KOOKMIN UNIVERSITY NIMS National Institute for Mathematical Sciences | South Korea

SICADA SIde Channel Analysis Design Academy

CHES 2018

Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations

Aesun Park[1] , Kyung-Ah Shim[2]*, Namhun Koo[2], and Dong-Guk Han[1]

[1]Department of Financial Information Security, Kookmin University, Seoul, Republic of Korea
[2]Division of Mathematical Modeling, National Institute for Mathematical Sciences, Daejeon, Republic of Korea

11. Sep. 2018

UOV Variants Signature schemes

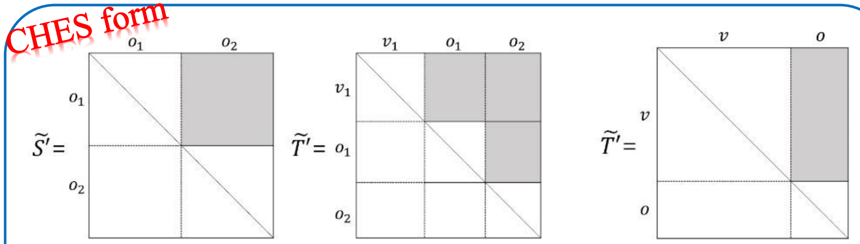
- EUROCRYPT — 1999 UOV
  - Improving efficiency and reducing the key sizes
- ACNS — 2005 (General) Rainbow : a layered MQ-signature scheme based on UOV
- SAC — 2006 efficient software implementations

Efficient Implementations in HW/SW

Reduction in the size of the public key

- CHES, Czypek et al. — 2012 (Efficient) Rainbow & UOV

CHES form



Rainbow   UOV

- ✓ reducing the key space and runtime
- ✓ removing the constant part
- ✓ Appling linear maps like the picture

- INDOCRYPT, Beullens et al. — 2017 Lifted UOV
  - For smaller UOV public keys
  - It uses the linear map T of CHES form

SCA on UOV Variants Signature schemes

Paul Kocher — 1996 **Timing** Attacks

1998 Simple **Power** Analysis

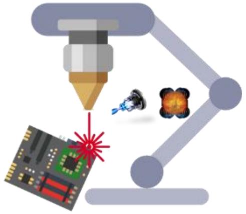
Differential Power Analysis

2004 Correlation Power Analysis

Implementations of post-quantum algorithms are vulnerable to PA

The studies of PA against UOV variants lack.

The Computer Journal
Yi et al. — 2017 **Semi-invasive** Attack on enTTS



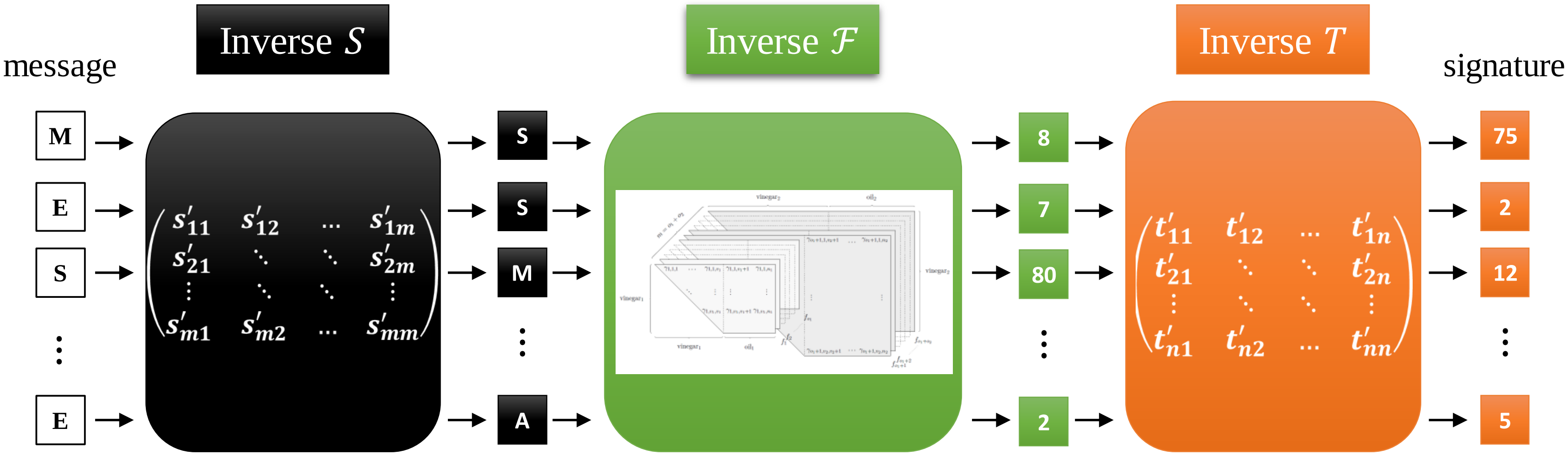
Fault Injection

CHES — 2018 **Ours**

Non-invasive Attacks on Rainbow and UOV

Signature generation on Rainbow

- Secret maps : $S, \mathcal{F}, T$



- Linear map S
- Matrix-vector product **over a field**

- Random values
- Solving the linear equations

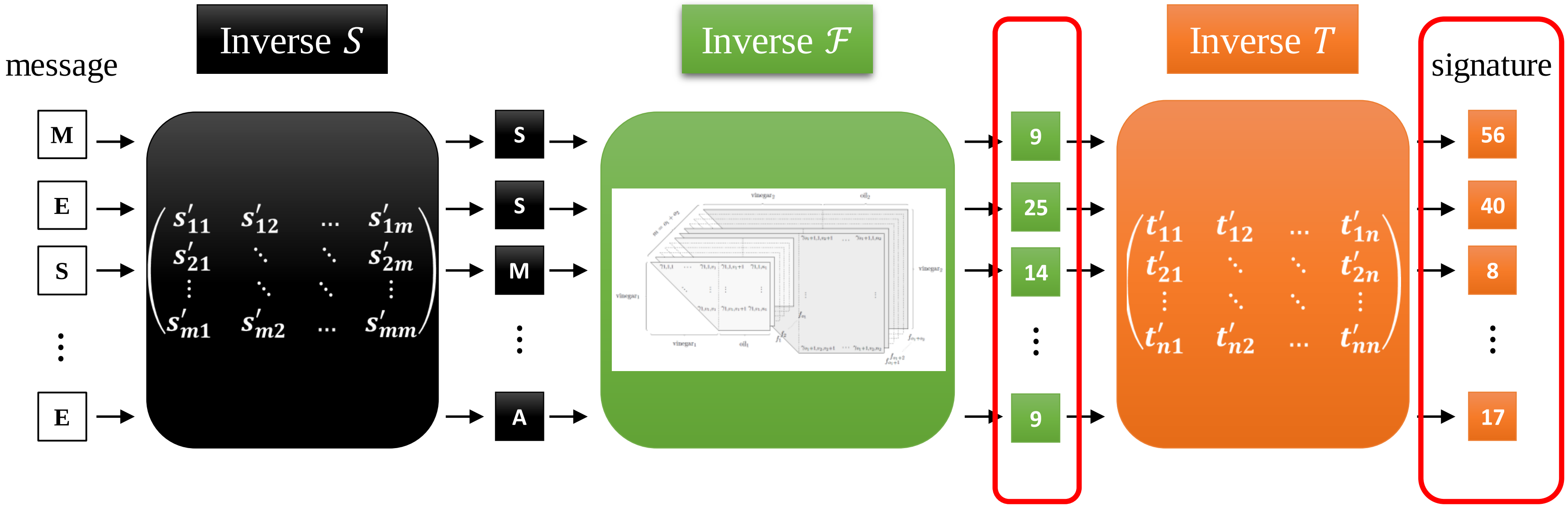
- Linear map T
- Matrix-vector product **over a field**

Basic operations

Field multiplications & additions

Signature generation on Rainbow

- Rainbow generates different signatures for the same message.



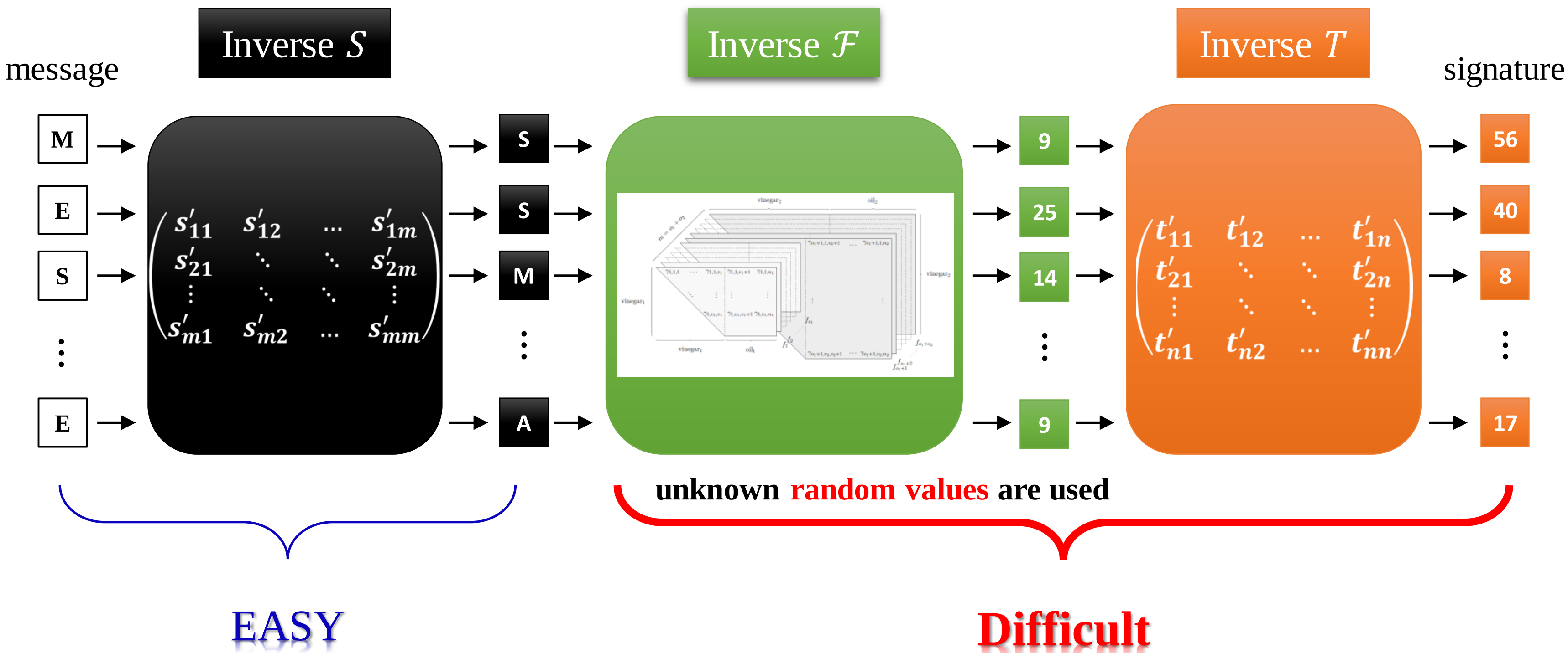
- Linear map S
- Matrix-vector product **over a field**
- **Random values**
- Solving the equations
- Linear map T
- Matrix-vector product **over a field**

Same Input (message) ➔ Different Output (signature)

Signature generation on Rainbow

❖ Applicability of Power Analysis

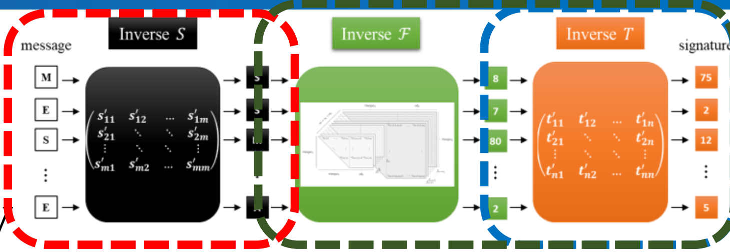
- ➢ Power analysis uses the position where the **fixed secret** value and **the random public** value are computed.

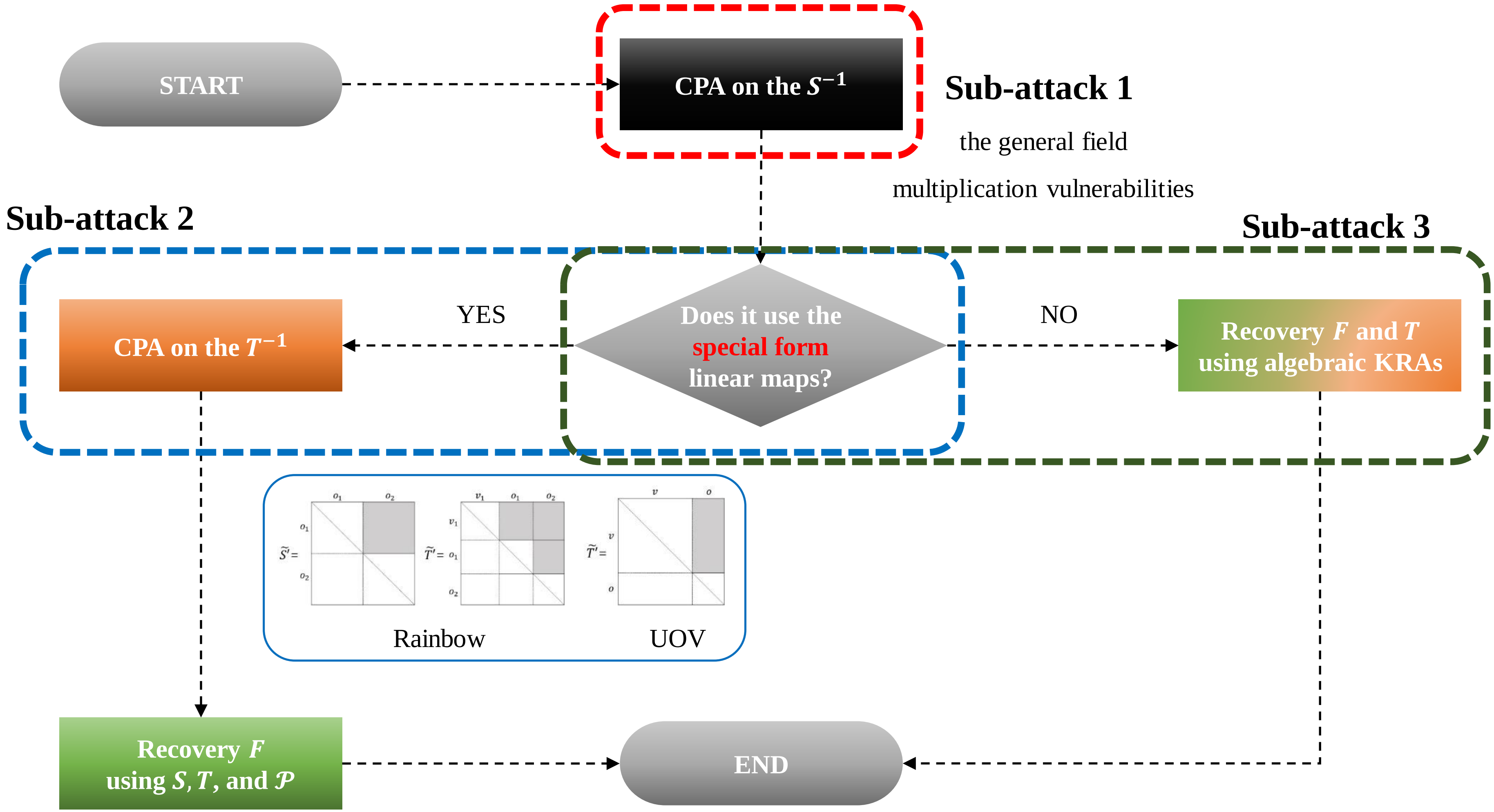


The methods for efficiency can be vulnerable to PA.

The flow of our proposed attacks

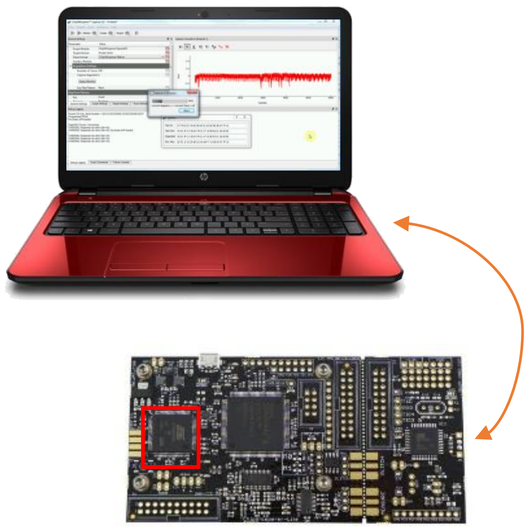
- [Goal] Secret maps recovery on Rainbow and UOV





Experimental setup

Environment	
Target chip	Atmel AVR XMEGA128
Sampling	7.38 MS/s
Algorithm	Matrix-vector product over GF(2^8)
Attack system	
ChipWhisperer-Lite, **500** traces	
Implementation	
8-bit implementation	



1st

$$\begin{aligned} y'_1{}^\wedge &= s'_{11}\cdot y_1 \\ y'_2{}^\wedge &= s'_{21}\cdot y_1 \\ &\vdots \\ y'_m{}^\wedge &= s'_{m1}\cdot y_1 \end{aligned}$$

2nd

$$\begin{aligned} y'_1{}^\wedge &= s'_{12}\cdot y_2 \\ y'_2{}^\wedge &= s'_{22}\cdot y_2 \\ &\vdots \\ y'_m{}^\wedge &= s'_{m2}\cdot y_2 \end{aligned}$$

…

To reduce the number of times y is loaded.

multiplication each loaded y by the i-th column.

SICADA Side Channel Analysis Design Academy

Sub-attack 1

- CPA on the S^{-1}

Invert S

$$\begin{pmatrix} s'_{11} & s'_{12} & \cdots & s'_{1m} \\ s'_{21} & \ddots & \ddots & s'_{2m} \\ \vdots & \ddots & \ddots & \vdots \\ s'_{m1} & s'_{m2} & \cdots & s'_{mm} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

$$s'_{11} \cdot y_1 + s'_{12} \cdot y_2 + \cdots + s'_{1m} \cdot y_m$$

Intermediate result

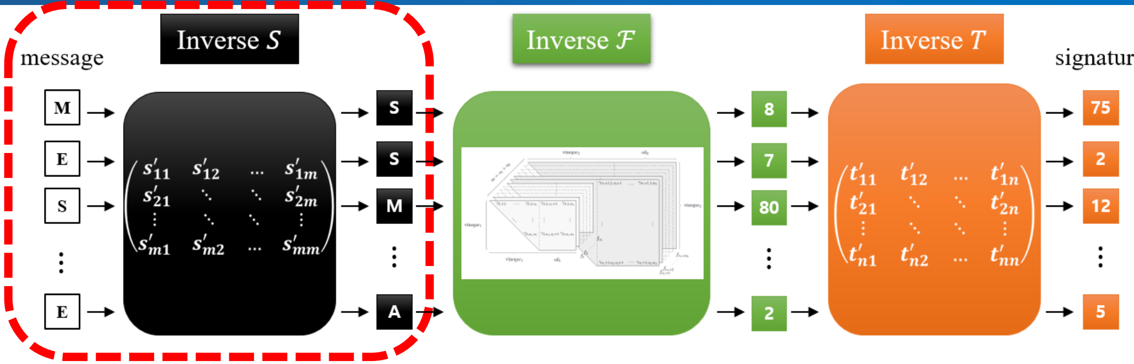
$$guess \cdot y_1$$

$$s'_{11} \cdot y_1 + guess \cdot y_2$$

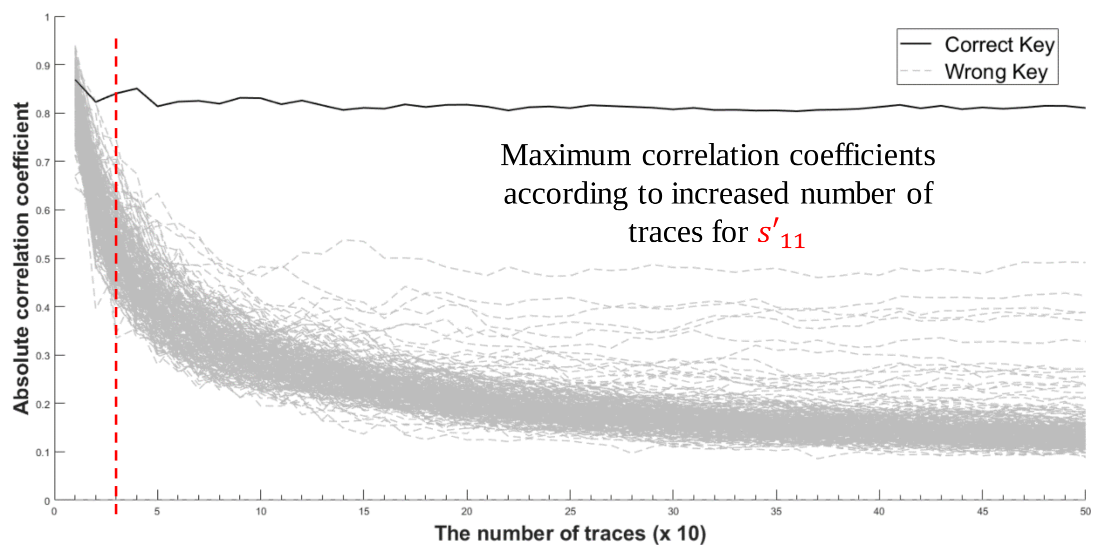
$$\vdots$$

$guess$: hypothetical key

■ Secret ■ Known

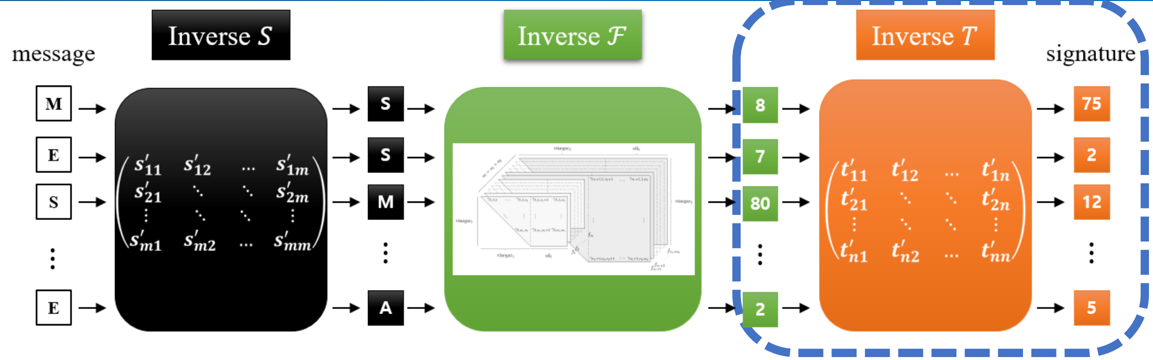


- the result of CPA for s'_{11}



Sub-attack 2

- CPA on the T^{-1}

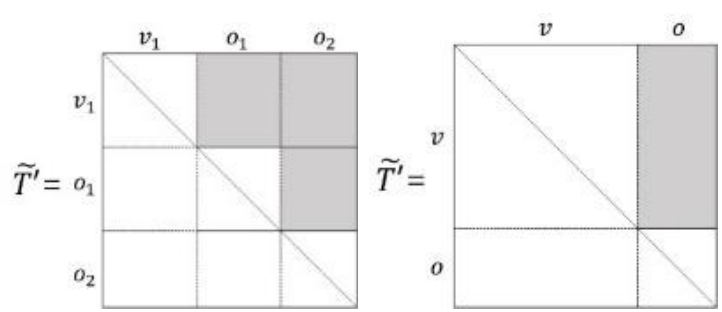


Invert T

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} t'_{11} & t'_{12} & \cdots & t'_{1n} \\ t'_{21} & \ddots & \ddots & t'_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ t'_{n1} & t'_{n2} & \cdots & t'_{nn} \end{pmatrix} \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$$

$$x_1 = t'_{11} \cdot x'_1 + t'_{12} \cdot x'_2 + \cdots + t'_{1n} \cdot x'_n$$

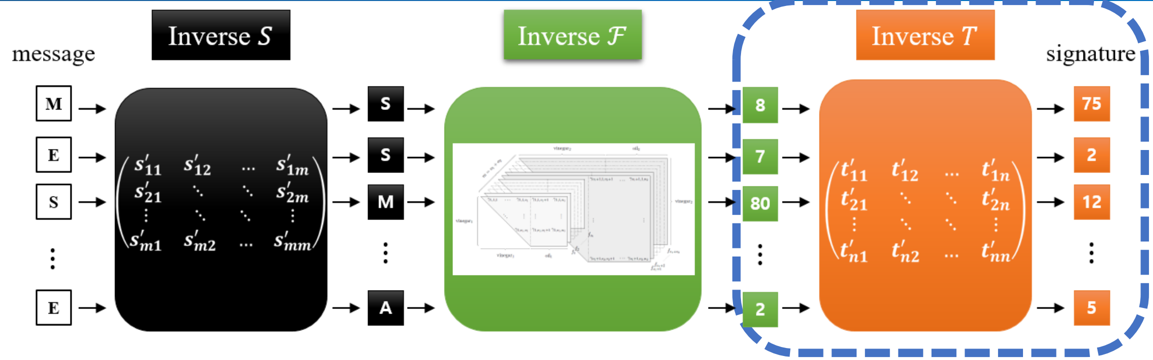
- Matrix-vector product **over a field**
- It is hard to compute X‘
  ➔ to compute the intermediate value is difficult

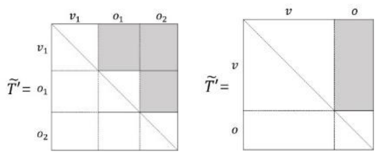


Rainbow UOV

Sub-attack 2

- CPA on the T^{-1}
  - (Assume) Special form T



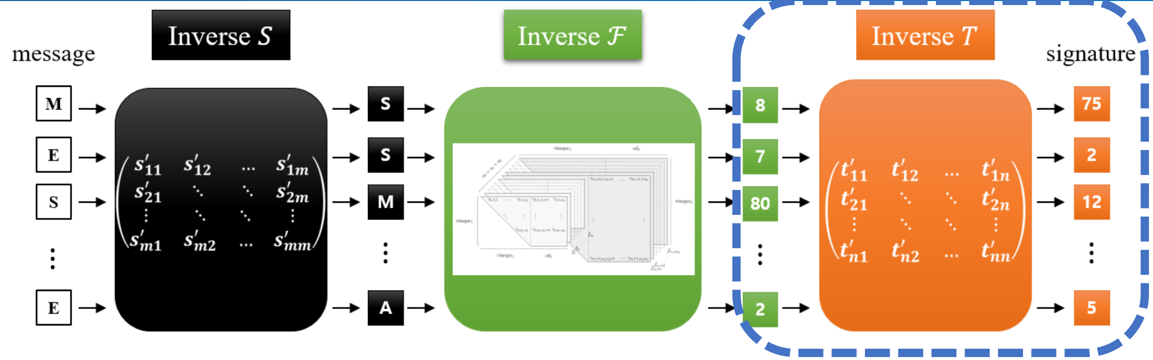


Rainbow UOV

Signature X

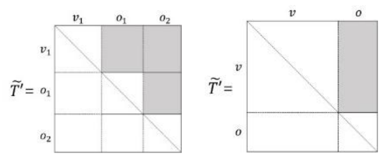
$$\begin{pmatrix} 01 & 00 & t'_{13} & t'_{14} & t'_{15} & t'_{16} & t'_{17} & t'_{18} \\ 00 & 01 & t'_{23} & t'_{24} & t'_{25} & t'_{26} & t'_{27} & t'_{28} \\ 00 & 00 & 01 & 00 & t'_{35} & t'_{36} & t'_{37} & t'_{38} \\ 00 & 00 & 00 & 01 & t'_{45} & t'_{46} & t'_{47} & t'_{48} \\ 00 & 00 & 00 & 00 & 01 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 01 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 01 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 01 \end{pmatrix} \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \\ x'_4 \\ x'_5 \\ x'_6 \\ x'_7 \\ x'_8 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}$$

✓ $x'_8 = x_8,\ x'_7 = x_7,\ x'_6 = x_6,\ x'_5 = x_5$



Sub-attack 2

- CPA on the T^{-1}
  - (Assume) Special form T



Rainbow UOV

Signature X

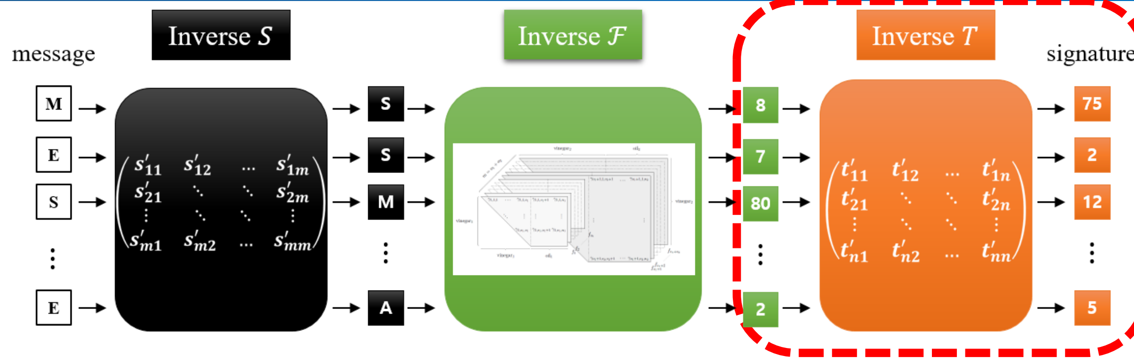
$$\begin{pmatrix} 01 & 00 & t'_{13} & t'_{14} & t'_{15} & t'_{16} & t'_{17} & t'_{18} \\ 00 & 01 & t'_{23} & t'_{24} & t'_{25} & t'_{26} & t'_{27} & t'_{28} \\ 00 & 00 & 01 & 00 & t'_{35} & t'_{36} & t'_{37} & t'_{38} \\ 00 & 00 & 00 & 01 & t'_{45} & t'_{46} & t'_{47} & t'_{48} \\ 00 & 00 & 00 & 00 & 01 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 01 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 01 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 01 \end{pmatrix} \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \\ x'_4 \\ x'_5 \\ x'_6 \\ x'_7 \\ x'_8 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}$$

$$0 \cdot x'_1 \oplus 0 \cdot x'_1 \oplus 1 \cdot x'_3 \oplus 0 \cdot x'_4 \oplus t'_{35} \cdot x'_5 \oplus t'_{36} \cdot x'_6 \oplus t'_{37} \cdot x'_7 \oplus t'_{38} \cdot x'_8 = x_3$$

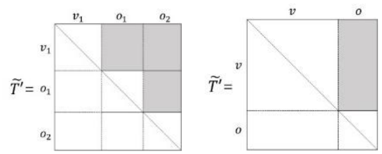
$$0 \cdot x'_1 \oplus 0 \cdot x'_1 \oplus 0 \cdot x'_3 \oplus 1 \cdot x'_4 \oplus t'_{45} \cdot x'_5 \oplus t'_{46} \cdot x'_6 \oplus t'_{47} \cdot x'_7 \oplus t'_{48} \cdot x'_8 = x_4$$

Intermediate result: $guess \cdot x'_5$, $guess \cdot x'_6$, $\cdots$

Sub-attack 2



- CPA on the T^{-1}
  - (Assume) Special form T



Rainbow UOV

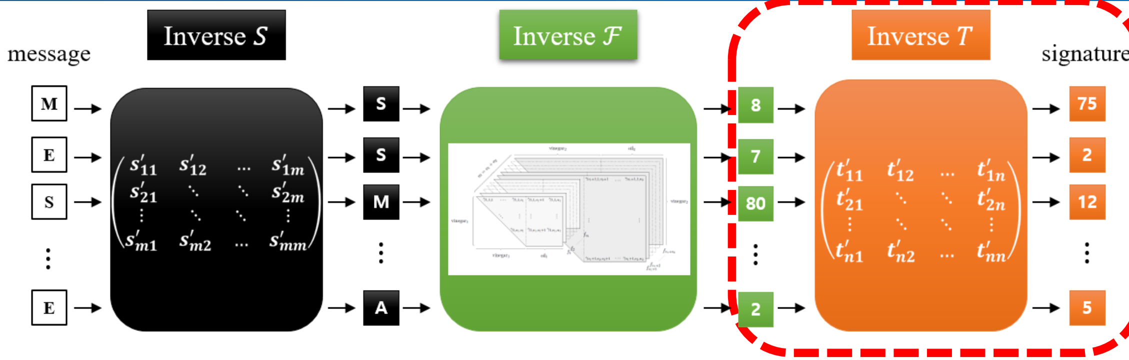
Signature X

$$\begin{pmatrix} 01 & 00 & t'_{13} & t'_{14} & t'_{15} & t'_{16} & t'_{17} & t'_{18} \\ 00 & 01 & t'_{23} & t'_{24} & t'_{25} & t'_{26} & t'_{27} & t'_{28} \\ 00 & 00 & 01 & 00 & t'_{35} & t'_{36} & t'_{37} & t'_{38} \\ 00 & 00 & 00 & 01 & t'_{45} & t'_{46} & t'_{47} & t'_{48} \\ 00 & 00 & 00 & 00 & 01 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 01 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 01 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 01 \end{pmatrix} \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \\ x'_4 \\ x'_5 \\ x'_6 \\ x'_7 \\ x'_8 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix}$$

Compute x'_3 and x'_4

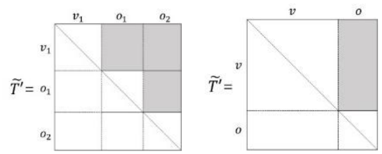
$$x_3 = x'_3 \oplus t'_{35} \cdot x'_5 \oplus t'_{36} \cdot x'_6 \oplus t'_{37} \cdot x'_7 \oplus t'_{38} \cdot x'_8$$

$$\Rightarrow \quad x'_3 = x_3 \oplus t'_{35} \cdot x'_5 \oplus t'_{36} \cdot x'_6 \oplus t'_{37} \cdot x'_7 \oplus t'_{38} \cdot x'_8$$



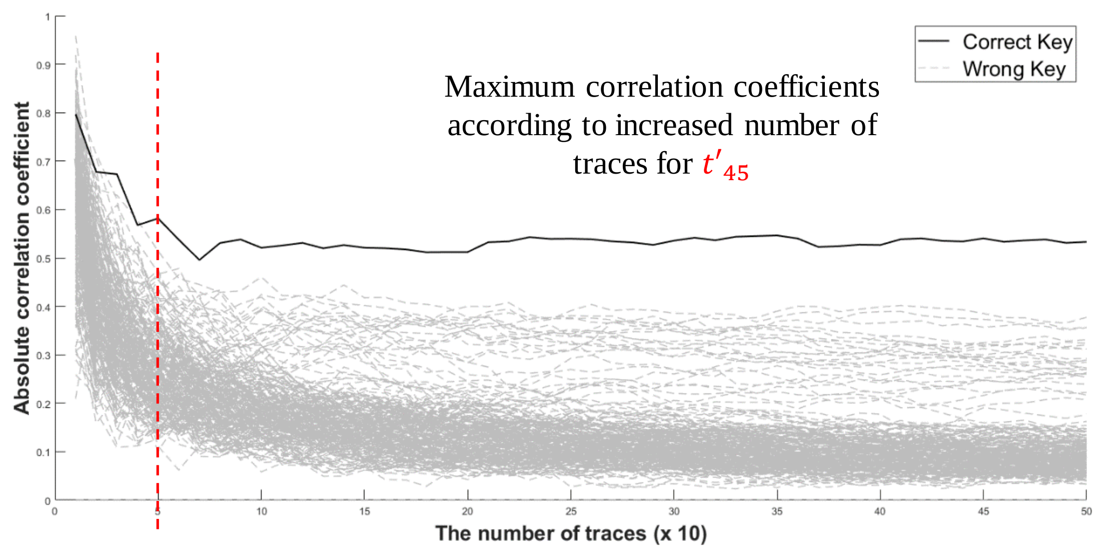
Sub-attack 2

- CPA on the T^{-1}
  - (Assume) Special form T

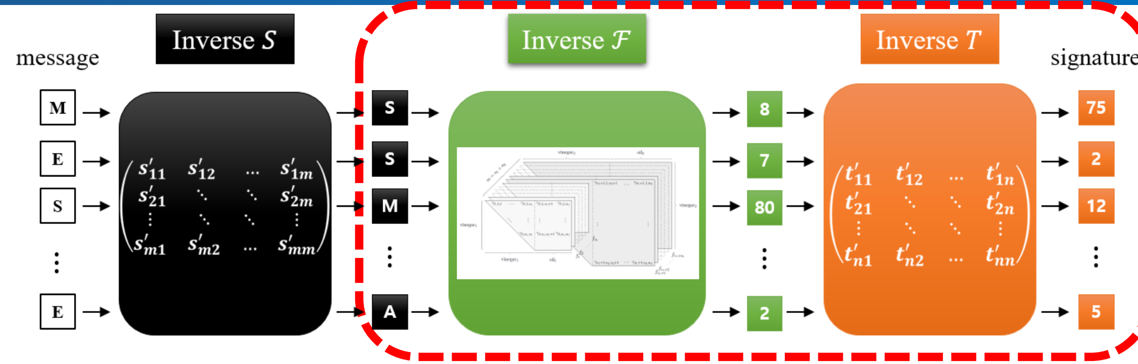


Rainbow UOV

- the result of CPA for t'_{45}



Sub-attack 3



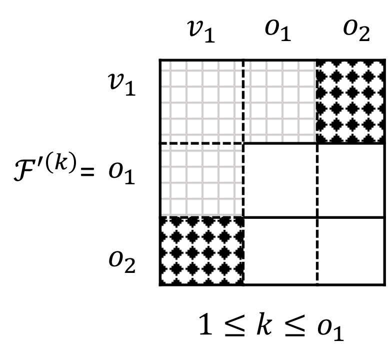
- Recovery $\boldsymbol{\mathcal{F}}$ and $\boldsymbol{T}$ using algebraic KRAs
  - (Assume) general form T, recovery S

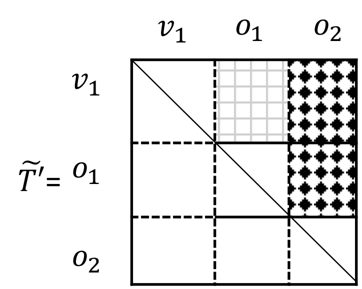
- $S^{-1} \circ \mathcal{P} = \mathcal{F} \circ T \Leftrightarrow \mathcal{P} \circ \tilde{T} = \mathcal{F}$; certain places with zero coefficients in $\mathcal{F}^{(k)}$ are known
  - Let $\mathcal{P} = S^{-1} \circ \mathcal{P}, \tilde{T} = T^{-1}$
  - Where $\mathcal{F}^{(k)}$ is the k-th component of the central map $\mathcal{F}$.

$$\mathcal{F}^{(k)} = \tilde{T}^T \cdot P^{(k)} \cdot \tilde{T} \quad \forall\, 1 \le k \le m$$

- Find an equivalent key $(\mathcal{F}', T')$ s.t $\mathcal{P} = \mathcal{F}' \circ T'$
  - The equivalent key $\boldsymbol{\mathcal{F}}'$ and $\boldsymbol{T}'$ have the form the figures.

No. equations	No. variables
$v_1 o_1 o_2$ (linear equations)	$(v_1 + o_1) o_2$

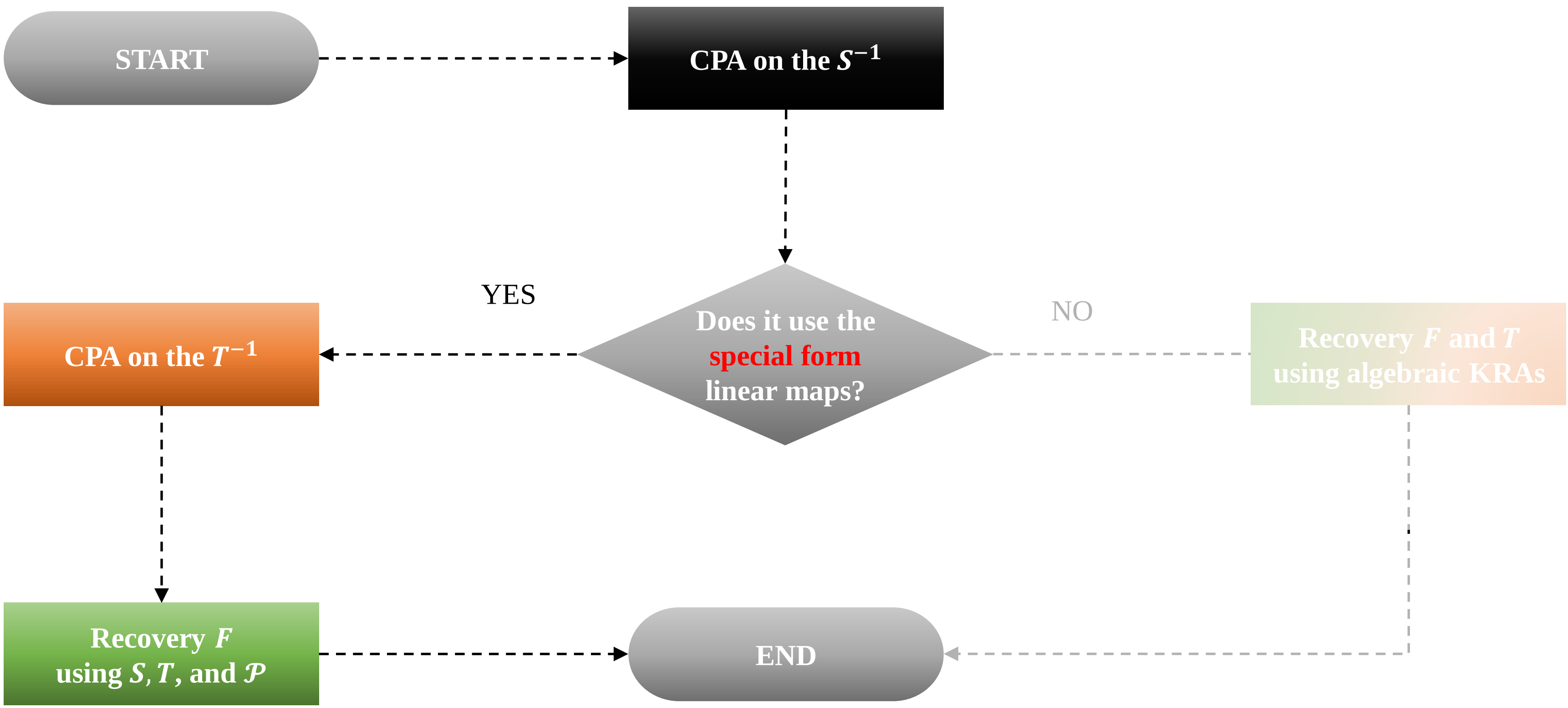




  - Rainbow$(\mathbb{F}, v_1, o_1, o_2)$ = Rainbow(GF(2^8), 36, 21, 22)
    - ✓ 0.46 milliseconds
    - ✓ Intel Xeon E5-2687W CPU 3.1 GHz with 256GB RAM

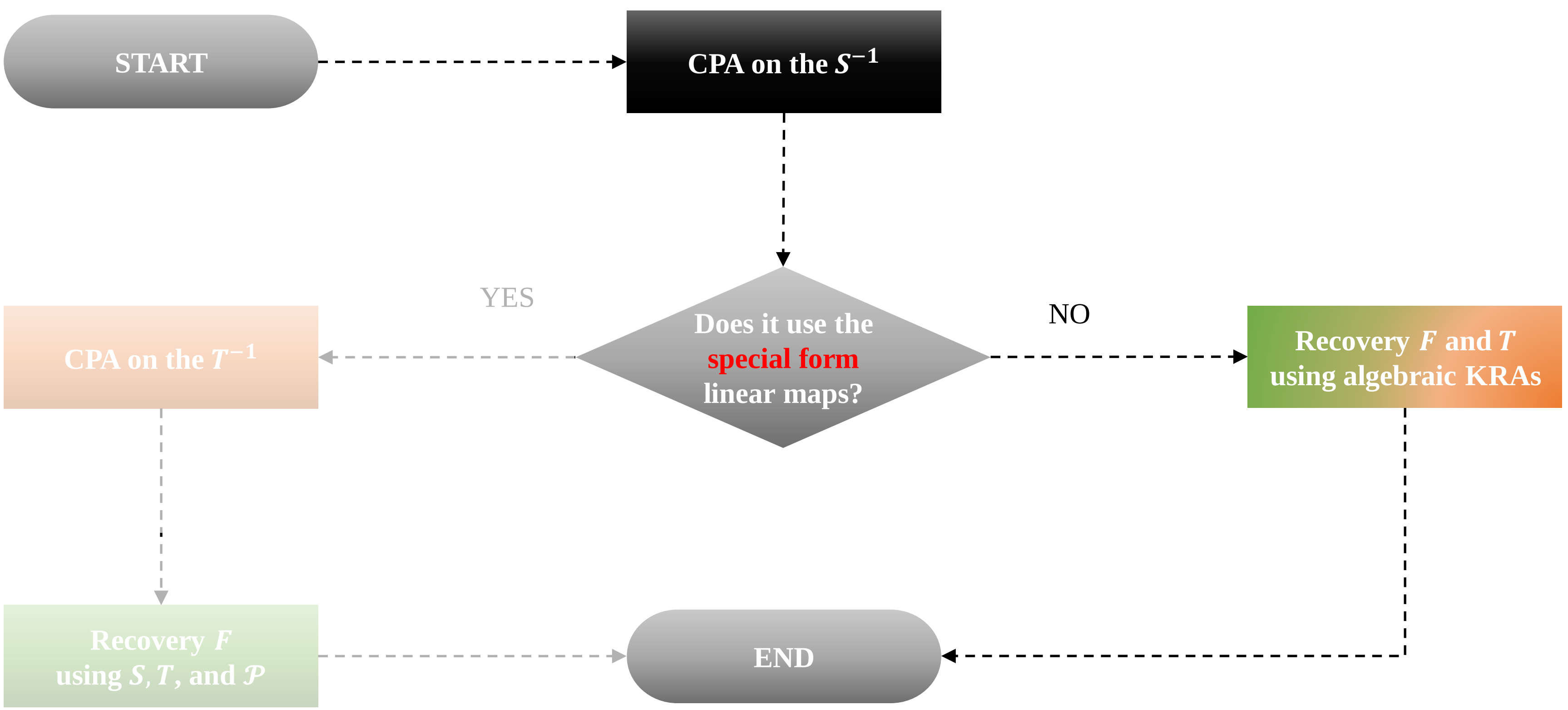
Attack 1 = sub-attack 1 + sub-attack 2

- CPA on Rainbow implementation **with Equivalent keys in CHES 2012**
  - Similar attack: CPA on UOV implementation with equivalent key



Attack 2 = sub-attack 1 + sub-attack 3

- Hybrid attack on Rainbow implementation **with random linear maps**



Other MQ-signature schemes

- UOV-like single layer schemes.
  - [INDOCRYPT 2017] Lifted UOV (LUOV)
  - LUOV is submitted to NIST for Post-Quantum Cryptography Standardization.
  - LUOV uses the form of the equivalent key proposed in CHES 2012.

Attack 1

- Rainbow-like multi-layered schemes.
  - Rainbow and HiMQ-3
  - affine-substitution (quadratic)-affine (ASA) structure
  - $\mathrm{GF}(2^{\mathrm{n}})$, $n > 1$

Attack 2

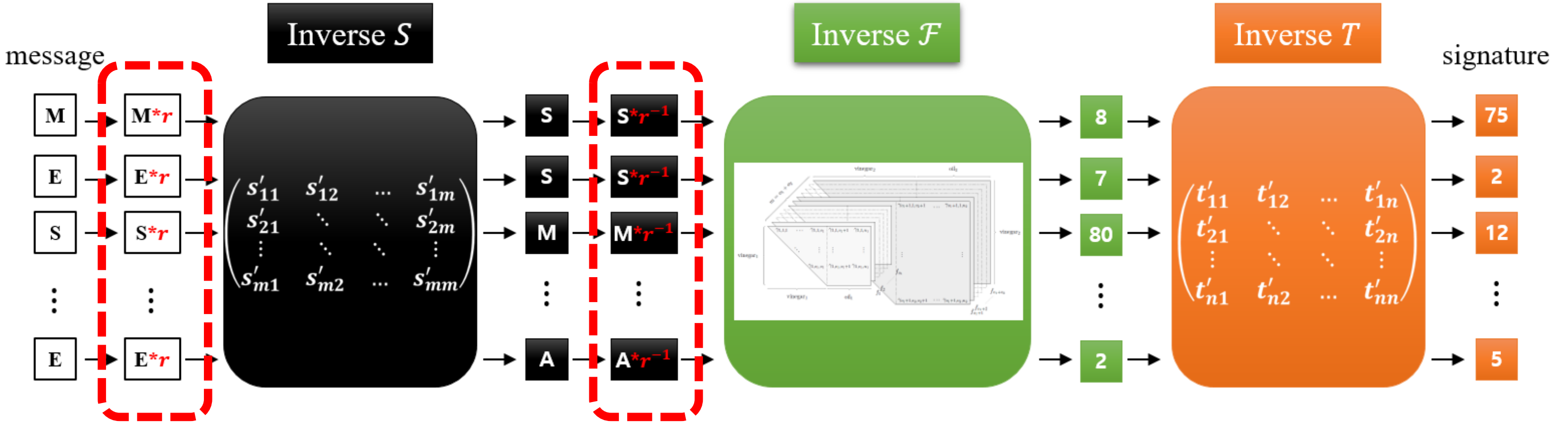
Countermeasures

UOV-like single layer schemes

- Use the T that is removed the relation between the signature value and the intermediate value.

Rainbow-like multi-layered schemes

- focus on implementing a secure matrix-vector product against PA
- Message randomization



- Overhead: $2m$ field multiplications and a field inversion

Conclusion

- Our contributions
  - CPA on Rainbow and UOV **implementation with equivalent keys in CHES 2012**
  - Hybrid attack on Rainbow **implementation with random linear maps**
  - Our attacks can **apply to other MQ-signature schemes**.
  - Countermeasure against first-order CPA

- Further work
  - More efficient countermeasures
  - Security analysis against high-order and fault injection attacks