NTNU
Norwegian University of
Science and Technology

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

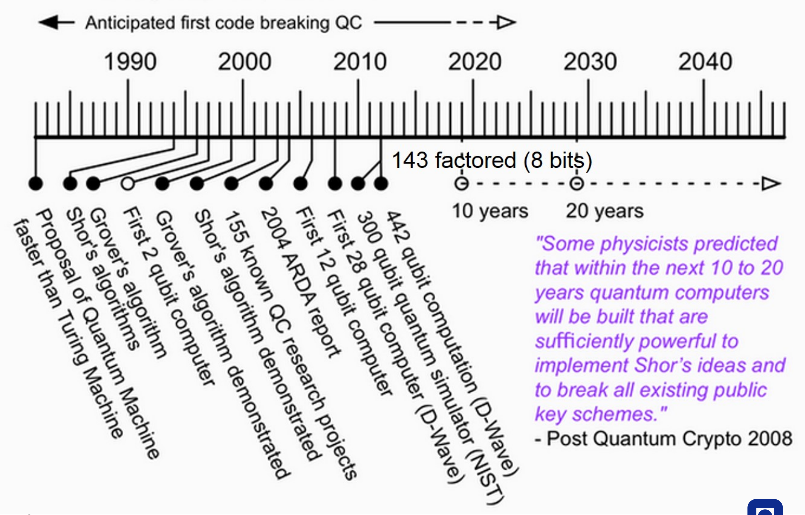
Linearity Measures for $\mathcal{MQ}$ Cryptography

Simona Samardjiska

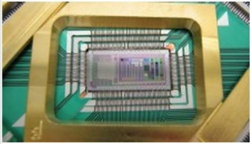
Department of Telematics, NTNU, Norway
FCSE, UKIM, Macedonia
simonas@item.ntnu.no, simona.samardjiska@finki.ukim.mk

COINS, October 13–15, 2014, Tromsø

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



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



The NSA is building a quantum computer to crack almost every kind of encryption

January 3, 2014 at 10:03 am

New documents leaked by Edward Snowden reveal two NSA programs that seek to build a "useful quantum computer" that can break all known forms of classical encryption. Such a quantum computer would obviously give the NSA unprecedented access to encrypted communications, but a working quantum computer is also vital for defensive purposes: If someone else gets their hands on a quantum computer first, then it is the US government that will suddenly have all of its encrypted communications cracked wide open.

Tweet 67 Like 131

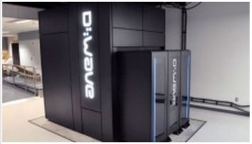
Scientists make largest ever quantum circuit board

December 4, 2013 at 8:01 am

Scientists have smashed the old record for simultaneous entangled systems in a quantum circuit board. The new laser-based system has over 10,000 quantum systems active at a given time.

Tweet 66 Like 82

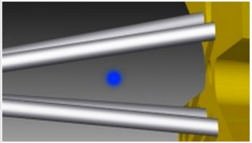
Post–Quantum Crypto *...Where have you been all this while?*



D-Wave, disentangled: Google explains the present and future of quantum computing February 26, 2014 at 12:00 pm

The D-Wave computer has produced some of the most interesting and occasionally perplexing results of any computer experiment to date. Google gives us a status update on where the project is, and where it plans to go.

Tweet 75 Like 94

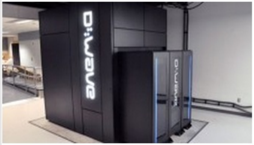


This single-atom engine breaks the laws of physics, could drive progress in quantum computing February 5, 2014 at 10:01 am

An incredible new engine is powered by just a single calcium atom, and by being so small it can run more efficiently than scientists had previously believed possible.

Tweet 100 Like 315

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



D-Wave confirmed as the first real quantum computer by new research June 12, 2014 at 10:30 am

New research suggests that D-Wave's quantum computer really is performing quantum computing — and that future generations will show the performance gains that theoretical models predict.

Tweet 116 Like 802

Google's Quantum Computing Playground turns your PC into a quantum computer May 22, 2014 at 10:47 am

Thanks to some ingenious engineers at Google, you can now turn your desktop PC into a quantum computer. Well, OK, not quite: You can simulate a quantum computer on your PC by running the Quantum Computing Playground web app for Chrome. The Playground allows you to run famous quantum algorithms, such as Grover's, or even to write your own quantum script. Short of buying your own quantum computer — which, despite what D-Wave says, you can't — this is the next best thing.

Tweet 104 Like 1.2k

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

- Current PKC algorithms are doomed once a big enough quantum computer arrives (10-15 years?)
- Research in algorithms secure in the quantum world
  - **Code-based systems**
  - **Lattice-based systems**
  - **Hash-based systems**
  - **Multivariate Quadratic systems**
- Gaining confidence for a standard (5-7 years?)
- Adopting a standard (10-12 years?)

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


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

Information Technology Laboratory

About ITL ▼ | Publications | Topic/Subject Areas ▼ | Products/Services ▼ | News/Multimedi

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

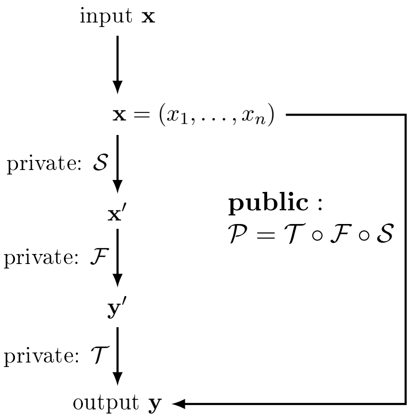
Workshop on Cybersecurity in a Post-Quantum World

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***,

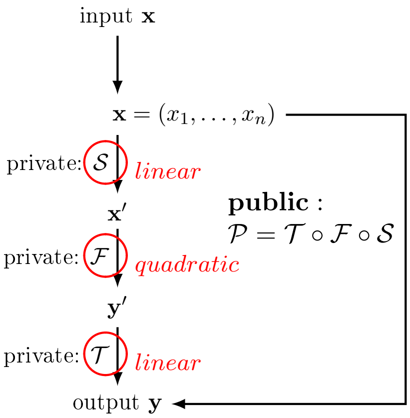
Multivariate ($\mathcal{MQ}$) Crypto

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

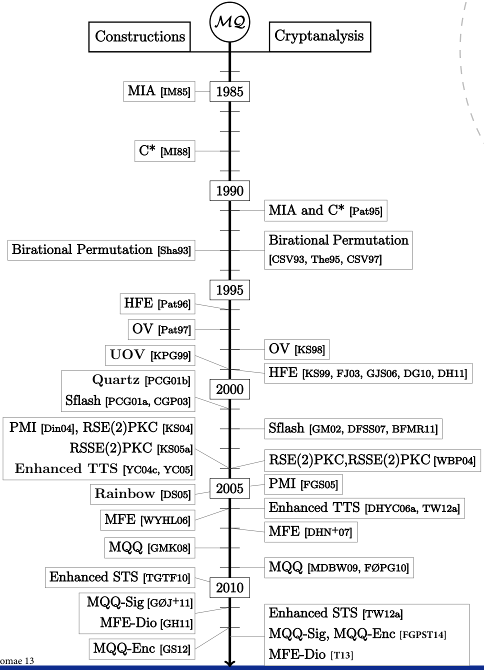


Multivariate ($\mathcal{MQ}$) Crypto

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



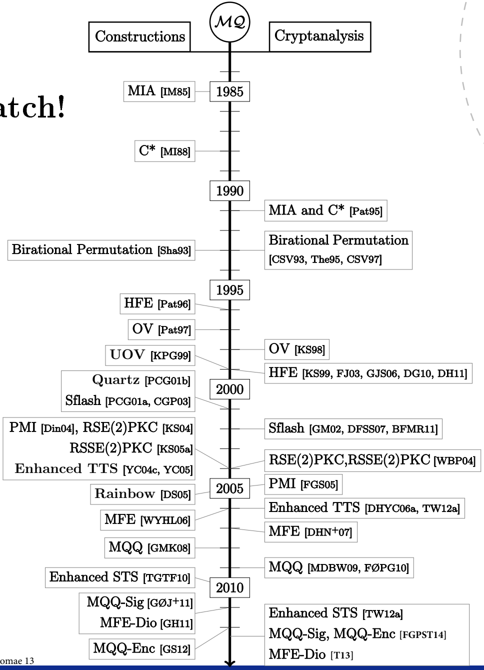
$\mathcal{MQ}$ History



Thomae 13

$\mathcal{MQ}$ History

Break and Patch!



Thomae 13

Attacks on $\mathcal{MQ}$ schemes

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

Attacks on $\mathcal{MQ}$ schemes

Linear subspaces!

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

Linearity measures for (n, m)-functions

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

$$D_w f(x) = f(x + w) - f(x) = f(w) - f(0)$$

for all $x \in \mathbb{F}_q^n$.

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

Linearity measures for (n, m)-functions

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

$$D_w f(x) = f(x+w) - f(x) = f(w) - f(0)$$

for all $x \in \mathbb{F}_q^n$.

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.**

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

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

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, $m = n$.

Linearity measures for (n, m)-functions

[Nyberg92] **Quadratic form f:**

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

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

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

Maximum nonlinearity:

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

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.**

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

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

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, $m = n$.

MinRank Attack

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

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

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

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

MinRank Attack

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

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

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

$$\textbf{MinRank} \quad \Leftrightarrow \quad \mathcal{L}(f) \geqslant q^{n-\frac{r}{2}}$$

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

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

$f:$

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

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

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

f is linear on the oil subspace!

(s,t)–linearity & Strong (s,t)–linearity

Boura and Canteaut FSE13:

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

$$\text{for all } w \in W,\ deg(w^\intercal \cdot f) \leqslant 1$$

on all cosets of 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,
$V = \langle(0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\rangle$, $W = \langle(1, 0, 0), (0, 1, 0)\rangle$

(s,t)–linearity & Strong (s,t)–linearity

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

for all $w \in W$,

V is a subspace of the linear space of $w^\intercal \cdot f$.

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

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.

The **MinRank problem** $MR(n, r, m, \mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m)$ has a solution
iff
f **is strongly** $(n-r, 1)$–**linear**.

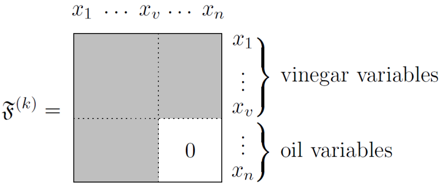
Equivalent Keys/Good Keys

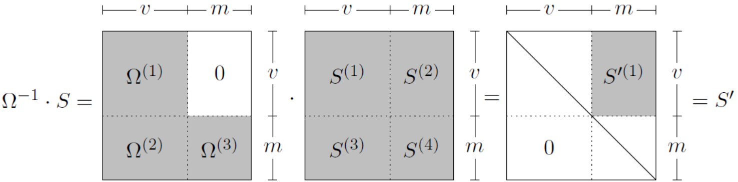
$$
\begin{aligned}
\mathcal{P} &= \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} \Leftrightarrow \\
\mathcal{P} &= \underbrace{\mathcal{T} \circ \Sigma^{-1}} \circ \underbrace{\Sigma \circ \mathcal{F} \circ \Omega} \circ \underbrace{\Omega^{-1} \circ \mathcal{S}} \Leftrightarrow \\
\mathcal{P} &= \quad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

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

Equivalent Keys/Good Keys

UOV

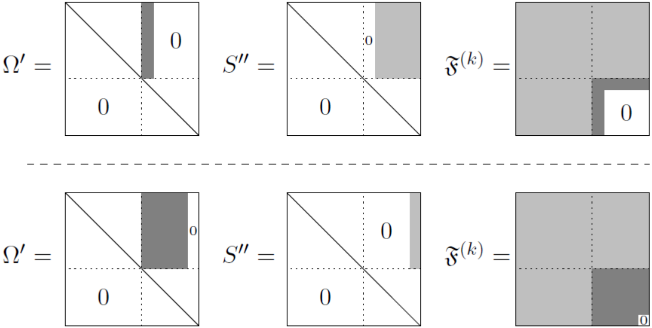




Equivalent Key for UOV

Equivalent Keys/Good Keys

UOV



Good Keys for UOV

Good Keys and (Strong) (s, t)–linearity

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

strong (s, t) separation key for $\mathcal{P}$
exploits strong (s, t)–linearity

(s, t) separation key for $\mathcal{P}$
exploits (s, t)–linearity

Good Keys and (Strong) (s,t)–linearity

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

strong (s,t) separation key for $\mathcal{P}$
exploits strong (s,t)–linearity

(s,t) separation key for $\mathcal{P}$
exploits (s,t)–linearity

Strong (s,t)–separation keys for some $\mathcal{MQ}$ cryptosystems

scheme	parameters	strong (s,t) separation keys
Branch.C^*	$(n_1,\dots,n_b)$	$(\sum_i n_i, n-\sum_i n_i)$
STS	$(r_1,\dots,r_L)$	$(n-r_k, r_k),\ k=1,\dots,L-1$
Rainbow	$(v_1,o_1,o_2)=(18,12,12)$	$(12,12)$
MQQ-SIG	$(q,d,n,r)=(2,8,160,80)$	$(k,80-k),\ k=1,\dots,79$
MFE	$(q^k,n,m)=((2^{256})^k,12,15)$	$(2k,10k),\ (4k,4k),(6k,2k),\ (8k,k)$
EnTTS	$(n,m)=(32,24)$	$(10,14),(14,10)$

(s,t)–separation keys for some $\mathcal{MQ}$ cryptosystems

scheme	parameters	(s,t) separation keys
UOV	(q,v,o)	(o,o)
Rainbow	$(q,v,o_1,o_2)=(2^8,18,12,12)$	$(12,24)$, $(24,12)$
MQQ-SIG	$(q,d,n,r)=(2,8,160,80)$	$(8+8i,80-8i), i\in\{0,...,9\}$
MFE	$(q^k,n,m)=((2^{256})^k,12,15)$	$(2k,2k)$,$(3k,2k)$,$(4k,4k)$
ℓIC	$(q^k,\ell)=(2^k,3)$	$(2k,2k)$,$(k,2k)$
EnTTS	$(n,m)=(32,24)$	$(10,24)$,$(14,14)$,$(24,10)$

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

Min-Max strategy

1. Look for the minimal (maximal) s and maximal (minimal) t s.t. there exists a strong (s, t) separation key
   - HighRank attack
   - MinRank attack
2. Recover the linear space determined by the key
3. Repeat the procedure for the remaining part of the polynomials

Thank you for listening!