Key Recovery Attack for all Parameters of HFE-

Jeremy Vates[1] & **Daniel Smith-Tone**[1,2]

[1]University of Louisville
[2]National Institute of Standards and Technology

28 June, 2017

Multivariate Public Key Cryptography

Nonlinear Systems

Base the security of the cryptographic scheme on the difficulty of finding a preimage of some element in the range of a system of nonlinear equations.

Multivariate Public Key Cryptography

Nonlinear Systems

Base the security of the cryptographic scheme on the difficulty of finding a preimage of some element in the range of a system of nonlinear equations.

Trapdoor

MPKC relies (typically) on the ability to invert specially constructed multivariate functions and the ability to mask such functions.

Masking

Polynomial Morphisms

Let $f, g : \mathbb{F}^n \to \mathbb{F}^m$ be polynomial functions. A *polynomial morphism* between f and g is a pair of affine transformations $T \in M_m(\mathbb{F})$ and $U \in M_n(\mathbb{F})$ such that

$$g = T \circ f \circ U.$$

Masking

Polynomial Morphisms

Let $f, g : \mathbb{F}^n \to \mathbb{F}^m$ be polynomial functions. A *polynomial morphism* between f and g is a pair of affine transformations $T \in M_m(\mathbb{F})$ and $U \in M_n(\mathbb{F})$ such that

$$g = T \circ f \circ U.$$

Isomorphism of Polynomials

If T and U are nonsingular, then the pair (T, U) is an *isomorphism of polynomials*. Further, if T is the identity, then U is called a one-sided isomorphism between f and g.

Masking

Polynomial Morphisms

Let $f, g : \mathbb{F}^n \to \mathbb{F}^m$ be polynomial functions. A *polynomial morphism* between f and g is a pair of affine transformations $T \in M_m(\mathbb{F})$ and $U \in M_n(\mathbb{F})$ such that

$$g = T \circ f \circ U.$$

Isomorphism of Polynomials

If T and U are nonsingular, then the pair (T, U) is an *isomorphism of polynomials*. Further, if T is the identity, then U is called a one-sided isomorphism between f and g.

Many, but not all properties of polynomial functions are preserved by polynomial isomorphisms.

Large Structure Schemes

One method of creating effectively invertible multivariate maps is to use algebraic properties of some associative algebra over the field $\mathbb{F}$. There are essentially two ways of doing this.

Large Structure Schemes

One method of creating effectively invertible multivariate maps is to use algebraic properties of some associative algebra over the field $\mathbb{F}$. There are essentially two ways of doing this.

Big Field Schemes

Construct an extension field k of $\mathbb{F}$. One may think of the extension as a commutative $\mathbb{F}$-algebra that happens to be a field. One utilizes the multiplication in k to construct an invertible map.

Large Structure Schemes

One method of creating effectively invertible multivariate maps is to use algebraic properties of some associative algebra over the field $\mathbb{F}$. There are essentially two ways of doing this.

Big Field Schemes

Construct an extension field k of $\mathbb{F}$. One may think of the extension as a commutative $\mathbb{F}$-algebra that happens to be a field. One utilizes the multiplication in k to construct an invertible map.

Matrix Algebra Schemes

Construct a matrix algebra $M_n(\mathbb{F})$. One then utilizes the multiplication in $M_n(\mathbb{F})$ to construct an invertible map.

Butterfly Construction

Big Field

$$\begin{array}{ccccccc} & & k^r & \xrightarrow{f} & k^s & & \\ & \overset{\phi_r}{\uparrow} & & & \downarrow \overset{\phi_s^{-1}}{} & & \\ \mathbb{F}_q^n & \xrightarrow{U} & \mathbb{F}_q^{rd} & \xrightarrow{F} & \mathbb{F}_q^{sd} & \xrightarrow{T} & \mathbb{F}_q^m \end{array} \qquad \begin{array}{c} k \\ \vert \\ \mathbb{F}_q \end{array} \Big\rceil d$$

Butterfly Construction

Big Field

$$\begin{array}{ccccccc} & & k^r & \xrightarrow{f} & k^s & & \\ & \overset{\phi_r}{\uparrow} & & & \downarrow \phi_s^{-1} & & \\ \mathbb{F}_q^n & \xrightarrow{U} & \mathbb{F}_q^{rd} & \xrightarrow{F} & \mathbb{F}_q^{sd} & \xrightarrow{T} & \mathbb{F}_q^m \end{array} \qquad \begin{array}{c} k \\ \uparrow \\ \mathbb{F}_q \end{array} \Big\rceil d$$

Matrix Algebra

$$\begin{array}{ccccccc} & & M_d(\mathbb{F}_q)^r & \xrightarrow{f} & M_d(\mathbb{F}_q)^s & & \\ & \overset{\phi_r}{\uparrow} & & & \downarrow \phi_s^{-1} & & \\ \mathbb{F}_q^n & \xrightarrow{U} & \mathbb{F}_q^{rd^2} & \xrightarrow{F} & \mathbb{F}_q^{sd^2} & \xrightarrow{T} & \mathbb{F}_q^m \end{array}$$

General Inversion

One of the most general inversion techniques in the big field setting is Berlekamp's Algorithm.

General Inversion

One of the most general inversion techniques in the big field setting is Berlekamp's Algorithm.

Complexity

Given a degree D polynomial for a fixed field k the Berlekamp Algorithm has complexity roughly $\mathcal{O}(D^3)$.

General Inversion

One of the most general inversion techniques in the big field setting is Berlekamp's Algorithm.

Complexity

Given a degree D polynomial for a fixed field k the Berlekamp Algorithm has complexity roughly $\mathcal{O}(D^3)$.

For HFE

$$f(x) = \sum_{\substack{i \leq j \\ q^i + q^j \leq D}} \alpha_{i,j} x^{q^i + q^j} + \sum_{\substack{i \\ q^i \leq D}} \beta_i x^{q^i} + \gamma,$$

where the coefficients $\alpha_{i,j}, \beta_i, \gamma \in k$. To get HFE-, remove some polynomials.

Parameter Sets

An Example for Odd Characteristic and 80-bit security:
HFE-$(q = 31, n = 36, D = 1922, a = 2)$

Parameter Sets

An Example for Odd Characteristic and 80-bit security:
HFE-$(q = 31, n = 36, D = 1922, a = 2)$

HFE Challenge -2
HFE-$(q = 16, n = 36, D = 4352, a = 4)$

Homogeneous Component as Quadratic Form

Any homogeneous $\mathbb{F}_q$-quadratic function $f : k \to k$ has the form

$$f(x) = \sum_{0 \le i \le j < n} \alpha_{ij} x^{q^i + q^j}.$$

Homogeneous Component as Quadratic Form

Any homogeneous $\mathbb{F}_q$-quadratic function $f : k \to k$ has the form

$$f(x) = \sum_{0 \le i \le j < n} \alpha_{ij} x^{q^i + q^j}.$$

We may consider f a quadratic form in $k[X_0, \ldots, X_{n-1}]$ by identifying x^{q^i} with X_i, obtaining:

$$\begin{bmatrix} X_0 & \cdots & X_{n-1} \end{bmatrix} \begin{bmatrix} \alpha_{0,0} & \alpha_{0,1}/2 & \cdots & \alpha_{0,n-1}/2 \\ \alpha_{0,1}/2 & \alpha_{1,1} & \cdots & \alpha_{1,n-1}/2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{0,n-1}/2 & \alpha_{1,n-1}/2 & \cdots & \alpha_{n-1,n-1} \end{bmatrix} \begin{bmatrix} X_0 \\ \vdots \\ X_{n-1} \end{bmatrix}.$$

Q-Rank

Q-Rank

The Q-Rank of f is the rank of f as a quadratic form over $k[X_0, \ldots, X_{n-1}]$. (This quantity is equivalent to the rank of the matrix representation of f.)

Q-Rank

Q-Rank

The Q-Rank of f is the rank of f as a quadratic form over $k[X_0, \ldots, X_{n-1}]$. (This quantity is equivalent to the rank of the matrix representation of f.)

1. Q-Rank is invariant under one-sided isomorphisms.

Q-Rank

Q-Rank

The Q-Rank of f is the rank of f as a quadratic form over $k[X_0, \ldots, X_{n-1}]$. (This quantity is equivalent to the rank of the matrix representation of f.)

1. Q-Rank is invariant under one-sided isomorphisms.
2. One-sided isomorphisms induce congruence of matrix representations, but not necessarily vice versa.

Q-Rank

Q-Rank

The Q-Rank of f is the rank of f as a quadratic form over $k[X_0, \ldots, X_{n-1}]$. (This quantity is equivalent to the rank of the matrix representation of f.)

1. Q-Rank is invariant under one-sided isomorphisms.
2. One-sided isomorphisms induce congruence of matrix representations, but not necessarily vice versa.

min-Q-Rank

min-Q-Rank is the minimum Q-Rank in the $\mathbb{F}_q$-span of f. min-Q-Rank is invariant under isomorphisms of polynomials.

Q-Rank of HFE

Since the HFE polynomial is given by

$$f(x) = \sum_{\substack{i \le j \\ q^i + q^j \le D}} \alpha_{i,j} x^{q^i + q^j} + \sum_{\substack{i \\ q^i \le D}} \beta_i x^{q^i} + \gamma,$$

the matrix representation of the quadratic form is given by

$$\begin{bmatrix} \alpha_{0,0} & \alpha_{0,1}/2 & \cdots & \alpha_{0,d}/2 & 0 & \cdots & 0 \\ \alpha_{0,1}/2 & \alpha_{1,1} & \cdots & \alpha_{1,d}/2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{0,d}/2 & \alpha_{1,d}/2 & \cdots & \alpha_{d,d} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Minimal Polynomial of an Algebraic Set

Definition (see Definition 1, (Daniels,S.-T., 2014))

The *minimal polynomial*, of the algebraic set $V \subseteq k$ is given by

$$\mathcal{M}_V := \prod_{v \in V} (x - v).$$

Equivalently, $\mathcal{M}_V$ is the generator of the principal ideal $I(V)$, the intersection of the maximal ideals $\langle x - v \rangle$ for all $v \in V$.

Absorbing the Minus

Lemma

Let $\Pi \circ T$ be a corank a linear transformation on $\mathbb{F}_q^n$. There exist both a nonsingular linear transformation S and a degree q^a linear polynomial π such that $\Pi \circ T = S \circ \pi$.

Proof.

Let V be the kernel of $\Pi \circ T$ and let $\pi = \mathcal{M}_V$. Extend a basis for V to k and let M be change of basis matrix taking the standard basis to B. Then both $M^{-1}(\Pi \circ T)M$ and $M^{-1}(\pi)M$ have the last a columns of 0.
Then there exist row operations A and A', such that:

$$AM^{-1}(\Pi \circ T)M = \left[\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right] = A'M^{-1}(\pi)M \tag{1}$$

Equivalence

Theorem

Let P be the public key of an $HFE^-(q, n, D, a)$ scheme. Then

$$P' := P \| \{p_{n-a}, p_{n-a+1} \dots, p_{n-1}\}$$

is a public key of an $HFE(q, n, q^a D)$ scheme for any choice of $p_i \in Span(P)$ where $i \in \{n-a, n-a+1, \dots, n-1\}$.

Structure of HFE Equivalent Key

Theorem

Let P be a public key for an instance of HFE$-(q, n, D, a)$ and let $P' = P \| \{p_{n-a}, p_{n-a+1} \ldots, p_{n-1}\}$ be a corresponding HFE$(q, n, q^a D)$ public key. Further, let (T', f', U') be any private key of P'. Then the representation of f' as a quadratic form over k is block diagonal of the form:

$$\mathbf{F}' = \begin{bmatrix} F_1 & 0 \\ 0 & 0 \end{bmatrix}, \tag{2}$$

where $F_1' = [f_{i,j}]_{i,j}$ is $(\lceil log_q(D) \rceil + a) \times (\lceil log_q(D) \rceil + a)$ and has the property that $f_{i,j} = 0$ if $|i - j| \geq \lceil log_q(D) \rceil$. That is, F_1' has only a diagonal "band" of nonzero values of width $2\lceil log_q(D) \rceil - 1$.

Recovering an Equivalent HFE- Key

Theorem

Let (T, f, U) be an $HFE^{-}(q, n, D, a)$ private key and let (T', f', U') be an equivalent $HFE(q, n, q^a D)$ key. Then a linear map T'' and a quadratic map f'' of degree bound D such that $\Pi \circ T'' \circ \phi^{-1} \circ f'' \circ \phi \circ U' = \Pi \circ T \circ \phi^{-1} \circ f \circ \phi \circ U$ can be recovered by solving two linear systems, the first of dimension a and the second of dimension $\binom{\lceil log_q(D) \rceil}{2}$.

Recovering an Equivalent HFE- Key, cont'd

Proof.

We know there is a degree bound D function f'' and

$$\pi(x) = \sum_{i=0}^{a} p_i x^{q^i}.$$

Recovering an Equivalent HFE- Key, cont'd

Proof.

We know there is a degree bound D function f'' and

$$\pi(x) = \sum_{i=0}^{a} p_i x^{q^i}.$$

The equation $f' = \pi \circ f''$ is bilinear in the unknowns p_i and the unknown coefficients of f''. We may set $p_0 = 1$ by "absorbing" the scalar into T''. Then all coefficients of x^{q^i+1} are the same in f' and $\pi \circ f''$.

Recovering an Equivalent HFE- Key, cont'd

Proof.

We know there is a degree bound D function f'' and

$$\pi(x) = \sum_{i=0}^{a} p_i x^{q^i}.$$

The equation $f' = \pi \circ f''$ is bilinear in the unknowns p_i and the unknown coefficients of f''. We may set $p_0 = 1$ by "absorbing" the scalar into T''. Then all coefficients of x^{q^i+1} are the same in f' and $\pi \circ f''$.

We can then obtain p_i by equating the coefficients of $x^{q^i+q^{d+i}}$ (a linear system). The system then becomes linear in the coefficients of f''.

Complexity

The complexity is dominated by the MinRank instance in the attack. We note a couple of things.

Complexity

The complexity is dominated by the MinRank instance in the attack. We note a couple of things.

1. The asymptotic complexity of MinRank(n, k, r) is $\mathcal{O}(k^{(r+1)\omega})$.

Complexity

The complexity is dominated by the MinRank instance in the attack. We note a couple of things.

1. The asymptotic complexity of MinRank(n, k, r) is $\mathcal{O}(k^{(r+1)\omega})$.
2. A better practical approximation is $\mathcal{O}(\binom{k+r+1}{r+1}^{\omega})$.

Complexity

The complexity is dominated by the MinRank instance in the attack. We note a couple of things.

1. The asymptotic complexity of MinRank(n, k, r) is $\mathcal{O}(k^{(r+1)\omega})$.
2. A better practical approximation is $\mathcal{O}(\binom{k+r+1}{r+1}^{\omega})$.
3. For this attack, $\mathcal{O}(\binom{n+\lceil log_q(D)\rceil+1}{\lceil log_q(D)\rceil+a+1}^{\omega})$.

Complexity

The complexity is dominated by the MinRank instance in the attack. We note a couple of things.

1. The asymptotic complexity of MinRank(n, k, r) is $\mathcal{O}(k^{(r+1)\omega})$.
2. A better practical approximation is $\mathcal{O}(\binom{k+r+1}{r+1}^{\omega})$.
3. For this attack, $\mathcal{O}(\binom{n+\lceil log_q(D)\rceil+1}{\lceil log_q(D)\rceil+a+1}^{\omega})$.
4. This quantity is much better than $\mathcal{O}(n^{(\lceil log_q(D)\rceil+a+1)\omega})$.

Complexity

The complexity is dominated by the MinRank instance in the attack. We note a couple of things.

1. The asymptotic complexity of MinRank(n, k, r) is $\mathcal{O}(k^{(r+1)\omega})$.
2. A better practical approximation is $\mathcal{O}(\binom{k+r+1}{r+1}^{\omega})$.
3. For this attack, $\mathcal{O}(\binom{n+\lceil log_q(D)\rceil+1}{\lceil log_q(D)\rceil+a+1}^{\omega})$.
4. This quantity is much better than $\mathcal{O}(n^{(\lceil log_q(D)\rceil+a+1)\omega})$.
5. Thus HFE-(q, n, D, a) is weaker than HFE$(q, n, q^a D)$.

Parameter Selection

Let $q = 7$, $n = 8$, $D = 14$ and $a = 2$. We construct the degree n extension $k = \mathbb{F}_7[x]/\left\langle x^8 + 4x^3 + 6x^2 + 2x + 3 \right\rangle$ and let $b \in k$ be a fixed root of this irreducible polynomial.

We randomly select $f : k \to k$ of degree D,

$$f(x) = b^{4100689}x^{14} + b^{1093971}x^8 + b^{5273323}x^2,$$

and two invertible linear transformations T and U:

$$T = \begin{bmatrix} 2 & 1 & 0 & 3 & 5 & 0 & 3 & 2 \\ 6 & 2 & 1 & 3 & 4 & 2 & 5 & 1 \\ 0 & 2 & 5 & 1 & 3 & 1 & 4 & 3 \\ 3 & 2 & 6 & 4 & 5 & 3 & 4 & 4 \\ 6 & 4 & 2 & 1 & 0 & 5 & 0 & 0 \\ 0 & 3 & 3 & 6 & 5 & 1 & 1 & 3 \\ 0 & 3 & 0 & 4 & 3 & 6 & 1 & 5 \\ 4 & 3 & 2 & 6 & 1 & 1 & 6 & 3 \end{bmatrix}, \; U = \begin{bmatrix} 5 & 1 & 4 & 1 & 4 & 2 & 5 & 3 \\ 0 & 6 & 1 & 5 & 3 & 5 & 3 & 2 \\ 3 & 3 & 5 & 0 & 3 & 4 & 2 & 2 \\ 4 & 0 & 5 & 4 & 0 & 6 & 4 & 1 \\ 2 & 6 & 4 & 0 & 0 & 5 & 3 & 5 \\ 0 & 2 & 4 & 0 & 2 & 0 & 6 & 5 \\ 4 & 3 & 0 & 3 & 3 & 2 & 2 & 6 \\ 6 & 2 & 5 & 3 & 5 & 4 & 0 & 0 \end{bmatrix}.$$

Structure of f

Recall that $f(x) = b^{4100689}x^{14} + b^{1093971}x^8 + b^{5273323}x^2$.

Since $b^{1093971}/2 = b^{4937171}$, we have

$$\mathbf{F} = \begin{bmatrix} b^{5273323} & b^{4937171} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{4937171} & b^{4100689} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Public Key

We fix $\Pi : \mathbb{F}_q^8 \to \mathbb{F}_q^6$, the projection onto the first 6 coordinates. Then the public key $P = \Pi \circ T \circ F \circ U$ in matrix form over $\mathbb{F}_q$ is given by:

$$\begin{bmatrix} 5 & 6 & 3 & 6 & 6 & 0 & 4 & 2 \\ 6 & 0 & 1 & 3 & 3 & 5 & 2 & 1 \\ 3 & 1 & 4 & 0 & 6 & 0 & 4 & 4 \\ 6 & 3 & 0 & 3 & 0 & 2 & 3 & 1 \\ 6 & 3 & 6 & 0 & 4 & 2 & 2 & 4 \\ 0 & 5 & 0 & 2 & 2 & 2 & 5 & 1 \\ 4 & 2 & 4 & 3 & 2 & 5 & 1 & 5 \\ 2 & 1 & 4 & 1 & 4 & 1 & 5 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 6 & 1 & 5 & 4 & 2 & 2 & 2 \\ 6 & 5 & 4 & 4 & 0 & 1 & 6 & 2 \\ 1 & 4 & 3 & 5 & 6 & 2 & 1 & 1 \\ 5 & 4 & 5 & 2 & 2 & 3 & 1 & 5 \\ 4 & 0 & 6 & 2 & 2 & 1 & 2 & 4 \\ 2 & 1 & 2 & 3 & 1 & 6 & 2 & 6 \\ 2 & 6 & 1 & 1 & 2 & 2 & 5 & 6 \\ 2 & 2 & 1 & 5 & 4 & 6 & 6 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 5 & 2 & 2 & 2 & 3 & 3 & 2 \\ 5 & 1 & 2 & 1 & 3 & 2 & 5 & 4 \\ 2 & 2 & 2 & 1 & 6 & 2 & 1 & 0 \\ 2 & 1 & 1 & 4 & 4 & 5 & 2 & 3 \\ 2 & 3 & 6 & 4 & 4 & 5 & 2 & 2 \\ 3 & 2 & 2 & 5 & 5 & 3 & 4 & 6 \\ 3 & 5 & 1 & 2 & 2 & 4 & 5 & 5 \\ 2 & 4 & 0 & 3 & 2 & 6 & 5 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 6 & 6 & 4 & 0 & 0 & 3 & 4 \\ 6 & 2 & 5 & 5 & 4 & 5 & 5 & 6 \\ 6 & 5 & 4 & 6 & 3 & 6 & 4 & 2 \\ 4 & 5 & 6 & 4 & 5 & 2 & 4 & 5 \\ 0 & 4 & 3 & 5 & 6 & 3 & 6 & 0 \\ 0 & 5 & 6 & 2 & 3 & 2 & 4 & 1 \\ 3 & 5 & 4 & 4 & 6 & 4 & 4 & 4 \\ 4 & 6 & 2 & 5 & 0 & 1 & 4 & 0 \end{bmatrix}, \begin{bmatrix} 4 & 4 & 5 & 2 & 6 & 6 & 5 & 2 \\ 4 & 4 & 0 & 0 & 3 & 4 & 1 & 6 \\ 5 & 0 & 5 & 3 & 3 & 0 & 1 & 0 \\ 2 & 0 & 3 & 4 & 1 & 3 & 3 & 2 \\ 6 & 3 & 3 & 1 & 6 & 5 & 0 & 1 \\ 6 & 4 & 0 & 3 & 5 & 4 & 6 & 0 \\ 5 & 1 & 1 & 3 & 0 & 6 & 2 & 6 \\ 2 & 6 & 0 & 2 & 1 & 0 & 6 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 2 & 6 & 1 & 6 & 2 & 3 & 4 \\ 2 & 4 & 2 & 0 & 3 & 1 & 5 & 0 \\ 6 & 2 & 5 & 1 & 4 & 3 & 1 & 1 \\ 1 & 0 & 1 & 5 & 0 & 0 & 3 & 0 \\ 6 & 3 & 4 & 0 & 1 & 4 & 1 & 4 \\ 2 & 1 & 3 & 0 & 4 & 5 & 5 & 5 \\ 3 & 5 & 1 & 3 & 1 & 5 & 1 & 2 \\ 4 & 0 & 1 & 0 & 4 & 5 & 2 & 6 \end{bmatrix},$$

Recovering a Related HFE Key - T'

We have an instance MinRank(n=8,k=6,r=4). We may fix one variable to make the ideal generated by the 5×5 minors zero-dimensional. There are $n = 8$ solutions, each of which consists of the Frobenius powers of the coordinates of

$$v = (1, b^{5656746}, b^{3011516}, b^{3024303}, b^{1178564}, b^{1443785}).$$

The combination $L = \sum_{i=0}^{5} v_i \mathbf{P_i}$ is now a rank 4 matrix with entries in k.
We next form $\widehat{v}$ from v by appending $a = 2$ random nonzero values from k to v. Now we compute

$$\phi^{-1} T'^{-1} \circ \phi = \sum_{i=0}^{8} \widehat{v}_i x^{q^i}.$$

Recovering a Related HFE Key - U'

Next we let K_i be the left kernel matrix of the $n - i$th Frobenius power of L for $i = 0, 1, \ldots, a + 1$. We then recover a vector w simultaneously in the right kernel of K_i for all i. For this example, each such element is a multiple in k of

$$w = (b^{4849804}, b^{3264357}, b^{4466027}, b^{638698}, b^{2449742}, b^{4337472}, b^{2752502}, b^{1186132}).$$

Then we may compute

$$\phi^{-1} \circ U \circ \phi = \sum_{i=0}^{8} w_i x^{q^i}.$$

Recovering a Related Key - F'

At this point we can recover $\phi^{-1} \circ f' \circ \phi = T'^{-1} \circ P \circ U'^{-1}$

$$T' = \begin{bmatrix} 1 & 4 & 4 & 5 & 4 & 5 & 5 & 2 \\ 0 & 6 & 6 & 0 & 4 & 4 & 5 & 5 \\ 0 & 5 & 0 & 4 & 2 & 0 & 0 & 3 \\ 0 & 4 & 4 & 2 & 5 & 6 & 6 & 6 \\ 0 & 3 & 6 & 2 & 5 & 6 & 0 & 0 \\ 0 & 2 & 0 & 4 & 4 & 6 & 2 & 2 \\ 0 & 1 & 5 & 5 & 0 & 5 & 2 & 6 \\ 0 & 3 & 3 & 3 & 6 & 5 & 2 & 2 \end{bmatrix}, \; U' = \begin{bmatrix} 6 & 2 & 1 & 4 & 4 & 4 & 1 & 6 \\ 1 & 6 & 0 & 2 & 3 & 0 & 4 & 2 \\ 2 & 5 & 3 & 6 & 3 & 3 & 0 & 4 \\ 0 & 5 & 6 & 5 & 4 & 1 & 4 & 2 \\ 6 & 5 & 3 & 5 & 4 & 6 & 3 & 2 \\ 0 & 4 & 6 & 1 & 4 & 0 & 1 & 5 \\ 6 & 0 & 2 & 3 & 6 & 5 & 6 & 3 \\ 5 & 2 & 0 & 4 & 1 & 2 & 4 & 5 \end{bmatrix}$$

$$\mathbf{F}' = \begin{bmatrix} b^{416522} & b^{5402526} & 0 & 0 & 0 & 0 & 0 & 0 \\ b^{5402426} & b^{3093518} & b^{5177024} & 0 & 0 & 0 & 0 & 0 \\ 0 & b^{5177024} & b^{5689467} & b^{5706144} & 0 & 0 & 0 & 0 \\ 0 & 0 & b^{5706144} & b^{3464750} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Recovering Equivalent Key - F''

There exists a degree $D = 14$ map $f''(x) = f''_{0,0}x^2 + 2f''_{0,1}x^8 + f''_{1,1}x^{14}$ with

$$\mathbf{F}'' = \begin{bmatrix} f''_{0,0} & f''_{0,1} & 0 & 0 & 0 & 0 & 0 & 0 \\ f''_{0,1} & f''_{1,1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

and a polynomial $\pi(x) = x + p_1x^7 + p_2x^{49}$ such that $f' = \pi \circ f''$.

Recovering Equivalent Key - F''

Thus we obtain the bilinear system of equations by equating $\mathbf{F}'$ to:

$$\widehat{\pi\mathbf{F}''} = \begin{bmatrix} f''_{0,0} & f''_{0,1} & 0 & 0 & 0 & 0 & 0 & 0 \\ f''_{0,1} & f''_{1,1} + p_1(f''_{0,0})^7 & p_1(f''_{0,1})^7 & 0 & 0 & 0 & 0 & 0 \\ 0 & p_1(f''_{0,1})^7 & p_1(f''_{1,1})^7 + p_2(f''_{0,0})^{49} & p_2(f''_{0,1})^{49} & 0 & 0 & 0 & 0 \\ 0 & 0 & p_2(f''_{0,1})^{49} & p_2(f''_{1,1})^{49} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We have $f''_{0,0}$ and $f''_{0,1}$ solve for p_i and then the remaining f''_{ij}. We obtain

$$\pi = x + b^{1948142}x^7 + b^{398370}x^{49} \text{ and}$$

$$f''(x) = b^{416522}x^2 + b^{1559326}x^8 + b^{1121420}x^{14}.$$

Recovering Equivalent Key - T''

We then obtain the matrix form of π over $\mathbb{F}_q$ and compose with T':

$$\widehat{\pi} = \begin{bmatrix} 2 & 6 & 6 & 0 & 2 & 2 & 5 & 5 \\ 6 & 3 & 5 & 3 & 1 & 4 & 5 & 0 \\ 5 & 2 & 6 & 0 & 6 & 6 & 6 & 1 \\ 1 & 1 & 3 & 6 & 4 & 1 & 1 & 6 \\ 5 & 6 & 2 & 4 & 6 & 6 & 1 & 6 \\ 5 & 3 & 1 & 5 & 0 & 1 & 0 & 4 \\ 3 & 2 & 1 & 3 & 3 & 1 & 3 & 5 \\ 4 & 2 & 1 & 1 & 1 & 4 & 4 & 2 \end{bmatrix}, \quad T' \circ \widehat{\pi} = \begin{bmatrix} 0 & 0 & 1 & 2 & 0 & 5 & 4 & 0 \\ 1 & 2 & 4 & 4 & 2 & 1 & 0 & 4 \\ 0 & 2 & 2 & 1 & 1 & 6 & 1 & 0 \\ 3 & 3 & 1 & 0 & 6 & 3 & 2 & 0 \\ 0 & 1 & 3 & 1 & 0 & 2 & 2 & 2 \\ 3 & 4 & 5 & 0 & 1 & 3 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Replacing the last two rows of $T' \circ \widehat{\pi}$ to make a full rank matrix produces T''. Then the original public key P is equal to $\Pi \circ T'' \circ \phi^{-1} \circ f'' \circ \phi \circ U'$.

Conclusion

1. HFE- offers a marginal increase in security over HFE.

Conclusion

1. HFE- offers a marginal increase in security over HFE.
2. Perhaps it is better to say that HFE- significantly improves performance at the cost of a little security in comparison to HFE with a larger degree bound.

Conclusion

1. HFE- offers a marginal increase in security over HFE.
2. Perhaps it is better to say that HFE- significantly improves performance at the cost of a little security in comparison to HFE with a larger degree bound.
3. HFE- should inspire the same confidence as very inefficient instances of HFE.

And as always, thanks for watching.

Thank you for your attention.
Questions?