Multivariate Cryptography
Part 3: HFE (Hidden Field Equations)

Albrecht Petzoldt

PQCrypto Summer School 2017
Eindhoven, Netherlands
Friday, 23.06.2017

Reminder: Construction of MPKCs

- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ (*central map*)
- Two invertible linear maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *Public key*: $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ supposed to look like a random system
- *Private key*: $\mathcal{S}, \ \mathcal{F}, \ \mathcal{T}$ allows to invert the public key

Workflow

Decryption / Signature Generation

$$\begin{tikzcd}[column sep=large, row sep=huge]
\mathbf{w} \in \mathbb{F}^m \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{x} \in \mathbb{F}^m \arrow[r, "\mathcal{F}^{-1}"] & \mathbf{y} \in \mathbb{F}^n \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{z} \in \mathbb{F}^n \arrow[lll, bend left, "\mathcal{P}"']
\end{tikzcd}$$

Encryption / Signature Verification

Big Field Schemes

- Central map $\mathcal{F}$ is defined over a degree n extension field $\mathbb{E}$ of $\mathbb{F}$
- $\bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi : \mathbb{F}^n \to \mathbb{F}^n$ quadratic

Decryption / Signature Generation

$$\begin{tikzcd}
& X \in \mathbb{E} \arrow[r, "\mathcal{F}^{-1}"] & Y \in \mathbb{E} \arrow[d, "\Phi^{-1}"] & \\
\mathbf{w} \in \mathbb{F}^n \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{x} \in \mathbb{F}^n \arrow[u, "\Phi"] \arrow[r, "\bar{\mathcal{F}}^{-1}"] & \mathbf{y} \in \mathbb{F}^n \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{z} \in \mathbb{F}^n \arrow[lll, bend left, "\mathcal{P}"]
\end{tikzcd}$$

Encryption / Signature Verification

Extension Fields

- $\mathbb{F}_q$: finite field with q elements
- $g(X)$ irreducible polynomial in $\mathbb{F}[X]$ of degree n
  $\Rightarrow \mathbb{F}_{q^n} \cong \mathbb{F}[X]/\langle g(X)\rangle$ finite field with q^n elements
- isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$, $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i \cdot X^{i-1}$
- Addition in $\mathbb{F}_{q^n}$: Addition in $\mathbb{F}_q[X]$
- Multiplication in $\mathbb{F}_{q^n}$: Multiplication in $\mathbb{F}_q[X]$ modulo $g(X)$

Example: The field $GF(2^2)$

- Start with the field $\mathbb{F}_2 = \{0, 1\}$ of two elements
- Choose an irreducible polynomial $g(X)$ of degree 2 in $\mathbb{F}_2[X]$, i.e. $g(X) = X^2 + X + 1$

$$\begin{aligned} \Rightarrow \mathbb{F}_{2^2} &\cong \mathbb{F}_2[X]/\langle X^2 + X + 1\rangle = \{0, 1, X, X + 1\} \\ &\cong \{0, 1, w, w^2\} \text{ for a root } w \text{ of } g(X) \end{aligned}$$

$+$	0	1	w	w^2
0	0	1	w	w^2
1	1	0	w^2	w
w	w	w^2	0	1
w^2	w^2	w	1	0

$\times$	0	1	w	w^2
0	0	0	0	0
1	0	1	w	w^2
w	0	w	w^2	1
w^2	0	w^2	1	w

The HFE Cryptosystem [Pa96]

- " Hidden Field Equations"
- proposed by Patarin in 1995
- BigField Scheme
- can be used both for encryption and signatures
- finite field $\mathbb{F}$, extension field $\mathbb{E}$ of degree n, isomorphism $\Phi : \mathbb{F}^n \rightarrow \mathbb{E}$

HFE - Key Generation

- central map $\mathcal{F} : \mathbb{E} \to \mathbb{E}$,

$$\mathcal{F}(X) = \sum_{0 \le i \le j}^{q^i + q^j \le D} \alpha_{ij} X^{q^i + q^j} + \sum_{i=0}^{q^i \le D} \beta_i \cdot X^{q^i} + \gamma$$

  $\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi : \mathbb{F}^n \to \mathbb{F}^n$ quadratic
- degree bound D needed for efficient decryption / signature generation
- linear maps $\mathcal{S}, \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *public key*: $\mathcal{P} = \mathcal{S} \circ \bar{\mathcal{F}} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- *private key*: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$

Encryption

Given: message (plaintext) $\mathbf{z} \in \mathbb{F}^n$

Compute ciphertext $\mathbf{w} \in \mathbb{F}^n$ by $\mathbf{w} = \mathcal{P}(\mathbf{z})$.

Decryption

Given: ciphertext $\mathbf{w} \in \mathbb{F}^n$

1. Compute $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^n$ and $X = \Phi(\mathbf{x}) \in \mathbb{E}$
2. Solve $\mathcal{F}(Y) = X$ over $\mathbb{E}$ via Berlekamp's algorithm
3. Compute $\mathbf{y} = \Phi^{-1}(Y) \in \mathbb{F}^n$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$

Plaintext: $\mathbf{z} \in \mathbb{F}^n$.

Remark

HFE central map is not bijective

$\Rightarrow$ Decryption process does not neccessarily produce unique solution

$\Rightarrow$ Use redundancy in the plaintext

Signature Generation

Given: message d

1. Use hash function $\mathcal{H} : \{0,1\}^\star \to \mathbb{F}^n$ to compute $\mathbf{w} = \mathcal{H}(d)$
2. Compute $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^n$ and $X = \Phi(\mathbf{x}) \in \mathbb{E}$
3. Solve $\mathcal{F}(Y) = X$ over $\mathbb{E}$ via Berlekamp's algorithm
4. Compute $\mathbf{y} = \Phi^{-1}(Y) \in \mathbb{F}^n$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$

Signature: $\mathbf{z} \in \mathbb{F}^n$.

Signature Verification

Given: signature $\mathbf{z} \in \mathbb{F}^n$, message d

- Compute $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^n$
- Compute $\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^n$
- Accept the signature $\mathbf{z} \;\Leftrightarrow \mathbf{w}' = \mathbf{w}$.

Remark

HFE central map is not bijective

$\Rightarrow$ Signature generation process does not output a signature for every input message

$\Rightarrow$ Append a counter to the message d

The Attack of Kipnis and Shamir [KS99]

Idea: Look at the scheme over the extemsion field $\mathbb{E}$

- the linear maps $\mathcal{S}$ and $\mathcal{T}$ relate to univariate maps $\mathcal{S}^\star(X) = \sum_{i=1}^{n-1} s_i \cdot X^{q^i}$ amd $\mathcal{T}^\star(X) = \sum_{i=1}^{n-1} t_i \cdot X^{q^i}$ with (unknown) coefficients s_i and $t_i \in \mathbb{E}$.
- the public key $\mathcal{P}^\star$ can be expressed as

$$\mathcal{P}^\star(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} p_{ij}^\star X^{q^i + q^j} = \underline{X} \cdot P^\star \cdot \underline{X}^T,$$

  where $P^\star = [p_{ij}^\star]$ and $\underline{X} = (X^{q^0}, X^{q^1}, \ldots, X^{q^{n-1}})$.
- The components of the matrix $P^\star$ can be found by polynomial interpolation.

The attack of Kipnis and Shamir (2)

- the relation $\mathcal{P}^\star(X) = \mathcal{S}^\star \circ \mathcal{F} \circ \mathcal{T}^\star(X)$ yields $(\mathcal{S}^\star)^{-1} \circ \mathcal{P}^\star(X) = \mathcal{F} \circ \mathcal{T}^\star(X)$ and

$$\tilde{P} = \sum_{k=0}^{n-1} s_k \cdot G^{\star k} = W \cdot F \cdot W^T$$

  with $g_{ij}^{\star\ k} = ({p^\star}_{i-k \bmod n, j-k \bmod n})^{q^k}$, $w_{ij} = s_{j-i \bmod n}^{q^i}$.

- We know that F has the form $F = \begin{pmatrix} \star & 0 \\ 0 & 0 \end{pmatrix}$.

  $\Rightarrow \mathrm{Rank}(F) \leq r$ with $r = \lfloor \log_q D - 1 \rfloor + 1$.
  $\Rightarrow \mathrm{Rank}(W \cdot F \cdot W^T) \leq r$
  $\Rightarrow$ We can recover the coefficients s_k by solving a MinRank problem over the extension field $\mathbb{E}$.

MinRank attack on HFE

- Computing the map $\mathcal{P}^\star$ is very costly
  $\Rightarrow$ The attack of Kipnis and Shamir is not very efficient.
- Work of Bettale et al: Perform the MinRank attack without recovering $\mathcal{P}^\star \Rightarrow$ HFE can be broken by using a MinRank problem over the base field $\mathbb{F}$.

$$\mathrm{Complexity}_{\mathrm{MinRank}} = \binom{n+r}{r}^{\omega}$$

with $2 < \omega \leq 3$ and $r = \lfloor \log_q(D-1) \rfloor + 1$.

Direct Attacks

- Experiments: Public Systems of HFE can be solved much faster than random systems
- Theoretical Explanation: Upper bound for d_{reg}

$$\mathrm{d_{reg}} \le \begin{cases} \frac{(q-1)\cdot(r-1)}{2} + 2 & q \text{ even and } r \text{ odd}, \\ \frac{(q-1)\cdot r}{2} + 2 & \text{otherwise.} \end{cases},$$

with $r = \lfloor \log_q(D-1) \rfloor + 1$.

$\Rightarrow$ Basic version of HFE is not secure

HFE Variants

Encryption Schemes

- IPHFE+ (not very efficient)
- ZHFE ($\rightarrow$ this conference)
- HFE- (for small minus parameter; $\rightarrow$ this conference)

Signature Schemes

- HFEv-, Gui
- MHFEv ($\rightarrow$ this conference)

HFE Variants

Encryption Schemes

- IPHFE$+$ (not very efficient)
- ZHFE ($\rightarrow$ this conference)
- HFE- (for small minus parameter; $\rightarrow$ this conference)

Signature Schemes

- HFEv-, Gui
- MHFEv ($\rightarrow$ this conference)

HFEv- - Key Generation

- finite field $\mathbb{F}$, extension field $\mathbb{E}$ of degree n, isomorphism $\Phi : \mathbb{F}^n \rightarrow \mathbb{E}$
- central map $\mathcal{F} : \mathbb{F}^v \times \mathbb{E} \rightarrow \mathbb{E}$,

$$\mathcal{F}(X) = \sum_{0 \le i \le j}^{q^i+q^j \le D} \alpha_{ij} X^{q^i+q^j} + \sum_{i=0}^{q^i \le D} \beta_i(v_1, \ldots, v_v) \cdot X^{q^i} + \gamma(v_1, \ldots, v_v)$$

$\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ (\Phi \times \mathrm{id}_v)$ quadratic map: $\mathbb{F}^{n+v} \rightarrow \mathbb{F}^n$

- linear maps $\mathcal{S} : \mathbb{F}^n \rightarrow \mathbb{F}^{n-a}$ and $\mathcal{T} : \mathbb{F}^{n+v} \rightarrow \mathbb{F}^{n+v}$ of maximal rank
- *public key*: $\mathcal{P} = \mathcal{S} \circ \bar{\mathcal{F}} \circ \mathcal{T} : \mathbb{F}^{n+v} \rightarrow \mathbb{F}^{n-a}$
- *private key*: $\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$

Signature Generation

Given: message (hash value) $\mathbf{w} \in \mathbb{F}^{n-a}$

1. Compute $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) \in \mathbb{F}^n$ and $X = \Phi(\mathbf{x}) \in \mathbb{E}$
2. Choose random values for the vinegar variables $v_1, \ldots, v_v$
   Solve $\mathcal{F}_{v_1,\ldots,v_v}(Y) = X$ over $\mathbb{E}$ via Berlekamps algorithm
3. Compute $\mathbf{y} = \Phi^{-1}(Y) \in \mathbb{F}^n$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y}||v_1||\ldots||v_v)$

Signature: $\mathbf{z} \in \mathbb{F}^{n+v}$.

Signature Verification

Given: signature $\mathbf{z} \in \mathbb{F}^{n+v}$, message (hash value) $\mathbf{w} \in \mathbb{F}^{n-a}$

- Compute $\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^{n-a}$
- Accept the signature $\mathbf{z} \; \Leftrightarrow \mathbf{w}' = \mathbf{w}$.

Workflow of HFEv-

Signature Generation

$$
\begin{tikzcd}
& X \in \mathbb{E} \arrow[rr, "\mathcal{F}^{-1}"] & & Y \in \mathbb{E} \arrow[dd, "\Phi^{-1}"] & \\
& & v_1, \dots, v_v & & \\
\mathbf{w} \in \mathbb{F}^{n-a} \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{x} \in \mathbb{F}^{n} \arrow[uu, "\Phi"] \arrow[rr, "\bar{\mathcal{F}}^{-1}"] & & \mathbf{y} \in \mathbb{F}^{n+v} \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{z} \in \mathbb{F}^{n+v} \arrow[llll, bend left, "\mathcal{P}"]
\end{tikzcd}
$$

Signature Verification

Toy Example - Key Generation

- $(q, n, D, a, v) = (4, 3, 17, 0, 1)$. w is a generator of the field $\mathbb{F} = \mathrm{GF}(4)$.
- Extension field $\mathbb{E} = \mathrm{GF}(4^3)$, $\mathbb{E} = \mathbb{F}[b]/\langle b^3 + w\rangle$
- isomorphism $\phi : \mathbb{F}^3 \to \mathbb{E}, (a_1, a_2, a_3) = a_1 + a_2 \cdot b + a_3 \cdot b^2$.
- affine map $\mathcal{S} : \mathbb{F}^3 \to \mathbb{F}^3$,

$$\mathcal{S}(x_1, \ldots, x_3) = \begin{pmatrix} w & w & 1 \\ w & 1 & 0 \\ w & 0 & w^2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} w \\ 0 \\ 1 \end{pmatrix}$$

- affine map $\mathcal{T} : \mathbb{F}^4 \to \mathbb{F}^4$,

$$\mathcal{T}(x_1, \ldots, x_4) = \begin{pmatrix} 0 & w & w & 1 \\ w^2 & 0 & w & w^2 \\ w^2 & 1 & w^2 & w^2 \\ w^2 & 0 & 1 & w^2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_4 \end{pmatrix} + \begin{pmatrix} w^2 \\ w \\ w \\ w^2 \end{pmatrix}$$

Key Generation (2)

The central map $\mathcal{F} : \mathbb{E} \times \mathbb{F} \to \mathbb{E}$ is given by

$$\begin{aligned} \mathcal{F} &= \alpha_{17} X^{17} + \alpha_8 X^8 + \alpha_5 X^5 + \alpha_2 X^2 \\ &+ \beta_{16}(x_4) \cdot X^{16} + \beta_4(x_4) \cdot X^4 + \beta_2(x_4) \cdot X^2 + \beta_1(x_4) \cdot X + \gamma(x_4) \end{aligned}$$

with $\alpha_{17} = b^2 + b + w$, $\alpha_8 = w^2$, $\alpha_5 = w^2 b^2 + w^2$, $\alpha_2 = wb^2 + wb + 1$,
$\beta_{16} = (w^2 x_4 + 1) \cdot b^2 + (wx_4 + 1) \cdot b + wx_4 + w^2$,
$\beta_4 = x_4 b^2 + (x_4 + w) \cdot b + x_4 + w$,
$\beta_1 = (w^2 x_4 + w^2) \cdot b^2 + (w^2 x_4 + w) \cdot b + x_4 + 1$ and

$$\gamma = (x_4^2 + w) \cdot b^2 + (wx_4^2 + x_4) \cdot b + x_4^2 + wx_4 + w.$$

Public Key Computation (1)

First, we lift the (first three components of the) map $\mathcal{T}$ to the extension field $\mathbb{E}$ (using the isomorphism Φ). We get

$$\begin{aligned}\hat{X} &= (w^2x_1 + x_2 + w^2x_3 + w^2x_4 + w) \cdot b^2 + (w^2x_1 + wx_3 + w^2x_4 + w) \cdot b \\ &+ wx_2 + wx_3 + x_4 + w^2\end{aligned}$$

Next we evaluate the central map $\mathcal{F}$ at $\hat{X}$. We get

$$\begin{aligned}\hat{Y} = \mathcal{F}(\hat{X}) &= (wx_1x_2 + wx_1x_4 + w^2x_2x_3 + wx_2x_4 + wx_3x_4 \\ &+ w^2x_3 + wx_4^2 + wx_4 + 1) \cdot b^2 \\ &+ (w^2x_1^2 + wx_1x_2 + wx_1x_3 + x_1x_4 + x_1 + x_2^2 + x_2x_4 \\ &+ x_2 + w^2x_3^2 + wx_3x_4 + x_3 + x_4^2 + w^2x_4 + w^2) \cdot b \\ &+ x_1x_2 + x_1x_3 + wx_1x_4 + x_1 + x_2^2 + wx_2x_3 + x_3^2 \\ &+ x_3 + x_4^2 + wx_4 + w\end{aligned}$$

Public Key Computation (2)

Finally, we move $\hat{Y}$ back to the vector space $\mathbb{F}^3$ and apply the second affine map $\mathcal{S}$. We obtain

$$\begin{aligned}
p^{(1)}(x_1,\ldots,x_4) &= x_1^2 + w^2x_1x_2 + x_1x_3 + w^2x_1x_4 + wx_2 + w^2x_3^2 \\
&+ x_3x_4 + w^2x_3 + wx_4^2 + 1, \\
p^{(2)}(x_1,\ldots,x_4) &= w^2x_1^2 + wx_1x_4 + w^2x_1 + w^2x_2^2 + w^2x_2x_3 + x_2x_4 \\
&+ x_2 + x_3^2 + wx_3x_4 + w^2x_3 + w^2x_4^2, \\
p^{(3)}(x_1,\ldots,x_4) &= w^2x_1x_2 + wx_1x_3 + wx_1x_4 + wx_1 + wx_2^2 + x_2x_3 \\
&+ x_2x_4 + wx_3^2 + x_3x_4 + w^2x_4^2 + wx_4 + 1.
\end{aligned}$$

Signature Generation

We want to generate a signature $\mathbf{z} \in \mathbb{F}^4$ for the message $\mathbf{w} = (0, w, w^2) \in \mathbb{F}^3$.
First, we invert the affine map $\mathcal{S}$ and obtain

$$\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w}) = (1, 1, w)$$

and lift $\mathbf{X}$ to the extension field $\mathbb{E}$, obtaining

$$X = \phi(\mathbf{x}) = 1 + b + wb^2.$$

We choose $x_4 = 1$ and substitute it into the central map $\mathcal{F}$. We get

$$\begin{aligned} \mathcal{F}_1(X) &= (b^2 + b + w) \cdot X^{17} + w^2 \cdot X^8 + (w^2 b^2 + w^2) \cdot X^5 \\ &+ (wb^2 + wb + 1) \cdot X^2 + (wb^2 + w^2 b + 1) \cdot X^{16} \\ &+ (b^2 + w^2 b + w^2) \cdot X^4 + b \cdot X + w^2 b^2 + w^2 b + 1. \end{aligned}$$

Signature Generation (2)

To invert the equation $\mathcal{F}_1(\mathbf{Y}) = \mathbf{X}$, we compute

$$\gcd(\mathcal{F}_1(X) - \mathbf{X}, X^{4^3} - X) = X + b^2 + w^2 b + w.$$

Therefore, a solution to the equation is given by $\mathbf{Y} = (b^2 + w^2 b + w)$. Moving $\mathbf{Y}$ down to the vector space and applying $\mathcal{T}^{-1}$ yields the signature

$$\mathbf{z} = (w^2, w^2, 1, w).$$

Signature Verification

To check, if $\mathbf{z}$ is indeed a valid signature for the message $\mathbf{w}$, we compute

$$\mathbf{w}' = \mathcal{P}(w^2, w^2, 1, w) = (0, w, w^2).$$

Since $\mathbf{w}' = \mathbf{w}$ holds, the signature $\mathbf{z}$ is accepted.

Security

Main Attacks

- MinRank Attack
  $\mathrm{Rank}(F) = r + a + v$

$$\Rightarrow \mathrm{Compl}_{\mathrm{MinRank}} = \binom{n + r + a + v}{r + a + v}^{\omega}$$

- Direct attack [DY13]

$$\mathrm{d_{reg}} \leq \begin{cases} \frac{(q-1)\cdot(r+a+v-1)}{2} + 2 & q \text{ even and } r + a \text{ odd}, \\ \frac{(q-1)\cdot(r+a+v)}{2} + 2 & \text{otherwise}. \end{cases},$$

with $r = \lfloor \log_q(D-1) \rfloor + 1$ and $2 < \omega \leq 3$.

Efficiency

Most costly step in the signature generation process: Inversion of the univariate polynomial equation

$$\mathcal{F}_{(v_1,\ldots,v_v)}(Y) = X \tag{1}$$

by Berlekamp's algorithm

$$\mathrm{Complexity}_{\mathrm{Berlekamp}} = \mathcal{O}(D^3 + n \cdot D^2)$$

$\Rightarrow$ Choose D as small as possible

Conflict

- Efficiency: Choose small D
- Security: $r = \lfloor \log_q(D-1) \rfloor + 1$ should not be too small

$\Rightarrow$ Choose small q, e.g. $q = 2$

Can we define a HFEv- like scheme over GF(2) [PD15]?

Remark: We only consider classical attacks (primarily)

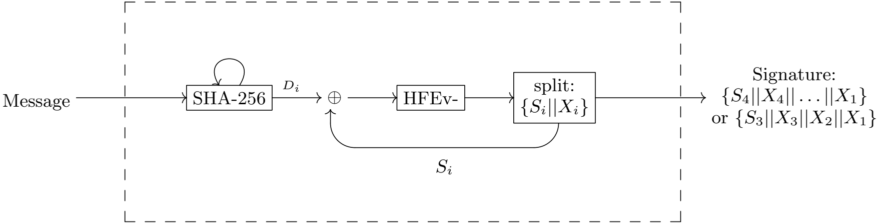
First Problem: Collision Resistance of the hash function

security level k bit $\Rightarrow$ hash length $2k$ $\Rightarrow$ public key size $> (2k)^3/2 = 4k^2$

	security level	# equations	publc key size
	80	160	>250 kB
	100	200	>500 kB
bit	128	256	>1 MB
	192	384	>3 MB
	256	512	> 8 MB

Solution: Specially designed signature generation process

- Generate several HFEv- signatures for different hash values of the same message
- Combine these HFEv- signatures to a single (shorter) signature



We call our new scheme Gui.

The Gui Signature Scheme

Why this name?

Gui

- Chinese pottery from Longshan period
- more than 4000 years old
- 3 legs: one in front, 2 in the back

- front leg : HFE
- back legs: Minus + Vinegar

Signature Generationi

Input: Gui private key $(\mathcal{S}, \mathcal{F}, \mathcal{T})$ message $\mathbf{d}$, repetition factor k

Output: signature $\sigma \in \mathrm{GF}(2)^{(n-a)+k(a+v)}$

```
h ← SHA-256(d)
S_0 ← 0 ∈ GF(2)^(n−a)
for i = 1 to k do
    D_i ← first n − a bits of h
    (S_i, X_i) ← HFEv−^(−1)(D_i ⊕ S_(i−1))
    h ← SHA-256(h)
end for
σ ← (S_k||X_k|| . . . ||X_1)
return σ
```

Signature Verification

Input: Gui public key $\mathcal{P}$, message $\mathbf{d}$, repetition factor k, signature $\sigma \in \mathrm{GF}(2)^{(n-a)+k(a+v)}$

Output: **TRUE** or **FALSE**

$\mathbf{h} \leftarrow$ SHA-256($\mathbf{d}$)
$(S_k, X_k, \ldots, X_1) \leftarrow \sigma$
for $i = 1$ to k **do**
    $D_i \leftarrow$ first $n - a$ bits of $\mathbf{h}$
    $\mathbf{h} \leftarrow$ SHA-256($\mathbf{h}$)
end for
for $i = k - 1$ to 0 **do**
    $S_i \leftarrow \mathcal{P}(S_{i+1} || X_{i+1}) \oplus D_{i+1}$
end for
if $S_0 = \mathbf{0}$ **then**
    return TRUE
else
    return FALSE
end if

How to find suitable parameters for HFEv- over GF(2)?

Collision attacks are no longer a problem

$\Rightarrow$ Parameters are determined by the complexity of MinRank and direct attacks

- For the complexity os the MinRank attack we have a concrete formula
- For the direct attack, we only have an upper bound on d_{reg}.

$$\mathrm{d_{reg}} \leq \begin{cases} \frac{(q-1)\cdot(r+a+v-1)}{2} + 2 & q \text{ even and } r+a \text{ odd,} \\ \frac{(q-1)\cdot(r+a+v)}{2} + 2 & \text{otherwise.} \end{cases} \qquad (\star)$$

$\Rightarrow$ Perform experiments to estimate d_{reg} in practice.

Experiments

We want to answer the following questions

1. Can we observe the tradeoff between d, a and v indicated by $(\star)$ by experiments?
2. Is the concrete ratio between a and v important for the security of the scheme?
3. Is the upper bound on d_{reg} given by $(\star)$ reasonably tight?
4. Can we reach high values of d_{reg} even for small values of D?
5. Is this still true for the hybrid approach?

Research Question 1

Can we observe the tradeoff between d and $(a+v)$ indicated by $(\star)$ by experiments?

- Fix number of equations and the degree D, increases $= a + v$
- Create HFEv-(n, D, a, v) systems
- add field equations $x_i^2 - x_i$
- solve the systems with the F_4 algorithm

		20 equations			
D	r	minimal s	d_{reg}	time (s)	memory (MB)
129	8	0	5	2.74	109.7
65	7	$s = 1$	5	2.69	110.7
33	6	$s = 2$	5	2.75	109.7
17	5	$s = 3$	5	2.72	109.7
9	4	$s = 4$	5	2.73	110.7
5	3	$s = 5$	5	2.73	109.6
random system			5	2.85	110.8

Research Question 2

Is the concrete ratio between a and v important for the security of the scheme?

- Fix number of equations, D and s, vary $a \in \{0, \ldots, s\}$ and set $v = s - a$
- Create HFEv-(n, D, a, v) systems
- add field equations
- solve the systems with F_4

D=5, a+v=8				
a	v	d_{reg}	time (s)	memory (MB)
0	8	6	246.6	7,582
1	7	6	246.2	7,579
2	6	6	246.6	7,580
3	5	6	248.1	7,581
4	4	6	247.1	7,581
5	3	6	248.3	7,582
6	2	6	248.3	7,554
7	1	**5**	**99.3**	**1,317**
8	0	**5**	**88.3**	**1,509**

Research Question 3

Is the upper bound on d_{reg} given by $(\star)$ reasonably tight?

- Fix D, a and v
- Increase n until we reach the upper bound on d_{reg} or run out of memory

Tight instances

D	a	v	upper bound for d_{reg} $(\star)$	d_{reg} (experimental)	
5	0	0	3	3	for $n \geq 10$
	1	1	4	4	for $n \geq 23$
9	0	1	4	4	for $n \geq 23$
	1	1	4	4	for $n \geq 21$
17	0	0	4	4	for $n \geq 15$
	0	1	4	4	for $n \geq 12$

$\Rightarrow$ For small values of D, a and v we could reach the bound.

$\Rightarrow$ For most of the other parameter sets we missed the upper bound only by 1.

Research Question 4

Can we reach high values of d_{reg} even for small values of D?

D	a	v	d_{reg} (experimental)		upper bound for d_{reg} ($\star$)
5	6	6	7	for $n \geq 38$	9
9	5	5	7	for $n \geq 37$	8
17	4	4	7	for $n \geq 37$	8

$\Rightarrow$ Even for small values of D we can, by increasing a and v,
reach $d_{\mathrm{reg}} \geq 7$.

Research Question 5

Is this still true when guessing some variables before applying F_4 (hybrid approach)?
$\Rightarrow$ Even when guessing up to 10 variables we can reach $d_{\mathrm{reg}} = 7$

By substituting $d_{\mathrm{reg}} = 7$ into the formula

$$\mathrm{Complexity}_{\mathrm{direct}} = 3 \cdot \binom{n + d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^2 \cdot \binom{n}{2}$$

gives a lower bound for the complexity of the direct attack against our scheme.

Parameter Choice of HFEv- over GF(2)

Efficiency $\Rightarrow$ Choose D as small as possible

- $D = 5 \Rightarrow r = \lfloor \mathrm{Log}_2(D-1) \rfloor + 1 = 3$
- $D = 9 \Rightarrow r = \lfloor \mathrm{Log}_2(D-1) \rfloor + 1 = 4$
- $D = 17 \Rightarrow r = \lfloor \mathrm{Log}_2(D-1) \rfloor + 1 = 5$

Increase a and v to reach the required security level
Choose a and v as equal as possible, i.e. $0 \leq v - a \leq 1$.

Parameters

We propose four versions of Gui

- Gui-96 with $(n, D, a, v) = (96, 5, 6, 6)$ providing a security level of 80 bit
- Gui-95 with $(n, D, a, v) = (95, 9, 5, 5)$ providing a security level of 80 bit
- Gui-94 with $(n, D, a, v) = (94, 17, 4, 4)$ providing a security level of 80 bit

  and
- Gui-127 with $(n, D, a, v) = (127, 9, 4, 6)$ providing a security level of 120 bit

Parameters and Key Sizes (pre-quantum)

scheme	security level (bit)	input size (bit)	signature size (bit)	public key size (Bytes)	private key size (Bytes)
Gui-96	80	90	126	63,036	3,175
Gui-95	80	90	120	60,600	3,053
Gui-94	80	90	122	58,212	2,943
Gui-127	120	123	163	142,576	5,350
RSA-1024	80	1024	1024	128	128
RSA-2048	112	2048	2048	256	256
ECDSA P160	80	160	320	40	60
ECDSA P192	96	192	384	48	72
ECDSA P256	128	256	512	64	96

Quantum Attacks

A determined multivariate system of m equations over GF(2) can be solved using

$$2^{m/2} \cdot 2 \cdot m^3$$

operations using a quantum computer.
$\Rightarrow$ we need a large number of equations (and variables) in the public key
$\Rightarrow$ very large public key size

Quantum Parameters

quantum security level (bit)		public key size (kB)	private key size (kB)	signature size (bit)
80	Gui (GF(2),120,9,3,3,2)	110.7	3.8	129
100	Gui (GF(2),161,9,6,7,2)	271.8	7.5	181
128	Gui (GF(2),219,9,11,11,2)	680.4	14.5	252
192	Gui (GF(2),350,9,18,19,2)	2,781.6	40.9	406
256	Gui (GF(2),483,9,26,26,2)	7,269.2	82.8	561

HFEv- - Summary

- very short signatures
- security well understood
- conflict between security and efficiency
- restricted to very small fields

HFEv- over GF(2)

- very large public keys (especially when considering quantum attacks)

$\Rightarrow$ Can we do better when increasing the field size slightly (e.g. GF(4), GF(5); ongoing work)

$\Rightarrow$ Alternative: MHFE ($\rightarrow$ this conference)

Other Multivariate Schemes

- symmetric schemes
  - hash functions, stream cipher (provable secure; not very efficient)
- zero knowledge identification
  $\Rightarrow$ provable secure signatures (MQDSS), (threshold) ring signature
- public key encryption (Simple Matrix)
- signature schemes with special properties
  - (sequential) aggregate signatures
  - blind signatures

Conclusion

Multivariate Cryptography

- major candidate for post-quantum cryptography
- fast, moderate computational requirements
- large keys
- many practical signature schemes
- not so good for encryption schemes

Open Problems

- security of multivariate schemes
- key size reduction
- develop other schemes (key exchange ...)

References

Pa96 J. Patarin: Hidden Field equations (HFE) and Isomorphisms of Polynomials (IP). EUROCRYPT 96, LNCS vol.1070, pp. 38–48, Springer, 1996.

KS99 A. Kipnis, A. Shamir: Cryptanalysis of the HFE Public Key Cryptosystem. CRYPTO 99, LNCS vol. 1666, pp. 19 - 30. Springer 1999.

PD15 A. Petzoldt, M.S. Chen, B.Y. Yang, C. Tao, J. Ding: Design Principles for HFEv- based Signature Schemes. ASIACRYPT 2015 - Part 1, LNCS vol. 9452, pp. 311-334. Springer, 2015.

DY13 J. Ding, B.Y. Yang: Degree of regularity for HFEv and HFEv-. PQCrypto 2013, LNCS vol. 7932, pp. 52 - 66. Springer, 2013.