HFERP - A New Multivariate Encryption Scheme

Yasuhiko Ikematsu (Kyushu University)
Ray Perlner (NIST)
Daniel Smith-Tone (NIST, University of Louisville)
Tsuyoshi Takagi (Kyushi University)
Jeremy Vates (University of Louisville)

10 April, 2018

Early History

- C^*
- "Triangular" Encryption schemes
- HFE

Early History

- C^*
- "Triangular" Encryption schemes
- HFE

All of these are essentially broken.

More Recent Attempts

- ABC Simple Matrix Scheme (quad and cubic)
- ZHFE
- Extension Field Cancellation
- HFE-
- **SRP**

Properties of Surviving Schemes

Typically have twice as many equations as variables (roughly).

Properties of Surviving Schemes

Typically have twice as many equations as variables (roughly).

Question

Can we have fewer equations with efficient key gen, encryption, decryption?

Idea for Constructing Encryption Scheme

Idea

Bootstrap the structure of successful signature schemes to achieve encryption. (Add some central equations that make the “choice” of “vinegar” variables in inversion deterministic.)

Idea for Constructing Encryption Scheme

Idea

Bootstrap the structure of successful signature schemes to achieve encryption. (Add some central equations that make the “choice” of “vinegar” variables in inversion deterministic.)

- Benefit: Security of the “shell” is well understood.

Idea for Constructing Encryption Scheme

Idea

Bootstrap the structure of successful signature schemes to achieve encryption. (Add some central equations that make the "choice" of "vinegar" variables in inversion deterministic.)

- Benefit: Security of the "shell" is well understood.
- Benefit: Do not need to add so many equations.

Idea for Constructing Encryption Scheme

Idea

Bootstrap the structure of successful signature schemes to achieve encryption. (Add some central equations that make the "choice" of "vinegar" variables in inversion deterministic.)

- Benefit: Security of the "shell" is well understood.
- Benefit: Do not need to add so many equations.
- Drawback: Not an original idea. (Usually weak!)

*RP

1. Use UOV (or Rainbow).

*RP

1. Use UOV (or Rainbow).
2. Use the plus modifier (adding random central equations).

*RP

1. Use UOV (or Rainbow).
2. Use the plus modifier (adding random central equations).
3. Drop in invertible central map *.

Constants and Structures

- Fix $d, o, r, s \in \mathbb{Z}^+$, $n = d + o$, and $m = d + o + r + s$,
- a finite field $k = GF(q)$,
- a degree d extension K of k,
- a basis $(\theta_1, \ldots, \theta_d)$ of K/k, and
- a k-vector space isomorphism

$$\phi : k^d \to K \text{ defined by } \phi(\mathbf{x}) = \sum_{i=1}^{d} x_i \theta_i.$$

Critical Layer

Use an efficiently invertible quadratic map

$$F_* : K \to K.$$

Rainbow Layer

- $V = \{1, \ldots, d\},\ O = \{d+1, \ldots, d+o = n\}$

$$f_1(x_1, \ldots, x_d, x_{d+1}, \cdots, x_n) = \sum_{i \in V, j \in O} a_{i,j}^{(1)} x_i x_j + \sum_{i,j \in V} b_{i,j}^{(1)} x_i x_j,$$

$$\vdots$$

$$f_{o+r}(x_1, \ldots, x_d, x_{d+1}, \cdots, x_n) = \sum_{i \in V, j \in O} a_{i,j}^{(o+r)} x_i x_j + \sum_{i,j \in V} b_{i,j}^{(o+r)} x_i x_j,$$

$$F_{\mathrm{R}} = (f_1, \ldots, f_{o+r}) : k^n \to k^{o+r} \quad \text{(quadratic map)}.$$

Plus Layer

$$f_1'(x_1, \ldots, x_{n'}) = \sum_{1 \le i \le j \le n} c_{i,j}^{(1)} x_i x_j,$$

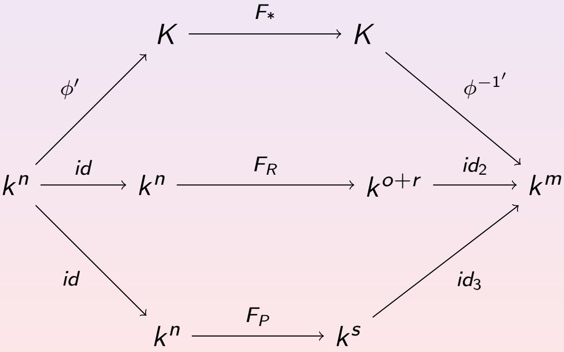
$$\vdots$$

$$f_s'(x_1, \ldots, x_{n'}) = \sum_{1 \le i \le j \le n} c_{i,j}^{(s)} x_i x_j,$$

$$F_P = (f_1', \ldots, f_s') : k^{n'} \to k^s \quad \text{(quadratic map)}.$$

*RP Central Map

$$F := (F_*, F_\mathrm{R}, F_\mathrm{P}) : k^n \to k^m$$



F is easily invertible

To solve $F(\mathbf{x}) = \mathbf{z}$,

- Solve $F_* \circ \phi(x_1, \cdots, x_d) = \phi^{-1}(z_1, \ldots, z_d)$
- Solve $F_R = (f_1, \ldots, f_{o+r}) : k^{n'} \to k^{o+r}$
  $V = \{1, \ldots, d\},\ O = \{d+1, \ldots, d+o\}$

$$z_{d+1} = \sum_{i \in V, j \in O} a_{i,j}^{(1)} x_i x_j + \sum_{i,j \in V} b_{i,j}^{(1)} x_i x_j,$$

$$\vdots$$

$$z_{o+r} = \sum_{i \in V, j \in O} a_{i,j}^{(o+r)} x_i x_j + \sum_{i,j \in V} b_{i,j}^{(o+r)} x_i x_j,$$

Secret Key and Public Key

- $S : k^n \to k^n$: invertible linear map
- $T : k^m \to k^m$: invertible linear map
- Public key

$$G_{*RP} : k^n \xrightarrow{S} k^n \xrightarrow{F} k^m \xrightarrow{T} k^m.$$

SRP

Use $F_* = F_S$ defined by

$$F_S(X) = X^2.$$

$$\begin{array}{ccc} K & \xrightarrow{F_*} & K \\ \phi \uparrow & & \downarrow \phi^{-1} \\ k^d & \xrightarrow{f_*} & k^d \end{array}$$

(Note that f_* is a quadratic map from k^d to k^d.)

A Relevant Algebra

Let $\Phi : \mathbb{E} \rightarrow \mathbb{A}$ be the representation defined by $\Phi(X) = (X, X^q, \ldots, X^{q^{n-1}})$.
Then we can represent $G(X) = \sum_{i,j} \alpha_{i,j} X^{q^i + q^j}$:

$$\begin{bmatrix} X & X^q & \ldots & X^{q^{n-1}} \end{bmatrix} \begin{bmatrix} \alpha_{0,0} & \frac{\alpha_{0,1}}{2} & \cdots & \frac{\alpha_{0,n-1}}{2} \\ \frac{\alpha_{0,1}}{2} & \alpha_{1,1} & \cdots & \frac{\alpha_{1,n-1}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{0,n-1}}{2} & \frac{\alpha_{1,n-1}}{2} & \cdots & \alpha_{n-1,n-1} \end{bmatrix} \begin{bmatrix} X \\ X^q \\ \vdots \\ X^{q^{n-1}} \end{bmatrix}.$$

F_S

$$F_S = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

MinRank Attack on SRP

$$\text{min-Q-rank}(F_S) = 1.$$

$$\text{min-Q-rank}(G_{SRP}) = 1.$$

Theorem (Petzoldt, ____, ____ 2017)

The complexity of this attack on $SRP(q, d, o, r, s)$ is

$$\mathcal{O}\left(\binom{m+1}{1+1}^2 \binom{m}{2}\right), \qquad m = d + o + r + s.$$

HFE

- Fix a degree bound D.

$$F_{HFE}(X) := \sum_{q^i+q^j \leq D} a_{i,j} X^{q^i+q^j} = \sum_{q^i+q^j \leq D} a_{i,j} X^{q^i} \cdot X^{q^j}, \ (a_{i,j} \in K).$$

$$\begin{array}{ccc} K & \xrightarrow{F_{\mathrm{HFE}}} & K \\ \phi \uparrow & & \downarrow \phi^{-1} \\ k^d & \xrightarrow{f_{\mathrm{HFE}}} & k^d \end{array}$$

- (Note that F_{HFE} is a quadratic map on k^d.)

HFE Part of Central Map

$$\begin{bmatrix} X & X^q & \cdots & X^{q^{n-1}} \end{bmatrix} \begin{bmatrix} \alpha_{0,0} & \frac{\alpha_{0,1}}{2} & \cdots & \frac{\alpha_{0,r-1}}{2} & 0 & \cdots & 0 \\ \frac{\alpha_{0,1}}{2} & \alpha_{1,1} & \cdots & \frac{\alpha_{1,r-1}}{2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{0,r-1}}{2} & \frac{\alpha_{r,r-1}}{2} & \cdots & \alpha_{r-1,r-1} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} X \\ X^q \\ \vdots \\ X^{q^{n-1}} \end{bmatrix}$$

More on HFE

Necessary Condition

The positive integer D must be chosen such that

$$F_0(X) = \alpha, \qquad (\alpha \in K), \; deg(F_0) \leq D$$

can be solved efficiently by Berlekamp's algorithm, of which the complexity is $\mathcal{O}(D^3 + dD^2 \log q)$.

Central map of HFERP

- Central map

$$F_{\mathrm{HFERP}} := (F_{\mathrm{HFE}}, F_{\mathrm{R}}, F_{\mathrm{P}}) : k^n \rightarrow k^m$$

- Public Key $G_{\mathrm{HFERP}} := T \circ F_{\mathrm{HFERP}} \circ S$.

Attacks for HFERP

1. MinRank attack on HFE primitive
2. Direct attack
3. Attacks on UOV (Rainbow) structure

Lemma

Assume $\mathrm{char}(k) \neq 2$.

$$G_{SRP} = (G_{SRP,1}, \cdots, G_{SRP,m}) \Rightarrow (P_1, P_2, \cdots, P_m)$$
$$G_{HFERP} = (G_{HFERP,1}, \cdots, G_{HFERP,m}) \Rightarrow (Q_1, Q_2, \cdots, Q_m)$$

MinRank Attack on HFERP

$$\text{min-Q-rank}(F_{\text{HFE}}) = \lfloor \log_q D \rfloor.$$

Theorem

The complexity of this attack on HFERP(q, d, o, r, s) is

$$\mathcal{O}\left(\binom{m + \lfloor \log_q D \rfloor}{1 + \lfloor \log_q D \rfloor}^2 \binom{m}{2}\right), \qquad m = d + o + r + s.$$

Direct Attack on HFERP

Theorem

The degree of regularity d_{reg} of $HFERP(q, d, o, r, s)$ is bounded by

$$d_{reg} \leq \begin{cases} (q-1)(\lfloor \log_q D \rfloor + 1)/2 + 2, & (q : \textit{odd or } \lfloor \log_q D \rfloor : \textit{odd}) \\ (q-1)(\lfloor \log_q D \rfloor + 2)/2 + 1, & \textit{otherwise} \end{cases}$$

Theorem

The complexity of the algebraic attack is given by

$$\mathcal{O}(\binom{n + d_{reg}}{d_{reg}}^2 \binom{n}{2}), \qquad n = d + o.$$

Base Field Rank Attacks - MinRank

MinRank

Find one or more vectors $\mathbf{w}_j$ satisfying

$$\sum_{i=1}^{m} t_i \mathbf{DG}_i(\mathbf{w}_j) = \mathbf{0}.$$

$$Comp_{MinRank} = \mathcal{O}\left(q^d m^\omega\right).$$

Base Field Rank Attacks - Dual Rank/HighRank

HighRank

Find linear combinations of the public polynomials in the span of the HFE maps and first layer Rainbow maps.

$$Comp_{HighRank} = \mathcal{O}\left(q^{m-d} n^{\omega}\right).$$

Parameter selections

$$k = \mathbb{F}_3$$

80-bit security parameters

$$\text{(A)} \quad (d = 42, o = 21, r = 15, s = 17, D = 3^7 + 1)$$
$$\text{(B)} \quad (d = 63, o = 21, r = 11, s = 10, D = 3^7 + 1)$$

128-bit security parameters

$$\text{(C)} \quad (d = 85, o_1 = o_2 = 70, r_1 = r_2 = 89, s = 61, D = 3^7 + 1)$$
$$\text{(D)} \quad (d = 60, o_1 = o_2 = 40, r_1 = r_2 = 23, s = 40, D = 3^9 + 1)$$

Environment

Platform

All the experiments were performed using Magma on a 2.6 GHz Intel Xeon CPU.

(These are *not* optimized implementations. They are barely implementations.)

Experimental Results 1

			HFERP		Random		
(d, o, r, s, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(8, 4, 3, 3, 2188)$	12	18	4, 4, 4, 4, 4	4, 4, 4, 4, 4	4, 4, 4, 4, 4	4, 4, 4, 4, 4	4
$(10, 5, 4, 3, 2188)$	15	22	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5
$(12, 6, 5, 4, 2188)$	18	27	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5
$(14, 7, 5, 5, 2188)$	21	31	6, 5, 5, 5, 5	6, 6, 6, 6, 6	5, 5, 5, 5, 5	6, 6, 6, 6, 6	6

Table 2.A. Direct Attack, $d = 2o, d + o \fallingdotseq 2(r + s), o = 4, 5, 6, 7$

			HFERP		Random		
(d, o, r, s, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(9, 3, 2, 2, 2188)$	12	16	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5
$(12, 4, 2, 2, 2188)$	16	20	5, 6, 6, 5, 5,	5, 6, 6, 6, 5	6, 5, 6, 6, 5	6, 6, 6, 6, 6	6
$(15, 5, 3, 3, 2188)$	20	26	6, 5, 5, 5, 5	6, 6, 6, 6, 6	5, 5, 5, 6, 5	6, 6, 6, 6, 6	6
$(18, 6, 3, 3, 2188)$	24	30	5, 5, 5, 5, 5	7, 7, 7, 7, 7	5, 5, 5, 5, 7	7, 7, 7, 7, 7	7

Table 2.B. Direct Attack, $d = 3o, r + s \fallingdotseq o, o = 3, 4, 5, 6$

Experimental Results 2

			HFERP		Random		
(d, o, r, s, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(3, 3_2, 4_2, 2, 2188)$	9	19	3, 3, 3, 3, 3	3, 3, 2, 3, 2	3, 3, 3, 3, 3	2, 3, 3, 2, 2	3
$(7, 6_2, 7_2, 5, 2188)$	19	38	4, 4, 4, 4, 4	4, 4, 4, 4, 4	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5
$(10, 8_2, 11_2, 7, 2188)$	26	55	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5
$(14, 11_2, 14_2, 10, 2188)$	36	74	5	6	5	6	6

Table 2.C. Direct Attack,
$d \fallingdotseq 3.4a, o \fallingdotseq (2.8a, 2.8a), r \fallingdotseq (3.56a, 3.56a), s \fallingdotseq 2.44a, a = 1, 2, 3, 4$

			HFERP		Random		
(d, o, r, s, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(5, 3_2, 2_2, 3, 3^9 + 1)$	11	18	4, 4, 4, 4, 4	4, 4, 4, 4, 4	4, 4, 4, 4, 4	4, 4, 4, 3, 4	4
$(7, 5_2, 3_2, 5, 3^9 + 1)$	17	28	4, 4, 4, 4, 4	4, 4, 4, 4, 4	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5
$(10, 6_2, 4_2, 6, 3^9 + 1)$	22	36	5, 5, 5, 5, 5	5, 5, 5, 5, 5	5, 5, 5, 5, 5	6, 6, 6, 6, 6	6
$(12, 8_2, 5_2, 8, 3^9 + 1)$	28	46	5, 5, 5, 5, 5	6, 6, 5, 6, 5	5, 5, 5, 5, 5	6, 6, 6, 6, 6	6

Table 2.D. Direct Attack,
$d \fallingdotseq 2.4a, o \fallingdotseq (1.6a, 1.6a), r \fallingdotseq (0.92a, 0.92a), s \fallingdotseq 1.6a, a = 2, 3, 4, 5$

Here $3_2 = (3, 3)$.

Experimental Results 3

	80-bit	80-bit	128-bit	128-bit
	(A)	(B)	(C)	(D)
Key Generation	0.299 s	0.572 s	20.498 s	3.43 s
Encryption	0.001 s	0.001 s	0.006 s	0.001 s
Decryption	3.977 s	8.671 s	49.182 s	124.27 s
Secret Key Size	19.8KB	31.7KB	1344.0KB	226.0KB
Public Key Size	48.2KB	93.6KB	2905.7KB	552.3KB

Future

- Improvements?
- How do we break this thing?

Coffee Break

Coffee now. Questions later.