NTNU
Norwegian University of
Science and Technology

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

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

Simona Samardjiska

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

Outline

- **Equivalent Keys/Good keys in $\mathcal{MQ}$ cryptography**
- Recent Contributions
  - **Linearity in $\mathcal{MQ}$ cryptography**
  - **Linear attacks**
    - measures for resistance to linear attacks
    - two generic attacks for separation of linear spaces
    - polynomial system modeling

Outline

- **Equivalent Keys/Good keys in $\mathcal{MQ}$ cryptography**
- **Recent Contributions**
  - **Linearity in $\mathcal{MQ}$ cryptography**
  - **Linear attacks**
    - measures for resistance to linear attacks
    - two generic attacks for separation of linear spaces
    - polynomial system modeling


Outline

- **Equivalent Keys/Good keys in $\mathcal{MQ}$ cryptography**
- **Recent Contributions**
  - **Linearity in $\mathcal{MQ}$ cryptography**
  - **Linear attacks**
    - measures for resistance to linear attacks
    - two generic attacks for separation of linear spaces
    - polynomial system modeling

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

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

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

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

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

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

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

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

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

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

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

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

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.**

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

Quadratic (n, m)-function

- 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, $m = n$.

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.**

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

Quadratic (n, m)-function

- 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, $m = n$.

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.**

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

Quadratic (n, m)-function

- 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, $m = n$.

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

Example 1:

f :

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

f' :

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

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

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

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

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

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.

(s,t)–linearity

Boura and Canteaut FSE13:

f - quadratic (n,m) function,
$V \subset \mathbb{F}_q^n$, $\mathrm{Dim}(V) = s$, and $W \subset \mathbb{F}_q^m$, $\mathrm{Dim}(W) = t$ - linear spaces.

f is (s,t)–linear with respect to V, W

- **iff** 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 whose rows are the components of linear functions over U.

- **iff** for $w \in W$

$$D_{a,b}(w^\intercal \cdot f), \text{ for every } a, b \in V \text{ vanishes.}$$


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

(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 $w^\intercal \cdot f$.

Strong (s,t)–linearity

f - quadratic (n,m) function,
$V \subset \mathbb{F}_q^n$, $\mathrm{Dim}(V) = s$, and $W \subset \mathbb{F}_q^m$, $\mathrm{Dim}(W) = t$ - linear spaces.

f is strongly (s,t)–linear with respect to V, W

- **iff** 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.

- **iff** for $w \in W$

$$D_a(w^\intercal \cdot f), \text{ for every } a \in V \text{ is constant.}$$


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

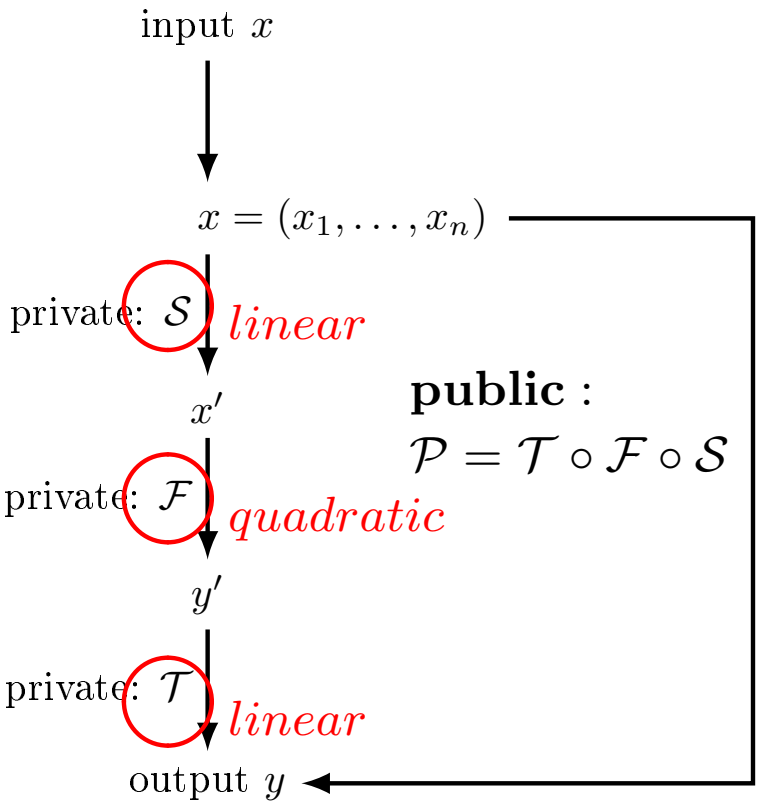

Simple but important properties

- Strong (s,t)–linearity
  $\Rightarrow$ Strong $(s-1,t)$ and $(s,t-1)$–linearity
- Strong (s,t)–linearity $\Rightarrow$ (s,t)–linearity
- $(\lceil \frac{n}{2} \rceil + s_1, 1)$–linearity $\Rightarrow$ strong $(2s_1, 1)$–linearity.

Multivariate ($\mathcal{MQ}$) schemes

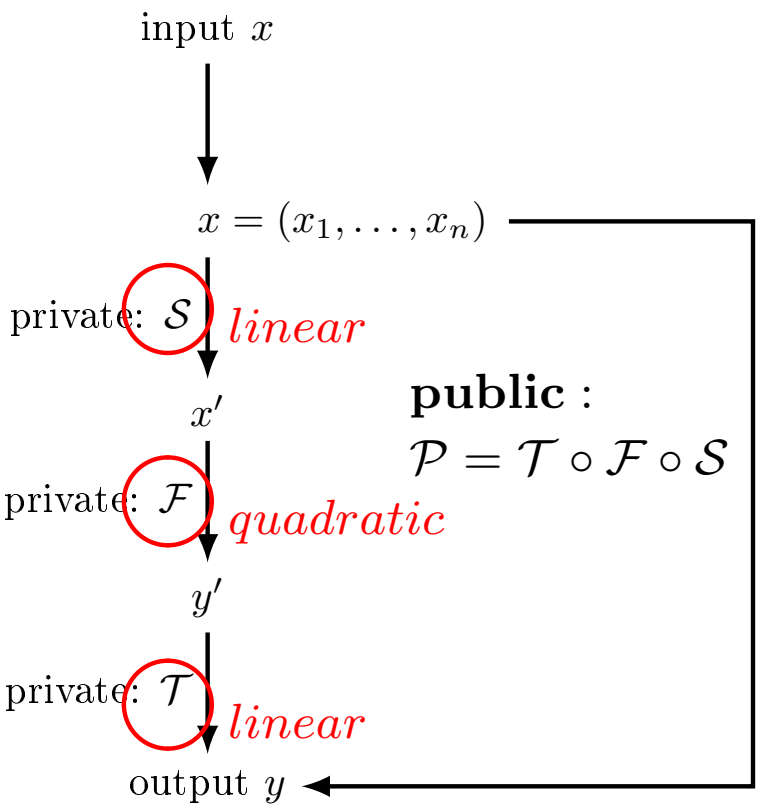
$$\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

Attacks:



Multivariate ($\mathcal{MQ}$) schemes

$$\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

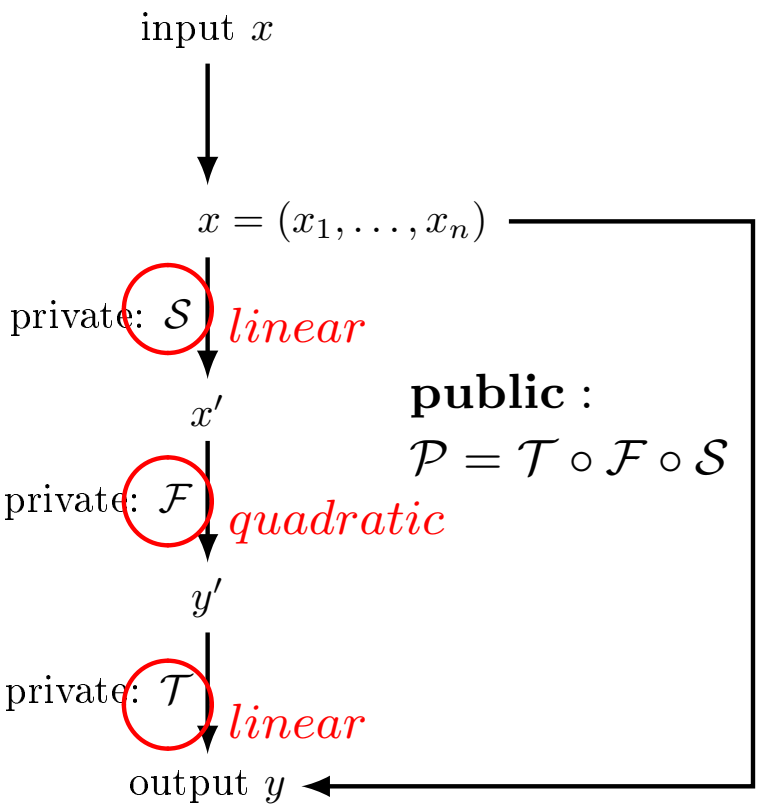


Attacks:

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

Multivariate ($\mathcal{MQ}$) schemes

$$\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$$



Attacks:

Linear subspaces!

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

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** $MR(n, r, m, \mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m)$
$(\text{Rank}\left(\sum_{i=1}^{k} \lambda_i \mathfrak{F}_i\right) \leqslant r)$ has a solution

iff

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

iff

f **is strongly** $(n-r, 1)$**–linear**.

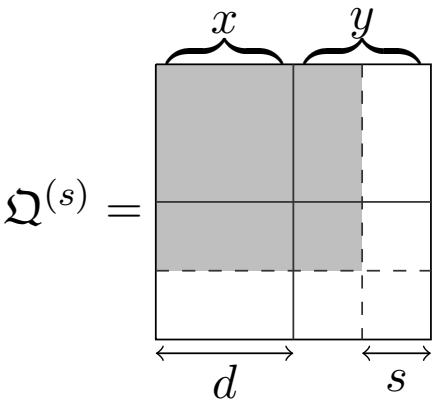
Equivalent Keys/Good Keys

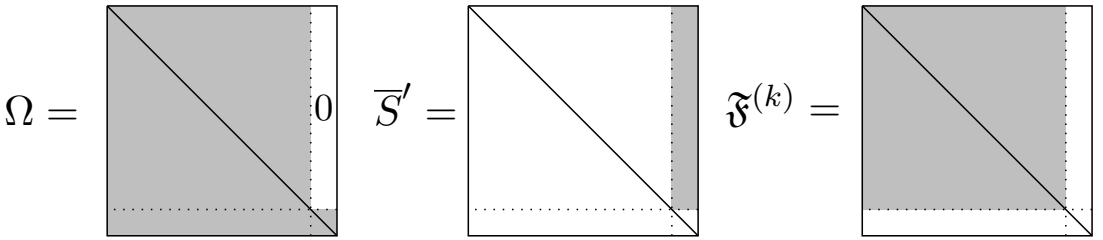
$$\begin{aligned}
\mathcal{P} &= \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} \Leftrightarrow \\
\mathcal{P} &= \underbrace{\mathcal{T} \circ \Sigma^{-1}}_{\mathcal{T}'} \circ \underbrace{\Sigma \circ \mathcal{F} \circ \Omega}_{\mathcal{F}'} \circ \underbrace{\Omega^{-1} \circ \mathcal{S}}_{\mathcal{S}'}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

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

Equivalent Keys/Good Keys

MQQ





Good Key for MQQ

Baby example MQQ

$$
\begin{aligned}
f_1(x_1,\ldots,x_6) &= x_2x_3 + x_4 + x_5 + x_6 \\
f_2(x_1,\ldots,x_6) &= x_1x_3 + x_5 + x_2x_4 + x_2x_5 + x_2x_6 \\
f_3(x_1,\ldots,x_6) &= x_2x_3 + x_5 + x_6 + x_4x_5 + x_5x_6 + x_3x_4 + x_3x_5 + x_3x_6
\end{aligned}
$$

$$
\mathfrak{F}^{(2)} = \begin{bmatrix}
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0
\end{bmatrix}
\qquad
\mathfrak{F}^{(3)} = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0
\end{bmatrix}
$$

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

After transforming:

$$
\begin{aligned}
f'_1(x_1,\ldots,x_6) &= x_2x_3 + x_4 + x_5 \\
f'_2(x_1,\ldots,x_6) &= x_1x_3 + x_5 + x_2x_4 + x_2x_5 \\
f'_3(x_1,\ldots,x_6) &= x_2x_3 + x_5 + x_6 + x_4x_5 + x_3x_4 + x_3x_5
\end{aligned}
$$

Baby example MQQ

$$
\begin{aligned}
f_1(x_1,\ldots,x_6) &= x_2x_3 + x_4 + x_5 + x_6 \\
f_2(x_1,\ldots,x_6) &= x_1x_3 + x_5 + x_2x_4 + x_2x_5 + x_2x_6 \\
f_3(x_1,\ldots,x_6) &= x_2x_3 + x_5 + x_6 + x_4x_5 + x_5x_6 + x_3x_4 + x_3x_5 + x_3x_6
\end{aligned}
$$

$$
\mathfrak{F}^{(2)} = \begin{bmatrix}
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0
\end{bmatrix}
\qquad
\mathfrak{F}^{(3)} = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0
\end{bmatrix}
$$

$$
\overline{S}' : \; x_4 \to x_4 + x_6 \;\Leftrightarrow\; (0,0,0,1,0,1) \in \mathrm{Ker}(\mathfrak{F}^{(1)}) \cap \mathrm{Ker}(\mathfrak{F}^{(2)}) \cap \mathrm{Ker}(\mathfrak{F}^{(3)})
$$

After transforming:

$$
\begin{aligned}
f'_1(x_1,\ldots,x_6) &= x_2x_3 + x_4 + x_5 \\
f'_2(x_1,\ldots,x_6) &= x_1x_3 + x_5 + x_2x_4 + x_2x_5 \\
f'_3(x_1,\ldots,x_6) &= x_2x_3 + x_5 + x_6 + x_4x_5 + x_3x_4 + x_3x_5
\end{aligned}
$$


Good Keys and Strong (s,t)–linearity

Let

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

$(\mathcal{F}', S', T')$ is called a **strong (s,t) separation key** for $\mathcal{P}$ if

- $\mathcal{P}$ is strongly (s,t)–linear with respect to two spaces V and W, $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$, and
- $S' = S_V^{\intercal}$, $\quad T' = T_W$,
  S_V,T_W with rows - bases of V, W.

Good key that exploits strong (s,t)–linearity

=

strong (s,t) separation key

Good Keys and Strong (s,t)–linearity

Let

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

$(\mathcal{F}', S', T')$ is called a **strong (s,t) separation key** for $\mathcal{P}$ if

- $\mathcal{P}$ is strongly (s,t)–linear with respect to two spaces V and W, $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$, and
- $S' = S_V^{\intercal}$, $\quad T' = T_W$,
  S_V,T_W with rows - bases of V, W.

Good key that exploits strong (s,t)–linearity

=

strong (s,t) separation key

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

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

1. A strong (s,t) separation key for $C^* \Rightarrow s \leqslant 1$, $t \leqslant 1$.
2. UOV using Maiorana-McFarland bent function does not posses a strong (s,t) separation key for any $s > 0$.

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

1. Determine the existence of a strong (s, t) separation key
2. Recover the linear space determined by the key
3. Repeat the procedure for the remaining part of the polynomials


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

1. Determine the existence of a strong (s, t) separation key
2. **Recover the linear space determined by the key**
3. Repeat the procedure for the remaining part of the polynomials


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

1. Determine the existence of a strong (s,t) separation key
2. **Recover the linear space determined by the key**
3. Repeat the procedure for the remaining part of the polynomials

(2) $\Leftrightarrow$ solving:

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

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


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

1. Determine the existence of a strong (s,t) separation key
2. **Recover the linear space determined by the key**
3. Repeat the procedure for the remaining part of the polynomials

Complexity:

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

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

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

Improved Min-Max strategy

1. Determine the existence of a strong (s,t) separation key
2. **Recover the linear space determined by the key**
3. Repeat the procedure for the remaining part of the polynomials

(2) $\Leftrightarrow$ solving:

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

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


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

Improved Min-Max strategy

1. Determine the existence of a strong (s,t) separation key
2. **Recover the linear space determined by the key**
3. Repeat the procedure for the remaining part of the polynomials

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

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

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


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

Improved Min-Max strategy

1. Determine the existence of a strong (s,t) separation key
2. **Recover the linear space determined by the key**
3. Repeat the procedure for the remaining part of the polynomials

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

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

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

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


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

Improved Min-Max strategy

1. Determine the existence of a strong (s,t) separation key
2. **Recover the linear space determined by the key**
3. Repeat the procedure for the remaining part of the polynomials

Complexity:

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

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

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

Improved Min-Max strategy

1. Determine the existence of a strong (s,t) separation key
2. **Recover the** **nined by the key**
3. Repeat the pr ni polynomials

if $n-s$ is small
MinRank

if $m-t$ is small
HighRank

Complexity:

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

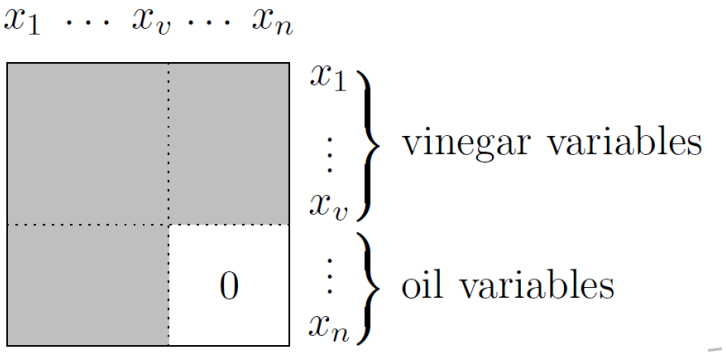
$$d_{reg}=\min\{(n-s)c_2,(m-t)c_1\}+1,$$
$2\leqslant\omega\leqslant 3$ - linear algebra constant.

Equivalent Keys/Good Keys

UOV

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

$$\mathfrak{F}^{(k)} =$$



Equivalent Keys/Good Keys

UOV

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

$$\mathfrak{F}^{(k)} = \begin{array}{c} \begin{array}{cccc} x_1 & \cdots & x_v & \cdots & x_n \end{array} \\ \left.\begin{array}{|c|c|} \hline & \\ \hline & 0 \\ \hline \end{array}\right. \begin{array}{l} x_1 \\ \vdots \\ x_v \end{array} \} \text{vinegar variables} \\ \begin{array}{l} \vdots \\ x_n \end{array} \} \text{oil variables} \end{array}$$

$$\Omega' = \begin{array}{|c|c|} \hline & 0 \\ \hline 0 & \\ \hline \end{array} \quad S'' = \begin{array}{|c|c|} \hline & 0 \\ \hline 0 & \\ \hline \end{array} \quad \mathfrak{F}^{(k)} = \begin{array}{|c|c|} \hline & \\ \hline & 0 \\ \hline \end{array}$$

$$\Omega' = \begin{array}{|c|c|} \hline & 0 \\ \hline 0 & \\ \hline \end{array} \quad S'' = \begin{array}{|c|c|} \hline 0 & \\ \hline 0 & \\ \hline \end{array} \quad \mathfrak{F}^{(k)} = \begin{array}{|c|c|} \hline & \\ \hline & 0 \\ \hline \end{array}$$

Good Key for UOV

Baby example UOV

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

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

$x_2 \to x_2 + x_5$

After transforming:

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

Baby example UOV

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

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

After transforming:

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

Good Keys and (s,t)–linearity

Let

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

$(\mathcal{F}', S', T')$ is called a (s,t) **separation key** for $\mathcal{P}$ if

- $\mathcal{P}$ is (s,t)–linear with respect to two spaces V and W, $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$, and
- $S' = S_V^{\intercal}, \quad T' = T_W$,
  S_V,T_W with rows - bases of V, W.

Good key that exploits (s,t)–linearity

=

(s,t) separation key

Good Keys and (s,t)–linearity

Let

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

$(\mathcal{F}', S', T')$ is called a (s,t) **separation key** for $\mathcal{P}$ if

- $\mathcal{P}$ is (s,t)–linear with respect to two spaces V and W, $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$, and
- $S' = S_V^{\intercal}, \quad T' = T_W$,
  S_V,T_W with rows - bases of V, W.

Good key that exploits (s,t)–linearity

=

(s,t) separation key

(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	$(n,m)=(32,24)$	$(10,24),(14,14),(24,10)$

Separation keys for C^* and SFLASH

- (d, n) separation key for C^* with secret map

$$\mathcal{F}(x) = x^{2^\ell+1}$$

  where $\gcd(2^\ell + 1, 2^n - 1) = 1$ and $\gcd(\ell, n) = d$.
- The size of the space V is invariant under restrictions of the public map (minus modifier).
- $\Rightarrow (d, k)$ separation key for SFLASH, where $k \leqslant n$ is the number of coordinates of the public key.


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

(n, m) function with coordinate functions p_i: $\mathfrak{P}_i := \widetilde{\mathfrak{P}}_i + \widetilde{\mathfrak{P}}_i^{\mathsf{T}}$

The task of finding an (s, m) separation key $(S_V^{\mathsf{T}}, T_{\mathbb{F}_q^m})$ is equivalent to solving

$$\begin{aligned} a^{(j)}\mathfrak{P}_i a^{(k)} &= 0,\ i \in \{1, ..., m\},\ j, k \in \{1, ..., s\}, j < k \\ a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} &= 0,\ i \in \{1, ..., m\},\ k \in \{1, ..., s\}, \end{aligned}$$

in the unknown basis vectors $a^{(j)}$ of the space V.

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

The key can equivalently be found by

1. First solving the quadratic

$$\begin{aligned} a^{(j)}\mathfrak{P}_i a^{(k)} &= 0,\ i \in \{1,...,m\},\ j,k \in \{1,...,c\}, j<k \\ a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} &= 0,\ i \in \{1,...,m\},\ k \in \{1,...,c\}, \end{aligned}$$

in the unknown basis vectors $a^{(k)}$ of the space V, for some c.

2. And then solving the linear

$$\begin{aligned} &a^{(j)}\mathfrak{P}_i a^{(k)} = 0, \\ &i \in \{1,...,m\}, j \in \{1,...,c\}, k \in \{c+1,...,s\}, j<k \end{aligned}$$

in the unknown basis vectors $a^{(k)}$ of the space V.

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

The key can equivalently be found by

1. First solving the quadratic

$$\begin{aligned} a^{(j)}\mathfrak{P}_i a^{(k)} &= 0,\ i \in \{1,...,m\},\ j,k \in \{1,...,c\}, j<k \\ a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} &= 0,\ i \in \{1,...,m\},\ k \in \{1,...,c\}, \end{aligned}$$

in the unknown basis vectors $a^{(k)}$ of the space V, for some c.

2. And then sol

$$a^{(}$$

$$i \in \{1,...,m\}, j \in \{1,...,c\}, k \in \{c+1,...,s\}, j<k$$

in the unknown basis vectors $a^{(k)}$ of the space V.

$m\binom{c+1}{2}$ equations

$(n-s)c$ variables

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

The key can equivalently be found by

1. First solving the quadratic

$$\begin{aligned} a^{(j)}\mathfrak{P}_i a^{(k)} &= 0,\ i \in \{1,...,m\},\ j,k \in \{1,...,c\}, j<k \\ a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} &= 0,\ i \in \{1,...,m\},\ k \in \{1,...,c\}, \end{aligned}$$

in the unknown basis vectors $a^{(k)}$ of the space V, for some c.

2. And then sol

$$a^{(}$$

$$i \in$$

We choose c s.t. $\quad m\binom{c+1}{2} > (n-s)c$

in the unknown basis vectors $a^{(k)}$ of the space V.

Reconciliation Attack on UOV in terms of (s,t)–linearity

Input: UOV public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.
$V_0 \leftarrow$ the zero-dimensional vector space
for $k := 1$ to m **do**
Find $a^{(k)} = (a_1^{(k)}, ..., a_v^{(k)}, 0, ..., 0, 1_{n-k+1}, 0, ..., 0) \in \mathbb{F}_q^n$,
by solving

$$\begin{aligned} a^{(j)} \mathfrak{P}_i a^{(k)} &= 0, \ i \in \{1, \ldots, m\}, j < k \\ a^{(k)} \widetilde{\mathfrak{P}}_i a^{(k)} &= 0, \ i \in \{1, \ldots, m\}, \end{aligned}$$

Construct a space $V_k \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V_k) = k$, s.t.

- $V_k = V_{k-1} \oplus Span\left\{a^{(k)}\right\}$, and
- $\mathcal{P}$ is (k,m)–linear with respect to $(V_k, \mathbb{F}_q^m)$.

end for
Output: An oil space $V = V_m$ of dimension m.


Reconciliation Attack on UOV in terms of (s,t)–linearity

Input: UOV public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.
$V_0 \leftarrow$ the zero-dimensional vector space
for $k := 1$ to m **do**
Find $a^{(k)} = (a_1^{(k)}, ..., a_v^{(k)}, 0, ..., 0, 1_{n-k+1}, 0, ..., 0) \in \mathbb{F}_q^n$,
by solving

$$\begin{aligned} a^{(j)}\mathfrak{P}_i a^{(k)} &= 0,\ i \in \{1,\dots,m\}, j < k \\ a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} &= 0,\ i \in \{1,\dots,m\}, \end{aligned}$$

Construct a spac

The attack takes $c = 1$

- $V_k = V_{k-1} \oplus$
- $\mathcal{P}$ is (k,m)–linear with respect to $(V_k, \mathbb{F}_q^m)$.

end for
Output: An oil space $V = V_m$ of dimension m.


Reconciliation Attack on UOV in terms of (s,t)–linearity

Input: UOV public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.
$V_0 \leftarrow$ the zero-dimensional vector space
for $k := 1$ to m **do**
Find $a^{(k)} = (a_1^{(k)}, ..., a_v^{(k)}, 0, ..., 0, 1_{n-k+1}, 0, ..., 0) \in \mathbb{F}_q^n$,
by solving

$$\begin{aligned} a^{(j)}\mathfrak{P}_i a^{(k)} &= 0, \ i \in \{1, \ldots, m\}, j < k \\ a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} &= 0, \ i \in \{1, \ldots, m\}, \end{aligned}$$

Construct a spac

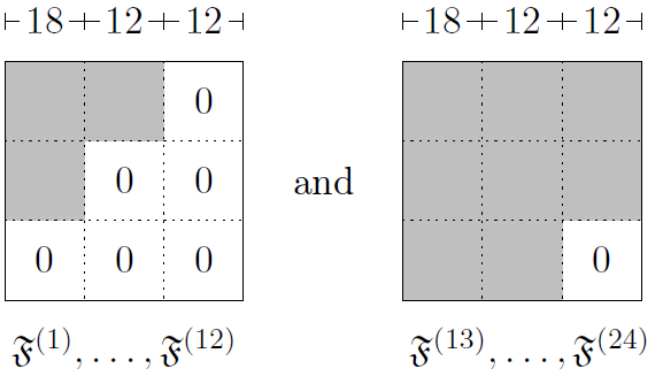
- $V_k = V_{k-1} \in$
- $\mathcal{P}$ is (k,m)–linear with respect to $(V_k, \mathbb{F}_q)$.

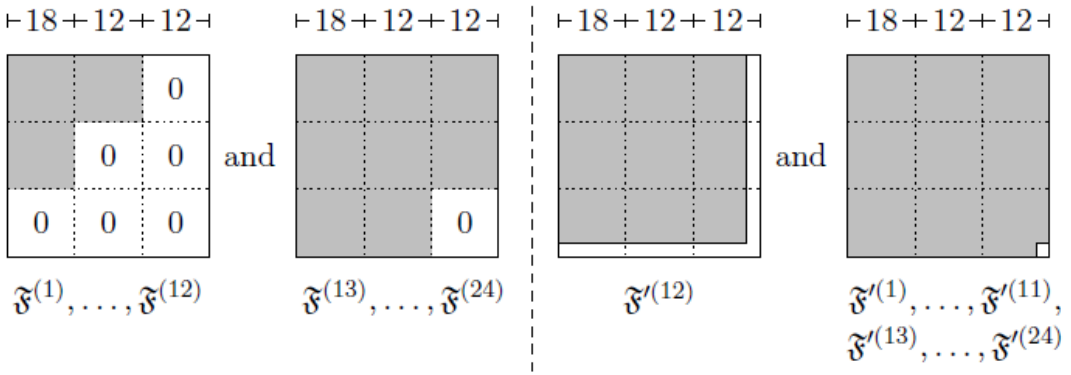
$c = 1$ **only good for** $n \approx 2m$

end for
Output: An oil space $V = V_m$ of dimension m.


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

Rainbow





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

Conclusions and future work

- Turns out:

We need to use prudent design principles similarly to the practice in symmetric cryptography

Linearity measure – First generic measure for resistance to linear attacks

- **Future work: Link to differential cryptanalysis?**
- **Future work: Applications in symmetric crypto?**


Conclusions and future work

- Turns out:

We need to use prudent design principles similarly to the practice in symmetric cryptography

Linearity measure – First generic measure for resistance to linear attacks

- Future work: Link to differential cryptanalysis?
- Future work: Applications in symmetric crypto?


Conclusions and future work

- Turns out:

We need to use prudent design principles similarly to the practice in symmetric cryptography

Linearity measure – First generic measure for resistance to linear attacks

- **Future work: Link to differential cryptanalysis?**
- **Future work: Applications in symmetric crypto?**


Conclusions and future work

- Turns out:

We need to use prudent design principles similarly to the practice in symmetric cryptography

Linearity measure – First generic measure for resistance to linear attacks

- **Future work: Link to differential cryptanalysis?**
- **Future work: Applications in symmetric crypto?**


Thank you for listening!