Efficient ZHFE Key Generation

John B. Baena[1] Daniel Cabarcas[1] Daniel E. Escudero[1]
Jaiberth Porras-Barrera[2] Javier A. Verbel[1]

Universidad Nacional de Colombia, Sede Medellín

Facultad de Ingeniería, Tecnológico de Antioquia

PQCrypto 2016

Context

- MPKC viable PQ alternative
- MPK signature schemes UOV, Rainbow, etc
- MPK encryption - many attacks
- HFE broken due to low rank of central map
- ZHFE use high rank central map
- ZHFE very slow key generation

Our Contribution

- A new efficient key generation algorithm for ZHFE
- Sort rows and cols of vanishing equation system to unveil its structure (close to block diagonal)
- New algorithm to construct matrix
- New algorithm to solve the system
- Complexity improvement from $\mathcal{O}(n^{3\omega})$ to $\mathcal{O}(n^{2\omega+1})$
- In practice from a couple of days to only a few minutes

Outline

1. Preliminaries
2. Efficient ZHFE Key Generation
3. Complexity of the New Method
4. Remarks About Security
5. Conclusion and Future Work

HFE Encryption Scheme

Let $\mathbb{F}$ be a finite field of size q, $\mathbb{K}$ a degree n field extension.
An **HFE polynomial** has the form

$$F(X) = \sum_{0 \le j \le i \le n} a_{ij} X^{q^i + q^j} + \sum_{i=0}^{n} b_i X^{q^i} + c, \quad \text{with} a_{ij}, b_i, c \in \mathbb{K}$$

Let $\varphi \colon \mathbb{K} \to \mathbb{F}^n$ be the typical vector space isomorphism, T and S randomly chosen affine maps over $\mathbb{F}$

- **Public Key:** $P = T \circ \varphi \circ F \circ \varphi^{-1} \circ S$
- **Private Key:** F, T, S
- **Encryption:** Evaluate P at plaintext $(x_1, \ldots, x_n)$
- **Decryption:** Invert T, φ, F, φ^{-1}, and S
- Degree of F small to be able to find preimages
- Broken in [KS99] (low rank)

ZHFE Encryption Scheme

- By Porras, Baena and Ding [PBD15]
- **Public key:** $P = (p_1, \ldots p_{2n}) = T \circ (\varphi \times \varphi) \circ (F, \tilde{F}) \circ \varphi^{-1} \circ S$, with F, $\tilde{F}$ high degree (and high rank) HFE polynomials
- **Secret key:** Choose F, $\tilde{F}$, and $\alpha_1, \ldots, \alpha_{2n}, \beta_1, \ldots, \beta_{2n} \in \mathbb{K}$ so that $\Psi = \Psi_0 + \Psi_1$ has degree less than D

$$\Psi_0 = X(\alpha_1 F_0 + \cdots + \alpha_n F_{n-1} + \beta_1 \tilde{F}_0 + \cdots + \beta_n \tilde{F}_{n-1})$$
$$\Psi_1 = X^q(\alpha_{n+1} F_0 + \cdots + \alpha_{2n} F_{n-1} + \beta_{n+1} \tilde{F}_0 + \cdots + \beta_{2n} \tilde{F}_{n-1}),$$

  where $F_i = F^{q^i} \bmod (X^{q^n} - X)$
- **Encryption:** Evaluate P at $(x_1, \ldots, x_n)$
- **Decryption:** Invert T, $\varphi \times \varphi$, then find a preimage of $(F, \tilde{F})$ using Ψ, and finally invert φ^{-1} and S.

Very slow ZHFE Key Generation

$$\Psi = X(\alpha_1 F_0 + \cdots + \alpha_n F_{n-1} + \beta_1 \tilde{F}_0 + \cdots + \beta_n \tilde{F}_{n-1}) + X^q(\alpha_{n+1} F_0 + \cdots + \alpha_{2n} F_{n-1} + \beta_{n+1} \tilde{F}_0 + \cdots + \beta_{2n} \tilde{F}_{n-1})$$

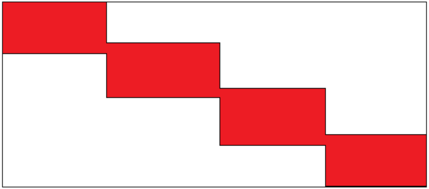
Key Generation:

- Randomly choose $\alpha_1, \ldots \alpha_{2n}, \beta_1, \ldots, \beta_{2n}$
- Determine coefficients of F and $\tilde{F}$ so that Ψ has degree less than D
- Yields a non-linear system $\mathcal{S}$ over $\mathbb{K}$
- Over $\mathbb{F}$, it is a linear homogeneous system $\mathcal{T}$ with matrix $\tilde{M}$
- Find the null space of $\tilde{M}$, and pick a random element on it

Problem: $\mathcal{T}$ is very large ($\mathcal{O}(n^3 \times n^3)$)

Efficient Key Generation

- We study combinatorial structure of Ψ
- Reordering variables and equations makes $\mathcal{S}$ quasi-block-diagonal
- $\tilde{M}$ preserves the structure
- We propose an algorithm to find an element in $\mathrm{Null}(\mathcal{T})$



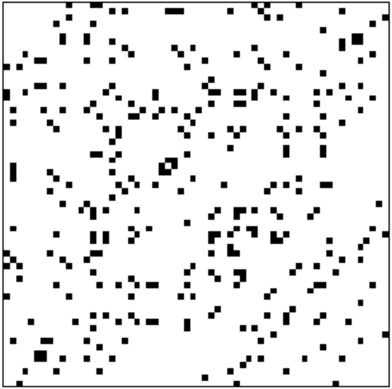
The system $\mathcal{S}$

A variable is a coefficient of
$F(X) = \sum_{0\leq j\leq i\leq n} a_{ij}X^{q^i+q^j} + \sum_{i=0}^{n} b_i X^{q^i} + c$,
$\tilde{F}(X) = \sum_{0\leq j\leq i\leq n} \tilde{a}_{ij}X^{q^i+q^j} + \sum_{i=0}^{n} \tilde{b}_i X^{q^i} + \tilde{c}$
and their Frobenious powers

An equation corresponds to a term of

$$\Psi = X(\alpha_1 F_0 + \cdots + \beta_n \tilde{F}_{n-1}) \\ + X^q(\alpha_{n+1} F_0 + \cdots + \beta_{2n} \tilde{F}_{n-1})$$

of degree $d > D$



Sorting Variables

Partition Variables

For $k \in \{0, \ldots, \frac{n}{2}\}$

$$\mathcal{A}_k := \begin{cases} \{(i, i+k \mod n) \mid 0 \leq i < n\}, & \text{if } 0 \leq k < \frac{n}{2} \\ \{(i, i+k) \mid 0 \leq i < \frac{n}{2}\}, & \text{if } k = \frac{n}{2}. \end{cases}$$

$$\mathcal{A} := \cup_{i=0}^{\frac{n}{2}} \mathcal{A}_i$$

Example, n=6

$$\begin{aligned} \mathcal{A}_0 &= \{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5)\} \\ \mathcal{A}_1 &= \{(0,1),(1,2),(2,3),(3,4),(4,5),(5,0)\} \\ \mathcal{A}_2 &= \{(0,2),(1,3),(2,4),(3,5),(4,0),(5,1)\} \\ \mathcal{A}_3 &= \{(0,3),(1,4),(2,5)\} \end{aligned}$$

Sorting Variables

For $(i,j) \in \mathcal{A}_k$, set $Z_h X^{q^i+q^j}$, with

	F	$\tilde{F}$
h	$2nk+i$	$2nk+n+i$

Example, n=6

$$\begin{aligned} F(X) = {} & Z_0 X^{q^0+q^0} + \cdots + Z_5 X^{q^5+q^5} \\ & + Z_{12} X^{q^0+q^1} + \cdots + Z_{17} X^{q^5+q^0} \\ & + Z_{24} X^{q^0+q^2} + \cdots + Z_{29} X^{q^5+q^1} + \cdots \end{aligned}$$

$$\begin{aligned} \tilde{F}(X) = {} & Z_6 X^{q^0+q^0} + \cdots + Z_{11} X^{q^5+q^5} \\ & + Z_{18} X^{q^0+q^1} + \cdots + Z_{23} X^{q^5+q^0} \\ & + Z_{30} X^{q^0+q^2} + \cdots + Z_{35} X^{q^5+q^1} + \cdots \end{aligned}$$

Properties of the Partition

the $k-$th part of F

${}_kF(X) := \sum_{(i,j)\in\mathcal{A}_k} Z_{2nk+i}X^{q^i+q^j}$

$$F(X) = \sum_{k=0}^{\frac{n}{2}} {}_kF(X) + \sum_{i=1}^{n-1} Z_{n(n+1)+i}X^{q^i} + c,$$

$$\tilde{F}(X) = \sum_{k=0}^{\frac{n}{2}} {}_k\tilde{F}(X) + \sum_{i=1}^{n-1} Z_{n(n+1)+n+i}X^{q^i} + \tilde{c}$$

Proposition

For $0 \leq \ell \leq n-1$, ${}_k\left[F(X)^{q^\ell}\right] = [{}_kF(X)]^{q^\ell}$

Properties of the Partition

$$\Psi = \Psi_0 + \Psi_1$$

$$\Psi_0 = X(\alpha_1 F_0 + \alpha_2 F_1 + \ldots + \alpha_n F_{n-1} + \beta_1 \tilde{F}_0 + \ldots + \beta_n \tilde{F}_{n-1})$$
$$\Psi_1 = X^q(\alpha_{n+1} F_0 + \alpha_{n+2} F_1 + \ldots + \alpha_{2n} F_{n-1} + \beta_{n+1} \tilde{F}_0 + \ldots + \beta_{2n} \tilde{F}_{n-1})$$

Corolario

For $(i, j) \in \mathcal{A}_k$ and $s \in \{0, 1\}$, the coefficient of $X^{q^s + q^i + q^j}$ in Ψ_s is

$$\sum_{\ell=0}^{n-1} \alpha_{ns+\ell+1} Z_{2n\mathbf{k}+(i\ominus\ell)}^{q^\ell} + \sum_{\ell=0}^{n-1} \beta_{ns+\ell+1} Z_{2n\mathbf{k}+n+(i\ominus\ell)}^{q^\ell}$$

$$\boxed{\Longrightarrow q^0 + q^i + q^j = q^1 + q^r + q^t ?}$$

Properties of the Partition

Lemma

Let $q > 2$, $0 \leq k < \frac{n}{2}$, $(i,j) \in \mathcal{A}_k$ and $(r,t) \in \mathcal{A}$. Then $q^0 + q^i + q^j = q^1 + q^r + q^t$ iff

- $i = 1$, $r = 0$ y $j = t$, or
- $j = 1$, $t = 0$ y $i = r$.

Example, coefficient of $X^{q^s+q^i+q^j}$ in ψ

With $(i,j) = (1,j) \in \mathcal{A}_k$ and $(r,t) = (0,j) \in \mathcal{A}_{k+1}$,

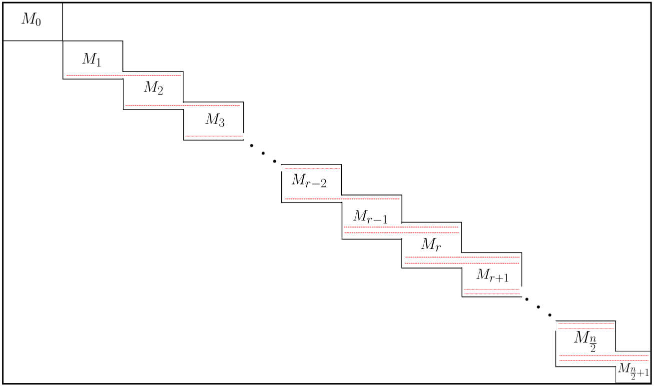
$$\left(\sum_{\ell=0}^{n-1} \alpha_{\ell+1} Z_{2n\mathbf{k}+(i\ominus\ell)}^{q^\ell} + \sum_{\ell=0}^{n-1} \beta_{\ell+1} Z_{2n\mathbf{k}+n+(i\ominus\ell)}^{q^\ell}\right) X^{q^0}(X^{q^1+q^j}) \text{ in } \Psi_0$$

$$\left(\sum_{\ell=0}^{n-1} \alpha_{n+\ell+1} Z_{2n(\mathbf{k}+\mathbf{1})+(i\ominus\ell)}^{q^\ell} + \sum_{\ell=0}^{n-1} \beta_{n+\ell+1} Z_{2n(\mathbf{k}+\mathbf{1})+n+(i\ominus\ell)}^{q^\ell}\right) X^{q^1}(X^{q^0+q^j}) \text{ in } \Psi_1$$

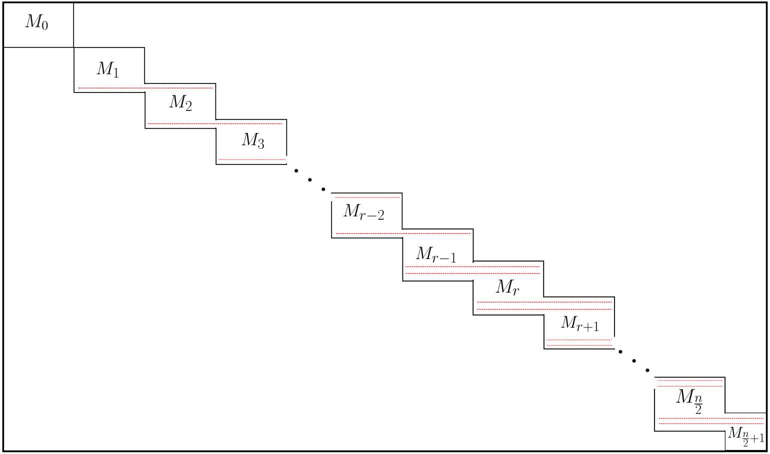
Main Result

Theorem

Let n, q, and D be positive integers such that $q > 2$, $1 < r = \lceil \log_q D \rceil < \frac{n}{2}$, and $q + 2q^{r-1} < D \leq q^r$. We can reorganize the matrix associated with $\mathcal{S}$ so that it has the form



Matrix Over the Small Field



An Algorithm to Solve the System

The matrix $\tilde{M}$ is almost block diagonal, with blocks $\tilde{M}_1, \ldots, \tilde{M}_{\frac{n}{2}}$ overlapping in a few rows.

Two blocks example:

$$\tilde{M} = \begin{bmatrix} U_1 & 0 \\ L_1 & U_2 \\ 0 & L_2 \end{bmatrix}$$

- Find $\mathbf{y}_2$ in the null space of L_2
- Compute $\mathbf{r} = U_2 \mathbf{y}_2$
- Find an element $\mathbf{y}_1$ such that $\begin{bmatrix} U_1 \\ L_1 \end{bmatrix} \mathbf{y}_1 = \begin{bmatrix} 0 \\ -\mathbf{r} \end{bmatrix}$
- It is easy to see that $\tilde{M} \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} = 0$

An Algorithm to Solve the System

Finds an element in the null space of $\tilde{M}$

Input: $\tilde{M}_0, \tilde{M}_1, \ldots, \tilde{M}_{\frac{n}{2}}$, blocks of $\tilde{M}$ as above

$W := \left\{ \mathbf{z} \mid L_{\frac{n}{2}} \mathbf{z} = \mathbf{0} \right\}$
for $i = \frac{n}{2}, \ldots, 1$ **do**
  $\mathbf{y}_i \xleftarrow{\$} W$
  $\mathbf{r}_i := U_i \mathbf{y}_i$
  $W := \left\{ \mathbf{z} \mid L_i \mathbf{z} = \left[\frac{\mathbf{0}}{-\mathbf{r}_i} \right] \right\}$
  if $W = \emptyset$ **then**
    return
$W := \left\{ \mathbf{z} \mid \tilde{M}_0 \mathbf{z} = \mathbf{0} \right\}$
$\mathbf{y}_0 \xleftarrow{\$} W$
return $\mathbf{y} = [\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n}{2}}]^T$

An Algorithm to Solve the System

- The algorithms returns an element in the null space
- Every $x \in \text{Null}(\tilde{M})$ can be output by the algorithm
- The distribution of the output over the null space is uniform
- Although the algorithm may not terminate, in millions of experiments we ran, the algorithm always terminated

Complexity of the new method

- Blocks: $\frac{n}{2} + 1$
- Block size: $2n^2 \times 2n^2$
- Complexity of reducing each block: $\mathcal{O}\left(\left(n^2\right)^\omega\right)$
- Complexity of the new method: $\mathcal{O}\left(n\left(n^2\right)^\omega\right) = \mathcal{O}\left(n^{2\omega+1}\right)$
- Improves naive approach: $\mathcal{O}\left(\left(n^3\right)^\omega\right) = \mathcal{O}\left(n^{3\omega}\right)$
- Experiments confirm a significant improvement against sparse methods

		New Method			Old Method		
q	D	n	time [s]	Memory [MB]	n	time [s]	Memory [MB]
7	106	8	0.07	≤ 32	8	0.43	≤ 32
7	106	16	1.46	≤ 32	16	25.41	131
7	106	32	67.29	64	32	2285.44	3452
7	106	56	1111.26	235	55	216076.27	53619
17	106	8	0.08	≤ 32	8	0.45	≤ 32
17	106	16	2.02	68	16	26.63	160
17	106	32	122.86	93	32	2095.94	3785
17	595	56	2712.63	353	55	226384.28	59658

Remarks About Security

- Security is not affected by the proposed key generation improvement
  - The key is chosen under the same uniform distribution
- New work exposes a rank weakness on ZHFE [PS16]
  - Writing
$$\Psi = x[L_{00}F + L_{01}\tilde{F}] + x^q[L_{10}F + L_{11}\tilde{F}]$$
  - If L_{ij} are nonsingular, the Q-rank of $F||\tilde{F}$ is $\log_q(D) + 2$
  - If we select the L_{ij} maps to have reasonable corank c, then the Q-rank does not appear to be a weakness
  - They propose parameters
$108 - \mathrm{ZHFE}^- : (q, n, D, r, c) = (7, 55, 393, 2, 3)$.
- Our new algorithm works for positive corank L_{ij} maps

Conclusion and Future Work

- A novel method to construct ZHFE keys
  - Expose almost-block diagonal structure of vanishing equation system
  - Construct the matrix faster, and store it more efficiently
  - Find solutions asymptotically faster
  - Turn ZHFE into a practical Post-Quantum public key encryption scheme.
- Our new algorithm works for positive corank L_{ij} maps
- Understanding combinatorial structure of Frobenius powers of q-Hamming-weight-two univariate polynomials
  - A tool to explore a bigger family of encryption schemes
  - Fix free variables in a way that further speeds up key generation and reduces secret key size

Thanks

CryptoCO 2016

Summer School on Cryptography

Bogotá, Colombia

July 5th to 9th, 2016

Facebook/Twitter: Cryptoco2016

Bibliography I

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the HFE public key cryptosystem by relinearization.
In *Advances in cryptology—CRYPTO '99 (Santa Barbara, CA)*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, Berlin, 1999.

Jaiberth Porras, John Baena, and Jintai Ding.
New candidates for multivariate trapdoor functions.
Revista Colombiana de Matemáticas, 49:57–76, 06 2015.

Ray A. Perlner and Daniel Smith-Tone.
Security analysis and key modification for ZHFE.
In *Post-Quantum Cryptography - 7th International Conference, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016. Proceedings*, 2016.

Wenbin Zhang and Chik How Tan.
personal communication, 11 2015.

Matrix Over the Small Field

- Let $A_{ns+\ell}$ be the matrix over $\mathbb{F}$ that represents $Z \mapsto \alpha_{ns+\ell+1} Z^{q^\ell}$
- Recall that the coefficient of $X^{q^s+q^i+q^j}$ in Ψ_s is

$$\sum_{\ell=0}^{n-1} \alpha_{ns+\ell+1} Z_{2nk+(i\ominus\ell)}^{q^\ell} + \sum_{\ell=0}^{n-1} \beta_{ns+\ell+1} Z_{2nk+n+(i\ominus\ell)}^{q^\ell} \tag{1}$$

- We can see the expression in (1) as an $\mathbb{F}$-linear transformation $T_{s,i}^k : \mathbb{K}^{2n} \to \mathbb{K}$ in the variables $Z_{2nk+ns+i}$
- The matrix that represents $T_{s,i}^k$ over $\mathbb{F}$ is $[A|B]$, where

$$A = \left[\; A_{ns+i} \;\middle|\; A_{ns+i-1} \;\middle|\; \cdots \;\middle|\; A_{ns} \;\middle|\; A_{ns+n-1} \;\middle|\; \cdots \;\middle|\; A_{ns+(i+1)} \; \right],$$
$$B = \left[\; B_{ns+i} \;\middle|\; B_{ns+i-1} \;\middle|\; \cdots \;\middle|\; B_{ns} \;\middle|\; B_{ns+n-1} \;\middle|\; \cdots \;\middle|\; B_{ns+(i+1)} \; \right]$$

Matrix Over the Small Field

The matrix that represents the $\mathbb{F}$-linear transformation $T_k = (T^k_{0,0}, \cdots, T^k_{0,n-1}, T^k_{1,0}, \cdots T^k_{1,n-1})$ is

$$
\left[\begin{array}{ccccc|ccccc}
A_0 & A_{n-1} & A_{n-2} & \cdots & A_1 & B_0 & B_{n-1} & B_{n-2} & \cdots & B_1 \\
A_1 & A_0 & A_{n-1} & \cdots & A_2 & B_1 & B_0 & B_{n-1} & \cdots & B_2 \\
A_2 & A_1 & A_0 & \cdots & A_3 & B_2 & B_1 & B_0 & \cdots & B_3 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
A_{n-2} & A_{n-3} & A_{n-4} & \cdots & A_{n-1} & B_{n-2} & B_{n-3} & B_{n-4} & \cdots & B_{n-1} \\
A_{n-1} & A_{n-2} & A_{n-3} & \cdots & A_0 & B_{n-1} & B_{n-2} & B_{n-3} & \cdots & B_0 \\
\hline
A_n & A_{2n-1} & A_{2n-2} & \cdots & A_{n+1} & B_n & B_{2n-1} & B_{2n-2} & \cdots & B_{n+1} \\
A_{n+1} & A_n & A_{2n-1} & \cdots & A_{n+2} & B_{n+1} & B_n & B_{2n-1} & \cdots & B_{n+2} \\
A_{n+2} & A_{n+1} & A_n & \cdots & A_{n+3} & B_{n+2} & B_{n+1} & B_n & \cdots & B_{n+3} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
A_{2n-2} & A_{2n-3} & A_{2n-4} & \cdots & A_{2n-1} & B_{2n-2} & B_{2n-3} & B_{2n-4} & \cdots & B_{2n-1} \\
A_{2n-1} & A_{2n-2} & A_{2n-3} & \cdots & A_n & B_{2n-1} & B_{2n-2} & B_{2n-3} & \cdots & B_n
\end{array}\right]
$$