NTNU
Norwegian University of
Science and Technology

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

Linear attacks in $\mathcal{MQ}$ cryptography - Part I

Simona Samardjiska

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

Outline

- $\mathcal{MQ}$ Public Key Cryptosystems
- The MinRank problem and applications in $\mathcal{MQ}$ cryptography
- Recent Contributions - PKC '15
  (joint work with Jean-Charles Faugère, Danilo Gligoroski, Ludovic Perret and Enrico Thomae)
  - Cryptanalysis of MQQ cryptosystems
  - Pitfalls of MinRank attacks

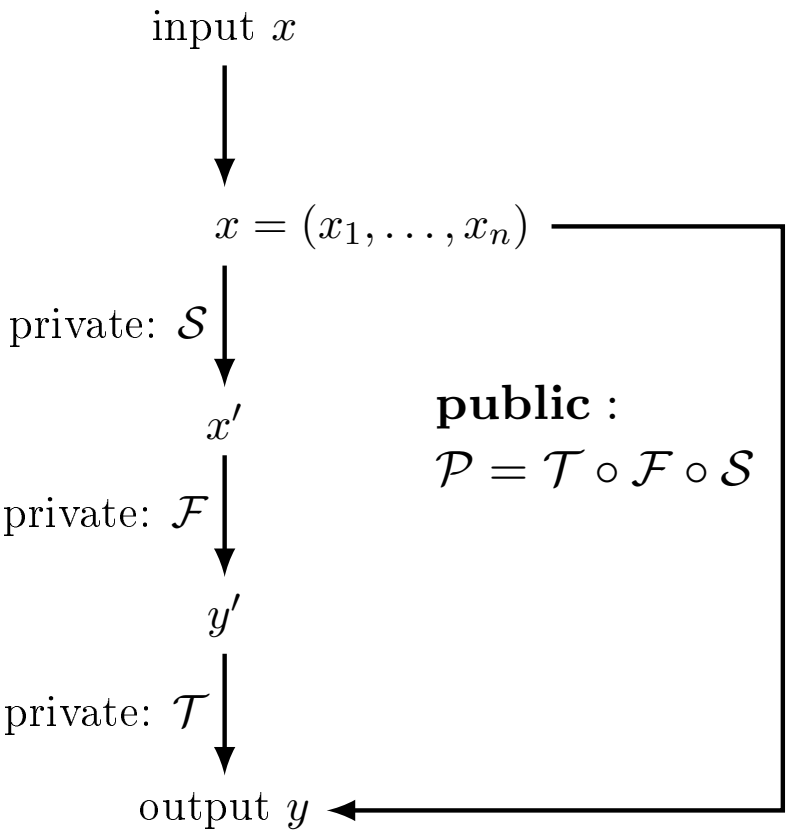
Outline

- $\mathcal{MQ}$ Public Key Cryptosystems
- The MinRank problem and applications in $\mathcal{MQ}$ cryptography
- Recent Contributions - PKC '15
  (joint work with Jean-Charles Faugère, Danilo Gligoroski, Ludovic Perret and Enrico Thomae)
  - Cryptanalysis of MQQ cryptosystems
  - Pitfalls of MinRank attacks

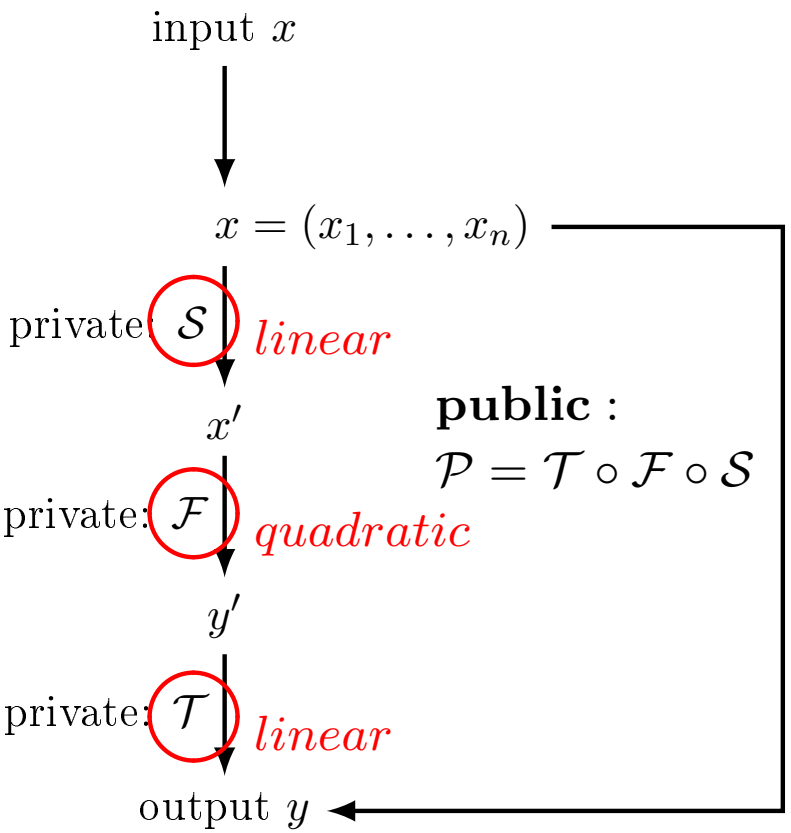

Outline

- **$\mathcal{MQ}$ Public Key Cryptosystems**
- **The MinRank problem and applications in $\mathcal{MQ}$ cryptography**
- **Recent Contributions - PKC '15**
  (joint work with Jean-Charles Faugère, Danilo Gligoroski, Ludovic Perret and Enrico Thomae)
  - **Cryptanalysis of MQQ cryptosystems**
  - **Pitfalls of MinRank attacks**


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



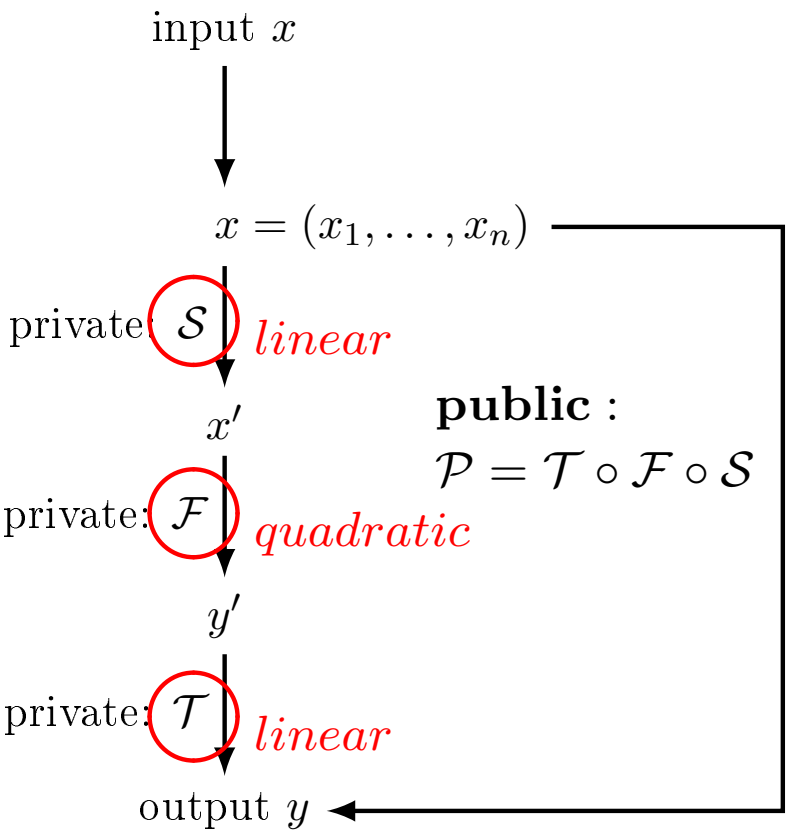
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$



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

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

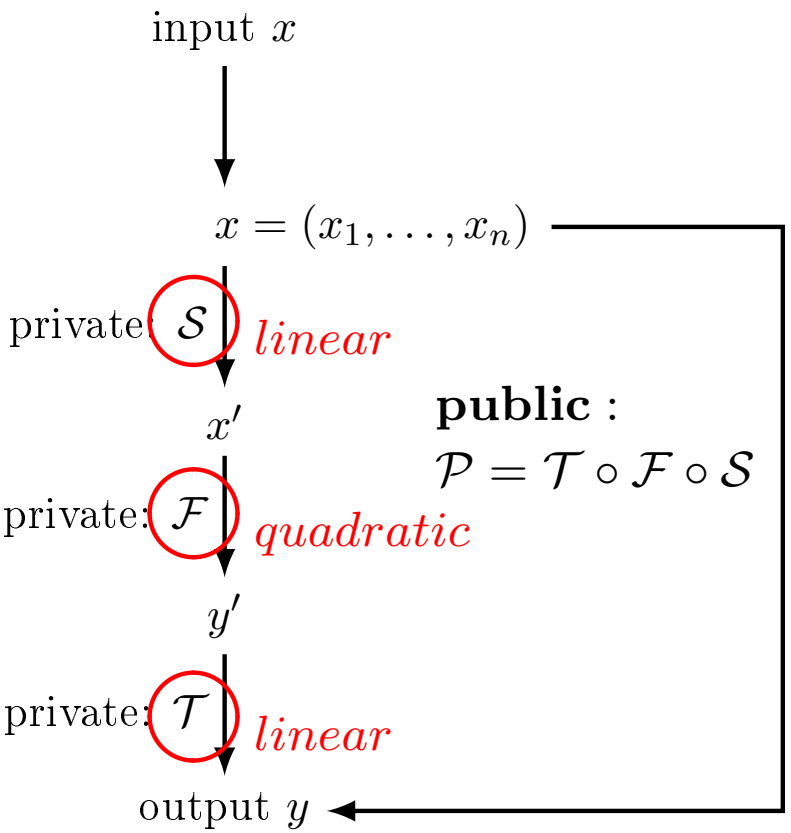
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$



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: $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$

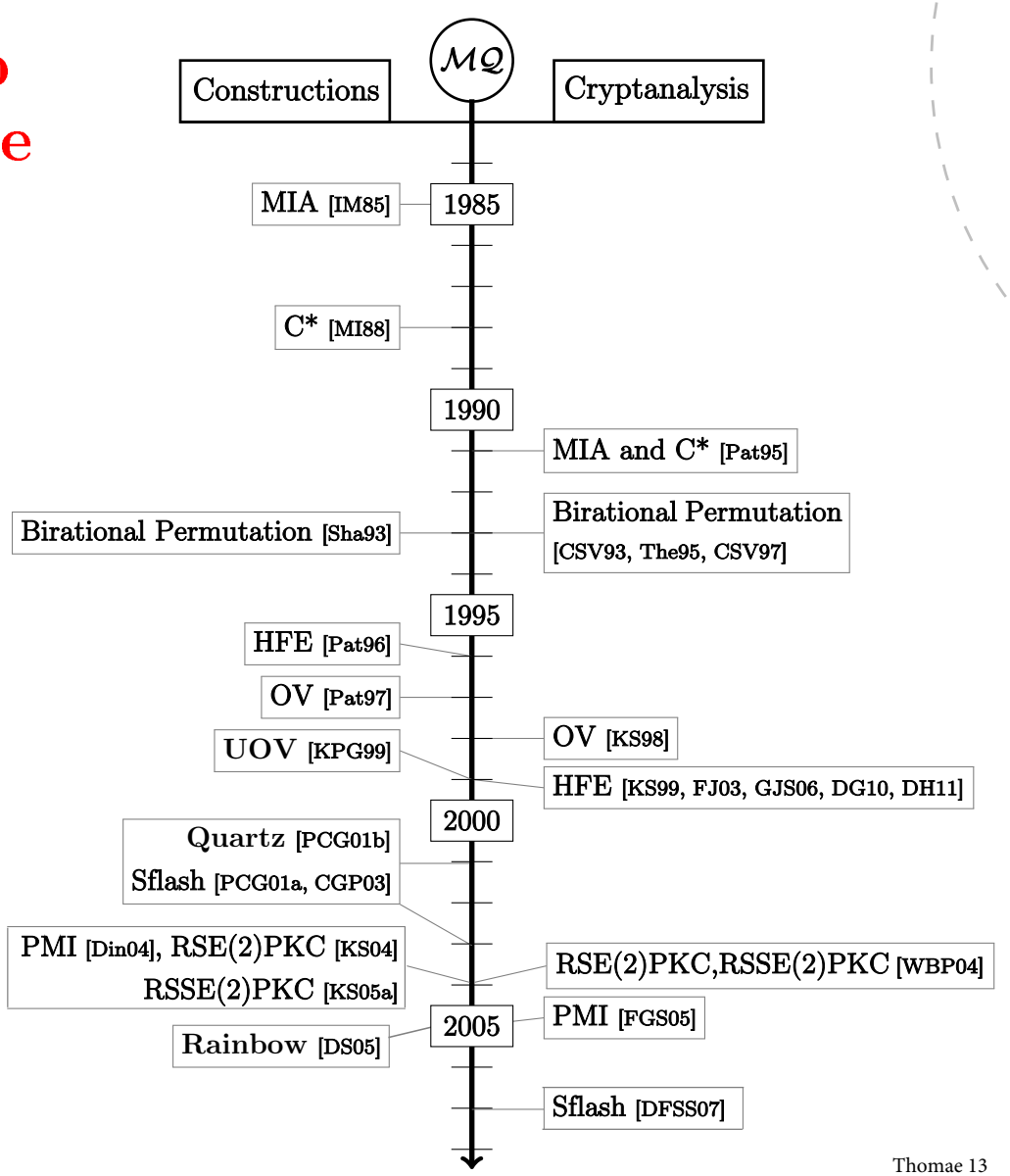


inverting $\mathcal{P}$ should be hard
- underlying NP-problem -
PoSSo

Post-Quantum secure

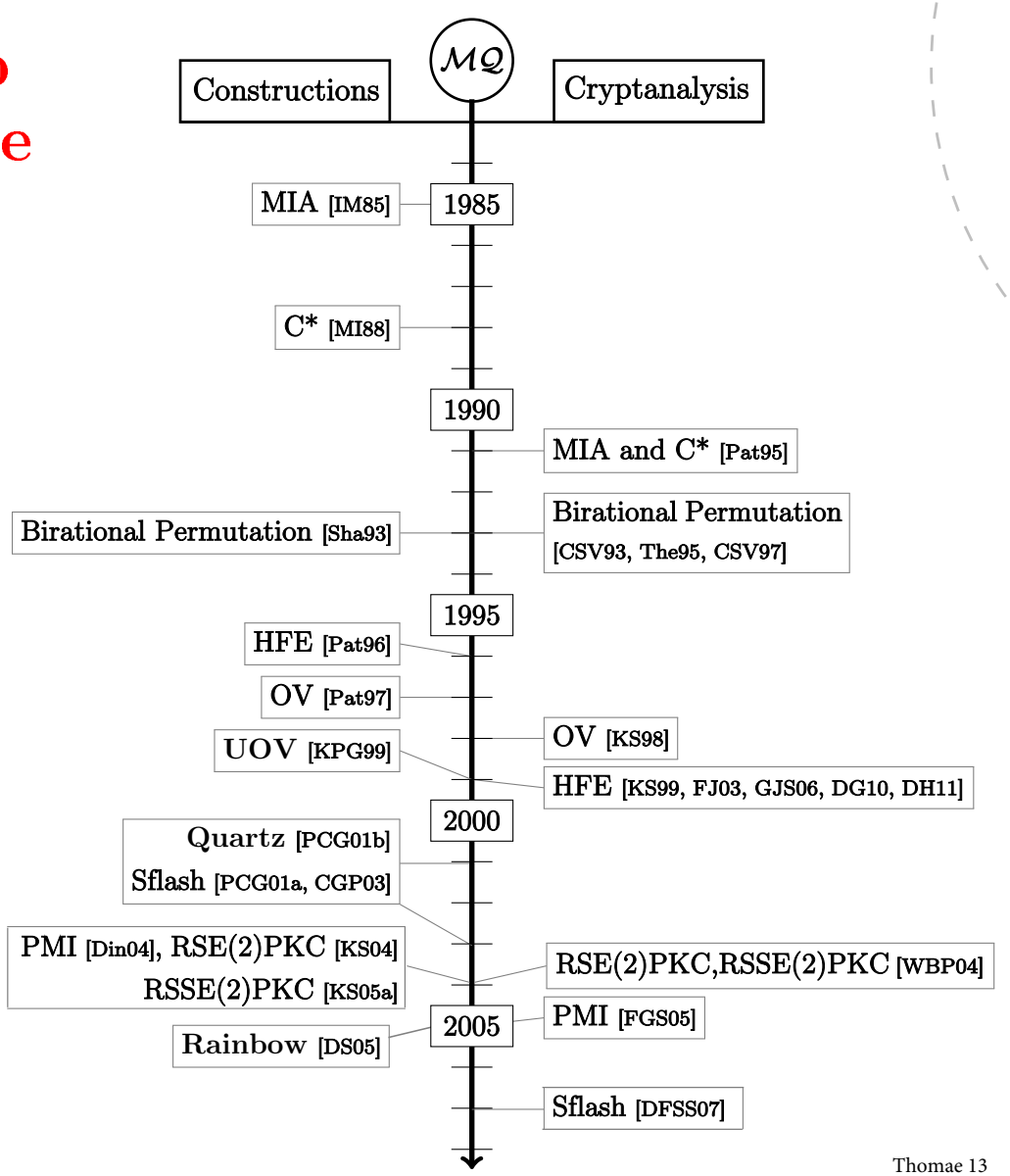
Matrix form: Public $\mathcal{P}$ - $x^\intercal \mathfrak{P}^{(s)} x$
Private $\mathcal{F}$ - $x^\intercal \mathfrak{F}^{(s)} x$

$\mathcal{MQ}$ crypto Prime Time



Thomae 13

$\mathcal{MQ}$ crypto Prime Time



Interest seriously declines

Solving Discrete Log – 2013/2014 Breakthroughs

Bitlength	Who	When	Complexity
127	Coppersmith	1984	L(1/3)
401	Gordon-McCurley	1992	
512	Weber-Denny	1998	
521	Joux-Lercier	2001	
607	Thome	2001	
613	Joux-Lercier	2005	
556	Joux-Lercier	2006	
676	Weber-Denny	2010	
923	Hayashi et al.	2012	
1175	Joux	Dec 2012	
1425	Joux	Jan 2013	
1778	Joux	11.02.2013	L(1/4)
1971	Gologlu et al.	19.02.2013	
4080	Joux	22.03.2013	
6120	Gologlu et al.	11.04.2013	
6168	Joux	21.05.2013	
	Barbulescu et al.	18.06.2013	L(1)


Solving Discrete Log – 2013/2014 Breakthroughs

Featured Research *from universities, journals, and other organizations*

New algorithm shakes up cryptography

Date: May 15, 2014

Source: CNRS

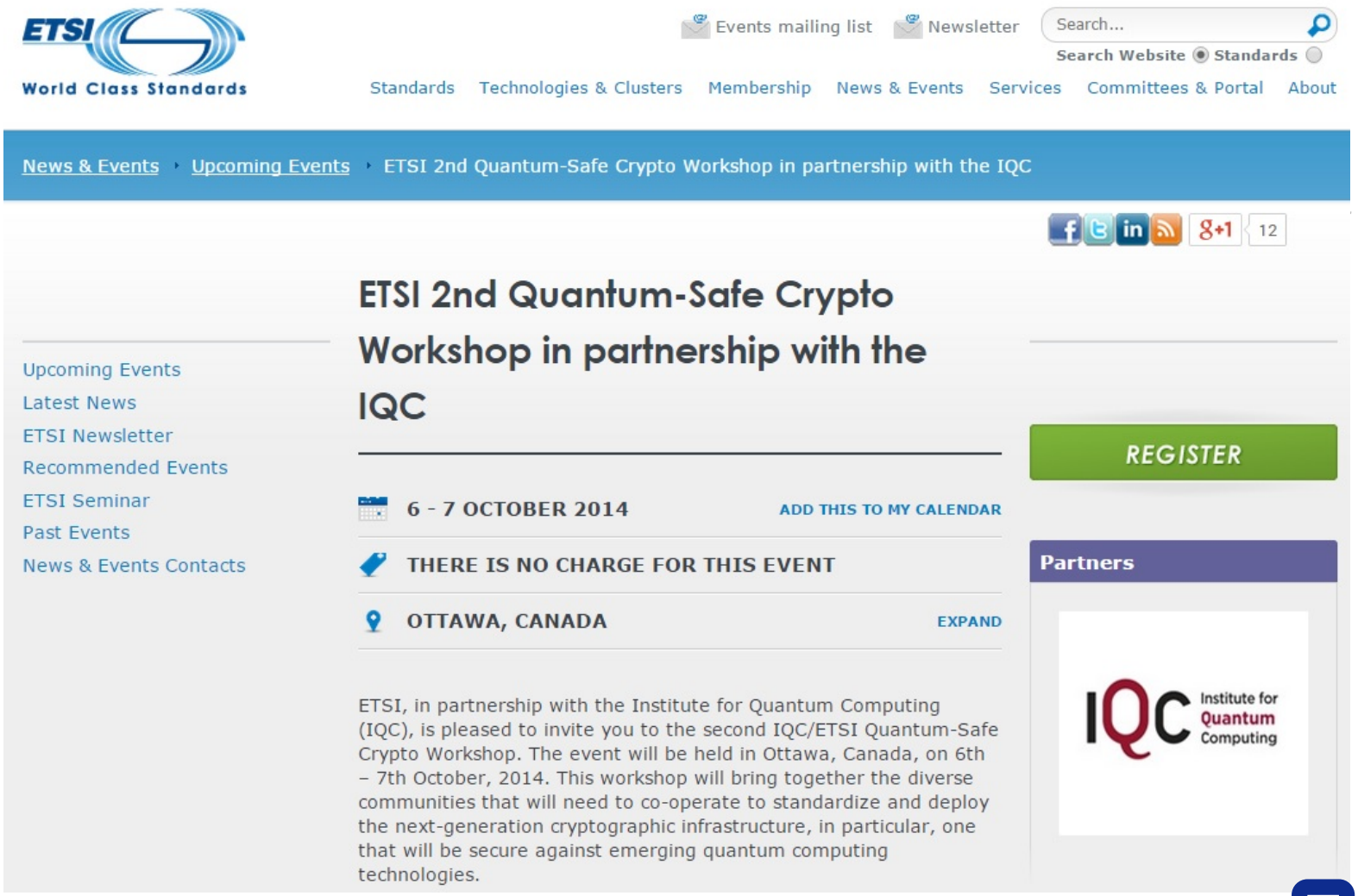
Summary: Researchers have solved one aspect of the discrete logarithm problem. This is considered to be one of the 'holy grails' of algorithmic number theory, on which the security of many cryptographic systems used today is based. They have devised a new algorithm that calls into question the security of one variant of this problem, which has been closely studied since 1976.

Advances in Cryptology – EUROCRYPT 2014
Lecture Notes in Computer Science Volume 8441, 2014, pp 1-16

A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic

Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé

Post–Quantum Crypto *...Where have you been all this while?*



ETSI World Class Standards

Events mailing list | Newsletter | Search... | Search Website Standards

Standards | Technologies & Clusters | Membership | News & Events | Services | Committees & Portal | About

News & Events › Upcoming Events › ETSI 2nd Quantum-Safe Crypto Workshop in partnership with the IQC

g+1 12

Upcoming Events
Latest News
ETSI Newsletter
Recommended Events
ETSI Seminar
Past Events
News & Events Contacts

ETSI 2nd Quantum-Safe Crypto Workshop in partnership with the IQC

REGISTER

6 - 7 OCTOBER 2014 ADD THIS TO MY CALENDAR

THERE IS NO CHARGE FOR THIS EVENT

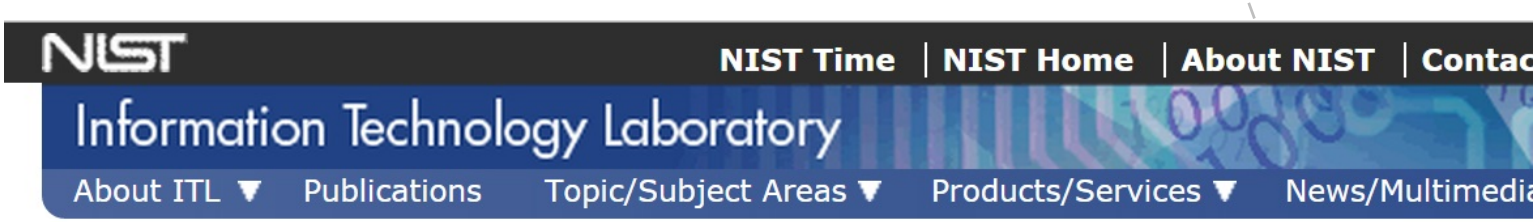
OTTAWA, CANADA EXPAND

ETSI, in partnership with the Institute for Quantum Computing (IQC), is pleased to invite you to the second IQC/ETSI Quantum-Safe Crypto Workshop. The event will be held in Ottawa, Canada, on 6th – 7th October, 2014. This workshop will bring together the diverse communities that will need to co-operate to standardize and deploy the next-generation cryptographic infrastructure, in particular, one that will be secure against emerging quantum computing technologies.

Partners

IQC Institute for Quantum Computing

Post–Quantum Crypto *...Where have you been all this while?*



Workshop on Cybersecurity in a Post-Quantum World

Purpose:

The advent of practical quantum computing will break all commonly used public key cryptographic algorithms. In response, NIST is researching cryptographic algorithms for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. NIST is holding this workshop to engage academic, industry, and government stakeholders. This workshop will be co-located with the ***2015 International Conference on Practice and Theory of Public-Key Cryptography***,

Research in $\mathcal{MQ}$ cryptography ?

- Bad reputation due to break and patch history
- But also...
  - UOV, HFEv- signatures - secure variants of Patarin's schemes
  - Provably secure identification scheme of Sakumoto et al.
  - QUAD - Provably secure stream cipher - Berbain et al.

More scrutiny needed
for understanding the security


Research in $\mathcal{MQ}$ cryptography ?

- Bad reputation due to break and patch history
- But also...
  - UOV, HFEv- signatures - secure variants of Patarin's schemes
  - Provably secure identification scheme of Sakumoto et al.
  - QUAD - Provably secure stream cipher - Berbain et al.

More scrutiny needed
for understanding the security


Research in $\mathcal{MQ}$ cryptography ?

- Bad reputation due to break and patch history
- But also...
  - UOV, HFEv- signatures - secure variants of Patarin's schemes
  - Provably secure identification scheme of Sakumoto et al.
  - QUAD - Provably secure stream cipher - Berbain et al.

More scrutiny needed
for understanding the security


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

MinRank

- Underlays the security of
  - HFE, STS, Rainbow, ... and many more

- Key-recovery attack
  - Equivalent keys/Good keys

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

MinRank

- Underlays the security of
  - HFE, STS, Rainbow, ... and many more
- Key-recovery attack
  - **Equivalent keys/Good keys**

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

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

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

- **NP-hard**, however
- instances in $\mathcal{MQ}$ crypto are **often easy**

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

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

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

- **NP-hard**, however
- instances in $\mathcal{MQ}$ crypto are **often easy**

Solving MinRank - Kernel Method [Courtois & Goubin '00]

- randomly generate vectors $\mathbf{x}_1, \ldots, \mathbf{x}_\ell$
- hope they are in the kernel of $\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0$
  - guessed correctly with probability at least $q^{-\lceil \frac{k}{n} \rceil r}$
- the k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ can be found by solving

$$\begin{pmatrix} x_{1,1} & \ldots & x_{1,n} \\ \vdots & & \vdots \\ x_{\ell,1} & \ldots & x_{\ell,n} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0 \right) = \mathbf{0}_{n \times n}.$$

where $\mathbf{x}_i = (x_{i,1} \ldots x_{i,n})$.

- unique solution for $\ell = \lceil \frac{k}{n} \rceil$

Complexity: $\mathcal{O}(q^{-\lceil \frac{k}{n} \rceil r} k^3)$

Solving MinRank - Kernel Method [Courtois & Goubin '00]

- randomly generate vectors $\mathbf{x}_1, \ldots, \mathbf{x}_\ell$
- hope they are in the kernel of $\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0$
  - guessed correctly with probability at least $q^{-\lceil \frac{k}{n} \rceil r}$
- the k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ can be found by solving

$$\begin{pmatrix} x_{1,1} & \ldots & x_{1,n} \\ \vdots & & \vdots \\ x_{\ell,1} & \ldots & x_{\ell,n} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0 \right) = \mathbf{0}_{n \times n}.$$

where $\mathbf{x}_i = (x_{i,1} \ldots x_{i,n})$.

- unique solution for $\ell = \lceil \frac{k}{n} \rceil$

Complexity: $\mathcal{O}(q^{-\lceil \frac{k}{n} \rceil r} k^3)$

Solving MinRank - Kernel Method [Courtois & Goubin '00]

- randomly generate vectors $\mathbf{x}_1, \ldots, \mathbf{x}_\ell$
- hope they are in the kernel of $\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0$
  - guessed correctly with probability at least $q^{-\lceil \frac{k}{n} \rceil r}$
- the k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ can be found by solving

$$\begin{pmatrix} x_{1,1} & \ldots & x_{1,n} \\ \vdots & & \vdots \\ x_{\ell,1} & \ldots & x_{\ell,n} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0 \right) = \mathbf{0}_{n \times n}.$$

where $\mathbf{x}_i = (x_{i,1} \ldots x_{i,n})$.

- unique solution for $\ell = \lceil \frac{k}{n} \rceil$

Complexity: $\mathcal{O}(q^{-\lceil \frac{k}{n} \rceil r} k^3)$

Solving MinRank - Kernel Method [Courtois & Goubin '00]

- randomly generate vectors $\mathbf{x}_1, \ldots, \mathbf{x}_\ell$
- hope they are in the kernel of $\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0$
  - guessed correctly with probability at least $q^{-\lceil \frac{k}{n} \rceil r}$
- the k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ can be found by solving

$$\begin{pmatrix} x_{1,1} & \ldots & x_{1,n} \\ \vdots & & \vdots \\ x_{\ell,1} & \ldots & x_{\ell,n} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0 \right) = \mathbf{0}_{n \times n}.$$

where $\mathbf{x}_i = (x_{i,1} \ldots x_{i,n})$.

- unique solution for $\ell = \lceil \frac{k}{n} \rceil$

Complexity: $\mathcal{O}(q^{-\lceil \frac{k}{n} \rceil r} k^3)$

Solving MinRank - Kipnis & Shamir '99

$n\,(n-r)$ quadratic (bilinear) equations in $r\,(n-r)+k$ variables

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

- Relinearization [KS99]
- Gröbner bases [FLP08]

$$d_{reg} \leqslant \min(n_X, n_Y) + 1,$$

for bilinear system in X, Y blocks of variables of sizes n_X, n_Y.

Complexity: $\mathcal{O}\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ (F5 algorithm [F02])

Solving MinRank - Kipnis & Shamir '99

$n\,(n-r)$ quadratic (bilinear) equations in $r\,(n-r)+k$ variables

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

- Relinearization [KS99]
- Gröbner bases [FLP08]

$$d_{reg} \leqslant \min(n_X, n_Y) + 1,$$

for bilinear system in X, Y blocks of variables of sizes n_X, n_Y.

Complexity: $\mathcal{O}\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ (F5 algorithm [F02])

Solving MinRank - Kipnis & Shamir '99

$n\,(n-r)$ quadratic (bilinear) equations in $r\,(n-r)+k$ variables

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

- Relinearization [KS99]
- Gröbner bases [FLP08]

$$d_{reg} \leqslant \min(n_X, n_Y) + 1,$$

for bilinear system in X, Y blocks of variables of sizes n_X, n_Y.

Complexity: $\mathcal{O}\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ (F5 algorithm [F02])

Solving MinRank - Kipnis & Shamir '99

$n\,(n-r)$ quadratic (bilinear) equations in $r\,(n-r)+k$ variables

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

- Relinearization [KS99]
- Gröbner bases [FLP08]

$$d_{reg} \leqslant \min(n_X, n_Y) + 1,$$

for bilinear system in X, Y blocks of variables of sizes n_X, n_Y.

Complexity: $\mathcal{O}\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ (F5 algorithm [F02])

Solving MinRank - Minors modeling [FLP08, FSS10]

- Find $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ such that all the minors of size $r+1$ of the matrix $\sum_{i=1}^{k} \lambda_i \mathbf{M}_i - \mathbf{M}_0$ are zero.
- Solve a system of $\binom{n}{r+1}^2$ equations in k variables,
  - Less variables than the Kipnis-Shamir modeling but equations of degree r.
  - Can be more efficient (MinRank auth. scheme [FSS10])

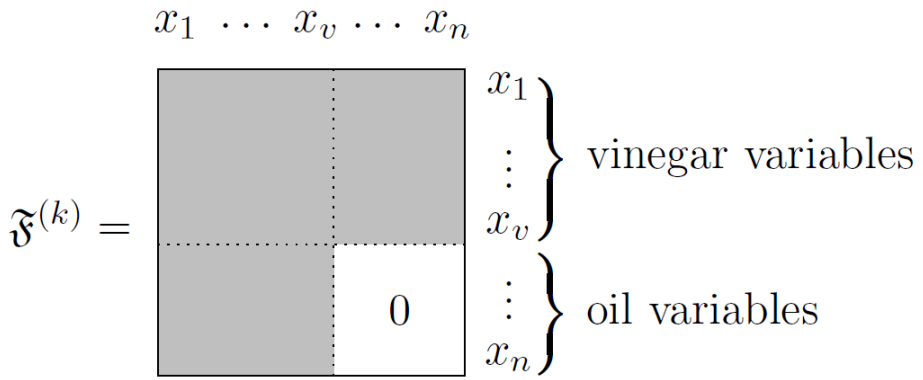
Equivalent Keys/Good Keys

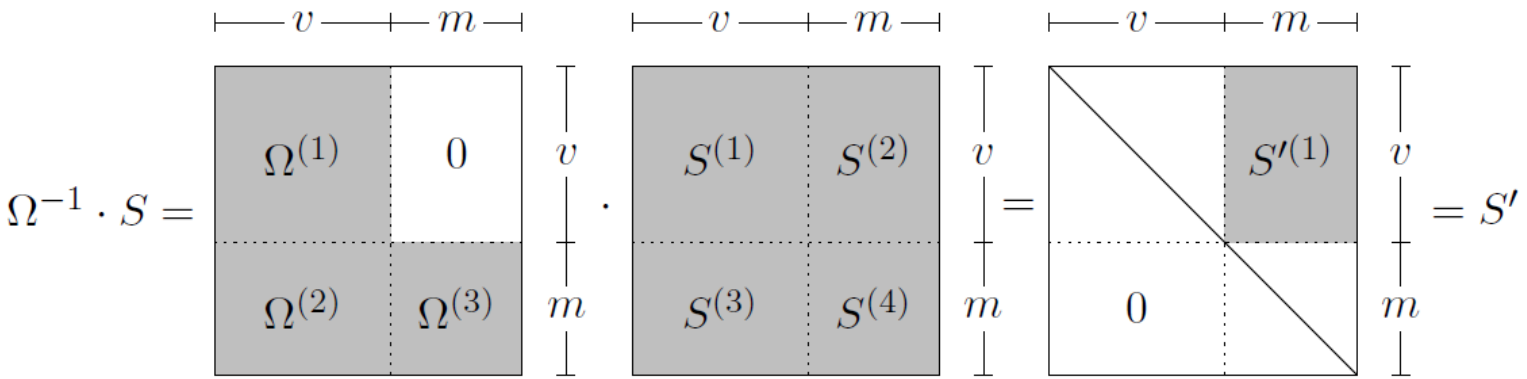
$$\begin{aligned}
\mathcal{P} &= \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} \Leftrightarrow \\
\mathcal{P} &= \underbrace{\mathcal{T} \circ \Sigma^{-1}} \circ \underbrace{\Sigma \circ \mathcal{F} \circ \Omega} \circ \underbrace{\Omega^{-1} \circ \mathcal{S}} \Leftrightarrow \\
\mathcal{P} &= \quad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

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

Equivalent Keys/Good Keys

UOV

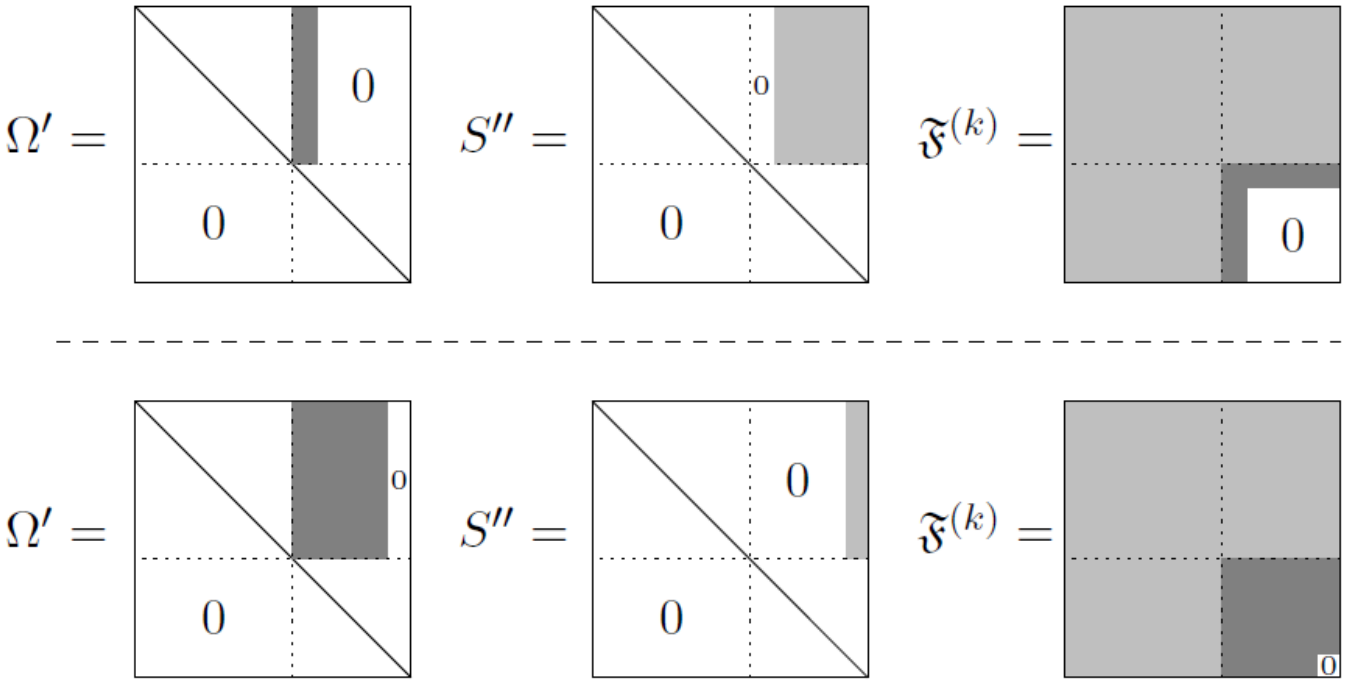




Equivalent Key for UOV

Equivalent Keys/Good Keys

UOV



Good Keys for UOV

A concrete example

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

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 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-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

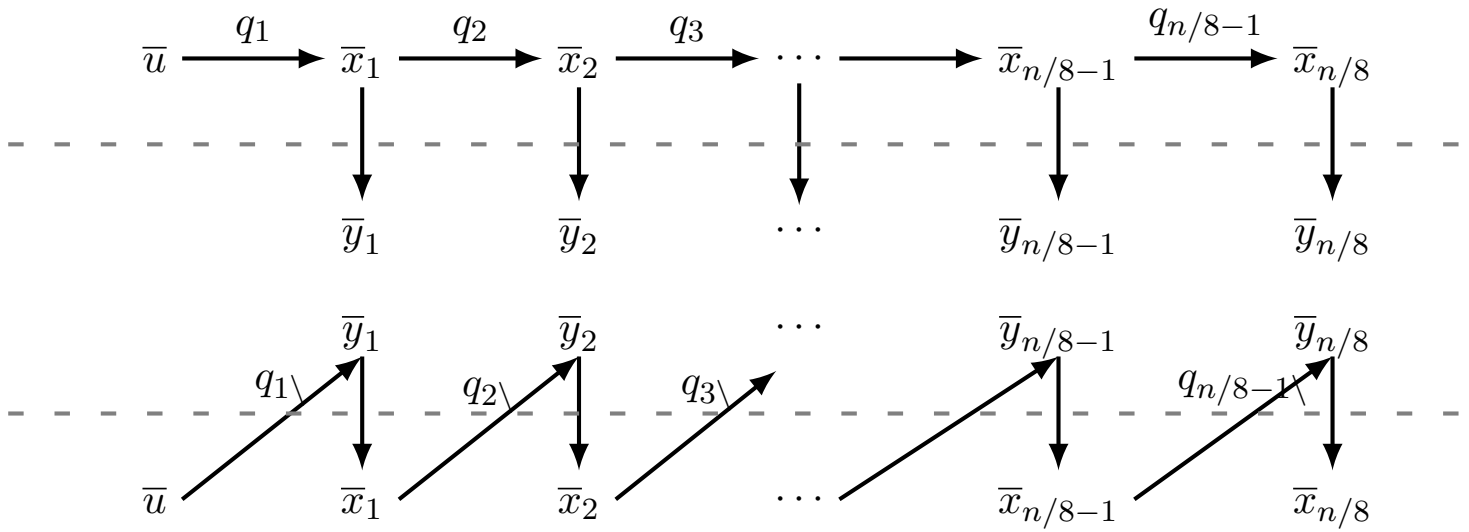
- **MQQ-SIG** [GØJPFKM11]
  - signature scheme
  - **fastest on (eBACS) SUPERCOP**
  - $n/2$ equations removed - measure against the attack
  - **Recommended parameters:** $n \in \{160, 192, 224, 256\}$ **for security levels of** 2^{80}, 2^{96}, 2^{112}, 2^{128}, **respectively.**

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

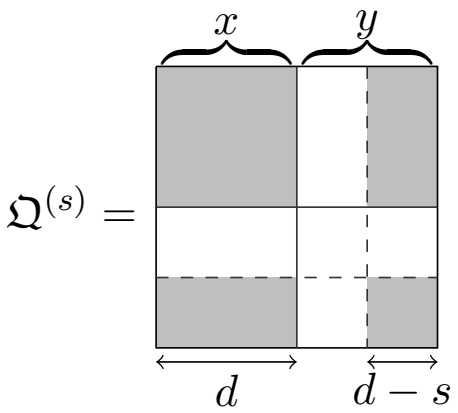
The central map of the MQQ cryptosystems

The central $\mathcal{F}$:

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



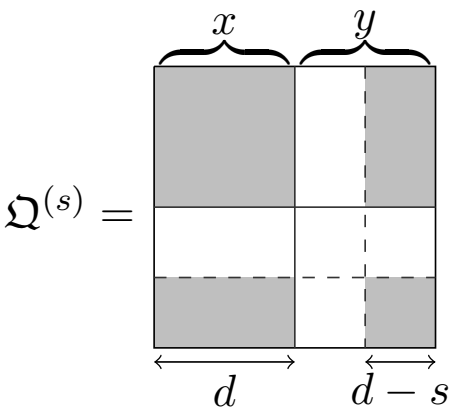
The central map of the MQQ cryptosystems



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

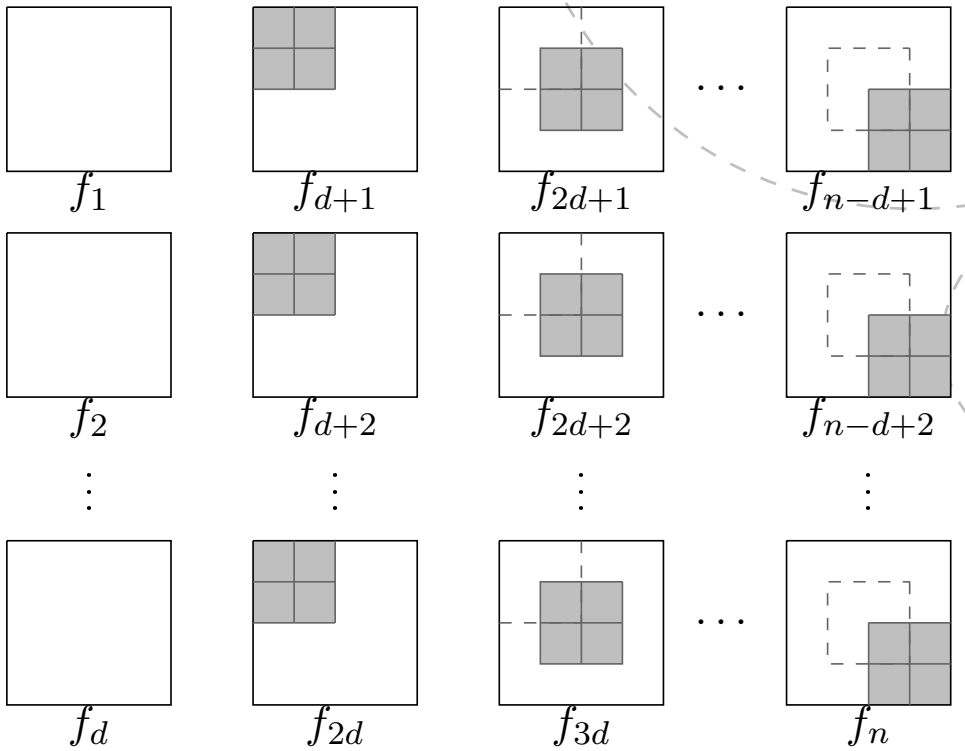
$D,\ D_y \in \mathrm{GL}_d(\mathbb{F}_{2^k})$,
$\overline{c}, \overline{c}_y$ – vectors of dimension d.

The central map of the MQQ cryptosystems



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

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



The central map

Crucial observation about the algebraic structure

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

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

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

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

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

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

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

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

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

Crucial observation about the algebraic structure

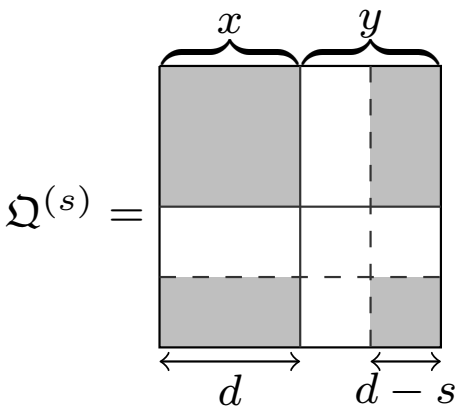
$$\mathcal{P} = \quad \mathcal{T} \quad \circ \quad \mathcal{F} \quad \circ \quad \mathcal{S} \quad \Leftrightarrow$$
$$[D \cdot \mathfrak{q}(\overline{x}, D_y \cdot \overline{y} + \overline{c}_y) + \overline{c}]$$

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

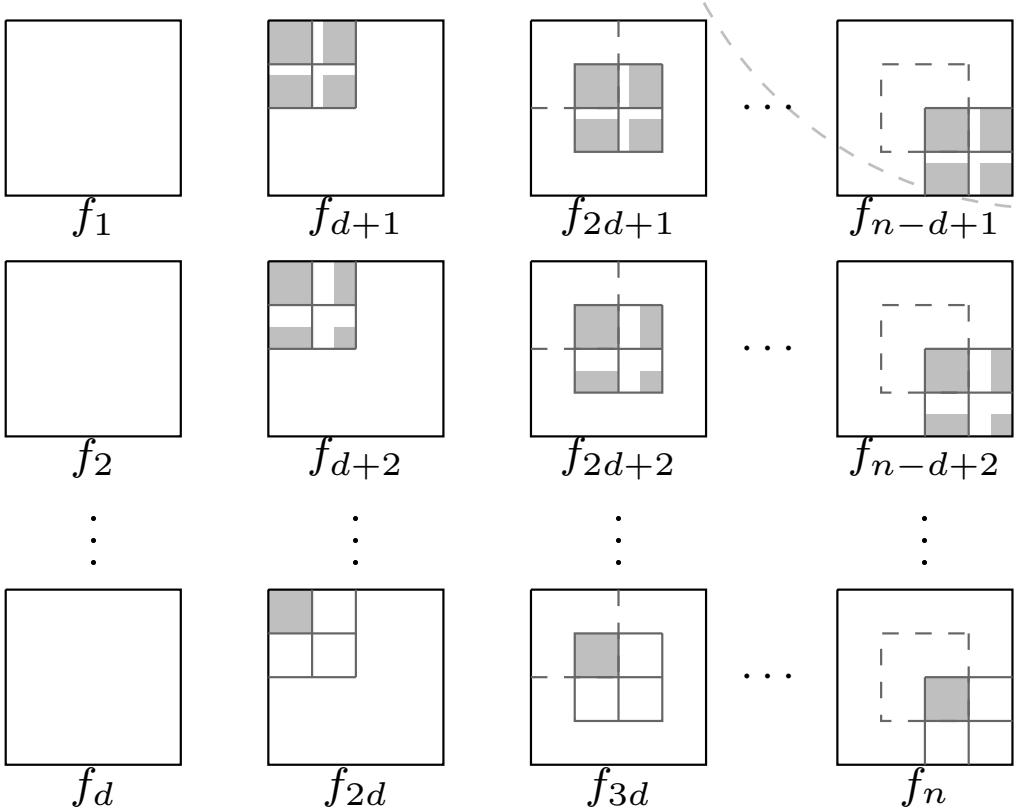
$$\mathcal{P} = \quad T \cdot (I_{\frac{n}{d}} \otimes D) \quad \circ \quad \mathcal{F}' \quad \circ \quad S \quad \Leftrightarrow$$
$$[\mathfrak{q}(\overline{x}, D_y \cdot \overline{y})]$$

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

Crucial observation about the algebraic structure

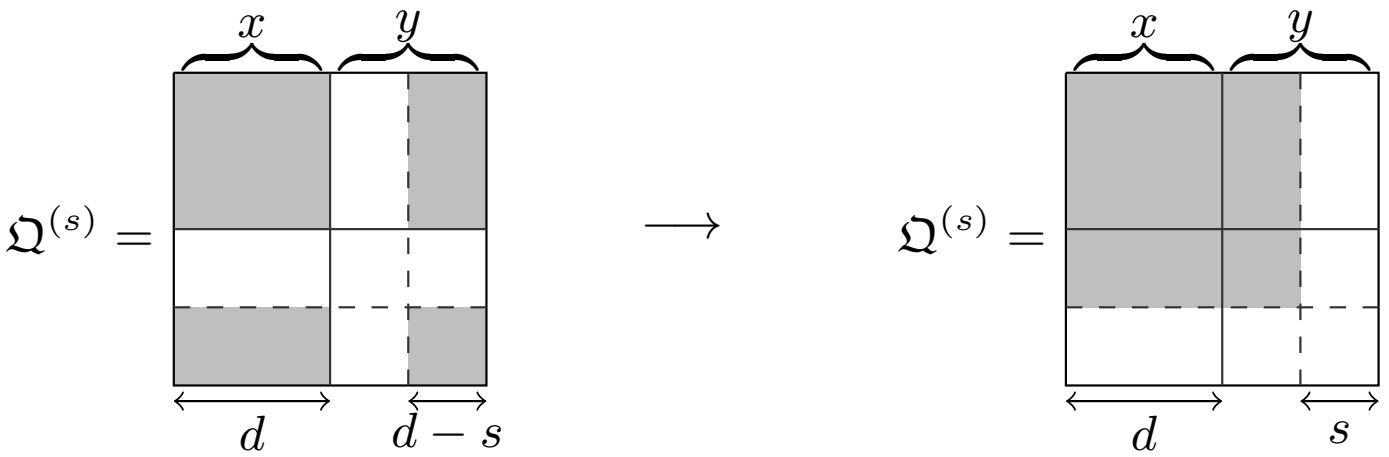


$\tilde{\mathfrak{q}}(\overline{x}, \overline{y})$



The central map

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
$\overline{S}' = \overline{S}'_n \circ \cdots \circ \overline{S}'_{r+2}$ 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 $\mathcal{P} \leftarrow \overline{T}'_N \circ \mathcal{P} \circ \overline{S}'_N$,

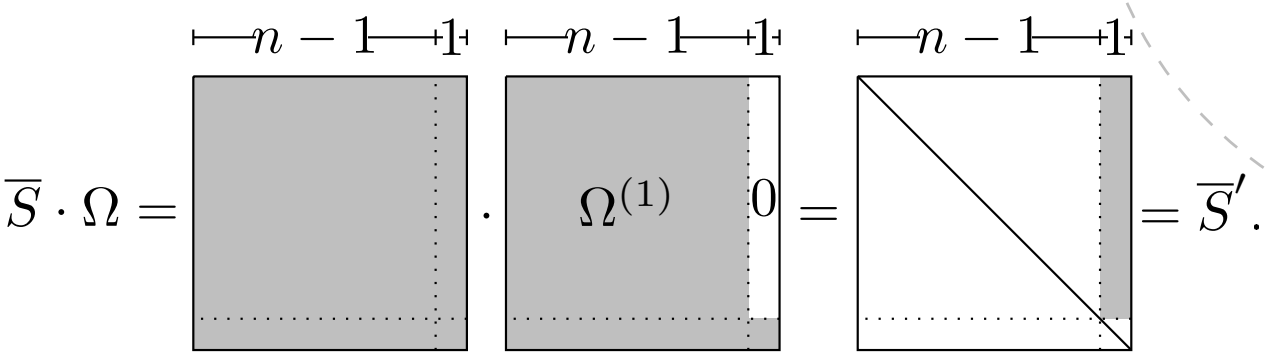
and if $N < n$ remove the first polynomial from $\mathcal{P}$.

end for;

Output: The equivalent key

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

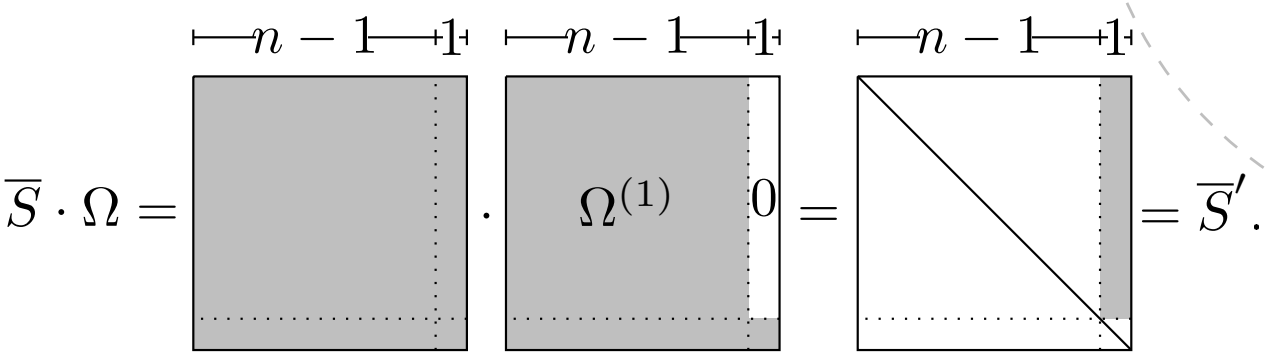
Finding a good key $(\overline{S}'_n, \overline{T}'_n)$



- 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: $\mathcal{P}^{(i)}_{rand} := S^{\intercal}_{rand} \mathcal{P}^{(i)} S_{rand}$
- **Solve:** ($m(n-1)$ linear equations in $(n-1)$ variables)

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

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

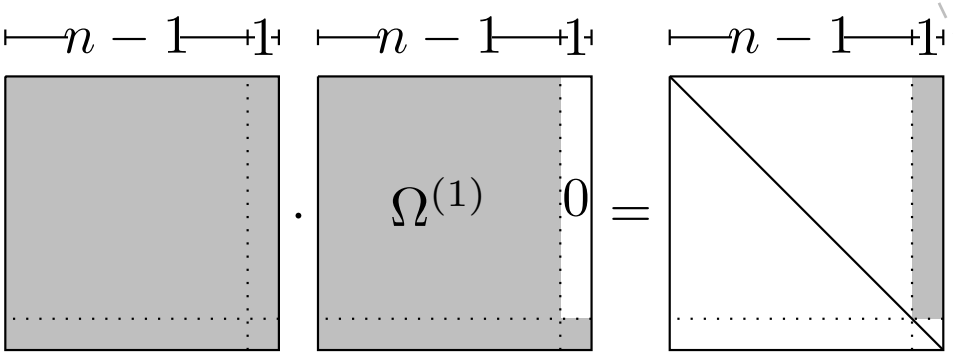


- Note that x_n does not appear quadratically
  $\Rightarrow$ We can take $\overline{T}'_n = I$
- A good key $\overline{S}'_n$ exists only if $\overline{S}_{nn} \neq 0$.
  $\Rightarrow$ Randomization: $\mathfrak{P}^{(i)}_{rand} := S^{\intercal}_{rand} \mathfrak{P}^{(i)} S_{rand}$
- **Solve:** ($m(n-1)$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

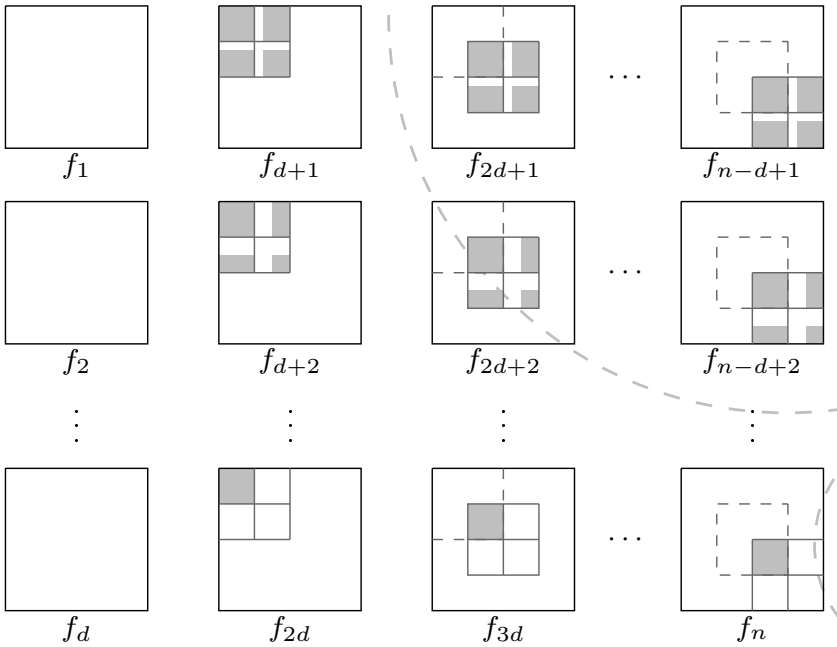
$$\overline{S} \cdot \Omega = \quad \cdot \quad = \quad = \overline{S}'.$$



- 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 ($N < n$)



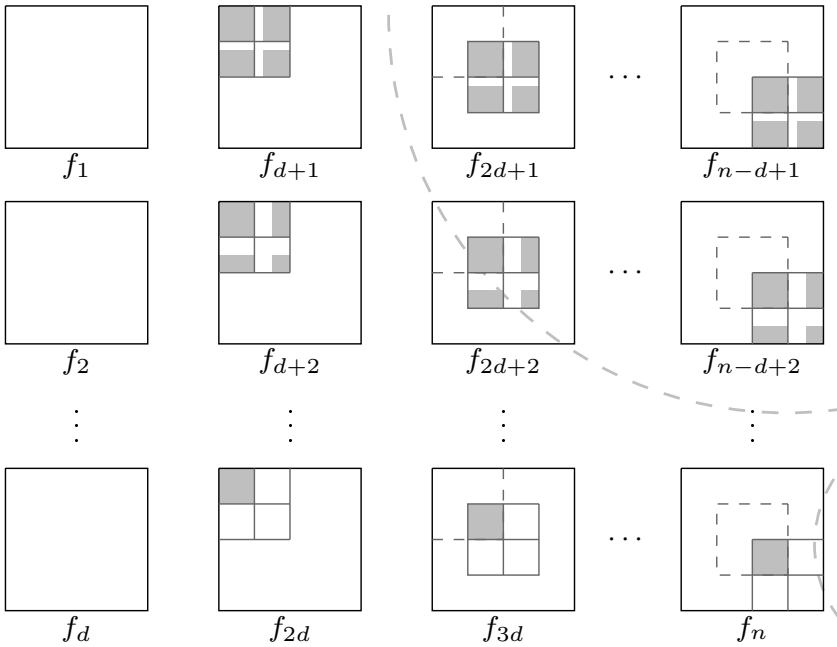
Note that x_N occurs quadratically in at most one polynomial of $\mathcal{F}$.

$\Rightarrow$ 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 $\mathcal{F}$.

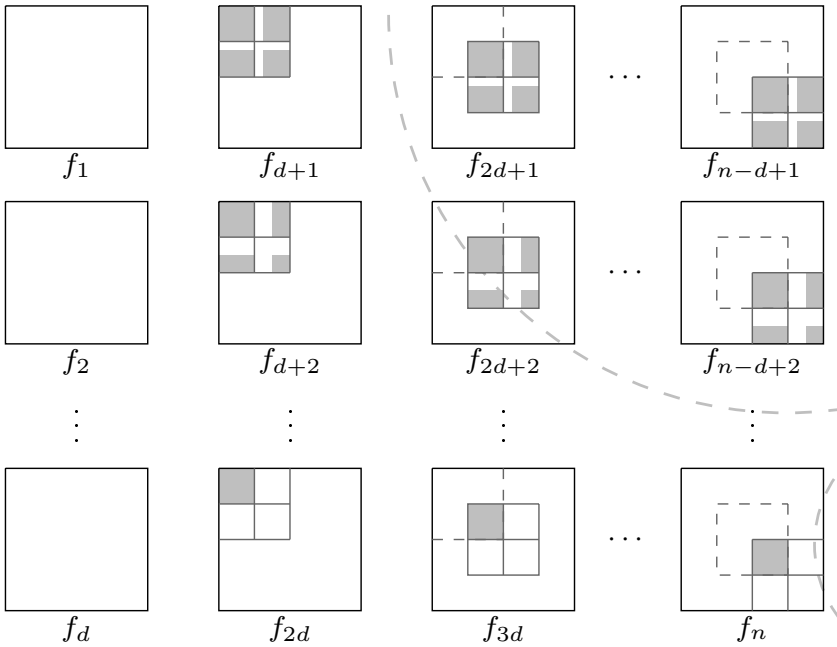


$\Rightarrow$ We look for a linear combination $\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}$ s.t. x_N vanishes.

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

Applying MinRank ($N < n$)

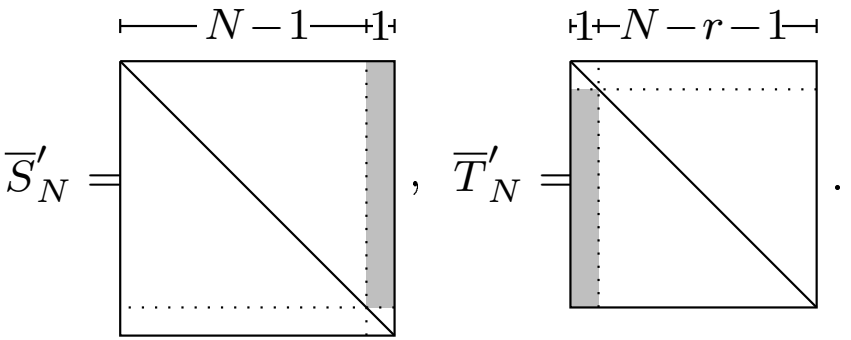
Note that x_N occurs quadratically in at most one polynomial of $\mathcal{F}$.



$\Rightarrow$ 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 $\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N$.

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



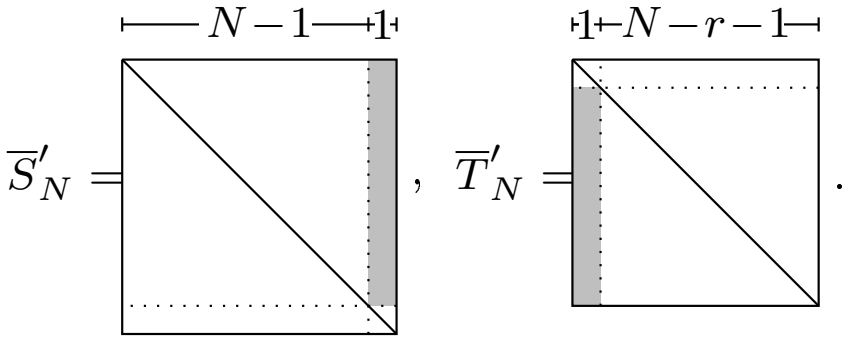
Theorem

$\overline{s}' = (\overline{s}'_{1,N}, \overline{s}'_{2,N}, \ldots, \overline{s}'_{N-1,N}, 1)$ 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 $(\overline{S}'_N, \overline{T}'_N)$



$\overline{S}'_N =$, $\overline{T}'_N =$.

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**)

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

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

Solving MinRank

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.).

Solving MinRank

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.).

Solving MinRank

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

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

- N **is even**: $\text{Rank}\left(\mathcal{P}^{(k)} + \lambda \mathcal{P}^{(1)}\right) \leq N - 2$.
  - $\text{Rank}\left(\mathcal{P}^{(1)}\right) \leq N - 1$ and $\text{Rank}\left(\mathcal{P}^{(k)}\right) \leq N - 1$
  - unique solution λ
  - q solutions for the good key $\overline{S}'_N$.
- N **is odd**: $\text{Rank}\left(\mathcal{P}^{(k)} + \lambda \mathcal{P}^{(1)}\right) < N$ trivially satisfied
  - $\text{Rank}\left(\mathcal{P}^{(1)}\right) \leq N - 1$ and $\text{Rank}\left(\mathcal{P}^{(k)}\right) \leq N - 1$
  - 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

Theorem:
Let $q = \mathcal{O}(n)$.
If there exists a pencil $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i)})$ of rank defect at most 1, 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**
- **yet, still polynomial in the number of variables**

Theorem:
If there exists a pencil $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i)})$ of rank defect at most 1, 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**
- **yet, still polynomial in the number of variables**

Theorem:
If there exists a pencil $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i)})$ of rank defect at most 1, 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

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


Conclusion

- MinRank - fundamental for $\mathcal{MQ}$ security
- Our attack
  - Works over characteristic 2
  - Independent of the field size
  - Works regardless of the number of removed equations

Simultaneous MinRank
– a proper way to model MinRank in $\mathcal{MQ}$ crypto –


Conclusion

- MinRank - fundamental for $\mathcal{MQ}$ security
- Our attack
  - Works over characteristic 2
  - Independent of the field size
  - Works regardless of the number of removed equations

Simultaneous MinRank
– a proper way to model MinRank in $\mathcal{MQ}$ crypto –

Thank you for listening!