Extension Field Cancellation
A New MQ Trapdoor Construction

February 2016
Alan Szepieniec\textsuperscript{1}, Jintai Ding\textsuperscript{2}, Bart Preneel\textsuperscript{1}
\textsuperscript{1}: KU Leuven, ESAT/COSIC
   first.secondname@esat.kuleuven.be
\textsuperscript{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 $x \in \mathbb{F}_q^m$
- 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!

```
encryption or signature verification

\[ \mathcal{P} \]

public knowledge
private knowledge

decryption or signature generation
```
Single-Field Schemes

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

$$\mathcal{F}_i(o, v) = (o^T \ v^T) \bar{\mathcal{F}}_i \begin{pmatrix} o \\ v \end{pmatrix} = (o^T \ v^T) \begin{pmatrix} 1 & \ldots & 1 \\ 1 & \ldots & 1 \end{pmatrix} \begin{pmatrix} o \\ v \end{pmatrix}$$

- 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 $\varphi(x) : \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^n} : x \mapsto x = x_0 + x_1 z + \ldots x_{n-1} z^{n-1}$
• let $f(x) = \sum_{i<d} \sum_{j<d} \alpha_{i,j} x^{q^i+q^j} + \sum_{k<d} \beta_k x^{q^k} + \gamma$
• $F(x) = \varphi^{-1} \circ f \circ \varphi(x)$
• or for simplicity: $F(x) = f(x)$
• invert $F(x) = y$:
  • factorize the polynomial $F(x) - y$
  • choose a root $x_r$ such that $F(x_r) - y = 0$
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:

$$F = \begin{pmatrix} \varphi_m(Ax)x \\ \varphi_m(Bx)x \end{pmatrix} = \begin{pmatrix} \alpha(X)X \\ \beta(X)X \end{pmatrix}$$
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 \textit{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: \( \mathcal{F}(\mathcal{X}) = \begin{pmatrix} \alpha(\mathcal{X}) \mathcal{X} \\ \beta(\mathcal{X}) \mathcal{X} \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} \)

- bilinear relation: \( \beta(\mathcal{X}) Y_1 = \alpha(\mathcal{X}) Y_2 \)

- there exists coefficients \( K_i, L_i \in \mathbb{F}_{q^n} \) such that
  \[
  \sum_{i=0}^{n-1} \mathcal{X}^{q^i} (K_i Y_1 + L_i Y_2) = 0
  \]

- attack:
  - generate many tuples \((\mathcal{X}, Y_1, Y_2)\)
  - compute \(K_i\) and \(L_i\) using linear algebra
  - given a ciphertext \( \mathcal{Y} = (Y_1, Y_2) \) 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
• $EFC_p^-, EFC_{pt^2}^-$
Algebraic Attack

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

\[
\mathcal{F}(\mathcal{X}) = \begin{pmatrix} \mathcal{X}^T \mathcal{F}_1 \mathcal{X} \\ \mathcal{X}^T \mathcal{F}_2 \mathcal{X} \end{pmatrix} \quad \text{where e.g.} \quad \mathcal{X}^T = (\mathcal{X}, \mathcal{X}^q, \mathcal{X}^{q^2} \ldots \mathcal{X}^{q^{n-1}})
Rank of Extension Field Quadratic Form

\[ F_1 = \alpha(X)X \sim \text{rank } = 2 \]

\[ F \circ S \sim \text{rank } = 2 \quad \text{(change of basis)} \]

\[ T \circ F \circ S \sim \text{full rank} \]

\[
T(X) = \sum t_i X^{q^i}
\]

\[
T \circ F(X) = \sum t_i (X^T \Phi X)^{q^i}
\]
• $F_4$ 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 $n = 35$
Decryption Errors

The graph shows the relationship between the error rate and the parameter $n$, for different values of $a$. The error rate decreases as $n$ increases, indicating a lower probability of decryption errors for larger values of $n$. Each curve represents a different value of $a$, with $a = 0$, $a = 2$, $a = 4$, $a = 6$, $a = 8$, and $a = 10$, $a = 12$.
Differential Symmetry Attack

\[ DF(x, y) = F(x + y) - F(x) - F(y) + F(0) \]

symmetry \( \Leftrightarrow \exists \Lambda, L . DF(Lx, y) + DF(x, Ly) = \Lambda DF(x, y) \)

broke SFLASH

solution (pSFLASH): \( S \) must be singular and \( n \) prime

EFC\(_p\):
  - \( \text{rank}(A) = \text{rank}(B) = n - 1 \)
  - \( n \) is prime
  - and \( \ker(A) \cap \ker(B) = \{0\} \)
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>$\text{EFC}^{-}_{pt2}, q = 2, n = 83, a = 8$</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>$\text{EFC}^{-}_{pt2}, q = 2, n = 83, a = 8$</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