



**HAL**  
open science

# Overview of side-channel and fault injection attacks on ML-KEM CRYSTALS-KYBER implementations

Simon Pontie

► **To cite this version:**

Simon Pontie. Overview of side-channel and fault injection attacks on ML-KEM CRYSTALS-KYBER implementations. Post-Quantum Cryptography conference by DGA at European Cyber Week, Nov 2024, Rennes, France. cea-04810887

**HAL Id: cea-04810887**

**<https://cea.hal.science/cea-04810887v1>**

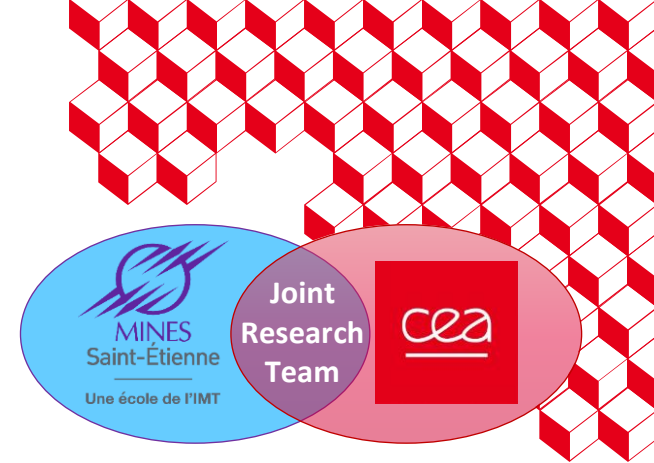
Submitted on 29 Nov 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Laboratoire Sécurité des Composants  
(LETI/DSYS/SSSEC/LSCO)



# Overview of side-channel and fault injection attacks on ML-KEM (CRYSTALS-KYBER) implementations

Simon Pontié

[simon.pontie@cea.fr](mailto:simon.pontie@cea.fr)

# Outline



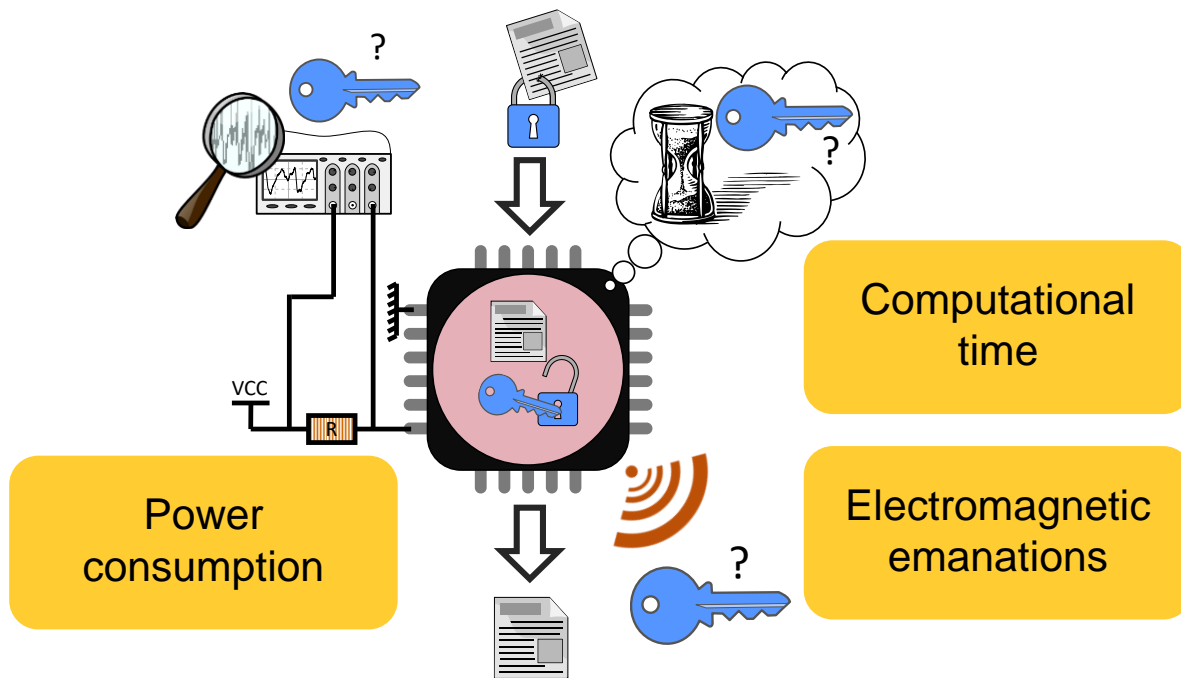
- I. Side Channel Analysis and Fault Injection
- II. ML-KEM
- III. 3 examples of Fault Injection attack on ML-KEM implementation
- IV. 2 examples of Side-Channel Analysis attack on ML-KEM implementation
- V. Conclusion

**Existing survey in the literature:** *Ravi, Prasanna, et al. "Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results." ACM Transactions on Embedded Computing Systems 23.2 (2024): 1-54.*

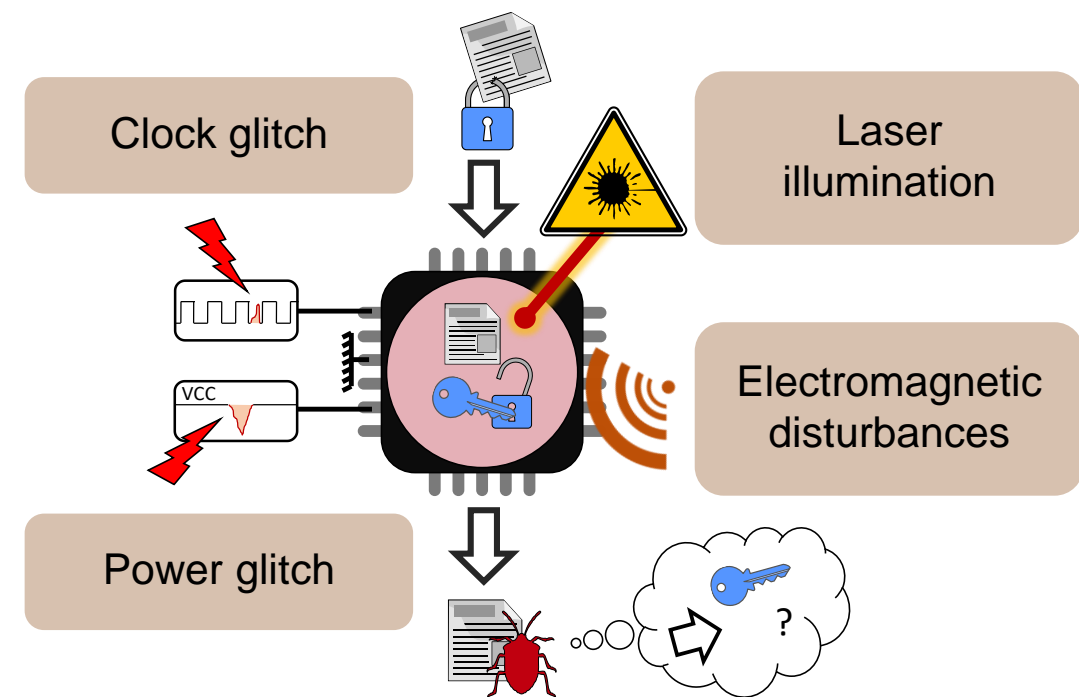
# Side Channel Analysis and Fault Injection

A cryptographic implementation can leak information about a secret even if it is an implementation of a secure cryptographic algorithm.

## Side-channel analysis (SCA) attacks



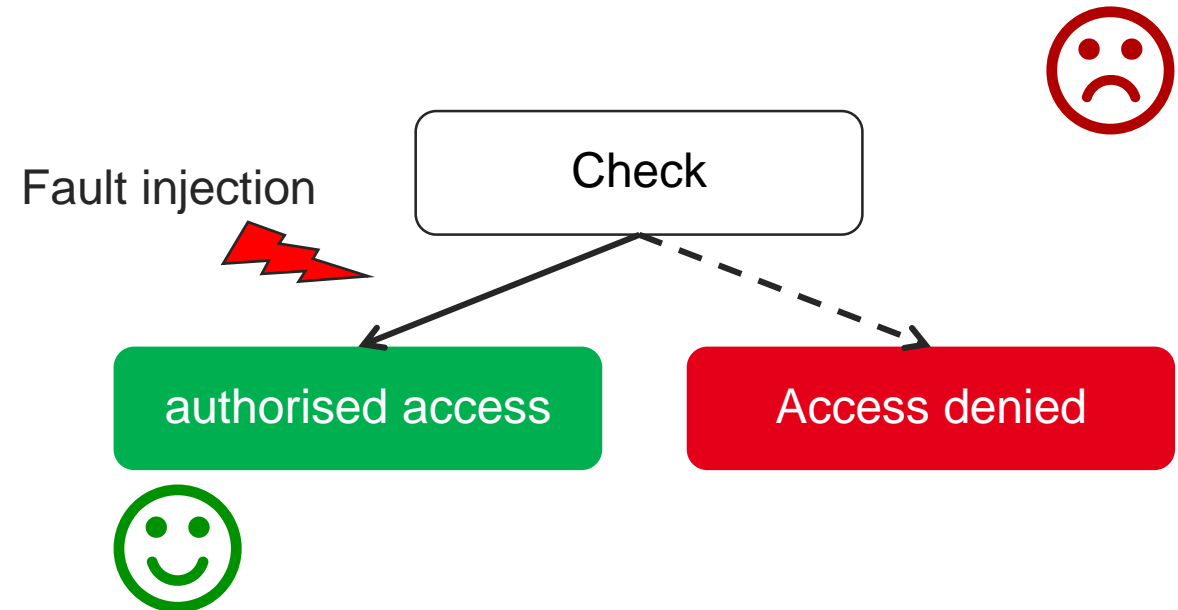
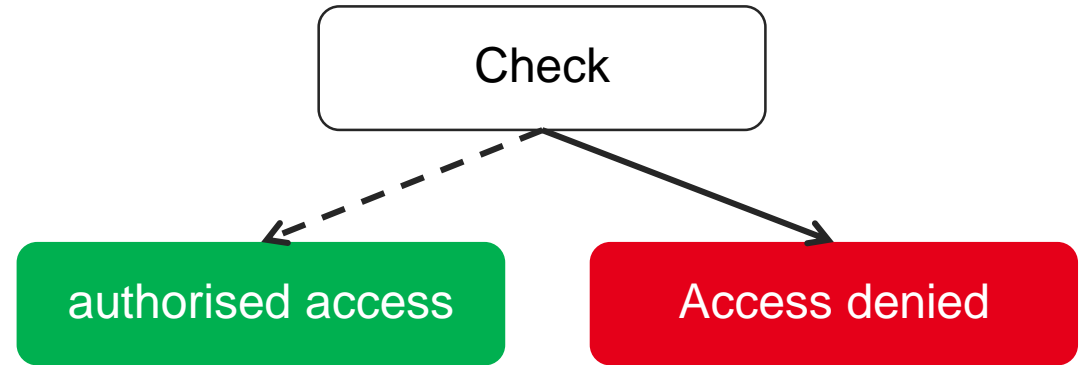
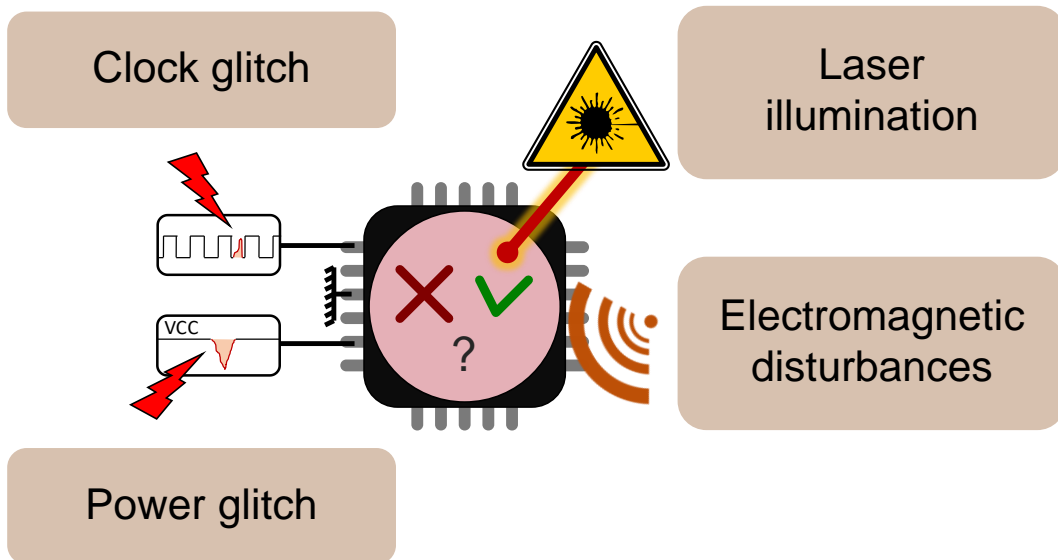
## Fault injection (FI) attacks



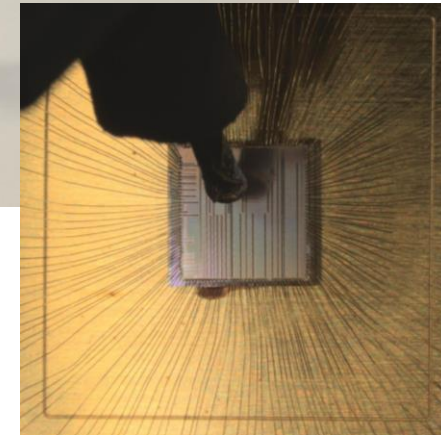
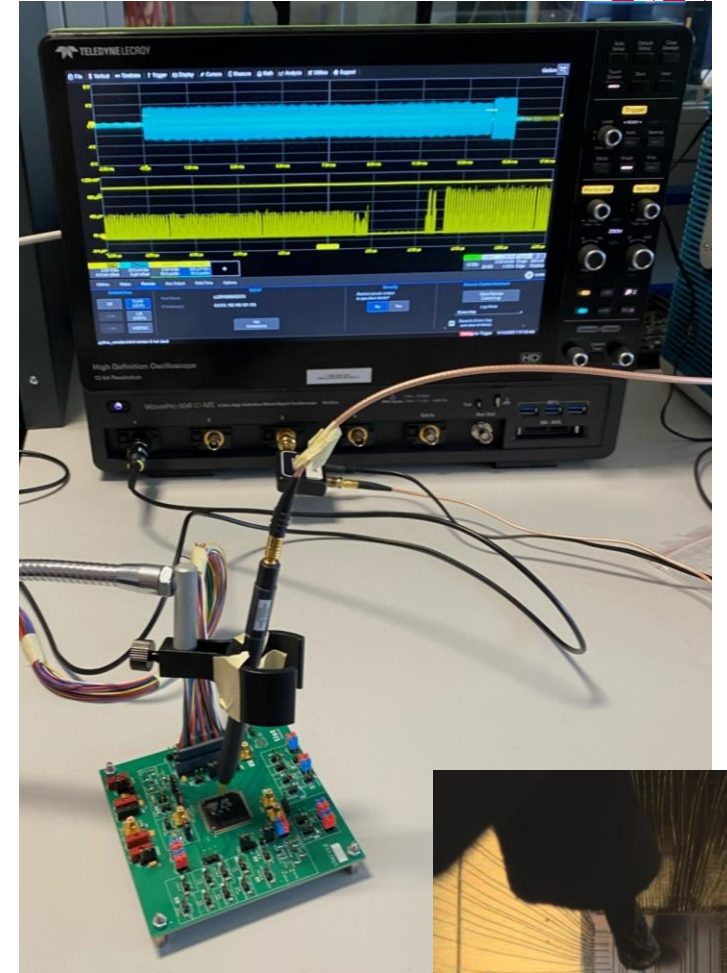
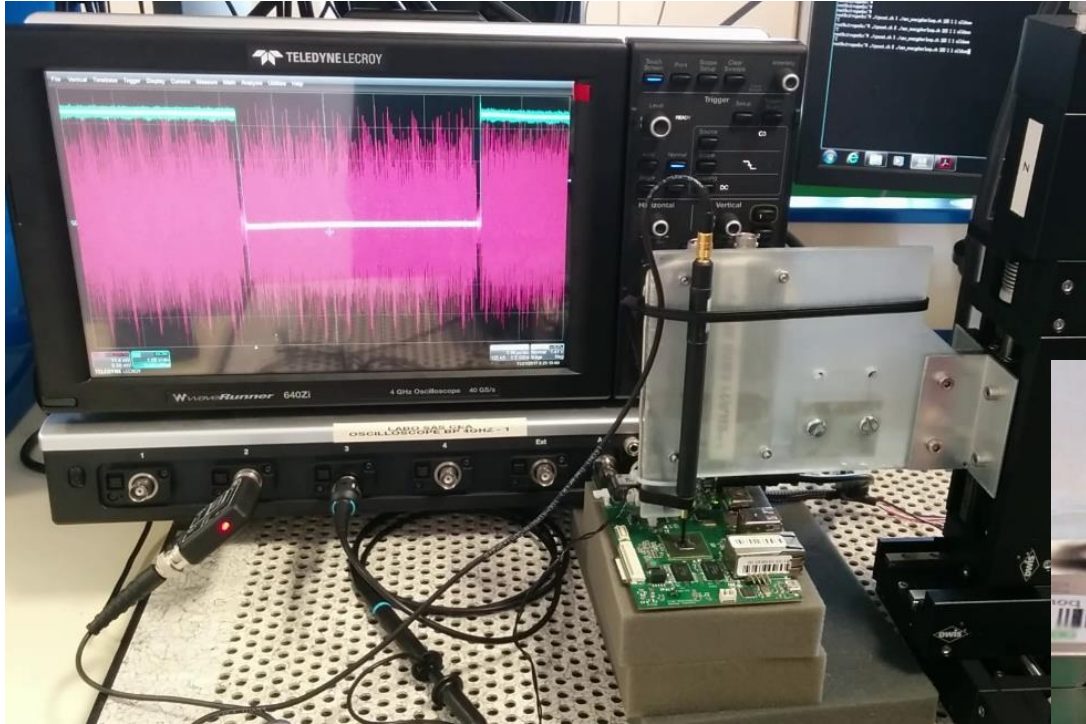
# Side Channel Analysis and Fault Injection

Fault injection attacks can also be used to bypass a security mechanism

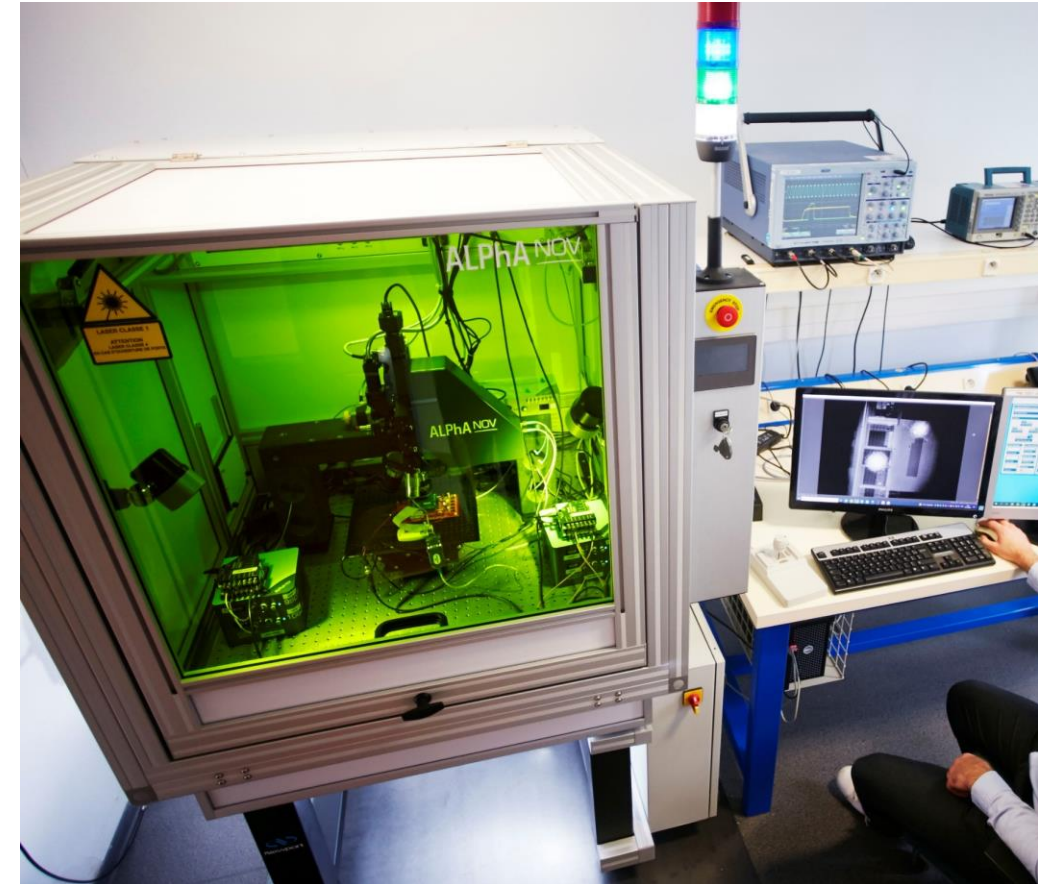
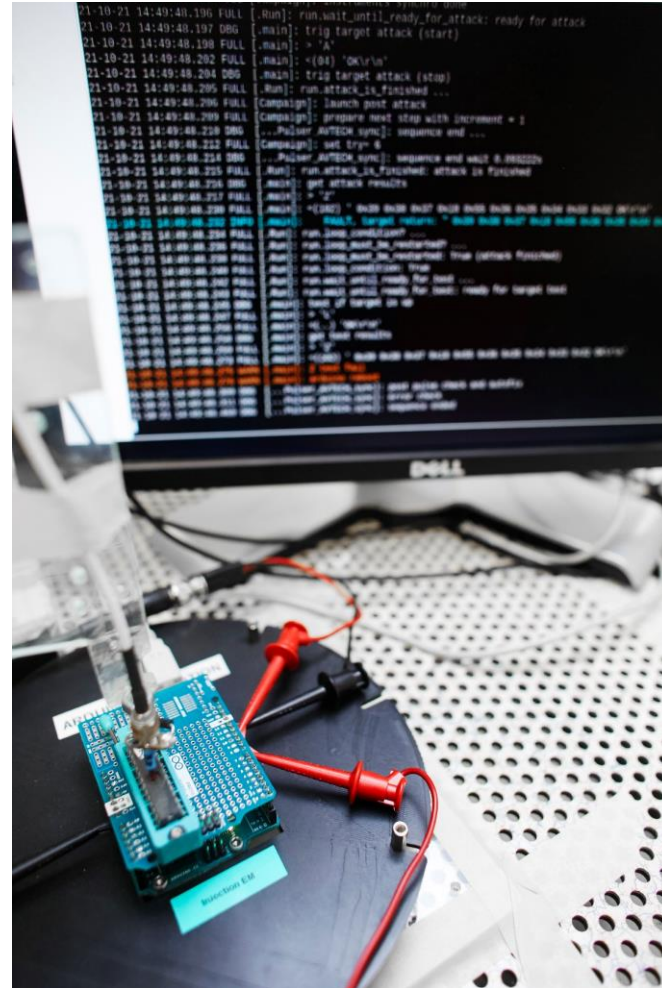
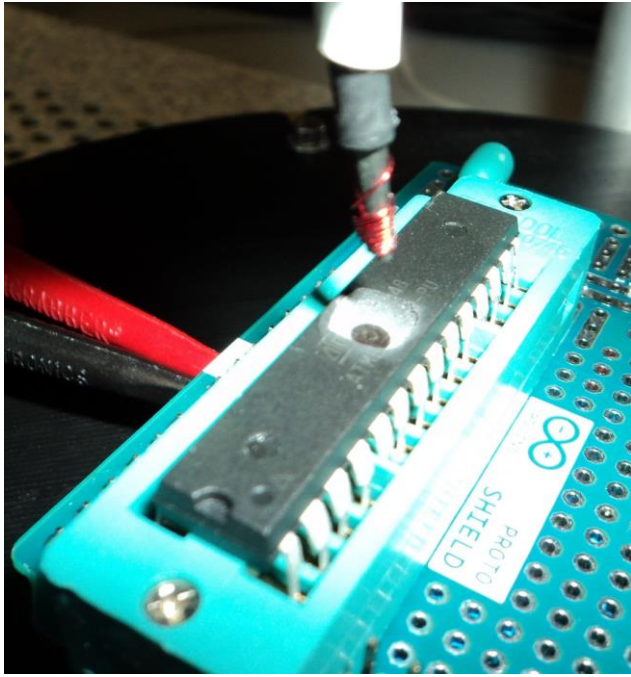
## Fault injection (FI) attacks



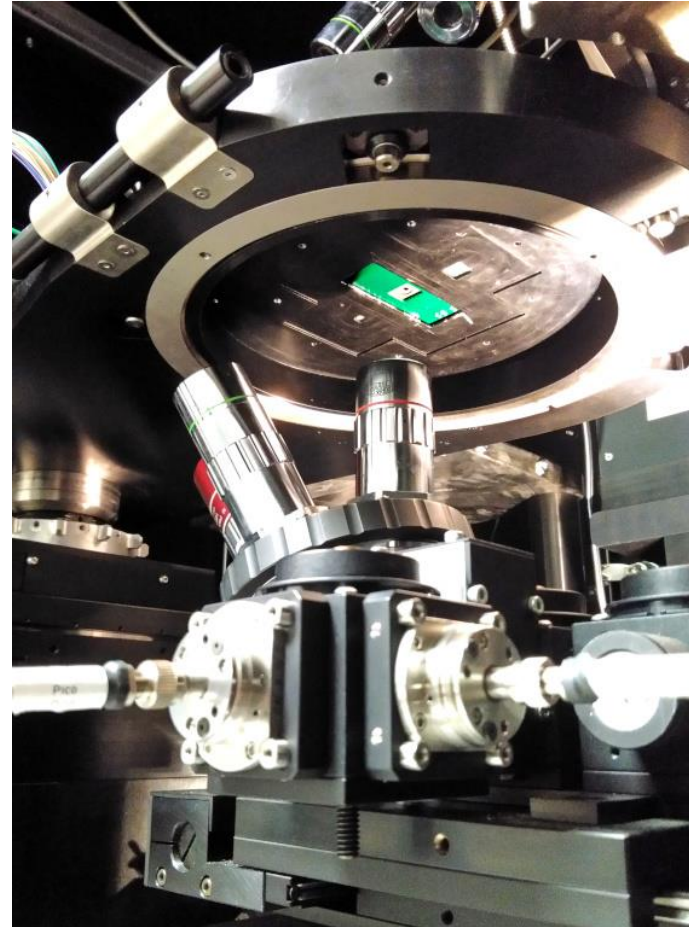
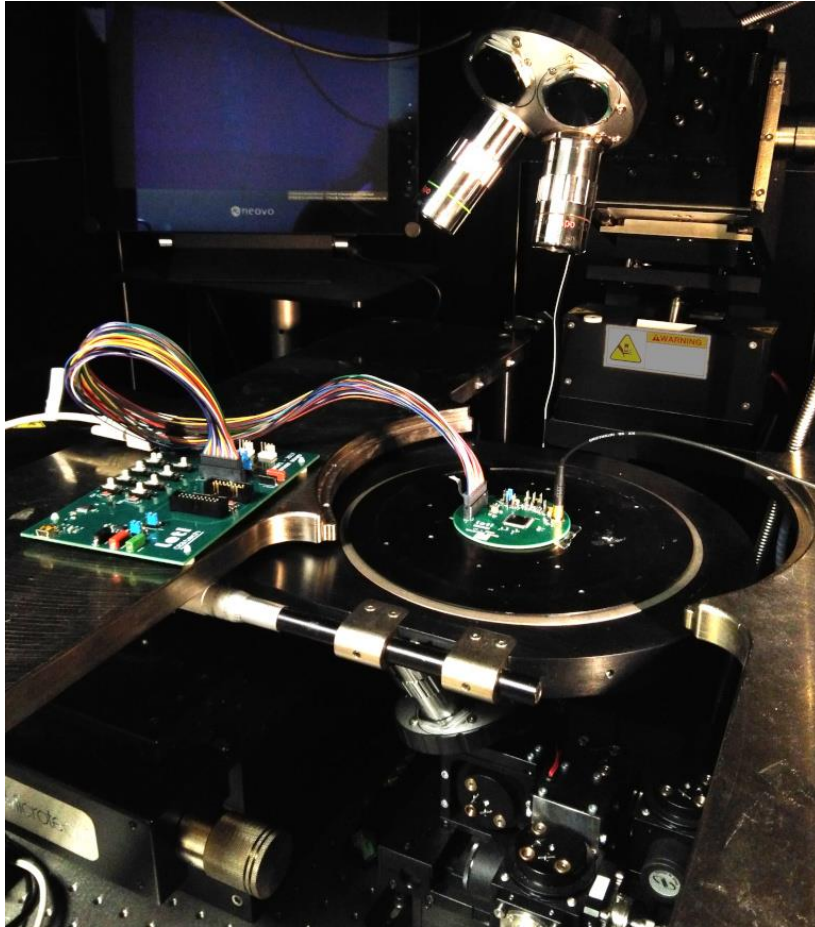
# Side Channel Analysis



# Fault Injection



# Fault Injection





# ML-KEM (close to Crystal-Kyber)

ML-KEM-512
Security level = 1
$q = 3329$
$n = 256$
$k = 2$
$\eta_1 = 3$
$\eta_2 = 2$
$d_u = 10$
$d_v = 4$

ML-KEM-768
Security level = 3
$q = 3329$
$n = 256$
$k = 3$
$\eta_1 = 2$
$\eta_2 = 2$
$d_u = 10$
$d_v = 4$

ML-KEM-1024
Security level = 5
$q = 3329$
$n = 256$
$k = 4$
$\eta_1 = 2$
$\eta_2 = 2$
$d_u = 11$
$d_v = 5$

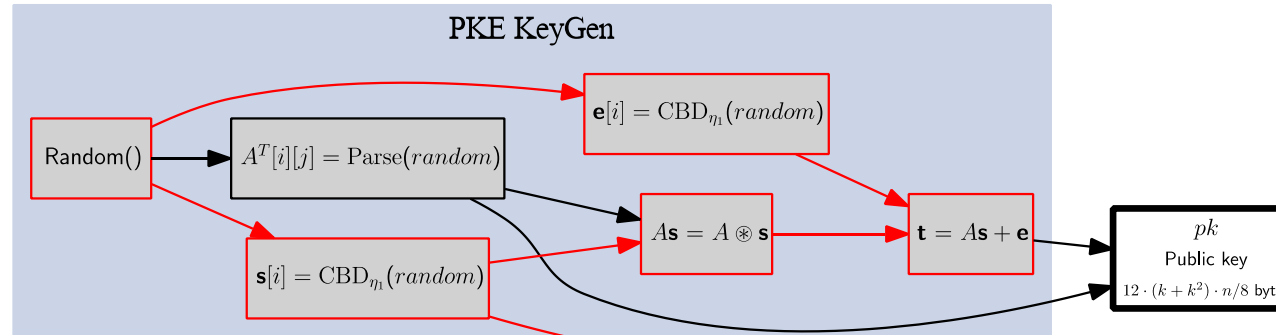
$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ (integer ring)
$R_q = \mathbb{Z}_q[X]/(X^n + 1)$ (polynomial ring, $n$ -degree polynomial)
$R_q^k$ (a $k$ -dimensional vector of polynomials with polynomials in $R_q$ )
$R_q^{k \times k}$ (module of dimension $k \times k$ , $k$ -by- $k$ matrix of polynomials with polynomials in $R_q$ )
$\zeta = 17$ (primitive $n$ -th root of unity modulo $q$ )

FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard

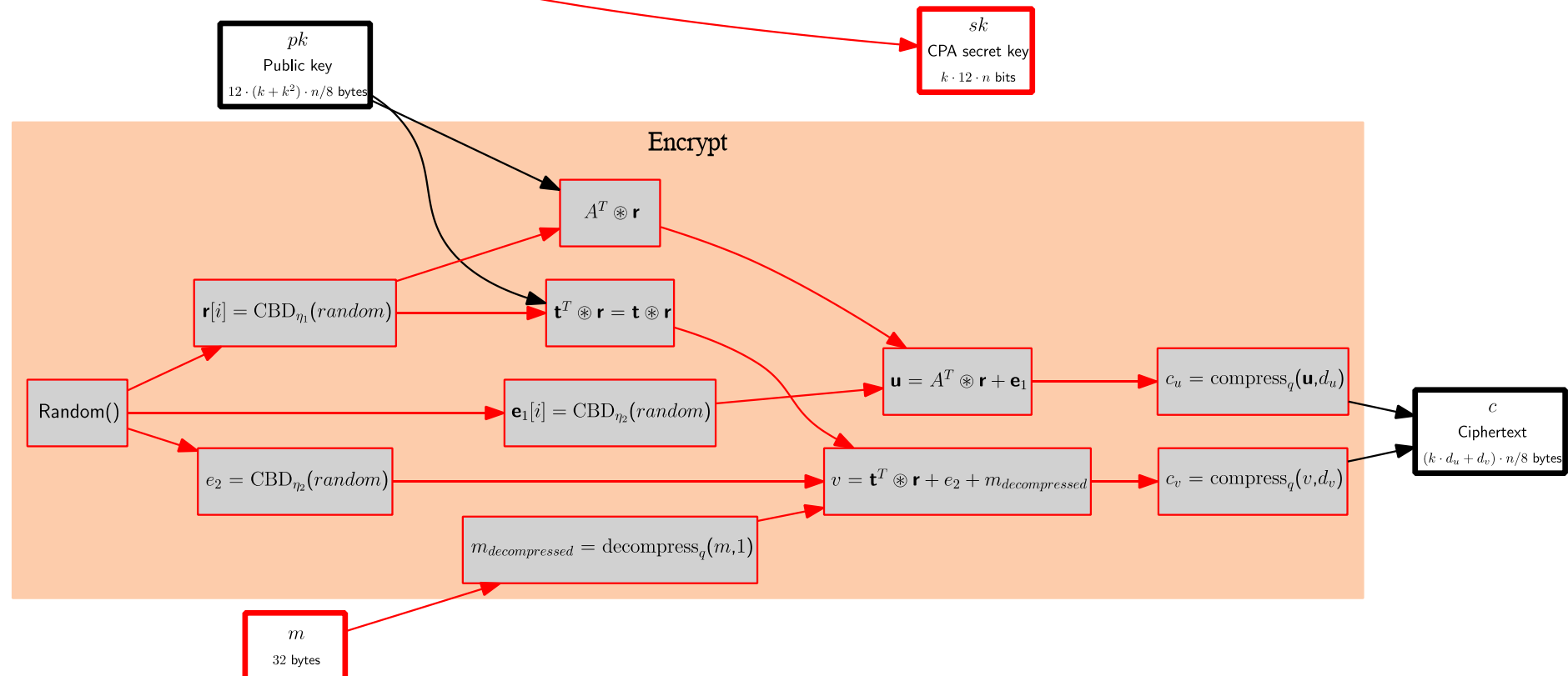
<https://doi.org/10.6028/NIST.FIPS.203>, Published August 13, 2024

# Simplified PKE in ML-KEM

- Key generation

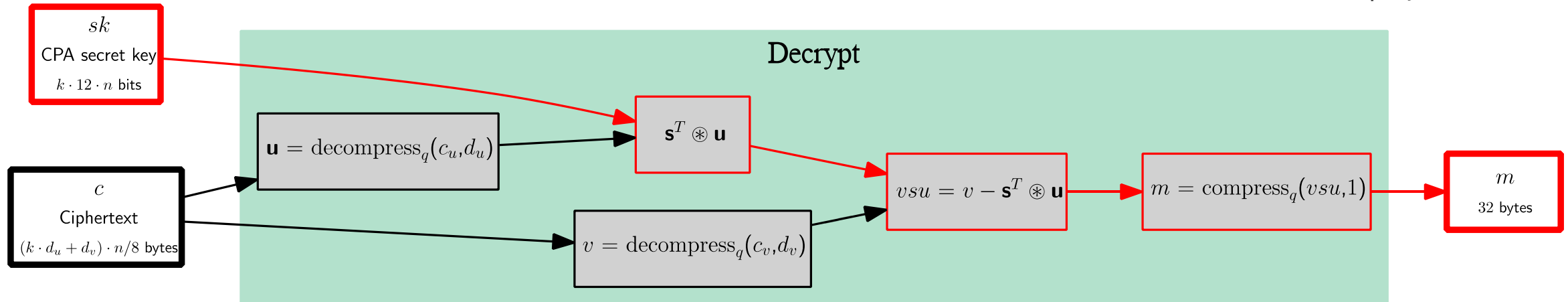
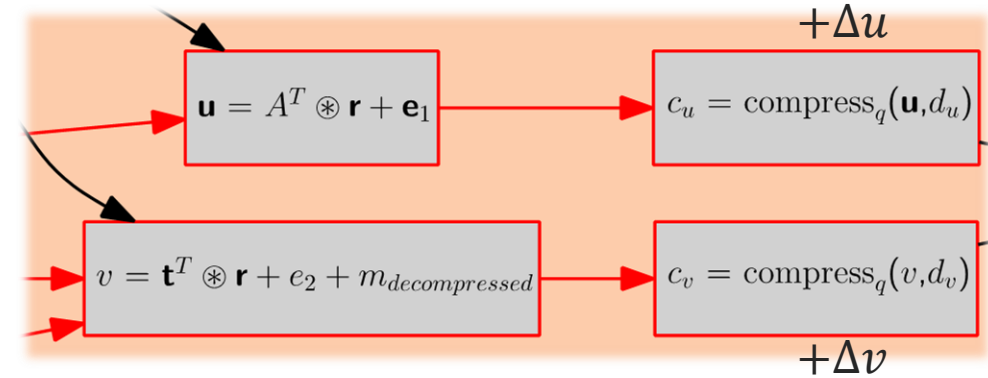


- Message Encryption



# Simplified PKE in ML-KEM

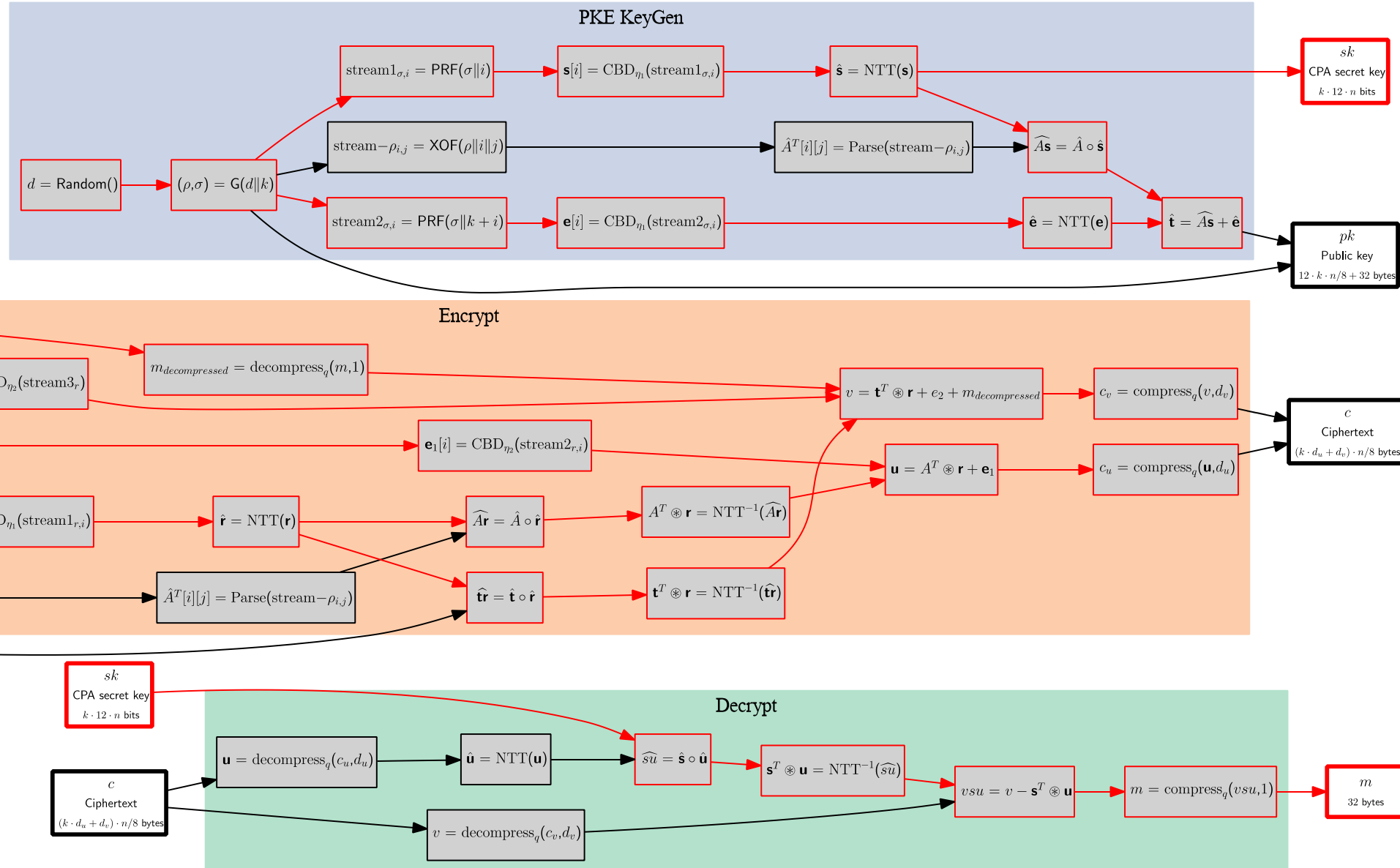
- Message decryption



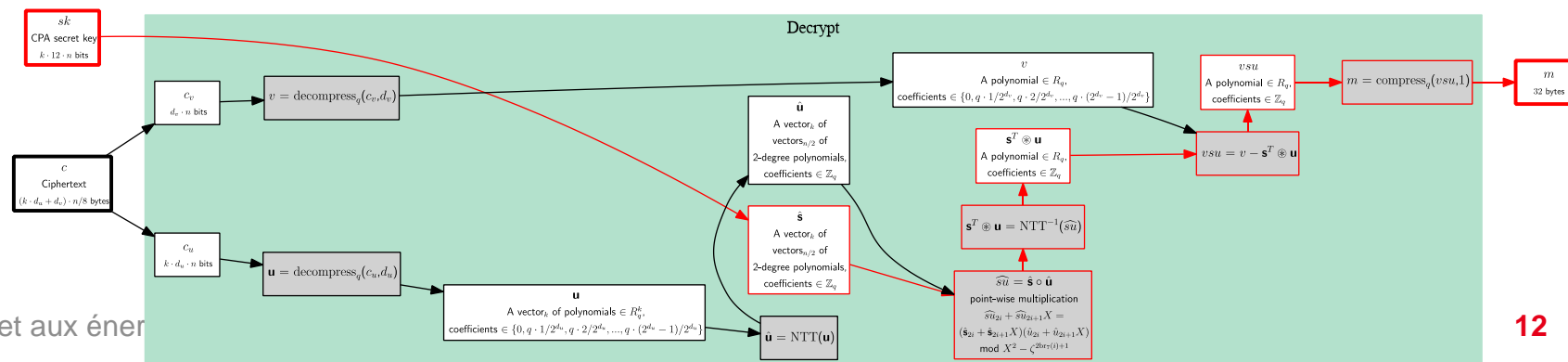
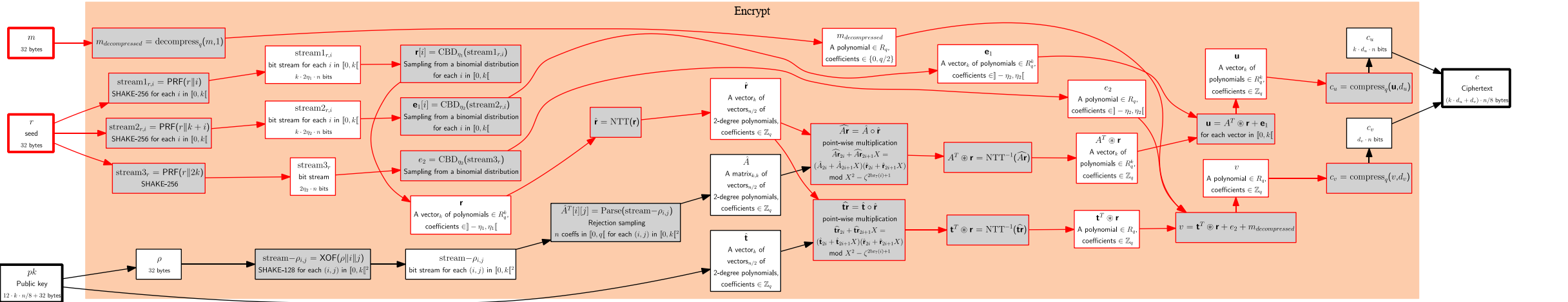
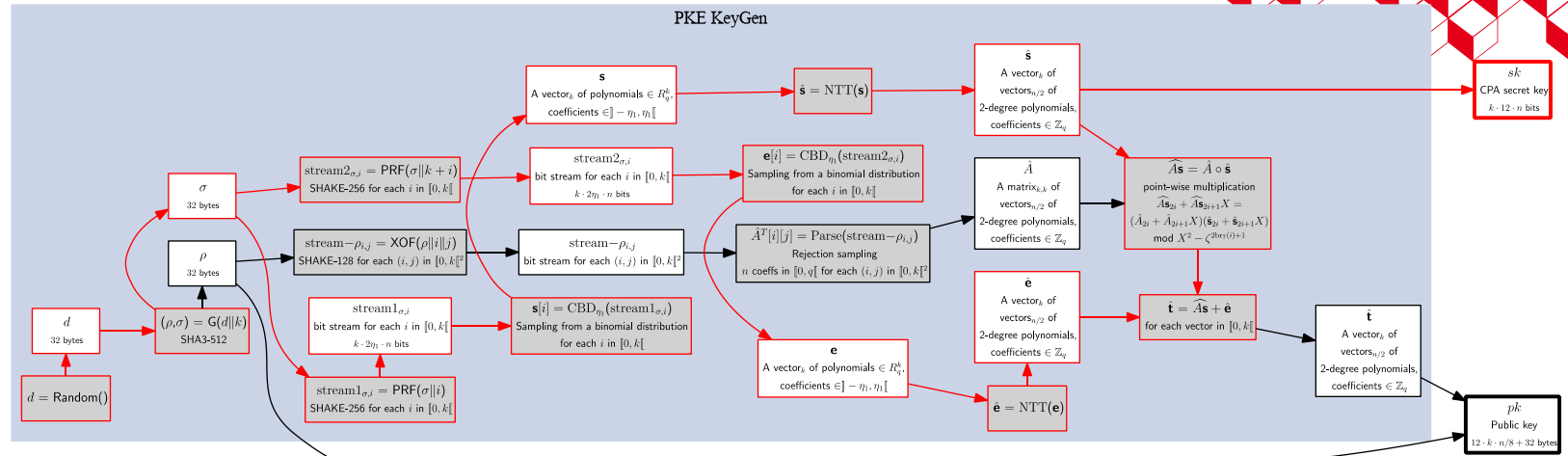
$$\begin{aligned}
 vsu &= v - s^T \otimes u \\
 &= (s^T \otimes A^T \otimes r + e^T \otimes r + e_2 + m + \Delta v) - (s^T \otimes A^T \otimes r + s^T \otimes e_1 + s^T \otimes \Delta u) \\
 &= m + e^T \otimes r + e_2 + \Delta v - s^T \otimes e_1 - s^T \otimes \Delta u \\
 &\simeq m
 \end{aligned}$$

# PKE in ML-KEM

- $\rho$  seed in KeyGen
- $r$  seed in Encrypt
- NTT



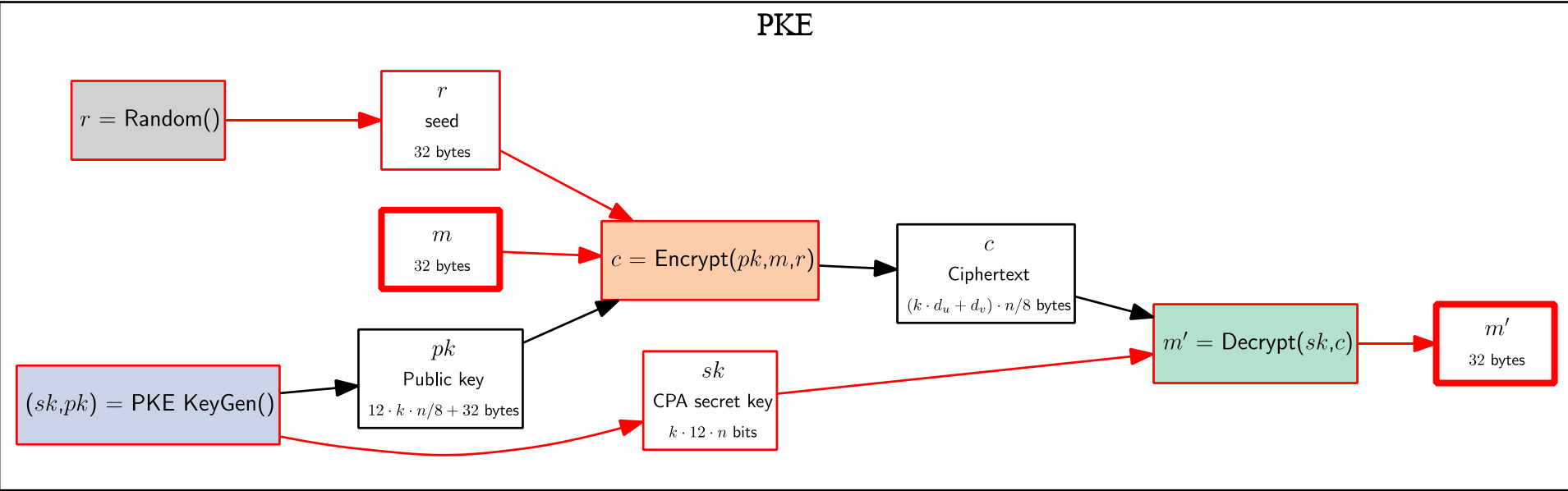
# PKE in ML-KEM



# PKE in ML-KEM



ML-KEM-768
Security level = 3
$q = 3329$
$n = 256$
$k = 3$
$\eta_1 = 2$
$\eta_2 = 2$
$d_u = 10$
$d_v = 4$
$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ (integer ring)
$R_q = \mathbb{Z}_q[X]/(X^n + 1)$ (polynomial ring, $n$ -degree polynomial)
$R_q^k$ (a $k$ -dimensional vector of polynomials with polynomials in $R_q$ )
$R_q^{k \times k}$ (module of dimension $k \times k$ , $k$ -by- $k$ matrix of polynomials with polynomials in $R_q$ )
$\zeta = 17$ (primitive $n$ -th root of unity modulo $q$ )



PKE = a Public-Key Encryption scheme from the MLWE problem.

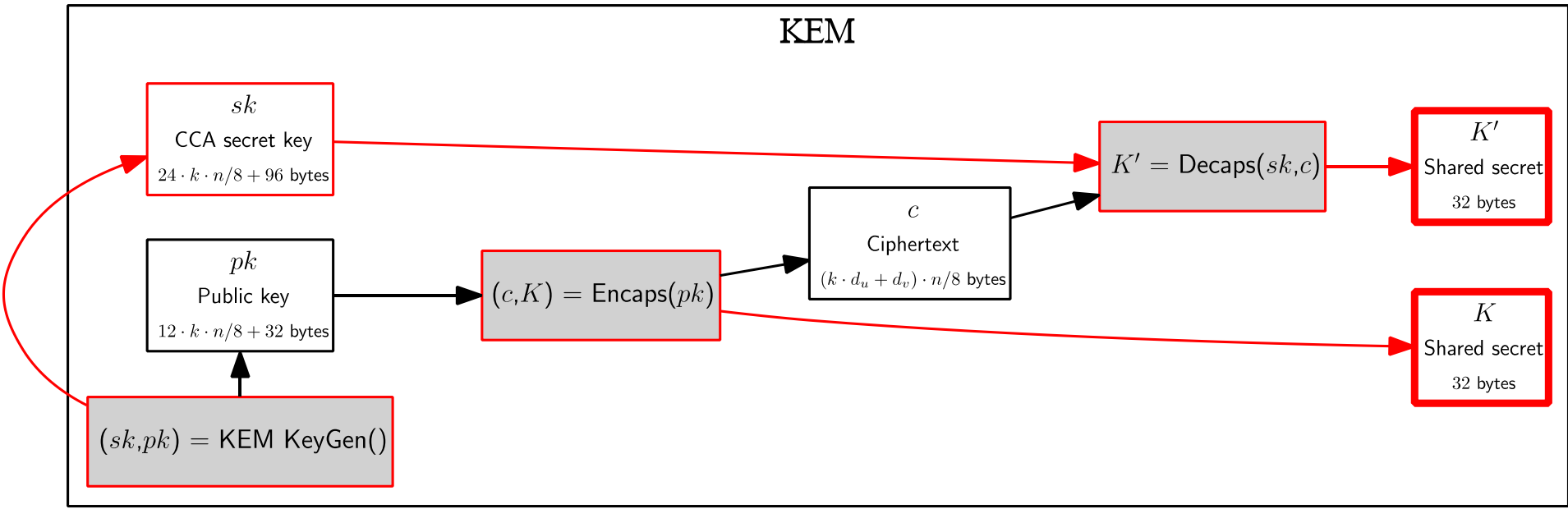
This PKE is indistinguishability under chosen plaintext attack (IND-CPA)  
(under the MLWE hardness assumption)

# ML-KEM (Crystal-Kyber)



ML-KEM-768
Security level = 3
$q = 3329$
$n = 256$
$k = 3$
$\eta_1 = 2$
$\eta_2 = 2$
$d_u = 10$
$d_v = 4$
$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ (integer ring)
$R_q = \mathbb{Z}_q[X]/(X^n + 1)$ (polynomial ring, $n$ -degree polynomial)
$R_q^k$ (a $k$ -dimensional vector of polynomials with polynomials in $R_q$ )
$R_q^{k \times k}$ (module of dimension $k \times k$ , $k$ -by- $k$ matrix of polynomials with polynomials in $R_q$ )
$\zeta = 17$ (primitive $n$ -th root of unity modulo $q$ )

Parameter set	Decapsulation failure rate
ML-KEM-512	$2^{-138.8}$
ML-KEM-768	$2^{-164.8}$
ML-KEM-1024	$2^{-174.8}$

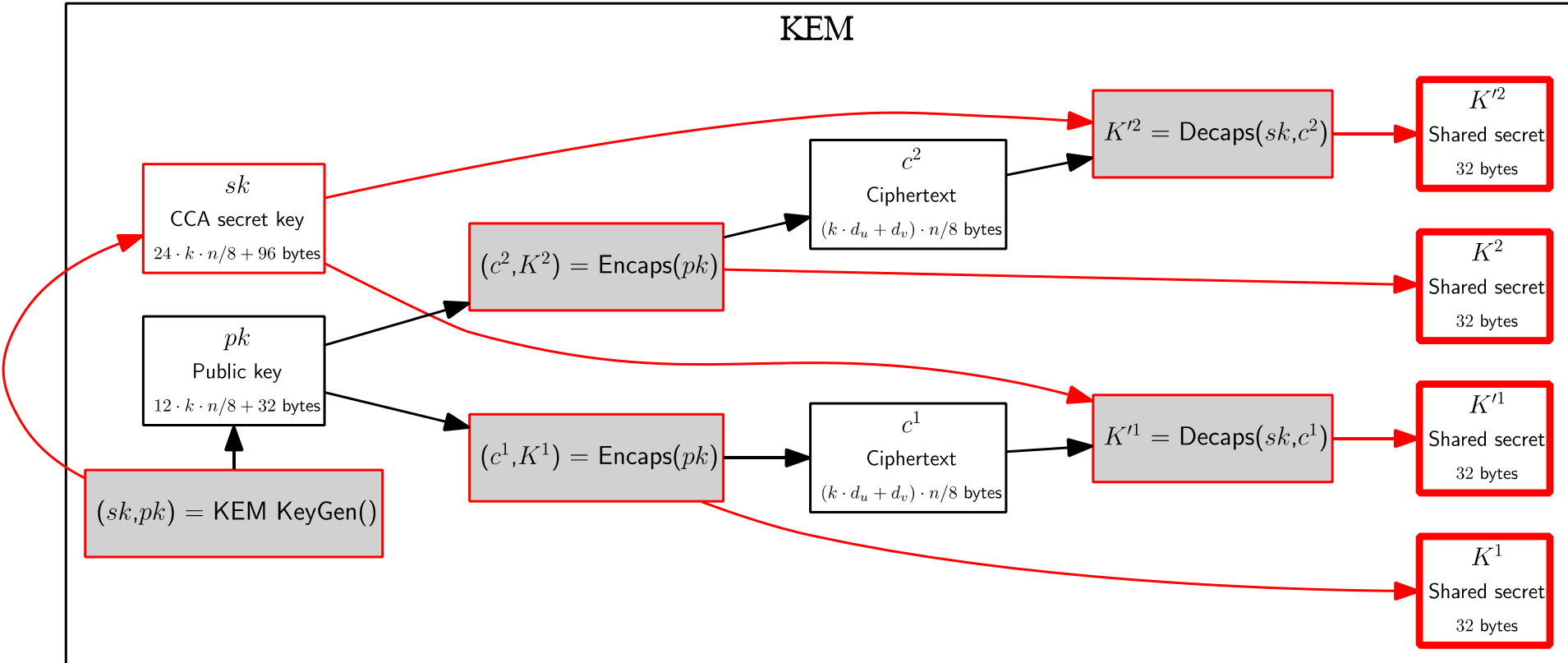


KEM = Key Encapsulation Mechanism

# ML-KEM (Crystal-Kyber)



ML-KEM-768
Security level = 3
$q = 3329$
$n = 256$
$k = 3$
$\eta_1 = 2$
$\eta_2 = 2$
$d_u = 10$
$d_v = 4$
$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ (integer ring)
$R_q = \mathbb{Z}_q[X]/(X^n + 1)$ (polynomial ring, $n$ -degree polynomial)
$R_q^k$ (a $k$ -dimensional vector of polynomials with polynomials in $R_q$ )
$R_q^{k \times k}$ (module of dimension $k \times k$ , $k$ -by- $k$ matrix of polynomials with polynomials in $R_q$ )
$\zeta = 17$ (primitive $n$ -th root of unity modulo $q$ )



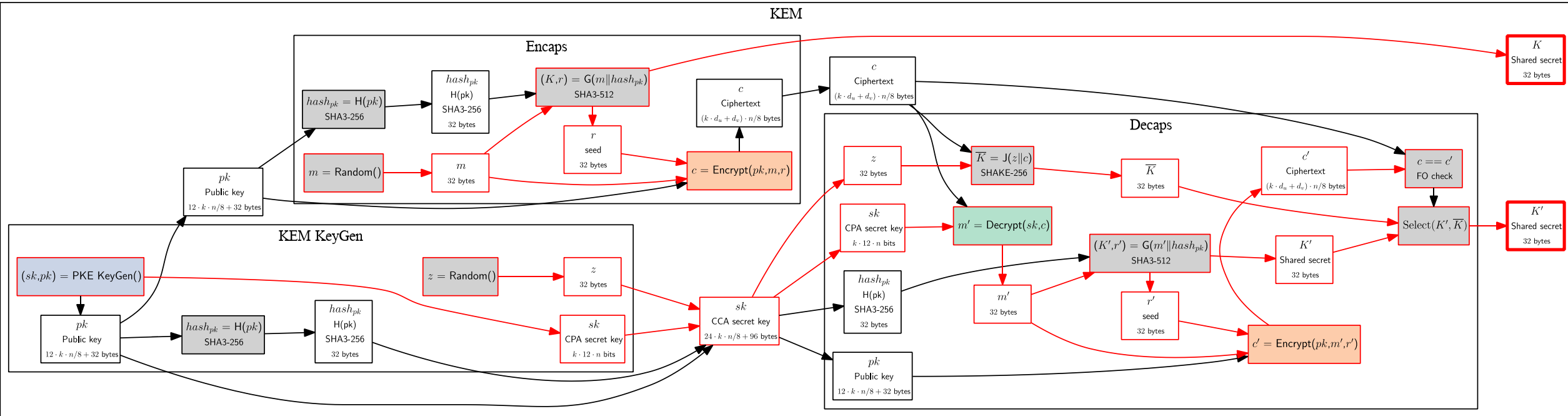
ML-KEM is indistinguishability under non-adaptative chosen ciphertext attacks (IND-CCA1).  
 ML-KEM is indistinguishability under adaptative chosen ciphertext attacks (IND-CCA2).

Almeida, José Bacelar, et al. "Formally Verifying Kyber: Episode V: Machine-Checked IND-CCA Security and Correctness of ML-KEM in EasyCrypt." Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2024.





# ML-KEM (Crystal-Kyber)



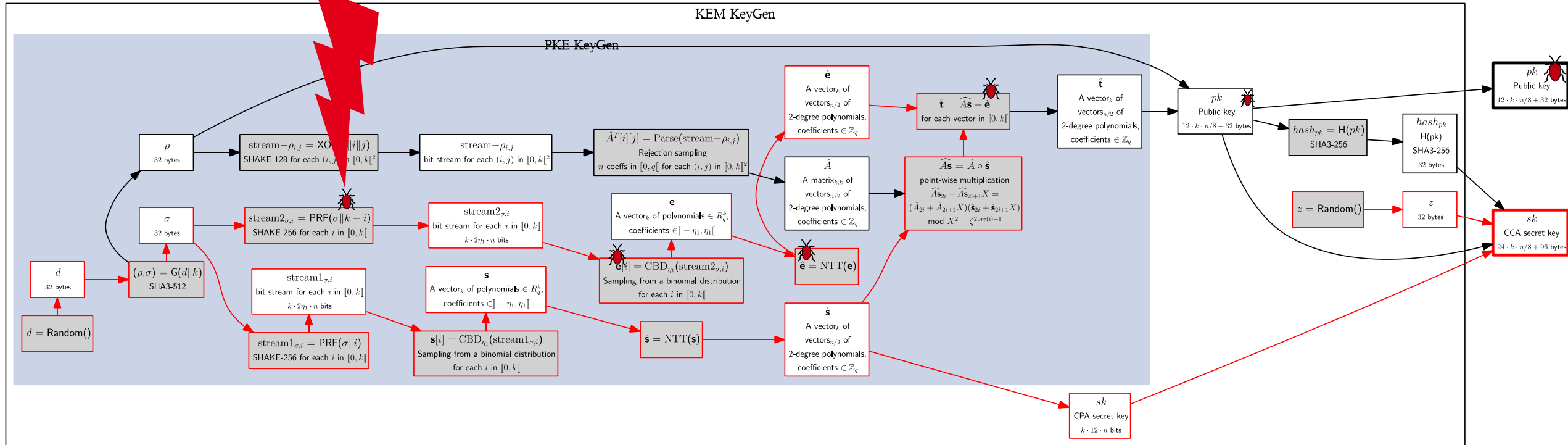
Fujisaki-Okamoto (FO) transform with implicit rejection  
except that the hash of the public key is fed as an additional argument into G

Fujisaki, Eiichiro, and Tatsuaki Okamoto. "Secure integration of asymmetric and symmetric encryption schemes." *Journal of cryptology* 26 (2013): 80-101.

<https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/C0D3W1KoINY/m/99klvydoAwAJ>

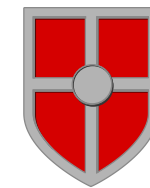
# PKE KeyGen, Fault injection attack

Encrypt can also be attacked



$$t = A \circledast s + e \quad \rightarrow \quad t = A \circledast s + s \quad \rightarrow \quad s$$

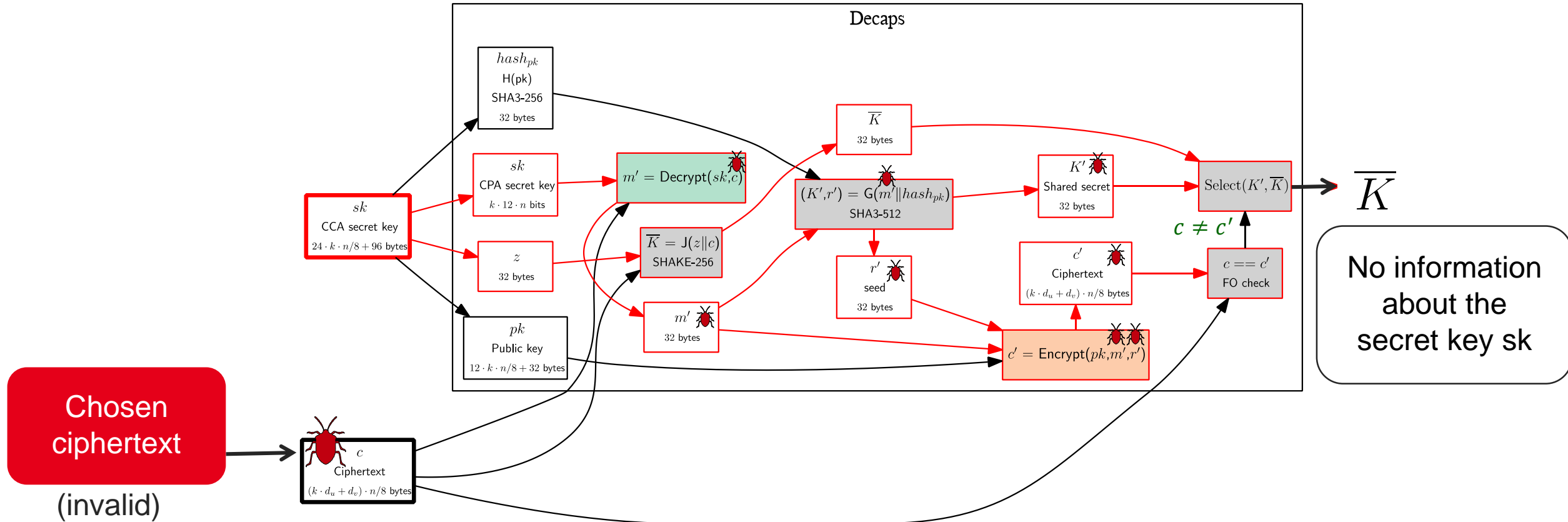
$$= (A + id) \circledast s$$



Check counter coin final value after all executions of PRF functions

Ravi, Prasanna, et al. "Number "not used" once-practical fault attack on pqm4 implementations of NIST candidates." *Constructive Side-Channel Analysis and Secure Design: 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3–5, 2019, Proceedings 10*. Springer International Publishing, 2019.  
Target = STM32F407, FI = EMFI.

# FO transform, Fault injection attack

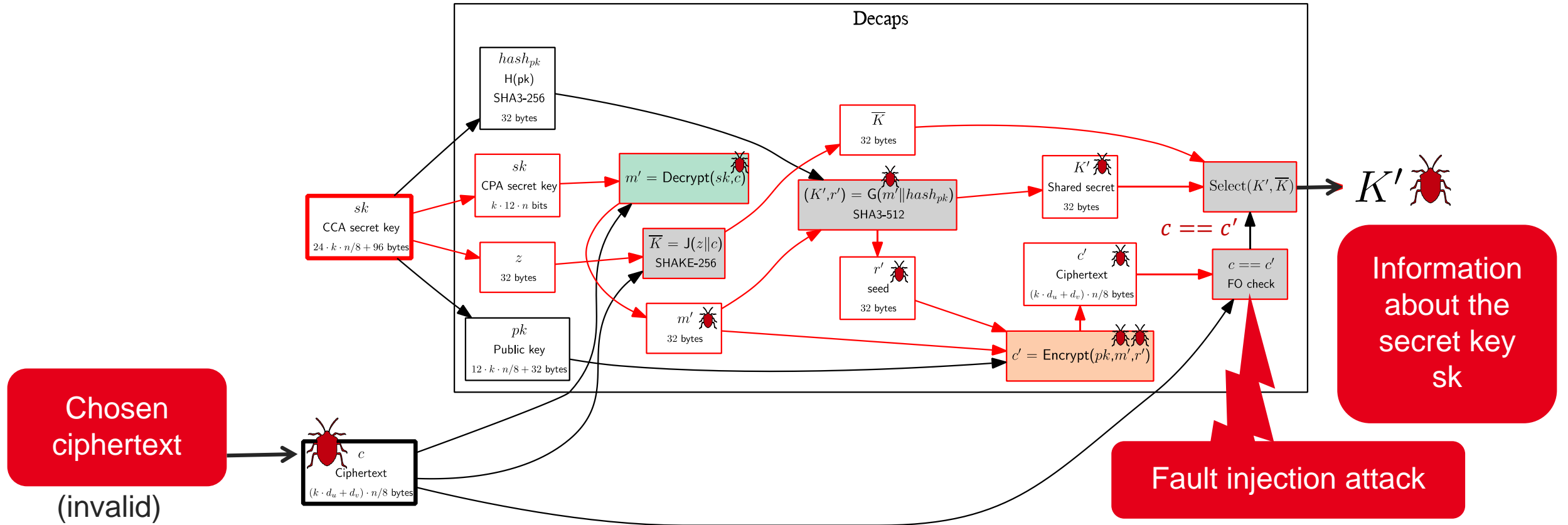


Fujisaki-Okamoto (FO) transform with implicit rejection  
except that the hash of the public key is fed as an additional argument into G

Fujisaki, Eiichiro, and Tatsuaki Okamoto. "Secure integration of asymmetric and symmetric encryption schemes." *Journal of cryptology* 26 (2013): 80-101.

<https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/C0D3W1KoINY/m/99klvydoAwAJ>

# FO transform, Fault injection attack



Compare  $K'$  to 2 candidates  $\Rightarrow$  1536 queries to recover  $sk$  for ML-KEM 512  
 Compare  $K'$  to  $2^a$  candidates  $\Rightarrow \frac{1536}{a}$  queries to recover  $sk$  for ML-KEM 512

 Redundancy  
 Ciphertext sanity check

Xagawa, Keita, et al. "Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates." *Advances in Cryptology—ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27*. Springer International Publishing, 2021.  
 Target = STM32F415, FI = CW Clock glitch.

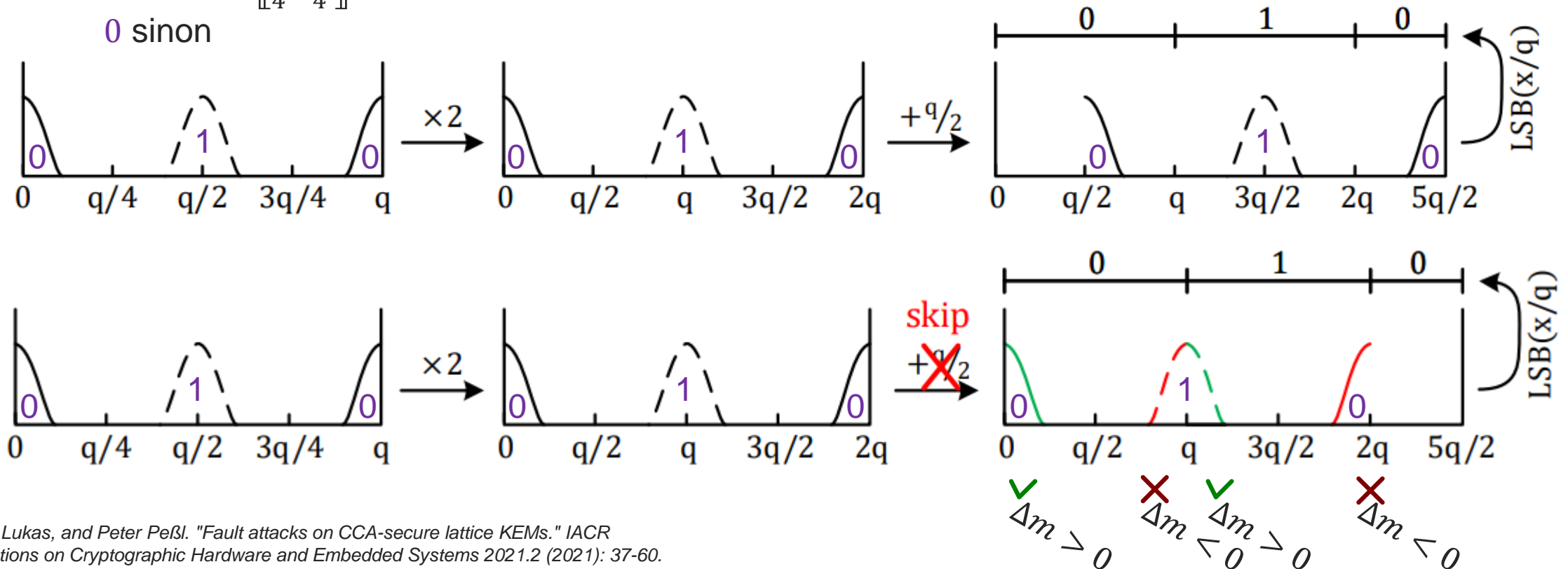
# Decrypt, Fault injection attack

$$vsu = m + \Delta m \quad \Delta m = e^T \odot r + e_2 + \Delta v - s^T \odot e_1 - s^T \odot \Delta u$$

$$\Delta m \in \left[ -\frac{q}{4}, \frac{q}{4} \right] \text{ for valid message decoding.}$$

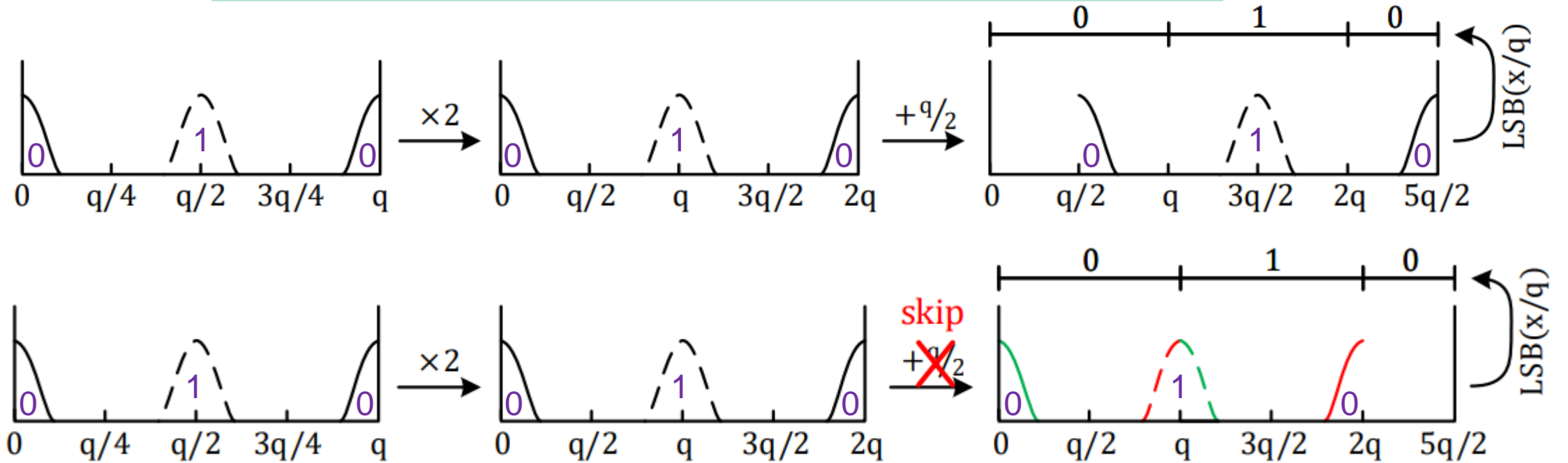
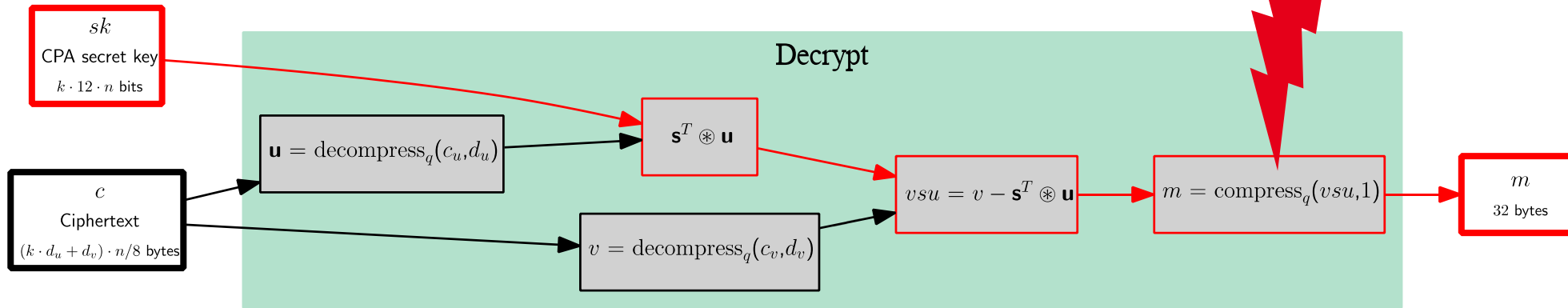
$$m[i] = 1 \text{ if } vsu \in \left[ \frac{q}{4}, \frac{3q}{4} \right]$$

0 sinon



Prokop, Lukas, and Peter Peßl. "Fault attacks on CCA-secure lattice KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems 2021.2 (2021): 37-60.  
Target = STM32F405, FI = CW Clock glitch.

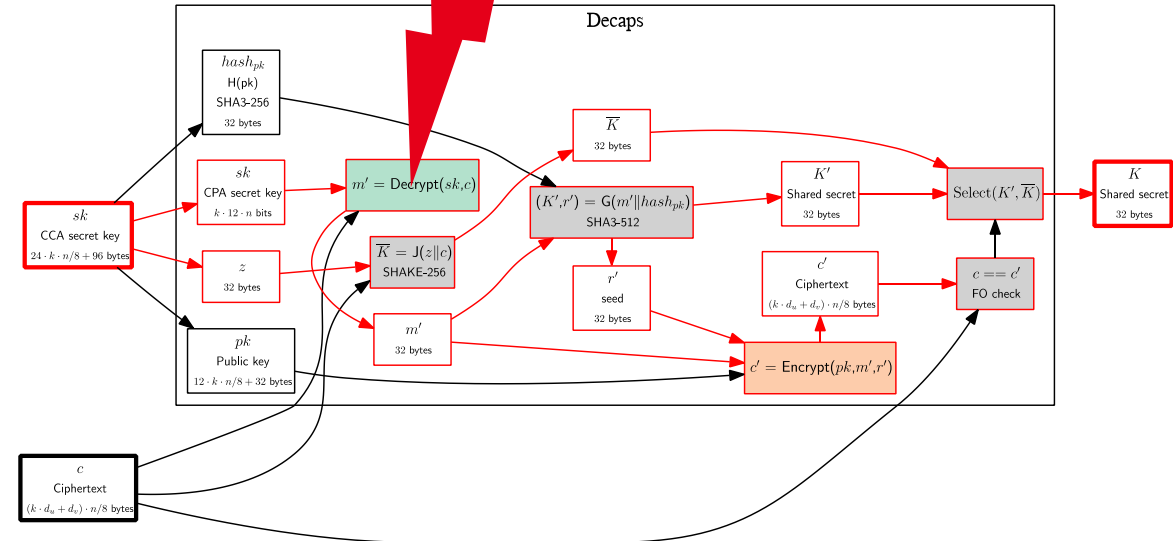
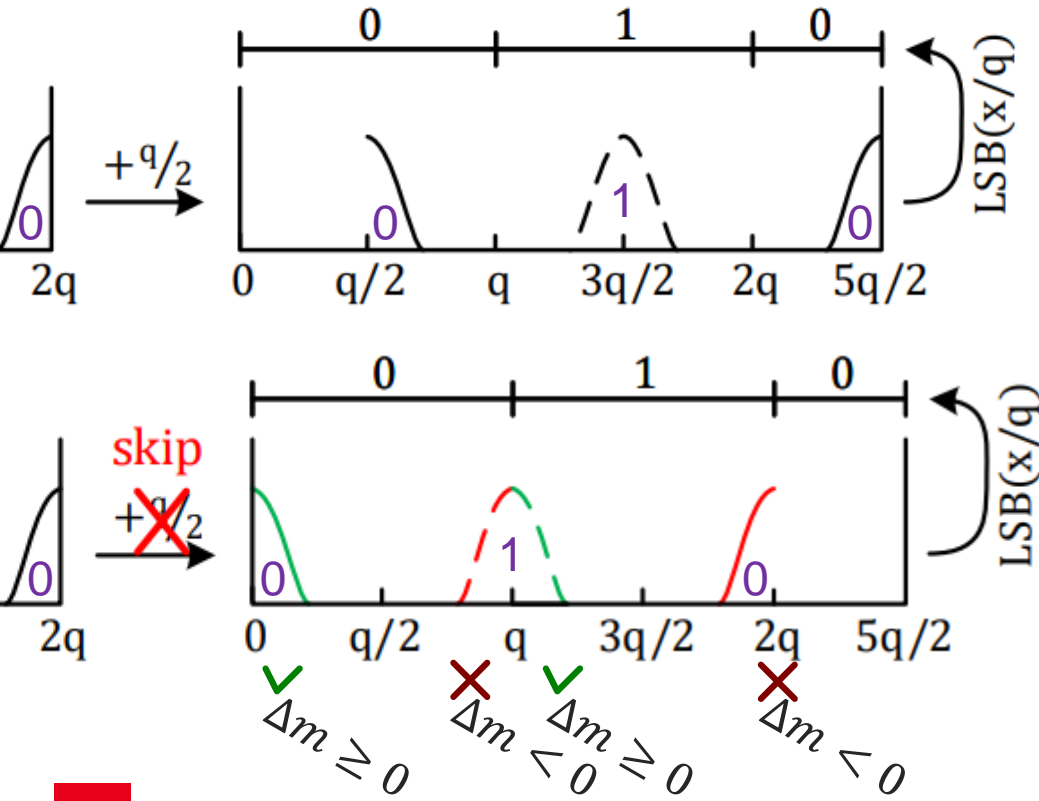
# Decrypt, Fault injection attack



Prokop, Lukas, and Peter Peßl. "Fault attacks on CCA-secure lattice KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems 2021.2 (2021): 37-60.  
 Target = STM32F405, FI = CW Clock glitch.

# Decrypt, Fault injection attack

$$\Delta m = e^T \circledast r + e_2 + \Delta v - s^T \circledast e_1 - s^T \circledast \Delta u$$



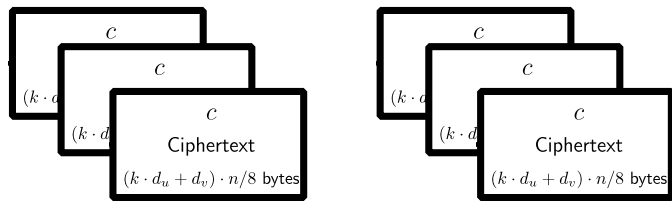
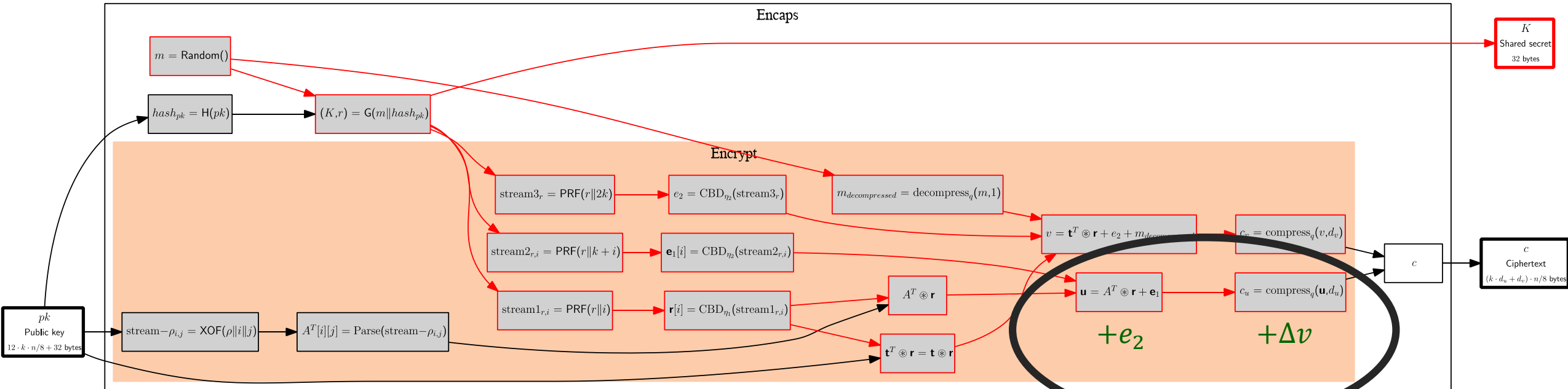
- ✓ Expected K :  
→ Ineffective fault →  $\Delta m \geq 0$
- ✗ Unexpected K:  
→ Effective fault →  $\Delta m < 0$

Prokop, Lukas, and Peter Peřl. "Fault attacks on CCA-secure lattice KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems 2021.2 (2021): 37-60. Target = STM32F405, FI = CW Clock glitch.

# Decrypt, Fault injection attack



Generate valid ciphertexts with  $|e_2 - \Delta v| < 10$



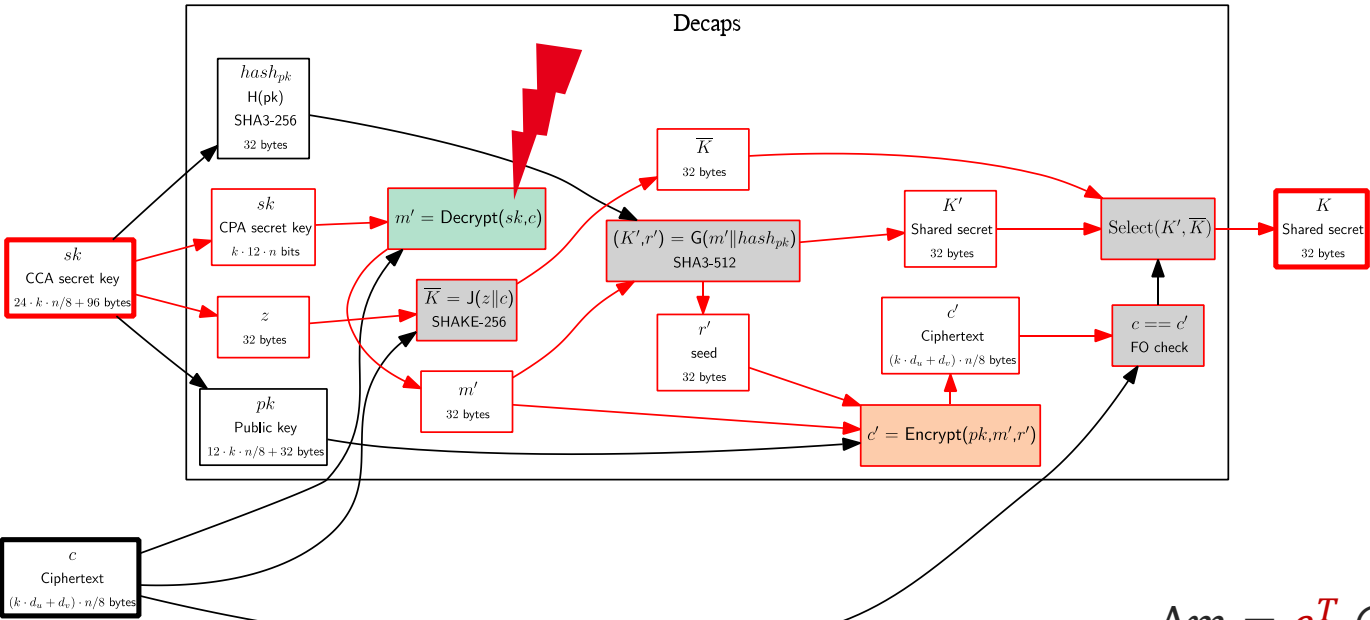
$$\Delta m = e^T \otimes r - s^T \otimes (e_1 - \Delta u) + (e_2 + \Delta v)$$

Small  $\Rightarrow$  More information about  $s$  and  $e$  in inequalities  $\Delta m < 0$

Prokop, Lukas, and Peter Peßl. "Fault attacks on CCA-secure lattice KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems 2021.2 (2021): 37-60. Target = STM32F405, FI = CW Clock glitch.



# Decrypt, Fault injection attack



$$\Delta m = e^T \circledast r - s^T \circledast (e_1 - \Delta u) + e_2 + \Delta v$$

✓ Expected K :

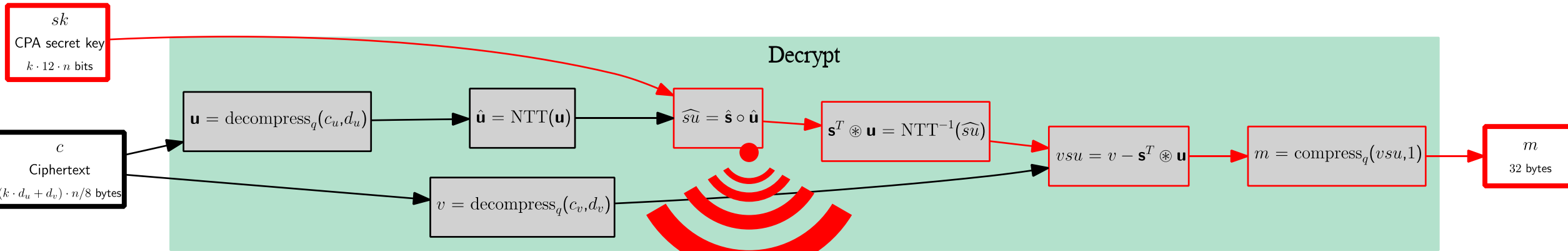
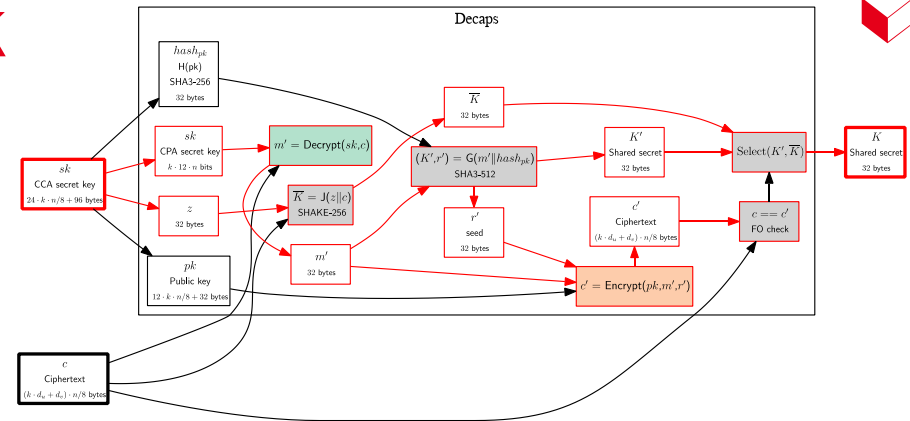
→ Ineffective fault →  $\Delta m \geq 0$  → Filter these inequalities that could be unsuccessful fault injection.

✗ Unexpected K:

→ Effective fault →  $\Delta m < 0$  → Solve the system of linear inequalities with belief-propagation techniques (60k or 125k Kyber512 decapsulations to recover  $s$  and  $e$ ).

Prokop, Lukas, and Peter Peßl. "Fault attacks on CCA-secure lattice KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems 2021.2 (2021): 37-60. Target = STM32F405, FI = CW Clock glitch.

# Decrypt, CPA side-channel attack



Leakage on  $\hat{s}$   $\Rightarrow$  Correlation Power Analysis (CPA) attack  
200 traces to recover  $\hat{s}$



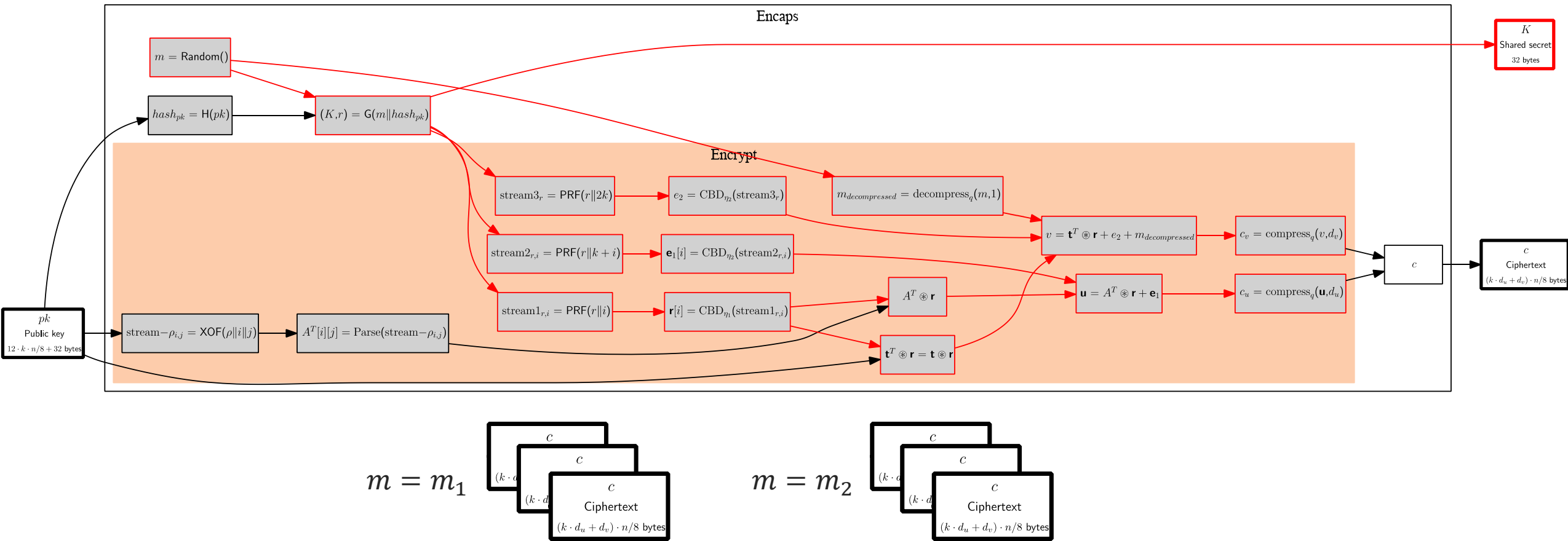
Masking

Mujdei, Catinca, et al. "Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication." ACM Transactions on Embedded Computing Systems 23.2 (2024): 1-23.  
Target = STM32F415, SCA = CW Power CPA.

# FO-Transform, Template side-channel attack

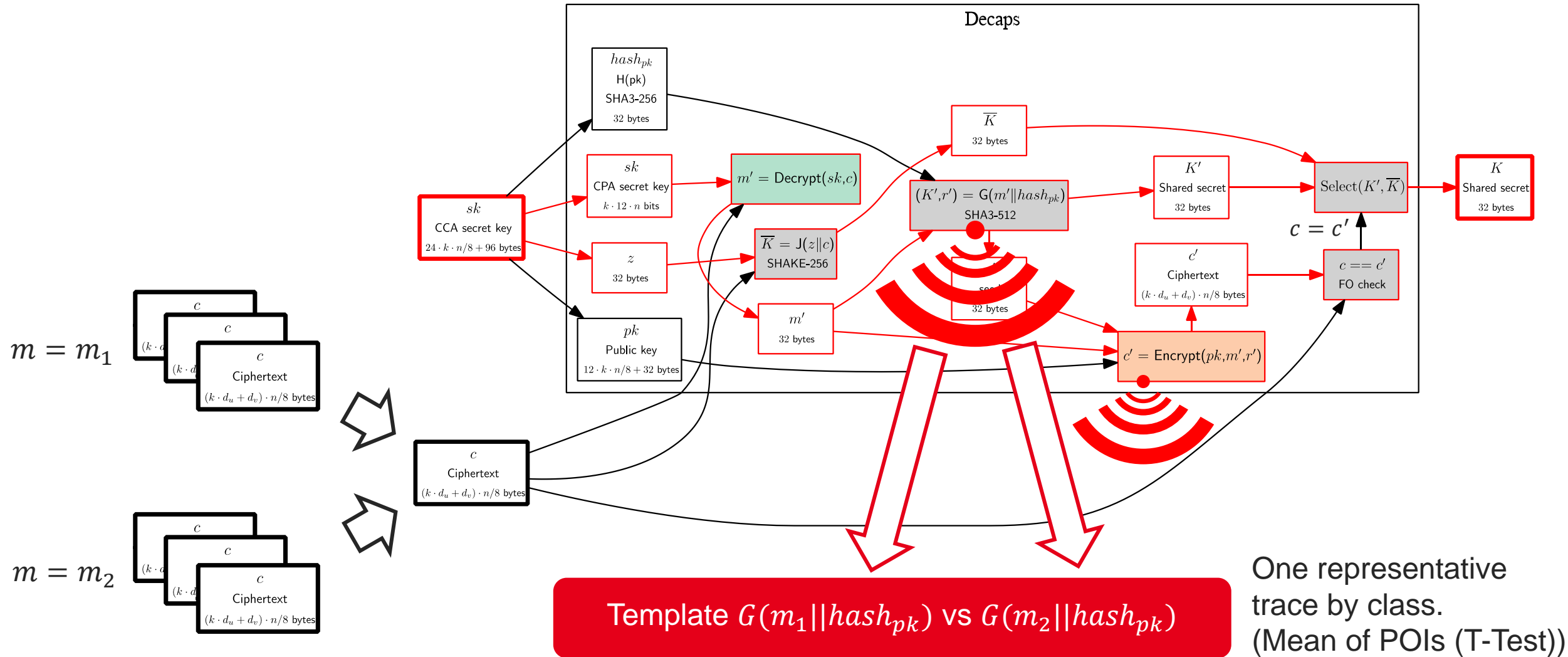


Build two classes of valid ciphertexts ( $m = m_1, m = m_2$ )



Ravi, Prasanna, et al. "Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs." IACR transactions on cryptographic hardware and embedded systems (2020): 307-335.  
Target = STM32F407, SCA = EM CPA.

# FO-Transform, Template side-channel attack

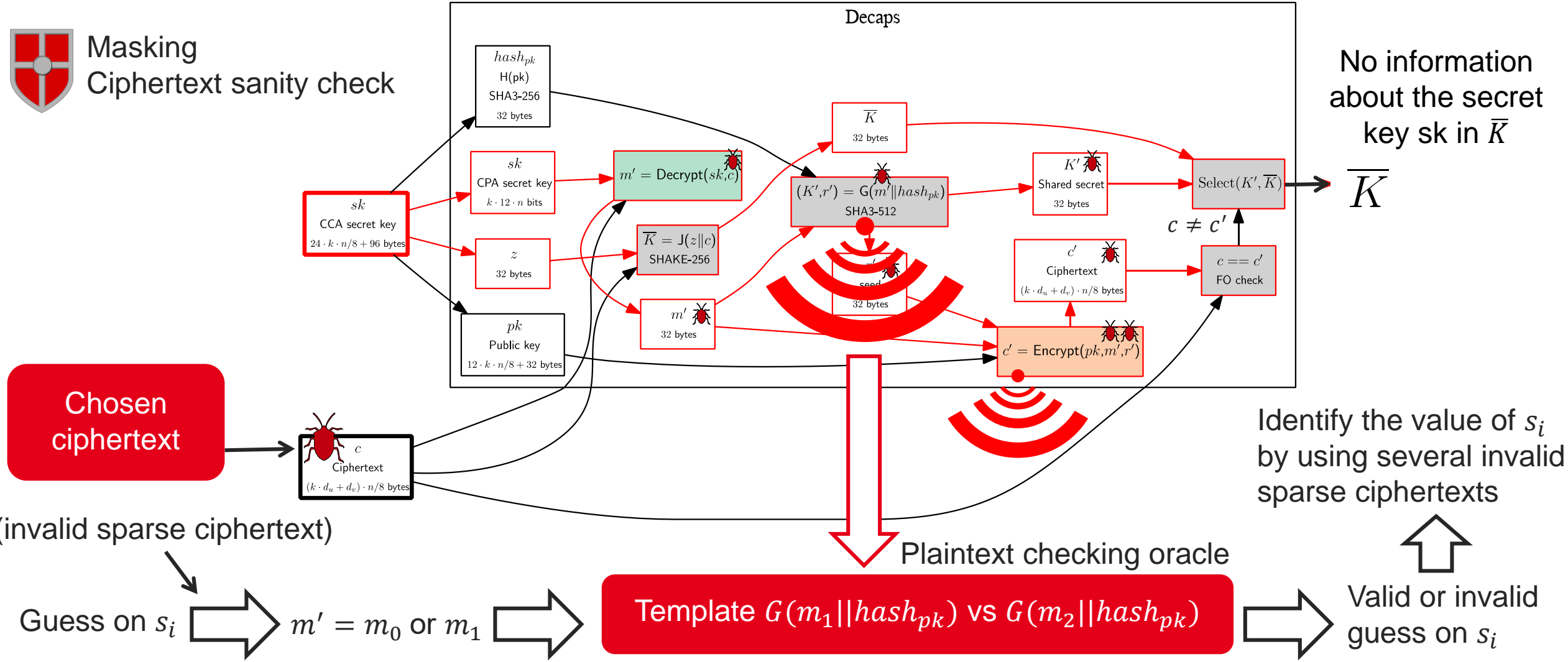


Ravi, Prasanna, et al. "Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs." IACR transactions on cryptographic hardware and embedded systems (2020): 307-335.  
Target = STM32F407, SCA = EM CPA.

# FO-Transform, Template side-channel attack



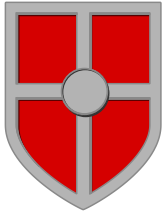
Masking  
Ciphertext sanity check



Ravi, Prasanna, et al. "Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs." IACR transactions on cryptographic hardware and embedded systems (2020): 307-335.  
Target = STM32F407, SCA = EM CPA.

# Conclusion

- Countermeasures must be combined to design secure ML-KEM implementation:



- Masking
- Shuffling
- Redundancy
- Sanity checks

- This overview is an introduction to some existing SCA and FI attacks on ML-KEM implementations:

- Warning: this overview is not an exhaustive one

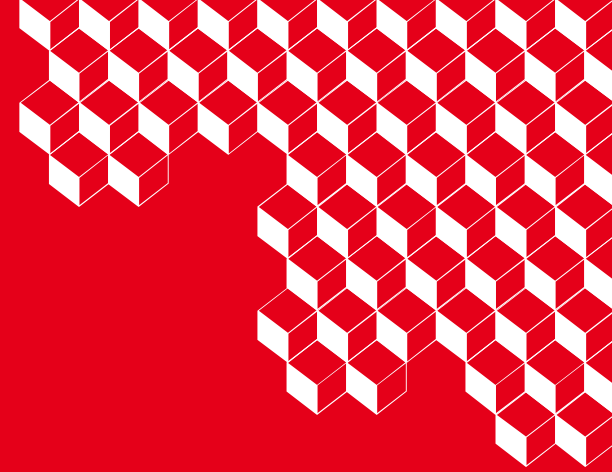
## Examples:

- *Hermelink, Julius, Peter Pessl, and Thomas Pöppelmann. "Fault-enabled chosen-ciphertext attacks on Kyber." Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22. Springer International Publishing, 2021.*
- *Ravi, Prasanna, et al. "Fiddling the twiddle constants-fault injection analysis of the number theoretic transform." IACR Transactions on Cryptographic Hardware and Embedded Systems (2023)*
- ...

- Warning: there are attacks against implementation with countermeasures

## Examples:

- **Soft-Analytical Side Channel Attack on NTT to recover secret from masked ML-KEM implementations**  
*Pessl, Peter, and Robert Primas. "More practical single-trace attacks on the number theoretic transform." Progress in Cryptology–LATINCRYPT 2019: 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2–4, 2019, Proceedings 6. Springer International Publishing, 2019.*
- *Qiao, Zehua, et al. "When NTT Meets SIS: Efficient Side-channel Attacks on Dilithium and Kyber." Cryptology ePrint Archive (2023).*
- ...



**Simon Pontié**

**[simon.pontie@cea.fr](mailto:simon.pontie@cea.fr)**