Efficient Key Recovery for all HFE Signature Variants

Chengdong Tao, Albrecht Petzoldt, Jintai Ding

3rd NIST Post-Quantum Standardization Conference

07.06.2021

Multivariate Cryptography

Public Key: System of multivariate quadratic polynomials

$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
&\;\;\vdots \\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}
\end{aligned}
$$

Multivariate Cryptography

Public Key: System of multivariate quadratic polynomials

$$
\begin{aligned}
p^{(1)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}
\end{aligned}
$$

Security based on the

Problem MQ: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}),\dots,p^{(m)}(\mathbf{x})$, find a vector $\bar{\mathbf{x}} = (\bar{x}_1,\dots,\bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \dots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

Construction (BigField Schemes)

- isomorphism $\Phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^n}$

Construction (BigField Schemes)

- isomorphism $\Phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^n}$
- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$
  $\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is quadratic

Construction (BigField Schemes)

- isomorphism $\Phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^n}$
- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$
  $\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is quadratic
- Two invertible linear maps $\mathcal{T} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ and $\mathcal{S} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$

Construction (BigField Schemes)

- isomorphism $\Phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^n}$
- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$
  $\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is quadratic
- Two invertible linear maps $\mathcal{T} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ and $\mathcal{S} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$
- *Public key*: $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ supposed to look like a random system

Construction (BigField Schemes)

- isomorphism $\Phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$
- Easily invertible quadratic map $\mathcal{F} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$
  $\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is quadratic
- Two invertible linear maps $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$
- *Public key*: $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ supposed to look like a random system
- *Private key*: $\mathcal{T}, \ \mathcal{F}, \ \mathcal{S}$ allows to invert the public key

BigField Signature Schemes

Signature Generation

$$
\begin{tikzcd}
 & & X \in \mathbb{F}_{q^n} \arrow[r, "\mathcal{F}^{-1}"] & Y \in \mathbb{F}_{q^n} \arrow[d, "\Phi^{-1}"] & \\
m \in \{0,1\}^\star \arrow[r] & \mathbf{w} \in \mathbb{F}_q^n \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{x} \in \mathbb{F}_q^n \arrow[u, "\Phi"] \arrow[r, "\bar{\mathcal{F}}^{-1}"] & \mathbf{y} \in \mathbb{F}_q^n \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{z} \in \mathbb{F}_q^n \arrow[lll, bend left, "\mathcal{P}"]
\end{tikzcd}
$$

Signature Verification

BigField Signature Schemes

Signature Generation

$$\begin{tikzcd}
 & & X \in \mathbb{F}_{q^n} \arrow[r, "\mathcal{F}^{-1}"] & Y \in \mathbb{F}_{q^n} \arrow[d, "\Phi^{-1}"] & \\
m \in \{0,1\}^{\star} \arrow[r] & \mathbf{w} \in \mathbb{F}_q^n \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{x} \in \mathbb{F}_q^n \arrow[u, "\Phi"] \arrow[r, "\bar{\mathcal{F}}^{-1}"] & \mathbf{y} \in \mathbb{F}_q^n \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{z} \in \mathbb{F}_q^n \arrow[lll, bend left, "\mathcal{P}"]
\end{tikzcd}$$

Signature Verification

Signature Generation: Given: message $m \in \{0,1\}^{\star}$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$ compute recursively $\mathbf{w} = \mathcal{H}(m)$, $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w})$, $X = \Phi(\mathbf{x})$, $Y = \mathcal{F}^{-1}(X)$, $\mathbf{y} = \Phi^{-1}(Y)$ and $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{y})$

BigField Signature Schemes

Signature Generation

$$\begin{tikzcd}
& & X \in \mathbb{F}_{q^n} \arrow[r, "\mathcal{F}^{-1}"] & Y \in \mathbb{F}_{q^n} \arrow[d, "\Phi^{-1}"] & \\
m \in \{0,1\}^\star \arrow[r] & \mathbf{w} \in \mathbb{F}_q^n \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{x} \in \mathbb{F}_q^n \arrow[u, "\Phi"] \arrow[r, "\bar{\mathcal{F}}^{-1}"] & \mathbf{y} \in \mathbb{F}_q^n \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{z} \in \mathbb{F}_q^n \arrow[lll, bend left, "\mathcal{P}"]
\end{tikzcd}$$

Signature Verification

Signature Generation: Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$ compute recursively $\mathbf{w} = \mathcal{H}(m)$, $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w})$, $X = \Phi(\mathbf{x})$, $Y = \mathcal{F}^{-1}(X)$, $\mathbf{y} = \Phi^{-1}(Y)$ and $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{y})$

Signature Verification: Given: message $m \in \{0,1\}^\star$, signature $\mathbf{z} \in \mathbb{F}_q^n$, public key $\mathcal{P}$ check if $\mathcal{P}(\mathbf{z}) = \mathcal{H}(m)$

HFEv^{-} - Key Generation

- BigField + Minus Modification + Vinegar Variation

HFEv$^-$ - Key Generation

- BigField + Minus Modification + Vinegar Variation
- central map $\mathcal{F} : \mathbb{F}_q^v \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$,

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

$\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi$ quadratic map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$

HFEv$^-$ - Key Generation

- BigField + Minus Modification + Vinegar Variation
- central map $\mathcal{F} : \mathbb{F}_q^v \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$,

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

$\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi$ quadratic map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$

- linear maps $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-a}$ and $\mathcal{S} : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n+v}$ of maximal rank

HFEv$^-$ - Key Generation

- BigField + Minus Modification + Vinegar Variation
- central map $\mathcal{F} : \mathbb{F}_q^v \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$,

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

$\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi$ quadratic map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$

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

HFEv$^-$ - Key Generation

- BigField + Minus Modification + Vinegar Variation
- central map $\mathcal{F}: \mathbb{F}_q^v \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$,

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

$\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi$ quadratic map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$

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

Signature Generation

Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$

Signature Generation

Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$

1. Compute the hash value $\mathbf{w} = \mathcal{H}(m) \in \mathbb{F}_q^{n-a}$

Signature Generation

Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$

1. Compute the hash value $\mathbf{w} = \mathcal{H}(m) \in \mathbb{F}_q^{n-a}$
2. Compute $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w}) \in \mathbb{F}_q^n$ and $X = \Phi(\mathbf{x}) \in \mathbb{F}_{q^n}$

Signature Generation

Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$

1. Compute the hash value $\mathbf{w} = \mathcal{H}(m) \in \mathbb{F}_q^{n-a}$
2. Compute $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w}) \in \mathbb{F}_q^n$ and $X = \Phi(\mathbf{x}) \in \mathbb{F}_{q^n}$
3. Choose random values for the vinegar variables $v_1, \ldots, v_v$

Signature Generation

Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$

1. Compute the hash value $\mathbf{w} = \mathcal{H}(m) \in \mathbb{F}_q^{n-a}$
2. Compute $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w}) \in \mathbb{F}_q^n$ and $X = \Phi(\mathbf{x}) \in \mathbb{F}_{q^n}$
3. Choose random values for the vinegar variables $v_1, \ldots, v_v$
   Solve $\mathcal{F}_{v_1,\ldots,v_v}(Y) = X$ over $\mathbb{F}_{q^n}$ via Berlekamps algorithm

Signature Generation

Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$

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

Signature Generation

Given: message $m \in \{0,1\}^\star$, private key $\mathcal{T}, \mathcal{F}, \mathcal{S}$

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

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

Signature Verification

Given: signature $\mathbf{z} \in \mathbb{F}_q^{n+v}$, document $m \in \{0,1\}^\star$

Signature Verification

Given: signature $\mathbf{z} \in \mathbb{F}_q^{n+v}$, document $m \in \{0,1\}^\star$

- Compute the hash value $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}_q^{n-a}$

Signature Verification

Given: signature $\mathbf{z} \in \mathbb{F}_q^{n+v}$, document $m \in \{0,1\}^\star$

- Compute the hash value $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}_q^{n-a}$
- Compute $\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}_q^{n-a}$

Signature Verification

Given: signature $\mathbf{z} \in \mathbb{F}_q^{n+v}$, document $m \in \{0,1\}^\star$

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

Previous Attacks against HFEv$^-$

- direct attack (signature forgery)
  degree of regularity is bounded by

$$\begin{cases} \frac{(q-1)(d+v+a-1)}{2} + 2 & \text{if } q \text{ is even and } d+a \text{ is odd,} \\ \frac{(q-1)(d+v+a)}{2} + 2 & \text{otherwise.} \end{cases} \qquad (d = \lfloor \log_q D \rfloor)$$

Previous Attacks against HFEv$^-$

- direct attack (signature forgery)
  degree of regularity is bounded by

$$\begin{cases} \frac{(q-1)(d+v+a-1)}{2} + 2 & \text{if } q \text{ is even and } d+a \text{ is odd,} \\ \frac{(q-1)(d+v+a)}{2} + 2 & \text{otherwise.} \end{cases} \qquad (d = \lfloor \log_q D \rfloor)$$

- MinRank attack (key recovery)
  min-Q-rank: degree of the public key as a quadratic form over the extension field

Previous Attacks against HFEv$^-$

- direct attack (signature forgery)
  degree of regularity is bounded by

$$\begin{cases} \frac{(q-1)(d+v+a-1)}{2} + 2 & \text{if } q \text{ is even and } d+a \text{ is odd,} \\ \frac{(q-1)(d+v+a)}{2} + 2 & \text{otherwise.} \end{cases} \qquad (d = \lfloor \log_q D \rfloor)$$

- MinRank attack (key recovery)
  min-Q-rank: degree of the public key as a quadratic form over the extension field
  min-Q-rank is bounded by $d + a + v$

Previous Attacks against HFEv$^-$

- direct attack (signature forgery)
  degree of regularity is bounded by

$$\begin{cases} \frac{(q-1)(d+v+a-1)}{2} + 2 & \text{if } q \text{ is even and } d+a \text{ is odd,} \\ \frac{(q-1)(d+v+a)}{2} + 2 & \text{otherwise.} \end{cases} \qquad (d = \lfloor \log_q D \rfloor)$$

- MinRank attack (key recovery)
  min-Q-rank: degree of the public key as a quadratic form over the extension field
  min-Q-rank is bounded by $d+a+v$

$$\mathcal{O}\left(\binom{n+d+a+v+1}{d+a+v+1}^{\omega} \right),$$

Our Result

We propose a MinRank style attack against all HFE signature variants.
The complexity of our attack is

$$\mathcal{O}\left(\binom{n+d+v+1}{d+1}^{\omega}\right)$$

Our Result

We propose a MinRank style attack against all HFE signature variants.
The complexity of our attack is

$$\mathcal{O}\left(\binom{n+d+v+1}{d+1}^{\omega}\right)$$

- independent of a

Our Result

We propose a MinRank style attack against all HFE signature variants.
The complexity of our attack is

$$\mathcal{O}\left(\binom{n+d+v+1}{d+1}^{\omega}\right)$$

- independent of a
- polynomial in v

Preliminaries

- We use the matrix representation of the HFE central map, i.e.

$\mathcal{F}(X, x_1, \ldots, x_v) = (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v) F^{*0} (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v)^t$ with

$$F^{*0} = \begin{pmatrix} \alpha_{00} & \alpha_{01} & \cdots & \alpha_{0,n-1} & \gamma_{00} & \gamma_{01} & \cdots & \gamma_{0,v-1} \\ \alpha_{10} & \alpha_{11} & \cdots & \alpha_{1,n-1} & \gamma_{10} & \gamma_{11} & \cdots & \gamma_{1,v-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1,0} & \alpha_{n-1,1} & \cdots & \alpha_{n-1,n-1} & \gamma_{n-1,0} & \gamma_{n-1,1} & \cdots & \gamma_{n-1,v-1} \\ \beta_{00} & \beta_{01} & \cdots & \beta_{0,n-1} & \delta_{00} & \delta_{01} & \cdots & \delta_{0,v-1} \\ \beta_{10} & \beta_{11} & \cdots & \beta_{1,n-1} & \delta_{10} & \delta_{11} & \cdots & \delta_{1,v-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{v-1,0} & \beta_{v-1,1} & \cdots & \beta_{v-1,n-1} & \delta_{v-1,0} & \delta_{v-1,1} & \cdots & \delta_{v-1,v-1} \end{pmatrix}$$

Preliminaries

- We use the matrix representation of the HFE central map, i.e.

$$\mathcal{F}(X, x_1, \ldots, x_v) = (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v) F^{*0} (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v)^t \text{ with}$$

$$F^{*0} = \begin{pmatrix} \alpha_{00} & \alpha_{01} & \cdots & \alpha_{0,n-1} & \gamma_{00} & \gamma_{01} & \cdots & \gamma_{0,v-1} \\ \alpha_{10} & \alpha_{11} & \cdots & \alpha_{1,n-1} & \gamma_{10} & \gamma_{11} & \cdots & \gamma_{1,v-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1,0} & \alpha_{n-1,1} & \cdots & \alpha_{n-1,n-1} & \gamma_{n-1,0} & \gamma_{n-1,1} & \cdots & \gamma_{n-1,v-1} \\ \beta_{00} & \beta_{01} & \cdots & \beta_{0,n-1} & \delta_{00} & \delta_{01} & \cdots & \delta_{0,v-1} \\ \beta_{10} & \beta_{11} & \cdots & \beta_{1,n-1} & \delta_{10} & \delta_{11} & \cdots & \delta_{1,v-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{v-1,0} & \beta_{v-1,1} & \cdots & \beta_{v-1,n-1} & \delta_{v-1,0} & \delta_{v-1,1} & \cdots & \delta_{v-1,v-1} \end{pmatrix}$$

$\Rightarrow$ We get

$$\mathcal{F}^{q^k}(X, x_1, \ldots, x_v) = (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v) F^{*k} (X, X^q, \ldots, X^{q^{n-1}}, x_1, \ldots, x_v)^t,$$

Preliminaries (2)

- We use a morphism $\Phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ given by the matrix

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^q & \cdots & \theta^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1} & (\theta^{n-1})^q & \cdots & (\theta^{n-1})^{q^{n-1}} \end{pmatrix}, \qquad (1)$$

(θ is a generator of $\mathbb{F}_{q^n}$)

Preliminaries (2)

- We use a morphism $\Phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ given by the matrix

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^q & \cdots & \theta^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1} & (\theta^{n-1})^q & \cdots & (\theta^{n-1})^{q^{n-1}} \end{pmatrix}, \qquad (1)$$

  (θ is a generator of $\mathbb{F}_{q^n}$)
- We get $\Phi(V) = (V, V^q, \ldots, V^{q^{n-1}}) \cdot M^{-1} =: (v_1, \ldots, v_n)$ and $\Phi^{-1}(v_1, \ldots, v_n) = \text{ first component of } (v_1, \ldots, v_n) \cdot M$

Preliminaries (2)

- We use a morphism $\Phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ given by the matrix

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^q & \cdots & \theta^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1} & (\theta^{n-1})^q & \cdots & (\theta^{n-1})^{q^{n-1}} \end{pmatrix}, \tag{1}$$

  (θ is a generator of $\mathbb{F}_{q^n}$)
- We get $\Phi(V) = (V, V^q, \ldots, V^{q^{n-1}}) \cdot M^{-1} =: (v_1, \ldots, v_n)$ and $\Phi^{-1}(v_1, \ldots, v_n) = \text{ first component of } (v_1, \ldots, v_n) \cdot M$
- In order to cover the Vinegar variables, we define

$$\widetilde{M} = \begin{pmatrix} M & 0 \\ 0 & I_v \end{pmatrix}$$

Preliminaries (3)

- We get

$$(v_1, v_2, \cdots, v_n, x_1, \cdots, x_v) \cdot \widetilde{M} = (V, V^q, \cdots, V^{q^{n-1}}, x_1, \cdots, x_v),$$

Preliminaries (3)

- We get
$$(v_1, v_2, \cdots, v_n, x_1, \cdots, x_v) \cdot \widetilde{M} = (V, V^q, \cdots, V^{q^{n-1}}, x_1, \cdots, x_v),$$
- Let S and T be the matrices representing the linear parts of $\mathcal{S}$ and $\mathcal{T}$. From
$$\mathcal{F} = (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v) F^{*0} (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v)^t,$$
we find
$$\begin{aligned} & \left(\widetilde{M}^{-1} S^{-1} P_0 (S^{-1})^t (\widetilde{M}^{-1})^t, \cdots, \widetilde{M}^{-1} S^{-1} P_{n-a-1} (S^{-1})^t (\widetilde{M}^{-1})^t\right) \\ = \ & \left(F^{*0}, \cdots, F^{*n-1}\right) M^{-1} T \end{aligned}$$

Preliminaries (3)

- We get
$$(v_1, v_2, \cdots, v_n, x_1, \cdots, x_v) \cdot \widetilde{M} = (V, V^q, \cdots, V^{q^{n-1}}, x_1, \cdots, x_v),$$
- Let S and T be the matrices representing the linear parts of $\mathcal{S}$ and $\mathcal{T}$. From
$$\mathcal{F} = (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v) F^{*0} (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v)^t,$$
we find
$$\begin{aligned} & \left(\widetilde{M}^{-1} S^{-1} P_0 (S^{-1})^t (\widetilde{M}^{-1})^t, \cdots, \widetilde{M}^{-1} S^{-1} P_{n-a-1} (S^{-1})^t (\widetilde{M}^{-1})^t\right) \\ = \; & \left(F^{*0}, \cdots, F^{*n-1}\right) M^{-1} T \end{aligned}$$
- Denoting $U = \widetilde{M}^{-1} S^{-1}$ and $W = M^{-1} T$ yields
$$(UP_0 U^t, \cdots, UP_{n-a-1} U^t) = \left(F^{*0}, \cdots, F^{*n-1}\right) W.$$

Preliminaries (3)

- We get
$$(v_1, v_2, \cdots, v_n, x_1, \cdots, x_v) \cdot \widetilde{M} = (V, V^q, \cdots, V^{q^{n-1}}, x_1, \cdots, x_v),$$
- Let S and T be the matrices representing the linear parts of $\mathcal{S}$ and $\mathcal{T}$. From
$$\mathcal{F} = (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v) F^{*0} (X, X^q, \cdots, X^{q^{n-1}}, x_1, \cdots, x_v)^t,$$
we find
$$\begin{aligned} & \left(\widetilde{M}^{-1} S^{-1} P_0 (S^{-1})^t (\widetilde{M}^{-1})^t, \cdots, \widetilde{M}^{-1} S^{-1} P_{n-a-1} (S^{-1})^t (\widetilde{M}^{-1})^t\right) \\ = & \left(F^{*0}, \cdots, F^{*n-1}\right) M^{-1} T \end{aligned}$$
- Denoting $U = \widetilde{M}^{-1} S^{-1}$ and $W = M^{-1} T$ yields
$$\boxed{(U P_0 U^t, \cdots, U P_{n-a-1} U^t) = \left(F^{*0}, \cdots, F^{*n-1}\right) W.}$$

Recovering S

- Let $\mathbf{a}_i$ be the first row of the matrix $F^{\star i}$ $(i = 1, \ldots, n-1)$

Recovering S

- Let $\mathbf{a}_i$ be the first row of the matrix $F^{\star i}$ $(i = 1, \ldots, n-1)$
- We can show

Lemma

The rank of the matrix $Q = W^t \cdot \begin{pmatrix} \mathbf{a}_0 \\ \vdots \\ \mathbf{a}_{n-1} \end{pmatrix}$ *is at most* $d = \lceil \log_q(D) \rceil$.

In particular, we have

$$\begin{pmatrix} \mathbf{a}_0 \\ \mathbf{a}_1 \\ \ldots \\ \mathbf{a}_{n-1} \end{pmatrix} = \begin{pmatrix} A_1 \\ 0 \\ A_2 \end{pmatrix},$$

Recovering S (2)

- From the Lemma we directly follow

Theorem

Let $\mathbf{u} = (u_0, u_1, \cdots, u_{n+v-1})$ *be the first row of* U *and* $\mathbf{b}_i = (u_0, u_1, \ldots, u_{n+v-1})P_i$, $(i = 0, 1, \ldots, n-a)$. *Define* $Z \in \mathcal{M}_{(n-a)\times(n+v)}(\mathbb{F}_{q^n})$ *as the matrix whose row vectors are the* $\mathbf{b}_i$. *Then the rank of* Z *is at most* d.

Recovering S (2)

- From the Lemma we directly follow

Theorem

Let $\mathbf{u} = (u_0, u_1, \cdots, u_{n+v-1})$ be the first row of U and $\mathbf{b}_i = (u_0, u_1, \ldots, u_{n+v-1})P_i$, $(i = 0, 1, \ldots, n-a)$. Define $Z \in \mathcal{M}_{(n-a)\times(n+v)}(\mathbb{F}_{q^n})$ as the matrix whose row vectors are the $\mathbf{b}_i$. Then the rank of Z is at most d.

- Furthermore we get

Lemma

Let A be an $m \times n$ matrix over $\mathbb{F}_q$ and $B = [b_{ij}] = M^{-1}A$. Then we have

$$b_{ij} = b_{i-1,j}^q, \quad \text{for all } i,j, \text{ with } 0 \leq i < n, 0 \leq j < m.$$

i.e. the matrix B is determined by its first row.

Recovering S - Summary

- Since we have $U = \widetilde{M}^{-1} S^{-1}$, it's enough to find U.

Recovering S - Summary

- Since we have $U = \widetilde{M}^{-1} S^{-1}$, it's enough to find U.
- We only have to find the first row of U to get the first n rows of U.

Recovering S - Summary

- Since we have $U = \widetilde{M}^{-1} S^{-1}$, it's enough to find U.
- We only have to find the first row of U to get the first n rows of U.
- Denote the first row of U by $u_0, \ldots, u_{n+v-1}$

Recovering S - Summary

- Since we have $U = \widetilde{M}^{-1} S^{-1}$, it's enough to find U.
- We only have to find the first row of U to get the first n rows of U.
- Denote the first row of U by $u_0, \ldots, u_{n+v-1}$
- Since we have to find only one of many equivalent keys, we can assume that $u_0 = 1$ holds.

Recovering S - Summary

- Since we have $U = \widetilde{M}^{-1} S^{-1}$, it's enough to find U.
- We only have to find the first row of U to get the first n rows of U.
- Denote the first row of U by $u_0, \ldots, u_{n+v-1}$
- Since we have to find only one of many equivalent keys, we can assume that $u_0 = 1$ holds.
- Since the rank of Z is $\leq d$, we can find $u_1, \ldots, u_{n+v-1}$ by solving a MinRank problem over the base field $\mathbb{F}_q$ with target rank d

Recovering S - Summary

- Since we have $U = \widetilde{M}^{-1} S^{-1}$, it's enough to find U.
- We only have to find the first row of U to get the first n rows of U.
- Denote the first row of U by $u_0, \ldots, u_{n+v-1}$
- Since we have to find only one of many equivalent keys, we can assume that $u_0 = 1$ holds.
- Since the rank of Z is $\leq d$, we can find $u_1, \ldots, u_{n+v-1}$ by solving a MinRank problem over the base field $\mathbb{F}_q$ with target rank d
- We can find the first n of U using the Frobenius isomorphism

Recovering S - Summary

- Since we have $U = \widetilde{M}^{-1}S^{-1}$, it's enough to find U.
- We only have to find the first row of U to get the first n rows of U.
- Denote the first row of U by $u_0, \ldots, u_{n+v-1}$
- Since we have to find only one of many equivalent keys, we can assume that $u_0 = 1$ holds.
- Since the rank of Z is $\leq d$, we can find $u_1, \ldots, u_{n+v-1}$ by solving a MinRank problem over the base field $\mathbb{F}_q$ with target rank d
- We can find the first n of U using the Frobenius isomorphism
- The remaining rows of U can be chosen at random such that U is invertible

Recovering S - The Algorithm

Input: HFEv- parameters (q, n, v, D, a), matrices $(P_0, \cdots, P_{n-a-1})$, matrix $\widetilde{M}$
Output: Equivalent linear transformation S.

1: Set $\mathbf{b}_i = (1, u_1, \cdots, u_{n+v-1})P_i$, $0 \leq i < n-a$, where $(u_1, \cdots, u_{n+v-1})$ are unknowns.
2: Construct a matrix Z whose row vectors are $\mathbf{b}_i$, $0 \leq i < n-a$.
3: Solve a MinRank problem for Z to find the unknowns $u_1, \cdots u_{n+v-1}$.
4: Set $U = \begin{pmatrix} 1 & u_1 & \cdots & u_{n+v-1} \\ 1 & u_1^q & \cdots & u_{n+v-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ 1 & u_1^{q^{n-1}} & \cdots & u_{n+v-1}^{q^{n-1}} \\ r_{00} & r_{01} & \cdots & r_{0,n+v-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{v-1,0} & r_{v-1,1} & \cdots & r_{v-1,n+v-1} \end{pmatrix}$,
5: Compute $S' = (\widetilde{M}U)^{-1}$.
6: **return** S'.

Recovering $\mathcal{F}$ and $\mathcal{T}$

- We can show

Lemma

As soon as U is known, we can recover F^{*0} by solving a determined linear system with $n-a-1$ variables, $(d+a)\cdot(n+v)$ additional linear equations in at most $d+v$ variables, and $\binom{v+1}{2}$ univariate polynomial equations of degree q^d.

Recovering $\mathcal{F}$ and $\mathcal{T}$

- We can show

Lemma

As soon as U is known, we can recover F^{*0} by solving a determined linear system with $n-a-1$ variables, $(d+a)\cdot(n+v)$ additional linear equations in at most $d+v$ variables, and $\binom{v+1}{2}$ univariate polynomial equations of degree q^d.

- We can use $F^{\star 0}$ to compute all $F^{\star i}$ $(i = 1, \ldots, n-1)$

Recovering $\mathcal{F}$ and $\mathcal{T}$

- We can show

Lemma

As soon as U is known, we can recover F^{*0} by solving a determined linear system with $n-a-1$ variables, $(d+a)\cdot(n+v)$ additional linear equations in at most $d+v$ variables, and $\binom{v+1}{2}$ univariate polynomial equations of degree q^d.

- We can use $F^{\star 0}$ to compute all $F^{\star i}$ $(i = 1, \ldots, n-1)$
- Furthermore we get

Lemma

As soon as the matrices $F^{*j}(0 \leq j < n)$ are known, T can be recovered by solving a system of $n-a$ linear equations in n variables.

Complexity of the Attack

- Most costly Step: Solution of the MinRank problem (target rank d)

Complexity of the Attack

- Most costly Step: Solution of the MinRank problem (target rank d)
- Two Possibilities
- Minors Modelling: Degree of Regularity in F_4: $d+1$

$$\mathcal{O}\left(\binom{n+v+d+1}{d+1}^{\omega}\right),$$

Complexity of the Attack

- Most costly Step: Solution of the MinRank problem (target rank d)
- Two Possibilities
- Minors Modelling: Degree of Regularity in F_4: $d+1$

$$\mathcal{O}\left(\binom{n+v+d+1}{d+1}^{\omega}\right),$$

- Support Minors Modelling
  we don't have a unique solution of the MinRank Problem $\Rightarrow$ We solve the system by F_4
  Experiments $\Rightarrow$ degree of regularity 3

$$\mathcal{O}\left((n+v)^2\binom{2d+2}{d}+(n+v)\binom{2d+2}{d}^2\right)^{\omega}$$

Application to GeMSS

NIST security category		parameters (q, n, v, D, a)	required security level	our attack using minors modeling	our attack using support minors modeling
I	GeMSS128	(2,174,12,513,12)	143	139	118
	BlueGeMSS128	(2,175,14,129,13)		119	99
	RedGeMSS128	(2,177,15,17,15)		86	72
II	GeMSS192	(2,265,20,513,22)	207	154	120
	BlueGeMSS192	(2,265,23,129,22)		132	101
	RedGeMSS192	(2,266,25,17,23)		95	75
III	GeMSS256	(2,354,33,513,30)	272	166	121
	BlueGeMSS256	(2,358,32,129,34)		141	103
	RedGeMSS256	(2,358,35,17,34)		101	76

Application to GeMSS (2)

1. The proposed parameters for GeMMS don't reach the required security levels.

Application to GeMSS (2)

1. The proposed parameters for GeMMS don't reach the required security levels.
2. Speeding up the signature generation process of GeMSS by decreasing D while increasing a and v is not possible.
   $\Rightarrow$ Modifications as in BlueGeMSS and RedGeMSS are not possible

Application to GeMSS (2)

1. The proposed parameters for GeMMS don't reach the required security levels.
2. Speeding up the signature generation process of GeMSS by decreasing D while increasing a and v is not possible.
   $\Rightarrow$ Modifications as in BlueGeMSS and RedGeMSS are not possible
3. For high levels of security, we need very high values of D
   e.g. NIST security level III: $d \geq 20$ or $D \geq 2^{19} + 1 = 524.289$
   $\Rightarrow$ Drastical slow down of the signature generation process

Application to GeMSS (2)

1. The proposed parameters for GeMMS don't reach the required security levels.
2. Speeding up the signature generation process of GeMSS by decreasing D while increasing a and v is not possible.
   $\Rightarrow$ Modifications as in BlueGeMSS and RedGeMSS are not possible
3. For high levels of security, we need very high values of D
   e.g. NIST security level III: $d \geq 20$ or $D \geq 2^{19} + 1 = 524.289$
   $\Rightarrow$ Drastical slow down of the signature generation process

The Techniques used in GeMSS don't suffice to create a HFE based signature scheme which is both efficient and reaches high levels of security

Conclusion

We proposed a new MinRank type attack against HFE signature variants. The complexity is

$$\mathcal{O}\left(\binom{n+d+v+1}{d+1}^{\omega}\right)$$

- exponential in d
- polynomial in v
- independent of a

Conclusion

We proposed a new MinRank type attack against HFE signature variants. The complexity is

$$\mathcal{O}\left(\binom{n+d+v+1}{d+1}^{\omega}\right)$$

- exponential in d
- polynomial in v
- independent of a

Consequences

- We can't speed up HFEv$^-$ by decreasing d while increasing a and v
- For high levels of security we need a large d

Conclusion

We proposed a new MinRank type attack against HFE signature variants. The complexity is

$$\mathcal{O}\left(\binom{n+d+v+1}{d+1}^{\omega}\right)$$

- exponential in d
- polynomial in v
- independent of a

Consequences

- We can't speed up HFEv$^-$ by decreasing d while increasing a and v
- For high levels of security we need a large d

$\Rightarrow$ Can we build an HFE based signature scheme which is both efficient and offers a high level of security?

Thank you for your Attention

Find our paper at
https://eprint.iacr.org/2020/1424.pdf