Improved Cryptanalysis of HFERP

PKC 2024

Max Cartor, Ryann Cartor*, Hiroki Furue, Daniel Smith-Tone

April 15, 2024

In this talk, we provide two attacks on the multivariate cryptosystem HFERP

Hidden Field Equations (HFE)

Hidden Field Equations (HFE)

$\mathcal{P} = T \circ F \circ S$ where $F = \phi^{-1} \circ f \circ \phi$ and

$$f(X) = \sum_{i \leq j}^{q^i + q^j < D} \alpha_{ij} X^{q^i + q^j} + \sum_{q^i < D} \beta_i X^{q^i} + \gamma$$

$$\begin{tikzcd}
 & \mathbb{F}_{q^n} \arrow[r, "f"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[u, "\phi"] & \mathbb{F}_q^n \arrow[r, "T"] & \mathbb{F}_q^n
\end{tikzcd}$$

Jaques Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms." Eurocrypt (1996)

Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix}$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} \begin{matrix} \leftarrow \text{vinegar variables} \\ \\ \leftarrow \text{oil variables} \end{matrix}$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} \begin{matrix} \leftarrow \text{vinegar variables} \\ \\ \leftarrow \text{oil variables} \end{matrix}$$

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)}$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} \begin{array}{l} \leftarrow \text{vinegar variables} \\ \\ \\ \\ \leftarrow \text{oil variables} \end{array}$$

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)}, \quad P = U \circ F \circ T$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} \begin{array}{l} \leftarrow \text{vinegar variables} \\ \\ \\ \leftarrow \text{oil variables} \end{array}$$

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)}, \quad P = U \circ F \circ T, \quad F = (f^{(1)}, \ldots, f^{(v+1)})$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} \begin{matrix} \leftarrow \text{vinegar variables} \\ \\ \leftarrow \text{oil variables} \end{matrix}$$

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)}, \quad P = U \circ F \circ T, \quad F = (f^{(1)}, \ldots, f^{(v+1)})$$

$$f^{(k)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j + \sum_{i=1}^{n} \gamma_{ik} x_i$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{array}{cl} \left(\begin{array}{c} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{array} \right) & \begin{array}{l} \leftarrow \text{vinegar variables} \\ \\ \\ \\ \leftarrow \text{oil variables} \end{array} \end{array}$$

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)}, \quad P = U \circ F \circ T, \quad F = (f^{(1)}, \dots, f^{(v+1)})$$

$$f^{(k)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j + \sum_{i=1}^{n} \gamma_{ik} x_i$$

Patarin, "The Oil and Vinegar Signature Scheme." (1997)
Kipnis, Shamir, "Cryptanalysis of the Oil & Vinegar Signature Scheme." (1998)

Rainbow

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)(n-v_\ell)}, \quad P = U \circ F \circ T, \quad F = \left(F^{(1)}, F^{(2)}, \ldots, F^{(v+1)}\right)$$

$$f_\ell^{(k)}(\mathbf{x}) = \sum_{i=1}^{v_\ell} \sum_{j=1}^{v_\ell} \alpha_{ij\ell} x_i x_j + \sum_{i=1}^{v_\ell} \sum_{j=v_\ell+1}^{n} \beta_{ij\ell} x_i x_j + \sum_{i=1}^{n} \gamma_{i\ell} x_i + \delta_\ell$$

$$0 < v_1 < v_2 < \ldots < v_L < n$$

Ding, Schmidt, "Rainbow, a New Multivariable Polynomial Signature Scheme." Applied Cryptography and Network Security (2005)

Plus Modifier

$$P = \begin{pmatrix} p_1 \\ \vdots \\ p_m \end{pmatrix}$$

Plus Modifier

$$P = \begin{pmatrix} p_1 \\ \vdots \\ p_m \end{pmatrix} \longrightarrow P^+ = \begin{pmatrix} p_1 \\ \vdots \\ p_m \\ p_{m+1} \\ \vdots \\ p_{m+a} \end{pmatrix}$$

HFERP

- Multivariate Encryption Scheme composed of:
  - An instance of HFE
  - A single layer Rainbow map
  - A plus modifier

Ikematsu, Perlner, Smith-Tone, Takagi, Vates, "HFERP - A New Multivariate

Structure of HFERP

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

$$\mathbb{F}_q^n \xrightarrow{U} \mathbb{F}_q^n$$

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

$$\begin{tikzcd}
& & \mathbb{F}_{q^d} \arrow[r, "\mathcal{F}_{HFE}"] & \mathbb{F}_{q^d} \arrow[d, "\phi^{-1}"] \\
& & \mathbb{F}_q^d \arrow[u, "\phi"] & \mathbb{F}_q^d \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[ur, "\pi_d"] & &
\end{tikzcd}$$

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

$$\begin{tikzcd}
 & & \mathbb{F}_{q^d} \arrow[r, "\mathcal{F}_{HFE}"] & \mathbb{F}_{q^d} \arrow[d, "\phi^{-1}"] \\
 & & \mathbb{F}_q^d \arrow[u, "\phi"] & \mathbb{F}_q^d \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[ur, "\pi_d"] \arrow[rr, "\mathcal{F}_R"] & & \mathbb{F}_q^o
\end{tikzcd}$$

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

$$\begin{tikzcd}
 & & \mathbb{F}_{q^d} \arrow[r, "\mathcal{F}_{HFE}"] & \mathbb{F}_{q^d} \arrow[d, "\phi^{-1}"] \\
 & & \mathbb{F}_q^d \arrow[u, "\phi"] & \mathbb{F}_q^d \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[ur, "\pi_d"] \arrow[rr, "\mathcal{F}_R"] \arrow[drr, "\mathcal{F}_P"'] & & \mathbb{F}_q^o \\
 & & & \mathbb{F}_q^s
\end{tikzcd}$$

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

$$\begin{tikzcd}
& & \mathbb{F}_{q^d} \arrow[r, "\mathcal{F}_{HFE}"] & \mathbb{F}_{q^d} \arrow[d, "\phi^{-1}"] \\
& & \mathbb{F}_q^d \arrow[u, "\phi"] & \mathbb{F}_q^d \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[ur, "\pi_d"] \arrow[rr, "\mathcal{F}_R"] \arrow[rrd, "\mathcal{F}_P"'] & & \mathbb{F}_q^o \\
& & & \mathbb{F}_q^s
\end{tikzcd}$$

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

$$\begin{tikzcd}
& & \mathbb{F}_{q^d} \arrow[r, "\mathcal{F}_{HFE}"] & \mathbb{F}_{q^d} \arrow[d, "\phi^{-1}"] & \\
& & \mathbb{F}_q^d \arrow[u, "\phi"] & \mathbb{F}_q^d & \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[ur, "\pi_d"] \arrow[rr, "\mathcal{F}_R"] \arrow[drr, "\mathcal{F}_P"'] & & \mathbb{F}_q^o \arrow[r, "T"] & \mathbb{F}_q^m \\
& & & \mathbb{F}_q^s &
\end{tikzcd}$$

Structure of HFERP

$$n = o + d$$
$$m = o + d + s + r$$

$$\begin{tikzcd}
 & & \mathbb{F}_{q^d} \arrow[r, "\mathcal{F}_{HFE}"] & \mathbb{F}_{q^d} \arrow[d, "\phi^{-1}"] & \\
 & & \mathbb{F}_q^d \arrow[u, "\phi"] & \mathbb{F}_q^d & \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[ur, "\pi_d"] \arrow[rr, "\mathcal{F}_R"] \arrow[drr, "\mathcal{F}_P"'] & & \mathbb{F}_q^o \arrow[r, "T"] & \mathbb{F}_q^m \\
 & & & \mathbb{F}_q^s &
\end{tikzcd}$$

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^m \quad P = T \circ (\mathcal{F}_{HFE} || \mathcal{F}_R || \mathcal{F}_P) \circ U$$

MinRank Attacks

MinRank Problem: Given $A_1, \ldots, A_k \in \mathbb{F}_q^{M \times N}$ and positive integer R, find $y_1, \ldots, y_k \in \mathbb{F}_q$ such that

$$\text{rank}\left(\sum_{i=1}^{k} y_i A_i\right) \leq R.$$

MinRank Attacks

MinRank Problem: Given $A_1, \ldots, A_k \in \mathbb{F}_q^{M \times N}$ and positive integer R, find $y_1, \ldots, y_k \in \mathbb{F}_q$ such that

$$\text{rank}\left(\sum_{i=1}^{k} y_i A_i\right) \leq R.$$

A Few MinRank Algorithms:

- Kipnis, Shamir, "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization." Crypto, (1999)
- Faugére, Levy-dit-Vehel, Perret, "Cryptanalysis of Minrank." Crypto (2008)
- Bardet, Bros, Cabarcas, Gaborit, Perlner, Smith-Tone, Tillich, Verbel, "Improvements of Algebraic Attacks for Solving the Rank Decoding and Minrank Problems." Asiacrypt (2020)

HFE Central Maps

HFE Central Maps

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_i = (\phi^{-1} \circ \mathcal{F}_{HFE} \circ \phi \circ \pi_d)_i$

HFE Central Maps

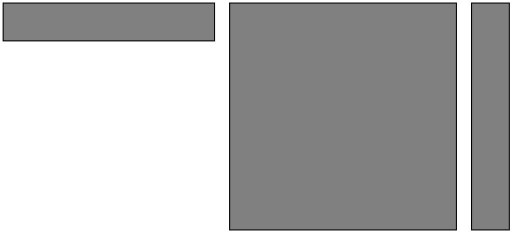
Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_i = (\phi^{-1} \circ \mathcal{F}_{HFE} \circ \phi \circ \pi_d)_i$

Consider matrices $\mathbf{F}_i$ such that $f_i(x) = \mathbf{x}^\top \mathbf{F_i} \mathbf{x}$.

HFE Central Maps

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_i = (\phi^{-1} \circ \mathcal{F}_{HFE} \circ \phi \circ \pi_d)_i$

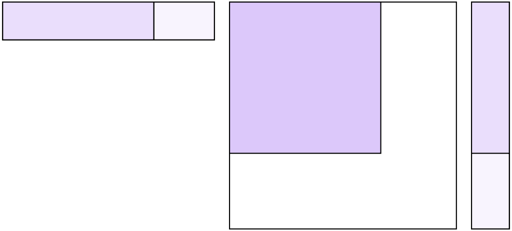
Consider matrices $\mathbf{F}_i$ such that $f_i(x) = \mathbf{x}^\top \mathbf{F_i} \mathbf{x}$.



HFE Central Maps

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_i = (\phi^{-1} \circ \mathcal{F}_{HFE} \circ \phi \circ \pi_d)_i$

Consider matrices $\mathbf{F}_i$ such that $f_i(x) = \mathbf{x}^\top \mathbf{F_i} \mathbf{x}$.



UOV Central Maps

UOV Central Maps

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j$.

UOV Central Maps

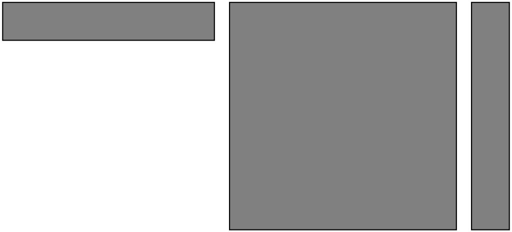
Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j$.

Consider matrices $\mathbf{F}_k$ such that $f_k(x) = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$.

UOV Central Maps

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j$.

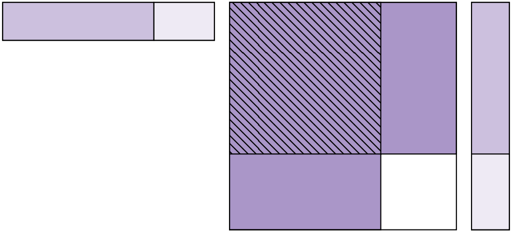
Consider matrices $\mathbf{F}_k$ such that $f_k(x) = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$.



UOV Central Maps

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j$.

Consider matrices $\mathbf{F}_k$ such that $f_k(x) = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$.



Plus Polynomials

Plus Polynomials

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{n} \sum_{j=i}^{n} \alpha_{ijk} x_i x_j$.

Plus Polynomials

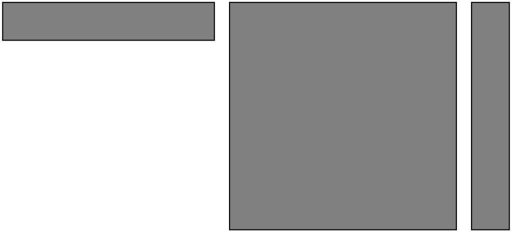
Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \displaystyle\sum_{i=1}^{n} \sum_{j=i}^{n} \alpha_{ijk} x_i x_j$.

Consider matrices $\mathbf{F}_k$ such that $f_k(x) = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$.

Plus Polynomials

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{n} \sum_{j=i}^{n} \alpha_{ijk} x_i x_j$.

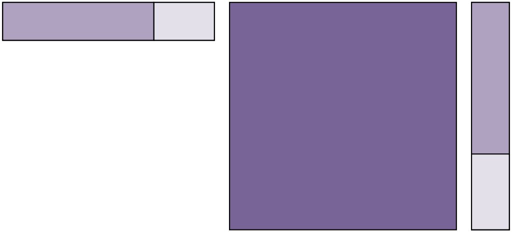
Consider matrices $\mathbf{F}_k$ such that $f_k(x) = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$.



Plus Polynomials

Let $\mathbf{x} \in \mathbb{F}_q^n$, $f_k = \sum_{i=1}^{n} \sum_{j=i}^{n} \alpha_{ijk} x_i x_j$.

Consider matrices $\mathbf{F}_k$ such that $f_k(x) = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$.



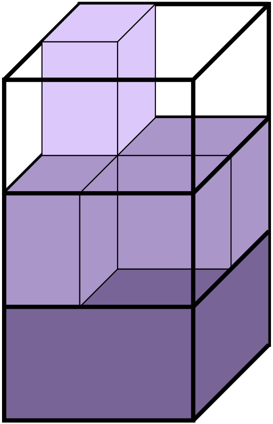
Simple Attack of Rainbow

- Find a layer two oil vector y by solving:

$$\begin{cases} P(y) = 0 \\ D_x(y) = 0 \end{cases}$$

Beullens, "Breaking rainbow takes a weekend on a laptop." Crypto (2022)

HFERP Central Maps



Simple Attack on HFERP

Finding y

- Let P_i be the matrix representation of the i^{th} public key polynomial
- Choose a random $\mathbf{z} \in \mathbb{F}_q^n$ and create the $m \times n$ matrix

$$A_{\mathbf{z}} = \begin{bmatrix} \mathbf{z}P_1 \\ \mathbf{z}P_2 \\ \vdots \\ \mathbf{z}P_m \end{bmatrix}$$

- Goal: Find a vector $\mathbf{y} \in \mathbb{F}_q^m$ such that

$$\begin{cases} \mathbf{y} \in Ker_L(A_{\mathbf{z}}) \\ Rank(\sum_{i=1}^{m} y_i P_i) \leq d. \end{cases}$$

Simple Attack on HFERP

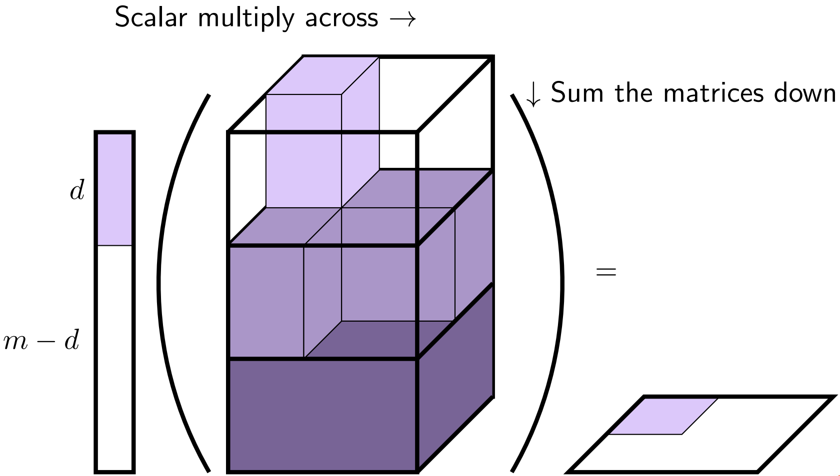
Finding y

If we can find a $\mathbf{y} \in \mathbb{F}_q^m$, then with high probability,

$$\mathbf{yT} = (\mathbf{a}||\mathbf{b}) \implies \mathbf{y} = (\mathbf{a}||\mathbf{b})\mathbf{T}^{-1},$$

where

- $\mathbf{a}$ is a length d vector in the kernel of the upper left $d \times d$ block of $A_{\mathbf{z}}$
- $\mathbf{b}$ is the length $m - d = o + r + s$ zero vector.


Scalar multiply across $\rightarrow$
$\downarrow$ Sum the matrices down
d
$m - d$
$=$

Finding the Oil and Vinegar Spaces

Simple Attack on HFERP: Inverting U

- Once we have a valid $\mathbf{y}$, compute the $n \times n$ matrix

$$P_{\mathbf{y}} = \sum_{i=1}^{m} y_i P_i.$$

- Note:

$$\text{rank}(P_{\mathbf{y}}) \leq d$$
$$\text{nullity}(P_{\mathbf{y}}) \geq o$$

- Recall,

$$\text{rank}(F_{HFE}^{(i)}) = d$$
$$\text{nullity}(F_{HFE}^{(i)}) = o$$

- Use basis vectors of $\text{Ker}(P_y)$, extend to a basis of $\mathbb{F}_q^n$.

Finding the Oil and Vinegar Spaces

Simple Attack on HFERP: Inverting U

We obtain the block matrix

$$\widehat{\mathbf{B}}\mathbf{P}_{\mathbf{y}}\widehat{\mathbf{B}}^{\top} = \begin{bmatrix} \alpha_i \mathbf{P}_{\mathbf{y}} \alpha_j^{\top} & 0 \\ 0 & 0 \end{bmatrix}$$

where $i, j \leq d$.

Finding the Oil and Vinegar Spaces

Simple Attack on HFERP: Inverting U

We obtain the block matrix

$$\widehat{\mathbf{B}}\mathbf{P_y}\widehat{\mathbf{B}}^\top = \begin{bmatrix} \alpha_i \mathbf{P_y} \alpha_j^\top & 0 \\ 0 & 0 \end{bmatrix}$$

where $i, j \leq d$.

Observe:

Finding the Oil and Vinegar Spaces

Simple Attack on HFERP: Inverting U

We obtain the block matrix

$$\widehat{\mathbf{B}}\mathbf{P}_{\mathbf{y}}\widehat{\mathbf{B}}^\top = \begin{bmatrix} \alpha_i \mathbf{P}_{\mathbf{y}} \alpha_j^\top & 0 \\ 0 & 0 \end{bmatrix}$$

where $i, j \leq d$.

Observe:

- Only the upper left $d \times d$ block has nonzero entries

Finding the Oil and Vinegar Spaces

Simple Attack on HFERP: Inverting U

We obtain the block matrix

$$\widehat{\mathbf{B}}\mathbf{P}_{\mathbf{y}}\widehat{\mathbf{B}}^{\top} = \begin{bmatrix} \alpha_i \mathbf{P}_{\mathbf{y}} \alpha_j^{\top} & 0 \\ 0 & 0 \end{bmatrix}$$

where $i, j \leq d$.

Observe:

- Only the upper left $d \times d$ block has nonzero entries
- $\widehat{\mathbf{B}}\mathbf{P}_{\mathbf{y}}\widehat{\mathbf{B}}^{\top}$ is a linear combination of HFE maps

Finding the Oil and Vinegar Spaces

Simple Attack on HFERP: Inverting U

We obtain the block matrix

$$\widehat{\mathbf{B}}\mathbf{P}_{\mathbf{y}}\widehat{\mathbf{B}}^{\top} = \begin{bmatrix} \alpha_i \mathbf{P}_{\mathbf{y}} \alpha_j^{\top} & 0 \\ 0 & 0 \end{bmatrix}$$

where $i, j \leq d$.

Observe:

- Only the upper left $d \times d$ block has nonzero entries
- $\widehat{\mathbf{B}}\mathbf{P}_{\mathbf{y}}\widehat{\mathbf{B}}^{\top}$ is a linear combination of HFE maps

Conclusion: We found equivalent U^{-1}

Inverting T

Simple Attack on HFERP

Consider the matrix representation of public key as composition of the secret keys.

$$\mathcal{P} = \mathcal{T} \circ \begin{bmatrix} F_{HFE} \\ F_R \\ F_p \end{bmatrix} \circ \mathcal{U}$$

$$\begin{bmatrix} p_1(\mathbf{x}) \\ \vdots \\ p_m(\mathbf{x}) \end{bmatrix} = \mathcal{T} \circ \begin{bmatrix} \mathbf{x} U F_1 U^\top \mathbf{x}^\top \\ \vdots \\ \mathbf{x} U F_m U^\top \mathbf{x}^\top \end{bmatrix}$$

$$\implies P_i = \sum_{k=1}^{m} t_{ik} \mathbf{U} \mathbf{F}_k \mathbf{U}^\top = \mathbf{U} \left(\sum_{k=1}^{m} t_{ik} \mathbf{F}_k \right) \mathbf{U}^\top$$

Inverting T

$$\widehat{\mathbf{B}} P_i \widehat{\mathbf{B}}^\top = \widehat{\mathbf{B}}\mathbf{U}\left(\sum_{k=1}^{m} t_{ik}\mathbf{F}_k\right)\mathbf{U}^\top\widehat{\mathbf{B}}^\top \cong \sum_{k=1}^{m} t_{ik}\mathbf{F}_k$$

Inverting T

$$\widehat{\mathbf{B}}P_i\widehat{\mathbf{B}}^\top = \widehat{\mathbf{B}}\mathbf{U}\left(\sum_{k=1}^{m} t_{ik}\mathbf{F}_k\right)\mathbf{U}^\top\widehat{\mathbf{B}}^\top \cong \sum_{k=1}^{m} t_{ik}\mathbf{F}_k$$

Each $\widehat{\mathbf{B}}P_i\widehat{\mathbf{B}}^\top$ is now seen to be a linear combination of the m central maps.

Structure of each F_k

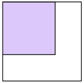
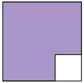
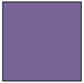
	$1 \leq k \leq d$	$d+1 \leq k \leq o+r$	$o+r+1 \leq k \leq m$
Structure of $\mathbf{F}_k$			
Rank$(\mathbf{F}_k) \leq$	d	n	n
Guaranteed zeros	Rows $d \leq i \leq m$ Columns $d \leq j \leq m$	Lower right $o \times o$ submatrix	None

Table: The table summarizes notable properties of the symmetric matrices corresponding to the F_{HFE}, F_R, and F_P polynomials.

Divide and Conquer

- We now have equivalent keys for every part of the secret map.
- Invert the HFE maps using Berlekamp's algorithm.
- We know O and V, so invert the UOV maps as they are linear in the oil variables.

Updated Security

Table: Complexity of the Simple Attack on proposed parameters of HFERP, where $D = 3^7 + 1$ is the degree bound of the HFE central map polynomial.

(q, d, o, r, s)	Claimed Sec	Simple Attack	MinRank Type
$(3, 42, 21, 15, 17)$	80 bit	$3 \cdot 3^{32} \cdot 63^{\omega} \approx 2^{69}$	Search
$(3, 63, 21, 11, 10)$	80 bit	$3 \cdot 3^{21} \cdot 84^{\omega} \approx 2^{52}$	Search
$(3, 60, o_i = 40, r_i = 23, 40)$	128 bit	$3 \cdot 3^{59} (86^{\omega} + 140^{\omega}) \approx 2^{115}$	Lin Alg

Big-Field Support Minors

Big-Field Support Minors

Can apply "big-field support minors" to HFERP in way similar to break of GeMSS.

Big-Field Support Minors

Can apply "big-field support minors" to HFERP in way similar to break of GeMSS. Makes HFERP even more broken!

Big-Field Support Minors

Can apply "big-field support minors" to HFERP in way similar to break of GeMSS. Makes HFERP even more broken! (Complexity does depend on D, whereas divide and conquer does not.)

(q, d, o, r, s)	Degree Bound	Claimed Sec	Update Comp	Algth Type
$(3, 42, 21, 15, 17)$	$D = 3^7 + 1$	80 bit	2^{57}	Wiedemann
$(3, 63, 21, 11, 10)$	$D = 3^7 + 1$	80 bit	2^{59}	Strassen
$(3, 85, o_i = 70, r_i = 89, 61)$	$D = 3^9 + 1$	128 bit	2^{63}	Strasssen
$(3, 60, o_i = 40, r_i = 23, 40)$	$D = 3^9 + 1$	128 bit	2^{69}	Wiedemann

Baena, Briaud, Cabarcas, Perlner, Smith-Tone, Verbel, "Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow." (2021)

Thank you for your attention!
Any questions?

https://github.com/maxcartor/HFERP-Cryptanalysis

rcartor@clemson.edu