Radboud University

Multivariate cryptography – Cryptanalysis techniques II

SLMath summer school:
Introduction to Quantum-Safe Cryptography (IBM Zurich)

Simona Samardjiska

July, 2024

Institute for Computing and Information Sciences
Radboud University

Recall the MinRank problem

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.:

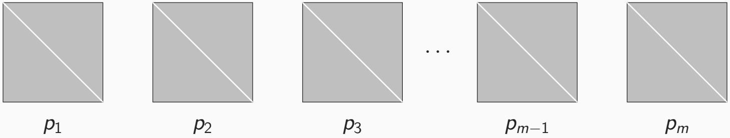
$$\text{Rank}\left(\sum_{i=1}^{m} \lambda_i M_i\right) \leqslant r.$$

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

How do we use MinRank in cryptanalysis?

$\mathcal{P} = (p_1, p_2, \ldots, p_m)$ - public polynomials,

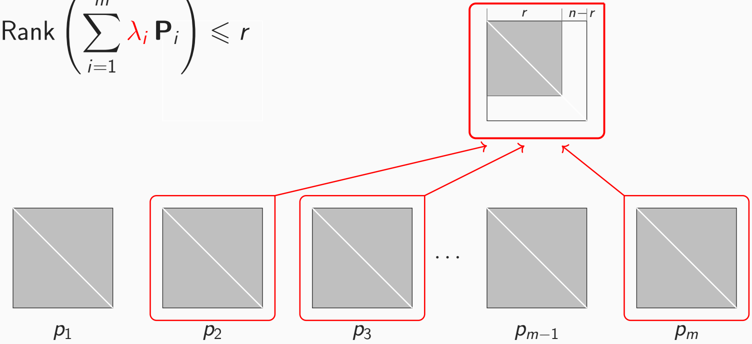
$\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_m$ - matrix representations of the coordinates of $\mathcal{P}$.



How do we use MinRank in cryptanalysis?

$\mathcal{P} = (p_1, p_2, \ldots, p_m)$ - public polynomials,
$\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_m$ - matrix representations of the coordinates of $\mathcal{P}$.

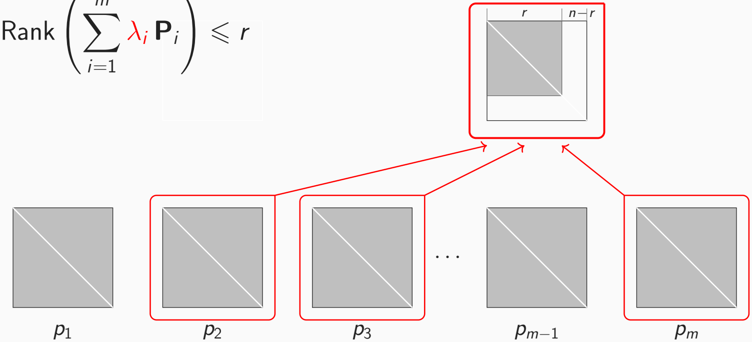
$$\mathrm{Rank}\left(\sum_{i=1}^{m} \lambda_i \mathbf{P}_i\right) \leqslant r$$



How do we use MinRank in cryptanalysis?

$\mathcal{P} = (p_1, p_2, \ldots, p_m)$ - public polynomials,
$\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_m$ - matrix representations of the coordinates of $\mathcal{P}$.

$$\text{Rank}\left(\sum_{i=1}^{m} {\color{red}\lambda_i}\, \mathbf{P}_i\right) \leqslant r$$



$\mathcal{S}$ is determined by

$$\text{Ker}\left(\sum_{i=1}^{m} {\color{red}\lambda_i}\, \mathbf{P}_i\right)$$

$\mathcal{T}$ is determined by

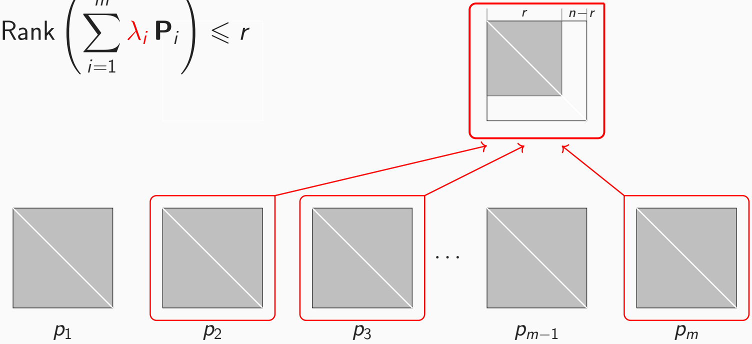
$$\langle {\color{red}(\lambda_1, \ldots, \lambda_m)} \rangle$$

How do we use MinRank in cryptanalysis?

$\mathcal{P} = (p_1, p_2, \ldots, p_m)$ - public polynomials,

$\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_m$ - matrix representations of the coordinates of $\mathcal{P}$.

$$\mathrm{Rank}\left(\sum_{i=1}^{m} \lambda_i \mathbf{P}_i\right) \leqslant r$$



$\mathcal{S}$ is determined by

$$\mathrm{Ker}\left(\sum_{i=1}^{m} \lambda_i \mathbf{P}_i\right)$$

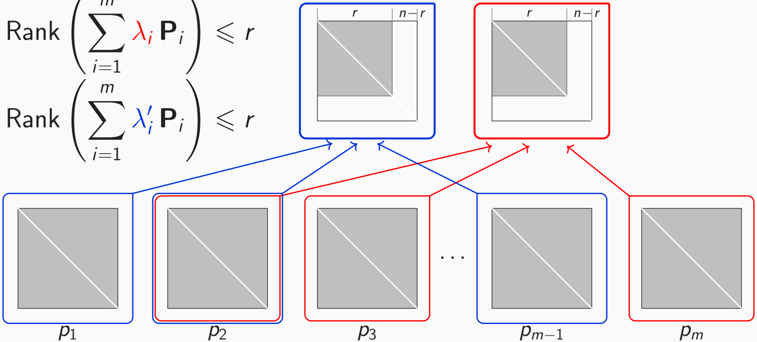
$\mathcal{T}$ is determined by

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

$\mathcal{P} = (p_1, p_2, \dots, p_m)$ - public polynomials,
$\mathbf{P}_1, \mathbf{P}_2, \dots, \mathbf{P}_m$ - matrix representations of the coordinates of $\mathcal{P}$.

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

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



$\mathcal{S}$ is determined by

$$\text{Ker}\left(\sum_{i=1}^{m} \lambda_i \mathbf{P}_i\right)$$

$\mathcal{T}$ is determined by

$$\langle(\lambda_1, \dots, \lambda_m)\rangle$$

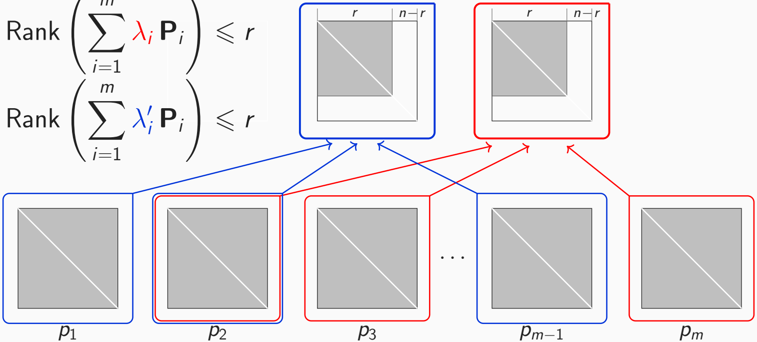
How do we use MinRank in cryptanalysis?

$\mathcal{P} = (p_1, p_2, \ldots, p_m)$ - public polynomials,

$\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_m$ - matrix representations of the coordinates of $\mathcal{P}$.

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

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



$\mathcal{S}$ is determined by

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

$\mathcal{T}$ is determined by

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

Baby example UOV

Similar approach works for UOV, although it is not a result of "rank defect" (at leaset not so obvious)

$$f_1(x_1, \ldots, x_6) = x_1x_2 + x_2x_4 + x_3x_6 + x_4x_6 + x_5x_6 + x_6$$

$$f_2(x_1, \ldots, x_6) = x_1x_4 + x_3x_4 + x_3x_6 + x_4x_6 + x_6$$

$$f_3(x_1, \ldots, x_6) = x_2x_3 + x_3x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_1x_6 + x_4x_6 + x_5x_6$$

Baby example UOV

Similar approach works for UOV, although it is not a result of “rank defect” (at leaset not so obvious)

$$f_1(x_1, \dots, x_6) = x_1x_2 + x_2x_4 + x_3x_6 + x_4x_6 + \color{red}{x_5x_6} + x_6$$

$$f_2(x_1, \dots, x_6) = x_1x_4 + x_3x_4 + x_3x_6 + x_4x_6 + x_6$$

$$f_3(x_1, \dots, x_6) = x_2x_3 + x_3x_5 + x_2x_4 + x_2x_6 + x_4x_5 + x_1x_6 + x_4x_6 + \color{red}{x_5x_6}$$

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

Baby example UOV

Similar approach works for UOV, although it is not a result of "rank defect" (at leaset not so obvious)

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

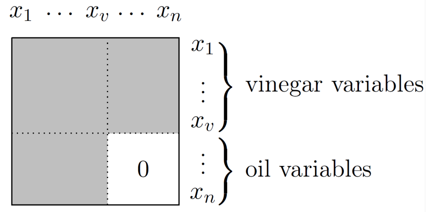
$$\overline{S}': \begin{aligned} x_4 &\to x_4 + x_6 \\ x_2 &\to x_2 + x_5 \end{aligned}$$

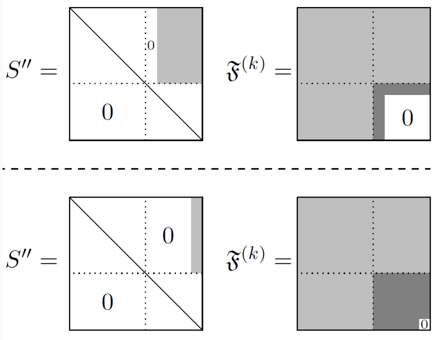
After change of variables, we have separated (some) of the oil space (x_5, x_6) :

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

UOV

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

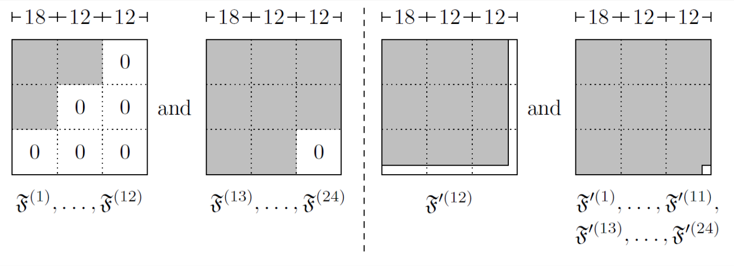


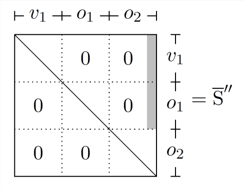


Good Keys for UOV

Rainbow partial revealing of structure ("good keys")

Rainbow before and after applying an input and output change of basis (separating a a good key)



Good key for Rainbow - 

Measuring linear spaces

Linear spaces of (n, m)-functions

- **Differential** of f: $\mathcal{D}_w f(x) = f(x+w) - f(x) - f(w) + f(0)$
- Linearity for (n, m) functions $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined already 1992 by Nyberg
- $w \in \mathbb{F}_q^n$ - **linear structure** of f if

$$\mathcal{D}_w f(x) = 0 \quad \forall\, x \in \mathbb{F}_q^n .$$

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

Quadratic form f**:** $\mathcal{D}_w f(x) = w^\intercal \mathbf{F} x$, for a symmetric matrix $\mathbf{F}$,

- Ker($\mathbf{F}$) - **linear space of** f**.**

[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** - Rank$(\mathbf{F}_w) = n$, even n, $m \leqslant n/2$,
- **Almost bent (AB) functions** - Rank$(\mathbf{F}_w) = n - 1$, odd $n = m$.

Linear spaces of (n, m)-functions

- **Differential** of f: $\mathcal{D}_w f(x) = f(x+w) - f(x) - f(w) + f(0)$
- Linearity for (n, m) functions $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined already 1992 by Nyberg
- $w \in \mathbb{F}_q^n$ - **linear structure** of f if

$$\mathcal{D}_w f(x) = 0 \quad \forall\, x \in \mathbb{F}_q^n .$$

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

Quadratic form f**:** $\mathcal{D}_w f(x) = w^\intercal \mathbf{F} x$, for a symmetric matrix $\mathbf{F}$,

- Ker($\mathbf{F}$) - **linear space of** f**.**

[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** - Rank$(\mathbf{F}_w) = n$, even n, $m \leqslant n/2$,
- **Almost bent (AB) functions** - Rank$(\mathbf{F}_w) = n - 1$, odd $n = m$.

Linear spaces of (n, m)-functions

- **Differential** of f: $\mathcal{D}_w f(x) = f(x+w) - f(x) - f(w) + f(0)$
- Linearity for (n, m) functions $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined already 1992 by Nyberg
- $w \in \mathbb{F}_q^n$ - **linear structure** of f if

$$\mathcal{D}_w f(x) = 0 \quad \forall\, x \in \mathbb{F}_q^n\,.$$

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

Quadratic form f**:** $\mathcal{D}_w f(x) = w^\intercal \mathbf{F} x$, for a symmetric matrix $\mathbf{F}$,

- Ker($\mathbf{F}$) - **linear space of** f**.**

[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** - Rank$(\mathbf{F}_w) = n$, even n, $m \leqslant n/2$,
- **Almost bent (AB) functions** - Rank$(\mathbf{F}_w) = n - 1$, odd $n = m$.

Example 1:

f :

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

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

f' :

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

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

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

Example 1:

f :

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

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

f' :

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

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

Both have maximum linearity, but f' is linear on a larger space!

It is an important measure!

Oil & Vinegar maps

f :

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

f is linear on the oil subspace (when you fix the vinegar variables)!

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

Oil & Vinegar maps

f :

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

f is linear on the oil subspace (when you fix the vinegar variables)!

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

Oil & Vinegar maps

f :

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

f is linear on the oil subspace (when you fix the vinegar variables)!

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

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.

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

(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.

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.

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

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

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.
- for $w \in W$, $\mathcal{D}_a w^\intercal \cdot f(b) = 0$, $\forall\ a, b \in V$.
- for $w \in W$, $f_W(0,y) = M(0)\cdot y + G(0) = 0, \forall\ (0,a) \in V$ - **all components in W vanish on the V space**

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,
$V = \langle(0,1,0,0),(0,0,1,0),(0,0,0,1)\rangle$, $W = \langle(1,0,0),(0,1,0)\rangle$

$\mathcal{D}_a f(b) = 0, \quad \forall\ a, b$ in the oil space O.

$f(0, a) = 0, \forall\ a \in O$ - **the oil and vinegar map vanishes on the oil space!**

Basis for the new definition of UOV [Beullens21]

A consequence? - **Reconciliation Attack [Ding et al.]**

In a nutshel: **Recover** (s, m) **linearity** of the public $\mathcal{P} : \mathbf{P}_1, \ldots, \mathbf{P}_m$

Solve:

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

in the unknown basis vectors $x^{(j)}$ of the oil space O,

where $\mathbf{P}_i := \widetilde{\mathbf{P}}_i + \widetilde{\mathbf{P}}_i^\mathsf{T}$.

Back to UOV - what does the above mean?

$\mathcal{D}_a f(b) = 0, \quad \forall\ a, b$ in the oil space O.
$f(0, a) = 0, \forall\ a \in O$ - **the oil and vinegar map vanishes on the oil space!**

Basis for the new definition of UOV [Beullens21]

A consequence? - **Reconciliation Attack [Ding et al.]**

In a nutshel: **Recover** (s, m) **linearity** of the public $\mathcal{P} : \mathbf{P}_1, \ldots, \mathbf{P}_m$

Solve:

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

in the unknown basis vectors $x^{(j)}$ of the oil space O,

where $\mathbf{P}_i := \widetilde{\mathbf{P}}_i + \widetilde{\mathbf{P}}_i^{\intercal}$.

Reconciliation attack [Ding et al.]

As given in [SG14]:

1. Solve the quadratic

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

   in the unknown basis vectors $x^{(k)}$ of the space O.

   [$m\binom{c+1}{2}$ **quadratic and bilinear equations** $(n-m)c$ **variables**
   We must choose c s.t. $m\binom{c+1}{2} \geq (n-m)c$ **(typically at least 2)**]

2. Then solve the linear

$$
x^{(j)}\mathbf{P}_i x^{(k)} = 0,\ \ i \in \{1, \dots, m\}, j \in \{1, \dots, c\}, k \in \{c+1, \dots, m\}, j < k
$$

   in the unknown basis vectors $x^{(k)}$ of the oil space O.

   [For first k, mc **linear equations** $(n-m)$ **variables**
   Works if $m(c+1) \geq n$,
   otherwise plug in in step 1 and solve easier quadratic system]

Making the reconciliation attack practical

Important about the attack:

- If c taken big enough in the first step, second step is always polynomial
- **First step is the expensive one**
- **Questions:**
  - Can we have a polynomial second step for smaller c?
  - **Yes, only one vector seems to be enough!**
  - Can we find easier (than step 1) vectors in the oil space?
  - **Yes, intersection attack!**

One oil vector breaks UOV!

- Shown in [Aulbach, Campos, Krämer, S, Stöttinger '23]
- Simpler view in [Pébereau'24]
  - Assume $n \leq 3m$
  - Assume an oil vector o is known
  - Recall that $\boxed{\mathcal{D}_o f(b) = 0, \quad \forall\ b \text{ in the oil space } O.}$

    so the oil space O lives in the kernel of the differential $\mathcal{D}_o$

    $$|\mathrm{Ker}(\mathcal{D}_o)| = n - m$$

  - Restrict the public key to $\mathrm{Ker}(\mathcal{D}_o)$ using a basis matrix $\mathbf{S}_{\mathrm{Ker}}$

    $$\mathcal{P}_{|\,\mathrm{Ker}(\mathcal{D}_o)} = \mathcal{P} \circ \mathbf{S}_{\mathrm{Ker}}$$

  - Obtain a $(n - m, m)$ UOV instance
    - Unknown oil space O' can be found by Kipnis-Shamir attack '98 (becomes polynomial)
    - Alternatively, use Step 2 of reconciliation attack for $c = 1$ (becomes polynomial)
  - Go back to original UOV instance
    - Basis of unknown oil space $\mathbf{B}_O = \mathbf{S}_{\mathrm{Ker}} \cdot \mathbf{B}_{O'}$

Finding one oil vector: enhancement of Kipnis-Shamir attack '98

- Kipnis-Shamir attack '98 - Broke Oil & Vinegar by Patarin ($n = 2m$)
- Recall that $\mathcal{D}_o f(b) = 0, \quad \forall\ b$ in the oil space O.
- In matrix form

$$
\begin{aligned}
o^{(j)} \mathbf{P}_i o^{(k)} &= 0,\ i \in \{1, ..., m\},\ j, k \in \{1, ..., m\} \\
\mathbf{P}_i \cdot O &\subset O^{\perp}
\end{aligned}
$$

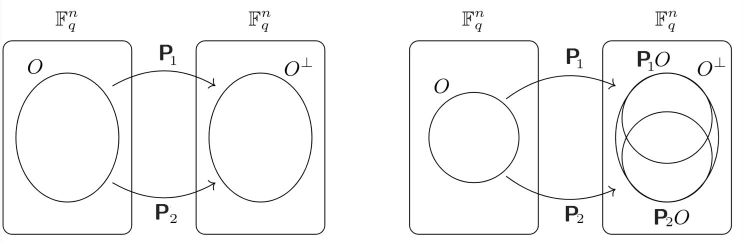
- $|\mathbf{P}_i \cdot O| = m, \ \left|O^{\perp}\right| = n - m$
- $|\mathbf{P}_i \cdot O \cap \mathbf{P}_j \cdot O| \geq |\mathbf{P}_i \cdot O| + |\mathbf{P}_j \cdot O| - \left|O^{\perp}\right| = 3m - n$

Finding one oil vector: enhancement of Kipnis-Shamir attack '98

- Kipnis-Shamir attack '98 - Broke Oil & Vinegar by Patarin ($n = 2m$)
- Recall that $\mathcal{D}_o f(b) = 0, \quad \forall\, b$ in the oil space O.
- In matrix form

$$\begin{aligned} o^{(j)} \mathbf{P}_i o^{(k)} &= 0,\ i \in \{1, \dots, m\},\ j,k \in \{1, \dots, m\} \\ \mathbf{P}_i \cdot O &\subset O^{\perp} \end{aligned}$$

- $|\mathbf{P}_i \cdot O| = m$, $\left|O^{\perp}\right| = n - m$
- $|\mathbf{P}_i \cdot O \cap \mathbf{P}_j \cdot O| \geq |\mathbf{P}_i \cdot O| + |\mathbf{P}_j \cdot O| - \left|O^{\perp}\right| = 3m - n$

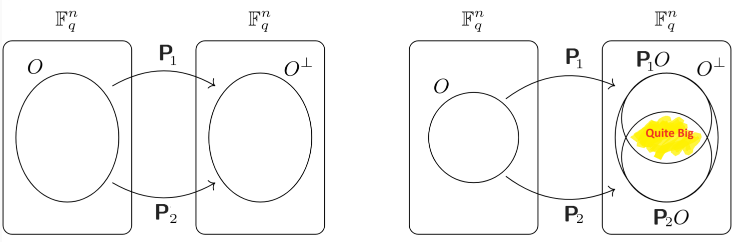


Finding one oil vector: enhancement of Kipnis-Shamir attack '98

- Kipnis-Shamir attack '98 - Broke Oil & Vinegar by Patarin ($n = 2m$)
- Recall that $\mathcal{D}_o f(b) = 0, \quad \forall\ b$ in the oil space O.
- In matrix form

$$\begin{aligned} o^{(j)} \mathbf{P}_i o^{(k)} &= 0,\ i \in \{1, ..., m\},\ j, k \in \{1, ..., m\} \\ \mathbf{P}_i \cdot O &\subset O^{\perp} \end{aligned}$$

- $|\mathbf{P}_i \cdot O| = m,\ \left|O^{\perp}\right| = n - m$
- $|\mathbf{P}_i \cdot O \cap \mathbf{P}_j \cdot O| \geq |\mathbf{P}_i \cdot O| + |\mathbf{P}_j \cdot O| - \left|O^{\perp}\right| = 3m - n$



Intersection attack [Beullens '20]

- Focus on $n < 3m$
- **We want to find x in the intersection $\mathbf{P}_i \cdot O \cap \mathbf{P}_j \cdot O$**
- But then **$\mathbf{P}_i^{-1}x \in O$ and $\mathbf{P}_j^{-1}x \in O$ are two oil vectors**
- We can do the reconciliation attack but on steroids!
  - Fix $3m - n$ coordinates of x and solve the quadratic system

$$
\begin{aligned}
(\mathbf{P}_1^{-1}x)^\top \mathbf{P}_i \mathbf{P}_2^{-1}x &= 0, \; i \in \{1, ..., m\} \\
(\mathbf{P}_1^{-1}x)^\top \widetilde{\mathbf{P}}_i (\mathbf{P}_1^{-1}x) &= 0, \; i \in \{1, ..., m\} \\
(\mathbf{P}_2^{-1}x)^\top \widetilde{\mathbf{P}}_i (\mathbf{P}_2^{-1}x) &= 0, \; i \in \{1, ..., m\}
\end{aligned}
$$

  - $3m$ equations and $2n - 3m$ variables
- **We now have two oil vectors, the rest is easy!**

Intersection attack [Beullens '20]

- Focus on $n < 3m$
- **We want to find x in the intersection $\mathbf{P}_i \cdot O \cap \mathbf{P}_j \cdot O$**
- But then **$\mathbf{P}_i^{-1}x \in O$ and $\mathbf{P}_j^{-1}x \in O$ are two oil vectors**
- We can do the reconciliation attack but on steroids!
  - Fix $3m - n$ coordinates of x and solve the quadratic system

$$\begin{aligned}(\mathbf{P}_1^{-1}x)^\top \mathbf{P}_i \mathbf{P}_2^{-1}x &= 0, \ i \in \{1, ..., m\}\\ (\mathbf{P}_1^{-1}x)^\top \widetilde{\mathbf{P}}_i (\mathbf{P}_1^{-1}x) &= 0, \ i \in \{1, ..., m\}\\ (\mathbf{P}_2^{-1}x)^\top \widetilde{\mathbf{P}}_i (\mathbf{P}_2^{-1}x) &= 0, \ i \in \{1, ..., m\}\end{aligned}$$

  - $3m$ equations and $2n - 3m$ variables
- **We now have two oil vectors, the rest is easy!**

Now, let's think again about our measures of linearity

Better said, let's take a different perspective...

So far we considered m symmetric matrices representing our polynomials.

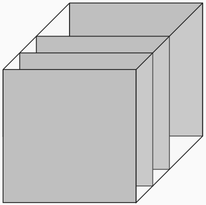
Like this:

Now, let's think again about our measures of linearity

Better said, let's take a different perspective...

So far we considered m symmetric matrices representing our polynomials.

Like this:

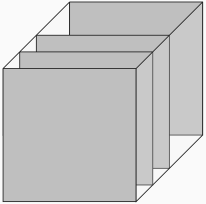


Now, let's think again about our measures of linearity

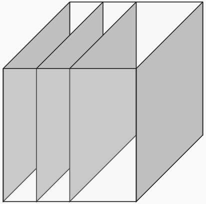
Better said, let's take a different perspective...

So far we considered m symmetric matrices representing our polynomials.

Like this:



But, this is also good...

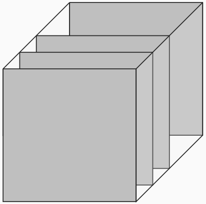


Now, let's think again about our measures of linearity

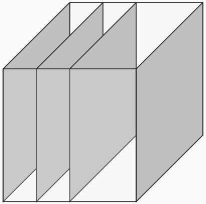
Better said, let's take a different perspective...

So far we considered m symmetric matrices representing our polynomials.

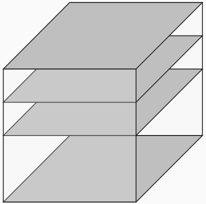
Like this:



But, this is also good...



And this!

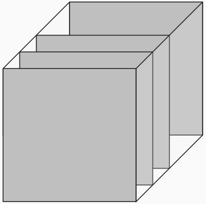


Now, let's think again about our measures of linearity

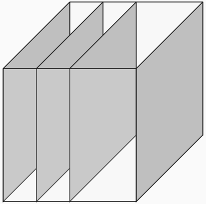
Better said, let's take a different perspective...

So far we considered m symmetric matrices representing our polynomials.

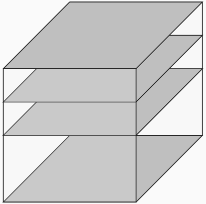
Like this:



But, this is also good. . .



And this!



- This is different **tensor view**, but the same object!
- Instead of array of two-dimensional matrices, we look at it as a three-dimensional qube!

How does this change perspective?

Recall, UOV has an important hidden linear spaces (the oil space)...

But no rank defects!

Sure?

How does this change perspective?

Recall, UOV has an important hidden linear spaces (the oil space). . .

But no rank defects!

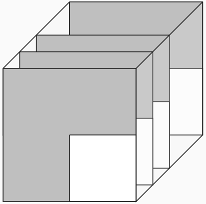
Sure?

How does this change perspective?

Recall, UOV has an important hidden linear spaces (the oil space). . .

But no rank defects!

Sure?

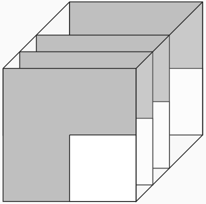


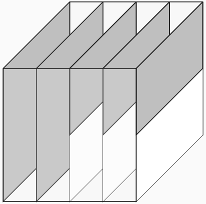
How does this change perspective?

Recall, UOV has an important hidden linear spaces (the oil space)...

But no rank defects!

Sure?



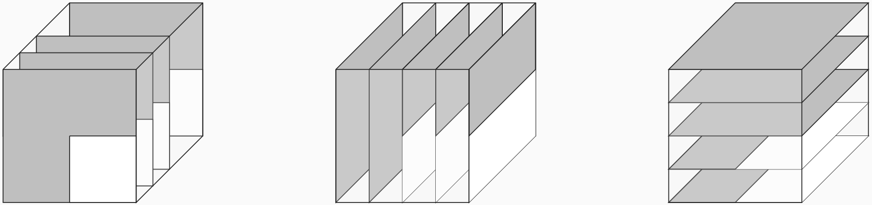


How does this change perspective?

Recall, UOV has an important hidden linear spaces (the oil space)...

But no rank defects!

Sure?



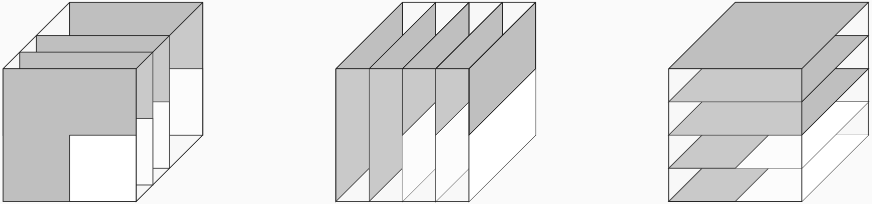
- In the second and third view, we observe a rank defect!
- We can use (Rectangular) MinRank!
- Beullens '22 used it to improve the analysis on UOV and Rainbow
- **Important takeaway:** The two types of important linear spaces can be characterized in the same way!

How does this change perspective?

Recall, UOV has an important hidden linear spaces (the oil space)...

But no rank defects!

Sure?



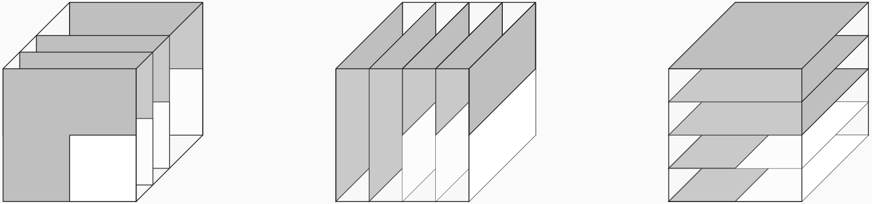
- In the second and third view, we observe a rank defect!
- We can use (Rectangular) MinRank!
- Beullens '22 used it to improve the analysis on UOV and Rainbow
- **Important takeaway:** The two types of important linear spaces can be characterized in the same way!

How does this change perspective?

Recall, UOV has an important hidden linear spaces (the oil space). . .

But no rank defects!

Sure?



- In the second and third view, we observe a rank defect!
- We can use (Rectangular) MinRank!
- Beullens '22 used it to improve the analysis on UOV and Rainbow
- **Important takeaway:** The two types of important linear spaces can be characterized in the same way!

Equivalent keys used wrong

- MQ-Sign - submitted to the Korean PQC competition for standardization
- **Now a finalist**
- MQ-Sign design principle:
  - UOV map
  - Sparse polynomials to reduce key size - only v coefficients per polynomial
  - Four variants with different level of sparsness
  - Equivalent keys technique to reduce key size
- **Polynomial time attack [AST23] on the sparse variants**
- Result of flawed use of equivalent keys

Equivalent keys used wrong

- MQ-Sign - submitted to the Korean PQC competition for standardization
- **Now a finalist**
- MQ-Sign design principle:
  - UOV map
  - Sparse polynomials to reduce key size - only v coefficients per polynomial
  - Four variants with different level of sparsness
  - Equivalent keys technique to reduce key size
- **Polynomial time attack [AST23] on the sparse variants**
- Result of flawed use of equivalent keys

Equivalent keys used wrong

- MQ-Sign - submitted to the Korean PQC competition for standardization
- **Now a finalist**
- MQ-Sign design principle:
  - UOV map
  - Sparse polynomials to reduce key size - only v coefficients per polynomial
  - Four variants with different level of sparsness
  - Equivalent keys technique to reduce key size
- **Polynomial time attack [AST23] on the sparse variants**
- Result of flawed use of equivalent keys

Equivalent keys used wrong

- MQ-Sign - submitted to the Korean PQC competition for standardization
- **Now a finalist**
- MQ-Sign design principle:
  - UOV map
  - Sparse polynomials to reduce key size - only v coefficients per polynomial
  - Four variants with different level of sparsness
  - Equivalent keys technique to reduce key size
- **Polynomial time attack [AST23] on the sparse variants**
- Result of flawed use of equivalent keys

MQ-Sign Central map

$$\mathcal{F}_V^{(1)} = \sum_{i=1}^{v} \gamma_i^{(1)} x_i x_{(i \bmod v)+1} \quad \rightarrow \quad \mathbf{F}_V^{(1)} = \begin{pmatrix} 0 & \gamma_1^{(1)} & 0 & \cdots & 0 \\ 0 & 0 & \gamma_2^{(1)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-1}^{(1)} \\ \gamma_v^{(1)} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$\mathcal{F}_V^{(2)} = \sum_{i=1}^{v} \gamma_i^{(2)} x_i x_{(i+1 \bmod v)+1} \quad \rightarrow \quad \mathbf{F}_V^{(2)} = \begin{pmatrix} 0 & 0 & \gamma_1^{(2)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-2}^{(2)} \\ \gamma_{v-1}^{(2)} & 0 & 0 & \cdots & 0 \\ 0 & \gamma_v^{(2)} & 0 & \cdots & 0 \end{pmatrix}$$

$$\vdots$$

MQ-Sign Central map

$$\mathcal{F}_V^{(1)} = \sum_{i=1}^{v} \gamma_i^{(1)} x_i x_{(i \bmod v)+1} \quad \to \quad \mathbf{F}_V^{(1)} = \begin{pmatrix} 0 & \gamma_1^{(1)} & 0 & \cdots & 0 \\ 0 & 0 & \gamma_2^{(1)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-1}^{(1)} \\ \gamma_v^{(1)} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$\mathcal{F}_V^{(2)} = \sum_{i=1}^{v} \gamma_i^{(2)} x_i x_{(i+1 \bmod v)+1} \quad \to \quad \mathbf{F}_V^{(2)} = \begin{pmatrix} 0 & 0 & \gamma_1^{(2)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-2}^{(2)} \\ \gamma_{v-1}^{(2)} & 0 & 0 & \cdots & 0 \\ 0 & \gamma_v^{(2)} & 0 & \cdots & 0 \end{pmatrix}$$

$$\vdots$$

MQ-Sign Central map

$$\mathcal{F}_V^{(1)} = \sum_{i=1}^{v} \gamma_i^{(1)} x_i x_{(i \bmod v)+1} \quad \rightarrow \quad \mathbf{F}_V^{(1)} = \begin{pmatrix} 0 & \gamma_1^{(1)} & 0 & \cdots & 0 \\ 0 & 0 & \gamma_2^{(1)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-1}^{(1)} \\ \gamma_v^{(1)} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

$$\mathcal{F}_V^{(2)} = \sum_{i=1}^{v} \gamma_i^{(2)} x_i x_{(i+1 \bmod v)+1} \quad \rightarrow \quad \mathbf{F}_V^{(2)} = \begin{pmatrix} 0 & 0 & \gamma_1^{(2)} & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{v-2}^{(2)} \\ \gamma_{v-1}^{(2)} & 0 & 0 & \cdots & 0 \\ 0 & \gamma_v^{(2)} & 0 & \cdots & 0 \end{pmatrix}$$

$$\vdots$$

Derive Linear Equations from Key Equation

Recall that the key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P^{(k)}} = \mathbf{S}^\top \mathbf{F^{(k)}} \mathbf{S}$, i.e.

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} = \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right)$$

$$= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\ (\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.$$

From the two upper blocks, as previous, we obtain the equations

$$\begin{aligned} \mathbf{P}_1^{(k)} &= \mathbf{F}_1^{(k)} \quad \text{and} \\ \mathbf{P}_2^{(k)} &= (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}. \end{aligned}$$

- The second is a system of linear equations in the entries of the secret $\mathbf{S_1}$
- Still, not possible to determine them, due to the secret coefficients in $\mathbf{F}_2^{(k)}$

Derive Linear Equations from Key Equation

Recall that the key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P}^{(\mathbf{k})} = \mathbf{S}^\top \mathbf{F}^{(\mathbf{k})} \mathbf{S}$, i.e.

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} = \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right)$$
$$= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\ (\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.$$

From the two upper blocks, as previous, we obtain the equations

$$\begin{aligned} \mathbf{P}_1^{(k)} &= \mathbf{F}_1^{(k)} \quad \text{and} \\ \mathbf{P}_2^{(k)} &= (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}. \end{aligned}$$

- The second is a system of linear equations in the entries of the secret $\mathbf{S}_1$
- Still, not possible to determine them, due to the secret coefficients in $\mathbf{F}_2^{(k)}$

Derive Linear Equations from Key Equation

Recall that the key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P^{(k)}} = \mathbf{S}^\top \mathbf{F^{(k)}} \mathbf{S}$, i.e.

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} = \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right)$$
$$= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\ (\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.$$

From the two upper blocks, as previous, we obtain the equations

$$\begin{aligned} \mathbf{P}_1^{(k)} &= \mathbf{F}_1^{(k)} \quad \text{and} \\ \mathbf{P}_2^{(k)} &= (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}. \end{aligned}$$

- The second is a system of linear equations in the entries of the secret $\mathbf{S_1}$
- Still, not possible to determine them, due to the secret coefficients in $\mathbf{F}_2^{(k)}$

Derive Linear Equations from Key Equation

Recall that the key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P}^{(\mathbf{k})} = \mathbf{S}^\top \mathbf{F}^{(\mathbf{k})} \mathbf{S}$, i.e.

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} = \texttt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right)$$
$$= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \texttt{Upper}\left(\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}\right) \end{pmatrix}.$$

From the two upper blocks, as previous, we obtain the equations

$$\begin{aligned} \mathbf{P}_1^{(k)} &= \mathbf{F}_1^{(k)} \quad \text{and} \\ \mathbf{P}_2^{(k)} &= (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}. \end{aligned}$$

- The second is a system of linear equations in the entries of the secret $\mathbf{S_1}$
- Still, not possible to determine them, due to the secret coefficients in $\mathbf{F}_2^{(k)}$

Derive Linear Equations from Key Equation

Recall that the key equation $\mathcal{P} = \mathcal{F} \circ \mathbf{S}$ translates to the matrix equations $\mathbf{P}^{(\mathbf{k})} = \mathbf{S}^\top \mathbf{F}^{(\mathbf{k})} \mathbf{S}$, i.e.

$$\begin{pmatrix} \mathbf{P}_1^{(k)} & \mathbf{P}_2^{(k)} \\ \mathbf{0} & \mathbf{P}_4^{(k)} \end{pmatrix} = \mathtt{Upper}\left(\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{S}_1^\top & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{F}_1^{(k)} & \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{S}_1 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \right)$$

$$= \begin{pmatrix} \mathbf{F}_1^{(k)} & (\mathbf{F}_1^{(k)} + \mathbf{F}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)} \\ \mathbf{0} & \mathtt{Upper}\ (\mathbf{S}_1^\top \mathbf{F}_1^{(k)} \mathbf{S}_1 + \mathbf{S}_1^\top \mathbf{F}_2^{(k)}) \end{pmatrix}.$$

From the two upper blocks, as previous, we obtain the equations

$$\begin{aligned} \mathbf{P}_1^{(k)} &= \mathbf{F}_1^{(k)} \quad \text{and} \\ \mathbf{P}_2^{(k)} &= (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}. \end{aligned}$$

- The second is a system of linear equations in the entries of the secret $\mathbf{S_1}$
- Still, not possible to determine them, due to the secret coefficients in $\mathbf{F}_2^{(k)}$

In two variants of MQ-Sign, the coefficients in $\mathbf{F}_2^{(k)}$ are chosen sparsely.

This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p'^{(k)}_{1,1} & \cdots & p'^{(k)}_{1,v} \\ \vdots & & \vdots \\ p'^{(k)}_{v,1} & \cdots & p'^{(k)}_{v,v} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\textbf{secret, but known structure}}$$

Efficient Key-Recovery

In two variants of MQ-Sign, the coefficients in $\mathbf{F}_2^{(k)}$ are chosen sparsely.

This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p_{1,1}^{,(k)} & \cdots & p_{1,v}^{,(k)} \\ \vdots & & \vdots \\ p_{v,1}^{,(k)} & \cdots & p_{v,v}^{,(k)} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\textbf{secret, but known structure}}$$

Efficient Key-Recovery

In two variants of MQ-Sign, the coefficients in $\mathbf{F}_2^{(\mathbf{k})}$ are chosen sparsely.

This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{public} = \underbrace{\begin{pmatrix} p'^{(k)}_{1,1} & \cdots & p'^{(k)}_{1,v} \\ \vdots & & \vdots \\ p'^{(k)}_{v,1} & \cdots & p'^{(k)}_{v,v} \end{pmatrix}}_{public} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{secret} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\textbf{secret, but known structure}}$$

Efficient Key-Recovery

In two variants of MQ-Sign, the coefficients in $\mathbf{F}_2^{(\mathbf{k})}$ are chosen sparsely.

This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p^{(k)}_{1,v+1} & \cdots & p^{(k)}_{1,v+m} \\ \vdots & & \vdots \\ p^{(k)}_{v,v+1} & \cdots & p^{(k)}_{v,v+m} \end{pmatrix}}_{public} = \underbrace{\begin{pmatrix} p^{,(k)}_{1,1} & \cdots & p^{,(k)}_{1,v} \\ \vdots & & \vdots \\ p^{,(k)}_{v,1} & \cdots & p^{,(k)}_{v,v} \end{pmatrix}}_{public} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{secret} + \underbrace{\begin{pmatrix} 0 & \gamma^{(k)}_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma^{(k)}_{m-1} \\ \gamma^{(k)}_m & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\textbf{secret, but known structure}}$$

Efficient Key-Recovery

In two variants of MQ-Sign, the coefficients in $\mathbf{F}_2^{(k)}$ are chosen sparsely.

This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p^{(k)}_{1,v+1} & \cdots & p^{(k)}_{1,v+m} \\ \vdots & & \vdots \\ p^{(k)}_{v,v+1} & \cdots & p^{(k)}_{v,v+m} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p'^{(k)}_{1,1} & \cdots & p'^{(k)}_{1,v} \\ \vdots & & \vdots \\ p'^{(k)}_{v,1} & \cdots & p'^{(k)}_{v,v} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

- Collect linear equations for all $k \in \{1, \ldots, m\}$ polynomials.
- Obtain system of $mv(m-1)$ equations in vm variables (can be divided into subsystems).
- Once $\mathbf{S}$ is known, the central polynomials can efficiently be found.

The constructed key is actually not equivalent to a UOV key, it is weaker!

Efficient Key-Recovery

In two variants of MQ-Sign, the coefficients in $\mathbf{F}_2^{(\mathbf{k})}$ are chosen sparsely.

This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p_{1,1}^{,(k)} & \cdots & p_{1,v}^{,(k)} \\ \vdots & & \vdots \\ p_{v,1}^{,(k)} & \cdots & p_{v,v}^{,(k)} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

- Collect linear equations for all $k \in \{1, \ldots, m\}$ polynomials.
- Obtain system of $mv(m-1)$ equations in vm variables (can be divided into subsystems).
- Once $\mathbf{S}$ is known, the central polynomials can efficiently be found.

The constructed key is actually not equivalent to a UOV key, it is weaker!

Efficient Key-Recovery

In two variants of MQ-Sign, the coefficients in $\mathbf{F}_2^{(\mathbf{k})}$ are chosen sparsely.

This removes unknown variables from the system

$$\mathbf{P}_2^{(k)} = (\mathbf{P}_1^{(k)} + \mathbf{P}_1^{(k)\top})\mathbf{S}_1 + \mathbf{F}_2^{(k)}.$$

$$\underbrace{\begin{pmatrix} p_{1,v+1}^{(k)} & \cdots & p_{1,v+m}^{(k)} \\ \vdots & & \vdots \\ p_{v,v+1}^{(k)} & \cdots & p_{v,v+m}^{(k)} \end{pmatrix}}_{\textit{public}} = \underbrace{\begin{pmatrix} p_{1,1}^{\prime(k)} & \cdots & p_{1,v}^{\prime(k)} \\ \vdots & & \vdots \\ p_{v,1}^{\prime(k)} & \cdots & p_{v,v}^{\prime(k)} \end{pmatrix}}_{\textit{public}} \underbrace{\begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{v1} & \cdots & s_{vm} \end{pmatrix}}_{\textit{secret}} + \underbrace{\begin{pmatrix} 0 & \gamma_1^{(k)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \gamma_{m-1}^{(k)} \\ \gamma_m^{(k)} & 0 & \cdots & 0 \\ \vdots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}}_{\text{secret, but known structure}}$$

- Collect linear equations for all $k \in \{1, \ldots, m\}$ polynomials.
- Obtain system of $mv(m-1)$ equations in vm variables (can be divided into subsystems).
- Once $\mathbf{S}$ is known, the central polynomials can efficiently be found.

The constructed key is actually not equivalent to a UOV key, it is weaker!