Cryptanalysis of Enhanced TTS, STS and all its Variants

or: How to Solve Structured Systems of Non-Linear Equations

Enrico Thomae and Christopher Wolf

Ifrane, 11.07.2012

Horst Görtz Institut für IT-Sicherheit

RUHR-UNIVERSITÄT BOCHUM

Contribution

- general view on algebraic key recovery attacks on $\mathcal{MQ}$-schemes, which covers and extends:
  - UOV-Reconciliation attack [BBD09]
  - Rainbow Band Separation attack [DYCCC08]
  - MinRank and HighRank attacks

Contribution

- general view on algebraic key recovery attacks on $\mathcal{MQ}$-schemes, which covers and extends:
  - UOV-Reconciliation attack [BBD09]
  - Rainbow Band Separation attack [DYCCC08]
  - MinRank and HighRank attacks
- uses generalization of equivalent keys - called *good keys*

Contribution

- general view on algebraic key recovery attacks on $\mathcal{MQ}$-schemes, which covers and extends:
  - UOV-Reconciliation attack [BBD09]
  - Rainbow Band Separation attack [DYCCC08]
  - MinRank and HighRank attacks
- uses generalization of equivalent keys - called *good keys*
- applies to: Unbalanced Oil and Vinegar
  - Rainbow, enhTTS
  - enhSTS, STS based on prime factorization (SCC'12)
  - MQQ-Enc (SCC'12), MQQ-Sig
  - MFE based on Diophantine equations

Contribution

- general view on algebraic key recovery attacks on $\mathcal{MQ}$-schemes, which covers and extends:
  - UOV-Reconciliation attack [BBD09]
  - Rainbow Band Separation attack [DYCCC08]
  - MinRank and HighRank attacks
- uses generalization of equivalent keys - called *good keys*
- applies to: Unbalanced Oil and Vinegar
  - Rainbow, enhTTS
  - enhSTS, STS based on prime factorization (SCC'12)
  - MQQ-Enc (SCC'12), MQQ-Sig
  - MFE based on Diophantine equations

full version on Eprint: *A Generalization of the Rainbow Band Separation Attack and its Applications to Multivariate Schemes* by Enrico Thomae (updated soon)

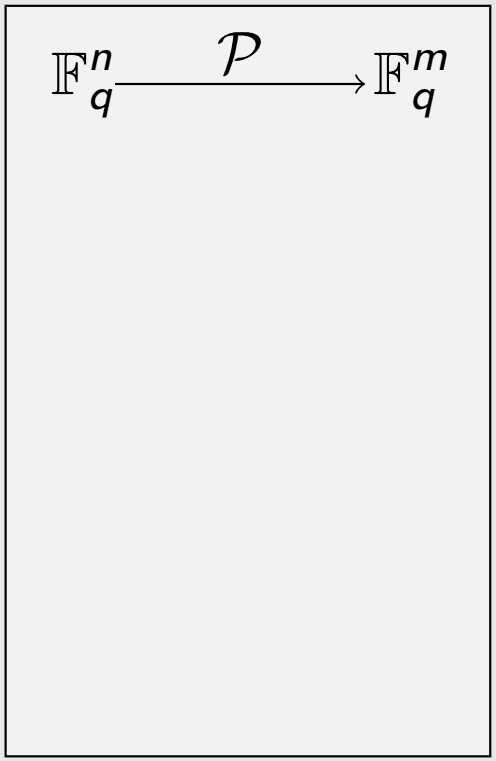
Multivariate Quadratic ($\mathcal{MQ}$) schemes

public key:

$$\mathcal{P} = \begin{pmatrix} p^{(1)}(x_1, \ldots, x_n) \\ \vdots \\ p^{(m)}(x_1, \ldots, x_n) \end{pmatrix}$$

$$p^{(k)} := \sum_{1 \le i \le j \le n} \widetilde{\gamma}_{ij}^{(k)} x_i x_j$$

$$= \mathbf{x}^\intercal \mathfrak{P}^{(k)} \mathbf{x}$$



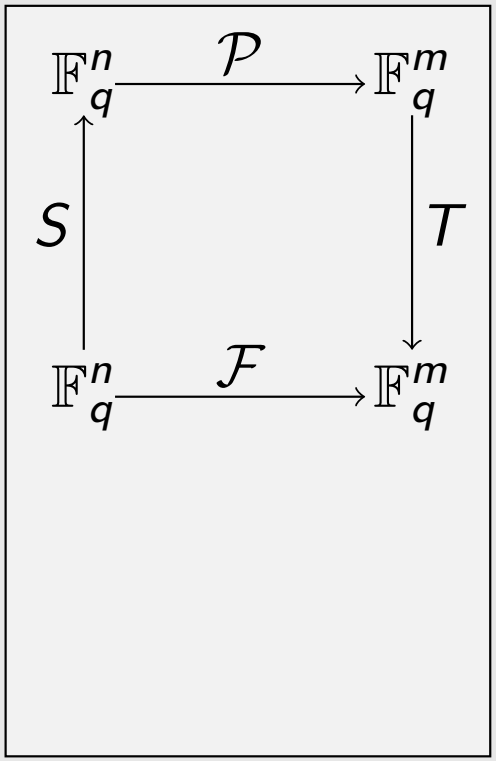
Multivariate Quadratic ($\mathcal{MQ}$) schemes

secret key:

$$S = \begin{pmatrix} s_{1,1} & \cdots & s_{1,n} \\ \vdots & & \vdots \\ s_{n,1} & \cdots & s_{n,n} \end{pmatrix}$$

$$T = \begin{pmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{pmatrix}$$

$$\mathcal{F} = \begin{pmatrix} f^{(1)}(u_1, \ldots, u_n) \\ \vdots \\ f^{(m)}(u_1, \ldots, u_n) \end{pmatrix}, \quad f^{(k)} := \sum_{1 \le i \le j \le n} \gamma_{ij}^{(k)} u_i u_j = \mathbf{u}^{\mathsf{T}} \mathfrak{F}^{(k)} \mathbf{u}$$



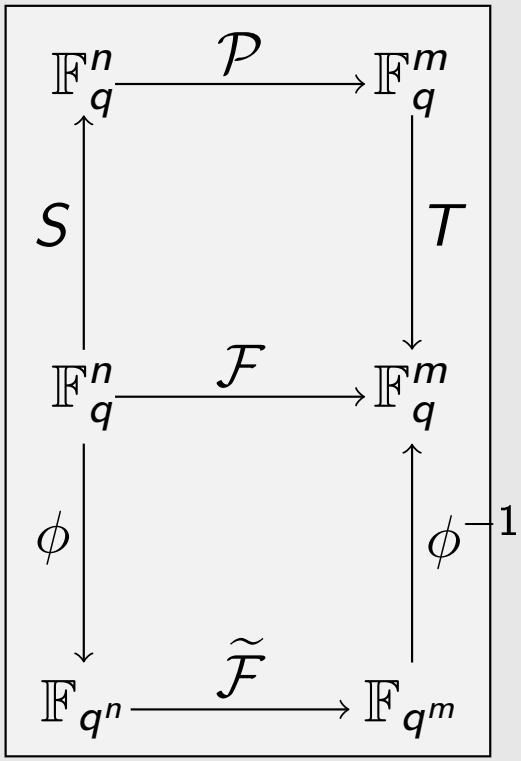
Multivariate Quadratic ($\mathcal{MQ}$) schemes

secret key:

$$S = \begin{pmatrix} s_{1,1} & \cdots & s_{1,n} \\ \vdots & & \vdots \\ s_{n,1} & \cdots & s_{n,n} \end{pmatrix}$$

$$T = \begin{pmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{pmatrix}$$

$$\widetilde{\mathcal{F}} = \sum_{1 \le i \le j \le n} \gamma_{ij} X^{q^i + q^j}$$



Algebraic Key Recovery Attacks

Our aim: Use structure of $\mathcal{F}$ to recover S and T and thereby $\mathcal{F}$ itself.

Algebraic Key Recovery Attacks

Our aim: Use structure of $\mathcal{F}$ to recover S and T and thereby $\mathcal{F}$ itself.

$$\begin{array}{ccccccc} \mathcal{F} & = & T & \circ & \mathcal{P} & \circ & S \\ \mathbf{u}^\mathsf{T}\mathfrak{F}^{(k)}\mathbf{u} & = & \mathbf{u}^\mathsf{T}\left(\sum_{i=1}^{m} t_{ki} S^\mathsf{T}\mathfrak{P}^{(k)} S\right)\mathbf{u} & \leftarrow & \mathbf{u}^\mathsf{T} S^\mathsf{T}\mathfrak{P}^{(k)} S\mathbf{u} & \leftarrow & S\mathbf{u} = \mathbf{x} \end{array}$$

Algebraic Key Recovery Attacks

Our aim: Use structure of $\mathcal{F}$ to recover S and T and thereby $\mathcal{F}$ itself.

$$\begin{array}{ccccccc} \mathcal{F} & = & T & \circ & \mathcal{P} & \circ & S \\ \mathbf{u}^{\mathsf{T}}\mathfrak{F}^{(k)}\mathbf{u} & = & \mathbf{u}^{\mathsf{T}}\left(\sum_{i=1}^{m} t_{ki} S^{\mathsf{T}}\mathfrak{P}^{(k)} S\right)\mathbf{u} & \leftarrow & \mathbf{u}^{\mathsf{T}} S^{\mathsf{T}}\mathfrak{P}^{(k)} S\mathbf{u} & \leftarrow & S\mathbf{u} = \mathbf{x} \end{array}$$

$$\Rightarrow \quad \boxed{\gamma_{ij}^{(k)} = \sum_{x=1}^{m}\sum_{y=1}^{n}\sum_{z=1}^{n} \alpha_{xyz}\, t_{kx}\, s_{yi}\, s_{zj}}$$

Unbalanced Oil and Vinegar

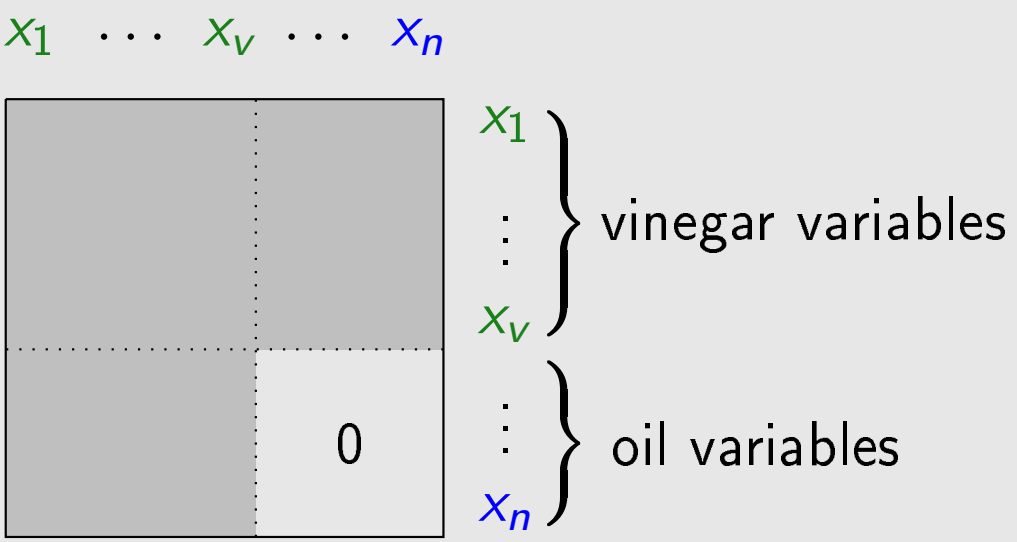
$$n := v + m, V := \{1, \ldots, v\}, O := \{v + 1, \ldots, n\}$$

Unbalanced Oil and Vinegar

$$n := v + m, V := \{1, \ldots, v\}, O := \{v+1, \ldots, n\}$$

$$f^{(k)}(u_1, \ldots, u_n) := \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} u_i u_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} u_i u_j$$

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



Unbalanced Oil and Vinegar

$$n := v + m, V := \{1, \ldots, v\}, O := \{v+1, \ldots, n\}$$

$$f^{(k)}(u_1, \ldots, u_n) := \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} u_i u_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} u_i u_j$$

$$\begin{aligned} \#\text{ cubic equ} &: m \cdot \tfrac{m(m+1)}{2} \\ \#\text{ variables} &: m^2 + n^2 \end{aligned}$$

$n = 84, m = 28$:

$$\begin{aligned} \#\text{ cubic equ} &: 11368 \\ \#\text{ variables} &: 7840 \end{aligned}$$

Equivalent Keys

Definition *(Equivalent Key)*

Let S, T and S', T' be regular matrices and

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

We call S' and T' equivalent to S and T, if $\mathcal{F}'$ and $\mathcal{F}$ share the same structure, i.e. contain the same systematic zero coefficients.

Equivalent Keys

Definition *(Equivalent Key)*

Let S, T and S', T' be regular matrices and

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

We call S' and T' equivalent to S and T, if $\mathcal{F}'$ and $\mathcal{F}$ share the same structure, i.e. contain the same systematic zero coefficients.

How do we find them?

Equivalent Keys

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

Equivalent Keys

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

$$\Leftrightarrow \mathcal{P} = T^{-1} \circ \mathcal{F} \circ S^{-1}$$

Equivalent Keys

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

$$\Leftrightarrow \mathcal{P} = T^{-1} \circ \mathcal{F} \circ S^{-1}$$

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

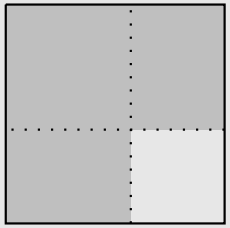
for some linear transformations Σ and Ω.

Equivalent Keys for UOV

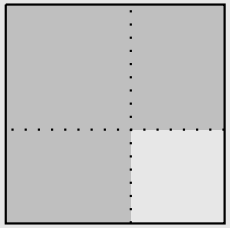
Back to UOV:

- obviously Σ can be chosen arbitrarily, e.g. $\Sigma = T^{-1}$

  $\Rightarrow T' = I$



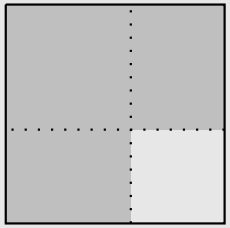
Equivalent Keys for UOV



Back to UOV:

- obviously Σ can be chosen arbitrarily, e.g. $\Sigma = T^{-1}$
  $\Rightarrow T' = I$
- $f^{(k)}(u_1, \ldots, u_n) := \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} u_i u_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} u_i u_j$

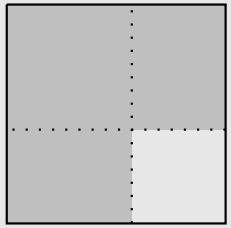
Equivalent Keys for UOV



Back to UOV:

- obviously Σ can be chosen arbitrarily, e.g. $\Sigma = T^{-1}$
  $\Rightarrow T' = I$
- $f^{(k)}(u_1, \ldots, u_n) := \boxed{u = \Omega w}_{i \in} u_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} u_i u_j$

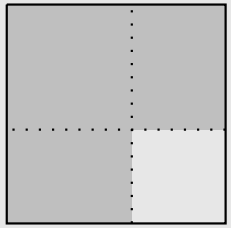
Equivalent Keys for UOV



Back to UOV:

- obviously Σ can be chosen arbitrarily, e.g. $\Sigma = T^{-1}$
  $\Rightarrow T' = I$
- $$f^{(k)}(w_1, \ldots, w_n) := \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} \sum_{r=1}^{n} \Omega_{ir} w_r \sum_{s=1}^{n} \Omega_{js} w_s + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} \sum_{r=1}^{n} \Omega_{ir} w_r \sum_{s=1}^{n} \Omega_{js} w_s$$

Equivalent Keys for UOV

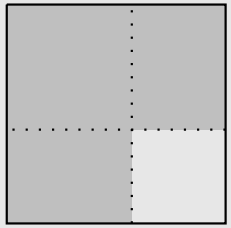


Back to UOV:

- obviously Σ can be chosen arbitrarily, e.g. $\Sigma = T^{-1}$
  $\Rightarrow T' = I$
- $$f^{(k)}(w_1, \ldots, w_n) := \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} \sum_{r=1}^{n} \Omega_{ir} w_r \sum_{s=1}^{n} \Omega_{js} w_s + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} \sum_{r=1}^{n} \Omega_{ir} w_r \sum_{s=1}^{n} \Omega_{js} w_s$$

$$\Omega = \begin{array}{|c|c|} \hline \Omega_1 & 0 \\ \hline \Omega_2 & \Omega_3 \\ \hline \end{array}$$

Equivalent Keys for UOV



Back to UOV:

- obviously Σ can be chosen arbitrarily, e.g. $\Sigma = T^{-1}$
  $\Rightarrow T' = I$
- $$f^{(k)}(w_1, \ldots, w_n) := \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} \sum_{r=1}^{n} \Omega_{ir} w_r \sum_{s=1}^{n} \Omega_{js} w_s + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} \sum_{r=1}^{n} \Omega_{ir} w_r \sum_{s=1}^{n} \Omega_{js} w_s$$

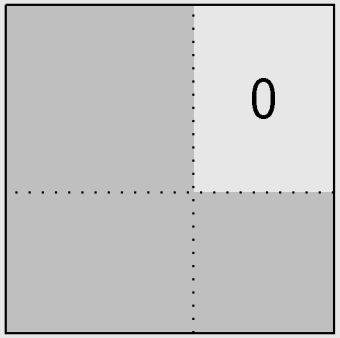
$$\Omega \cdot S = \begin{array}{|c|c|}\hline \Omega_1 & 0 \\ \hline \Omega_2 & \Omega_3 \\ \hline \end{array} \cdot \begin{array}{|c|c|}\hline S_1 & S_2 \\ \hline S_3 & S_4 \\ \hline \end{array}$$

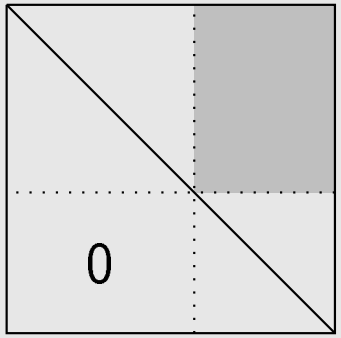
Set: $\Omega_1 S_1 = I$

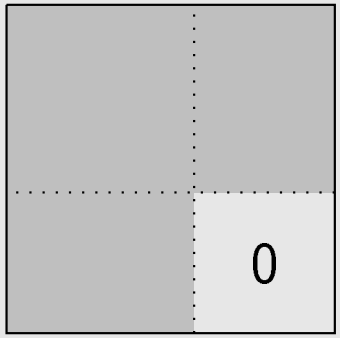
$\Omega_2 S_1 + \Omega_3 S_3 = 0$

$\Omega_2 S_2 + \Omega_3 S_4 = I$

Equivalent Keys for UOV

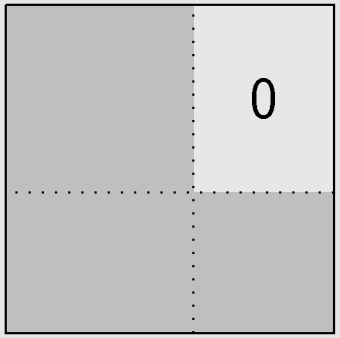
$\Omega =$ 

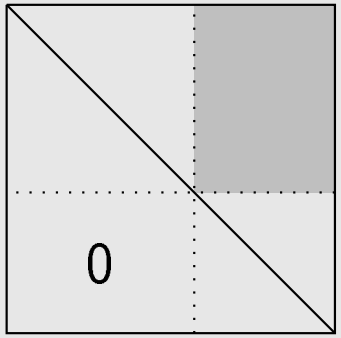
$S' =$ 

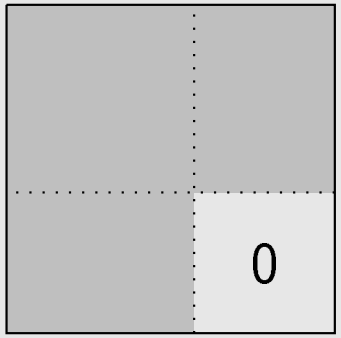


$\mathfrak{F}^{(1)}, \ldots, \mathfrak{F}^{(m)}$

Equivalent Keys for UOV

$\Omega =$ 

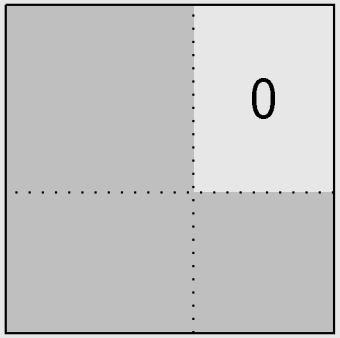
$S' =$ 

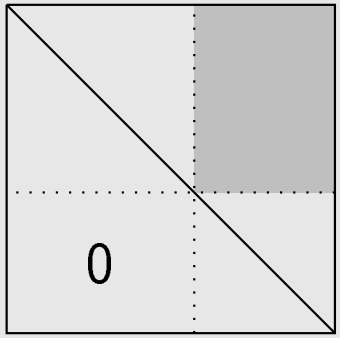


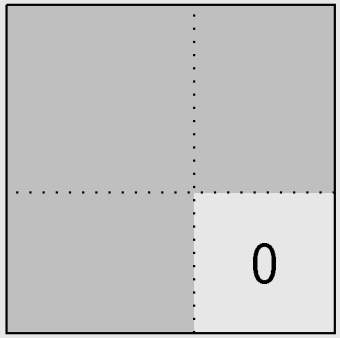
$\mathcal{F}^{(1)}$ $\mathcal{F}^{(m)}$

# quadr equ	:	$m \cdot \frac{m(m+1)}{2}$
# variables	:	mv
$n = 84, m = 28$:		
# quadr equ	:	11368
# variables	:	1568

Equivalent Keys for UOV

$\Omega =$ 

$S' =$ 

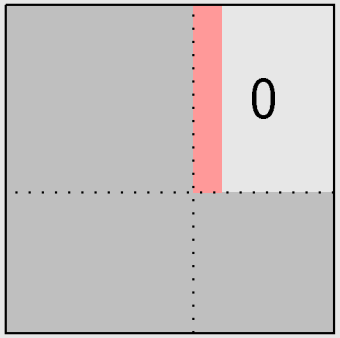


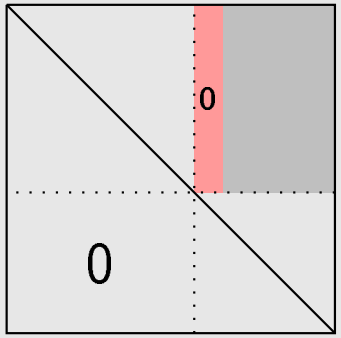
$\mathfrak{F}^{(1)}$ $\mathfrak{F}^{(m)}$

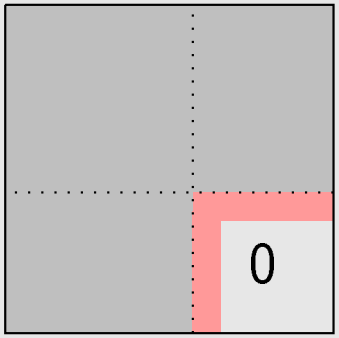
# quadr equ	:	$m \cdot \frac{m(m+1)}{2}$
# variables	:	mv
$n = 84, m = 28$:		
# quadr equ	:	11368
# variables	:	1568

What if we do not preserve all the structure in $\mathfrak{F}$?

Good Keys for UOV

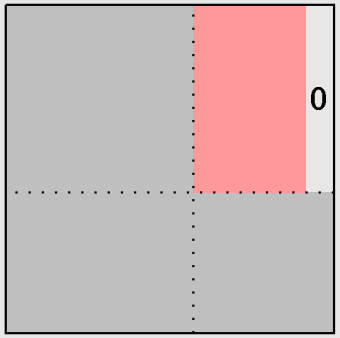
$\Omega =$ 

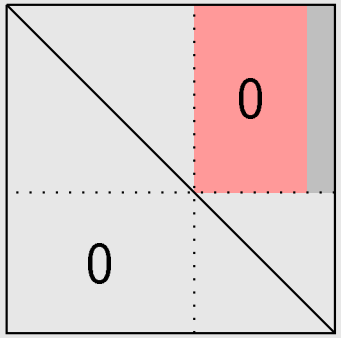
$S' =$ 

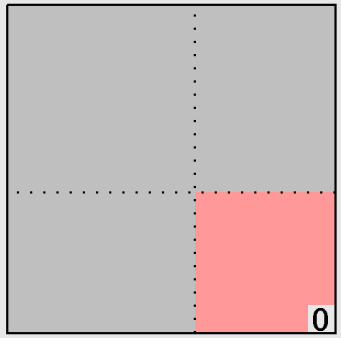


$\mathfrak{F}^{(1)}, \ldots, \mathfrak{F}^{(m)}$

Good Keys for UOV

$\Omega =$ 

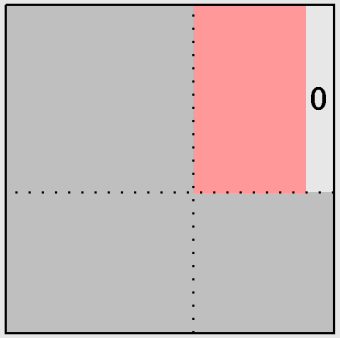
$S' =$ 

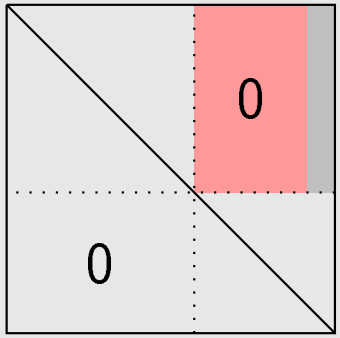


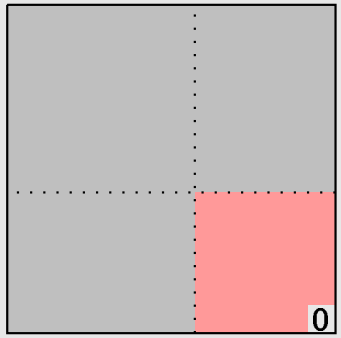
$\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(m)}$

# quadr equ	:	m
# variables	:	v
$n = 84, m = 28$:		
# quadr equ	:	28
# variables	:	56

Good Keys for UOV

$\Omega =$ 

$S' =$ 



$\mathcal{F}^{(1)}, \ldots, \mathcal{F}^{(m)}$

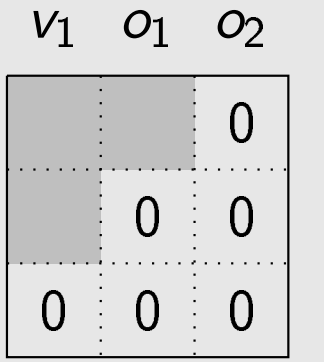
$$\begin{aligned} \#\text{ quadr equ} &: \binom{k+1}{2} m \\ \#\text{ variables} &: kv \end{aligned}$$

$n = 84, m = 28, k = 3$:

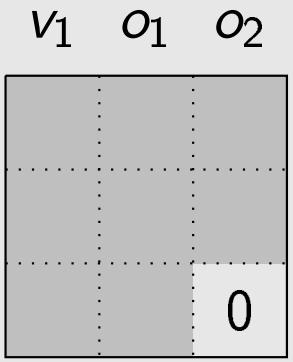
$$\begin{aligned} \#\text{ quadr equ} &: 168 \\ \#\text{ variables} &: 168 \end{aligned}$$

Known as Reconciliation Attack

Equivalent Keys for Rainbow

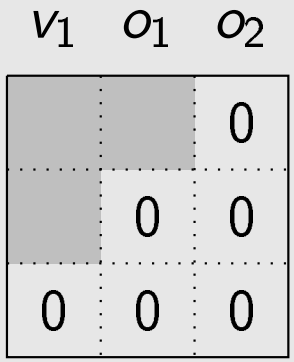


$\mathfrak{F}^{(1)}, \ldots, \mathfrak{F}^{(o_1)}$

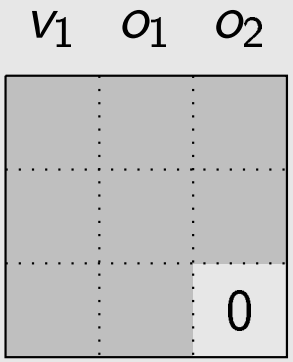


$\mathfrak{F}^{(o_1+1)}, \ldots, \mathfrak{F}^{(o_1+o_2)}$

Equivalent Keys for Rainbow

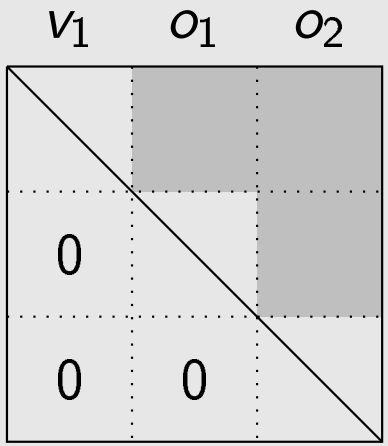


$\mathfrak{F}^{(1)}, \ldots, \mathfrak{F}^{(o_1)}$

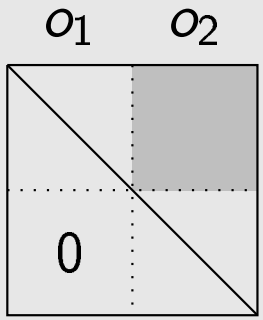


$\mathfrak{F}^{(o_1+1)}, \ldots, \mathfrak{F}^{(o_1+o_2)}$

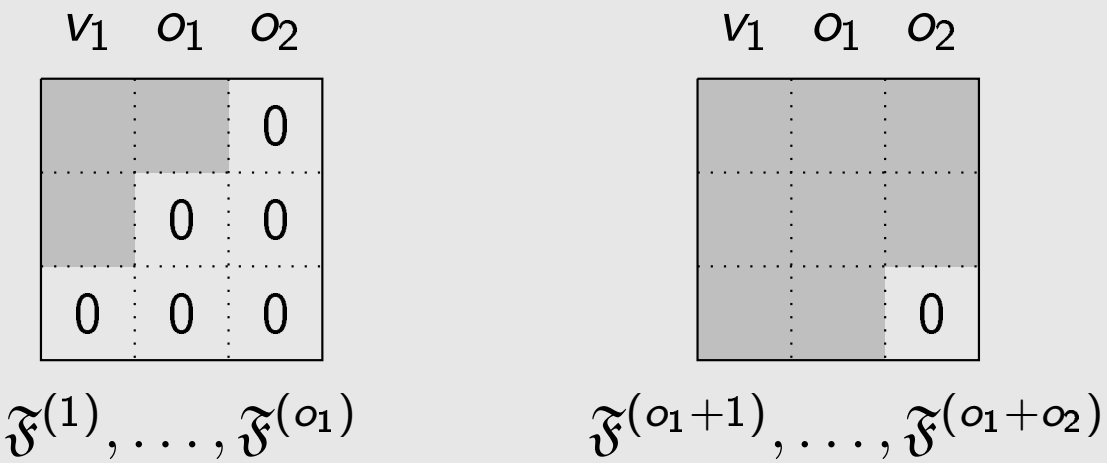
$S' =$



$T' =$



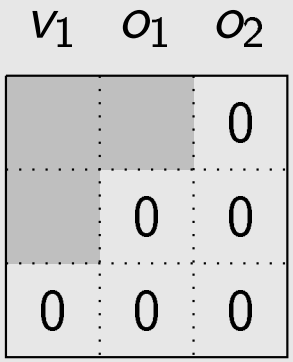
Equivalent Keys for Rainbow



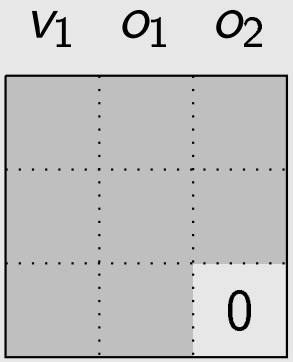
$v_1 = 18, o_1 = 12, o_2 = 12$:

# cub equ	:	7128
# variables	:	720

Good Keys for Rainbow

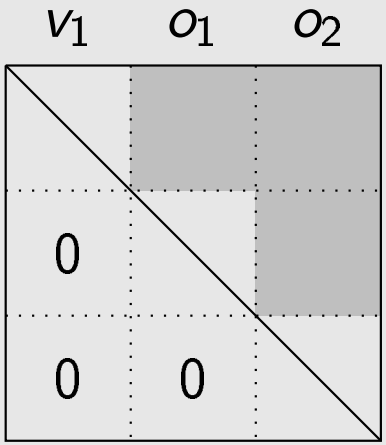


$\mathfrak{F}^{(1)}$

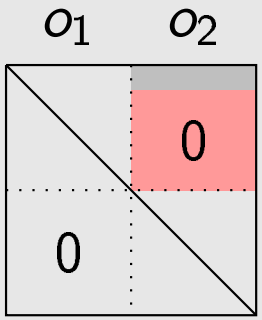


$\mathfrak{F}^{(2)}, \ldots, \mathfrak{F}^{(o_1+o_2)}$

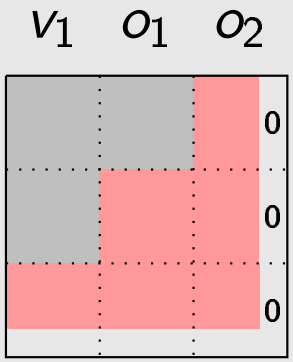
$S' =$



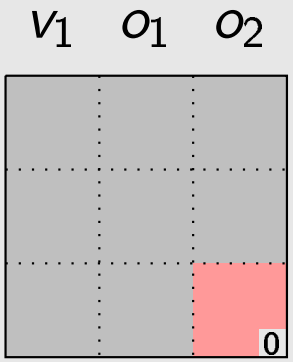
$T' =$



Good Keys for Rainbow

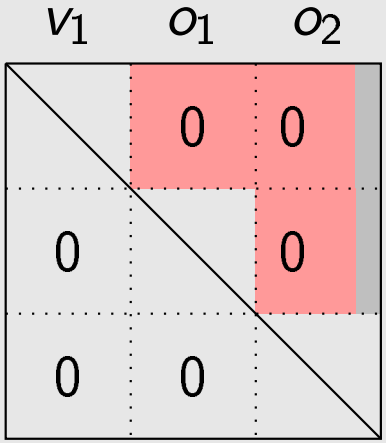


$\mathfrak{F}^{(1)}$

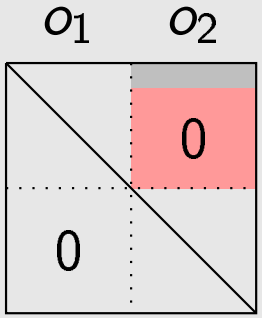


$\mathfrak{F}^{(2)}, \ldots, \mathfrak{F}^{(o_1+o_2)}$

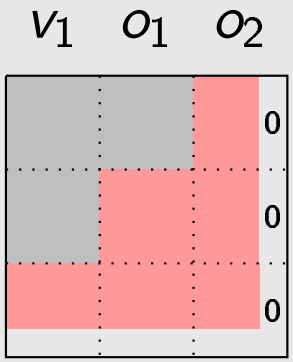
$S' =$



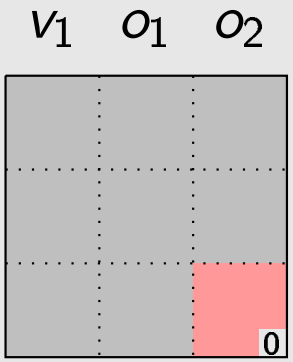
$T' =$



Good Keys for Rainbow



$\mathfrak{F}^{(1)}$



$\mathfrak{F}^{(2)}, \ldots, \mathfrak{F}^{(o_1+o_2)}$

$v_1 = 18, o_1 = 12, o_2 = 12$:

# quad equ	:	23
# bilinear equ	:	41
# cub equ	:	1
# variables	:	42

Known as Rainbow Band Separation Attack [DYC+08]

STS based schemes

$$
\text{Step } 1 \begin{cases} f^{(1)}(u_1, \ldots, u_r) \\ \vdots \\ f^{(r)}(u_1, \ldots, u_r) \end{cases}
$$

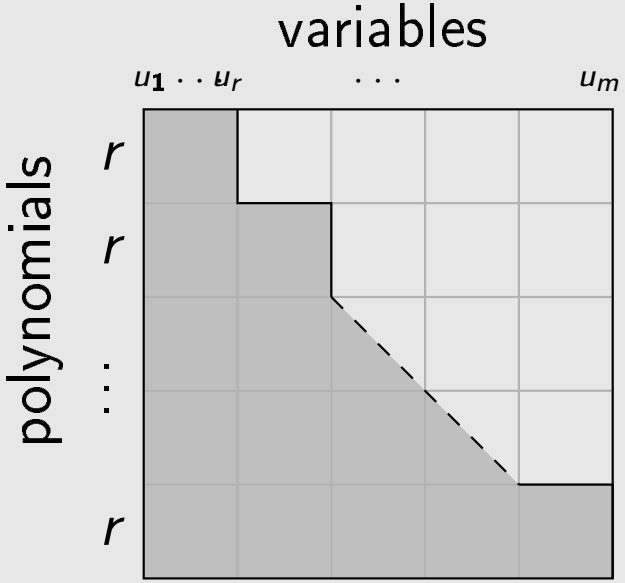
$$
\vdots
$$

$$
\text{Step } i \begin{cases} f^{((i-1)r+1)}(u_1, \ldots, u_{ir}) \\ \vdots \\ f^{(ir)}(u_1, \ldots, u_{ir}) \end{cases}
$$

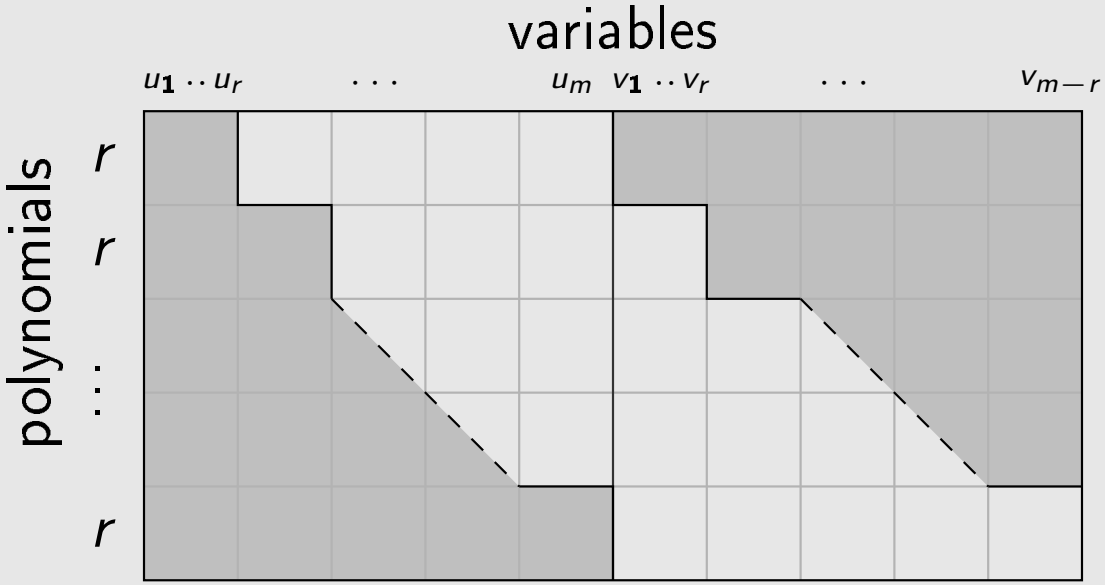
$$
\vdots
$$

$$
\text{Step } L \begin{cases} f^{((L-1)r+1)}(u_1, \ldots, u_m) \\ \vdots \\ f^{(m)}(u_1, \ldots, u_m) \end{cases}
$$

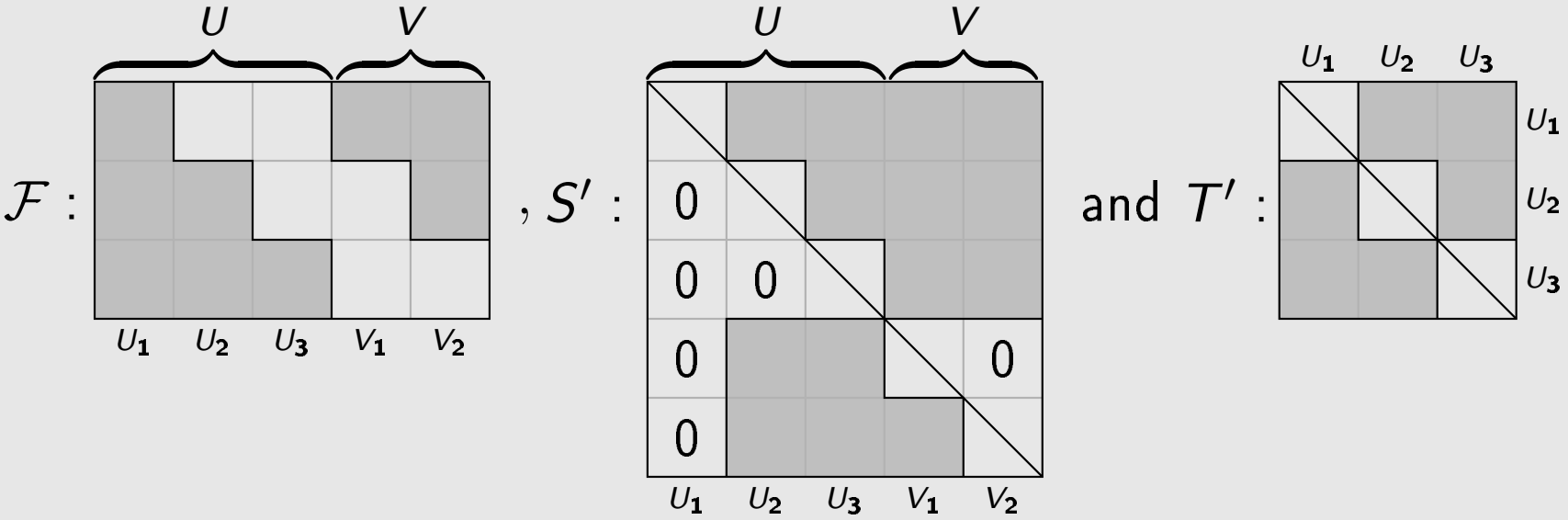
resp.



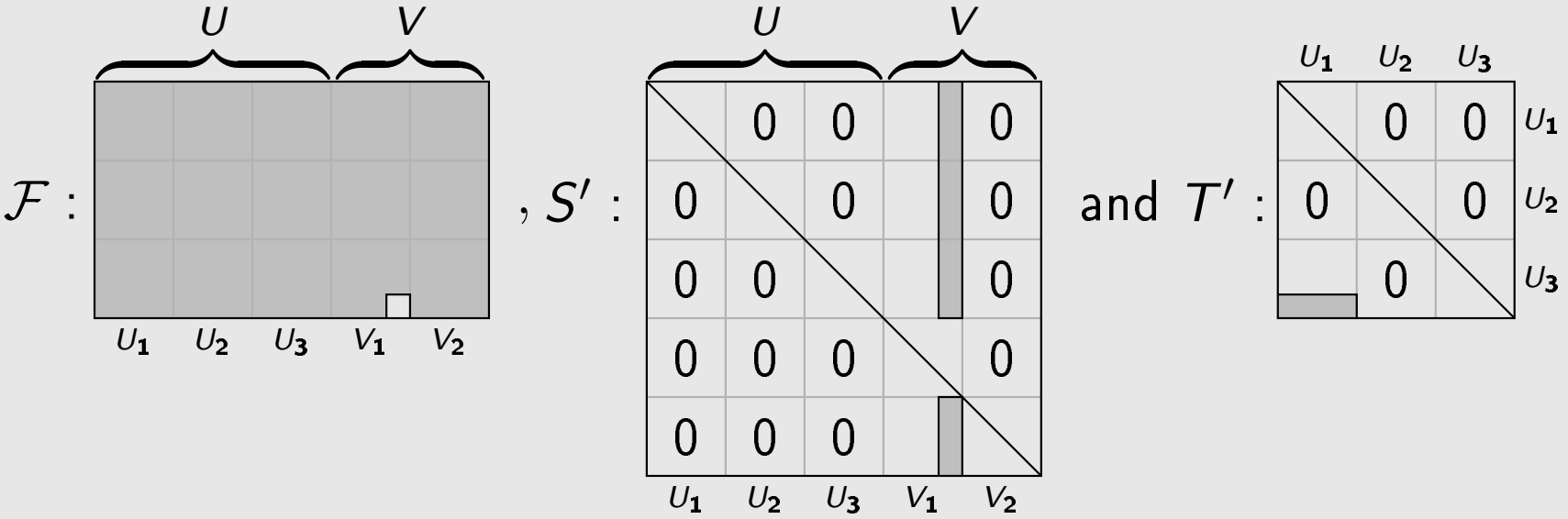
enhanced STS based schemes



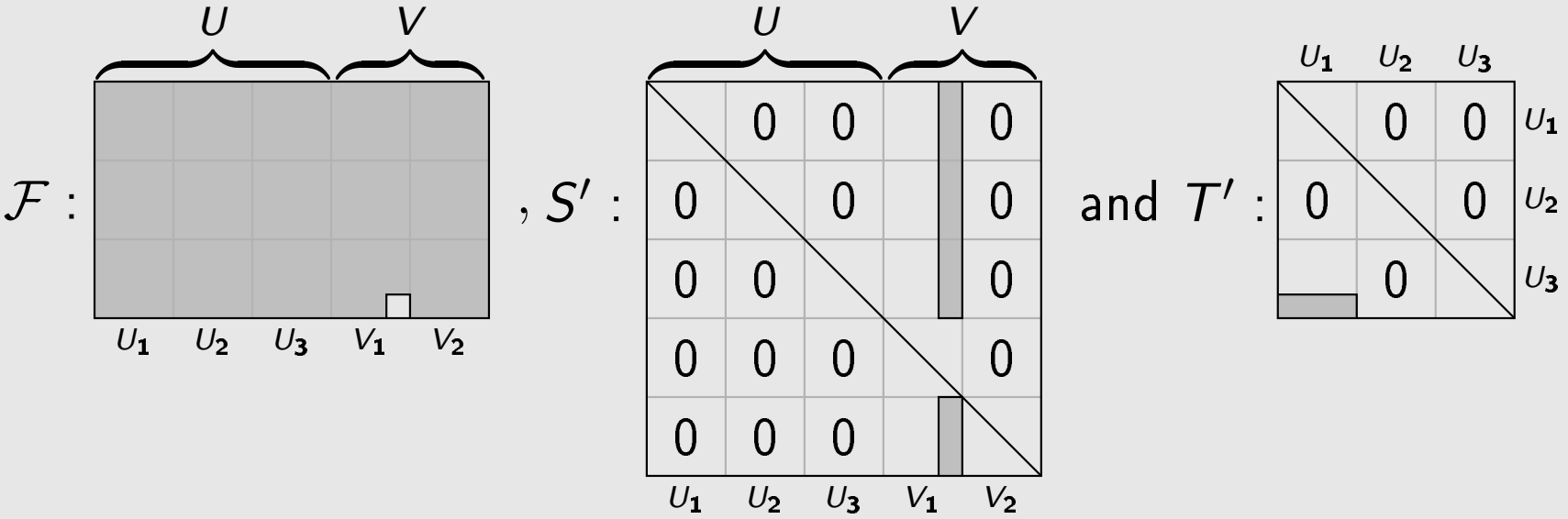
Good Keys for enhanced STS



Good Keys for enhanced STS



Good Keys for enhanced STS



$$\begin{aligned} \#\text{ bihom equ} &: |U| + |V| - 1 \\ \#\text{ cub equ} &: 1 \\ \#\text{ variables} &: |U| + |V| \end{aligned}$$

$$q\binom{2m-1}{|U_1|}^{2.8}$$

Where do we take it from here?

- secure encryption based on $\mathcal{MQ}$ seems to be very difficult even for a generalization of LWE (c.f. PKC [Herold12])
- secure signatures based on $\mathcal{MQ}$ are possible
  c.f. Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials (Crypto [SSH11])

Thank you! Any questions?