State of the art of HFE variants: Is it possible to repair HFE with appropriate modifiers?

Benoît Cogliati [1] Gilles Macariot-Rat [2] Jacques Patarin[1]
PierreVarjabedian [1]

THALES, Meudon, France,
{benoit-michel.cogliati,jacques.patarin,pierre.varjabedian}@thalesgroup.com

Orange, Chatillon, France,
gilles.macariorat@orange.com

June 12, 2024

Outline

Outline

HFE

- Multivariate scheme
- Uses the vector space structure of a Finite Field extension
- Created in 1996
- Many Variants

General Structure

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

- High degree in the “big” field. Degree 2 in the “small” field
- Public key: $P = T \circ \phi \circ H \circ \phi^{-1} \circ S$

General Idea

For a signature scheme:

- Send a vector $Y = (y_1, ...y_n)$
- Send back $X = (x_1, ..., x_n)$ such that $P(X) = Y$
- Hard in the small field, easy in the big field

Short State of the Art

HFE is created as a reparation of C* of Mastumoto and Imai (1988)

- HFE is attacked by a direct attack (Gröbner Basis) (2003)
- HFE security is threatened by a Min-rank attack on the matrix **T** (2007)
- Variants are created to counter these attacks (minus, vinegar) (2002)
- New Min-rank attack on the matrix **S** (2017)

Outline

Matrix Representation

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^ith power of the secret polynomial h.

$$\mathbf{H} = \begin{pmatrix} \overbrace{\mathbf{A}}^{d\times d} & 0 \\ 0 & 0 \end{pmatrix}$$

Min-rank Problem

Definition

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

Min-rank attack on the matrix $\mathbf{T}$

- Let $(\mathbf{P}_1, \ldots \mathbf{P}_n)$ the public key and $\mathbf{T}, \mathbf{S}, \mathbf{H}$ the secret key. Then,

$$\mathbf{T}^{-1}(\mathbf{P}_1, \ldots \mathbf{P}_n) = \mathbf{HS}$$

- $\mathbf{rank}(\mathbf{H}) = r$ is small
- It's a Min-rank problem

Min-rank attack on the matrix $\mathbf{S}$

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

Let $\mathbf{U} = \mathbf{T}^{-1}\mathbf{M}_n^{-1}$ and $\mathbf{W} = \mathbf{S}\mathbf{M}_n$ Then

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

Let

$$\mathbf{Q} = (\mathbf{U}^{-1})^t \begin{pmatrix} r_0 \\ \vdots \\ r_n \end{pmatrix}$$

r_i is the first row of $\mathbf{H}^{*i}$

Min-rank attack on the matrix $\mathbf{S}$

$$\mathbf{Q} = \left(\mathbf{U}^{-1}\right)^t \begin{pmatrix} r_0 \\ \vdots \\ r_n \end{pmatrix} = \left(\mathbf{U}^{-1}\right)^t \begin{pmatrix} \overbrace{A_1}^{1\times d} \\ 0 \\ \underbrace{A_2}_{(d-1)\times d} \end{pmatrix}$$

Min-rank attack on the matrix S

$$(\mathbf{H}^{*0},\ldots,\mathbf{H}^{*n-1}) =$$

$$\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \vdots & \vdots \\ \ldots & \ldots & \ldots \end{pmatrix}, \begin{pmatrix} a'_{1,1} & \ldots & a'_{1,n} \\ \vdots & \vdots & \vdots \\ \ldots & \ldots & \ldots \end{pmatrix} \ldots, \begin{pmatrix} a"_{1,1} & \ldots & a"_{1,n} \\ \vdots & \vdots & \vdots \\ \ldots & \ldots & \ldots \end{pmatrix}$$

$$\begin{pmatrix} a_{1,1} & \ldots & a_{1,d} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{d,1} & \ldots & a_{d,d} & 0 & \ldots & 0 \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \end{pmatrix}, \begin{pmatrix} 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ a'_{1,1} & \ldots & a'_{1,d} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a'_{d,1} & \ldots & a'_{d,d} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \end{pmatrix} \ldots$$

Outline

HFE Variant minus perturbation

In this variants the public key is only partially unveiled.
From a public key $P = (\mathbf{P}_0, \ldots, \mathbf{P}_{n-1})$, then the public key of HFE$-$ will be $P_- = (\mathbf{P}_0, \mathbf{P}_1, \ldots, \mathbf{P}_{n-1-a})$

- Resist to Gröbner attacks and Min-rank on **T**
- Inefficient against Min-rank on **S**

HFE Variant internal perturbation (IP)

$$\mathbf{H} = \begin{pmatrix} \overbrace{\mathbf{A}}^{d\times d} & 0 \\ 0 & 0 \end{pmatrix} + \underbrace{Z}_{\text{small rank}} \overbrace{\begin{pmatrix} p_{1,1} & \cdots & p_{1,n} \\ \vdots & \vdots & \vdots \\ p_{n,1} & \cdots & p_{n,n} \end{pmatrix}}^{\text{random quadratic map}} \underbrace{Z^t}_{\text{small rank}}$$

Effect of Internal perturbation (IP) on T attack

- Rank of $\mathbf{Z} = \pi$
- Rank of the central map is $d + \pi$
- Attack on $\mathbf{T}$ slightly harder

Effect of Internal perturbation on S attack

- Matrix **Z** is full and therefore **H** also
- The Frobenius breaks the linear bounds between elements of **Z**
- The Rank is highly increased (higher than n/2)

Effect of Internal perturbation (IP) on S attack

$$\overbrace{\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \vdots & \vdots \\ \dots & \dots & \dots \end{pmatrix}}^{\text{only take the first row}}, \begin{pmatrix} a'_{1,1} & \dots & a'_{1,n} \\ \vdots & \vdots & \vdots \\ \dots & \dots & \dots \end{pmatrix} \dots, \begin{pmatrix} a"_{1,1} & \dots & a"_{1,n} \\ \vdots & \vdots & \vdots \\ \dots & \dots & \dots \end{pmatrix}$$

a_i's are now most likely non zero and rows are likely independent

Summary of complexity on all variants

	Min-rank T	Min-rank S	Gröbner basis
v	$\mathcal{O}\left(d_v(n_p)^4\binom{2(d_v)+1}{d_v}^2\right)$	$\mathcal{O}\left(d(n_p+v)^4\binom{2d+1}{d}^2\right)$	$\frac{(q-1)(d+v)}{2}+2$
+	$\mathcal{O}\left(d(n_p)^4\binom{2d+1}{d}^2\right)$	$\mathcal{O}\left(d(n_p)^4\binom{2d+1}{d}^2\right)$	?
-	$\mathcal{O}\left((d_a)(n_p)^4\binom{2(d_a)+1}{d_a}^2\right)$	$\mathcal{O}\left(d(n_p)^4\binom{2d+1}{d}^2\right)$	$\frac{(q-1)(d+a)}{2}+2$
p	$\mathcal{O}\left(d(n_p)^4\binom{2d+1}{d}^2\right)$	$\mathcal{O}\left((d_t)(n_p)^4\binom{2(d_t)+1}{d+t}^2\right)$	?
$\hat{+}$	$\mathcal{O}\left((d_t)(n_p)^4\binom{2(d_t)+1}{d+t}^2\right)$	$\mathcal{O}\left((d_p)(n_p)^4\binom{2(d_p)+1}{d_p}^2\right)$	?
IP	$\mathcal{O}\left((d_\pi)(n_p)^4\binom{2(d_\pi)+1}{d_\pi}^2\right)$	$\mathcal{O}\left((\frac{n}{2})(n_p)^4\binom{2(\frac{n}{2})+1}{\frac{n}{2}}^2\right)$	$\frac{(q-1)(d+\pi)}{2}+2$

Here $n_p = n-1$, $d_v = d+v$, $d_a = d+a$, $d_p = d+p$, $d_t = d+t$, $d_\pi = d+\pi$.

Cost of the variants

	Signature	Decryption
v	$\mathcal{O}(1)$	$\mathcal{O}(q^v)$
+	$\mathcal{O}(q^t)$	$\mathcal{O}(1)$
-	$\mathcal{O}(1)$	$\mathcal{O}(q^a)$
p	$\mathcal{O}(q^p)$	$\mathcal{O}(1)$
$\hat{+}$	$\mathcal{O}(q^t)$	$\mathcal{O}(q^t)$
IP	$\mathcal{O}(q^\pi)$	$\mathcal{O}(q^\pi)$

Outline

HFE IP- performance (1)

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

Table: Parameter and performance of a HFE$^f IP-$ schemes (Performance extrapolated from GeMSS reference implementation)

Advantages and Shortcomings of the scheme

- Very Small signature
- Post-quantum
- Rather Slow
- Big public key

Thank You !