NTNU
Norwegian University of
Science and Technology

"Ss. Cyril and Methodius" University in Skopje
FACULTY OF COMPUTER
SCIENCE AND ENGINEERING

A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems

Jean-Charles Faugère, Danilo Gligoroski, Ludovic Perret, Simona Samardjiska, Enrico Thomae

Department of Telematics, NTNU, Norway
FCSE, UKIM, Macedonia
simonas@item.ntnu.no

Contributions

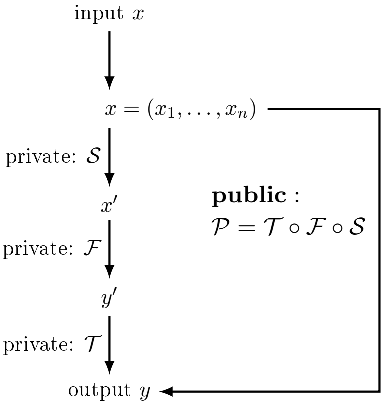
- **Cryptanalysis** of MQQ cryptosystems
  - **MQQ-SIG**
  - **MQQ-ENC**
- **Pitfalls of MinRank and Good Keys attacks**
  - Even characteristic fields
  - Complexity bounds independent of the field size

Contributions

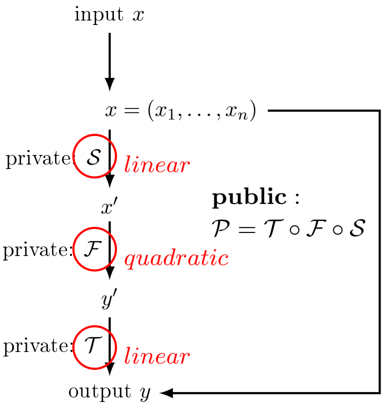
- **Cryptanalysis** of MQQ cryptosystems
  - **MQQ-SIG**
  - **MQQ-ENC**

- **Pitfalls of MinRank and Good Keys attacks**
  - Even characteristic fields
  - Complexity bounds independent of the field size

Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



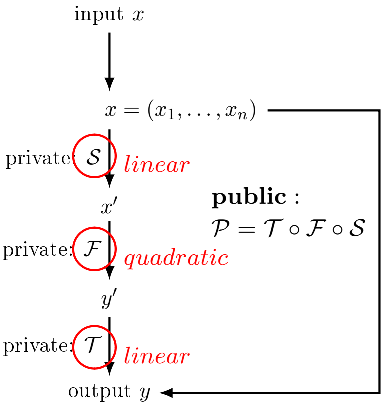
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



Matrix form: Public $\mathcal{P}$ - $x^\intercal \mathfrak{P}^{(s)} x$

Private $\mathcal{F}$ - $x^\intercal \mathfrak{F}^{(s)} x$

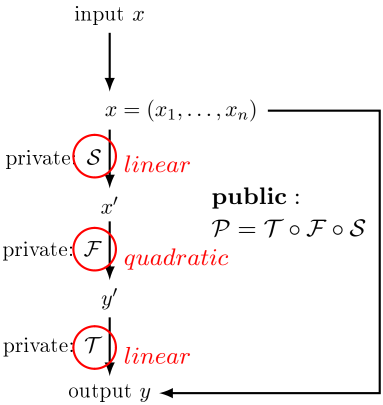
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$



inverting $\mathcal{P}$ should be hard
- underlying NP-problem -
PoSSo

Matrix form: Public $\mathcal{P}$ - $x^\intercal \mathfrak{P}^{(s)} x$
Private $\mathcal{F}$ - $x^\intercal \mathfrak{F}^{(s)} x$

Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



inverting $\mathcal{P}$ should be hard
- underlying NP-problem -
PoSSo

Post-Quantum secure

Matrix form: Public $\mathcal{P}$ - $x^\intercal \mathfrak{P}^{(s)} x$
Private $\mathcal{F}$ - $x^\intercal \mathfrak{F}^{(s)} x$

Crucial for the security of $\mathcal{MQ}$ schemes

- **MinRank**
- **Equivalent keys/Good keys**

Underlay the security of

- HFE, STS, Rainbow, ... and many more

Crucial for the security of $\mathcal{MQ}$ schemes

- **MinRank**
- **Equivalent keys/Good keys**

Underlay the security of

- HFE, STS, Rainbow, ... and many more

MinRank $MR(n, r, k, M_1, \ldots, M_k)$

Input: $n, m, r, k \in \mathbb{N}$, where $n < m$ and $M_0, M_1, \ldots, M_k \in \mathcal{M}_{n \times m}(\mathbb{F}_q)$.
Question: Find – if any – a k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k \setminus \{(0, 0, \ldots, 0)\}$ such that:

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i - M_0\right) \leqslant r.$$

Kipnis-Shamir Modeling:

$$\begin{pmatrix} 1 & & & x_{1,1} & \cdots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{n-r,1} & \cdots & x_{n-r,r} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i M_i - M_0\right) = \mathbf{0}_{n \times n}.$$

MinRank $MR(n, r, k, M_1, \ldots, M_k)$

Input: $n, m, r, k \in \mathbb{N}$, where $n < m$ and $M_0, M_1, \ldots, M_k \in \mathcal{M}_{n\times m}(\mathbb{F}_q)$.
Question: Find – if any – a k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k \setminus \{(0, 0, \ldots, 0)\}$ such that:

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i \, M_i - M_0\right) \leqslant r.$$

Kipnis-Shamir Modeling:

$$\begin{pmatrix} 1 & & & x_{1,1} & \ldots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{n-r,1} & \ldots & x_{n-r,r} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i \, M_i - M_0\right) = \mathbf{0}_{n\times n}.$$

Equivalent Keys/Good Keys

$$
\begin{aligned}
\mathcal{P} &= \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} \Leftrightarrow \\
\mathcal{P} &= \underbrace{\mathcal{T} \circ \Sigma^{-1}}_{\mathcal{T}'} \circ \underbrace{\Sigma \circ \mathcal{F} \circ \Omega}_{\mathcal{F}'} \circ \underbrace{\Omega^{-1} \circ \mathcal{S}}_{\mathcal{S}'} \Leftrightarrow \\
\mathcal{P} &= \mathcal{T}' \circ \mathcal{F}' \circ \mathcal{S}'
\end{aligned}
$$

- **Equivalent Keys** - preserve all structure
- **Good Keys** - preserve some structure

Equivalent Keys/Good Keys

UOV

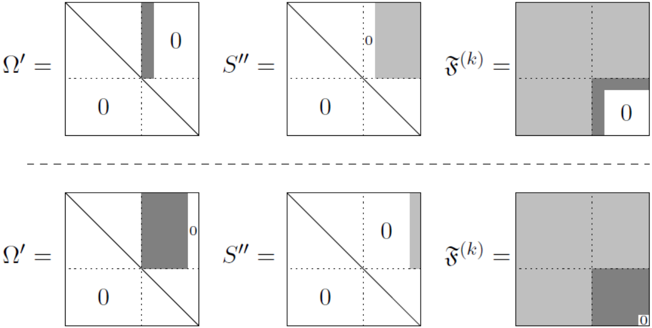
$$\mathfrak{F}^{(k)} = \begin{array}{c} \begin{array}{ccccc} x_1 & \cdots & x_v & \cdots & x_n \end{array} \\ \left[\begin{array}{c:c} & \\ \hdashline & 0 \end{array}\right] \end{array} \begin{array}{l} \left.\begin{array}{c} x_1 \\ \vdots \\ x_v \end{array}\right\} \text{vinegar variables} \\ \left.\begin{array}{c} \vdots \\ x_n \end{array}\right\} \text{oil variables} \end{array}$$

$$\Omega^{-1} \cdot S = \begin{array}{cc} v & m \\ \hline \Omega^{(1)} & 0 \\ \Omega^{(2)} & \Omega^{(3)} \end{array} \begin{array}{c} \\ v \\ m \end{array} \cdot \begin{array}{cc} v & m \\ \hline S^{(1)} & S^{(2)} \\ S^{(3)} & S^{(4)} \end{array} \begin{array}{c} \\ v \\ m \end{array} = \begin{array}{cc} v & m \\ \hline \diagdown & S'^{(1)} \\ 0 & \diagdown \end{array} \begin{array}{c} \\ v \\ m \end{array} = S'$$

Equivalent Key for UOV

Equivalent Keys/Good Keys

UOV



Good Keys for UOV

The MQQ family of cryptosystems

- **MQQ (Multivariate Quadratic Quasigroups)** [GMK08]
  - Encryption scheme
  - The private $\mathcal{F}$ - quasigroup string transformations of MQQs

Quasigroup: $\mathfrak{q} : \mathbb{F}_q^d \times \mathbb{F}_q^d \rightarrow \mathbb{F}_q^d$

$$\forall \overline{u}, \overline{v} \in Q, \exists! \, \overline{x}, \overline{y} \in Q : \quad \mathfrak{q}(\overline{u}, \overline{x}) = \overline{v}, \quad \mathfrak{q}(\overline{y}, \overline{u}) = \overline{v}.$$

  - Direct algebraic attack using Gröbner bases (small degree of regularity)

The MQQ family of cryptosystems

- **MQQ (Multivariate Quadratic Quasigroups)** [GMK08]
  - Encryption scheme
  - The private $\mathcal{F}$ - quasigroup string transformations of MQQs

    Quasigroup: $\mathfrak{q} : \mathbb{F}_q^d \times \mathbb{F}_q^d \to \mathbb{F}_q^d$

    $$\forall\, \overline{u}, \overline{v} \in Q, \exists!\, \overline{x}, \overline{y} \in Q : \quad \mathfrak{q}(\overline{u}, \overline{x}) = \overline{v}, \quad \mathfrak{q}(\overline{y}, \overline{u}) = \overline{v}.$$

  - Direct algebraic attack using Gröbner bases (small degree of regularity)

The MQQ family of cryptosystems

- **MQQ (Multivariate Quadratic Quasigroups)** [GMK08]
  - Encryption scheme
  - The private $\mathcal{F}$ - quasigroup string transformations of MQQs

    Quasigroup: $\mathfrak{q} : \mathbb{F}_q^d \times \mathbb{F}_q^d \to \mathbb{F}_q^d$

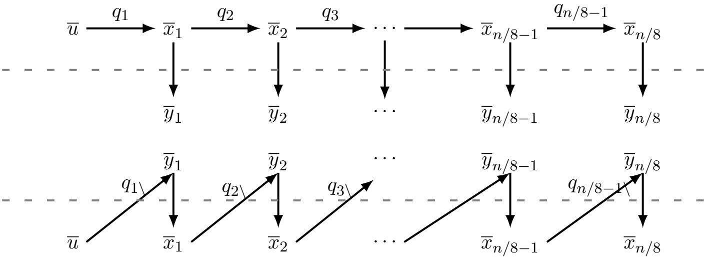
    $$\forall\, \overline{u}, \overline{v} \in Q, \exists!\, \overline{x}, \overline{y} \in Q : \quad \mathfrak{q}(\overline{u}, \overline{x}) = \overline{v}, \quad \mathfrak{q}(\overline{y}, \overline{u}) = \overline{v}.$$

  - Direct algebraic attack using Gröbner bases (small degree of regularity)

The central map of the MQQ cryptosystems

The central $\mathcal{F}$:

$$
\begin{array}{llll}
(f_1, & \ldots, & f_d\ ) & := \mathfrak{q}_1(\overline{u}, \overline{x}_1), \\
(f_{d+1}, & \ldots, & f_{2d}) & := \mathfrak{q}_2(\overline{x}_1, \overline{x}_2), \\
 & \vdots & & \qquad \vdots \\
(f_{(\ell-1)d+1}, & \ldots, & f_{\ell d}) & := \mathfrak{q}_\ell(\overline{x}_{\ell-1}, \overline{x}_\ell).
\end{array}
$$



The MQQ family of cryptosystems

- **MQQ-SIG** [GØJPFKM11]
  - signature scheme
  - **fastest on (eBACS) SUPERCOP**
  - $n/2$ equations removed - measure against the attack
  - **Recommended parameters:** $n \in \{160, 192, 224, 256\}$ **for security levels of** 2^{80}, 2^{96}, 2^{112}, 2^{128}**, respectively.**

- **MQQ-ENC** [GS12]
  - Encryption scheme
  - light use of minus modifier
  - Left MQQs - less structure
  - **Recommended parameters for security level of** 2^{128}**:** $(n, k, r) \in \{(256, 1, 8), (128, 2, 4), (64, 4, 4), (32, 8, 1)\}$.

The MQQ family of cryptosystems

- **MQQ-SIG** [GØJPFKM11]
  - signature scheme
  - **fastest on (eBACS) SUPERCOP**
  - $n/2$ equations removed - measure against the attack
  - **Recommended parameters:** $n \in \{160, 192, 224, 256\}$ **for security levels of** 2^{80}, 2^{96}, 2^{112}, 2^{128}, **respectively.**

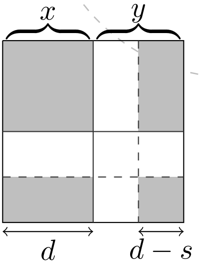
- **MQQ-ENC** [GS12]
  - Encryption scheme
  - light use of minus modifier
  - Left MQQs - less structure
  - **Recommended parameters for security level of** 2^{128}**:** $(n, k, r) \in \{(256, 1, 8), (128, 2, 4), (64, 4, 4), (32, 8, 1)\}$.

The Left MQQs in MQQ-ENC (MQQ-SIG)

$$\mathfrak{q} = (\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_d) : \mathbb{F}_{2^k}^{2d} \rightarrow \mathbb{F}_{2^k}^{d}$$

$$\begin{aligned}
\mathfrak{q}_s \quad &= \quad p_s(y_s) + \sum_{1 \leq i,j \leq d} \alpha_{i,j}^{(s)} x_i x_j \\
&+ \quad \sum_{s < i,j \leq d} \beta_{i,j}^{(s)} y_i y_j + \sum_{1 \leq i \leq d, s < j \leq d} \gamma_{i,j}^{(s)} x_i y_j \\
&+ \quad \sum_{1 \leq i \leq d} \delta_i^{(s)} x_i + \sum_{s < i \leq d} \epsilon_i^{(s)} y_i + \eta^{(s)},
\end{aligned}$$

$\mathfrak{Q}^{(s)} =$



where $p_s(y_s) \in \{a^{(s)} y_s, a^{(s)} y_s^2\}$,
for all $s, 1 \leq s \leq d$.

$$\hat{\mathfrak{q}}(\overline{x}, \overline{y}) := D \cdot \mathfrak{q}(\overline{x}, D_y \cdot \overline{y} + \overline{c}_y) + \overline{c}$$

$D,\ D_y \in \mathrm{GL}_d(\mathbb{F}_{2^k})$, $\overline{c}, \overline{c}_y$ – vectors of dimension d.

Crucial observation about the algebraic structure

$$\mathcal{P} = \quad \mathcal{T} \quad \circ \quad \mathcal{F} \quad \circ \quad \mathcal{S} \quad \Leftrightarrow$$
$$[D \cdot \mathfrak{q}(\overline{x}, D_y \cdot \overline{y} + \overline{c}_y) + \overline{c}]$$

$$\mathcal{P} = \quad T \quad \circ \quad \mathcal{F} \quad \circ \quad S \quad \Leftrightarrow$$
$$[D \cdot \mathfrak{q}(\overline{x}, D_y \cdot \overline{y})]$$

$$\mathcal{P} = \quad T \cdot (I_{\frac{n}{d}} \otimes D) \quad \circ \quad \mathcal{F}' \quad \circ \quad S \quad \Leftrightarrow$$
$$[\mathfrak{q}(\overline{x}, D_y \cdot \overline{y})]$$

$$\mathcal{P} = \quad T \cdot (I_{\frac{n}{d}} \otimes D) \quad \circ \quad \mathcal{F}'' \quad \circ \quad (I_{\frac{n}{d}} \otimes D_y^{-1}) \cdot S$$
$$[\mathfrak{q}(D_y^{-1}\overline{x}, \overline{y}) = \tilde{\mathfrak{q}}(\overline{x}, \overline{y})]$$

Crucial observation about the algebraic structure

$$\mathcal{P} = \quad \mathcal{T} \quad \circ \quad \mathcal{F} \quad \circ \quad \mathcal{S} \quad \Leftrightarrow$$

$$[D \cdot \mathfrak{q}(\overline{x}, D_y \cdot \overline{y} + \overline{c}_y) + \overline{c}]$$

$$\mathcal{P} = \quad T \quad \circ \quad \mathcal{F} \quad \circ \quad S \quad \Leftrightarrow$$

$$[D \cdot \mathfrak{q}(\overline{x}, D_y \cdot \overline{y})]$$

$$\mathcal{P} = \quad T \cdot (I_{\frac{n}{d}} \otimes D) \quad \circ \quad \mathcal{F}' \quad \circ \quad S \quad \Leftrightarrow$$

$$[\mathfrak{q}(\overline{x}, D_y \cdot \overline{y})]$$

$$\mathcal{P} = \quad T \cdot (I_{\frac{n}{d}} \otimes D) \quad \circ \quad \mathcal{F}'' \quad \circ \quad (I_{\frac{n}{d}} \otimes D_y^{-1}) \cdot S$$

$$[\mathfrak{q}(D_y^{-1}\overline{x}, \overline{y}) = \tilde{\mathfrak{q}}(\overline{x}, \overline{y})]$$

Crucial observation about the algebraic structure

$$\mathcal{P} = \mathcal{T} \circ \underset{[D\cdot\mathfrak{q}(\overline{x}, D_y\cdot\overline{y}+\overline{c}_y)+\overline{c}]}{\mathcal{F}} \circ \mathcal{S} \Leftrightarrow$$

$$\mathcal{P} = T \circ \underset{[D\cdot\mathfrak{q}(\overline{x}, D_y\cdot\overline{y})]}{\mathcal{F}} \circ S \Leftrightarrow$$

$$\mathcal{P} = T\cdot(I_{\frac{n}{d}}\otimes D) \circ \underset{[\mathfrak{q}(\overline{x}, D_y\cdot\overline{y})]}{\mathcal{F}'} \circ S \Leftrightarrow$$

$$\mathcal{P} = T\cdot(I_{\frac{n}{d}}\otimes D) \circ \underset{[\mathfrak{q}(D_y^{-1}\overline{x}, \overline{y}) = \tilde{\mathfrak{q}}(\overline{x}, \overline{y})]}{\mathcal{F}''} \circ (I_{\frac{n}{d}}\otimes D_y^{-1})\cdot S$$

Crucial observation about the algebraic structure

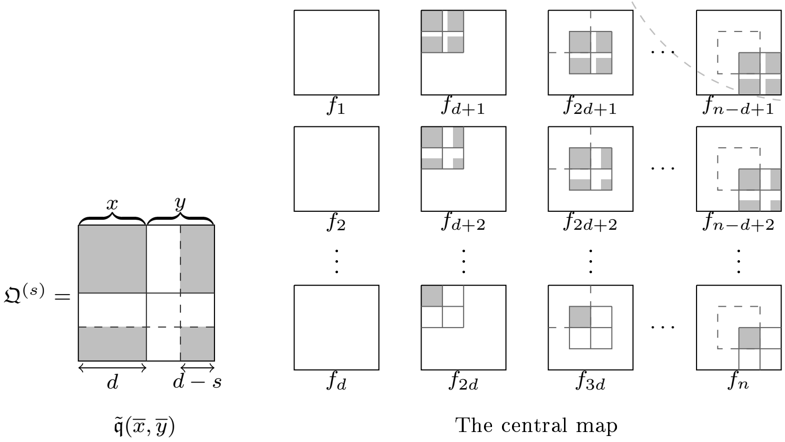
$$\mathcal{P} = \quad \mathcal{T} \quad \circ \quad \underset{[D\cdot\mathfrak{q}(\overline{x}, D_y\cdot\overline{y}+\overline{c}_y)+\overline{c}]}{\mathcal{F}} \quad \circ \quad \mathcal{S} \quad \Leftrightarrow$$

$$\mathcal{P} = \quad T \quad \circ \quad \underset{[D\cdot\mathfrak{q}(\overline{x}, D_y\cdot\overline{y})]}{\mathcal{F}} \quad \circ \quad S \quad \Leftrightarrow$$

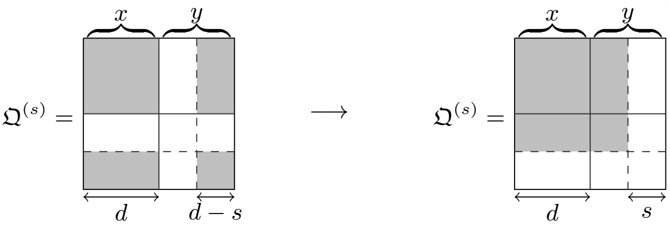
$$\mathcal{P} = \quad T\cdot(I_{\frac{n}{d}}\otimes D) \quad \circ \quad \underset{[\mathfrak{q}(\overline{x}, D_y\cdot\overline{y})]}{\mathcal{F}'} \quad \circ \quad S \quad \Leftrightarrow$$

$$\mathcal{P} = \quad T\cdot(I_{\frac{n}{d}}\otimes D) \quad \circ \quad \underset{[\mathfrak{q}(D_y^{-1}\overline{x}, \overline{y})=\tilde{\mathfrak{q}}(\overline{x}, \overline{y})]}{\mathcal{F}''} \quad \circ \quad (I_{\frac{n}{d}}\otimes D_y^{-1})\cdot S$$

Crucial observation about the algebraic structure



A simplification



Key Recovery Attack

Algorithm 1 High Level Description – Key-Recovery Attack

Input: $n - r$ public polynomials $\mathcal{P}$ in n variables.

for $N := n$ down to $r + 2$ do

Consider that all public polynomials involve $\leq N$ variables.

Step N**:**

Find a good key $(\overline{S}'_N, \overline{T}'_N)$.

Transform the public key as $\mathcal{P} \leftarrow \overline{T}'_N \circ \mathcal{P} \circ \overline{S}'_N$,

and if $N < n$ remove the first polynomial from $\mathcal{P}$.

end for;

Output: The equivalent key

$$\overline{S}' = \overline{S}'_n \circ \cdots \circ \overline{S}'_{r+2} \text{ and } \overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_n.$$

Key Recovery Attack

Algorithm 1 High Level Description – Key-Recovery Attack

Input: $n-r$ public polynomials $\mathcal{P}$ in n variables.

for $N := n$ down to $r+2$ do

Consider that all public polynomials involve $\leq N$ variables.

Step N**:**

Find a good key $(\overline{S}'_N, \overline{T}'_N)$.

Transform the public key as $\mathcal{P} \leftarrow \overline{T}'_N \circ \mathcal{P} \circ \overline{S}'_N$,

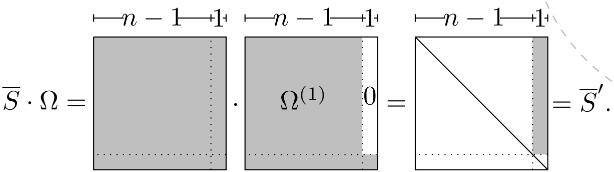
and if $N < n$ remove the first polynomial from $\mathcal{P}$.

end for;

Output: The equivalent key

$\overline{S}' = \overline{S}'_n \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_n$.

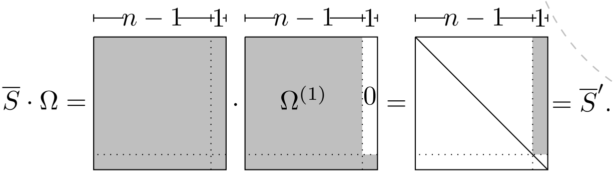
Finding a good key $(\overline{S}'_n, \overline{T}'_n)$



- Note that x_n does not appear quadratically
  $\Rightarrow$ We can take $\overline{T}'_n = I$
- A good key $\overline{S}'_n$ exists only if $\overline{S}_{nn} \neq 0$.
  $\Rightarrow$ Randomization: $\mathfrak{P}^{(i)}_{rand} := S^{\intercal}_{rand} \mathfrak{P}^{(i)} S_{rand}$
- **Solve:** ($m(n-1)$ linear equations in $(n-1)$ variables)

$$\sum_{y=1}^{n} \mathfrak{P}^{(k)}_{yj} \overline{s}'_{y,n} = 0, \quad \forall 1 \leq k \leq m, 1 \leq j < n.$$

Finding a good key $(\overline{S}'_n, \overline{T}'_n)$

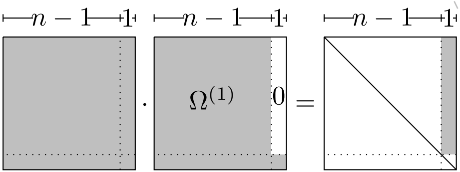


- Note that x_n does not appear quadratically
  $\Rightarrow$ We can take $\overline{T}'_n = I$
- A good key $\overline{S}'_n$ exists only if $\overline{S}_{nn} \neq 0$.
  $\Rightarrow$ Randomization: $\mathfrak{P}^{(i)}_{rand} := S^{\intercal}_{rand}\mathfrak{P}^{(i)}S_{rand}$
- **Solve:** $(m(n-1)$ linear equations in $(n-1)$ variables)

$$\sum_{y=1}^{n} \mathfrak{P}^{(k)}_{yj}\overline{s}'_{y,n} = 0, \quad \forall 1 \leq k \leq m, 1 \leq j < n.$$

Finding a good key $(\overline{S}'_n, \overline{T}'_n)$

$\overline{S} \cdot \Omega =$



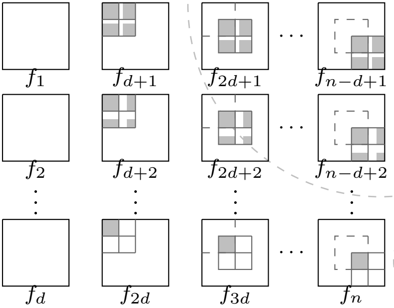
$= \overline{S}'.$

- Note that x_n does not appear quadratically
  $\Rightarrow$ We can take $\overline{T}'_n = I$
- A good key $\overline{S}'_n$ exists only if $\overline{S}_{nn} \neq 0$.
  $\Rightarrow$ Randomization: $\mathfrak{P}^{(i)}_{rand} := S^{\intercal}_{rand}\mathfrak{P}^{(i)}S_{rand}$
- **Solve:** ($m(n-1)$ linear equations in $(n-1)$ variables)

$$\sum_{y=1}^{n} \mathfrak{P}^{(k)}_{yj}\overline{s}'_{y,n} = 0, \quad \forall 1 \leq k \leq m, 1 \leq j < n.$$

Applying MinRank $(N < n)$

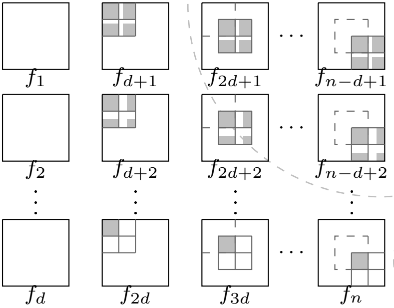
Note that x_N occurs quadratically in at most one polynomial of $\mathcal{F}$.



$\Rightarrow$ We look for a linear combination $\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}$ s.t. x_N vanishes.

Find $\lambda \in \mathbb{F}_q$ **such that** $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N$.

Applying MinRank ($N < n$)

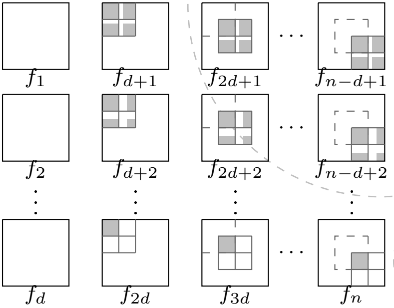


Note that x_N occurs quadratically in at most one polynomial of $\mathcal{F}$.

$\Rightarrow$ We look for a linear combination $\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}$ s.t. x_N vanishes.

Find $\lambda \in \mathbb{F}_q$ **such that** $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N$.

Applying MinRank ($N < n$)

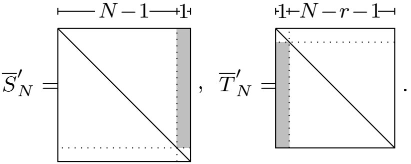


Note that x_N occurs quadratically in at most one polynomial of $\mathcal{F}$.

$\Rightarrow$ We look for a linear combination $\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)}$ s.t. x_N vanishes.

Find $\lambda \in \mathbb{F}_q$ **such that** $\text{Rank}\left(\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)}\right) < N$.

Finding a good key $(\overline{S}'_N, \overline{T}'_N)$



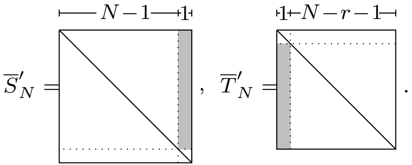
Theorem

$\overline{s}' = (\overline{s}'_{1,N}, \overline{s}'_{2,N}, \ldots, \overline{s}'_{N-1,N}, 1)$ and $\overline{t}' = (1, \overline{t}'_{2,1}, \overline{t}'_{3,1}, \ldots, \overline{t}'_{N-r+1,1})$ – unknown vectors.
The solution of (k **simultaneous MinRank problems**)

$$\overline{s}' \left(\mathfrak{P}^{(k)} + \overline{t}'_{k1} \mathfrak{P}^{(1)} \right) = \mathbf{0}_{1\times N}, \quad \forall 1 < k \leq N-r+1$$

gives the unknown columns of $\overline{S}'_N, \overline{T}'_N$.

Finding a good key $(\overline{S}'_N, \overline{T}'_N)$



Theorem (Equivalent):

Block matrices: $\mathfrak{P} = [\mathfrak{P}^{(2)}|\mathfrak{P}^{(3)}|\ldots|\mathfrak{P}^{(N-r+1)}]_{N\times N(N-r)}$,
$\mathfrak{P}_i = [\mathbf{0}|\ldots|\mathbf{0}|\mathfrak{P}^{(1)}|\mathbf{0}|\ldots|\mathbf{0}]_{N\times N(N-r)}$, $\overline{s}'$, $\overline{t}'$ – unknown.

The solution of (**one Rectangular MinRank problem**)

$$\mathrm{Rank}\left(\mathfrak{P} + \sum_{k=2}^{N-r+1} \overline{t}'_{k1}\mathfrak{P}_k\right) < N$$

gives the unknown columns of $\overline{S}'_N, \overline{T}'_N$.

Algorithm 2: Key Recovery

Input: $n - r$ public polynomials $\mathcal{P}$ in n variables.

for $N := n$ **down to** $r + 2$ **do**

If $N = n$, set $b = 0$, **otherwise** set $b = 1$.

Step Rectangular MinRank(N)

Transform the public key: $\mathcal{P} \leftarrow \overline{T}'_N \circ \mathcal{P} \circ \overline{S}'_N$,

If $b = 1$ remove the first polynomial from $\mathcal{P}$.

end for;

Output: The equivalent keys $\overline{S}' = \overline{S}'_n \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_n$.

Complexity of the Key Recovery Attack

Find $\lambda \in \mathbb{F}_q$ **such that** $\text{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N$.

Pitfalls over even characteristic fields – $\mathfrak{P}^{(s)}$ have always even rank

- N **is even**: $\text{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) \leq N - 2$.
  - $\text{Rank}\left(\mathfrak{P}^{(1)}\right) \leq N - 1$ and $\text{Rank}\left(\mathfrak{P}^{(k)}\right) \leq N - 1$
  - unique solution λ
  - q solutions for the good key $\overline{S}'_N$.
- N **is odd**: $\text{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N$ trivially satisfied
  - $\text{Rank}\left(\mathfrak{P}^{(1)}\right) \leq N - 1$ and $\text{Rank}\left(\mathfrak{P}^{(k)}\right) \leq N - 1$
  - every $\lambda \in \mathbb{F}_q$
  - q solutions for the good key $\overline{S}'_N$ (when rank defect is min.).

Complexity of the Key Recovery Attack

Find $\lambda \in \mathbb{F}_q$ **such that** $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N.$

Pitfalls over even characteristic fields –
$\mathfrak{P}^{(s)}$ **have always even rank**

- N **is even**: $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) \leq N - 2.$
  - $\mathrm{Rank}\left(\mathfrak{P}^{(1)}\right) \leq N - 1$ and $\mathrm{Rank}\left(\mathfrak{P}^{(k)}\right) \leq N - 1$
  - unique solution λ
  - q solutions for the good key $\overline{S}'_N$.
- N **is odd**: $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N$ trivially satisfied
  - $\mathrm{Rank}\left(\mathfrak{P}^{(1)}\right) \leq N - 1$ and $\mathrm{Rank}\left(\mathfrak{P}^{(k)}\right) \leq N - 1$
  - every $\lambda \in \mathbb{F}_q$
  - q solutions for the good key $\overline{S}'_N$ (when rank defect is min.).

Complexity of the Key Recovery Attack

Find $\lambda \in \mathbb{F}_q$ **such that** $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)}\right) < N$.

Pitfalls over even characteristic fields –
$\mathfrak{P}^{(s)}$ **have always even rank**

- N **is even**: $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)}\right) \leq N - 2$.
  - $\mathrm{Rank}\left(\mathfrak{P}^{(1)}\right) \leq N - 1$ and $\mathrm{Rank}\left(\mathfrak{P}^{(k)}\right) \leq N - 1$
  - unique solution λ
  - q solutions for the good key $\overline{S}'_N$.
- N **is odd**: $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)}\right) < N$ trivially satisfied
  - $\mathrm{Rank}\left(\mathfrak{P}^{(1)}\right) \leq N - 1$ and $\mathrm{Rank}\left(\mathfrak{P}^{(k)}\right) \leq N - 1$
  - every $\lambda \in \mathbb{F}_q$
  - q solutions for the good key $\overline{S}'_N$ (when rank defect is min.).

Complexity of the Key Recovery Attack

A pencil $(A, B) \in \mathbb{F}_q^N \times \mathbb{F}_q^N$ **is generic** if the rank defect is at most 1.

Theorem:
Let $\mathfrak{P}^{(1)}, \ldots, \mathfrak{P}^{(N-r+1)} \in \mathbb{F}_q^{N \times N}$, $q = \mathcal{O}(n)$.
If $\exists i,\ 2 \leq i \leq (N - r + 1)$ such that $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i)})$ is generic, then, our attack recovers a key equivalent to the secret-key in

$$\mathcal{O}\left(n^{\omega+3}\right)$$

with probability $1 - 1/q$.

Complexity of the Key Recovery Attack

A pencil $(A,B) \in \mathbb{F}_q^N \times \mathbb{F}_q^N$ **is generic** if the rank defect is at most 1.

Theorem:
Let $\mathfrak{P}^{(1)}, \ldots, \mathfrak{P}^{(N-r+1)} \in \mathbb{F}_q^{N \times N}$, $q = \mathcal{O}(n)$.
If $\exists i,\ 2 \leq i \leq (N-r+1)$ such that $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i)})$ is generic, then, our attack recovers a key equivalent to the secret-key in

$$\mathcal{O}\left(n^{\omega+3}\right)$$

with probability $1 - 1/q$.

Complexity of the Key Recovery Attack

- **independent of the field size**
- **polynomial in the number of variables**

Theorem:
Let $\mathfrak{P}^{(1)}, \ldots, \mathfrak{P}^{(N-r+1)} \in \mathbb{F}_q^{N \times N}$.
If $\exists i,\ 2 \leq i \leq (N-r+1)$ such that $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i)})$ is generic, and if we assume that the corresponding kernels behave like random, then, our attack recovers a key equivalent to the secret-key in

$$\mathcal{O}(n^{3\omega+1})$$

field operations with probability $\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^{n-3}}\right)$.

Complexity of the Key Recovery Attack

- **independent of the field size**
- **polynomial in the number of variables**

Theorem:
Let $\mathfrak{P}^{(1)}, \dots, \mathfrak{P}^{(N-r+1)} \in \mathbb{F}_q^{N\times N}$.
If $\exists i,\ 2 \le i \le (N-r+1)$ such that $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i)})$ is generic, and if we assume that the corresponding kernels behave like random, then, our attack recovers a key equivalent to the secret-key in

$$\mathcal{O}(n^{3\,\omega+1})$$

field operations with probability $\left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^{n-3}}\right)$.

Theoretical Complexities ($C(n,r) = \sum_{N=r+2}^{n-1} \binom{N+4}{3}^{\omega}.$)

Table: Theoretical Key Recovery MQQ-ENC (for claimed security of $\mathcal{O}(2^{128})$).

2^k	k	n	r	d	Decryption	Key Recovery
2	1	256	8	8	2^{25}	$2^{56.3}$
4	2	128	4	8	2^{23}	$2^{48.2}$
16	4	64	2	8	2^{21}	$2^{40.3}$
256	8	32	1	8	2^{20}	$2^{32.5}$

Table: Theoretical Key Recovery MQQ-SIG

Security	n	d	Key Recovery
2^{80}	160	8	$2^{50.8}$
2^{96}	192	8	$2^{52.9}$
2^{112}	224	8	$2^{54.7}$
2^{128}	256	8	$2^{56.2}$

Experimental Results MQQ-ENC

2^k	k	n	r	d	Key Recovery Theoretical	Key Recovery Practical		
						cycles	sec	$d_{\max}$
2	1	64	8	8	$2^{40.3}$	$2^{43.4}$	5421	3
2	1	96	8	8	$2^{44.9}$	$2^{47.8}$	111844	3
4	2	64	4	8	$2^{40.3}$	$2^{43.7}$	6978	3
4	2	96	4	8	$2^{44.9}$	$2^{47.8}$	109258	3
4	2	128	4	8	$2^{48.2}$	$2^{50.6}$	787214	3
16	4	32	2	8	$2^{32.5}$	$2^{34.7}$	14	3
16	4	48	2	8	$2^{37.0}$	$2^{38.9}$	251	3
16	4	64	2	8	$2^{40.3}$	$2^{41.6}$	1783	3

Experimental Results MQQ-SIG

n	r	d	Key Recovery Theoretical	Key Recovery Practical		
				cycles	sec	$d_{\max}$
64	32	8	$2^{40.3}$	$2^{40.1}$	560	3
96	48	8	$2^{44.9}$	$2^{43.2}$	4822	3
128	64	8	$2^{48.2}$	$2^{46.0}$	34376	3
160	80	8	$2^{50.8}$	$2^{48.0}$	120882	3

Conclusions

- MinRank - fundamental for $\mathcal{MQ}$ security
- Our attack
  - Works over characteristic 2
  - Works regardless of the number of removed equations
- Very hard to design a secure scheme based on an easily invertible MQQ structure
  - For any advancement
    – **deeper insights in quasigroup theory needed**.

Conclusions

- MinRank - fundamental for $\mathcal{MQ}$ security
- Our attack
  - Works over characteristic 2
  - Works regardless of the number of removed equations
- Very hard to design a secure scheme based on an easily invertible MQQ structure
  - For any advancement
    – **deeper insights in quasigroup theory needed**.

Thank you for listening!