A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems

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

PKC 2015, March 30 - April 1, Maryland, USA

Summary

- **Cryptanalysis** of the Multivariate cryptosystems
  - **MQQ-SIG** [Gligoroski, Ødegård, Jensen, Perret, Faugère, Knapskog & Markovski '11]
  - **MQQ-ENC** [Gligoroski & Samardjiska '12]

Summary

- **Cryptanalysis** of the Multivariate cryptosystems
  - **MQQ-SIG** 80 bits security in less than **1.5 days**
  - **MQQ-ENC** 128 bits security in **9 days**

Summary

- **Cryptanalysis** of the Multivariate cryptosystems
  - **MQQ-SIG** — 80 bits security in less than **1.5 days**
  - **MQQ-ENC** — 128 bits security in **9 days**

Poly-time complexity $\mathcal{O}(n^{10})$

Summary

- **Cryptanalysis** of the Multivariate cryptosystems
  - **MQQ-SIG** — 80 bits security in less than **1.5 days**
  - **MQQ-ENC** — 128 bits security in **9 days**

Poly-time complexity $\mathcal{O}(n^{10})$

  - The attack - **Recovery of equivalent key**

MinRank + Good keys

Summary

- **Cryptanalysis** of the Multivariate cryptosystems
  - **MQQ-SIG** — 80 bits security in less than **1.5 days**
  - **MQQ-ENC** — 128 bits security in **9 days**

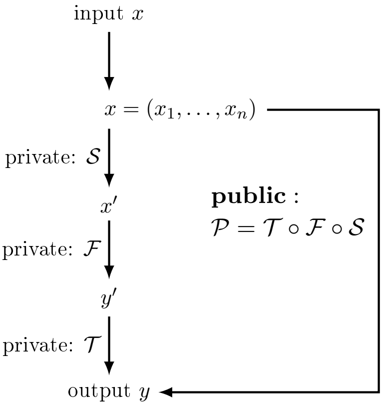
Poly-time complexity $\mathcal{O}(n^{10})$

  - The attack - **Recovery of equivalent key**

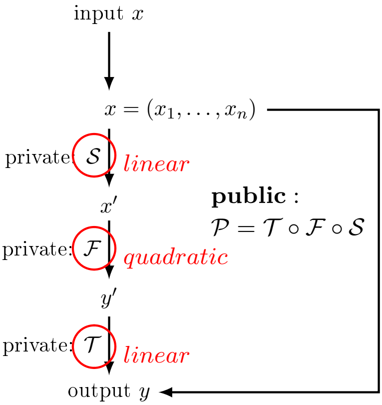
MinRank + Good keys

- **Solved problems** of MinRank attacks over **even characteristic**
  - **Simultaneous MinRank**
  - **Proven complexity bounds independent of the field size**

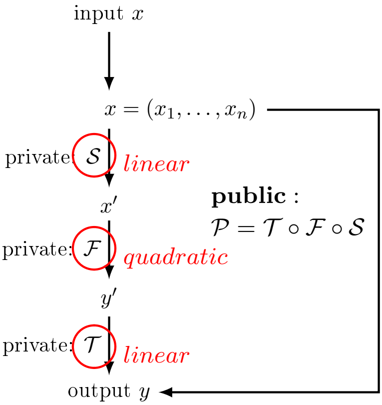
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



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



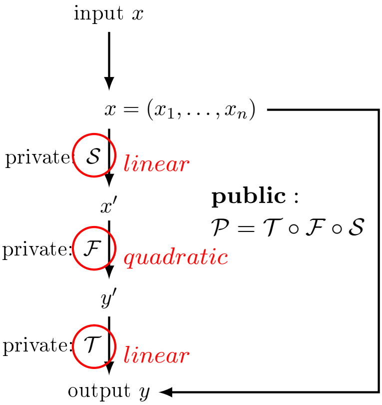
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



Public $\mathcal{P}$

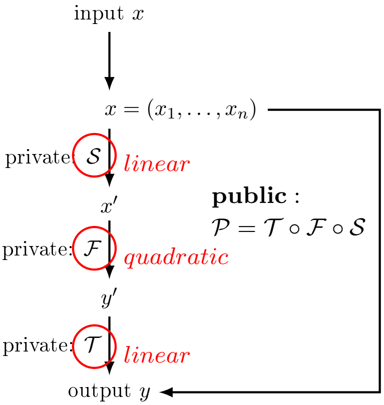
$$p_1(x_1, \ldots, x_n)$$
$$p_2(x_1, \ldots, x_n)$$
$$\cdots$$
$$p_m(x_1, \ldots, x_n)$$

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



Public $\mathcal{P}$	Matrix form:
$p_1(x_1, \ldots, x_n)$	$x^\intercal \mathfrak{P}_1 x$
$p_2(x_1, \ldots, x_n)$	$x^\intercal \mathfrak{P}_2 x$
$\ldots$	$\ldots$
$p_m(x_1, \ldots, x_n)$	$x^\intercal \mathfrak{P}_m x$

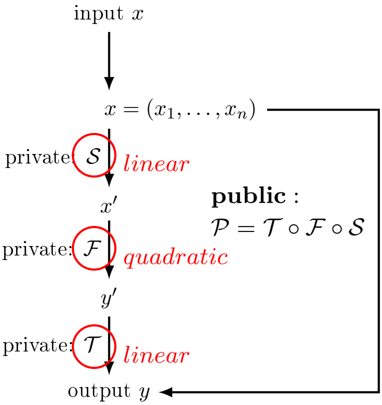
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



Public $\mathcal{P}$	Matrix form:
$p_1(x_1, \dots, x_n)$	$x^\intercal \mathfrak{P}_1 x$
$p_2(x_1, \dots, x_n)$	$x^\intercal \mathfrak{P}_2 x$
$\dots$	$\dots$
$p_m(x_1, \dots, x_n)$	$x^\intercal \mathfrak{P}_m x$

Matrices representing
the quadratic part
of the polynomials

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



Inverting $\mathcal{P}$ should be hard

Underlying NP-complete problem

PoSSo:

Input:

$p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$

Question:

Find - if any - $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ st.

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

Research in $\mathcal{MQ}$ cryptography ?

- Post - Quantum security

NIST | NIST Time | NIST Home | About NIST | Contac

Information Technology Laboratory

About ITL ▼ Publications Topic/Subject Areas ▼ Products/Services ▼ News/Multimedia

NIST Home > ITL > Computer Security Division > Cryptographic Technology Group > Workshop on (

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***,

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

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.

IQC Institute for Quantum Computing

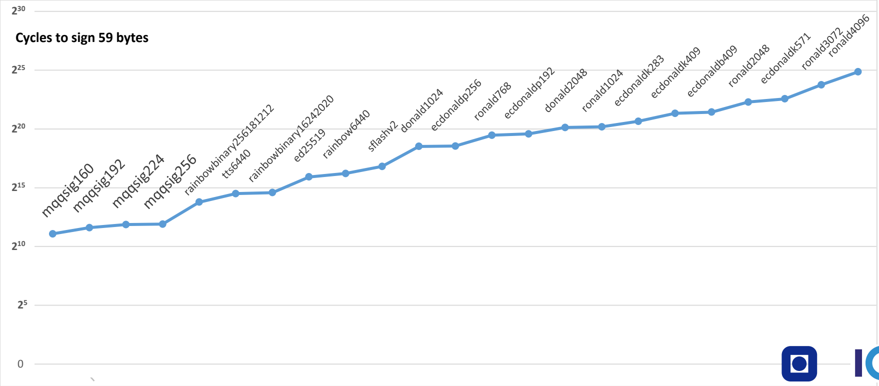
Research in $\mathcal{MQ}$ cryptography ?

- $\mathcal{MQ}$ schemes are naturally parallelizable!

Research in $\mathcal{MQ}$ cryptography ?

- $\mathcal{MQ}$ schemes are naturally parallelizable!
- up to 1000s times faster than classical

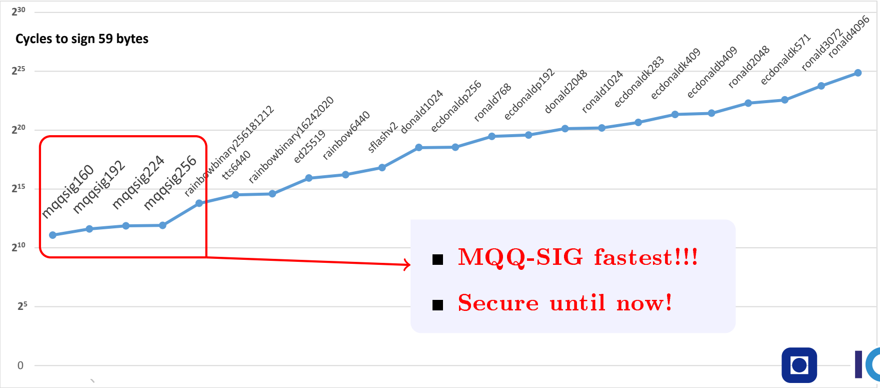
amd64; HW+AES (306c3); 2013 Intel Xeon E3-1275 V3; 4 x 3500MHz; titan0, supercop-20141124



Research in $\mathcal{MQ}$ cryptography ?

- $\mathcal{MQ}$ schemes are naturally parallelizable!
- up to 1000s times faster than classical

amd64; HW+AES (306c3); 2013 Intel Xeon E3-1275 V3; 4 x 3500MHz; titan0, supercop-20141124



- **MQQ-SIG fastest!!!**
- **Secure until now!**

The MQQ family of cryptosystems

- **MQQ (Multivariate Quadratic Quasigroups)** [GMK08]
  - Encryption scheme
  - Direct algebraic attack [Mohamed et al.'09, Faugère et al.'10]

MQQ-SIG [GØJPFKM11]

- $n/2$ equations removed - measure against the attack
- **Recommended parameters:**

Security	2^{80}	2^{96}	2^{112}	2^{128}
n	160	192	224	256

MQQ-ENC [GS12]

- only r equations removed
- Left MQQs - less structure
- **Recommended parameters for security level of 2^{128}:**

field	$\mathbb{F}_2$	$\mathbb{F}_4$	$\mathbb{F}_{16}$	$\mathbb{F}_{256}$
n	256	128	64	32
r	8	4	2	1

The MQQ family of cryptosystems

- MQQ (Multivariate Quadratic Quasigroups) [GMK08]
  - Encryption scheme
  - Direct algebraic attack [Mohamed et al.'09, Faugère et al.'10]

MQQ-SIG [GØJPFKM11]

- $n/2$ equations removed - measure against the attack
- **Recommended parameters:**

Security	2^{80}	2^{96}	2^{112}	2^{128}
n	160	192	224	256

MQQ-ENC [GS12]

- only r equations removed
- Left MQQs - less structure
- **Recommended parameters for security level of 2^{128}:**

field	$\mathbb{F}_2$	$\mathbb{F}_4$	$\mathbb{F}_{16}$	$\mathbb{F}_{256}$
n	256	128	64	32
r	8	4	2	1

The MQQ family of cryptosystems

- MQQ (Multivariate Quadratic Quasigroups) [GMK08]
  - Encryption scheme
  - Direct algebraic attack [Mohamed et al.'09, Faugère et al.'10]

MQQ-SIG [GØJPFKM11]

- $n/2$ equations removed - measure against the attack
- **Recommended parameters:**

Security	2^{80}	2^{96}	2^{112}	2^{128}
n	160	192	224	256

MQQ-ENC [GS12]

- only r equations removed
- Left MQQs - less structure
- **Recommended parameters for security level of 2^{128}:**

field	$\mathbb{F}_2$	$\mathbb{F}_4$	$\mathbb{F}_{16}$	$\mathbb{F}_{256}$
n	256	128	64	32
r	8	4	2	1

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

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

Input: $n, \mathbf{r}, k \in \mathbb{N}$, and $M_1, \ldots, M_k \in \mathcal{M}_n(\mathbb{F}_q)$.

Question: Find – if any – a nonzero k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ s.t.:

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

[Kipnis, Shamir '99], [Buss, Shallit '99]

- **NP-hard!!!** [Courtois '01], however,
- **Instances in $\mathcal{MQ}$ crypto** can be **much easier**, even **polynomial!**
- Underlays the security of HFE, STS, Rainbow, ... and more
- **In this talk:**

Use MinRank to recover equivalent key of MQQ system

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

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

Input: $n, \mathbf{r}, k \in \mathbb{N}$, and $M_1, \ldots, M_k \in \mathcal{M}_n(\mathbb{F}_q)$.
Question: Find – if any – a nonzero k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ s.t.:

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

[Kipnis, Shamir '99], [Buss, Shallit '99]

- **NP-hard!!!** [Courtois '01], however,
- **Instances in $\mathcal{MQ}$ crypto** can be **much easier**, even **polynomial!**
- Underlays the security of HFE, STS, Rainbow, ... and more
- **In this talk:**

Use MinRank to recover equivalent key of MQQ system

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

MinRank $MR(n, \mathbf{r}, k, M_1, \dots, M_k)$

Input: $n, \mathbf{r}, k \in \mathbb{N}$, and $M_1, \dots, M_k \in \mathcal{M}_n(\mathbb{F}_q)$.

Question: Find – if any – a nonzero k-tuple $(\lambda_1, \dots, \lambda_k) \in \mathbb{F}_q^k$ s.t.:

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

[Kipnis, Shamir '99], [Buss, Shallit '99]

- **NP-hard!!!** [Courtois '01], however,
- **Instances in $\mathcal{MQ}$ crypto** can be **much easier**, even **polynomial!**
- Underlays the security of HFE, STS, Rainbow, ... and more
- **In this talk:**

Use MinRank to recover equivalent key of MQQ system

Solving MinRank - Minors modeling

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \leq \mathbf{r} \;\Leftrightarrow\; \text{all minors of size } \mathbf{r}+1 \text{ of } \left(\sum_{i=1}^{k} \lambda_i M_i\right) \text{vanish.}$$

$$\binom{n}{\mathbf{r}+1}^2 \text{ equations of degree } \mathbf{r}+1, \text{ in } k \text{ variables}$$

Solving MinRank - Minors modeling

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \leq \mathbf{r} \iff \text{all minors of size } \mathbf{r}+1 \text{ of } \left(\sum_{i=1}^{k} \lambda_i M_i\right) \text{vanish.}$$

$$\binom{n}{\mathbf{r}+1}^2 \text{ equations of degree } \mathbf{r}+1, \text{ in } k \text{ variables}$$

- [Faugère & Levy-dit-Vehel & Perret '08],
  - Cryptanalysis of MinRank authentication scheme [Courtois '01]
- [Faugère & Safey El Din & Spaenlehauer '13]
  - Precise complexity bounds

Solving MinRank - Kipnis-Shamir modeling

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \leq \mathbf{r} \;\Leftrightarrow\; \exists\, x^{(1)}, \ldots, x^{(n-\mathbf{r})} \in \text{Ker}\left(\sum_{i=1}^{k} \lambda_i M_i\right)$$

$$\begin{pmatrix} 1 & & & x_1^1 & \ldots & x_{\mathbf{r}}^{(1)} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_1^{(n-\mathbf{r})} & \ldots & x_{\mathbf{r}}^{(n-\mathbf{r})} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i M_i\right) = \mathbf{0}_{n\times n}.$$

$n(n-\mathbf{r})$ quadratic (bilinear) equations in $\mathbf{r}(n-\mathbf{r})+k$ variables

Solving MinRank - Kipnis-Shamir modeling

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \le \mathbf{r} \;\Leftrightarrow\; \exists\, x^{(1)}, \ldots, x^{(n-\mathbf{r})} \in \text{Ker}\left(\sum_{i=1}^{k} \lambda_i M_i\right)$$

$$\begin{pmatrix} 1 & & & x_1^1 & \ldots & x_{\mathbf{r}}^{(1)} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_1^{(n-\mathbf{r})} & \ldots & x_{\mathbf{r}}^{(n-\mathbf{r})} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i M_i\right) = \mathbf{0}_{n\times n}.$$

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

- Relinearization [Kipnis & Shamir '99]

Solving MinRank - Kipnis-Shamir modeling

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \leq \mathbf{r} \;\Leftrightarrow\; \exists\, x^{(1)}, \ldots, x^{(n-\mathbf{r})} \in \text{Ker}\left(\sum_{i=1}^{k} \lambda_i M_i\right)$$

$$\begin{pmatrix} 1 & & & x_1^1 & \ldots & x_{\mathbf{r}}^{(1)} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_1^{(n-\mathbf{r})} & \ldots & x_{\mathbf{r}}^{(n-\mathbf{r})} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i M_i\right) = \mathbf{0}_{n\times n}.$$

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

- Gröbner bases [Faugère & Levy-dit-Vehel & Perret '08]
  - Complexity of F5 algorithm: $\mathcal{O}\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ [Faugère '02] with $2 \leqslant \omega \leqslant 3$ - the linear algebra constant

Solving MinRank - Kipnis-Shamir modeling

$$\text{Rank}\left(\sum_{i=1}^{k} \lambda_i M_i\right) \leq \mathbf{r} \ \Leftrightarrow\ \exists\ x^{(1)}, \ldots, x^{(n-\mathbf{r})} \in \text{Ker}\left(\sum_{i=1}^{k} \lambda_i M_i\right)$$

$$\begin{pmatrix} 1 & & & x_1^1 & \ldots & x_{\mathbf{r}}^{(1)} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_1^{(n-\mathbf{r})} & \ldots & x_{\mathbf{r}}^{(n-\mathbf{r})} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i M_i\right) = \mathbf{0}_{n \times n}.$$

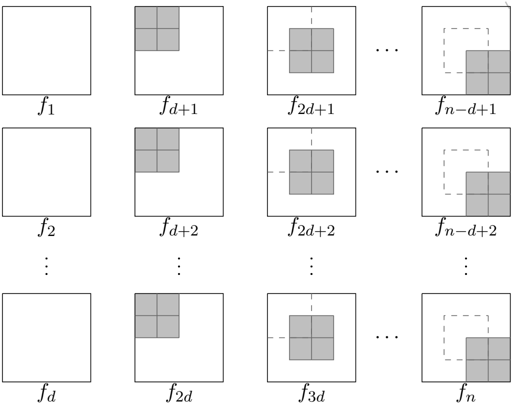
$n\,(n-\mathbf{r})$ quadratic (bilinear) equations in $\mathbf{r}\,(n-\mathbf{r})+k$ variables

- Gröbner bases [Faugère & Levy-dit-Vehel & Perret '08]
  - Complexity of F5 algorithm: $\mathcal{O}\left(\binom{n+d_{\text{reg}}}{d_{\text{reg}}}^{\omega}\right)$ [Faugère '02] with $2 \leqslant \omega \leqslant 3$ - the linear algebra constant

$$d_{reg} \leqslant \min(n_X, n_Y) + 2,$$

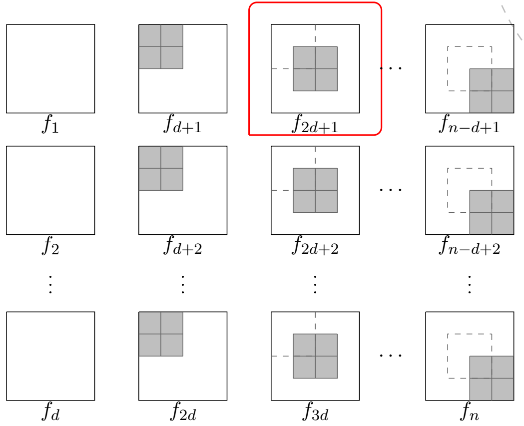
for bilinear system in X, Y blocks of variables of sizes n_X, n_Y.

The central map of the MQQ cryptosystems



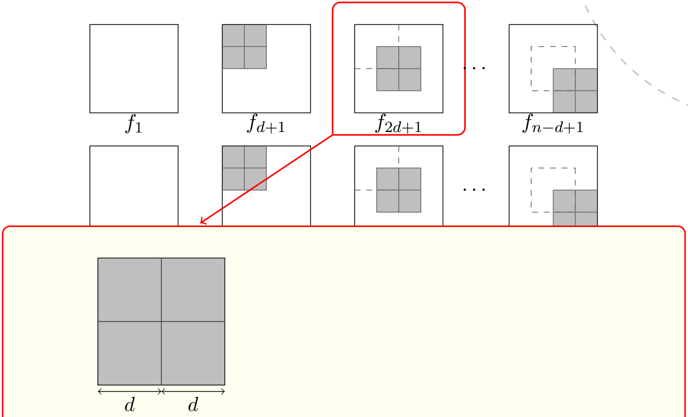
Matrix notation of $\mathcal{F}$

Crucial observation about the algebraic structure



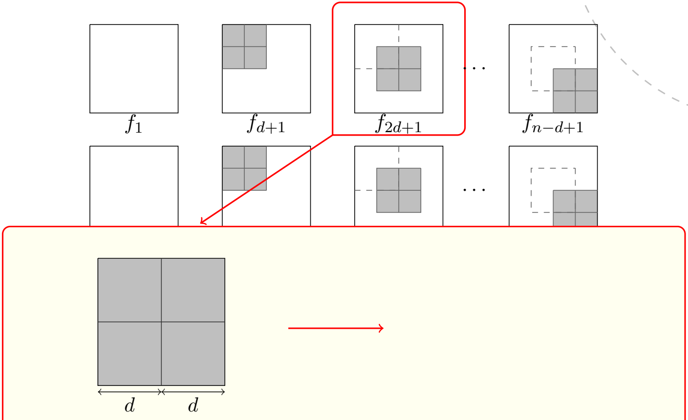
Matrix notation of $\mathcal{F}$

Crucial observation about the algebraic structure



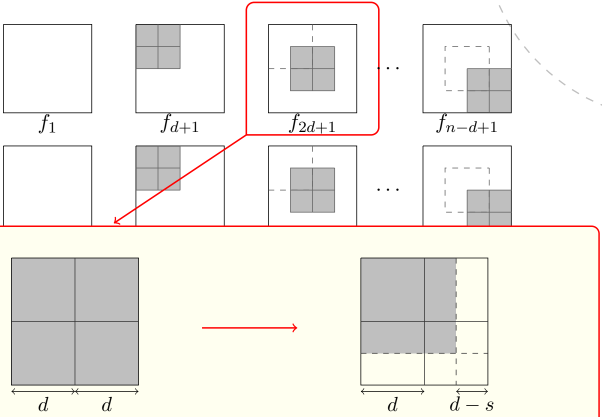
$\mathcal{P} = \quad T \quad \circ \quad \mathcal{F} \quad \circ \quad S$

Crucial observation about the algebraic structure



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

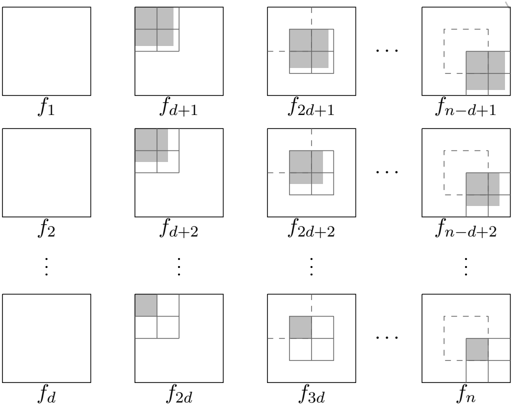
Crucial observation about the algebraic structure



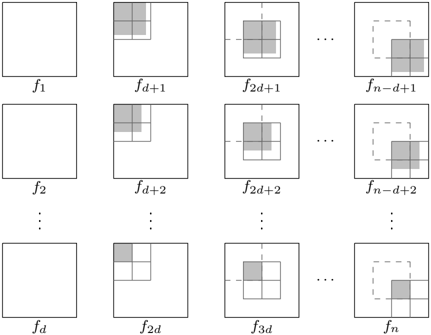
$\mathcal{P} = T \circ \mathcal{F} \circ S$

$\mathcal{P} = (T \cdot B_1) \circ \mathcal{F}' \circ (B_2 \cdot S)$

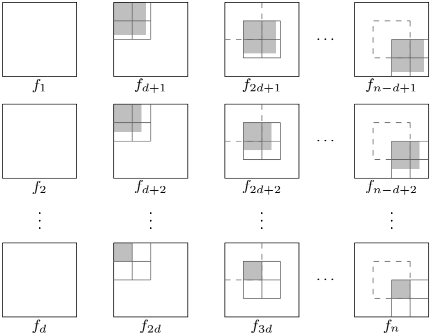
$\Longrightarrow$ We obtain an equivalent central map



Matrix notation of $\mathcal{F}'$

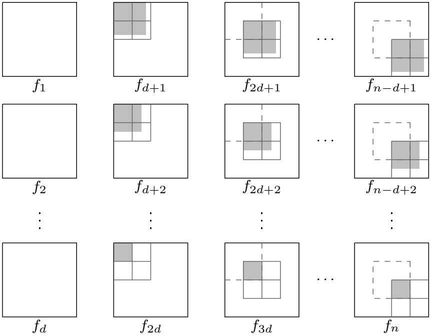


Initially, note



Initially, note

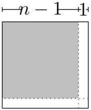
x_n does not occur quadratically!



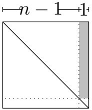
Initially, note

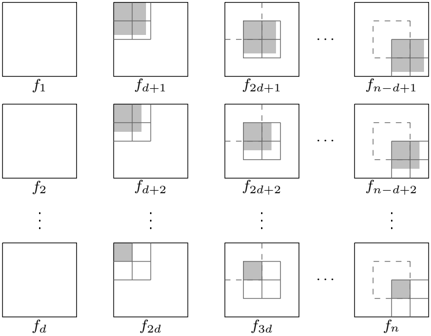
x_n does not occur quadratically!

Recover structure



Transform input space $\overline{S}'_n =$

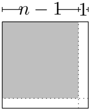




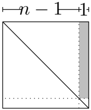
Initially, note

x_n does not occur quadratically!

Recover structure



Transform input space $\overline{S}'_n =$



Solve: ($m(n-1)$ linear equations in $(n-1)$ variables)

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

Key Recovery Attack

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

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

Step N**:**

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

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

end for;

Output: An equivalent key
$\overline{S}' = \overline{S}'_n \circ \overline{S}'_{n-1} \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_{n-1} \circ \overline{T}'_n$.

Key Recovery Attack

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

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

Step N**:**

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

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

end for;

Output: **An equivalent key**
$\overline{S}' = \overline{S}'_n \circ \overline{S}'_{n-1} \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_{n-1} \circ \overline{T}'_n$.

Essential structure preserved

Key Recovery Attack

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

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

The structure gradually revealed

Step N:

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

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

end for;

Output: **An equivalent key**
$\overline{S}' = \overline{S}'_n \circ \overline{S}'_{n-1} \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_{n-1} \circ \overline{T}'_n$.

Essential structure preserved

Key Recovery Attack

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

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

The structure gradually revealed

Step N**:**

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

one column at a time

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

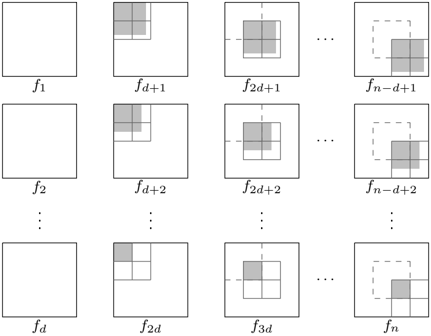
end for;

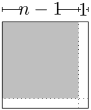
Output: **An equivalent key**
$\overline{S}' = \overline{S}'_n \circ \overline{S}'_{n-1} \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_{n-1} \circ \overline{T}'_n$.

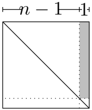
Essential structure preserved

Step n

x_n does not occur quadratically!

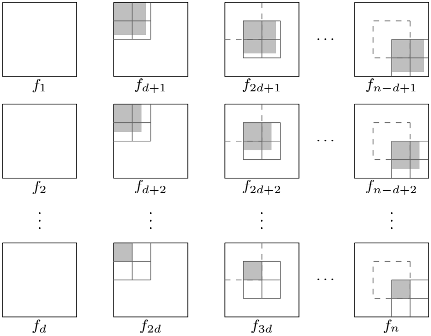


Recover structure 

Find good key $\overline{S}'_n =$ 

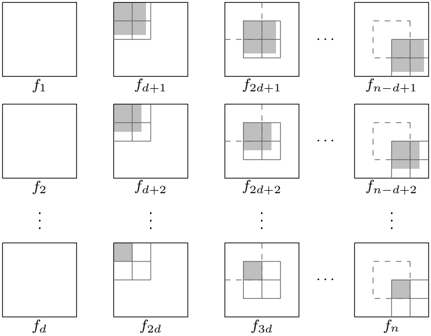
Solve: ($m(n-1)$ linear equations in $(n-1)$ variables)

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



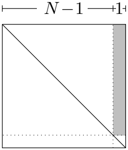
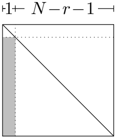
Step N

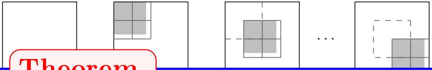
x_N occurs quadratically in at most one polynomial!



Step N

x_N occurs quadratically in at most one polynomial!

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



Step N

Theorem

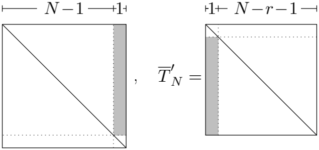
The solution of the **Simultaneous MinRank problems:**

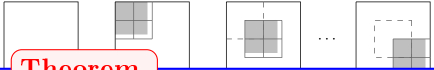
$$\text{Find } \overline{t}'_{k1} \in \mathbb{F}_q,\ 1 < k \leqslant N - r + 1 \text{ such that}$$

$$\text{Rank}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right) < N \quad \text{and} \quad \overline{s}' \in \bigcap_k \text{Ker}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right),$$

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

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





Step N

Theorem

The solution of the **Simultaneous MinRank problems:**

$$\text{Find } \overline{t}'_{k1} \in \mathbb{F}_q,\ 1 < k \leqslant N - r + 1 \text{ such that}$$

$$\text{Rank}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right) < N \quad \text{and} \quad \overline{s}' \in \bigcap_k \text{Ker}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right),$$

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

Kipnis-Shamir:

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

[$N(N-r+1)$ equations in $(N-1) + (N-r-1)$ variables]

Practical Key Recovery

Key Recovery MQQ-ENC

field	n	r	Security	Theoretical ($\omega = 3$)	Practical	time
$\mathbb{F}_2$	256	8	2^{128}	$\mathbf{2^{69}}$		
$\mathbb{F}_4$	128	4	2^{128}	$\mathbf{2^{59}}$	$\mathbf{2^{50.6}}$	**9.1 days**
$\mathbb{F}_{16}$	64	2	2^{128}	$\mathbf{2^{50}}$		
$\mathbb{F}_{256}$	32	1	2^{128}	$\mathbf{2^{40}}$		

Key Recovery MQQ-SIG

n	Security	Theoretical ($\omega = 3$)	Practical	time
160	2^{80}	$\mathbf{2^{62}}$	$\mathbf{2^{48.0}}$	**1.4 days**
192	2^{96}	$\mathbf{2^{65}}$		
224	2^{112}	$\mathbf{2^{67}}$		
256	2^{128}	$\mathbf{2^{69}}$		

Implemented in Magma 2.19-10 on 32 core Intel Xeon 2.27GHz, 1TB RAM.

Complexity Analysis – over even characteristic

Solving Simultaneous MinRank

Find $\overline{t}'_{k1} \in \mathbb{F}_q,\ 1 < k \leqslant N - r + 1$ **such that**

$$\text{Rank}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right) < N, \textbf{ and } \overline{s}' \in \bigcap \text{Ker}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right)$$

Complexity Analysis – over even characteristic

Solving Simultaneous MinRank

Find $\overline{t}'_{k1} \in \mathbb{F}_q,\ 1 < k \leqslant N - r + 1$ **such that**

$$\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right) < N, \textbf{ and } \overline{s}' \in \bigcap \mathrm{Ker}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right)$$

$q = \mathcal{O}(n)$

Solve one MinRank and use exhaustion over $\mathbb{F}_q$

Plausible to have small rank defect (for ex. 1)

Complexity Analysis – over even characteristic

Solving Simultaneous MinRank

Find $\overline{t}'_{k1} \in \mathbb{F}_q,\ 1 < k \leqslant N - r + 1$ **such that**

$$\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right) < N, \textbf{ and } \overline{s}' \in \bigcap \mathrm{Ker}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right)$$

$q = \mathcal{O}(n)$

Solve one MinRank and use exhaustion over $\mathbb{F}_q$

Plausible to have small rank defect (for ex. 1)

Theorem

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

with probability $1 - 1/q$.

Complexity Analysis – over even characteristic

Solving Simultaneous MinRank

Find $\overline{t}'_{k1} \in \mathbb{F}_q,\ 1 < k \leqslant N - r + 1$ **such that**

$$\mathrm{Rank}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right) < N, \textbf{ and } \overline{s}' \in \bigcap \mathrm{Ker}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right)$$

$q = \mathcal{O}(n)$ → **Solve one MinRank and use exhaustion over $\mathbb{F}_q$**

Plausible to have small rank defect (for ex. 1)

Any q → **Solve few of the MinRank(s)**

few=2 with high probability!

Theorem

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

with probability $1 - 1/q$.

Complexity Analysis – over even characteristic

Solving Simultaneous MinRank

Find $\overline{t}'_{k1} \in \mathbb{F}_q,\ 1 < k \leqslant N - r + 1$ **such that**

$$\text{Rank}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right) < N, \textbf{ and } \overline{s}' \in \bigcap \text{Ker}\left(\mathfrak{P}^{(k)} + \overline{t}'_{k1}\mathfrak{P}^{(1)}\right)$$

$q = \mathcal{O}(n)$ →

Solve one MinRank and use exhaustion over $\mathbb{F}_q$

Plausible to have small rank defect (for ex. 1)

Theorem

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

with probability $1 - 1/q$.

Any q →

Solve few of the MinRank(s)

few=2 with high probability!

Theorem

Complexity: $\mathcal{O}\left(n^{3\omega+1}\right)$

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

Practical Results

Key Recovery MQQ-ENC

field	n	r	Theoretical ($\omega = 3$)	Practical
$\mathbb{F}_2$	64	8	$\mathbf{2^{50}}$	$\mathbf{2^{43}}$
$\mathbb{F}_2$	96	8	$\mathbf{2^{55}}$	$\mathbf{2^{48}}$
$\mathbb{F}_4$	96	4	$\mathbf{2^{55}}$	$\mathbf{2^{48}}$
$\mathbb{F}_4$	128	4	$\mathbf{2^{59}}$	$\mathbf{2^{51}}$
$\mathbb{F}_{16}$	48	2	$\mathbf{2^{46}}$	$\mathbf{2^{39}}$
$\mathbb{F}_{16}$	64	2	$\mathbf{2^{50}}$	$\mathbf{2^{42}}$

Key Recovery MQQ-SIG

n	r	Theoretical ($\omega = 3$)	Practical
64	32	$\mathbf{2^{50}}$	$\mathbf{2^{40}}$
96	48	$\mathbf{2^{55}}$	$\mathbf{2^{43}}$
128	64	$\mathbf{2^{59}}$	$\mathbf{2^{46}}$
160	80	$\mathbf{2^{62}}$	$\mathbf{2^{48}}$

Implemented in Magma 2.19-10 on 32 core Intel Xeon 2.27GHz, 1TB RAM.

Practical Results

Key Recovery MQQ-ENC

field	n	r	Theoretical ($\omega = 3$)	Practical	Security	time
$\mathbb{F}_2$	64	8	$\mathbf{2^{50}}$	$\mathbf{2^{43}}$		
$\mathbb{F}_2$	96	8	$\mathbf{2^{55}}$	$\mathbf{2^{48}}$		
$\mathbb{F}_4$	96	4	$\mathbf{2^{55}}$	$\mathbf{2^{48}}$		
$\mathbb{F}_4$	128	4	$\mathbf{2^{59}}$	$\mathbf{2^{51}}$	$\mathbf{2^{128}}$	**9.1 days**
$\mathbb{F}_{16}$	48	2	$\mathbf{2^{46}}$	$\mathbf{2^{39}}$		
$\mathbb{F}_{16}$	64	2	$\mathbf{2^{50}}$	$\mathbf{2^{42}}$		

Key Recovery MQQ-SIG

n	r	Theoretical ($\omega = 3$)	Practical	Security	time
64	32	$\mathbf{2^{50}}$	$\mathbf{2^{40}}$		
96	48	$\mathbf{2^{55}}$	$\mathbf{2^{43}}$		
128	64	$\mathbf{2^{59}}$	$\mathbf{2^{46}}$		
160	80	$\mathbf{2^{62}}$	$\mathbf{2^{48}}$	$\mathbf{2^{80}}$	**1.4 days**

Implemented in Magma 2.19-10 on 32 core Intel Xeon 2.27GHz, 1TB RAM.

Conclusion

- **Very hard to design a secure scheme based on easily invertible MQQ structure**
  - For any advancement
    – **deeper insights in quasigroup theory needed**
- 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

- **Very hard to design a secure scheme based on easily invertible MQQ structure**
  - For any advancement
    – **deeper insights in quasigroup theory needed**
- 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

- **Very hard to design a secure scheme based on easily invertible MQQ structure**
  - For any advancement – **deeper insights in quasigroup theory needed**
- 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

- **Very hard to design a secure scheme based on easily invertible MQQ structure**
  - For any advancement – **deeper insights in quasigroup theory needed**
- 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!

?