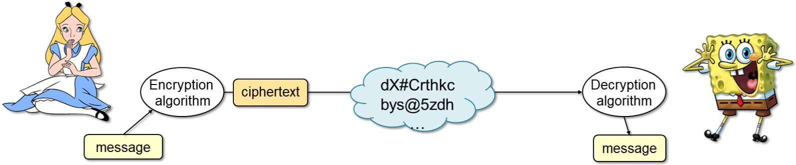
Quasigroups for cryptography

Simona Samardjiska

Digital Security Group, Radboud University, Nijmegen, The Netherlands

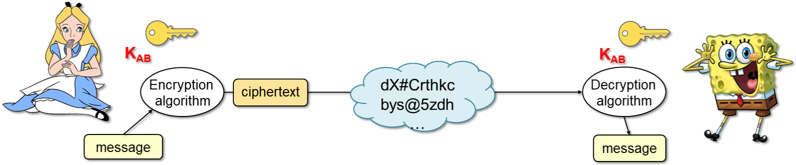
2019-07-12
LOOPS 19

A typical everyday scenario



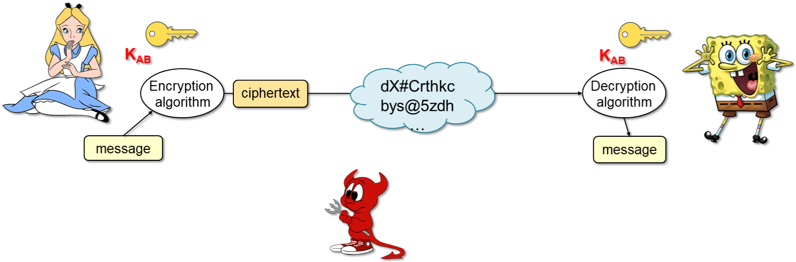
- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

A typical everyday scenario



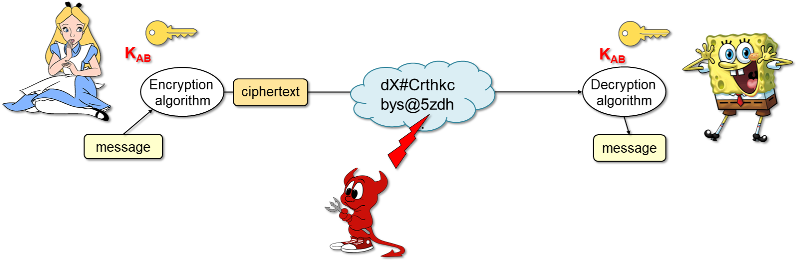
- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

A typical everyday scenario



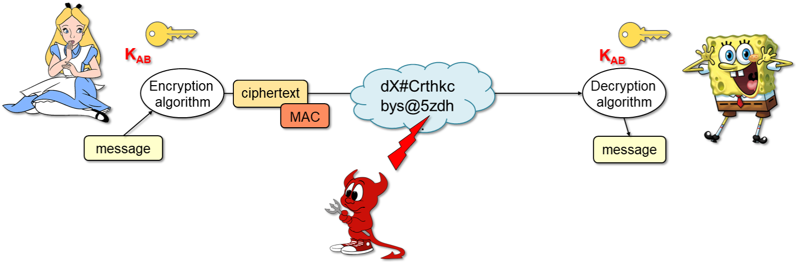
- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

A typical everyday scenario



- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

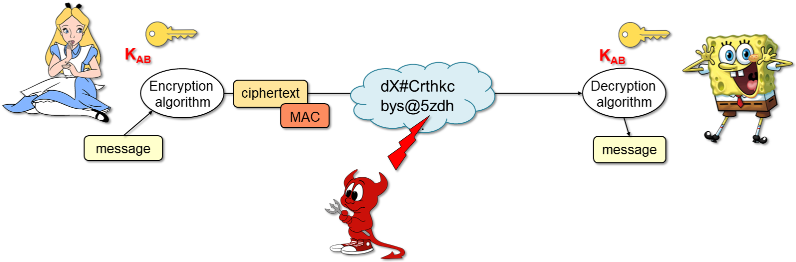
A typical everyday scenario



- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation

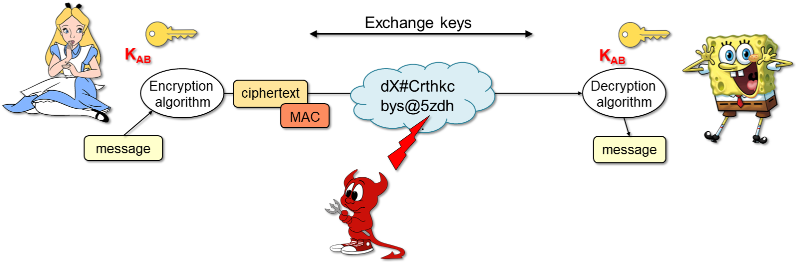
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

A typical everyday scenario



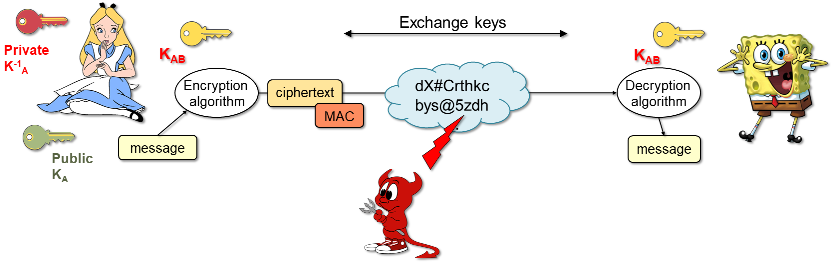
- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

A typical everyday scenario



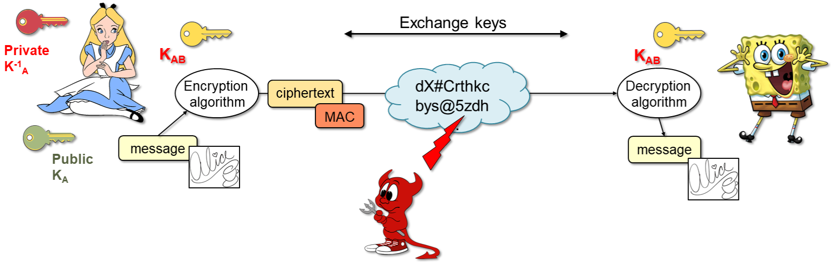
- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

A typical everyday scenario



- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

A typical everyday scenario



- Symmetric cryptography
  - Secrecy (encrypt the traffic)
  - Integrity of messages
- Public key cryptography
  - Exchange symmetric keys
  - Entity authentication
  - Non-repudiation
- Adversary
  - Can listen to the traffic (passive)
  - Can change the traffic (active)

Crypto comes in many flavors....(none of which is cryptocurrency)

- Symmetric cryptography
  - PRNGs
  - Stream ciphers
  - Block ciphers
  - hash functions
  - AEAD
  - Lightweight crypto
  - ...
- Public key cryptography
  - Digital signatures
  - Encryption schemes
  - KEMs
  - Identifications schemes
  - ...

Crypto comes in many flavors....(none of which is cryptocurrency)

- Symmetric cryptography
  - PRNGs
  - Stream ciphers
  - Block ciphers
  - hash functions
  - AEAD
  - Lightweight crypto
  - ...

- Public key cryptography
  - Digital signatures
  - Encryption schemes
  - KEMs
  - Identifications schemes
  - ...

Crypto comes in many flavors....(none of which is cryptocurrency) ... even in quasigroup flavor ...

- Symmetric cryptography
  - PRNGs
  - Stream ciphers
  - Block ciphers
  - hash functions
  - AEAD
  - Lightweight crypto
  - ...
- Public key cryptography
  - Digital signatures
  - Encryption schemes
  - KEMs
  - Identifications schemes
  - ...

Crypto comes in many flavors....(none of which is cryptocurrency)
... even in quasigroup flavor ...

- Symmetric cryptography
  - PRNGs
  - Stream ciphers Edon80
  - Block ciphers
  - hash functions NaSHA, EDON-R, BMW
  - AEAD π-cipher
  - Lightweight crypto GAGE, InGAGE
  - ...
- Public key cryptography
  - Digital signatures MQQ-Sig
  - Encryption schemes MQQ, MQQ-Enc
  - KEMs Edon-K
  - Identifications schemes Keedwel IDS
  - ...

Typical design choices in quasigroup based cryptography

- Quasigroups of order 4
  - Edon80, GAGE, InGAGE
- Quasigroups string transformations
  - All designs
- Mixing using Orthogonal latin squares
  - All symmetric designs
- Huge quasigroups from ARX operations
  - Edon-R, π-Cipher, BMW
- Multivariate Quadratic Quasigroups (MQQ)
  - MQQ-Sig, MQQ-Enc, IDS from quasigroups

$\bullet_0$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

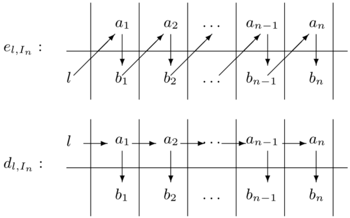
$\bullet_1$	0	1	2	3
0	1	3	0	2
1	0	1	2	3
2	2	0	3	1
3	3	2	1	0

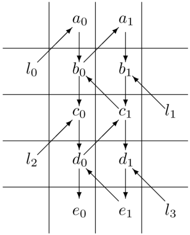
$\bullet_2$	0	1	2	3
0	2	1	0	3
1	1	2	3	0
2	3	0	2	1
3	0	3	1	2

$\bullet_3$	0	1	2	3
0	3	2	1	0
1	1	0	3	2
2	0	3	2	1
3	2	1	0	3

Typical design choices in quasigroup based cryptography

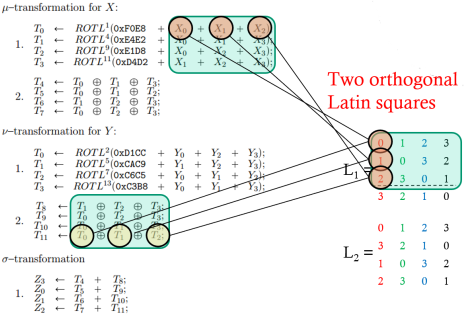
- Quasigroups of order 4
  - Edon80, GAGE, InGAGE
- Quasigroups string transformations
  - All designs
- Mixing using Orthogonal latin squares
  - All symmetric designs
- Huge quasigroups from ARX operations
  - Edon-R, π-Cipher, BMW
- Multivariate Quadratic Quasigroups (MQQ)
  - MQQ-Sig, MQQ-Enc, IDS from quasigroups





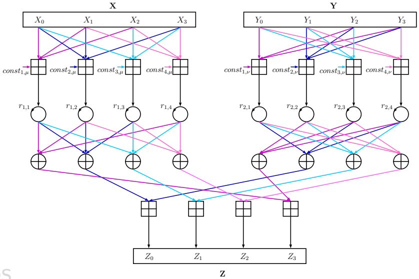
Typical design choices in quasigroup based cryptography

- Quasigroups of order 4
  - Edon80, GAGE, InGAGE
- Quasigroups string transformations
  - All designs
- Mixing using Orthogonal latin squares
  - All symmetric designs
- Huge quasigroups from ARX operations
  - Edon-R, π-Cipher, BMW
- Multivariate Quadratic Quasigroups (MQQ)
  - MQQ-Sig, MQQ-Enc, IDS from quasigroups



Typical design choices in quasigroup based cryptography

- Quasigroups of order 4
  - Edon80, GAGE, InGAGE
- Quasigroups string transformations
  - All designs
- Mixing using Orthogonal latin squares
  - All symmetric designs
- Huge quasigroups from ARX operations
  - Edon-R, π-Cipher, BMW
- Multivariate Quadratic Quasigroups (MQQ)
  - MQQ-Sig, MQQ-Enc, IDS from quasigroups



Typical design choices in quasigroup based cryptography

- Quasigroups of order 4
  - Edon80, GAGE, InGAGE
- Quasigroups string transformations
  - All designs
- Mixing using Orthogonal latin squares
  - All symmetric designs
- Huge quasigroups from ARX operations
  - Edon-R, π-Cipher, BMW
- Multivariate Quadratic Quasigroups (MQQ)
  - MQQ-Sig, MQQ-Enc, IDS from quasigroups

MQQ of order 8

*	0	1	2	3	4	5	6	7
0	2	3	6	7	0	1	5	4
1	6	7	5	4	2	3	0	1
2	3	2	7	6	1	0	4	5
3	7	6	4	5	3	2	1	0
4	4	5	0	1	7	6	2	3
5	0	1	3	2	5	4	7	6
6	5	4	1	0	6	7	3	2
7	1	0	2	3	4	5	6	7

$$q = (q^{(1)}, q^{(2)}, q^{(3)}) : \mathbb{F}_2^6 \to \mathbb{F}_2^3$$

$$q^{(1)} = x_1 + x_3 + y_2 + x_1y_2 + x_1y_3,$$
$$q^{(2)} = 1 + x_3 + x_1y_2 + y_3 + x_1y_3,$$
$$q^{(3)} = x_2 + y_1 + x_1y_2 + x_3y_3 + y_2y_3$$

The status of these cryptosystems?

- Symmetric cryptography
  - Stream ciphers Edon80
  - hash functions NaSHA, EDON-R, BMW
  - AEAD π-cipher
  - Lightweight crypto GAGE, InGAGE
- Public key cryptography
  - Digital signatures MQQ-Sig
  - Encryption schemes MQQ, MQQ-Enc
  - KEMs Edon-K
  - Identifications schemes Keedwel IDS
- Some broken, some avoided
- Problems: Lack of understanding the security
- Needed: Minimal assumptions and standard evaluation of security

The status of these cryptosystems?

- Symmetric cryptography
  - Stream ciphers Edon80
  - hash functions NaSHA, EDON-R, BMW
  - AEAD π-cipher
  - Lightweight crypto GAGE, InGAGE
- Public key cryptography
  - Digital signatures MQQ-Sig
  - Encryption schemes MQQ, MQQ-Enc
  - KEMs Edon-K
  - Identifications schemes Keedwel IDS
- Some broken, some avoided
- Problems: Lack of understanding the security
- Needed: Minimal assumptions and standard evaluation of security

Standard security evaluation in symmetric key crypto

Security from ideal primitives $+$ Cryptanalysis of real constructions

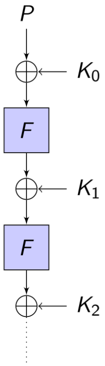


Figure: Typical Design

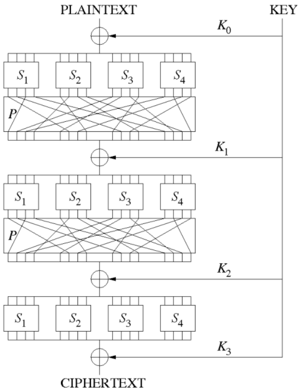


Figure: Classical SPN

Linear cryptanalysis

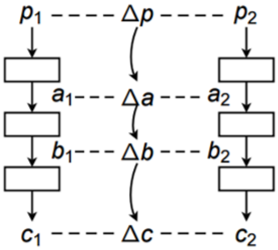
- Invented by Mitsuru Matsui 1993
- Main idea:
  1. approximate the non-linear parts of the cipher by a linear relation between plaintext, (partial) keys and ciphertext
  2. calculate the probability that the relation holds
  3. if high enough, use as a distinguisher or a key recovery attack

Linear cryptanalysis

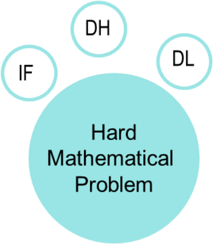
- Invented by Mitsuru Matsui 1993
- Main idea:
  1. approximate the non-linear parts of the cipher by a linear relation between plaintext, (partial) keys and ciphertext
  2. calculate the probability that the relation holds
  3. if high enough, use as a distinguisher or a key recovery attack

Differential cryptanalysis

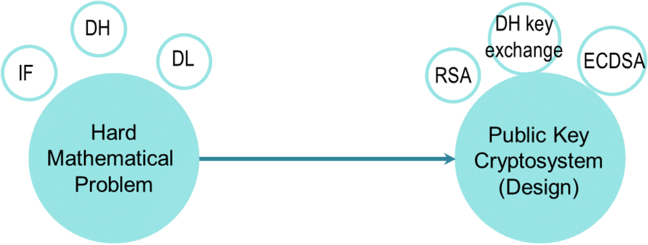
- Invented by Biham and Shamir, late '80s
- Main idea:
  1. Observe the difference between two ciphertexts as a function of the difference between the plaintexts
  2. Find the highest probability differential through several rounds
  3. if high enough, use as a distinguisher or a key recovery attack



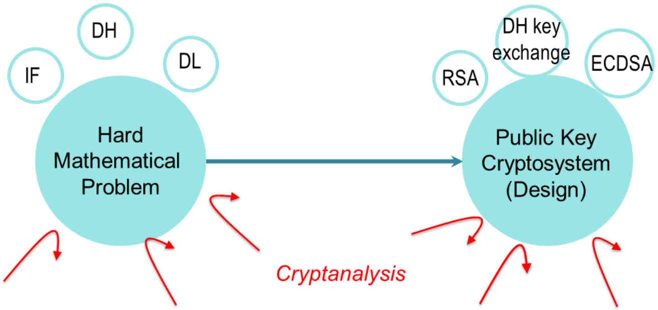
Standard security evaluation in public key crypto



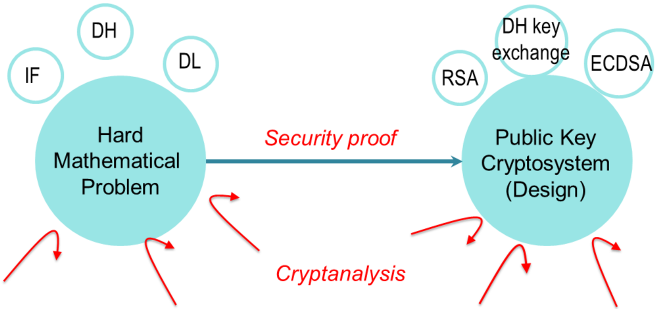
Standard security evaluation in public key crypto



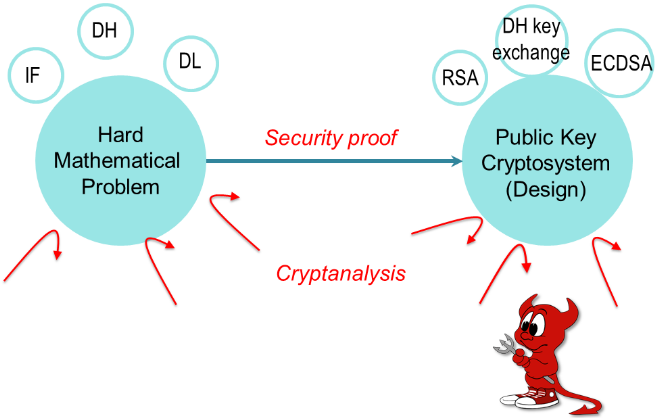
Standard security evaluation in public key crypto



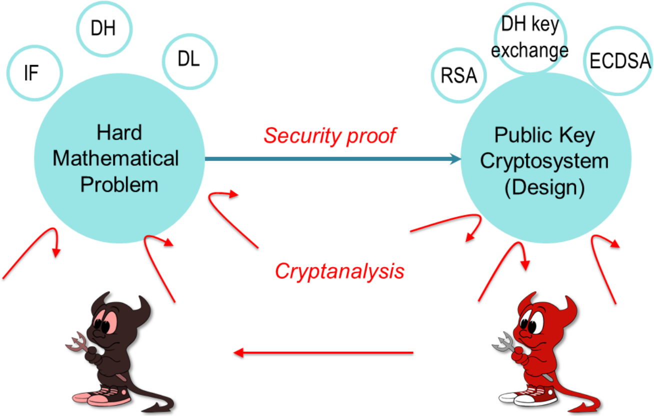
Standard security evaluation in public key crypto



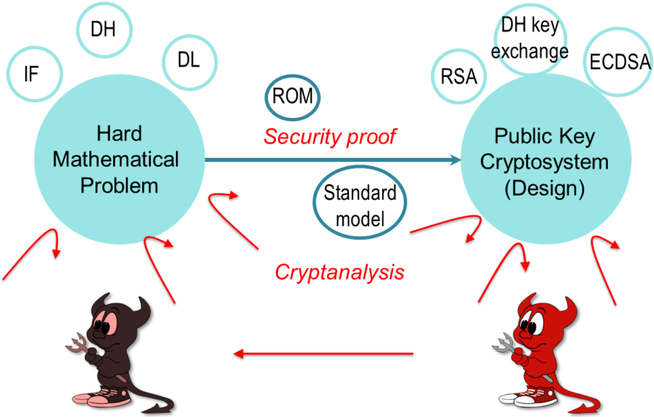
Standard security evaluation in public key crypto



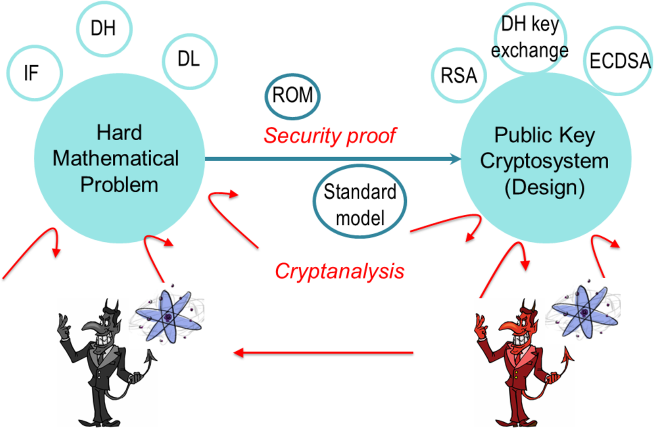
Standard security evaluation in public key crypto



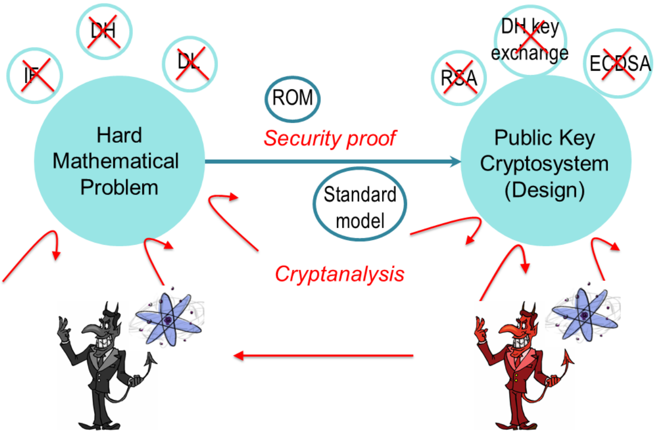
Standard security evaluation in public key crypto



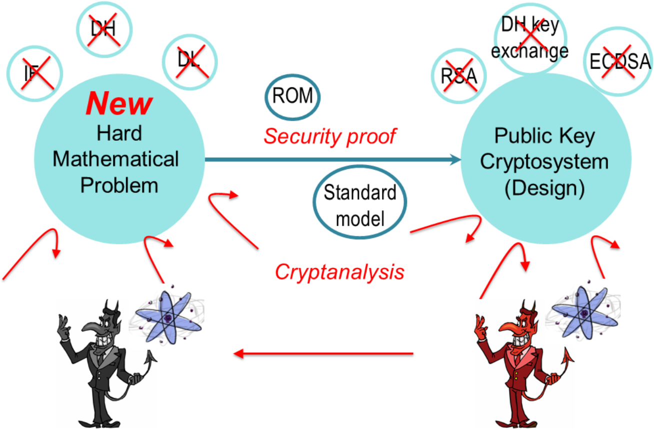
Standard security evaluation in public key crypto



Standard security evaluation in public key crypto



Standard security evaluation in public key crypto



Linearity measures for (n, m)-functions

Linearity measures for (n, m)-functions

Linearity of (n, m) functions $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$:

$$\mathcal{L}(f) = \max_{w \in \mathbb{F}_q^m \setminus \{0\}, u \in \mathbb{F}_q^n} \left| \sum_{x \in \mathbb{F}_q^n} (-1)^{w^\intercal \cdot f(x) + u^\intercal \cdot x} \right|$$

Nonlinearity of (n, m) functions f:

$$\mathcal{N}(f) = (q-1)(q^{n-1} - \frac{1}{q}\mathcal{L}(f)).$$

$w \in \mathbb{F}_q^n$ - **linear structure** of f if

$$D_w f(x) = f(x+w) - f(x) = f(w) - f(0) \quad \forall\, x \in \mathbb{F}_q^n.$$

Linear space of f - generated by the linear structures of f.

Linearity measures for (n, m)-functions

Linearity of (n, m) functions $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$:

$$\mathcal{L}(f) = \max_{w \in \mathbb{F}_q^m \setminus \{0\}, u \in \mathbb{F}_q^n} \left| \sum_{x \in \mathbb{F}_q^n} (-1)^{w^\intercal \cdot f(x) + u^\intercal \cdot x} \right|$$

Nonlinearity of (n, m) functions f:

$$\mathcal{N}(f) = (q-1)(q^{n-1} - \frac{1}{q}\mathcal{L}(f)).$$

$w \in \mathbb{F}_q^n$ - **linear structure** of f if

$$D_w f(x) = f(x+w) - f(x) = f(w) - f(0) \quad \forall\, x \in \mathbb{F}_q^n .$$

Linear space of f - generated by the linear structures of f.

Linearity measures for (n, m)-functions

Linearity of (n, m) functions $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$:

$$\mathcal{L}(f) = \max_{w \in \mathbb{F}_q^m \setminus \{0\}, u \in \mathbb{F}_q^n} \left| \sum_{x \in \mathbb{F}_q^n} (-1)^{w^\intercal \cdot f(x) + u^\intercal \cdot x} \right|$$

Nonlinearity of (n, m) functions f:

$$\mathcal{N}(f) = (q-1)(q^{n-1} - \frac{1}{q}\mathcal{L}(f)).$$

$w \in \mathbb{F}_q^n$ - **linear structure** of f if

$$D_w f(x) = f(x+w) - f(x) = f(w) - f(0) \quad \forall\, x \in \mathbb{F}_q^n.$$

Linear space of f - generated by the linear structures of f.

Linearity measures for (n, m)-functions

[Nyberg92] **Quadratic form f:**

- $x^{\intercal}\mathfrak{F}x$, $\mathrm{Rank}(\mathfrak{F}) = r$.
- $\mathrm{Ker}(\mathfrak{F})$ - **linear space of f.**

$$\mathcal{L}(f) = q^{n-\frac{r}{2}}$$

[Nyberg92] **Quadratic (n, m)-function f:**

- Linearity - measured using the **smallest rank r** of any of the components $w^{\intercal} \cdot f$.

Linearity measures for (n, m)-functions

[Nyberg92] **Quadratic form f:**

- $x^\intercal \mathfrak{F} x$, $\mathrm{Rank}(\mathfrak{F}) = r$.
- $\mathrm{Ker}(\mathfrak{F})$ - **linear space of f.**

$$\mathcal{L}(f) = q^{n - \frac{r}{2}}$$

[Nyberg92] **Quadratic** (n, m)**-function** f**:**

- Linearity - measured using the **smallest rank** r of any of the components $w^\intercal \cdot f$.

Linearity measures for (n, m)-functions

[Nyberg92] **Quadratic form f:**

- $x^\intercal \mathfrak{F} x$, $\mathrm{Rank}(\mathfrak{F}) = r$.
- $\mathrm{Ker}(\mathfrak{F})$ - **linear space of f.**

$$\mathcal{L}(f) = q^{n-\frac{r}{2}}$$

[Nyberg92] **Quadratic (n, m)-function f:**

- Linearity - measured using the **smallest rank r** of any of the components $w^\intercal \cdot f$.

Maximum nonlinearity:

- **Bent functions** - $\mathrm{Rank}(\mathfrak{F}_v) = n$, even n, $m \leqslant n/2$,
- **Almost bent (AB) functions** - $\mathrm{Rank}(\mathfrak{F}_v) = n - 1$, odd $n = m$.

Example 1:

f :

$$\begin{aligned} f_1 &= x_1x_2 + x_3 \\ f_2 &= x_1x_3 + x_2 + x_3 \\ f_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f_4 &= x_1x_2 \end{aligned}$$

$\mathcal{L}(f) = 2^3$

$(1,0,0,1)^\intercal \quad \cdot f$ is linear

f' :

$$\begin{aligned} f'_1 &= x_1x_2 + x_3 \\ f'_2 &= x_1x_2 + x_2 + x_3 \\ f'_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f'_4 &= x_1x_2 + x_2x_3 \end{aligned}$$

$\mathcal{L}(f') = 2^3$

$(1,0,1,1)^\intercal \quad \cdot f'$ is linear

$(1,1,0,0)^\intercal \quad \cdot f'$ is linear

Example 1:

f :

$$\begin{aligned} f_1 &= x_1x_2 + x_3 \\ f_2 &= x_1x_3 + x_2 + x_3 \\ f_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f_4 &= x_1x_2 \end{aligned}$$

$\mathcal{L}(f) = 2^3$

$(1,0,0,1)^\intercal \quad \cdot f$ is linear

f' :

$$\begin{aligned} f'_1 &= x_1x_2 + x_3 \\ f'_2 &= x_1x_2 + x_2 + x_3 \\ f'_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f'_4 &= x_1x_2 + x_2x_3 \end{aligned}$$

$\mathcal{L}(f') = 2^3$

$(1,0,1,1)^\intercal \quad \cdot f'$ is linear

$(1,1,0,0)^\intercal \quad \cdot f'$ is linear

Example 1:

f :

$$\begin{aligned} f_1 &= x_1x_2 + x_3 \\ f_2 &= x_1x_3 + x_2 + x_3 \\ f_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f_4 &= x_1x_2 \end{aligned}$$

$\mathcal{L}(f) = 2^3$

$(1,0,0,1)^\intercal \cdot f$ is linear

f' :

$$\begin{aligned} f'_1 &= x_1x_2 + x_3 \\ f'_2 &= x_1x_2 + x_2 + x_3 \\ f'_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f'_4 &= x_1x_2 + x_2x_3 \end{aligned}$$

$\mathcal{L}(f') = 2^3$

$(1,0,1,1)^\intercal \cdot f'$ is linear

$(1,1,0,0)^\intercal \cdot f'$ is linear

It is important to measure the size of!

Example 2: Oil & Vinegar

f :

$$f_1(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4 + x_1x_2 + x_3$$
$$f_2(x_1, x_2, x_3, x_4) = x_2x_3 + x_1x_4 + x_2x_4 + x_3$$

$\mathcal{L}(f) = 2^2$

$$f_1(c_1, c_2, x_3, x_4) = c_1x_3 + c_2x_4 + c_1c_2 + x_3$$
$$f_2(c_1, c_2, x_3, x_4) = c_2x_3 + c_1x_4 + c_2x_4 + x_3$$

f is linear on the oil subspace!

Example 2: Oil & Vinegar

f :

$$f_1(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4 + x_1x_2 + x_3$$
$$f_2(x_1, x_2, x_3, x_4) = x_2x_3 + x_1x_4 + x_2x_4 + x_3$$

$\mathcal{L}(f) = 2^2$

$$f_1(c_1, c_2, x_3, x_4) = c_1x_3 + c_2x_4 + c_1c_2 + x_3$$
$$f_2(c_1, c_2, x_3, x_4) = c_2x_3 + c_1x_4 + c_2x_4 + x_3$$

f is linear on the oil subspace!

Example 2: Oil & Vinegar

f :

$$f_1(x_1, x_2, x_3, x_4) = x_1 x_3 + x_2 x_4 + x_1 x_2 + x_3$$
$$f_2(x_1, x_2, x_3, x_4) = x_2 x_3 + x_1 x_4 + x_2 x_4 + x_3$$

$\mathcal{L}(f) = 2^2$

$$f_1(c_1, c_2, x_3, x_4) = c_1 x_3 + c_2 x_4 + c_1 c_2 + x_3$$
$$f_2(c_1, c_2, x_3, x_4) = c_2 x_3 + c_1 x_4 + c_2 x_4 + x_3$$

f is linear on the oil subspace!

(s,t)–linearity of quadratic (n,m) function f

Boura and Canteaut FSE13:

f is said to be **(s,t)–linear** if there exist linear subspaces $V \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V) = s$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(W) = t$, s.t.

$$\forall\, w \in W, \;\; w^{\intercal} \cdot f \text{ is linear on all cosets } V \oplus a \text{ of } V.$$

(s,t)–linearity of quadratic (n,m) function f

Boura and Canteaut FSE13:

f is said to be **(s,t)–linear** if there exist linear subspaces $V \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V) = s$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(W) = t$, s.t.

$$\forall\ w \in W,\ \ w^\intercal \cdot f \text{ is linear on all cosets } V \oplus a \text{ of } V.$$

- f_W corresponding to all $w^\intercal \cdot f$, $w \in W$ can be written as

$$f_W(x,y) = M(x) \cdot y + G(x)$$

where $\mathbb{F}_q^n = U \oplus V$, $G : U \to \mathbb{F}_q^t$ and $M(x)$ is a $t \times s$ matrix with rows - components of linear functions over U.

(s,t)–linearity of quadratic (n,m) function f

Boura and Canteaut FSE13:

f is said to be **(s,t)–linear** if there exist linear subspaces $V \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V) = s$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(W) = t$, s.t.

$$\forall\ w \in W,\ \ w^{\intercal} \cdot f \text{ is linear on all cosets } V \oplus a \text{ of } V.$$

- f_W corresponding to all $w^{\intercal} \cdot f$, $w \in W$ can be written as

$$f_W(x,y) = M(x) \cdot y + G(x)$$

  where $\mathbb{F}_q^n = U \oplus V$, $G : U \to \mathbb{F}_q^t$ and $M(x)$ is a $t \times s$ matrix with rows - components of linear functions over U.

- for $w \in W$, $\quad D_{a,b}(w^{\intercal} \cdot f) = 0, \quad \forall\ a, b \in V$.

Example:

$$f_1(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4 + x_1x_2 + x_3$$
$$f_2(x_1, x_2, x_3, x_4) = x_2x_3 + x_1x_4 + x_2x_4 + x_3$$

f is $(2, 2)$–linear,
$V = \langle (0, 0, 1, 0), (0, 0, 0, 1) \rangle$, $W = \langle (1, 0), (0, 1) \rangle$

$$f_1(x_1, x_2, x_3, x_4) = x_1x_3 + x_1x_4 + x_2$$
$$f_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_4 + x_1x_3$$
$$f_3(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_3 + x_2x_4$$

f is $(3, 2)$–linear,
$V = \langle (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1) \rangle$, $W = \langle (1, 0, 0), (0, 1, 0) \rangle$

Example:

$$f_1(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4 + x_1x_2 + x_3$$
$$f_2(x_1, x_2, x_3, x_4) = x_2x_3 + x_1x_4 + x_2x_4 + x_3$$

f is $(2,2)$–linear,
$V = \langle(0,0,1,0),(0,0,0,1)\rangle,\ W = \langle(1,0),(0,1)\rangle$

$$f_1(x_1, x_2, x_3, x_4) = x_1x_3 + x_1x_4 + x_2$$
$$f_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_4 + x_1x_3$$
$$f_3(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_3 + x_2x_4$$

f is $(3,2)$–linear,
$V = \langle(0,1,0,0),(0,0,1,0),(0,0,0,1)\rangle,\ W = \langle(1,0,0),(0,1,0)\rangle$

Strong (s,t)–linearity of quadratic (n,m) function f

f is said to be **strongly (s,t)–linear** if there exist subspaces $V \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V) = s$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(W) = t$, s.t.

$$\forall\, w \in W, \;\; V \subset \mathrm{Ker}(w^{\mathsf{T}} \cdot f).$$

Strong (s, t)–linearity of quadratic (n, m) function f

f is said to be **strongly (s, t)–linear** if there exist subspaces $V \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V) = s$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(W) = t$, s.t.

$$\forall\, w \in W, \;\; V \subset \mathrm{Ker}(w^\intercal \cdot f).$$

- f_W corresponding to all $w^\intercal \cdot f$, $w \in W$ can be written as

$$f_W(x, y) = g_W(x) + L_W(y)$$

where $\mathbb{F}_q^n = U \oplus V$, $g_W : U \to \mathbb{F}_q^t$ and $L_W : V \to \mathbb{F}_q^t$ is linear.

Strong (s,t)–linearity of quadratic (n,m) function f

f is said to be **strongly (s,t)–linear** if there exist subspaces $V \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V) = s$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(W) = t$, s.t.

$$\forall\, w \in W, \;\; V \subset \mathrm{Ker}(w^\intercal \cdot f).$$

- f_W corresponding to all $w^\intercal \cdot f$, $w \in W$ can be written as

$$f_W(x,y) = g_W(x) + L_W(y)$$

where $\mathbb{F}_q^n = U \oplus V$, $g_W : U \to \mathbb{F}_q^t$ and $L_W : V \to \mathbb{F}_q^t$ is linear.

- for $w \in W$

$$D_a(w^\intercal \cdot f) = const., \quad \forall\, a \in V.$$

Example:

f :

$$\begin{aligned} f_1 &= x_1x_2 + x_3 \\ f_2 &= x_1x_3 + x_2 + x_3 \\ f_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f_4 &= x_1x_2 \end{aligned}$$

strongly $(3,1)$–linear
$V = \mathbb{F}_2^3$
$W = \langle(1,0,0,1)\rangle$

f' :

$$\begin{aligned} f_1 &= x_1x_2 + x_3 \\ f_2 &= x_1x_2 + x_2 + x_3 \\ f_3 &= x_2x_3 + x_1 + x_2 + x_3 \\ f_4 &= x_1x_2 + x_2x_3 \end{aligned}$$

strongly $(3,2)$–linear
$V = \mathbb{F}_2^3$
$W = \langle(1,1,0,0),(1,0,1,1)\rangle$

Simple but important properties

- **Strong** (s, t)**–linearity**
  $\Rightarrow$ **Strong** $(s-1, t)$**–linearity**
  $\Rightarrow$ **Strong** $(s, t-1)$**–linearity**
- (s, t)**–linearity**
  $\Rightarrow$ $(s-1, t)$**–linearity**
  $\Rightarrow$ $(s, t-1)$**–linearity**
- **Strong** (s, t)**–linearity** $\Rightarrow$ (s, t)**–linearity**

New development in linear attacks

- Propagation of affine subspaces
  - linked to both (s, t)–linearity and strong (s, t)–linearity
  - asks for classification of functions with respect to these two properties
- Invariant subspace attacks
  - powerful against lightweight ciphers
  - explained only recently [Leander et al. '15, Beierle et al. '17, Beyne '18, Liu et al. '19]

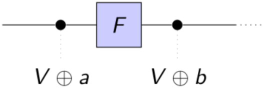
New development in linear attacks

- Propagation of affine subspaces
  - linked to both (s, t)–linearity and strong (s, t)–linearity
  - asks for classification of functions with respect to these two properties
- Invariant subspace attacks
  - powerful against lightweight ciphers
  - explained only recently [Leander et al. '15, Beierle et al. '17, Beyne '18, Liu et al. '19]

New development in linear attacks

- Propagation of affine subspaces
  - linked to both (s,t)–linearity and strong (s,t)–linearity
  - asks for classification of functions with respect to these two properties

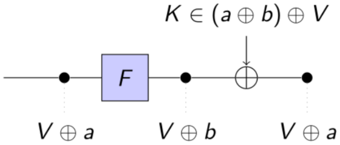
- Invariant subspace attacks
  - powerful against lightweight ciphers
  - explained only recently [Leander et al. '15, Beierle et al. '17, Beyne '18, Liu et al. '19]



Consider a permutation formed by iterating a permutation F xored with a fixed round key K. Assume the round function maps a coset $V \oplus a$ to a coset $V \oplus b$

New development in linear attacks

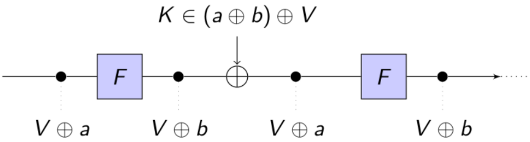
- Propagation of affine subspaces
  - linked to both (s, t)–linearity and strong (s, t)–linearity
  - asks for classification of functions with respect to these two properties
- Invariant subspace attacks
  - powerful against lightweight ciphers
  - explained only recently [Leander et al. '15, Beierle et al. '17, Beyne '18, Liu et al. '19]



...and that the fixed round key K is in $V \oplus (a \oplus b)$.

New development in linear attacks

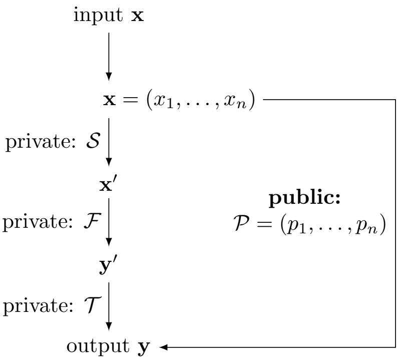
- Propagation of affine subspaces
  - linked to both (s, t)–linearity and strong (s, t)–linearity
  - asks for classification of functions with respect to these two properties
- Invariant subspace attacks
  - powerful against lightweight ciphers
  - explained only recently [Leander et al. '15, Beierle et al. '17, Beyne '18, Liu et al. '19]



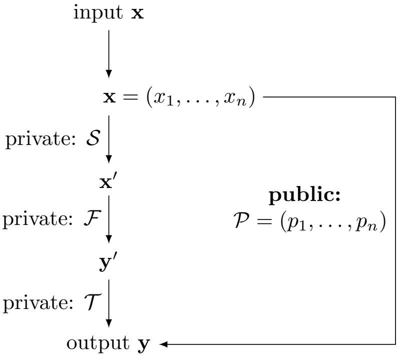
Then this process repeats itself.
Plaintexts in coset $V \oplus a$ are mapped to itself

Strong (s, t)–linearity vs $\mathcal{MQ}$ cryptography

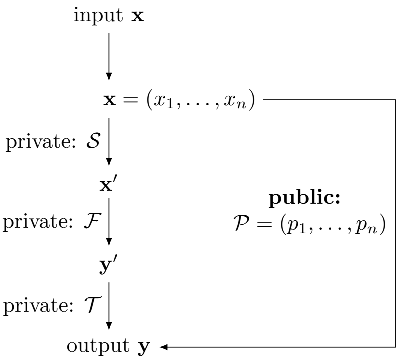
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



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



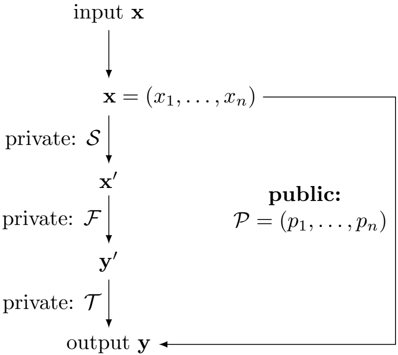
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



Public $\mathcal{P}$

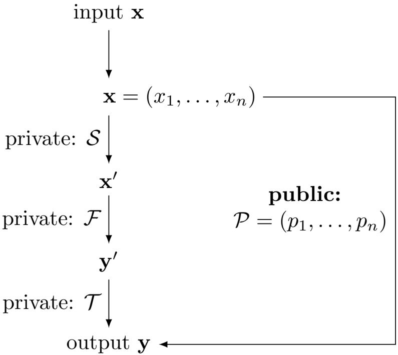
$$p_1(x_1, \ldots, x_n)$$
$$p_2(x_1, \ldots, x_n)$$
$$\ldots$$
$$p_m(x_1, \ldots, x_n)$$

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



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

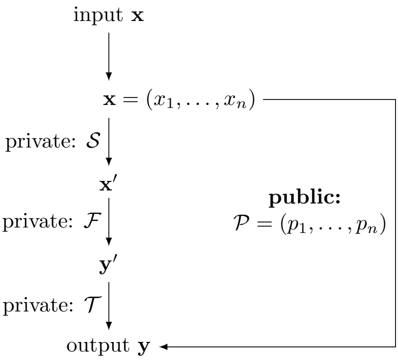
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



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

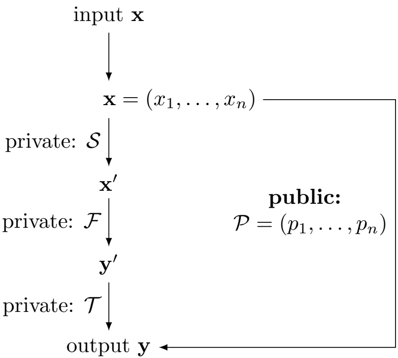
Symmetric matrices representing the quadratic part of the polynomials

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



Inverting $\mathcal{P}$ should be hard

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:

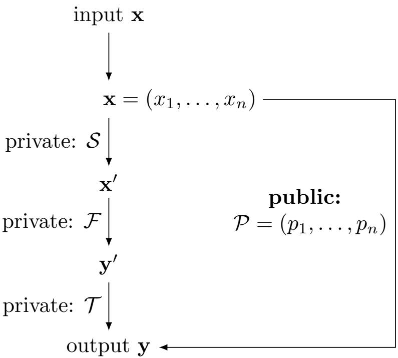
$p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$

Question:

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

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

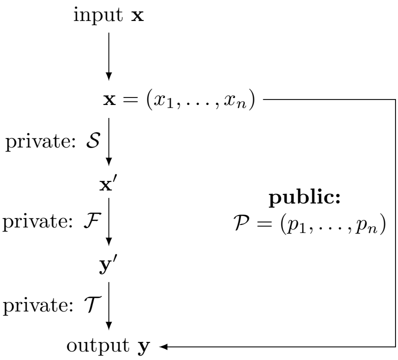
Multivariate ($\mathcal{MQ}$) public key scheme: $\mathbb{F}_q^n \to \mathbb{F}_q^m$



Attacks:

- MinRank
- Reconciliation/
  Band separation attack
- Equivalent keys/
  Good keys
- Differential attacks

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



Attacks:

Linear subspaces!

- **MinRank**
- **Reconciliation/ Band separation attack**
- **Equivalent keys/ Good keys**
- Differential attacks

MinRank $MR(n, m, r, M_1, \ldots, M_m)$

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

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

[Courtois '01], [Buss & Shallit '99]

- **NP-hard!!!**, however,
- **Instances in $\mathcal{MQ}$ crypto** can be **much easier**, even **polynomial!**
- Underlays the security of HFE, MQQ, Rainbow, LUOV, GeMss
- Underlies the security of Code based cryptosystems in the rank metric
  Decoding is essentially structured MinRank
- Very recently [S, Santini, Perisheti, Banegas '19]
  Decryption failure attack for Rank based cryptosystems

MinRank $MR(n, m, r, M_1, \ldots, M_m)$

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

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

[Courtois '01], [Buss & Shallit '99]

- **NP-hard!!!**, however,
- **Instances in $\mathcal{MQ}$ crypto** can be **much easier**, even **polynomial!**
- Underlays the security of HFE, MQQ, Rainbow, LUOV, GeMss
- Underlies the security of Code based cryptosystems in the rank metric
  Decoding is essentially structured MinRank
- Very recently [S, Santini, Perisheti, Banegas '19]
  Decryption failure attack for Rank based cryptosystems

MinRank $MR(n, m, r, M_1, \ldots, M_m)$

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

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

[Courtois '01], [Buss & Shallit '99]

- **NP-hard!!!**, however,
- **Instances in $\mathcal{MQ}$ crypto** can be **much easier**, even **polynomial!**
- Underlays the security of HFE, MQQ, Rainbow, LUOV, GeMss
- Underlies the security of Code based cryptosystems in the rank metric
  Decoding is essentially structured MinRank
- Very recently [S, Santini, Perisheti, Banegas '19]
  Decryption failure attack for Rank based cryptosystems

MinRank $MR(n, m, r, M_1, \ldots, M_m)$

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

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

[Courtois '01], [Buss & Shallit '99]

- **NP-hard!!!**, however,
- **Instances in $\mathcal{MQ}$ crypto** can be **much easier**, even **polynomial!**
- Underlays the security of HFE, MQQ, Rainbow, LUOV, GeMss
- Underlies the security of Code based cryptosystems in the rank metric
  Decoding is essentially structured MinRank
- Very recently [S, Santini, Perisheti, Banegas '19]
  Decryption failure attack for Rank based cryptosystems

Solving MinRank - Kipnis-Shamir modeling

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

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

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

Solving MinRank - Kipnis-Shamir modeling

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

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

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

- Relinearization [Kipnis & Shamir '99]

Solving MinRank - Kipnis-Shamir modeling

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

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

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

- Gröbner bases [Faugère & Levy-dit-Vehel & Perret '08]
  - Complexity of F5 algorithm: $\mathcal{O}\left(\binom{n+d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^{\omega}\right)$ [Faugère '02]

Solving MinRank - Kipnis-Shamir modeling

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

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

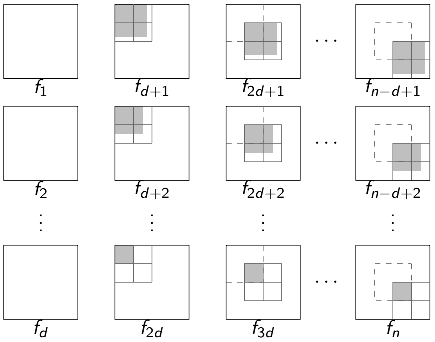
$n(n-r)$ quadratic (bilinear) equations in $r(n-r)+m$ variables

- Gröbner bases [Faugère & Levy-dit-Vehel & Perret '08]
  - Complexity of F5 algorithm: $\mathcal{O}\left(\binom{n+d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^{\omega}\right)$ [Faugère '02]

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

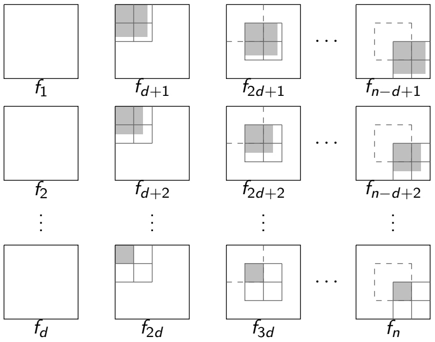
for bilinear system in X, Y blocks of variables of sizes n_X, n_Y.

Examples MinRank Cryptanalysis of MQQ [PKC '15]



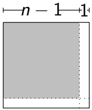
Hidden structure of secret $\mathcal{F}$

Examples MinRank Cryptanalysis of MQQ [PKC '15]



Hidden structure of secret $\mathcal{F}$

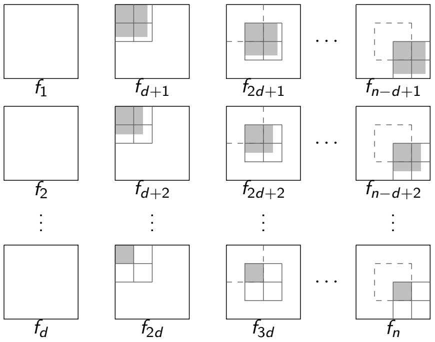
Recover structure



Find $(\lambda_1, \ldots, \lambda_m) \in (\mathbb{F}_q)^m$ s.t.

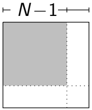
$$\text{rank}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{P}_i\right) < n.$$

Examples MinRank Cryptanalysis of MQQ [PKC '15]



Hidden structure of secret $\mathcal{F}$

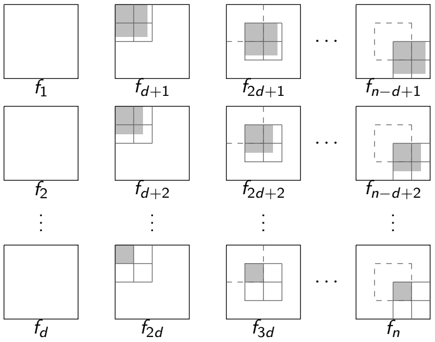
Recover structure



Find $(\lambda_1, \ldots, \lambda_{m'}) \in (\mathbb{F}_q)^{m'}$ s.t.

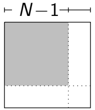
$$\operatorname{rank}\left(\sum_{i=1}^{m'} \lambda_i \mathfrak{P}'_i\right) < N.$$

Examples MinRank Cryptanalysis of MQQ [PKC '15]



Hidden structure of secret $\mathcal{F}$

Recover structure



Find $(\lambda_1, \ldots, \lambda_{m'}) \in (\mathbb{F}_q)^{m'}$ s.t.

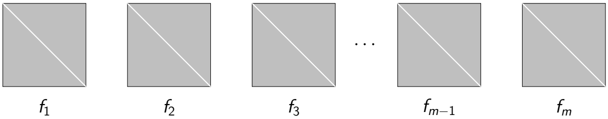
$$\text{rank}\left(\sum_{i=1}^{m'} \lambda_i \mathfrak{P}'_i\right) < N.$$

Complexity of MQQ Key recovery using MinRank with Gröbner bases:

$$\mathcal{O}(n^{10})$$

MinRank and Strong (s, t)–linearity

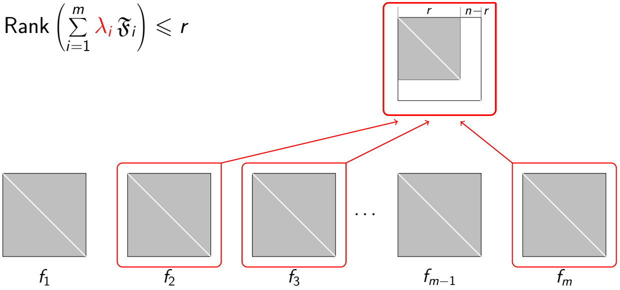
$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.



MinRank and Strong (s, t)–linearity

$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.

$\text{Rank}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right) \leqslant r$

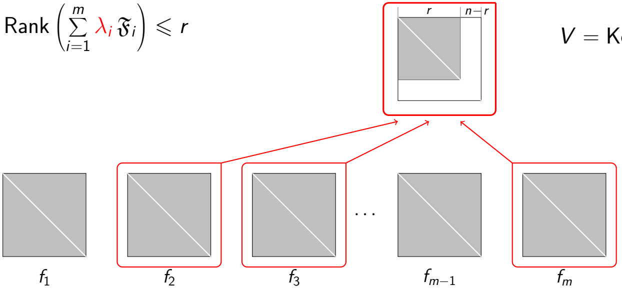


MinRank and Strong (s, t)–linearity

$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.

$\text{Rank}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right) \leqslant r$

$V = \text{Ker}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right)$



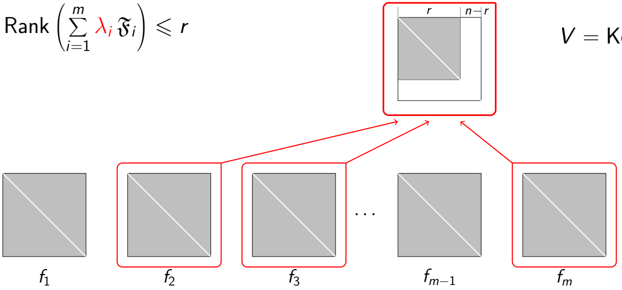
$W = \langle(\lambda_1, \ldots, \lambda_m)\rangle$

MinRank and Strong (s, t)–linearity

$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.

$\text{Rank}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right) \leqslant r$

$V = \text{Ker}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right)$



$W = \langle(\lambda_1, \ldots, \lambda_m)\rangle$

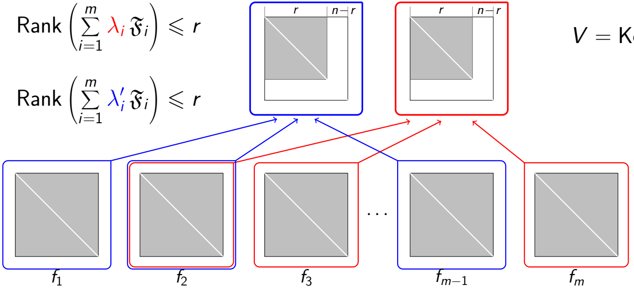
$MR(n, m, r, \mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m)$ has a solution **iff** $\mathcal{L}(f) \geqslant q^{n-\frac{r}{2}}$
iff f **is strongly** $(n - r, 1)$**–linear**.

MinRank and Strong (s, t)–linearity

$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.

$$\text{Rank}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right) \leqslant r$$

$$\text{Rank}\left(\sum_{i=1}^{m} \lambda'_i \mathfrak{F}_i\right) \leqslant r$$



$$V = \text{Ker}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right)$$

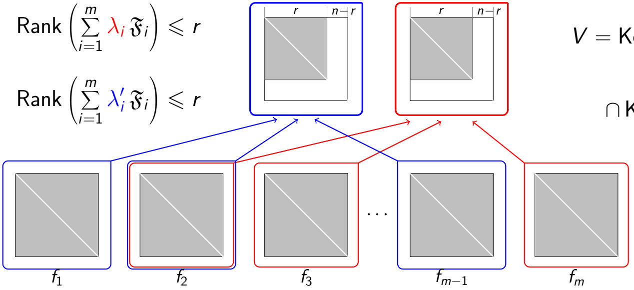
$$W = \langle(\lambda_1, \ldots, \lambda_m)\rangle$$

MinRank and Strong (s, t)–linearity

$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.

$$\text{Rank}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right) \leqslant r$$

$$\text{Rank}\left(\sum_{i=1}^{m} \lambda'_i \mathfrak{F}_i\right) \leqslant r$$



$$V = \text{Ker}\left(\sum_{i=1}^{m} \lambda_i \mathfrak{F}_i\right) \cap \text{Ker}\left(\sum_{i=1}^{m} \lambda'_i \mathfrak{F}_i\right)$$

$$W = \langle(\lambda_1, \ldots, \lambda_m), (\lambda_1, \ldots, \lambda_m)\rangle$$

Baby example

$$f_1(x_1,\ldots,x_6) = x_1x_3 + x_3x_5 + x_4x_5 + x_5 + x_4x_6 + x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\ldots,x_6) = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_5 + x_4x_6 + x_5x_6$$

$$\mathfrak{F}_1 = \begin{bmatrix} 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \end{bmatrix} \qquad \mathfrak{F}_2 = \begin{bmatrix} 0 & \mathbf{1} & \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 & 0 \end{bmatrix} \qquad \mathfrak{F}_3 = \begin{bmatrix} 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 \end{bmatrix}$$

Baby example

$$f_1(x_1,\ldots,x_6) = x_1x_3 + x_3x_5 + x_4x_5 + x_5 + x_4x_6 + x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\ldots,x_6) = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_5 + x_4x_6 + x_5x_6$$

$$\mathfrak{F}_1 = \begin{bmatrix} 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \end{bmatrix} \qquad \mathfrak{F}_2 = \begin{bmatrix} 0 & \mathbf{1} & \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 & 0 \end{bmatrix} \qquad \mathfrak{F}_3 = \begin{bmatrix} 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 \end{bmatrix}$$

$\mathrm{Rank}(\mathfrak{F}_3) = 4$

$\mathrm{Rank}(\mathfrak{F}_2 + \mathfrak{F}_3) = 4$

Baby example

$$f_1(x_1,\dots,x_6) = x_1x_3 + x_3x_5 + x_4x_5 + x_5 + x_4x_6 + x_6$$
$$f_2(x_1,\dots,x_6) = x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\dots,x_6) = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_5 + x_4x_6 + x_5x_6$$

$$\mathfrak{F}_1 = \begin{bmatrix} 0&0&\mathbf{1}&0&0&0\\ 0&0&0&0&0&0\\ \mathbf{1}&0&0&0&\mathbf{1}&0\\ 0&0&0&0&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&\mathbf{1}&0&0\\ 0&0&0&\mathbf{1}&0&0 \end{bmatrix} \qquad \mathfrak{F}_2 = \begin{bmatrix} 0&\mathbf{1}&\mathbf{1}&0&\mathbf{1}&\mathbf{1}\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ \mathbf{1}&0&0&\mathbf{1}&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ \mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{1}&0&0 \end{bmatrix} \qquad \mathfrak{F}_3 = \begin{bmatrix} 0&\mathbf{1}&0&\mathbf{1}&0&0\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ 0&\mathbf{1}&0&0&\mathbf{1}&0\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ 0&0&0&\mathbf{1}&\mathbf{1}&0 \end{bmatrix}$$

$$\mathrm{Rank}(\mathfrak{F}_3) = 4$$
$$\mathrm{Rank}(\mathfrak{F}_2 + \mathfrak{F}_3) = 4$$

$$\mathrm{Ker}(\mathfrak{F}_3) \cap \mathrm{Ker}(\mathfrak{F}_2 + \mathfrak{F}_3) = \langle (0,1,0,1,1,0), (1,1,1,1,1,1) \rangle$$

Baby example $\quad f$ is $(2,2)$-strongly linear

$$f_1(x_1,\ldots,x_6) = x_1x_3 + x_3x_5 + x_4x_5 + x_5 + x_4x_6 + x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\ldots,x_6) = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_5 + x_4x_6 + x_5x_6$$

$$\mathfrak{F}_1 = \begin{bmatrix} 0&0&\mathbf{1}&0&0&0\\ 0&0&0&0&0&0\\ \mathbf{1}&0&0&0&\mathbf{1}&0\\ 0&0&0&0&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&\mathbf{1}&0&0\\ 0&0&0&\mathbf{1}&0&0 \end{bmatrix} \qquad \mathfrak{F}_2 = \begin{bmatrix} 0&\mathbf{1}&\mathbf{1}&0&\mathbf{1}&\mathbf{1}\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ \mathbf{1}&0&0&\mathbf{1}&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ \mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{1}&0&0 \end{bmatrix} \qquad \mathfrak{F}_3 = \begin{bmatrix} 0&\mathbf{1}&0&\mathbf{1}&0&0\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ 0&\mathbf{1}&0&0&\mathbf{1}&0\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ 0&0&0&\mathbf{1}&\mathbf{1}&0 \end{bmatrix}$$

$$\text{Rank}(\mathfrak{F}_3) = 4$$
$$\text{Rank}(\mathfrak{F}_2 + \mathfrak{F}_3) = 4$$

$$\text{Ker}(\mathfrak{F}_3) \cap \text{Ker}(\mathfrak{F}_2 + \mathfrak{F}_3) = \langle (0,1,0,1,1,0), (1,1,1,1,1,1) \rangle$$

$\dim(W) = 2$ $\qquad$ $\dim(V) = 2$

Baby example $\quad f$ is $(2,2)$-strongly linear

$$f_1(x_1,\ldots,x_6) = x_1x_3 + x_3x_5 + x_4x_5 + x_5 + x_4x_6 + x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\ldots,x_6) = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_5 + x_4x_6 + x_5x_6$$

$$\mathfrak{F}_1 = \begin{bmatrix} 0&0&\mathbf{1}&0&0&0\\ 0&0&0&0&0&0\\ \mathbf{1}&0&0&0&\mathbf{1}&0\\ 0&0&0&0&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&\mathbf{1}&0&0\\ 0&0&0&\mathbf{1}&0&0 \end{bmatrix} \quad \mathfrak{F}_2 = \begin{bmatrix} 0&\mathbf{1}&\mathbf{1}&0&\mathbf{1}&\mathbf{1}\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ \mathbf{1}&0&0&\mathbf{1}&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ \mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{1}&0&0 \end{bmatrix} \quad \mathfrak{F}_3 = \begin{bmatrix} 0&\mathbf{1}&0&\mathbf{1}&0&0\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ 0&\mathbf{1}&0&0&\mathbf{1}&0\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ 0&0&0&\mathbf{1}&\mathbf{1}&0 \end{bmatrix}$$

$\text{Rank}(\mathfrak{F}_3) = 4$

$\text{Rank}(\mathfrak{F}_2 + \mathfrak{F}_3) = 4$

$$\text{Ker}(\mathfrak{F}_3) \cap \text{Ker}(\mathfrak{F}_2 + \mathfrak{F}_3) = \langle (0,1,0,1,1,0), (1,1,1,1,1,1) \rangle$$

$\dim(W) = 2$ $\qquad \dim(V) = 2$

Two MinRank problems with common kernel

Baby example $\quad f$ is $(2,2)$-strongly linear

$$f_1(x_1,\ldots,x_6) = x_1x_3 + x_3x_5 + x_4x_5 + x_5 + x_4x_6 + x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\ldots,x_6) = x_1x_2 + x_2x_3 + x_1x_4 + x_3x_5 + x_4x_6 + x_5x_6$$

$$\mathfrak{F}_1 = \begin{bmatrix} 0&0&\mathbf{1}&0&0&0\\ 0&0&0&0&0&0\\ \mathbf{1}&0&0&0&\mathbf{1}&0\\ 0&0&0&0&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&\mathbf{1}&0&0\\ 0&0&0&\mathbf{1}&0&0 \end{bmatrix} \qquad \mathfrak{F}_2 = \begin{bmatrix} 0&\mathbf{1}&\mathbf{1}&0&\mathbf{1}&\mathbf{1}\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ \mathbf{1}&0&0&\mathbf{1}&\mathbf{1}&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ \mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{1}&0&0 \end{bmatrix} \qquad \mathfrak{F}_3 = \begin{bmatrix} 0&\mathbf{1}&0&\mathbf{1}&0&0\\ \mathbf{1}&0&\mathbf{1}&0&0&0\\ 0&\mathbf{1}&0&0&\mathbf{1}&0\\ \mathbf{1}&0&0&0&0&\mathbf{1}\\ 0&0&\mathbf{1}&0&0&\mathbf{1}\\ 0&0&0&\mathbf{1}&\mathbf{1}&0 \end{bmatrix}$$

$\mathrm{Rank}(\mathfrak{F}_3) = 4$

$\mathrm{Rank}(\mathfrak{F}_2 + \mathfrak{F}_3) = 4$

$$\mathrm{Ker}(\mathfrak{F}_3) \cap \mathrm{Ker}(\mathfrak{F}_2 + \mathfrak{F}_3) = \langle (0,1,0,1,1,0), (1,1,1,1,1,1) \rangle$$

$\dim(W) = 2$ $\qquad$ $\dim(V) = 2$

After change of variables :

$$f_1(x_1,\ldots,x_6) = x_1x_4 + x_1x_6 + x_2x_3 + x_3x_4 + x_3x_5 + x_4x_5$$
$$f_2(x_1,\ldots,x_6) = x_1x_2 + x_1x_4 + x_2x_3$$
$$f_3(x_1,\ldots,x_6) = x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4$$

MinRank and Strong (s, t)–linearity

$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.

f is strongly (s, t)–linear

iff

$MR(n, m, n - s, \mathfrak{F}_1, \ldots, \mathfrak{F}_m)$
has t independent solutions $w_1, w_2, \ldots, w_t \in \mathbb{F}_q^m$ s.t.

$$\mathrm{Dim}\Big(\bigcap_i \mathrm{Ker}(\mathfrak{F}_{w_i})\Big) \geqslant s$$

MinRank and Strong (s,t)–linearity

$f = (f_1, f_2, \ldots, f_m)$ - quadratic (n, m) function,
$\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ - matrix representations of the coordinates of f.

f **is strongly** (s, t)**–linear**

iff

$MR(n, m, n - s, \mathfrak{F}_1, \ldots, \mathfrak{F}_m)$
has t independent solutions $w_1, w_2, \ldots, w_t \in \mathbb{F}_q^m$ s.t.

$$\mathrm{Dim}\left(\bigcap_i \mathrm{Ker}(\mathfrak{F}_{w_i})\right) \geqslant s$$

Simultaneous MinRank

Strong (s, t)–linearity v.s. $\mathcal{MQ}$ crypto

Simultaneous MinRank - Reveal strong (s, t) - linearity

Strong (s, t)–linearity v.s. $\mathcal{MQ}$ crypto

Simultaneous MinRank - Reveal strong (s, t) - linearity

Strongly (s, t)-linear
w.r.t. **unknown V, W**

Public $\mathcal{P}$

Strong (s, t)–linearity v.s. $\mathcal{MQ}$ crypto

Simultaneous MinRank - Reveal strong (s, t) - linearity

Strongly (s, t)-linear
w.r.t. **unknown V, W**

Goal: $\mathcal{P} \longrightarrow \mathcal{P}'$

Strongly (s, t)-linear
w.r.t. **standard basis**

Strong (s,t)–linearity v.s. $\mathcal{MQ}$ crypto

Simultaneous MinRank - Reveal strong (s,t) - linearity

Strongly (s,t)-linear
w.r.t. **unknown V, W**

Goal: $$\mathcal{P} = T' \circ \mathcal{P}' \circ S'$$

Strongly (s,t)-linear
w.r.t. **standard basis**

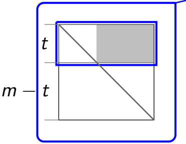
Strong (s, t)–linearity v.s. $\mathcal{MQ}$ crypto

Simultaneous MinRank - Reveal strong (s, t) - linearity

Strongly (s, t)-linear
w.r.t. **unknown V, W**

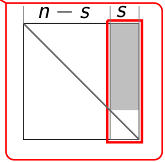
$$\mathcal{P} \; = \; T' \circ \mathcal{P}' \circ S'$$

Transform output space



Strongly (s, t)-linear
w.r.t. **standard basis**

Transform input space



Strong (s,t)–linearity v.s. $\mathcal{MQ}$ crypto

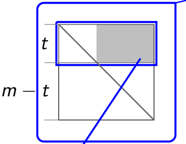
Simultaneous MinRank - Reveal strong (s,t) - linearity

Strongly (s,t)-linear
w.r.t. **unknown** V, W

$$\mathcal{P} \;=\; T' \circ \mathcal{P}' \circ S'$$

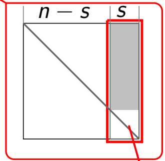
Transform output space

Transform input space



Strongly (s,t)-linear
w.r.t. **standard basis**

[Separate the spaces V, W]



basis of W

basis of V

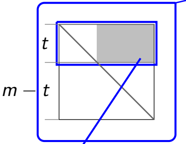
Strong (s, t)–linearity v.s. $\mathcal{MQ}$ crypto

Simultaneous MinRank - Reveal strong (s, t) - linearity

Strongly (s, t)-linear
w.r.t. **unknown** V**,** W

$$\mathcal{P} \;=\; T' \circ \mathcal{P}' \circ S'$$

Transform output space

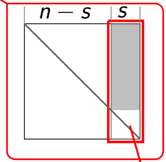


basis of W

Strongly (s, t)-linear
w.r.t. **standard basis**

[Separate the spaces V, W]

Transform input space



basis of V

(S', T') - **strong** (s, t) - **separation key**

Generic separation key attack for $\mathcal{MQ}$ cryptosystems

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) Recover the linear spaces determined by the key

All structure of Central map $\mathcal{F}'$ revealed

Generic separation key attack for $\mathcal{MQ}$ cryptosystems

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

Generic separation key attack for $\mathcal{MQ}$ cryptosystems

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

(2) $\Leftrightarrow$ solving **Simultaneous MinRank**:

$$\mathfrak{P}_{w^{(i)}} \cdot v^{(j)} = 0,\ i \in \{1, \ldots, t\},\ j \in \{1, \ldots, s\},$$

in the unknown: - basis vectors $w^{(i)}$ of the space W,
- basis vectors $v^{(j)}$ of the space V.

Generic separation key attack for $\mathcal{MQ}$ cryptosystems

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

Complexity:

$$\mathcal{O}\left(\binom{(n-s)s + (m-t)t + d_{reg}}{d_{reg}}^{\omega}\right)$$

$d_{reg} = \min\{(n-s)s, (m-t)t\} + 1$,
$2 \leqslant \omega \leqslant 3$ - linear algebra constant.

Generic separation key attack for $\mathcal{MQ}$ cryptosystems

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

Complexity:

$$\mathcal{O}\left(\binom{(n-s)s+(m-t)t+d_{reg}}{d_{reg}}^{\omega}\right)$$

$d_{reg} = \min\{(n-s)s, (m-t)t\} + 1$,
$2 \leqslant \omega \leqslant 3$ - linear algebra constant.

Not polynomial - time!

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

(2) $\Leftrightarrow$ solving:

$$\mathfrak{P}_{w^{(i)}} \cdot v^{(j)} = 0, \; i \in \{1, \ldots, t\}, \; j \in \{1, \ldots, s\},$$

in the unknown: - basis vectors $w^{(i)}$ of the space W,
- basis vectors $v^{(j)}$ of the space V.

Generic separation key attack for $\mathcal{MQ}$ cryptosystems

Improved Min-Max strategy

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

(2) $\Leftrightarrow$ solving: The quadratic:

$$\mathfrak{P}_{w^{(i)}} \cdot v^{(j)} = 0, \ i \in \{1, \ldots, c_1\}, \ j \in \{1, \ldots, c_2\}\},$$

in the unknown: - basis vectors $w^{(i)}$ of the space W,
- basis vectors $v^{(j)}$ of the space V.

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

(2) $\Leftrightarrow$ solving: And then the linear:

$$\mathfrak{P}_{w^{(i)}} \cdot v^{(j)} = 0, \; i \in \{c_1+1, ..., t\}, \; j \in \{1, ..., c_2\},$$

$$\mathfrak{P}_{w^{(i)}} \cdot v^{(j)} = 0, \; i \in \{1, ..., c_1\}, \; j \in \{c_2+1, ..., s\},$$

in the unknown: - basis vectors $w^{(i)}$ of the space W,

- basis vectors $v^{(j)}$ of the space V.

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

Complexity:

$$\mathcal{O}\left(\binom{(n-s)c_2 + (m-t)c_1 + d_{reg}}{d_{reg}}^{\omega}\right)$$

$d_{reg} = \min\{(n-s)c_2, (m-t)c_1\} + 1$,
$2 \leqslant \omega \leqslant 3$ - linear algebra constant.

Generic separation key attack for $\mathcal{MQ}$ cryptosystems

Improved Min-Max strategy

Repeat until

(1) Determine the existence of a strong (s, t) separation key

(2) **Recover the linear space determined by the key**

All structure of Central map $\mathcal{F}'$ revealed

Complexity:

$$\mathcal{O}\left(\binom{(n-s)c_2+(m-t)c_1+d_{reg}}{d_{reg}}^{\omega}\right)$$

$d_{reg} = \min\{(n-s)c_2, (m-t)c_1\} + 1$,
$2 \leqslant \omega \leqslant 3$ - linear algebra constant.

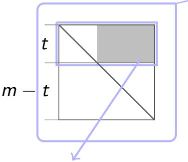
Polynomial - time!

An improved attack

Simultaneous MinRank - Reveal strong (s, t) - linearity

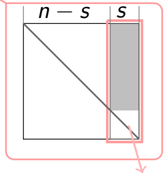
$$\mathcal{P} \;=\; T' \circ \mathcal{P}' \circ S'$$

Transform output space



basis of W

Transform input space



basis of V

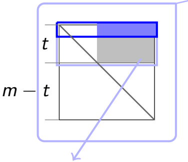
An improved attack

Simultaneous MinRank - Reveal strong (s, t) - linearity

$$\mathcal{P} = T' \circ \mathcal{P}' \circ S'$$

Transform output space

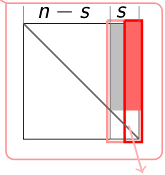
Transform input space



basis of W

Find only c_1 vectors from W

Find only c_2 vectors from V



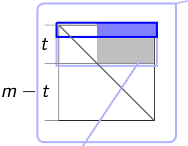
basis of V

An improved attack

Simultaneous MinRank - Reveal strong (s,t) - linearity

$$\mathcal{P} \;=\; T' \circ \mathcal{P}' \circ S'$$

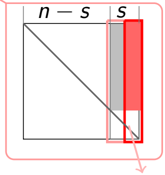
Transform output space



basis of W

Find only c_1 vectors from W
Find only c_2 vectors from V

Transform input space



basis of V

Choose c_1 and c_2 s.t.
the system has unique solution

First strong (c_2, c_1) - linearity
then strong (c_2, t) - linearity
then strong (s, t) - linearity

An improved attack

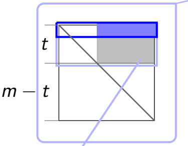
Simultaneous MinRank - Reveal strong (s,t) - linearity

Type of **good key** [Thomae-Wolf '12]
with "good enough" structure

$$\mathcal{P} \;=\; T' \circ \mathcal{P}' \circ S'$$

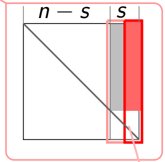
Transform output space

Transform input space



basis of W

← Find only c_1 vectors from W
Find only c_2 vectors from V →



basis of V

Choose c_1 and c_2 s.t.
the system has unique solution

First strong (c_2, c_1) - linearity
then strong (c_2, t) - linearity
then strong (s, t) - linearity

Recall: (s,t)–linearity of quadratic (n,m) function f

Boura and Canteaut FSE13:

f is said to be (s,t)**–linear** if there exist linear subspaces $V \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V) = s$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(W) = t$, s.t.

$$\forall\, w \in W,\;\; w^{\intercal} \cdot f \text{ is linear on all cosets of } V.$$

- f_W corresponding to all $w^{\intercal} \cdot f$, $w \in W$ can be written as

$$f_W(x,y) = M(x) \cdot y + G(x)$$

where $\mathbb{F}_q^n = U \oplus V$, $G : U \to \mathbb{F}_q^t$ and $M(x)$ is a $t \times s$ matrix with rows - components of linear functions over U.

Baby example UOV

$$f_1(x_1,\dots,x_6) = x_1x_2 + x_2x_4 + x_3x_6 + x_4x_6 + x_5x_6 + x_6$$
$$f_2(x_1,\dots,x_6) = x_1x_4 + x_3x_4 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\dots,x_6) = x_2x_3 + x_3x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_1x_6 + x_4x_6 + x_5x_6$$

Baby example UOV

$$f_1(x_1, \ldots, x_6) = x_1x_2 + x_2x_4 + x_3x_6 + x_4x_6 + x_5x_6 + x_6$$
$$f_2(x_1, \ldots, x_6) = x_1x_4 + x_3x_4 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1, \ldots, x_6) = x_2x_3 + x_3x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_1x_6 + x_4x_6 + x_5x_6$$

$\overline{S}'$: $x_4 \to x_4 + x_6$
$x_2 \to x_2 + x_5$

Baby example UOV

$$f_1(x_1,\ldots,x_6) = x_1x_2 + x_2x_4 + x_3x_6 + x_4x_6 + x_5x_6 + x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_4 + x_3x_4 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\ldots,x_6) = x_2x_3 + x_3x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_1x_6 + x_4x_6 + x_5x_6$$

$$\overline{S}': \begin{array}{l} x_4 \to x_4 + x_6 \\ x_2 \to x_2 + x_5 \end{array}$$

After change of variables :

$$f_1(x_1,\ldots,x_6) = x_1x_2 + x_1x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_3x_6 + x_4x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_4 + x_1x_6 + x_3x_4 + x_4x_6$$
$$f_3(x_1,\ldots,x_6) = x_2x_3 + x_2x_4 + x_4x_6 + x_1x_6 + x_6$$

Baby example UOV

$$f_1(x_1,\ldots,x_6) = x_1x_2 + x_2x_4 + x_3x_6 + x_4x_6 + x_5x_6 + x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_4 + x_3x_4 + x_3x_6 + x_4x_6 + x_6$$
$$f_3(x_1,\ldots,x_6) = x_2x_3 + x_3x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_1x_6 + x_4x_6 + x_5x_6$$

$\overline{S}'$: $x_4 \to x_4 + x_6$ $\Leftrightarrow$ Linear on every coset of
$x_2 \to x_2 + x_5$ $\quad Span(\{(0,0,0,1,0,1),(0,1,0,0,1,0)\})$

After change of variables :

$$f_1(x_1,\ldots,x_6) = x_1x_2 + x_1x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_3x_6 + x_4x_6$$
$$f_2(x_1,\ldots,x_6) = x_1x_4 + x_1x_6 + x_3x_4 + x_4x_6$$
$$f_3(x_1,\ldots,x_6) = x_2x_3 + x_2x_4 + x_4x_6 + x_1x_6 + x_6$$

(s,t)–linearity v.s. $\mathcal{MQ}$ crypto

(s,t)-linear
w.r.t. **unknown** V**,** W

Public $\mathcal{P}$

(s, t)–linearity v.s. $\mathcal{MQ}$ crypto

(s, t)-linear
w.r.t. **unknown** V**,** W

Goal: $\mathcal{P} = T' \circ \mathcal{P}' \circ S'$

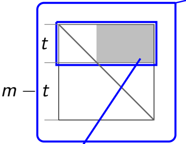
(s, t)-linear
w.r.t. **standard basis**

(s, t)–linearity v.s. $\mathcal{MQ}$ crypto

(s, t)-linear
w.r.t. **unknown** V**,** W

$$\mathcal{P} = T' \circ \mathcal{P}' \circ S'$$

Transform output space

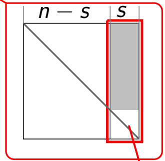


basis of W

(s, t)-linear
w.r.t. **standard basis**

[Separate the spaces V, W]

Transform input space



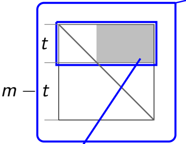
basis of V

(s,t)–linearity v.s. $\mathcal{MQ}$ crypto

(s,t)-linear
w.r.t. **unknown** V**,** W

$$\mathcal{P} = T' \circ \mathcal{P}' \circ S'$$

Transform output space

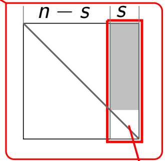


basis of W

(s,t)-linear
w.r.t. **standard basis**

[Separate the spaces V, W]

Transform input space



basis of V

(S', T') - (s,t) - **separation key**

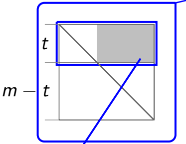
(s,t)–linearity v.s. $\mathcal{MQ}$ crypto

A realistic scenario - $(n, \mathbf{m})$ function is $(s, \mathbf{m})$ - linear

(s,t)-linear
w.r.t. **unknown** V, W

$$\mathcal{P} = T' \circ \mathcal{P}' \circ S'$$

Transform output space

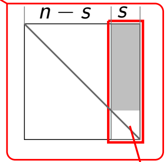


basis of W

(s,t)-linear
w.r.t. **standard basis**

[Separate the spaces V, W]

Transform input space



basis of V

(S', T') - (s,t) - separation key

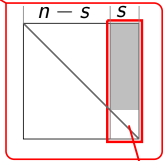
(s,t)–linearity v.s. $\mathcal{MQ}$ crypto

(s, m)-linear
w.r.t. **unknown** V

$$\mathcal{P} = \quad \mathcal{P}' \circ S'$$

(s, m)-linear
w.r.t. **standard basis**

Transform input space



basis of V

(s, t)–linearity v.s. $\mathcal{MQ}$ crypto

(s, m)-linear
w.r.t. **unknown** V

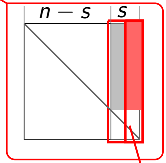
$$\mathcal{P} = \quad \mathcal{P}' \circ S'$$

(s, m)-linear
w.r.t. **standard basis**

Find only c vectors from V

First reveal (c, m) - linearity
then (s, m) - linearity

Transform input space



basis of V

(s, t)–linearity v.s. $\mathcal{MQ}$ crypto

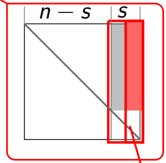
Type of **good key**

(s, m)-linear
w.r.t. **unknown** V

$$\mathcal{P} = \quad \mathcal{P}' \circ S'$$

(s, m)-linear
w.r.t. **standard basis**

Transform input space



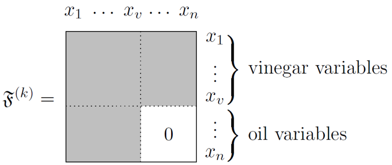
basis of V

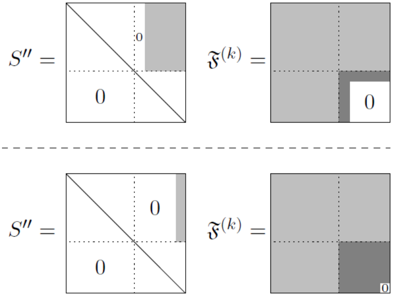
Find only c vectors from V

First reveal (c, m) - linearity
then (s, m) - linearity

UOV

$$f_s(x) = \sum_{i \in V, j \in V} \gamma_{ij}^{(s)} x_i x_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(s)} x_i x_j,$$

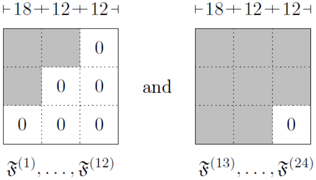


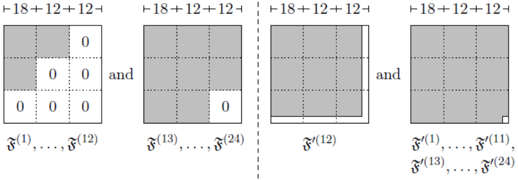


Good Keys for UOV

Combining strong (s,t)–linearity and (s,t)–linearity

Rainbow





We can choose $c_1 = c_2 = c = 1$

A challenge:

Post-Quantum Cryptography
from hard problems in Quasigroup theory

Canonical Identification Schemes

$\mathcal{P}, \mathsf{sk}$		$\mathcal{V}, \mathsf{pk}$
$\mathsf{com} \leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \mathsf{ChS}(1^k)$
$\mathsf{resp} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{resp}}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$

Informally:

1. Prover commits to some (randomized) value derived from sk
2. Verifier picks a challenge ‘ch’
3. Prover computes response ‘resp’
4. Verifier checks if response matches challenge

Properties of Canonical 3-pass IDS

$\mathcal{P}$, sk		$\mathcal{V}$, pk
com $\leftarrow_R \mathcal{P}_0$(sk)	com $\longrightarrow$	
	ch $\longleftarrow$	ch $\leftarrow_R$ ChS(1^k)
resp $\leftarrow \mathcal{P}_1$(sk, com, ch)	resp $\longrightarrow$	
		$b \leftarrow$ Vf(pk, com, ch, resp)

Soundness (with soundness error κ)

Probability that a PPT adversary $\mathcal{A}$ gets verified is $\kappa + \mathrm{negl}(k)$

- r rounds until $\kappa^r = negl(k)$
- guaranties negligible success of cheating Prover

Properties of Canonical 3-pass IDS

$\mathcal{P}, \mathsf{sk}$		$\mathcal{V}, \mathsf{pk}$
$\mathsf{com} \leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \mathsf{ChS}(1^k)$
$\mathsf{resp} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{resp}}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$

Special Soundness

There exists PPT algorithm $\mathcal{K}$ - knowledge extractor s.t. given two accepting transcripts:

$$\mathsf{trans} = (\mathsf{com}, \mathsf{ch}, \mathsf{resp}),\ \mathsf{trans}' = (\mathsf{com}, \mathsf{ch}', \mathsf{resp}'), \qquad \mathsf{ch} \neq ch',$$

extracts the secret sk with non-negligible probability

- random challenges can be answered only if Prover knows a witness
- implies soundness and knowledge

Properties of Canonical 3-pass IDS

$\mathcal{P}$, sk		$\mathcal{V}$, pk
com $\leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\text{com}}$	
	$\xleftarrow{\text{ch}}$	ch $\leftarrow_R \mathsf{ChS}(1^k)$
resp $\leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\text{resp}}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$

(statistical) Honest-Verifier Zero-Knowledge

There exists a PPT algorithm $\mathcal{S}$, called the simulator, such that the statistical distance between the real transcript and the simulated transcript is negligible in k.

- guaranties no leakage of secret

The Fiat-Shamir transform

IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0\ (\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \mathsf{ChS}\ (1^k)$
$\mathsf{resp} \leftarrow \mathcal{P}_1\ (\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{resp}}$	
		$b \leftarrow \mathsf{Vf}\ (\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$

↓ ↓ ↓

FS signature

Signer
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$
$\mathsf{ch} \leftarrow H(m, \mathsf{com})$
$\mathsf{resp} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$
output : $\sigma = (\mathsf{com}, \mathsf{resp})$

Verifier
$\mathsf{ch} \leftarrow H(m, \mathsf{com})$
$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$
output : b

The Fiat-Shamir transform

IDS

$\mathcal{P}^r$		$\mathcal{V}^r$
$\text{com} \leftarrow \mathcal{P}_0{}^r(\text{sk})$	$\xrightarrow{\text{com}}$	
	$\xleftarrow{\text{ch}}$	$\text{ch} \leftarrow_R \text{ChS}^r(1^k)$
$\text{resp} \leftarrow \mathcal{P}_1{}^r(\text{sk}, \text{com}, \text{ch})$	$\xrightarrow{\text{resp}}$	
		$b \leftarrow \text{Vf}^r(\text{pk}, \text{com}, \text{ch}, \text{resp})$

$\downarrow \downarrow \downarrow$

FS signature

Signer

$\text{com} \leftarrow \mathcal{P}_0(\text{sk})$

$\text{ch} \leftarrow H(m, \text{com})$

$\text{resp} \leftarrow \mathcal{P}_1(\text{sk}, \text{com}, \text{ch})$

output : $\sigma = (\text{com}, \text{resp})$

Verifier

$\text{ch} \leftarrow H(m, \text{com})$

$b \leftarrow \text{Vf}(\text{pk}, \text{com}, \text{ch}, \text{resp})$

output : b

The Fiat-Shamir transform

IDS

$\mathcal{P}^r$		$\mathcal{V}^r$
$\text{com} \leftarrow {\mathcal{P}_0}^r(\text{sk})$	$\xrightarrow{\text{com}}$	
$\text{ch} \leftarrow_R \text{ChS}^r(1^k)$	$\xleftarrow{\text{ch}}$	
$\text{resp} \leftarrow {\mathcal{P}_1}^r(\text{sk}, \text{com}, \text{ch})$	$\xrightarrow{\text{resp}}$	
		$b \leftarrow \text{Vf}^r(\text{pk}, \text{com}, \text{ch}, \text{resp})$

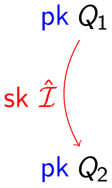
$\downarrow \quad \downarrow \quad \downarrow$

FS signature

Signer
$\text{com} \leftarrow \mathcal{P}_0(\text{sk})$
$\text{ch} \leftarrow H(m, \text{com})$
$\text{resp} \leftarrow \mathcal{P}_1(\text{sk}, \text{com}, \text{ch})$
output : $\sigma = (\text{com}, \text{resp})$

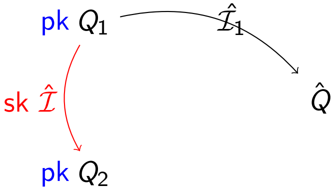
Verifier
$\text{ch} \leftarrow H(m, \text{com})$
$b \leftarrow \text{Vf}(\text{pk}, \text{com}, \text{ch}, \text{resp})$
output : b

Provably secure IDS and signatures from quasigroups? Certainly!



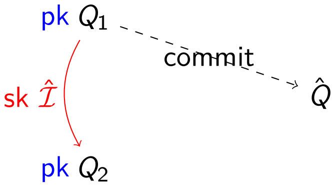
$\mathcal{P}$, sk		$\mathcal{V}$, pk
$\hat{\mathcal{I}}_1 \leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\hat{\mathcal{I}}_1 \text{ (com)}}$	
	$\xleftarrow{\text{ch}}$	$\mathsf{ch} \leftarrow_R \{0,1\}$
$\hat{\mathcal{I}_{\mathsf{ch}}} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\hat{\mathcal{I}_{\mathsf{ch}}} \text{ (resp)}}$	
		$b \leftarrow \hat{\mathcal{I}_{\mathsf{ch}}}(Q_{\mathsf{ch}}) \stackrel{?}{=} \hat{Q}$

Provably secure IDS and signatures from quasigroups? Certainly!



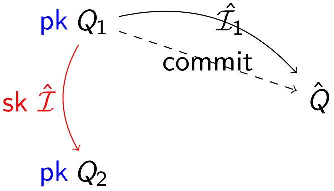
$\mathcal{P}$, sk		$\mathcal{V}$, pk
$\hat{\mathcal{I}}_1 \leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\hat{\mathcal{I}}_1\ (\mathsf{com})}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \{0,1\}$
$\hat{\mathcal{I}_{\mathsf{ch}}} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\hat{\mathcal{I}_{\mathsf{ch}}}\ (\mathsf{resp})}$	
		$b \leftarrow \hat{\mathcal{I}_{\mathsf{ch}}}(Q_{\mathsf{ch}}) \stackrel{?}{=} \hat{Q}$

Provably secure IDS and signatures from quasigroups? Certainly!



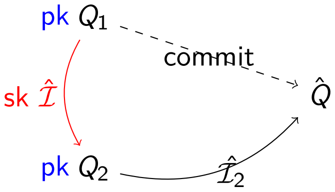
$\mathcal{P}$, sk		$\mathcal{V}$, pk
$\hat{\mathcal{I}}_1 \leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\hat{\mathcal{I}}_1\ (\mathsf{com})}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \{0,1\}$
$\hat{\mathcal{I}_{\mathsf{ch}}} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\hat{\mathcal{I}_{\mathsf{ch}}}\ (\mathsf{resp})}$	
		$b \leftarrow \hat{\mathcal{I}_{\mathsf{ch}}}(Q_{\mathsf{ch}}) \stackrel{?}{=} \hat{Q}$

Provably secure IDS and signatures from quasigroups? Certainly!



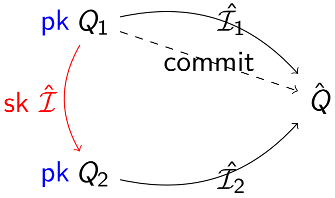
$\mathcal{P}, \mathsf{sk}$		$\mathcal{V}, \mathsf{pk}$
$\hat{\mathcal{I}}_1 \leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\hat{\mathcal{I}}_1 \text{ (com)}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \{0, 1\}$
$\hat{\mathcal{I}_{\mathsf{ch}}} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\hat{\mathcal{I}_{\mathsf{ch}}} \text{ (resp)}}$	
		$b \leftarrow \hat{\mathcal{I}_{\mathsf{ch}}}(Q_{\mathsf{ch}}) \stackrel{?}{=} \hat{Q}$

Provably secure IDS and signatures from quasigroups? Certainly!



$\mathcal{P}, \mathsf{sk}$		$\mathcal{V}, \mathsf{pk}$
$\hat{\mathcal{I}}_1 \leftarrow_R \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\hat{\mathcal{I}}_1 \text{ (com)}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \{0, 1\}$
$\hat{\mathcal{I}_{\mathsf{ch}}} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\hat{\mathcal{I}_{\mathsf{ch}}} \text{ (resp)}}$	
		$b \leftarrow \hat{\mathcal{I}_{\mathsf{ch}}}(Q_{\mathsf{ch}}) \stackrel{?}{=} \hat{Q}$

Provably secure IDS and signatures from quasigroups? Certainly!



- Big communication cost
- Do we actually need quasigroups?
  - Works perfectly well for random isomorphic quadratic polynomials
  - no use of quasigroup structure

$\mathcal{P}$, sk — $\mathcal{V}$, pk

$\hat{\mathcal{I}}_1 \leftarrow_R \mathcal{P}_0(\mathsf{sk})$

$\xrightarrow{\hat{\mathcal{I}}_1 \text{ (com)}}$

$\xleftarrow{\mathsf{ch}}$ $\quad \mathsf{ch} \leftarrow_R \{0, 1\}$

$\hat{\mathcal{I}}_{\mathsf{ch}} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$

$\xrightarrow{\hat{\mathcal{I}}_{\mathsf{ch}} \text{ (resp)}}$

$b \leftarrow \hat{\mathcal{I}}_{\mathsf{ch}}(Q_{\mathsf{ch}}) \stackrel{?}{=} \hat{Q}$

Provably secure IDS and signatures from quasigroups?

- Can we use the problem of completing partial Latin squares?

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

$\longrightarrow$

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

- Hard problem even when only 3 integers remain unfilled
- Prover shows the knowledge of a “completion”
- Open problem: How to do it in Zero Knowledge manner
- Open problem: Evaluation of the practical security of the problem

Provably secure IDS and signatures from quasigroups?

- Can we use the problem of completing partial Latin squares?

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

$\longrightarrow$

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

- Hard problem even when only 3 integers remain unfilled
- Prover shows the knowledge of a "completion"
- Open problem: How to do it in Zero Knowledge manner
- Open problem: Evaluation of the practical security of the problem

Provably secure IDS and signatures from quasigroups?

- Can we use the problem of completing partial Latin squares?

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

$\longrightarrow$

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

- Hard problem even when only 3 integers remain unfilled
- Prover shows the knowledge of a “completion”
- Open problem: How to do it in Zero Knowledge manner
- Open problem: Evaluation of the practical security of the problem

Provably secure IDS and signatures from quasigroups?

- Can we use the problem of completing partial Latin squares?

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

$\longrightarrow$

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

- Hard problem even when only 3 integers remain unfilled
- Prover shows the knowledge of a “completion”
- Open problem: How to do it in Zero Knowledge manner
- Open problem: Evaluation of the practical security of the problem

Thank you for listening!