Improved Cryptanalysis of HFEv- via Projection

Jintai Ding, Ray Perlner, Albrecht Petzoldt, Daniel Smith-Tone

PQ Crypto 2018

Fort Lauderdale, Florida
04/10/2018

Outline

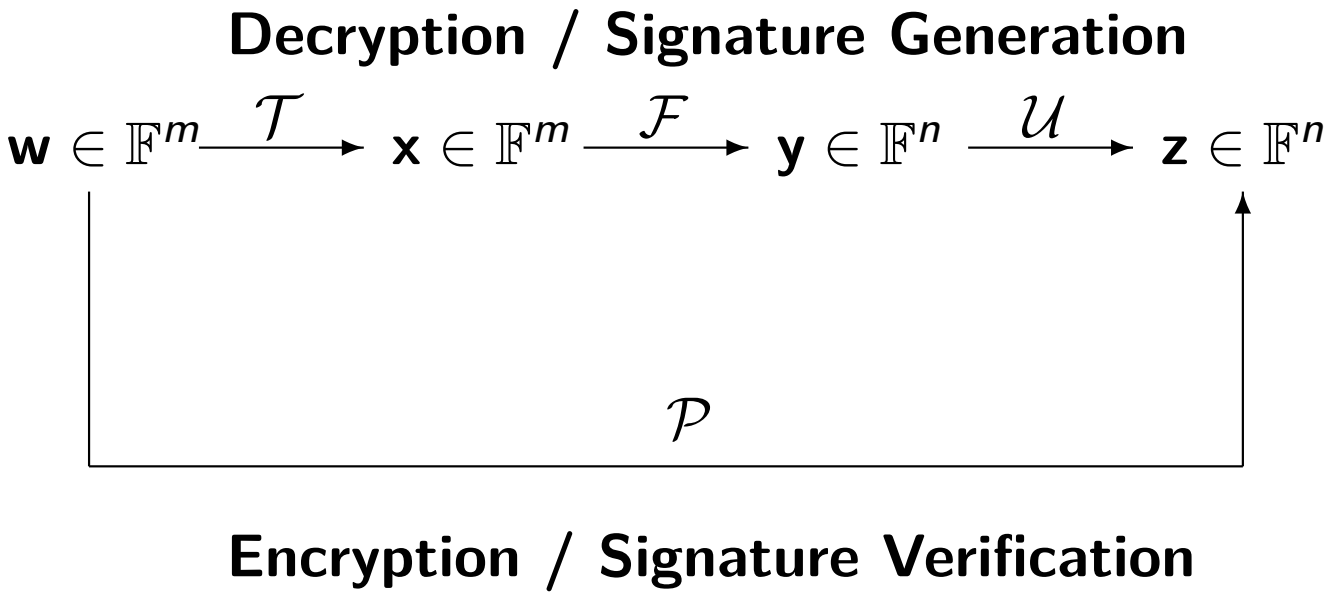
Multivariate Cryptography

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

The security of multivariate schemes is based on the

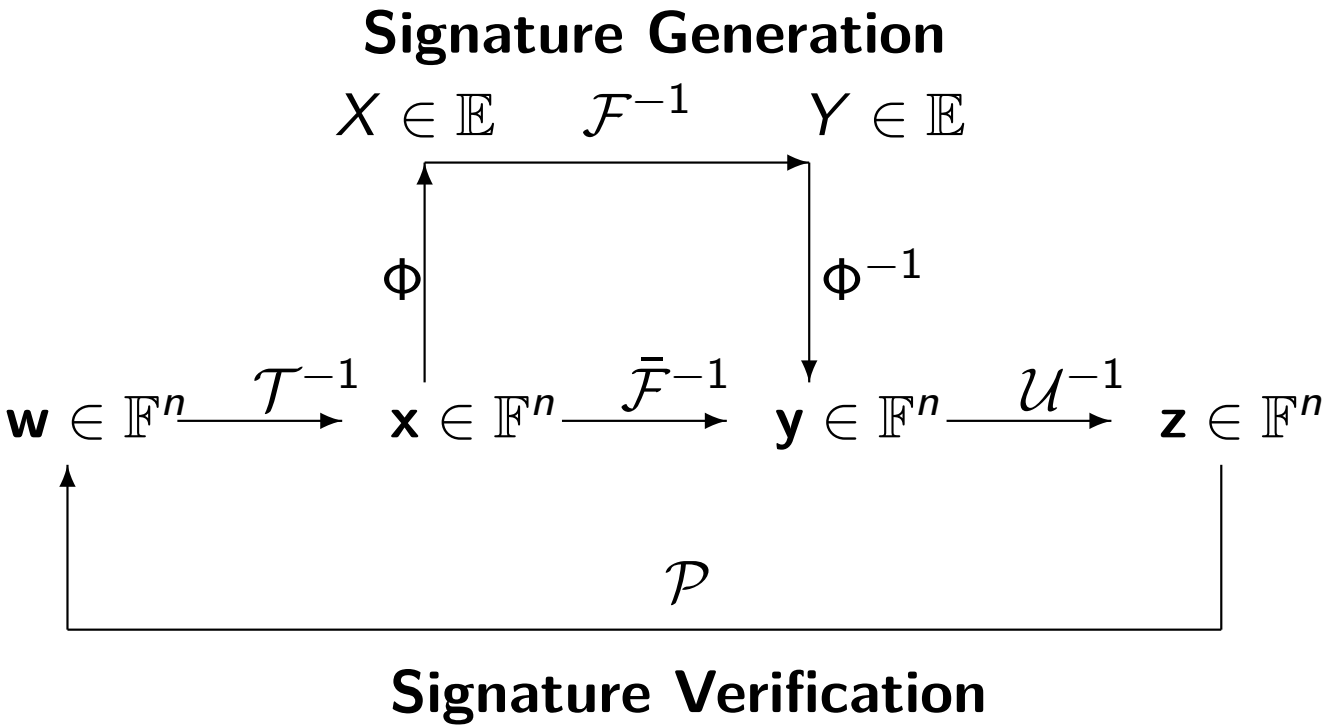
Problem MQ: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}),\ldots,p^{(m)}(\mathbf{x})$, find a vector $\bar{\mathbf{x}} = (\bar{x}_1,\ldots,\bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \ldots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

Construction



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

Big Field Signature Schemes



HFEv$^-$ - Key Generation

- BigField + Minus Equations + Vinegar Variation
- central map $\mathcal{F} : \mathbb{F}^v \times \mathbb{E} \to \mathbb{E}$,

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

  $\Rightarrow \bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi$ quadratic
- linear maps $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^{n-a}$ and $\mathcal{U} : \mathbb{F}^{n+v} \to \mathbb{F}^{n+v}$ of maximal rank
- *public key*: $\mathcal{P} = \mathcal{T} \circ \bar{\mathcal{F}} \circ \mathcal{U} : \mathbb{F}^{n+v} \to \mathbb{F}^{n-a}$
- *private key*: $\mathcal{T}$, $\mathcal{F}$, $\mathcal{U}$

Signature Generation

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

1. Compute $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w}) \in \mathbb{F}^n$ 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 $\mathbf{z} = \mathcal{U}^{-1}(\mathbf{y}||v_1||\ldots||v_v)$

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 $\mathbf{z} \Leftrightarrow \mathbf{w}' = \mathbf{w}$.

Direct Attack

$$\text{Complexity}_{\text{direct}} = 3 \cdot \binom{n-a}{d_{\text{reg}}}^2 \cdot \binom{n-a}{2}$$

Experiments: HFEv- systems can be solved faster than random systems

Reason: low degree of regularity

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

with $r = \lfloor \log_q(D-1) \rfloor + 1$.
Experiments: $d_{\text{reg}} \approx \frac{r+a+v+7}{3}$ for HFEv- systems over GF(2).

Q-Rank

Definition

Let $\mathbb{E}$ be a degree n extension of the field $\mathbb{F}_q$. The *Q-rank* of a quadratic map $\mathcal{F}(\overline{x})$ on $\mathbb{F}_q^n$ is the rank of the quadratic form $\phi \circ \mathcal{F} \circ \phi^{-1}$ in $\mathbb{E}[X_0, \ldots, X_{n-1}]$ via the identification $X_i = X^{q^i}$.

$\mathcal{F}$: n quadratic polynomials $f^{(1)}, \ldots f^{(n)}$ in $\mathbb{F}_q[x_o, \ldots, x_{n-1}]$
Interpolation $\Rightarrow$ $\mathcal{F}^\star : \sum_{i=0}^{n-1} \sum_{j=i}^{n-1} \alpha_{ji} X^{q^i} \cdot X^{q^j}$ in $\mathbb{E}[X]$

$\overset{x_i = X^{q^i}}{\rightarrow}$ $\hat{\mathcal{F}}^\star : \sum_{i=0}^{n-1} \sum_{j=i}^{n-1} \alpha_{ij} X_i X_j$ in $\mathbb{E}[X_0, \ldots, X_{n-1}]$
$\Rightarrow \hat{\mathcal{F}}^\star : (X_0, \ldots, X_{n-1}) \cdot M \cdot (X_0, \ldots X_{n-1})^T$
Q-rank$(\mathcal{F}) =$ Rank(M)

Q-Rank is invariant under invertible affine transformations $\mathcal{F} \rightarrow \mathcal{F} \circ \mathcal{T}$, but not under isomorphisms $\mathcal{F} \rightarrow \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$

Q-Rank (2)

Definition

Let $\mathbb{E}$ be a degree $d < n$ extension field of $\mathbb{F}_q$. The *min-Q-rank* of a quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ over $\mathbb{E}$ is

$$\text{min-Q-rank}(\mathcal{F}) = \min_{\mathcal{S}} \max_{\mathcal{T}} \{\text{Q-rank}\,(\mathcal{S} \circ \mathcal{F} \circ \mathcal{T})\},$$

where $\mathcal{S} : \mathbb{F}_q^d \to \mathbb{F}_q^m$ and $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^d$ are nonzero linear transformations.

The min-Q-Rank of a multivariate quadratic system is invariant under isomorphisms of polynomials.

The KS-attack on HFE

- Idea: Use the low min-Q-rank of the central map $\mathcal{F}$ to recover an equivalent private key
- Lift public map $\mathcal{P}$ to the extension field $\mathbb{E}$ (polynomial interpolation)
- Solve a MinRank Problem to find linear map N with $N \circ \mathcal{P}$ of low rank
- Later Improvement (Minors Modelling): N can be found by computing a Gröbner basis over $\mathbb{F}$ (and computing the variety over $\mathbb{E}$)

$$\text{Complexity}_{\text{MinRank}} = O\left(\binom{n+r+1}{r}^{\omega}\right)$$

with $2 < \omega \leq 3$.

The algebra $\mathbb{A}$

- $\mathbb{E}$: degree n extension field of $\mathbb{F}$, θ: primitive element of $\mathbb{E}$
- $\phi : \mathbb{F}^n \to \mathbb{E}, \phi(x_0, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} x_i \alpha^i$ isomorphism
- $\Phi : \mathbb{E} \to \mathbb{A}, \Phi(a) = (a, a^q, \ldots, a^{q^{n-1}}) \in \mathbb{A} \subset \mathbb{E}^n$

$\Rightarrow$ We can pass between elements $(x_0, \ldots, x_{n-1}) \in \mathbb{F}^n$ and $(X, X^q, \ldots, X^{q^{n-1}}) \in \mathbb{A}$ by right multiplication with $\mathbf{M}_n$ and $\mathbf{M}_n^{-1}$, where

$$\mathbf{M}_n = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \theta & \theta^q & \ldots & \theta^{q^{n-1}} \\ \theta^2 & \theta^{2q} & \ldots & \theta^{2q^{n-1}} \\ \vdots & & & \vdots \\ \theta^{n-1} & \theta^{(n-1)q} & \ldots & \theta^{(n-1)q^{n-1}} \end{pmatrix}$$

The algebra $\mathbb{A}$ (cont.)

To cover the vinegar variables $v_1, \ldots, v_v$, we define

$$\widetilde{\mathbf{M}}_n = \begin{pmatrix} \mathbf{M}_n & 0_{n \times v} \\ 0_{v \times n} & I_v \end{pmatrix}$$

lifting a vector $(x_0, \ldots, x_{n-1}, v_1, \ldots, v_v) \in \mathbb{F}^n$ to an element of $\mathbb{A} \times \mathbb{F}^v$.

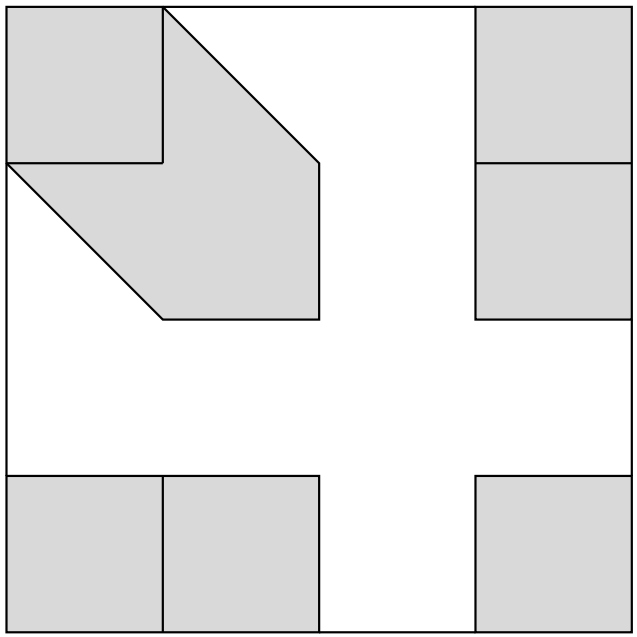
MinRank then Projection

We find

$$(\mathbf{P}_1, \ldots, \mathbf{P}_n)\mathbf{T}^{-1}\mathbf{M}_n = (\mathbf{U}\widetilde{\mathbf{M}_n}\mathbf{F}^{\star 0}\widetilde{\mathbf{M}_n}^T\mathbf{U}^T, \ldots, \mathbf{U}\widetilde{\mathbf{M}_n}\mathbf{F}^{\star(n-1)}\widetilde{\mathbf{M}_n}^T\mathbf{U}^T),$$

where $\mathbf{U}$, $\mathbf{T}$ and $\mathbf{P}_i$ are the matrix representations of the affine transformations $\mathcal{U}$ and $\mathcal{T}$ and the public polynomials $\mathcal{P}_i$, and $\mathbf{F}^{\star i}$ is the i-th Frobenius power of $\mathcal{F}$ over $\mathbb{A} \times \mathbb{F}^v$.

We find that $\mathbf{F}^{\star 0}$ has the form



$$\mathrm{Rank}(\mathbf{F}^{\star 0}) = r + a + v$$

MinRank then Projection (2)

1. Apply a MinRank attack on the matrices $\mathbf{P}_i$ (with target rank $r + a + v$)
   $\Rightarrow$ equivalent output transformation $\mathcal{T}'$
   $\Rightarrow$ matrix $\mathbf{L}$ representing the low $\mathcal{Q}$-rank quadratic form
   $\mathbf{L} = \mathbf{U}'\widetilde{\mathbf{M}_n}\mathbf{F}^{\star 0}\widetilde{\mathbf{M}_n}^T\mathbf{U}'^T$.
2. Find the vinegar subspace of $\mathcal{L}$.
   - project $\mathcal{L}$ to the orthogonal complement of a codimension 1 subspace of $\ker(\mathbf{L})$. Denote the result by $\hat{\mathcal{L}}$.
   - Apply a further codimension one projection π to $\hat{\mathcal{L}}$. If there is a nontrivial intersection between $\ker(\pi)$ and the vinegar subspace, the rank of $\hat{\mathcal{L}}$ will drop.

$$Comp_{MP} = \mathcal{O}\left(\binom{n+r+v}{r+a+v}^2 \cdot \binom{n-a}{2} + (r+a+v+1)^3 \cdot q^{r+a+1}\right).$$

Project then MinRank

1. Apply a projection π, projecting the plaintext space to a codimension k subspace
2. Apply the MinRank attack

If there is a nontrivial intersection between $\ker(\pi)$ and the vinegar subspace, we can find a quadratic form of degree less then $r + a + v$.

$$Comp_{PM} = \mathcal{O}\left(q^{c(r+a+\sqrt{n-a})-\binom{c+1}{2}} \binom{n+r+v-c}{r+a+v-c}^2 \cdot \binom{n-a}{2} \right).$$

The Distinguisher

Observation 1:

- Two HFEv- public keys $\mathcal{P}_1$ and $\mathcal{P}_2$ with same values for n, D and a but different values v_1 and v_2
- Fix variables to get determined systems and solve the systems with F_4

$\Rightarrow$ The step degrees of the F_4 algorithm will be different
$\Rightarrow$ This also holds when guessing (not too many) additional variables (hybrid approach)

The Distinguisher (2)

Observation 2:

- HFEv-(n, D, a, v) public key $\mathcal{P}$
- Define $\mathcal{V} = \mathrm{span}(\mathcal{T}_{n+1}, \ldots, \mathcal{T}_{n+v})$
- Append $\ell \in V$ to the system $\mathcal{P}$ and apply F_4

$\Rightarrow$ The so obtained system $\mathcal{P}'$ behaves exactly like an

$$\mathrm{HFEv}-(n-1, D, a, \mathbf{v}-\mathbf{1})$$

public key.

The Distinguisher (3)

- Consider an HFEv-(n, D, a, v) public key $\mathcal{P}$
- Add the field equations $\{x_i^2 - x_i = 0\}$ to $\mathcal{P}$
- Add randomly chosen linear equations $\ell_1, \ldots, \ell_k$ to $\mathcal{P}$
- Solve the system with F_4

$\Rightarrow$ By looking at the F_4 step degrees, we can distinguish the two cases

1) $\mathrm{span}(\ell_1, \ldots, \ell_k) \cap \mathcal{V} = \emptyset$ and
2) $\mathrm{span}(\ell_1, \ldots, \ell_k) \cap \mathcal{V} \neq \emptyset$.

The Attack

Having found $\ell_1, \ldots, \ell_k$ such that $\mathrm{span}(\ell_1, \ldots, \ell_k) \cap \mathcal{V} = \{\tilde{\ell}\}$, we can recover the private HFEv- key as follows

1. Recover the exact form of $\tilde{\ell} = \sum_{i=1}^{k} \lambda_i \cdot \ell_i$
   - Remove ℓ_1 from the system. If the distinguisher still works, the coefficient λ_1 is zero. Otherwise, $\lambda_1 = 1$.
   - Continue this step to find all the coefficients λ_i
2. Add $\tilde{\ell}$ to the HFEv- system and run the distinguisher again to find another linear equation $\hat{\ell} \in \mathcal{V}$. After having recovered v of these linear equations the system will behave like an HFE- system.
3. Apply any attack against HFE- (e.g [VS, PQCrypto2017]) to complete the attack.

Complexity of the Distinguisher

Complexity of the Distinguisher (finding $\tilde{\ell} \in \mathcal{V}$) depends on

- number of distinguisher runs

$$\Pr(\ell \in \mathcal{V}) = 2^{-n}$$

$$\Pr(\mathrm{span}(\ell_1, \ldots, \ell_{\bar{k}}) \cap \mathcal{V} \neq \emptyset) = 1 - (1 - 2^{-n})^{2^{\bar{k}}} \approx 2^{\bar{k}-n}$$

- cost of a single run ($=$ 1 run of F_4)

$$Comp_{F_4} = \mathcal{O}\left(\binom{n+v-\bar{k}}{d^{\star}_{\mathrm{reg}}}^2 \cdot \binom{n+v-\bar{k}}{2}\right)$$

Complexity of the Distinguisher

$$Comp_{\text{Distinguisher; classical}} = \mathcal{O}\left(2^{n-\bar{k}} \cdot \binom{n+v-\bar{k}}{d_{\text{reg}}^{\star}}^2 \cdot \binom{n+v-\bar{k}}{2}\right)$$

$$Comp_{\text{Distinguisher; quantum}} = \mathcal{O}\left(2^{(n-\bar{k})/2} \cdot \binom{n+v-\bar{k}}{d_{\text{reg}}^{\star}}^2 \cdot \binom{n+v-\bar{k}}{2}\right).$$

The cost of the remaining steps (finding the exact form of $\tilde{\ell}$ and removing the other Vinegar variables from the system, breaking the remaining HFE- system) is much smaller.

$\Rightarrow$ A strategy to estimate $\bar{k}$ and $d_{\text{reg}}^{\star}$ for concrete HFEv- systems can be found in our paper.

Conclusion

We presented three new attacks against HFEv- using the idea of projection

- MinRank then Projection
- Projection then MinRank
- Distinguishing based attack
  - Better performance than existing attacks against some HFEv- systems (see example in the paper)
  - Less memory consumption than all known attacks (for all parameter sets)

$\Rightarrow$ New insights in the security of HFEv-

$\Rightarrow$ Restrictions for the parameter choice of HFEv- based schemes

The End

Thank you for your attention

Questions?