



# Extension Field Cancellation

A New MQ Trapdoor Construction

February 2016

**Alan Szepieniec**<sup>1</sup>, Jintai Ding<sup>2</sup>, Bart Preneel<sup>1</sup>

1: KU Leuven, ESAT/COSIC

`first.secondname@esat.kuleuven.be`

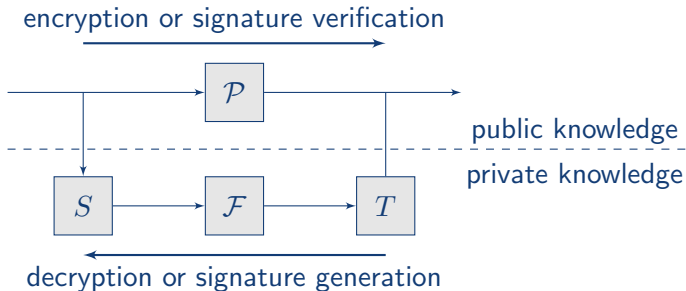
2: University of Cincinnati, `jintai.ding@uc.edu`

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



## Single-Field Schemes

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

- $\mathcal{F}_i(\mathbf{o}, \mathbf{v}) = (\mathbf{o}^\top \quad \mathbf{v}^\top) \tilde{\mathfrak{F}}_i \begin{pmatrix} \mathbf{o} \\ \mathbf{v} \end{pmatrix} = (\mathbf{o}^\top \quad \mathbf{v}^\top) \begin{pmatrix} \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare \end{pmatrix} \begin{pmatrix} \mathbf{o} \\ \mathbf{v} \end{pmatrix}$

- invert  $\mathcal{F}(\mathbf{o}, \mathbf{v}) = \mathbf{y}$ :
  - fix  $\mathbf{v}$  at random
  - solve  $\mathcal{F}(\mathbf{o}, \mathbf{v}) = \mathbf{y}$  for  $\mathbf{o}$
  - 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  $\varphi(\mathbf{x}) : \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^n} : \mathbf{x} \mapsto \mathcal{X} = x_0 + x_1z + \dots + x_{n-1}z^{n-1}$
- let  $f(\mathcal{X}) = \sum_{i < d} \sum_{j < d} \alpha_{i,j} \mathcal{X}^{q^i + q^j} + \sum_{k < d} \beta_k \mathcal{X}^{q^k} + \gamma$
- $\mathcal{F}(\mathbf{x}) = \varphi^{-1} \circ f \circ \varphi(\mathbf{x})$
- or for simplicity:  $\mathcal{F}(\mathcal{X}) = f(\mathcal{X})$
- invert  $\mathcal{F}(\mathcal{X}) = \mathcal{Y}$ :
  - factorize the polynomial  $\mathcal{F}(\mathcal{X}) - \mathcal{Y}$
  - choose a root  $\mathcal{X}_r$  such that  $\mathcal{F}(\mathcal{X}_r) - \mathcal{Y} = 0$

# MQ Encryption Schemes

- ZHFE
  - mixed-field
  - 2 high-degree polynomials  $\mathcal{F}(\mathcal{X})$  and  $\hat{\mathcal{F}}(\mathcal{X})$  linked to 1 low-degree polynomial  $\Psi(\mathcal{X})$
  - inversion: factorize  $\Psi(\mathcal{X})$
- 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  $\mathbf{x} \in \mathbb{F}_q^n$  to the matrix representation of  $\mathcal{X} \in \mathbb{F}_{q^n}$ .
- let  $A, B \in \mathbb{F}_q^{n \times n}$  be matrices and  $\alpha(\mathcal{X}) = \varphi(A\mathbf{x})$ ,  $\beta(\mathcal{X}) = \varphi(B\mathbf{x})$
- Central map:

$$\mathcal{F} = \begin{pmatrix} \varphi_m(A\mathbf{x})\mathbf{x} \\ \varphi_m(B\mathbf{x})\mathbf{x} \end{pmatrix} = \begin{pmatrix} \alpha(\mathcal{X})\mathcal{X} \\ \beta(\mathcal{X})\mathcal{X} \end{pmatrix}$$

## EFC: Basic Trapdoor

Central map:

$$\mathcal{F} = \begin{pmatrix} \varphi_m(A\mathbf{x})\mathbf{x} \\ \varphi_m(B\mathbf{x})\mathbf{x} \end{pmatrix} = \begin{pmatrix} \alpha(\mathcal{X})\mathcal{X} \\ \beta(\mathcal{X})\mathcal{X} \end{pmatrix}$$

How to invert?

$$\mathcal{F}(\mathcal{X}) = \begin{pmatrix} \alpha(\mathcal{X})\mathcal{X} \\ \beta(\mathcal{X})\mathcal{X} \end{pmatrix} = \begin{pmatrix} \mathcal{D}_1 \\ \mathcal{D}_2 \end{pmatrix}$$

Solution:

$$\beta(\mathcal{X})\mathcal{D}_1 - \alpha(\mathcal{X})\mathcal{D}_2 = 0$$

*i.e.*, solve for  $\mathbf{x}$ :

$$\varphi_m(B\mathbf{x})\mathbf{d}_1 - \varphi_m(A\mathbf{x})\mathbf{d}_2 = 0$$

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?

$$\mathcal{E}(\mathcal{X}) = \begin{pmatrix} \alpha(\mathcal{X})\mathcal{X} + \beta(\mathcal{X})^3 \\ \beta(\mathcal{X})\mathcal{X} + \alpha(\mathcal{X})^3 \end{pmatrix} = \begin{pmatrix} \mathcal{D}_1 \\ \mathcal{D}_2 \end{pmatrix}$$

Solution: solve for  $\mathcal{X}$ :

$$\alpha(\mathcal{X})\mathcal{D}_2 - \beta(\mathcal{X})\mathcal{D}_1 = \alpha(\mathcal{X})^4 - \beta(\mathcal{X})^4$$

or for  $\mathbf{x}$ :

$$\alpha_m(\mathbf{x})\mathbf{d}_2 - \beta_m(\mathbf{x})\mathbf{d}_1 = Q_2(A\mathbf{x} - B\mathbf{x})$$

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:  $\mathcal{F}(\mathcal{X}) = \begin{pmatrix} \alpha(\mathcal{X})\mathcal{X} \\ \beta(\mathcal{X})\mathcal{X} \end{pmatrix} = \begin{pmatrix} \mathcal{Y}_1 \\ \mathcal{Y}_2 \end{pmatrix}$
- 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
- $EFC_p^-$ ,  $EFC_{pt^2}^-$

## 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

$$\mathcal{F}(\mathcal{X}) = \begin{pmatrix} \mathcal{X}^T \mathfrak{F}_1 \mathcal{X} \\ \mathcal{X}^T \mathfrak{F}_2 \mathcal{X} \end{pmatrix} \quad \text{where e.g. } \mathcal{X}^T = (\mathcal{X}, \mathcal{X}^q, \mathcal{X}^{q^2} \dots \mathcal{X}^{q^{n-1}})$$

## Rank of Extension Field Quadratic Form

$$\mathcal{F}_1 = \alpha(\mathcal{X})\mathcal{X} \sim$$



rank = 2

$$\mathcal{F} \circ S \sim$$



rank = 2

(change of basis)

$$T \circ \mathcal{F} \circ S \sim$$



full rank

$$T(\mathcal{X}) = \sum t_i \mathcal{X}^{q^i}$$

$$T \circ \mathcal{F}(\mathcal{X}) = \sum t_i (\mathbf{x}^\top \mathfrak{F} \mathbf{x})^{q^i}$$

## Fast Gröbner Basis



- $F_4$  implicitly recovers  $T$

# Minus

- solution: drop  $a$  rows from  $T$
- $F_4$  can only recover  $n - a$  rows of  $T$

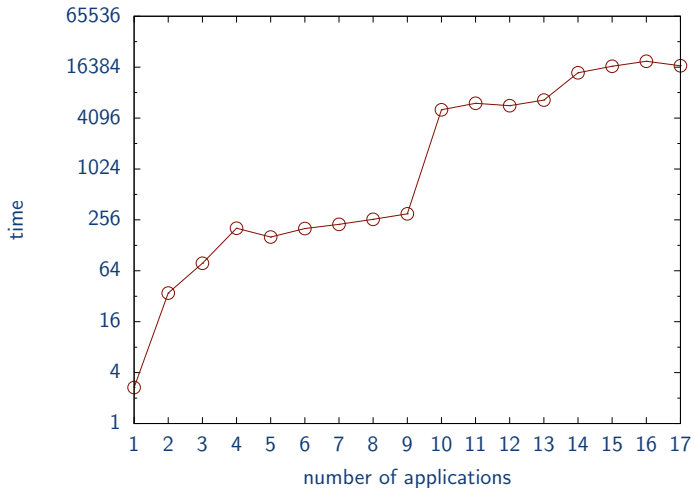


- rank  $r = 2 + a$
- drawback: guess  $a$  values during decryption

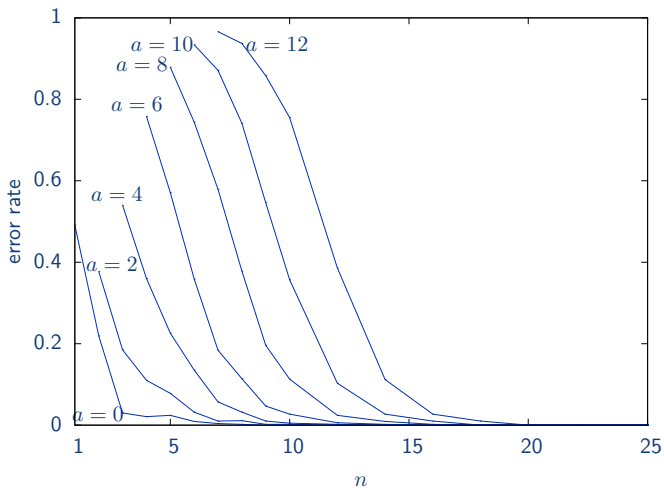


## Effect of Minus

- fixed  $n = 35$



# Decryption Errors



# Differential Symmetry Attack

- $D\mathcal{F}(\mathbf{x}, \mathbf{y}) = \mathcal{F}(\mathbf{x} + \mathbf{y}) - \mathcal{F}(\mathbf{x}) - \mathcal{F}(\mathbf{y}) + \mathcal{F}(\mathbf{0})$
- symmetry  $\Leftrightarrow \exists \Lambda, L . D\mathcal{F}(L\mathbf{x}, \mathbf{y}) + D\mathcal{F}(\mathbf{x}, L\mathbf{y}) = \Lambda D\mathcal{F}(\mathbf{x}, \mathbf{y})$
- 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  $\ker(A) \cap \ker(B) = \{\mathbf{0}\}$

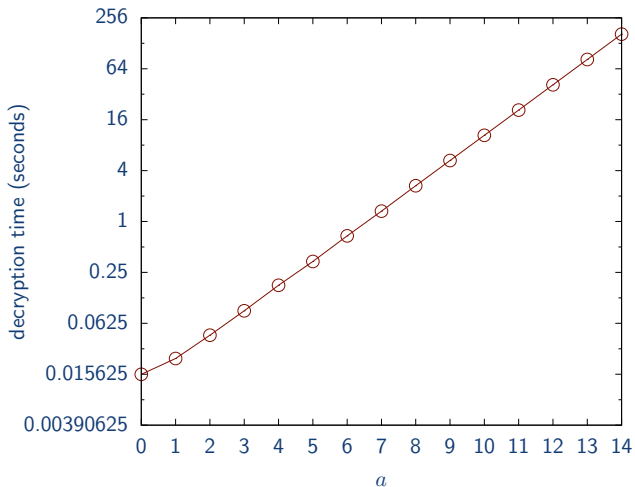
## Estimating Security

- 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:  $O(\tau T^2)$
- 

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

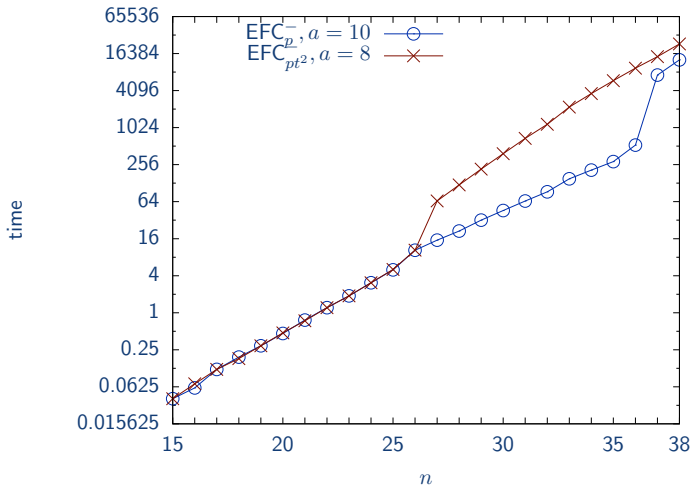
$n$	$q$	$t^2$	$a$	$D_{\text{reg}}$	security
83	2		10	8	82
83	2	✓	8	8	82
59	3		6	10	82

## Decryption Time as a Function of $a$



# Algebraic Attack Time

- implementation in Magma (has  $F_4$ )



## Implementation Results

construction	sec. key	pub. key	ctxt.
$EFC_p^-, q = 2, n = 83, a = 10$	48.3 KB	509 KB	20 B
$EFC_{pt^2}^-, q = 2, n = 83, a = 8$	48.3 KB	523 KB	20 B
$EFC_p^-, q = 3, n = 59, a = 6$	48.8 KB	375 KB	28 B

construction	key gen.	enc.	dec.
$EFC_p^-, q = 2, n = 83, a = 10$	2.45 s	0.004 s	9.074 s
$EFC_{pt^2}^-, q = 2, n = 83, a = 8$	3.982 s	0.004 s	2.481 s
$EFC_p^-, q = 3, n = 59, a = 6$	2.938 s	0.004 s	12.359 s

## 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