Extension Field Cancellation
A New MQ Trapdoor Construction

February 2016
Alan Szepieniec¹, Jintai Ding², Bart Preneel¹
1: KU Leuven, ESAT/COSIC
   first.secondname@esat.kuleuven.be
2: University of Cincinnati, jintai.ding@uc.edu
Outline

- Introduction
- Extension Field Cancellation
  - Basic Trapdoor
  - Frobenius Tail
- Attacks and Defenses
  - Bilinear Attack
  - Algebraic Attack – Minus
  - Differential Symmetry – Projection
- Security & Efficiency
  - Security Estimation
  - Implementation Results
- Conclusion
Multivariate Quadratic Cryptosystems

- public key: $\mathcal{P} \in (\mathbb{F}_q[x_1, \ldots, x_n])^m$
- public operation: evaluate in $\mathbf{x} \in \mathbb{F}_q^n$
- secret key: $(S, T, \mathcal{F})$ where $S \in \text{GL}_n(\mathbb{F}_q), T \in \text{GL}_m(\mathbb{F}_q), \mathcal{F} \in (\mathbb{F}_q[x_1, \ldots, x_n])^m$
  such that $\mathcal{P} = T \circ \mathcal{F} \circ S$
- private operation: invert $S, \mathcal{F}, T$ — all easy!

![Diagram](image_url)
Single-Field Schemes

- all arithmetic occurs in $\mathbb{F}_q$
- canonical example: UOV

\[
\mathcal{F}_i(o, v) = (o^T \ v^T) \tilde{s}_i \begin{pmatrix} o \\ v \end{pmatrix} = (o^T \ v^T) \begin{pmatrix} \ast & \ast \\ \ast & \ast \end{pmatrix} \begin{pmatrix} o \\ v \end{pmatrix}
\]

- invert $\mathcal{F}(o, v) = y$:
  - fix $v$ at random
  - solve $\mathcal{F}(o, v) = y$ for $o$
  - linear system!
Mixed-Field Schemes

- arithmetic occurs in $\mathbb{F}_q$ as well as in $\mathbb{F}_{q^n} \cong \mathbb{F}_q[z]/\langle p(z) \rangle$
- canonical example: HFE
- let $\varphi(x) : \mathbb{F}_q^n \to \mathbb{F}_{q^n} : x \mapsto \lambda = x_0 + x_1z + \ldots + x_{n-1}z^{n-1}$
- let $f(\lambda) = \sum_{i<d} \sum_{j<d} \alpha_{i,j} \lambda^{q^i+q^j} + \sum_{k<d} \beta_k \lambda^{q^k} + \gamma$
- $F(x) = \varphi^{-1} \circ f \circ \varphi(x)$
- or for simplicity: $F(\lambda) = f(\lambda)$
- invert $F(\lambda) = y$:
  - factorize the polynomial $F(\lambda) - y$
  - choose a root $\lambda_r$ such that $F(\lambda_r) - y = 0$
MQ Encryption Schemes

- **ZHFE**
  - mixed-field
  - 2 high-degree polynomials $F(X)$ and $\hat{F}(X)$ linked to 1 low-degree polynomial $\Psi(X)$
  - inversion: factorize $\Psi(X)$

- **ABC / Simple Matrix Encryption**
  - single-field, but embeds matrix algebra
  - reduces inversion to linear system solving

- **Extension Field Cancellation (EFC)**
  - mixed-field
  - 2 high-degree polynomials
  - reduces inversion to linear system solving

!! All three are expanding maps $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^{2n}$ !!
EFC: Basic Trapdoor

• let \( \varphi_m : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n \times n} \) map a vector \( x \in \mathbb{F}_q^n \) to the matrix representation of \( X \in \mathbb{F}_q^n \).

• let \( A, B \in \mathbb{F}_q^{n \times n} \) be matrices and
  \( \alpha(X) = \varphi(Ax), \beta(X) = \varphi(Bx) \)

• Central map:

\[
\mathcal{F} = \begin{pmatrix} \varphi_m(Ax)x \\ \varphi_m(Bx)x \end{pmatrix} = \begin{pmatrix} \alpha(X)X \\ \beta(X)X \end{pmatrix}
\]
EFC: Basic Trapdoor

Central map:

$$\mathcal{F} = \begin{pmatrix} \varphi_m(Ax)x \\ \varphi_m(Bx)x \end{pmatrix} = \begin{pmatrix} \alpha(x)x \\ \beta(x)x \end{pmatrix}$$

How to invert?

$$\mathcal{F}(x) = \begin{pmatrix} \alpha(x)x \\ \beta(x)x \end{pmatrix} = \begin{pmatrix} D_1 \\ D_2 \end{pmatrix}$$

Solution:

$$\beta(x)D_1 - \alpha(x)D_2 = 0$$

i.e., solve for $x$:

$$\varphi_m(Bx)d_1 - \varphi_m(Ax)d_2 = 0$$

which is a linear system.
Enhanced Trapdoor

- key idea: use Frobenius isomorphism
- disadvantage: restricted to characteristic 2 only

\[ \mathcal{E}(\mathcal{X}) = \begin{pmatrix} \alpha(\mathcal{X})\mathcal{X} + \beta(\mathcal{X})^3 \\ \beta(\mathcal{X})\mathcal{X} + \alpha(\mathcal{X})^3 \end{pmatrix} \]
Enhanced Trapdoor: Inversion

How to invert?

\[ \mathcal{E}(\mathcal{X}) = \begin{pmatrix} \alpha(\mathcal{X})\mathcal{X} + \beta(\mathcal{X})^3 \\ \beta(\mathcal{X})\mathcal{X} + \alpha(\mathcal{X})^3 \end{pmatrix} = \begin{pmatrix} D_1 \\ D_2 \end{pmatrix} \]

Solution: solve for \( \mathcal{X} \):

\[ \alpha(\mathcal{X})D_2 - \beta(\mathcal{X})D_1 = \alpha(\mathcal{X})^4 - \beta(\mathcal{X})^4 \]

or for \( x \):

\[ \alpha_m(x)d_2 - \beta_m(x)d_1 = Q_2(Ax - Bx) \]

where \( Q_2 \in \mathbb{F}_q^{n \times n} \) is the matrix associated with the Frobenius transform \( \mathcal{X} \mapsto \mathcal{X}^4 \).
Bilinear Attack

- basic variant: \( F(\mathcal{X}) = \begin{pmatrix} \alpha(\mathcal{X}) \mathcal{X} \\ \beta(\mathcal{X}) \mathcal{X} \end{pmatrix} = \begin{pmatrix} \mathcal{Y}_1 \\ \mathcal{Y}_2 \end{pmatrix} \)

- bilinear relation: \( \beta(\mathcal{X}) \mathcal{Y}_1 = \alpha(\mathcal{X}) \mathcal{Y}_2 \)

- there exists coefficients \( K_i, L_i \in \mathbb{F}_{q^n} \) such that

\[
\sum_{i=0}^{n-1} \mathcal{X}^{q^i} (K_i \mathcal{Y}_1 + L_i \mathcal{Y}_2) = 0
\]

- attack:
  - generate many tuples \((\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2)\)
  - compute \( K_i \) and \( L_i \) using linear algebra
  - given a ciphertext \( \mathcal{Y} = (\mathcal{Y}_1, \mathcal{Y}_2) \) and given the coefficients \( K_i, L_i \), computing \( \mathcal{X} \) is easy
Other Attacks and Defenses

- same basic idea
- protect against Bilinear Attack: minus
- protect against Algebraic Attack: more minus
- protect against Differential Symmetry Attack: projection
- $\text{EFC}_p^-, \text{EFC}_{pt^2}^-$
Algebraic Attack

- Algebraic Attack: decent Gröbner bases algorithms (e.g. $F_4$, $F_5$, MutantXL)
- Running time depends on \textit{degree of regularity}
- $D_{\text{reg}}$ depends on rank of quadratic form

\[
\mathcal{F}(\mathcal{X}) = \begin{pmatrix}
\mathcal{X}^T \tilde{\mathcal{S}}_1 \mathcal{X} \\
\mathcal{X}^T \tilde{\mathcal{S}}_2 \mathcal{X}
\end{pmatrix}
\]

where e.g.
\[
\mathcal{X}^T = (\mathcal{X}, \mathcal{X}^q, \mathcal{X}^{q^2} \ldots \mathcal{X}^{q^{n-1}})
\]
Rank of Extension Field Quadratic Form

\[ F_1 = \alpha (x) x \sim \]
rank = 2

\[ F \circ S \sim \]
rank = 2
(change of basis)

\[ T \circ F \circ S \sim \]
full rank

\[ T(x) = \sum t_i x^{q_i} \]

\[ T \circ F(x) = \sum t_i (x^T S x)^{q_i} \]
Fast Gröbner Basis

- $F_4$ implicitly recovers $T$
• solution: drop $a$ rows from $T$

• $F_4$ can only recover $n - a$ rows of $T$

• rank $r = 2 + a$

• drawback: guess $a$ values during decryption
Effect of Minus

- fixed $n = 35$
Differential Symmetry Attack

- \( D\mathcal{F}(x, y) = \mathcal{F}(x + y) - \mathcal{F}(x) - \mathcal{F}(y) + \mathcal{F}(0) \)
- symmetry \( \iff \exists \Lambda, L \cdot D\mathcal{F}(Lx, y) + D\mathcal{F}(x, Ly) = \Lambda D\mathcal{F}(x, y) \)
- broke SFLASH
- solution (pSFLASH): \( S \) must be singular and \( n \) prime
- \( \text{EFC}_p \):
  - \( \text{rank}(A) = \text{rank}(B) = n - 1 \)
  - \( n \) is prime
  - and \( \text{ker}(A) \cap \text{ker}(B) = \{0\} \)
Estimating Security

- algebraic attack: Gaussian elimination in matrix with
  \( T = \binom{n}{D_{\text{reg}}} \) monomials
- \( \tau = \binom{n}{2} \) nonzero terms per row
- complexity of Wiedemann algorithm: \( O(\tau T^2) \)

\[
D_{\text{reg}} \leq \frac{(q - 1)(r + a)}{2} + 2
\]

<table>
<thead>
<tr>
<th>( n )</th>
<th>( q )</th>
<th>( t^2 )</th>
<th>( a )</th>
<th>( D_{\text{reg}} )</th>
<th>security</th>
</tr>
</thead>
<tbody>
<tr>
<td>83</td>
<td>2</td>
<td>10</td>
<td>8</td>
<td>8</td>
<td>82</td>
</tr>
<tr>
<td>83</td>
<td>2</td>
<td>✔</td>
<td>8</td>
<td>8</td>
<td>82</td>
</tr>
<tr>
<td>59</td>
<td>3</td>
<td>6</td>
<td>10</td>
<td>8</td>
<td>82</td>
</tr>
</tbody>
</table>
Decryption Time as a Function of $a$
Algebraic Attack Time

- implementation in Magma (has $F_4$)
## Implementation Results

<table>
<thead>
<tr>
<th>construction</th>
<th>sec. key</th>
<th>pub. key</th>
<th>ctxt.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{EFC}_p^-, q = 2, n = 83, a = 10$</td>
<td>48.3 KB</td>
<td>509 KB</td>
<td>20 B</td>
</tr>
<tr>
<td>$\text{EFC}_{pt^2}^-, q = 2, n = 83, a = 8$</td>
<td>48.3 KB</td>
<td>523 KB</td>
<td>20 B</td>
</tr>
<tr>
<td>$\text{EFC}_p^-, q = 3, n = 59, a = 6$</td>
<td>48.8 KB</td>
<td>375 KB</td>
<td>28 B</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>construction</th>
<th>key gen.</th>
<th>enc.</th>
<th>dec.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{EFC}_p^-, q = 2, n = 83, a = 10$</td>
<td>2.45 s</td>
<td>0.004 s</td>
<td>9.074 s</td>
</tr>
<tr>
<td>$\text{EFC}_{pt^2}^-, q = 2, n = 83, a = 8$</td>
<td>3.982 s</td>
<td>0.004 s</td>
<td>2.481 s</td>
</tr>
<tr>
<td>$\text{EFC}_p^-, q = 3, n = 59, a = 6$</td>
<td>2.938 s</td>
<td>0.004 s</td>
<td>12.359 s</td>
</tr>
</tbody>
</table>
Conclusion

• extension field cancellation (EFC)
  • MQ mixed field trapdoor construction
  • generate a pair of high-degree quadratic polynomials
  • uses commutativity of extension field to cancel the polynomials’ complexity
  • end up with a linear system

• modifiers
  • Frobenius Tail in char 2 (speed)
  • Minus (protects against Algebraic Attack)
  • Projection (destroys Differential Symmetry)

• future work
  • get rid of Minus modifier
  • better security argument
  • shrink public keys
  • hardware implementation