sets of parameters that we can regroup in two groups of four. The first group is a set of parameters for each expected security 80, 128, 192, 256 bits that tries to optimize the size of the signature but with no regard to the time to sign. The nomenclature of the scheme will be "HFE^sIP- *" where s stands for Short Signature and * the expected security. The second group of four set of parameters for each expected security 80, 128, 192, 256 that tries to optimize the size of the signature but with reasonable time to sign. The nomenclature of the scheme will be "HFE^fIP- *" where f stands for Fast Signature and * the expected security.

Here on Table 4 is the scheme built to optimize the size of signature but too slow to be used.

| Name | param. (q,n,D, π ,a) | Cycles to sign | pk (KB) | sign (b) | N_{ite} |
|--------------------------|--------------------------|---------------------|----------|-----------|-----------|
| | (2, 102, 513, 2, 2) | 3735M | 66 | 113 | 4 |
| $\text{HFE}^{s}IP - 128$ | (2, 182, 513, 4, 11) | 42296M | 356 | 204 | 3 |
| $\text{HFE}^{s}IP - 192$ | (2, 283, 513, 4, 27) | $133564 \mathrm{M}$ | 1286 | 337 | 3 |
| $\text{HFE}^{s}IP - 256$ | (2, 385, 513, 3, 43) | 213304M | 3177 | 468 | 3 |

Table 4. Parameter and performance of a $HFE^{s}IP-$ schemes

| Name | Param. (q,n,D,π,a) | Cycles to sign | pk (KB) | sign (b) | N_{ite} |
|--------------------------|------------------------|----------------|----------|-----------|-----------|
| $\text{HFE}^{f}IP - 80$ | (2, 107, 17, 2, 7) | 35M | 73 | 128 | 4 |
| $\text{HFE}^{f}IP - 128$ | (2, 189, 17, 3, 17) | 56M | 387 | 223 | 3 |
| $\text{HFE}^{f}IP - 192$ | (2, 289, 17, 3, 33) | 120M | 1341 | 355 | 3 |
| $\text{HFE}^{f}IP - 256$ | (2, 390, 17, 4, 48) | 160M | 3260 | 486 | 3 |

Table 5. Parameter and performance of a $HFE^{f}IP$ - schemes

The second set of parameters (Table 5) or $\text{HFE}^{f}IP$ is the set we consider the most efficient as it is reasonably fast and still have very good signature size. On the other hand, the first set of parameters should be more considered as a demonstrators as the slow signature limits its uses. Note that we did not mention the verification time because it is extremely faster than the time to sign.

Performance results. Our results are estimates of the real number of cycles required to sign, as we made our tests using the reference implementation of GeMSS (HFEv-) and estimated the impact of the IP modifier. We could not use the optimized version as it did not allow for re-parametrization. The code was made in C++ and used the library NTL for the operations on \mathbb{F}_2 . Benchmarking was done on an Intel Core i7-10850H CPU with 32GB of RAM.

8.3 Cryptanalysis

In this section we will give security complexity for $\text{HFE}^{f}IP-$, we have similar results for $\text{HFE}^{s}IP-$. The complexity of the direct attack depends on the degree of regularity d_{reg} of the public key which satisfies $d_{reg} \geq \lfloor \frac{r+\pi+a}{3} \rfloor + 2$. We have then the following lower bound for the complexity in the following table 6.

| | Security |
|--------------------------|----------|
| $\text{HFE}^{f}IP - 80$ | |
| $\text{HFE}^{f}IP - 128$ | |
| $\text{HFE}^{f}IP - 192$ | |
| $\text{HFE}^{f}IP - 256$ | 326 bits |

Table 6. Complexity of direct attacks based on Gröbner basis over $HFE^{f}IP-$ with their respective parameters.

| Name | Security |
|--------------------------|-----------|
| $\text{HFE}^{s}IP - 80$ | 98 bits |
| $\text{HFE}^{s}IP - 128$ | 163 bits |
| $\text{HFE}^{s}IP - 192$ | |
| $\text{HFE}^{s}IP-256$ | 326 bits |

Table 7. Complexity of direct attacks based on Gröbner basis over $HFE^{s}IP-$ with their respective parameters.

As this variant uses internal perturbation we have to take into account the differential attack of Dubois *et al* [DGS07]. With the parameters of $\text{HFE}^{f}IP$ –128 we have found a complexity of 2^{150} far above the level of security of 128 bits. For $\text{HFE}^{f}IP$ –80 we have found a complexity of 2^{130} . For all other parameters the attack fails as the advantage of the opponent is far too small (almost 0).

We can also try MinRank attacks. Because of the presence of minus and IP modifiers the target rank via **T** will be $d+a+\pi$. For MinRank attacks that target **S** we require an evaluation of the rank of the target matrix. Indeed, we know that minus modifier have no effect on this attack however we have no proper formula for the effect of IP. The tests we have performed however showed that we can expect a very high rank, namely at least n/2 for a parameter of IP = 1. In reality for the parameters we used, our tests showed that we ought to obtain almost a full rank matrix. But in the following Table 8 we will keep a pessimistic lower bound for the rank of n/2.

| Name | Attack on T | Attack on ${\bf S}$ |
|--------------------------|------------------------|---------------------|
| $\text{HFE}^{f}IP - 80$ | 81 bits | 240 bits |
| $\text{HFE}^{f}IP - 128$ | $128 	ext{ bits}$ | 406 bits |
| $\text{HFE}^{f}IP - 192$ | $195 \; \mathrm{bits}$ | 609 bits |
| $\text{HFE}^{f}IP - 256$ | 257 bits | 812 bits |

Table 8. Complexity of the best MinRank attacks (in bold) over $HFE^{f}IP-$ with their respective parameters.

| Name | Attack on T | Attack on ${\bf S}$ |
|--------------------------|------------------------|---------------------|
| $\text{HFE}^{s}IP-80$ | 81 bits | 228 bits |
| $\text{HFE}^{s}IP - 128$ | $128 \; \mathrm{bits}$ | 392 bits |
| $\text{HFE}^{s}IP - 192$ | $195 \; \mathrm{bits}$ | 597 bits |
| $\text{HFE}^{s}IP-256$ | 257 bits | 803 bits |

Table 9. Complexity of the best MinRank attacks (in bold) over $HFE^{s}IP-$ with their respective parameters.

Obviously, the results show that any attack on \mathbf{S} with the current form of MinRank is impossible. The attack on \mathbf{T} remains our best attack, and any moderate improvement in the complexity of the attack could be countered by increasing a. Note that this would not dramatically worsen our performance, the size of the signature or the public key. On the other hand, it seems unlikely that an attack on \mathbf{S} in its current form could threaten our scheme without a way to somehow eliminate the effect of the IP variant.

9 Conclusion

Consequently to the new MinRank attacks that broke the NIST submission GeMSS, it is generally considered that HFE and all its variants do not allow interesting signatures with a security of at least 128 bits. This is because the size of the public key would then be unrealistic (although for 80 bits of security unmodified HFE is still competitive but for most usage 80 bits remains insufficient). In this article however, we showed that a small range of parameters still offers a good security against all known attacks (with 128 or even 256 bits of security) and a reasonable time to sign. Furthermore, with these parameters we obtain very short signatures (less than 2λ bits where λ is the required security). This is the variant HFEIP-. It uses two modifiers, namely IP and minus. Both are required to counter all attack types, especially MinRank attacks. Naturally only the future will tell if this range of parameters remains unbroken or if new attacks will make this scheme vulnerable again. Hence, we do not recommend using this scheme for sensitive applications. The most important aspect of this scheme is that it currently offers the shortest public key signatures (quantum resistant or not). For example, ECDSA (Elliptic Curve Digital Signature Algorithm) is only able to have signatures at least three time the length of the security parameter or up to 2.5 in some variants (and is not post quantum), while we can get with HFE IP - a signature length less than twice the size of the security parameter and still expect it to be post quantum.

References

- BBB⁺22. Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, and Jean-Pierre Tillich. Revisiting algebraic attacks on MinRank and on the rank decoding problem. Cryptology ePrint Archive, Report 2022/1031, 2022. https://eprint.iacr.org/2022/1031.
- BBC⁺22. John Baena, Pierre Briaud, Daniel Cabarcas, Ray A. Perlner, Daniel Smith-Tone, and Javier A. Verbel. Improving support-minors rank attacks: Applications to GeMSS and rainbow. In Yevgeniy Dodis and Thomas Shrimpton, editors, CRYPTO 2022, Part III, volume 13509 of LNCS, pages 376–405. Springer, Heidelberg, August 2022.
- Beu21. Ward Beullens. Improved cryptanalysis of UOV and Rainbow. In Anne Canteaut and François-Xavier Standaert, editors, EUROCRYPT 2021, Part I, volume 12696 of LNCS, pages 348–373. Springer, Heidelberg, October 2021.

- BFP11. Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of multivariate and odd-characteristic HFE variants. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 441–458. Springer, Heidelberg, March 2011.
- BFS99. Jonathan F Buss, Gudmund S Frandsen, and Jeffrey O Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58(3):572–596, 1999.
- CFMR⁺20. A. Casanova, J.C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. Gemss: A great multivariate short signature. In *NIST CSRC*, 2020.
- Cou03. Nicolas Courtois. Generic attacks and the security of Quartz. In Yvo Desmedt, editor, *PKC 2003*, volume 2567 of *LNCS*, pages 351–364. Springer, Heidelberg, January 2003.
- CS17. Ryann Cartor and Daniel Smith-Tone. An updated security analysis of PFLASH. In Lange and Takagi [LT17], pages 241–254.
- CZ81. David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36(154):587– 592, 1981.
- DGS07. Vivien Dubois, Louis Granboulan, and Jacques Stern. Cryptanalysis of HFE with internal perturbation. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *PKC 2007*, volume 4450 of *LNCS*, pages 249–265. Springer, Heidelberg, April 2007.
- DS05. Jintai Ding and Dieter Schmidt. Cryptanalysis of HFEv and internal perturbation of HFE. In Serge Vaudenay, editor, *PKC 2005*, volume 3386 of *LNCS*, pages 288–301. Springer, Heidelberg, January 2005.
- DS13. Jintai Ding and Dieter Schmidt. Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields, pages 34–49. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- DY13. Jintai Ding and Bo-Yin Yang. Degree of regularity for HFEv and HFEv-. In Philippe Gaborit, editor, Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, pages 52–66. Springer, Heidelberg, June 2013.
- Fau99. Jean-Charles Faugère. A new efficient algorithm for computing gröbner bases (f4). Journal of Pure and Applied Algebra, 139(1):61–88, 1999.
- Fau02. Jean Charles Faugère. 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 '02, page 75–83, New York, NY, USA, 2002. Association for Computing Machinery.
- FJ03. Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases. In Annual International Cryptology Conference, 2003.
- FmRPP22. Jean-Charles Faugère, Gilles macario Rat, Jacques Patarin, and Ludovic Perret. A new perturbation for multivariate public key schemes such as HFE and UOV. Cryptology ePrint Archive, Report 2022/203, 2022. https://eprint.iacr.org/2022/203.
- KS99. Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In Michael J. Wiener, editor, CRYPTO'99, volume 1666 of LNCS, pages 19–30. Springer, Heidelberg, August 1999.
- LT17. Tanja Lange and Tsuyoshi Takagi, editors. Post-Quantum Cryptography -8th International Workshop, PQCrypto 2017. Springer, Heidelberg, 2017.

- MI88. Tsutomu Matsumoto and Hideki Imai. Public quadratic polynominaltuples for efficient signature-verification and message-encryption. In C. G. Günther, editor, *EUROCRYPT'88*, volume 330 of *LNCS*, pages 419–453. Springer, Heidelberg, May 1988.
 ØSV21. Morten Øygarden, Daniel Smith-Tone, and Javier A. Verbel. On the effect
- OSV21. Morten Øygarden, Daniel Smith-Tone, and Javier A. Verbel. On the effect of projection on rank attacks in multivariate cryptography. In Jung Hee Cheon and Jean-Pierre Tillich, editors, Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, pages 98–113. Springer, Heidelberg, 2021.
- Pat96a. Jacques Patarin. Asymmetric cryptography with a hidden monomial. In Neal Koblitz, editor, CRYPTO'96, volume 1109 of LNCS, pages 45–60. Springer, Heidelberg, August 1996.
- Pat96b. Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 33–48. Springer, Heidelberg, May 1996.
- Pet17. Albrecht Petzoldt. On the complexity of the hybrid approach on HFEv-. Cryptology ePrint Archive, Report 2017/1135, 2017. https://eprint. iacr.org/2017/1135.
- PMBK20. Jacques Patarin, Gilles Macario-Rat, Maxime Bros, and Eliane Koussa. Ultra-short multivariate public key signatures. Cryptology ePrint Archive, Report 2020/914, 2020. https://eprint.iacr.org/2020/914.
- TPD21. Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. Efficient key recovery for all HFE signature variants. In Tal Malkin and Chris Peikert, editors, CRYPTO 2021, Part I, volume 12825 of LNCS, pages 70–93, Virtual Event, August 2021. Springer, Heidelberg.
- VS17. Jeremy Vates and Daniel Smith-Tone. Key recovery attack for all parameters of HFE-. In Lange and Takagi [LT17], pages 272–288.