NIST Lightweight Cryptography Workshop 2020

Active and Passive Side-Channel Key Recovery Attacks on Ascon

Keyvan Ramezanpour [1,2]

Abubakr Abdulgadir [3]

William Diehl [1]

Jens-Peter Kaps [3]

Paul Ampadu [2]

[1] Signatures Analysis Laboratory (SAL), Virginia Tech, Blacksburg, VA 24060

[2] Multifunction Integrated Circuits and Systems Group (MICS), Virginia Tech, Blacksburg, VA 24060

[3] Cryptographic Engineering Research Group (CERG), George Mason University, Fairfax, VA 22033

October 19-21, 2020

Outline

- Introduction to side-channel analysis (SCA)
- Attack setup for active and passive SCA
- Key recovery attacks on Ascon
  - Active SCA with Voltage Glitch on FPGA
  - Passive SCA with power measurements on FPGA
- Results
- Conclusions

Introduction

Security in Internet-of-Things (IoT)

- Authenticated ciphers are trending for lightweight applications;
  - *Confidentiality*, data *integrity* and *authentication* with *single* algorithm.
  - Possible lower overhead of security protocol implementation in hardware/software.

- NIST LWC Competition:
  - Assessing security of candidates for lightweight cryptography (LWC) and Hash functions, and
  - Robustness of the implementations (and ease of inclusion of countermeasures) against side-channel analysis (SCA).
- Ascon authenticated cipher:
  - The first choice of CAESAR committee for lightweight use case (Feb. 2019).
  - Selected as a candidate for the second round of NIST LWC Competition.
- We demonstrate vulnerability of Ascon to both active and passive SCA attacks.

Side-Channel Analysis (SCA)

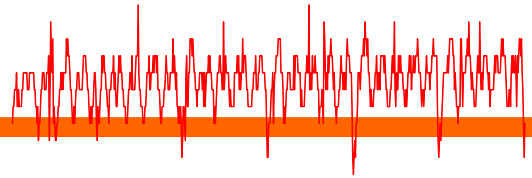
- **Physical *Implementation* of cryptographic algorithms leak secret information**
  - **Side-channel analysis (SCA) exploits runtime signatures to infer secret information.**

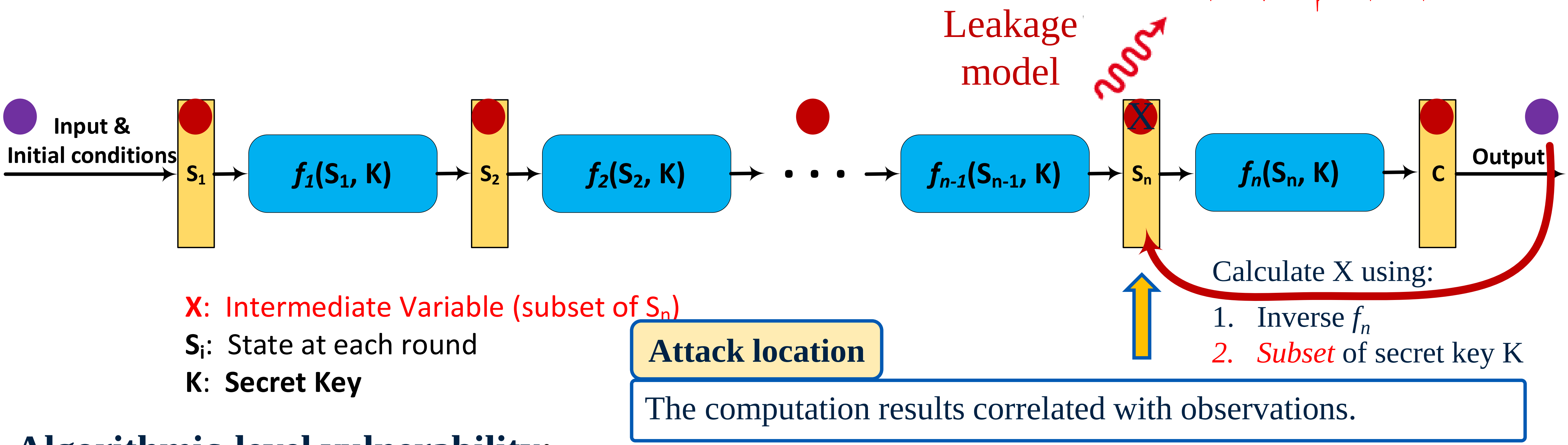
Two categories of SCA analysis:

1. **Passive SCA: measure signals and correlate with secret;**
   - Power Analysis (PA) and electromagnetic (EM) Analysis;
   - Power consumption of device is correlated with processed (secret) data.
2. **Active SCA: induce a stimulus and observe data-dependent behavior;**
   - Fault Injection Analysis (FIA): inject fault during execution with known properties;
     - *Only* correct key guess exhibits expected fault properties.

Key Recovery with SCA

Passive SCA:
Power Analysis (PA)





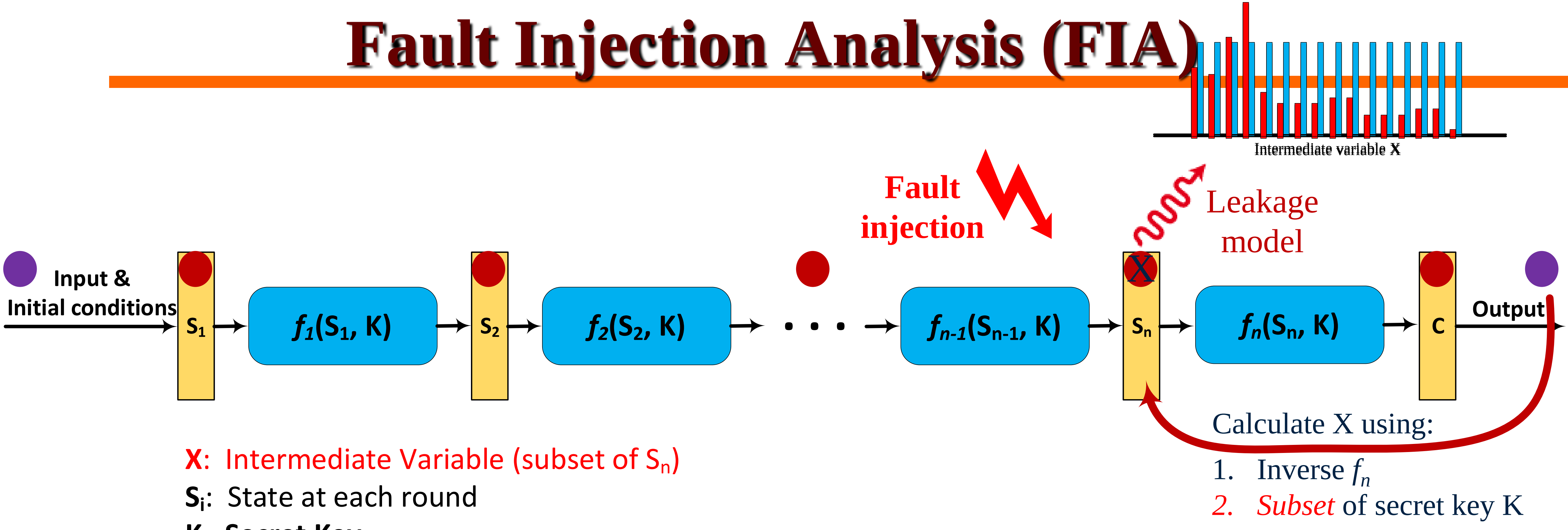
Algorithmic-level vulnerability:

- A subset of key K is sufficient to calculate intermediate variable X from input or output.

Implementation-level vulnerability:

- Power consumption during execution correlated with data.

Active SCA:
Fault Injection Analysis (FIA)



X: Intermediate Variable (subset of S_n)

S_i: State at each round

K: **Secret Key**

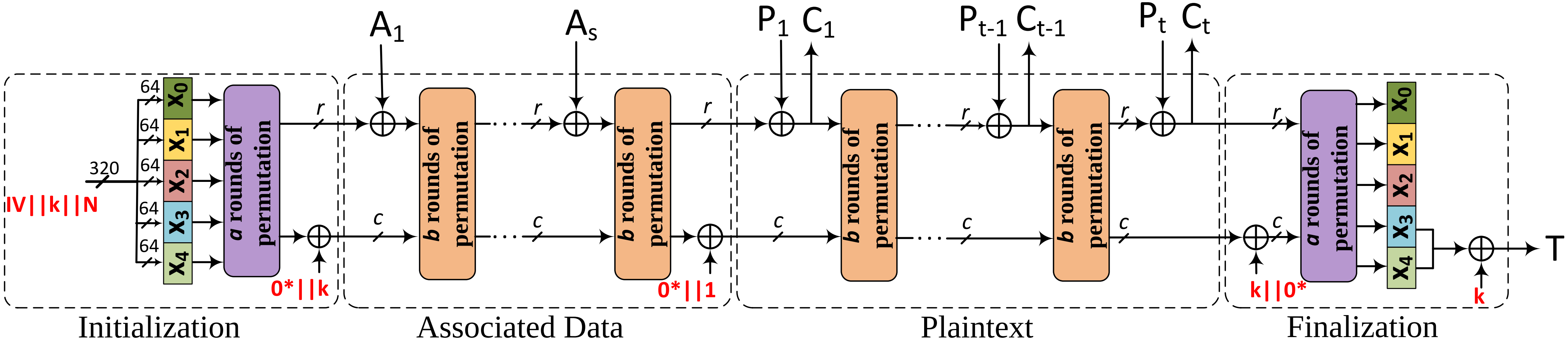
Algorithmic-level vulnerability:

- A subset of key K is sufficient to calculate intermediate variable X from input or output.

Implementation-level vulnerability:

- Data distribution under fault injection is different from max-entropy distribution.

Ascon Authenticated Cipher



k: 128-bit secret key

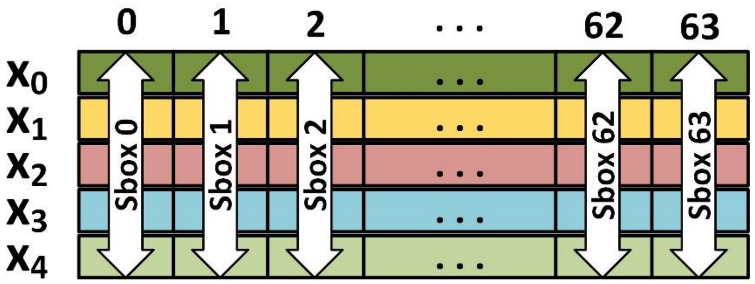
IV: Initial Vector **N**: Nonce

$\{A_1, \dots, A_s\}$: Blocks of associated data

$\{P_1, \dots, P_t\}$: Blocks of plaintext

$\{C_1, \dots, C_t\}$: Blocks of ciphertext

T: 128-bit tag

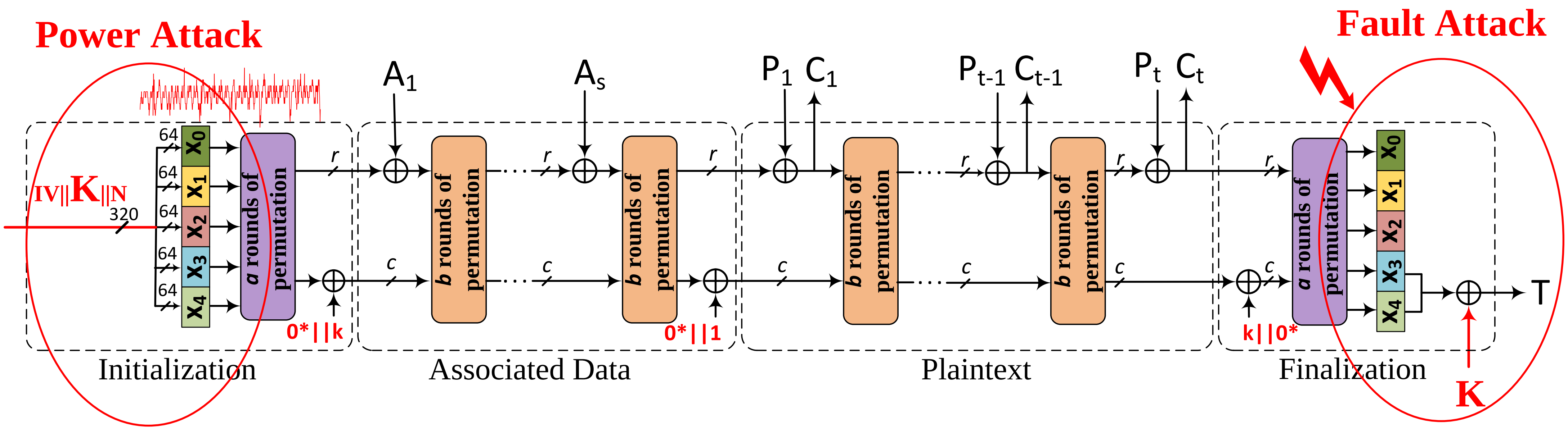


Diffusion (matrix notation):

$$\boldsymbol{\Sigma}_i(\boldsymbol{x}_i) = (\mathrm{L}_i \boldsymbol{x}_i) \bmod 2, \quad i = 0, 1, \dots, 4$$

SCA Attack Setup

SCA Attack on Ascon



Vulnerability to fault attack (active SCA):

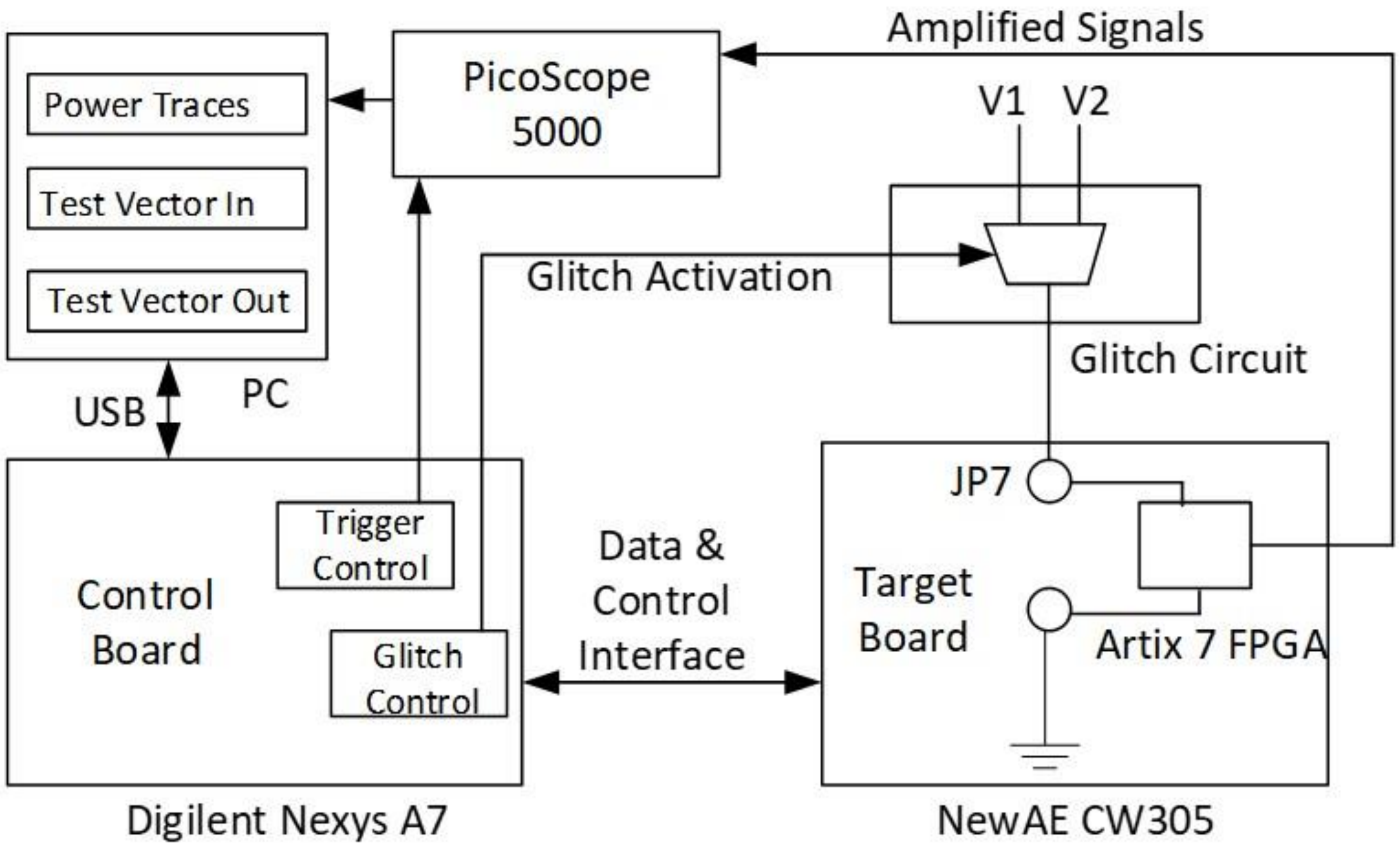
- Addition of secret key at the end of Finalization for *authentication tag* generation.

Vulnerability to power attack (passive SCA):

- Initialization of cipher state with secret key at the beginning of Initialization Stage.

Attack Setup

FOBOS: Flexible Open-source workBench fOr Side-channel analysis.



Target board (under attack):

Artix-7 FPGA executing Ascon.

Control board:

Data, configuration and synchronization.

Power attack:

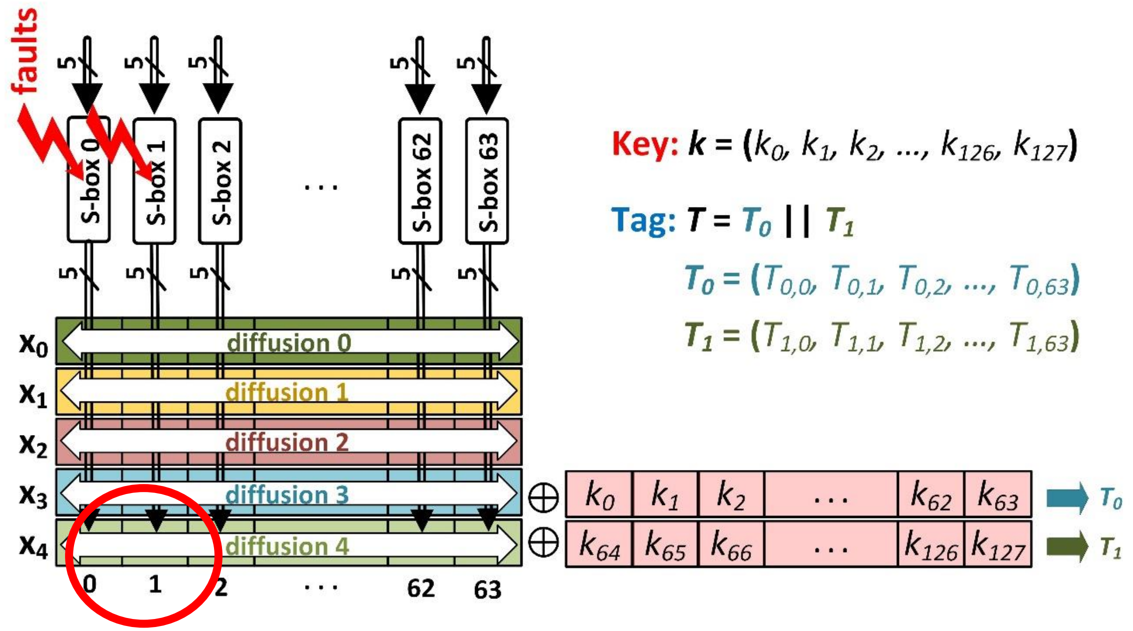
PicoScope 5000 measuring power consumption of target FPGA chip.

Fault attack:

Single-pole double-thru (SPDT) analog switch for switching V_{DD} of target FPGA chip.

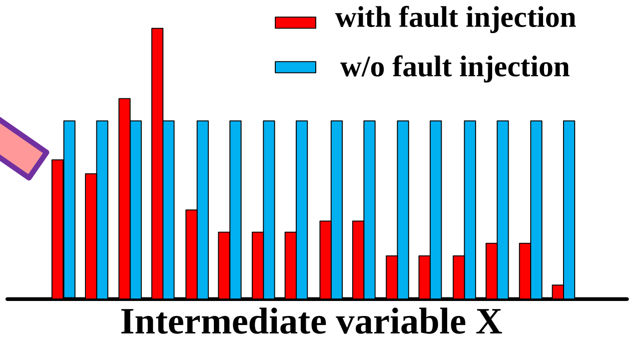
Fault Attack on Ascon (Active SCA)

Statistical Ineffective Fault Analysis (SIFA)



Intermediate Variable

Inspect *distribution* of (correct) data under fault injection

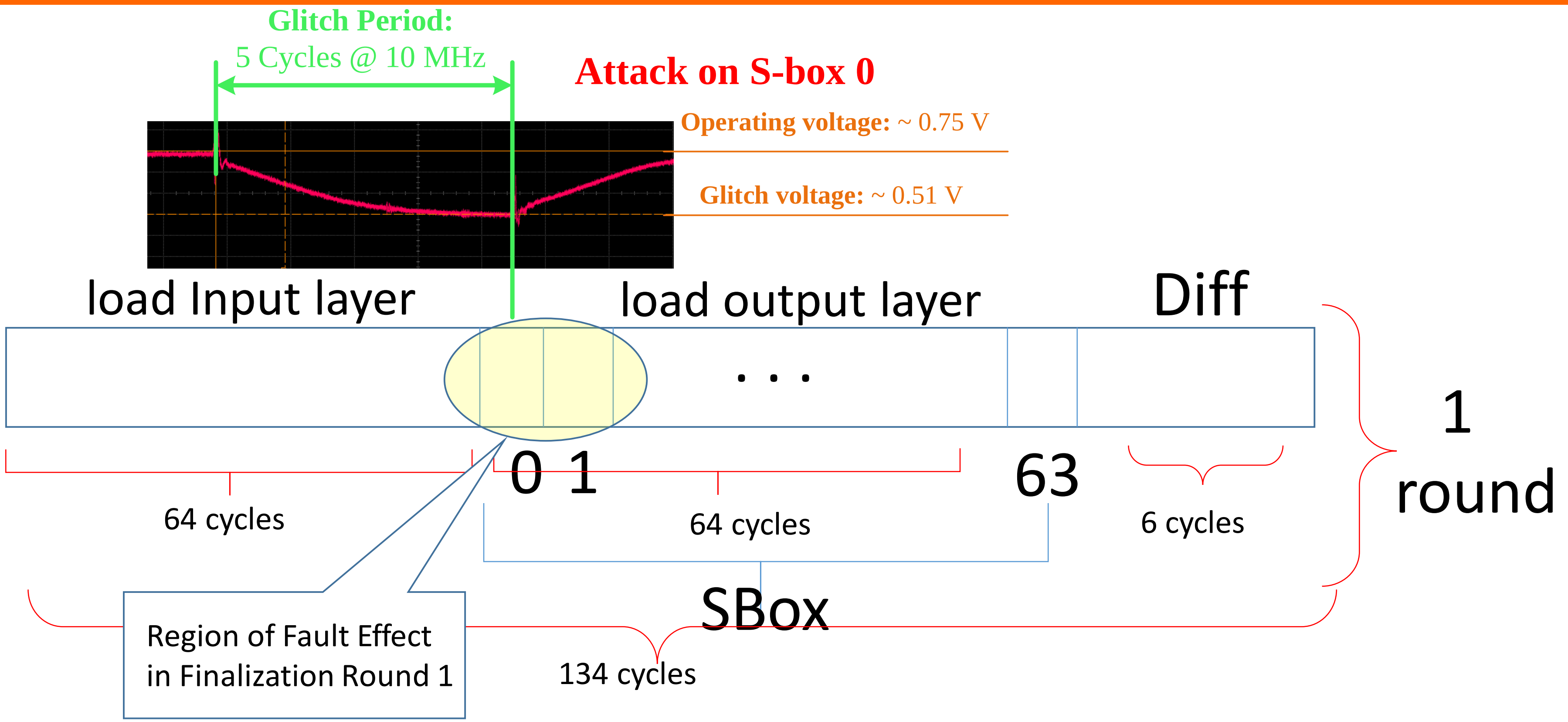


- Inject fault at last round of finalization.
- Collect multiple outputs (tags) for random inputs.
- Requires only ***correct*** outputs. (successful even if countermeasures suppress faulty values.)
- For every key guess:
    1. Calculate the output of Sbox pairs under attack.
    2. Find the distribution of calculated data.
    3. Calculate the SEI* of data distribution.
- Key guess with highest SEI is the correct key.

*SEI: Square Euclidean Imbalance

K. Ramezanpour, P. Ampadu, and W. Diehl, "A Statistical Fault Analysis Methodology for the Ascon Authenticated Cipher," *HOST* 2019.
K. Ramezanpour, P. Ampadu, and W. Diehl, "FIMA: Fault Intensity Map Analysis," *COSADE'19*. Springer, Cham, 2019.

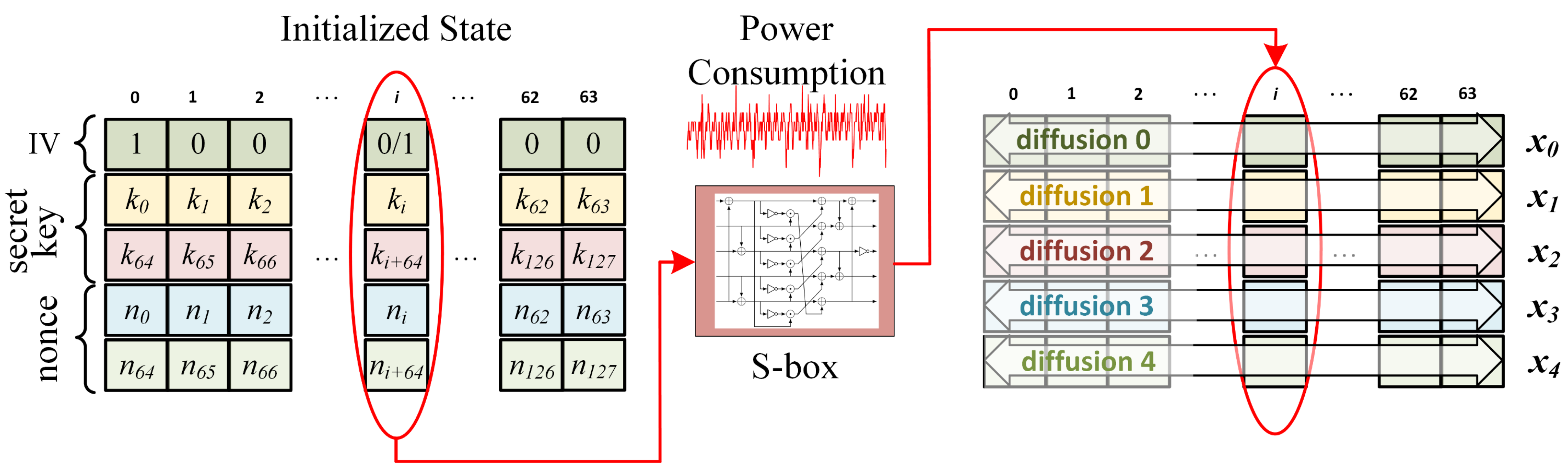
SIFA Attack on Ascon with Voltage Glitch



- Set operation conditions at high frequency/low voltage corner.
- <u>Our setup</u>: Artix-7 FPGA executing Ascon with V_{DD}=0.75V @ 10 MHz without errors.
- Reducing V_{DD} to 0.51V (with SPDT switch) results in desired fault effect.

Power Attack on Ascon (Passive SCA)

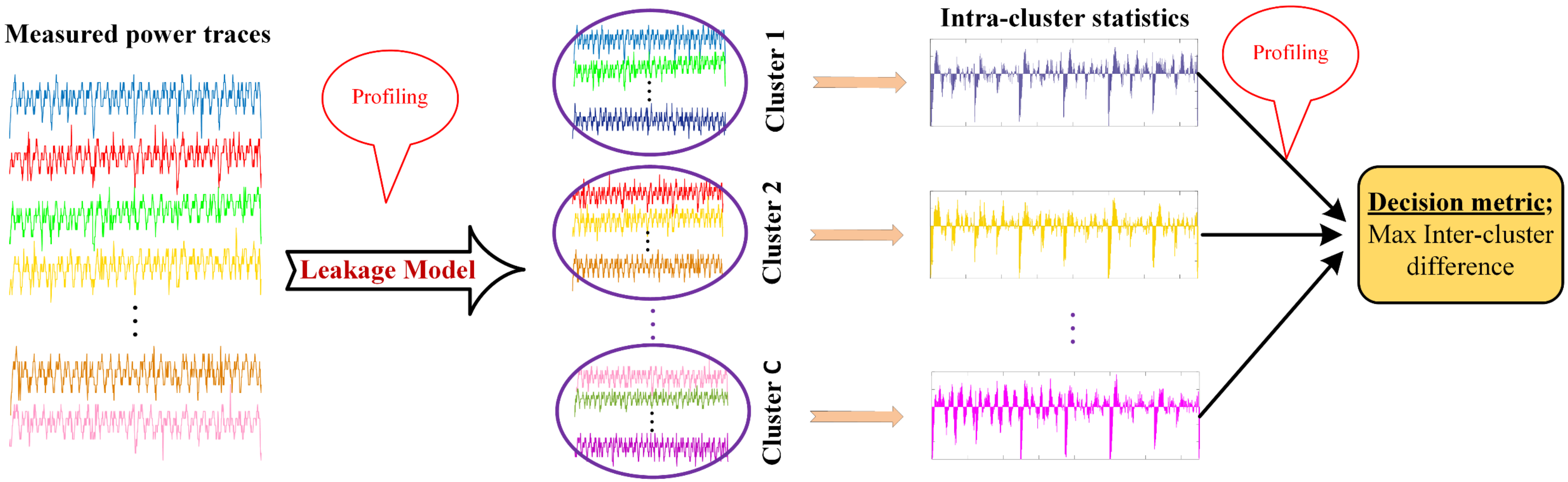
Power Attack on Ascon



- **Cipher state initialized with initial vector (IV), secret key and nonce.**
- **Nonce values are known in the proposed power attack.**
- **Bit-sliced implementation of S-box with one S-box operation at every clock cycle (lightweight implementation).**

K. Ramezanpour, P. Ampadu, and W. Diehl, "SCAUL: Power Side-Channel Analysis with Unsupervised Learning," *arXiv preprint arXiv:2001.05951* (2020).

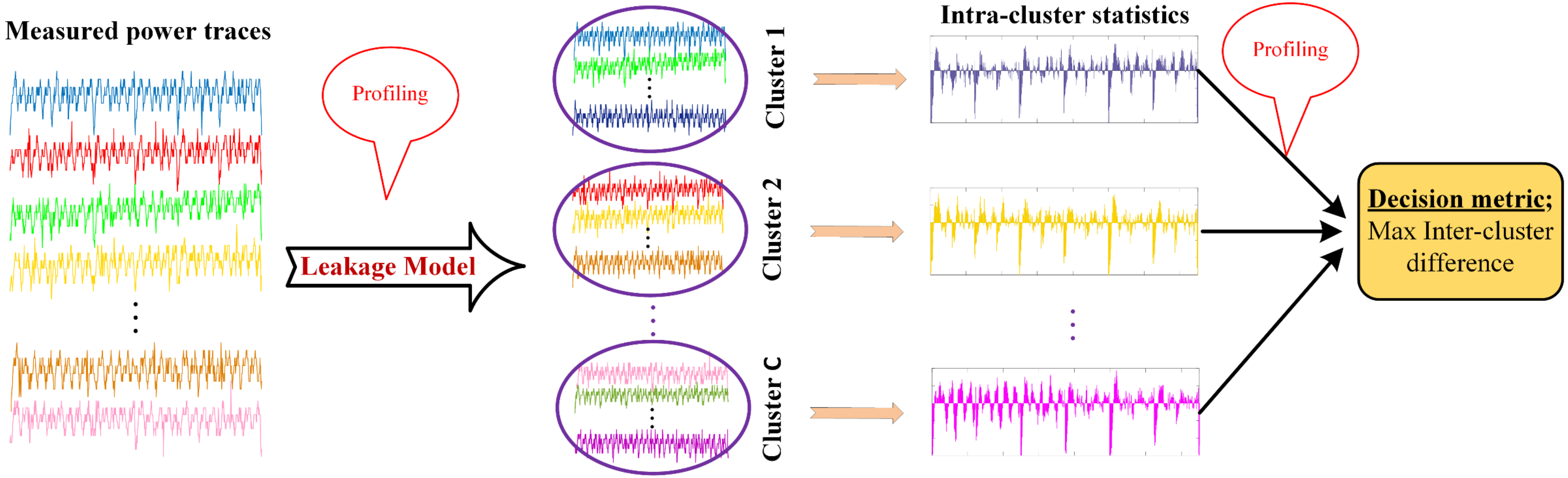
Clustering-based PA Techniques



Available information:

- A set of power traces with the corresponding input data (nonce values in Ascon).
- A leakage model describing the relationship between power traces and intermediate variable.
- Intermediate variable can be calculated from the input data and a subset of secret key.

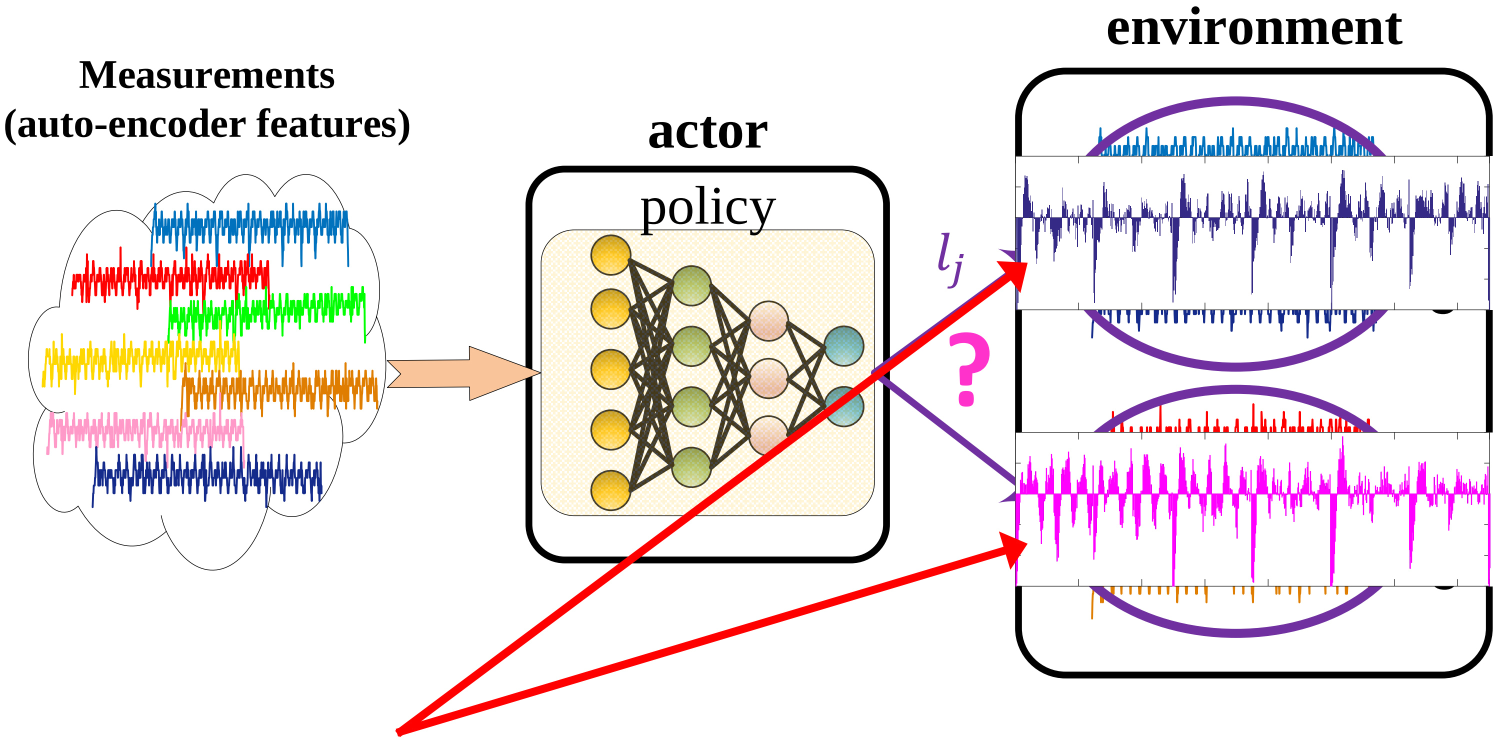
Clustering-based PA Techniques



For every key candidate:

1. Calculate intermediate variable corresponding to all power traces.
2. Calculate the value of the leakage model using the intermediate variables.
3. Cluster power traces in which similar power traces exhibit similar leakage values.
4. Calculate the difference between a statistics (e.g. mean in 1^{st} order SCA) of power traces in clusters.
5. The inter-cluster difference of the statistics is the measure for ranking key candidates.

Side-Channel Analysis with Reinforcement Learning (SCARL)



State: inter-cluster difference

Reward: $r(s_t, a_t) = \max(|s_t|) - \mathcal{D}_{KL}(Q||P)$

Max difference — Even assignment

Leakage model (generic):

$$L(X) = \alpha_0 + \sum_{U \in \mathbb{F}_2^m \setminus \{0\}} \alpha_U X^U + \epsilon$$

Estimated leakage for every key candidate:

$$\alpha_U^* = \min_{\alpha_U} \mathrm{E}_j \left[|L(X_j^*) - l_j|^2 \right], \; U \in \mathbb{F}_2^m$$

Low-order leakage:

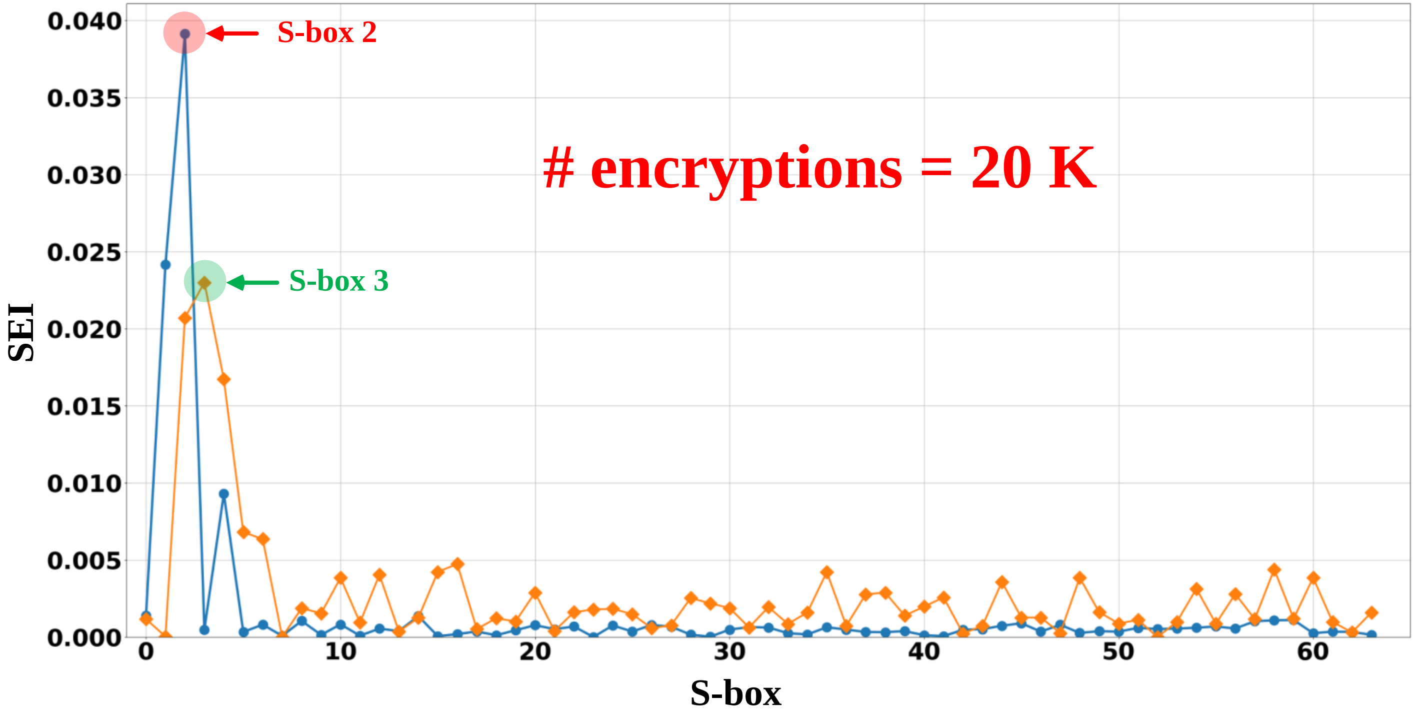
$$l_j^* = \alpha_0^* + \sum_{U \in \mathbb{F}_2^m \setminus \{0\},\, HW(U) \leq m_0} \alpha_U^* (X_j^*)^U$$

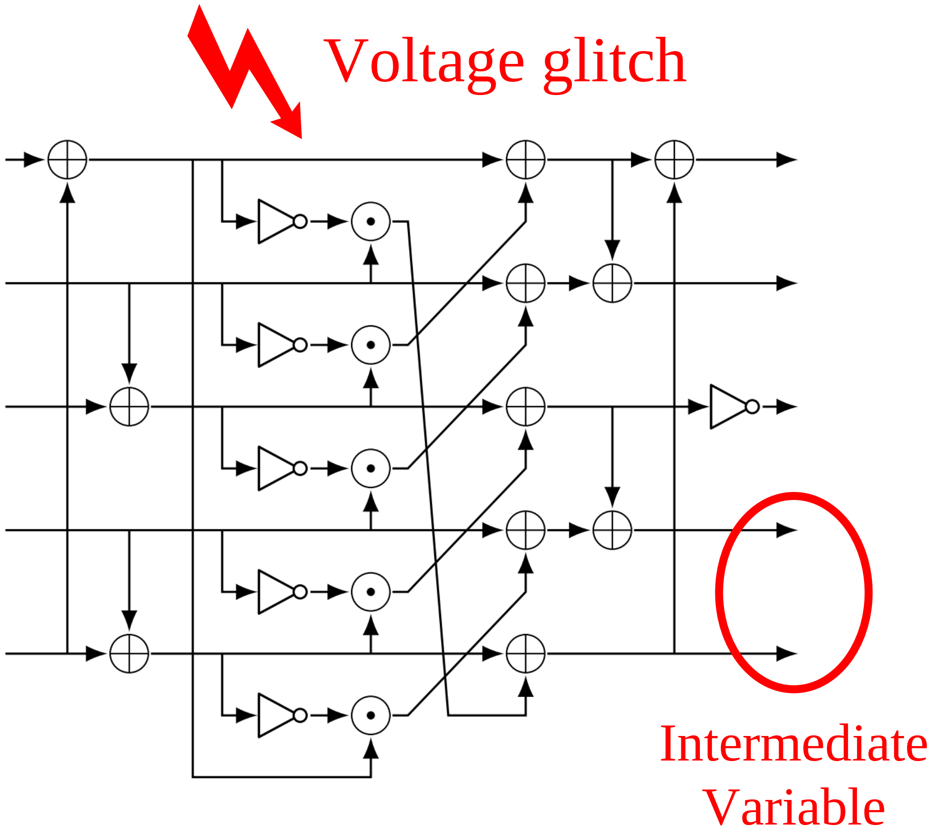
K. Ramezanpour, P. Ampadu, and W. Diehl, "SCARL: Side-Channel Analysis with Reinforcement Learning on the Ascon Authenticated Cipher," *arXiv preprint arXiv:2006.03995* (2020).

Results

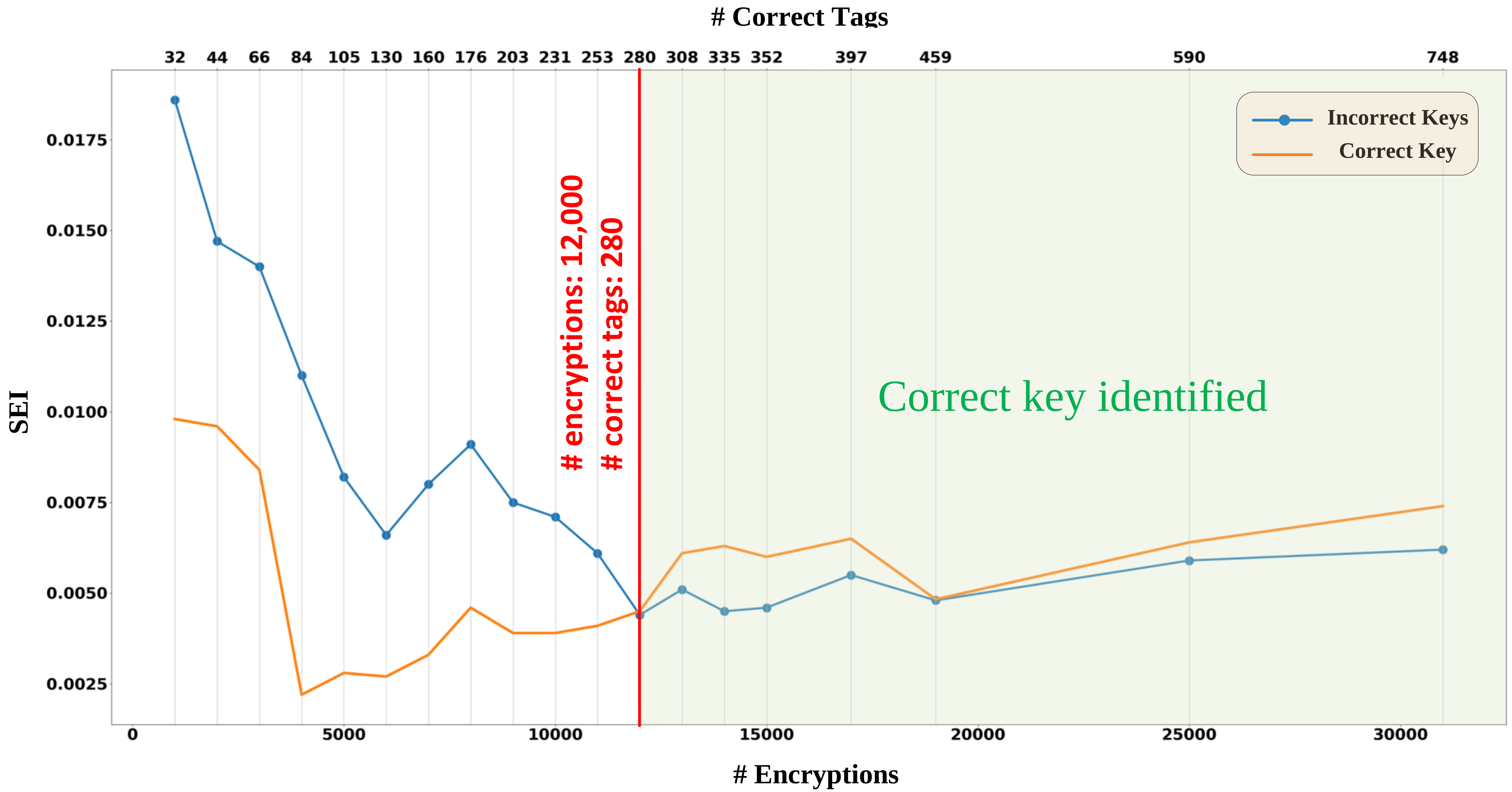
Results of Voltage Glitch on Ascon

- Intermediate Value: 2 least significant bits at output of S-box under attack.
- Bias of intermediate values with fault locations at S-boxes 3 & 4:

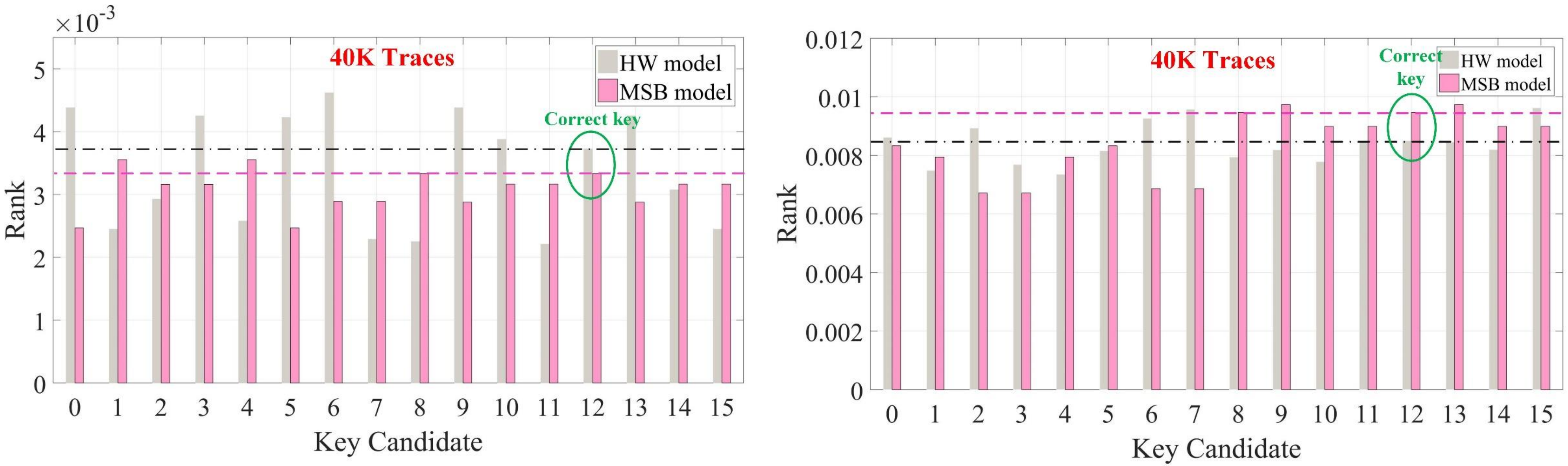




Key Recovery with Voltage Glitch



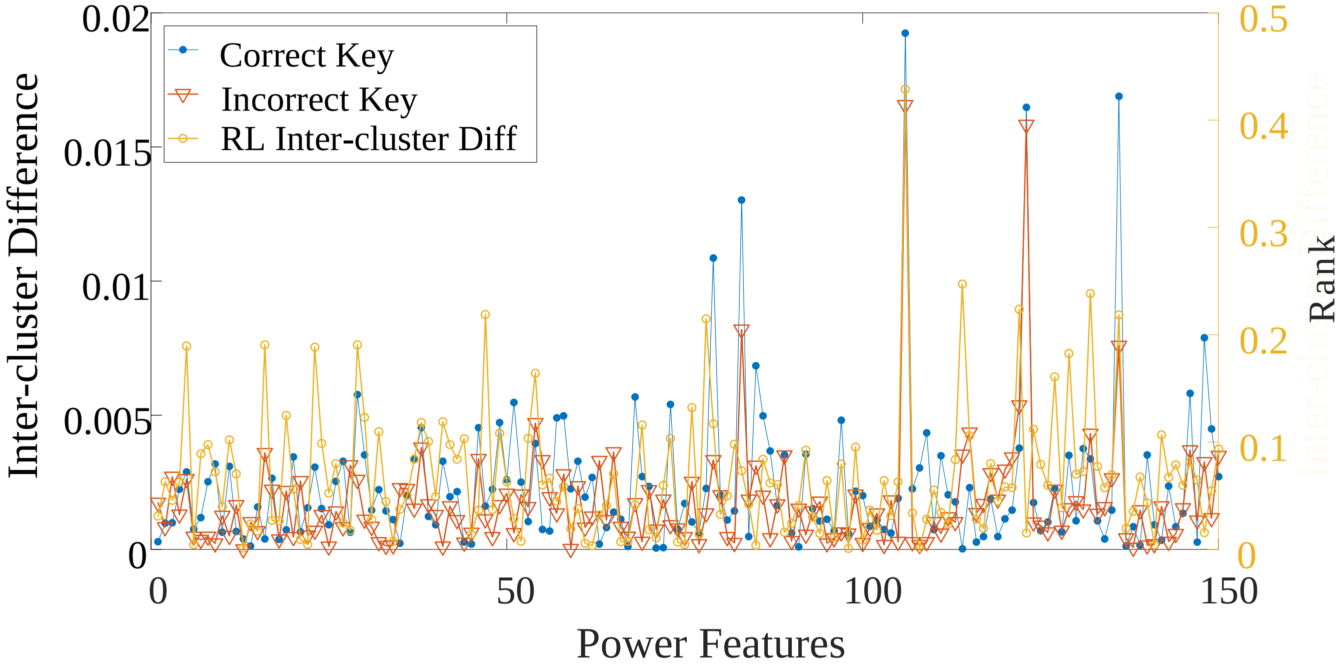
Classical PA Attacks on Ascon



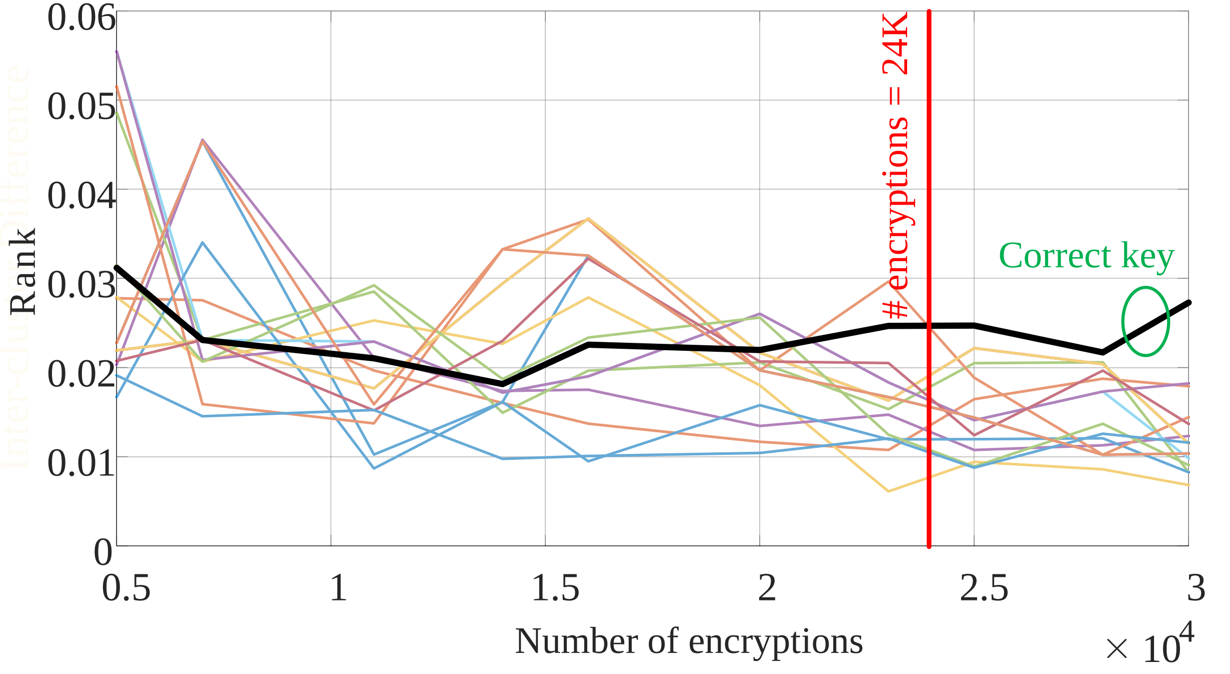
(a) DPA **(b) CPA**

- **Differential power analysis (DPA) and correlation power analysis (CPA) with two different leakage models:**
  - **Hamming weight (Hw) and most significant bit (MSB) of intermediate variable (S-box output) correlated with power traces.**
- **Both techniques fail to detect the correct key with 40K traces.**

SCARL Attack on Ascon



(a) Inter-cluster difference



(b) Rank vs. data size

- **SCARL attack based on deep learning able to recover the secret key with 24K traces.**

Conclusions

- Protection of cryptographic hardware implementations is critical for security.

- Algorithmic properties and implementation vulnerability of ciphers are exploited in side-channel analysis to recover the Ascon secret key.
  - Addition of secret key for tag generation exploited in fault injection attack.
  - Initialization of the cipher state with secret key exploited in power attack.

- Voltage glitch on FPGA implementation of Ascon induces significant bias into the S-box outputs which is exploited in a fault attack.
- Reinforcement learning technique more efficient than DPA or CPA.

Thank you!