Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants

Luk Bettale[1] Jean-Charles Faugère Ludovic Perret

LIP6 - SALSA
UPMC, CNRS, INRIA Paris-Rocquencourt

Public Key Cryptography 2011
March 6-9, 2011 - Taormina, Italy

[1] author partially supported by DGA/MRIS

Motivations

Multivariate Public Key Cryptosystems

- Fast encryption, small signatures
- Long term security
- Alternative to RSA and ECC
- Post-Quantum cryptography.

- Many proposals (HFE, UOV, SFLASH, Rainbow, TTS, IP, . . .)

Motivations

Multivariate Public Key Cryptosystems

- Fast encryption, small signatures
- Long term security
- Alternative to RSA and ECC
- Post-Quantum cryptography.

- Many proposals (HFE, UOV, ~~SFLASH~~, ~~Rainbow~~, ~~TTS~~, ~~IP~~, . . .)
- Security not well mastered.

Multivariate Cryptography: General Principle

Private Key

$\mathcal{F} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$ easy to invert.

$$f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$f_n(x_1, \ldots, x_n).$$

$\mathcal{S}, \mathcal{T} \in \mathrm{Aff}(n, \mathbb{F}_q)$.

Public Key

$\mathcal{G} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$

$$g_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$g_n(x_1, \ldots, x_n).$$

$\mathcal{G} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$.

Multivariate Cryptography: General Principle

Private Key

$\mathscr{F} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$ easy to invert.

$$f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$f_n(x_1, \ldots, x_n).$$

$\mathscr{S}, \mathscr{T} \in \mathrm{Aff}(n, \mathbb{F}_q)$.

Public Key

$\mathscr{G} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$

$$g_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$g_n(x_1, \ldots, x_n).$$

$\mathscr{G} = \mathscr{T} \circ \mathscr{F} \circ \mathscr{S}$.

Encrypt:

$\underline{c} = \mathscr{G}(\underline{m})$.

Multivariate Cryptography: General Principle

Private Key

$\mathscr{F} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$ easy to invert.

$$f_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$f_n(x_1, \ldots, x_n).$$

$\mathscr{S}, \mathscr{T} \in \mathrm{Aff}(n, \mathbb{F}_q)$.

Decrypt:

$\underline{m} = \mathscr{S}^{-1} \circ \mathscr{F}^{-1} \circ \mathscr{T}^{-1}(\underline{c})$.

Public Key

$\mathscr{G} : (\mathbb{F}_q)^n \mapsto (\mathbb{F}_q)^n$

$$g_1(x_1, \ldots, x_n),$$
$$\vdots$$
$$g_n(x_1, \ldots, x_n).$$

$\mathscr{G} = \mathscr{T} \circ \mathscr{F} \circ \mathscr{S}$.

Encrypt:

$\underline{c} = \mathscr{G}(\underline{m})$.

History of Hidden Field Equations (HFE)

- Patarin 1996
- Generalization of Matsumoto-Imai's C* (EUROCRYPT '88)
- Encryption/Signature.

Jacques Patarin.
Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms.
In *Advances in Cryptology – EUROCRYPT '96*.

History of Hidden Field Equations (HFE)

- Patarin 1996
- Generalization of Matsumoto-Imai's C* (EUROCRYPT '88)
- Encryption/Signature.

Jacques Patarin.
Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms.
In *Advances in Cryptology – EUROCRYPT '96*.

Known attacks

- Message recovery attack [FaugèreJoux03]
  - First HFE challenge broken (80 bits security)
  - efficient in char 2.
- Key recovery attack [KipnisShamir99]
  - not practical
  - complexity conjectured.

Variants of HFE: Multi-HFE

- Use odd-characteristic field to prevent [FJ03] attack
- Various additional variants (minus, embedding).

[BPS08] Olivier Billet, Jacques Patarin, and Yannick Seurin.
Analysis of Intermediate Field Systems.
In *SCC 2008*.

[CCDWY08] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang.
Odd-char multivariate Hidden Field Equations.
Cryptology ePrint Archive, 2008.

Variants of HFE: Multi-HFE

- Use odd-characteristic field to prevent [FJ03] attack
- Various additional variants (minus, embedding).

[BPS08] Olivier Billet, Jacques Patarin, and Yannick Seurin.
Analysis of Intermediate Field Systems.
In *SCC 2008*.

[CCDWY08] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang.
Odd-char multivariate Hidden Field Equations.
Cryptology ePrint Archive, 2008.

- No known attacks
- Efficient implementations.

Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, and Bo-Yin Yang.
SSE implementation of multivariate PKCs on modern x86 CPUs.
In *Cryptographic Hardware and Embedded Systems – CHES 2009*.

HFE shape

$F(X) \in \mathbb{F}_{q^n}[X]$, $D \in \mathbb{N}$

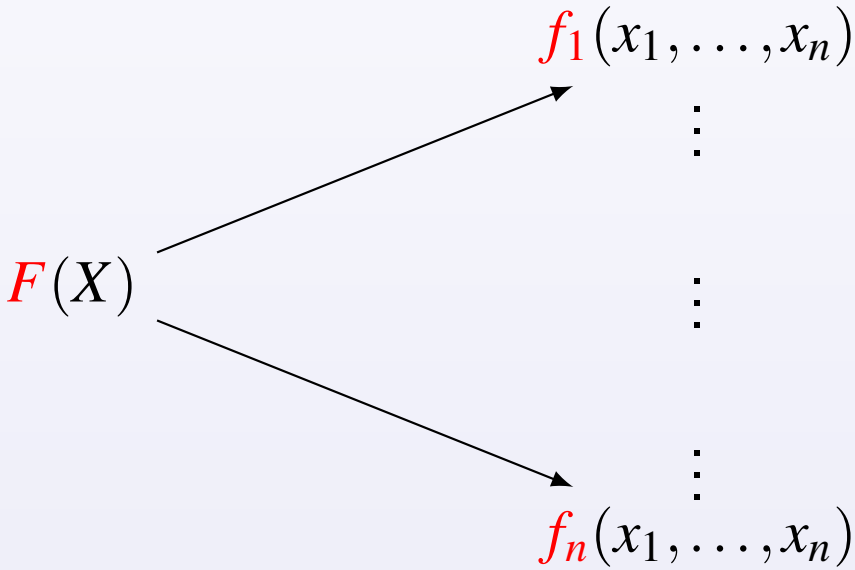
$$F(X) = \sum_{\substack{0 \leqslant i \leqslant j < n \\ q^i + q^j \leqslant D}} A_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leqslant i < n \\ q^i \leqslant D}} B_i X^{q^i} + C.$$

HFE Trapdoor

HFE shape

$F(X) \in \mathbb{F}_{q^n}[X]$, $D \in \mathbb{N}$

$$F(X) = \sum_{\substack{0 \leqslant i \leqslant j < n \\ q^i + q^j \leqslant D}} A_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \leqslant i < n \\ q^i \leqslant D}} B_i X^{q^i} + C.$$



with $F\left(\sum_{i=1}^n \theta_i x_i\right) = \sum_{i=1}^n \theta_i f_i(x_1, \ldots, x_n)$ where $(\theta_1, \ldots, \theta_n) \in (\mathbb{F}_{q^n})^n$ is a basis of the $\mathbb{F}_q$-vector space $(\mathbb{F}_q)^n$.

Multi-HFE Trapdoor

Multi-HFE shape

$$F_1(X_1,\ldots,X_N),\ldots,F_N(X_1,\ldots,X_N) \in (\mathbb{F}_{q^d}[X_1,\ldots,X_N])^N, \quad n = Nd$$

$$F_k(X_1,\ldots,X_N) = \sum_{1\leqslant i\leqslant j\leqslant N} A_{k,i,j} X_i X_j + \sum_{1\leqslant i\leqslant N} B_{k,i} X_i + C_k \quad \text{for } 1 \leqslant k \leqslant N.$$

Multi-HFE Trapdoor

Multi-HFE shape

$$F_1(X_1,\dots,X_N),\dots,F_N(X_1,\dots,X_N) \in (\mathbb{F}_{q^d}[X_1,\dots,X_N])^N, \quad n = Nd$$

$$F_k(X_1,\dots,X_N) = \sum_{1\leqslant i\leqslant j\leqslant N} A_{k,i,j} X_i X_j + \sum_{1\leqslant i\leqslant N} B_{k,i} X_i + C_k \quad \text{for } 1 \leqslant k \leqslant N.$$

$$q = 7, 11, 31, \dots$$

$$\begin{array}{ccc} & & f_1(x_1,\dots,x_n) \\ & \nearrow & \vdots \\ F_1(X_1,\dots,X_N) & & \\ & \searrow & f_d(x_1,\dots,x_n) \\ \vdots & & \vdots \\ F_N(X_1,\dots,X_N) & \longrightarrow & f_{n-d+1}(x_1,\dots,x_n) \\ & \searrow & \vdots \\ & & f_n(x_1,\dots,x_n) \end{array}$$

with $F_k\left(\sum_{i=1}^d \theta_i x_i, \dots, \sum_{i=1}^d \theta_i x_{(k-1)d+i}\right) = \sum_{i=1}^d \theta_i f_{(k-1)d+i}(x_1,\dots,x_n)$
for $1 \leqslant k \leqslant N$ where $(\theta_1,\dots,\theta_n) \in (\mathbb{F}_{q^d})^d$ is a basis of $(\mathbb{F}_q)^d$.

Table: Status of HFE and Multi-HFE variants.

construction	message recovery	key recovery
HFE (q odd)	[FJ03] (if $q < 7$)	[KS99] theoretical
HFE ($q = 2$)	[FJ03]	[KS99] theoretical ?
Multi-HFE ($q = 2$)	[FJ03] + [BPS08]	–
Multi-HFE (q odd)	–	–
(Multi-)HFE$^-$	–	–
(Multi-)HFE w/ emb.	–	–
(Multi-)HFEv	–	–

Status of HFE / Multi-HFE (main results)

Table: Status of HFE and Multi-HFE variants.

construction	message recovery	key recovery
HFE (q odd)	[FJ03] (if $q < 7$)	[KS99] theoretical $\rightarrow$ improved [KS99] attack
HFE ($q = 2$)	[FJ03]	[KS99] theoretical ? $\rightarrow$ extended [KS99] attack
Multi-HFE ($q = 2$)	[FJ03] + [BPS08]	new attack
Multi-HFE (q odd)	–	new attack
(Multi-)HFE$^-$	–	new attack (if $N > 1$)
(Multi-)HFE w/ emb.	–	new attack
(Multi-)HFEv	–	–

Kipnis-Shamir attack

Key recovery attack on HFE: $N = 1$.

Univariate representation ($G \in \mathbb{F}_{q^n}[X]$)

$$\mathscr{G} = \mathscr{T} \circ \mathscr{F} \circ \mathscr{S} \qquad \rightsquigarrow \qquad G(X) = T(F(S(X))).$$

Use interpolation.

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.
In *Advances in Cryptology – CRYPTO '99*.

Kipnis-Shamir attack

Key recovery attack on HFE: $N = 1$.

Univariate representation ($G \in \mathbb{F}_{q^n}[X]$)

$$\mathcal{G} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} \qquad \rightsquigarrow \qquad G(X) = T(F(S(X))).$$

Use interpolation.

Matrix representation (non-standard quadratic form)

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

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$ and $g_{i,j} \in \mathbb{F}_{q^n}$.

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization.
In *Advances in Cryptology – CRYPTO '99*.

Matrix representation

Matrix representation (non-standard quadratic form)

$$F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i + q^j} = \underline{X} \mathbf{F} \underline{X}^t$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

Matrix representation (non-standard quadratic form)

$$F(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{i,j} X^{q^i+q^j} = \underline{X}\mathbf{F}\underline{X}^t$$

with $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

$$\begin{pmatrix} f_{1,1} & \cdots & f_{1,\ell} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{\ell,1} & \cdots & f_{\ell,\ell} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

We have that $\mathrm{rank}(\mathbf{F}) = \log_q(\deg(F(X)))$.

Kipnis-Shamir attack: a MinRank problem

Let $\mathbf{G}^{*k}$ obtained from $\mathbf{G}$,
$T^{-1}(X) = \sum_{i=0}^{n} t_i X^{q^i}$, $S(X) = \sum_{i=0}^{n} s_i X^{q^i}$ and $\widetilde{\mathbf{W}} = [s_{j-i}^{q^i}]$.

Fundamental equation

$$\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k} = \widetilde{\mathbf{W}} \mathbf{F} \widetilde{\mathbf{W}}^t.$$

Kipnis-Shamir attack: a MinRank problem

Let $\mathbf{G}^{*k}$ obtained from $\mathbf{G}$,
$T^{-1}(X) = \sum_{i=0}^{n} t_i X^{q^i}$, $S(X) = \sum_{i=0}^{n} s_i X^{q^i}$ and $\widetilde{\mathbf{W}} = [s_{j-i}^{q^i}]$.

Fundamental equation

$$\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k} = \widetilde{\mathbf{W}} \mathbf{F} \widetilde{\mathbf{W}}^t.$$

Find a vector $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^n})^n$ such that

$$\operatorname{rank}\left(\sum_{k=1}^{n} \lambda_k \mathbf{G}^{*(k-1)} \right) = \log_q(D).$$

Kipnis-Shamir attack: a MinRank problem

Let $\mathbf{G}^{*k}$ obtained from $\mathbf{G}$,
$T^{-1}(X) = \sum_{i=0}^{n} t_i X^{q^i}$, $S(X) = \sum_{i=0}^{n} s_i X^{q^i}$ and $\widetilde{\mathbf{W}} = [s^{q^i}_{j-i}]$.

Fundamental equation

$$\sum_{k=0}^{n-1} t_k \mathbf{G}^{*k} = \widetilde{\mathbf{W}} \mathbf{F} \widetilde{\mathbf{W}}^t.$$

Find a vector $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^n})^n$ such that

$$\operatorname{rank}\left(\sum_{k=1}^{n} \lambda_k \mathbf{G}^{*(k-1)} \right) = \log_q(D).$$

- Solve the MinRank problem on matrices over $\mathbb{F}_{q^n}$
- Allows to recover the transformation $\mathbf{T}$
- Solve a linear system to recover $\mathbf{S}$.

A New Approach

Use directly the quadratic forms of $(g_1, \ldots, g_n)$.

Matrix Representation of Quadratic Form

$$g_1(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_1}\,\underline{x}^t$$

$$\vdots$$

$$g_n(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_n}\,\underline{x}^t.$$

A low rank linear combination of the public quadratic forms.

Improvement of Kipnis-Shamir's Attack

Let $\mathbf{M}_n$ a change basis matrix between $(x_1,\ldots,x_n)$ and $(X^{q^0},\ldots,X^{q^{n-1}})$, $g_k(\underline{x}) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$, $\mathbf{T}^{-1}\mathbf{M}_n = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\,\mathbf{M}_n = \mathbf{W}$.

Fundamental equation

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{WFW}^t.$$

Improvement of Kipnis-Shamir's Attack

Let $\mathbf{M}_n$ a change basis matrix between $(x_1, \ldots, x_n)$ and $(X^{q^0}, \ldots, X^{q^{n-1}})$, $g_k(\underline{x}) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$, $\mathbf{T}^{-1}\mathbf{M}_n = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\,\mathbf{M}_n = \mathbf{W}$.

Fundamental equation

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{WFW}^t.$$

Find a vector $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^n})^n$ such that

$$\operatorname{rank}\left(\sum_{k=1}^{n} \lambda_k \mathbf{G_k}\right) = \log_q(D).$$

Improvement of Kipnis-Shamir's Attack

Let $\mathbf{M}_n$ a change basis matrix between $(x_1,\ldots,x_n)$ and $(X^{q^0},\ldots,X^{q^{n-1}})$, $g_k(\underline{x}) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$, $\mathbf{T}^{-1}\mathbf{M}_n = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\,\mathbf{M}_n = \mathbf{W}$.

Fundamental equation

$$\sum_{k=0}^{n-1} u_{k,0}\mathbf{G_{k+1}} = \mathbf{WFW}^t.$$

Find a vector $(\lambda_1,\ldots,\lambda_n) \in (\mathbb{F}_{q^n})^n$ such that

$$\operatorname{rank}\left(\sum_{k=1}^{n} \lambda_k \mathbf{G_k}\right) = \log_q(D).$$

- The MinRank problem on matrices over $\mathbb{F}_q \rightsquigarrow$ faster solving
- Standard quadratic form representation
- Clean description as matrix/vector operations.

Kipnis-Shamir Attack vs. New Attack on HFE ($N = 1$)

Table: Comparison between KS attack and new attack on HFE with parameters $q = 31$, $N = 1$, $D = 31^2 + 31 = 992$ from 60 to 80 bits security.

d	12	13	14	15	16
KS attack (in sec.)	374	1305	1790	2719	14763
new attack (in sec.)	3.2	6.7	12.9	26.1	54.9
ratio	170	195	139	104	269

Using Magma (V2.17-1) on a 2.93 GHz Intel® Xeon® CPU.

MinRank solved using Gröbner bases.

Extension of the New Attack

Let $\mathbf{M}_{N,d} = \mathrm{Diag}(\mathbf{M}_d, \ldots \mathbf{M}_d)$, $g_k(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$,
$\mathbf{T}^{-1}\mathbf{M}_{N,d} = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\mathbf{M}_{N,d} = \mathbf{W}$.

Fundamental equations

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

Extension of the New Attack

Let $\mathbf{M}_{N,d} = \mathrm{Diag}(\mathbf{M}_d, \ldots \mathbf{M}_d)$, $g_k(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$,
$\mathbf{T}^{-1}\mathbf{M}_{N,d} = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\mathbf{M}_{N,d} = \mathbf{W}$.

Fundamental equations

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

Find N vectors $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^d})^n$ such that

$$\mathrm{rank}\left(\sum_{k=0}^{n-1} \lambda_k \mathbf{G_k}\right) = N \log_q(D).$$

Extension of the New Attack

Let $\mathbf{M}_{N,d} = \mathrm{Diag}(\mathbf{M}_d, \ldots \mathbf{M}_d)$, $g_k(x_1, \ldots, x_n) = \underline{x}\,\mathbf{G_k}\,\underline{x}^t$,
$\mathbf{T}^{-1}\mathbf{M}_{N,d} = \mathbf{U} = [u_{i,j}]$, $\mathbf{S}\mathbf{M}_{N,d} = \mathbf{W}$.

Fundamental equations

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

Find N vectors $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{F}_{q^d})^n$ such that

$$\mathrm{rank}\left(\sum_{k=0}^{n-1} \lambda_k \mathbf{G_k}\right) = N \log_q(D).$$

N MinRank relations "equivalent up to Frobenius transforms"
$\Rightarrow$ only one to be solved.

Proposed Parameters Practically Broken

Table: Proposed parameters of Multi-HFE [CCDWY08]. Broken on a 2.93 GHz Intel Xeon CPU..

using Magma (V2.16-10).

q	N	d	D	security	time (Magma)	mem (Magma)	d_{reg}
31	2	15	2	150 bits	2 m 27 s	434 MB	3
31	3	10	2	150 bits	1 h 38 m	1.5 GB	3
31	3	15	2	192 bits	2 d 1 h	12 GB	3
31	3	18	2	256 bits	9 d 16 h	33 GB	3

using FGb.

q	N	d	D	security	time (FGb)	mem (FGb)	d_{reg}
31	2	15	2	150 bits	21.1 s	276 MB	3
31	3	10	2	150 bits	24 m 56 s.	1.6 GB	3

Solving Multi-HFE's MinRank

- Gröbner bases for solving MinRank
- Explicit method to compute d_{reg}.

Theorem

For a MinRank coming from Multi-HFE with parameters q, N, d, D

$$d_{reg} \leqslant \psi(q, N, d, D)$$

where $\psi(q, N, d, D)$ can be computed for explicit values of q, N, d, D.

Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer
Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology.
In *ISSAC 2010*.

Conjectured formula (verified for a wide range of parameters)

$$\psi(q, N, d, D) = N \log_q(D) + 1.$$

Complexity of the Attack

Proposition

The complexity of solving the Multi-HFE MinRank with Gröbner bases is

$$\mathscr{O}\left(d^{(N\log_q(D)+1)\,\omega}\right)$$

when $d \to \infty$, *with* $2 \leqslant \omega < 3$ *the linear algebra constant.*

- The complexity is polynomial in d, the degree of the extension

Complexity of the Attack

Proposition

The complexity of solving the Multi-HFE MinRank with Gröbner bases is

$$\mathscr{O}\left(d^{(N\log_q(D)+1)\,\omega}\right)$$

when $d \to \infty$, *with* $2 \leqslant \omega < 3$ *the linear algebra constant.*

- The complexity is polynomial in d, the degree of the extension
- For equally sized keys, Multi-HFE is less secure than HFE.

$$\text{Complexity}_{\text{attack}}(N,d) < \text{Complexity}_{\text{attack}}(1,n), \quad \text{when} \quad n = Nd.$$

Attack on Multi-HFE Variants

Key result

Many equivalent keys $\Rightarrow N$ degrees of freedom.

Multi-HFE$^-$ (sign.)

Private key: Unchanged.
Public key: **s** equations removed
$\rightsquigarrow$ under-determined system.

Multi-HFE w/ embedding (encr.)

Private key: add $\rho : \mathbb{F}_q^{n-r} \to (\mathbb{F}_q)^n$.
Public key: **r** variables less
$\rightsquigarrow$ over-determined system.

Attack on Multi-HFE Variants

Key result

Many equivalent keys $\Rightarrow N$ degrees of freedom.

Multi-HFE$^-$ (sign.)

Private key: Unchanged.
Public key: $\mathbf{s}$ equations removed
$\rightsquigarrow$ under-determined system.

Ideas of the attack:

- When $\mathbf{s} < N$, MinRank with no additional cost !
- Adapt the recovery of the matrix $\mathbf{T}$.

Multi-HFE w/ embedding (encr.)

Private key: add $\rho : \mathbb{F}_q^{n-r} \to (\mathbb{F}_q)^n$.
Public key: $\mathbf{r}$ variables less
$\rightsquigarrow$ over-determined system.

Ideas of the attack:

- Solve MinRank on $(n - \mathbf{r} \times n - \mathbf{r})$-matrices
- Complete a rectangular matrix $\mathbf{S}$.

Attack on Multi-HFE Variants

Key result

Many equivalent keys $\Rightarrow N$ degrees of freedom.

Multi-HFE$^-$ (sign.)

Private key: Unchanged.
Public key: $\mathbf{s}$ equations removed
$\rightsquigarrow$ under-determined system.

Ideas of the attack:

- When $\mathbf{s} < N$, MinRank with no additional cost !
- Adapt the recovery of the matrix $\mathbf{T}$.

Multi-HFE w/ embedding (encr.)

Private key: add $\rho : \mathbb{F}_q^{n-r} \to (\mathbb{F}_q)^n$.
Public key: $\mathbf{r}$ variables less
$\rightsquigarrow$ over-determined system.

Ideas of the attack:

- Solve MinRank on $(n - \mathbf{r} \times n - \mathbf{r})$-matrices
- Complete a rectangular matrix $\mathbf{S}$.

Efficient attack: more details in the paper.

Summary

Main Results

- Improved key recovery attack on HFE
- Extension of the attack to Multi-HFE
- Practical challenges from [CCDWY08] broken
- Proved theoretical complexity of the attack
- Characterization of equivalent keys
- Attack on Multi-HFE variants.
- Careful recovery of **S** and **T**

Summary

Main Results

- Improved key recovery attack on HFE
- Extension of the attack to Multi-HFE
- Practical challenges from [CCDWY08] broken
- Proved theoretical complexity of the attack
- Characterization of equivalent keys
- Attack on Multi-HFE variants.
- Careful recovery of $\mathbf{S}$ and $\mathbf{T}$

Characteristic 2

- KS attack does not work: Issue when recovering $\mathbf{S}$ and $\mathbf{T}$
- Extended algorithm in full version.