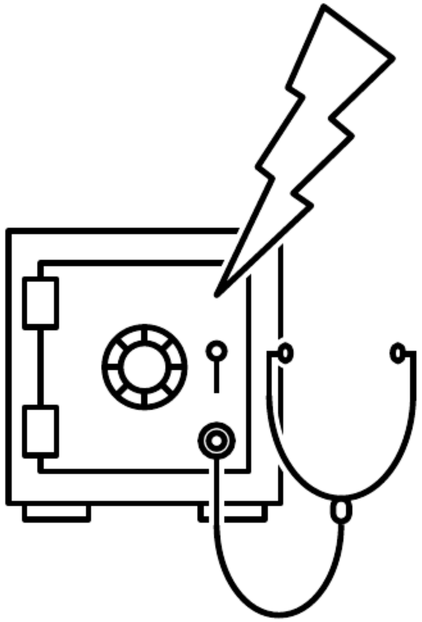
Statistical Ineffective Fault Attacks

Florian Mendel

joint work with:

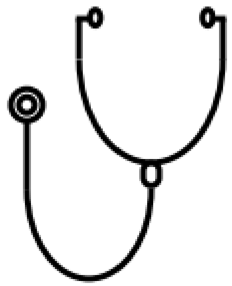
Christoph Dobraunig, Maria Eichlseder, Thomas Korak, Hannes Groß, Stefan Mangard, Robert Primas

Motivation

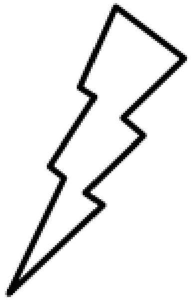


Building cryptographic implementations is challenging

- Requires usage of secure cryptographic schemes
- Additional defences mechanisms against implementation attacks



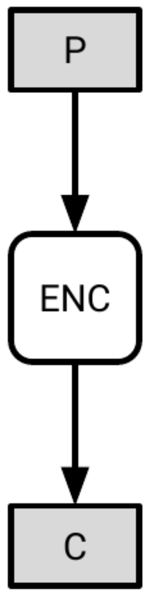
Power Analysis



Fault Attacks

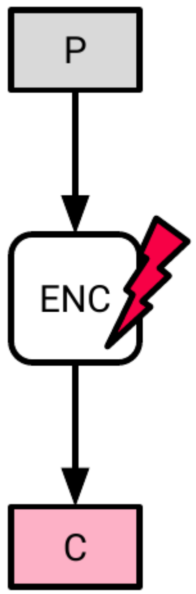
Basic Idea – Differential Fault Attack [BS97]

- Get physical access to target device
  - Set plaintexts
  - Observe ciphertexts



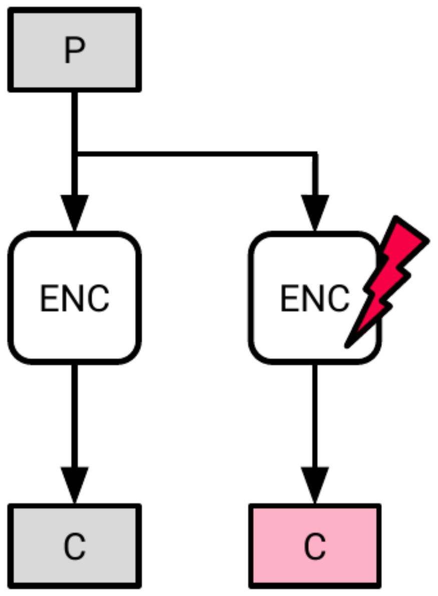
Basic Idea – Differential Fault Attack [BS97]

- Get physical access to target device
  - Set plaintexts
  - Observe ciphertexts
- Cause erroneous computations via
  - Clock glitches
  - Voltage glitches
  - Lasers



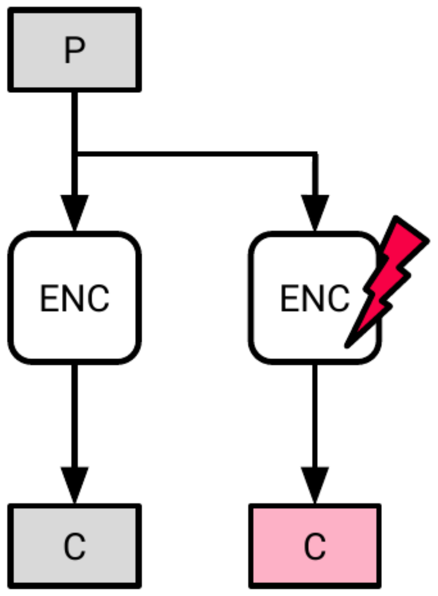
Basic Idea – Differential Fault Attack [BS97]

- Get physical access to target device
  - Set plaintexts
  - Observe ciphertexts
- Cause erroneous computations via
  - Clock glitches
  - Voltage glitches
  - Lasers
- Observe faulty and correct ciphertext

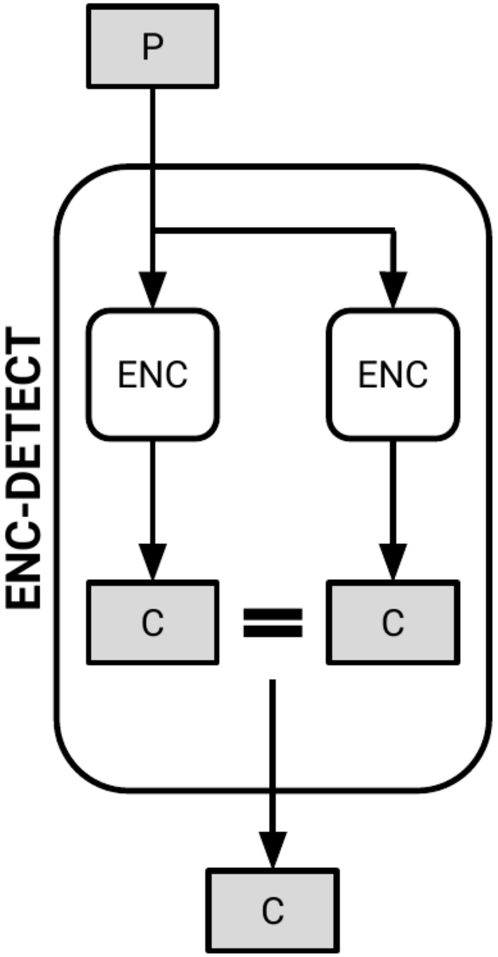


Basic Idea – Differential Fault Attack [BS97]

- Get physical access to target device
  - Set plaintexts
  - Observe ciphertexts
- Cause erroneous computations via
  - Clock glitches
  - Voltage glitches
  - Lasers
- Observe faulty and correct ciphertext
- Key recovery exploits differences in state bytes

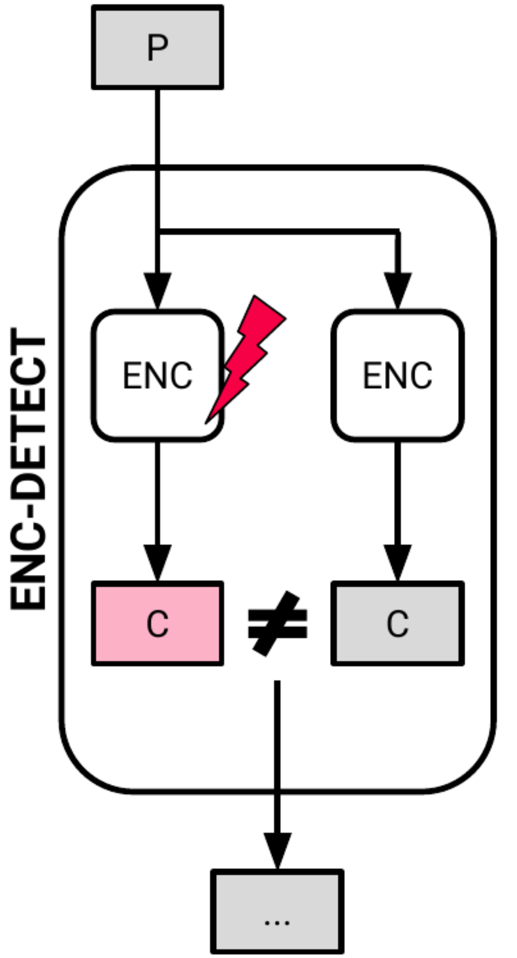


Countermeasures – Detection



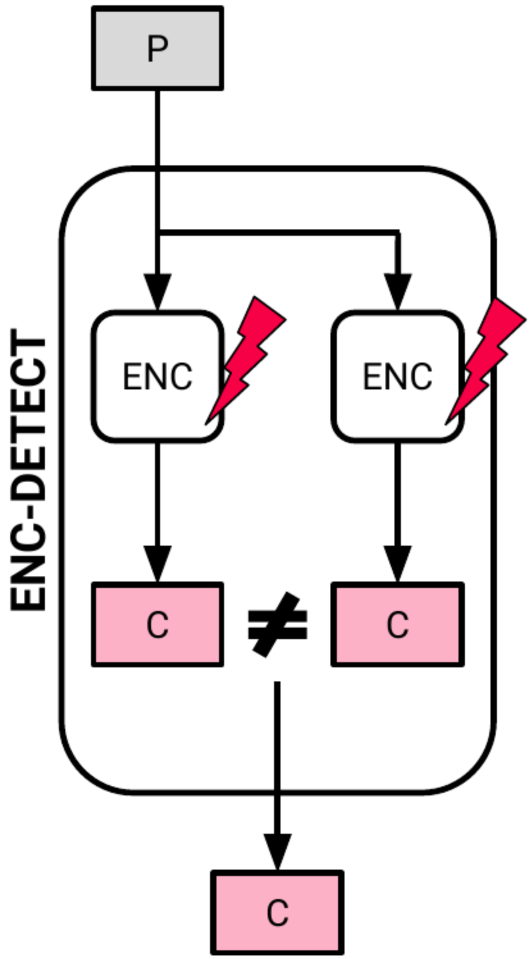
- Use redundancy to detect faults

Countermeasures – Detection



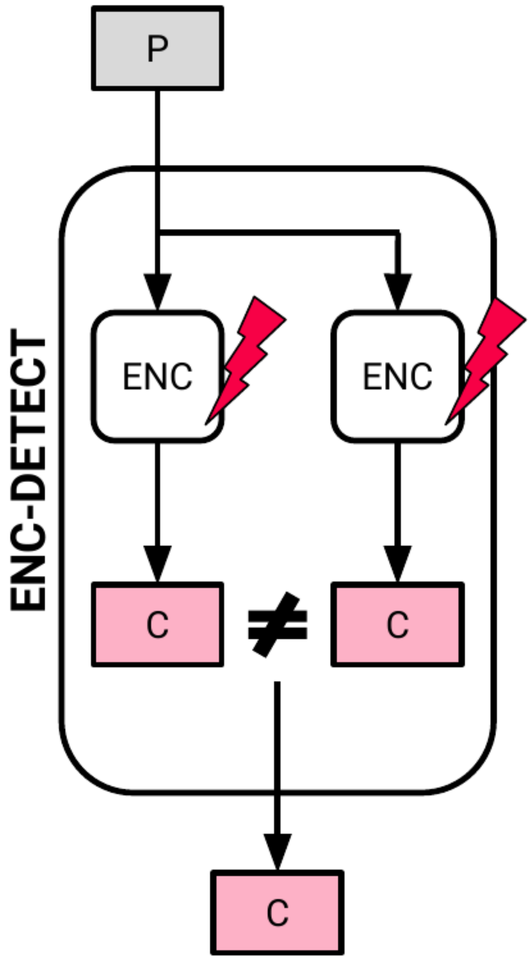
- Use redundancy to detect faults
- Fault detected → no ciphertext

Countermeasures – Detection



- Use redundancy to detect faults
- Fault detected → no ciphertext
- 2 identical faults necessary for attack

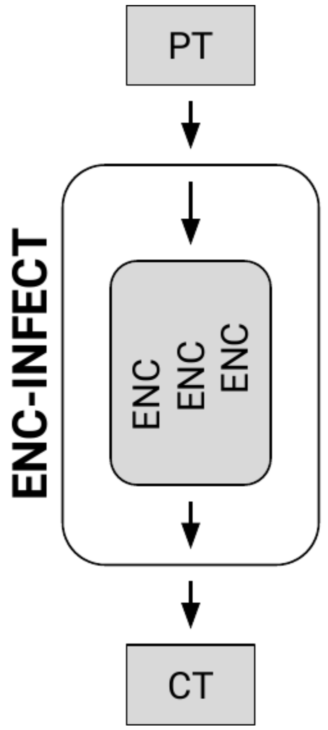
Countermeasures – Detection



- Use redundancy to detect faults
- Fault detected → no ciphertext
- 2 identical faults necessary for attack

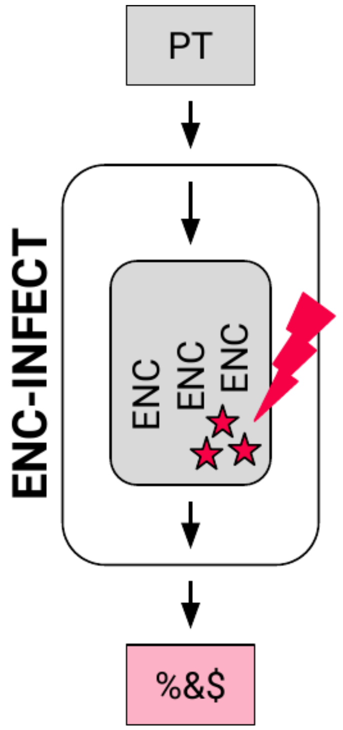
→ More redundancy, Enc-Dec, etc...

Countermeasures – Infection



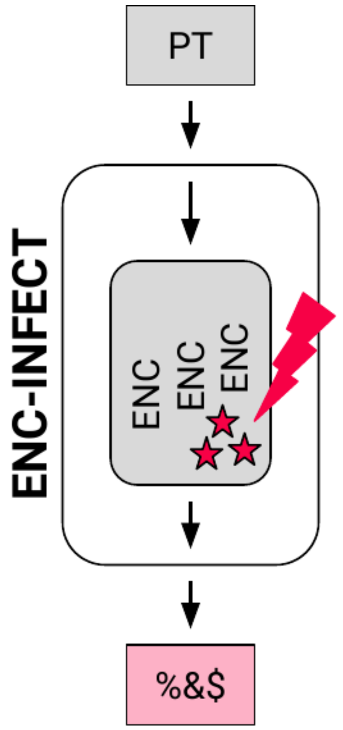
- Use redundancy, interleaved computation and dummy rounds

Countermeasures – Infection



- Use redundancy, interleaved computation and dummy rounds
- Faults are amplified s.t. ciphertext is not related to the key anymore → key recovery not possible

Countermeasures – Infection



- Use redundancy, interleaved computation and dummy rounds
- Faults are amplified s.t. ciphertext is not related to the key anymore → key recovery not possible
- Fault attacks still possible but quite hard …

Statistical Ineffective Fault Attacks [DEK+18]

Statistical Ineffective Fault Attacks [DEK+18]

- Ineffective Fault Attacks [Cla07]
  - Exploits only correct ciphertexts (similar to safe error attacks)
  - Requires precise faults with known effect
- Statistical Fault Analysis [FJLT13]
  - Any fault, even if effect is unknown
  - Mitigated by detection/infection

Statistical Ineffective Fault Attacks [DEK+18]

- Ineffective Fault Attacks [Cla07]
  - Exploits only correct ciphertexts (similar to safe error attacks)
  - Requires precise faults with known effect
- Statistical Fault Analysis [FJLT13]
  - Any fault, even if effect is unknown
  - Mitigated by detection/infection

⇒ Statistical Ineffective Fault Attacks [DEK+18]

- Exploits only correct ciphertexts
- Any fault, even if effect is unknown

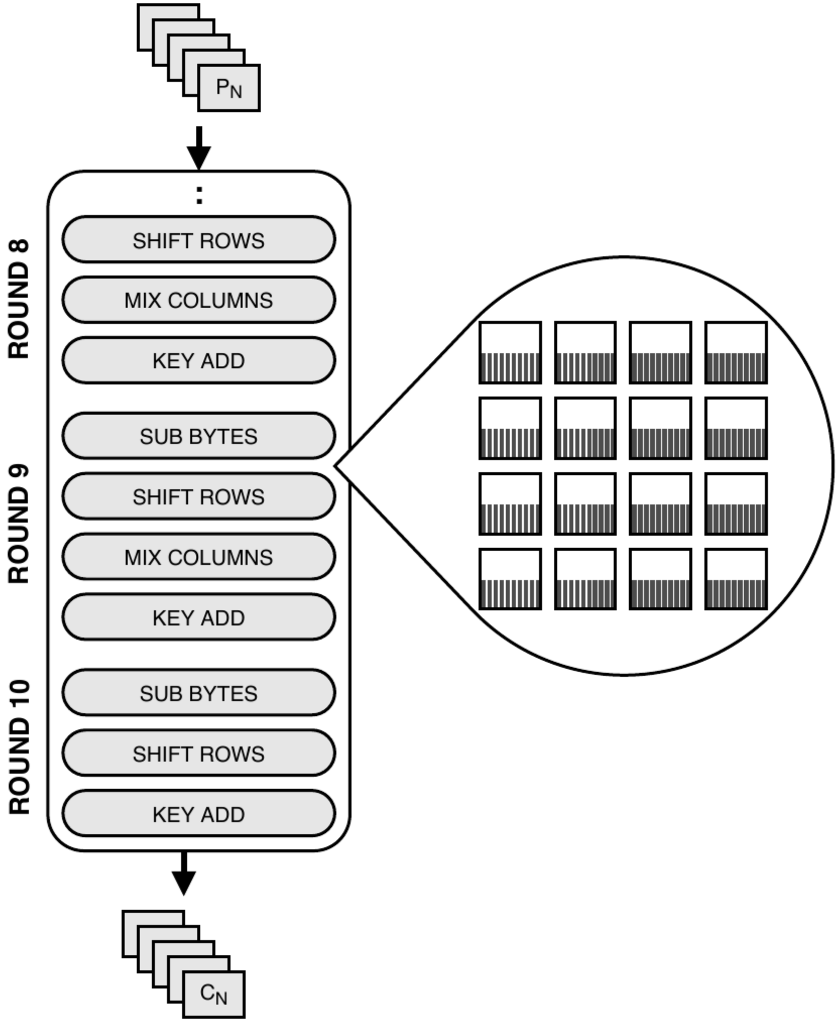
Basic Idea – Statistical Fault Attacks [FJLT13]

- Exploit faulty ciphertexts only
- Plaintexts can be unknown but need to vary
  - *Opposite* requirement compared to differential attacks
- Usually needs several faulted encryptions
- Key recovery exploits statistical distributions of state bytes (in contrast to differences)

Statistical Fault Attacks on AES-128

AES is a PRP

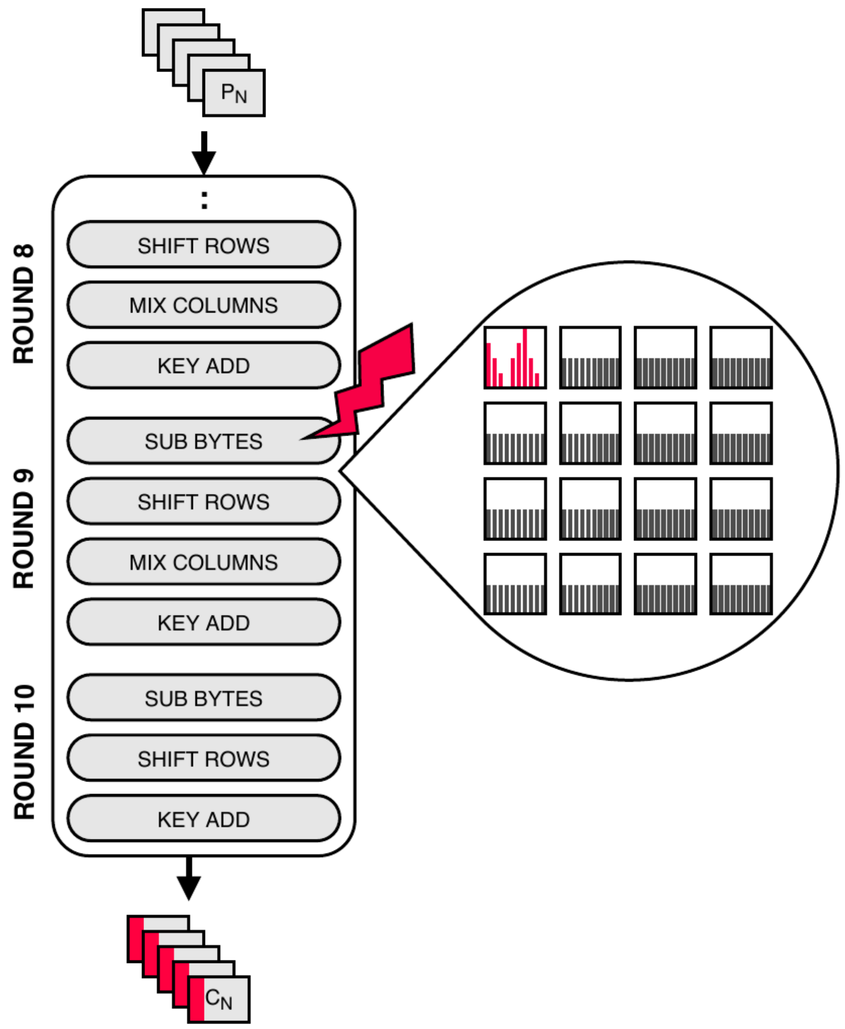
- Distribution of ciphertext is uniform
- (Also after only 9 rounds)



Statistical Fault Attacks on AES-128

Assume fault disturbs distribution of one state byte in round 9

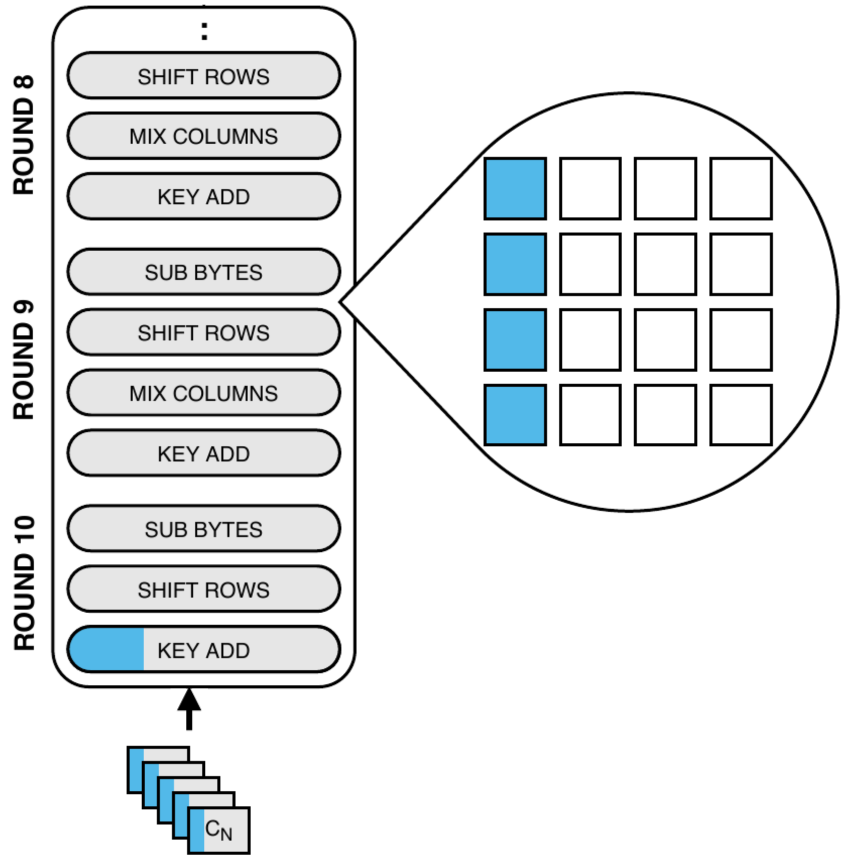
- Stuck-at, bitflip, random, etc.
- Attacker does not need to know the caused bias
- 4 ciphertext bytes are affected



Statistical Fault Attacks on AES-128

4 state bytes in round 9 can be calculated from

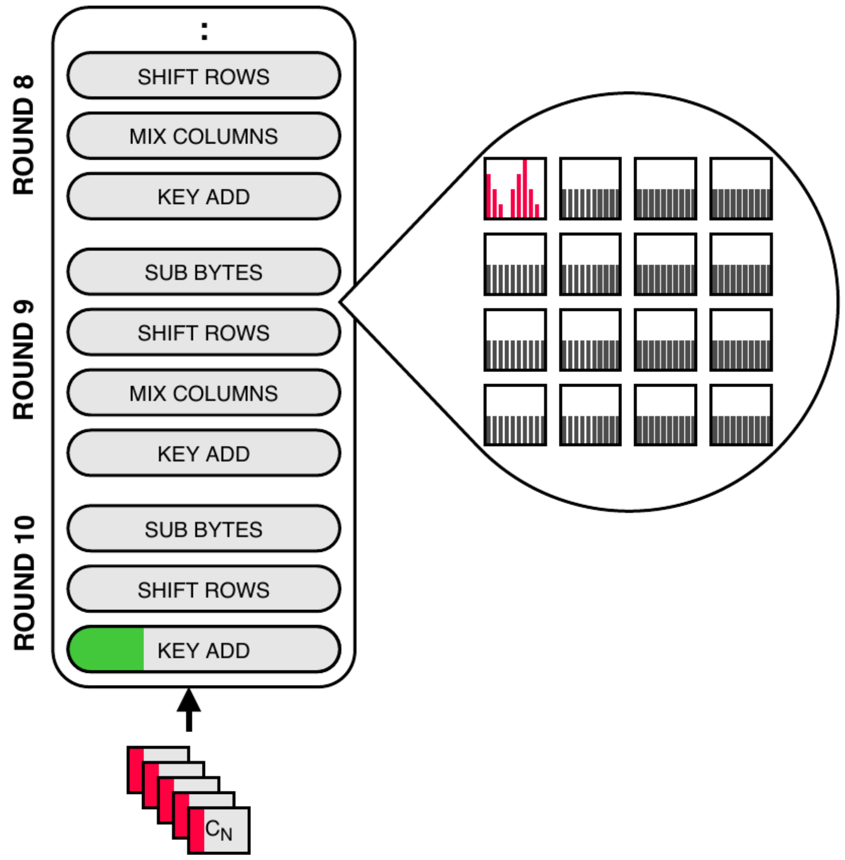
- 4 ciphertext bytes
- 4 key bytes



Statistical Fault Attacks on AES-128

4 state bytes in round 9 can be calculated from

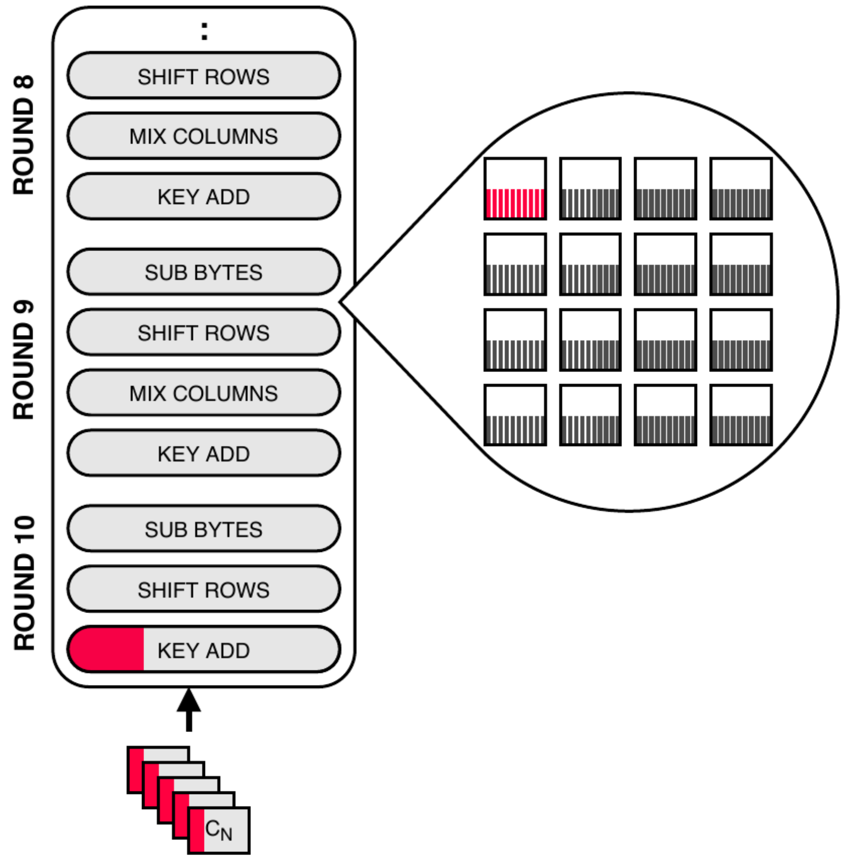
- 4 ciphertext bytes
- 4 key bytes (correct)



Statistical Fault Attacks on AES-128

4 state bytes in round 9 can be calculated from

- 4 ciphertext bytes
- 4 key bytes (incorrect)

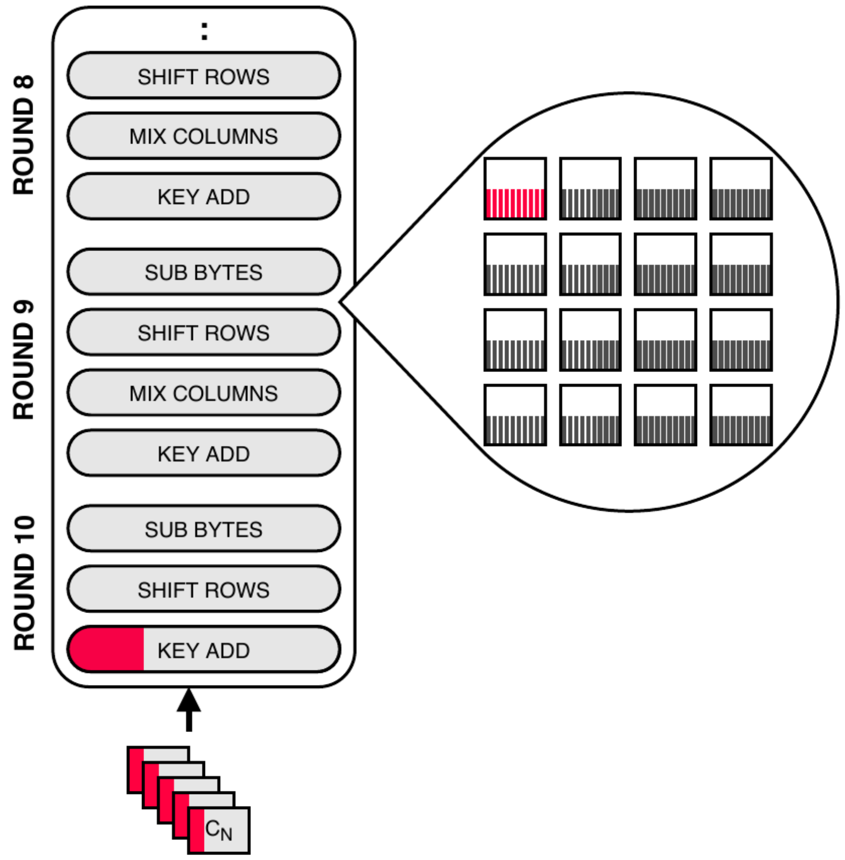


Statistical Fault Attacks on AES-128

4 state bytes in round 9 can be calculated from

- 4 ciphertext bytes
- 4 key bytes (incorrect)

→ Complexity of the attack depends on bias caused by the fault



Considered Fault Models [FJLT13]

- Stuck-at zero fault model with probability 1
  → 6 *faulty* encryptions
- Stuck-at zero fault model with probability 1/2
  → 14 *faulty* encryptions
- Stuck-at fault model with an unknown and random value e
  → 80 *faulty* encryptions

Considered Fault Models [FJLT13]

- Stuck-at zero fault model with probability 1
  →6 *faulty* encryptions
- Stuck-at zero fault model with probability 1/2
  →14 *faulty* encryptions
- Stuck-at fault model with an unknown and random value e
  →80 *faulty* encryptions

- In practice the number of needed faulty encryptions also depends on the fault setup, injection method, etc.

Practical Evaluation/Results [DEK+16]

- AES Software Implementation

  Method: clock glitches

  # Faulty encryptions: 30

- AES Hardware co-processor A

  Method: clock glitches

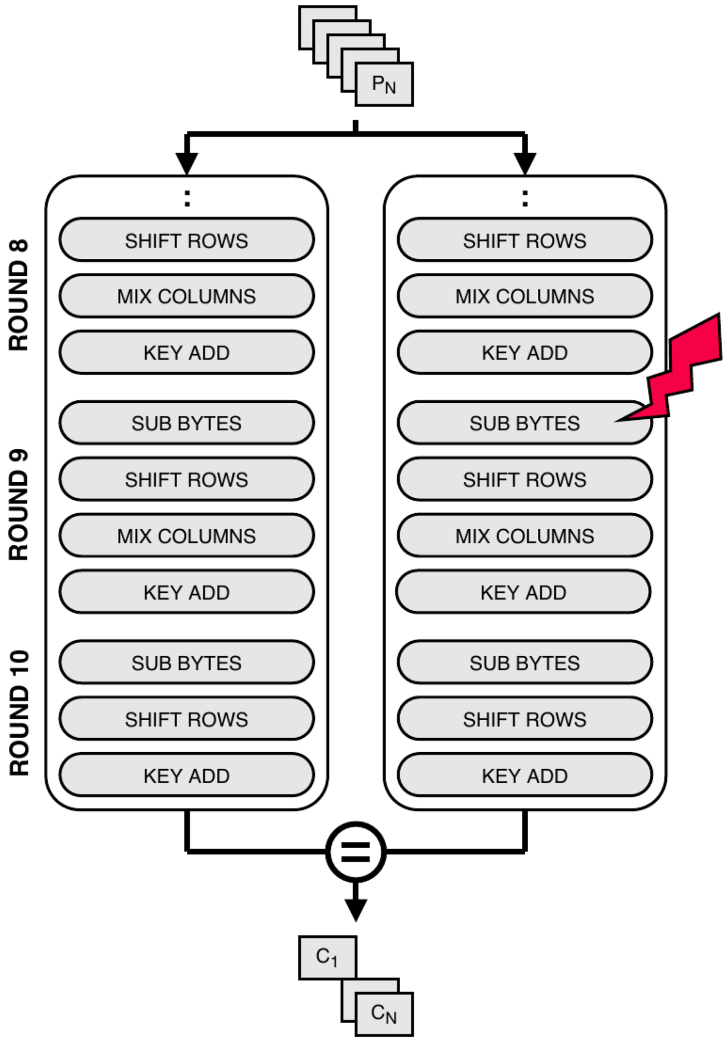
  # Faulty encryptions: 20

- AES Hardware co-processor B

  Method: clock glitches

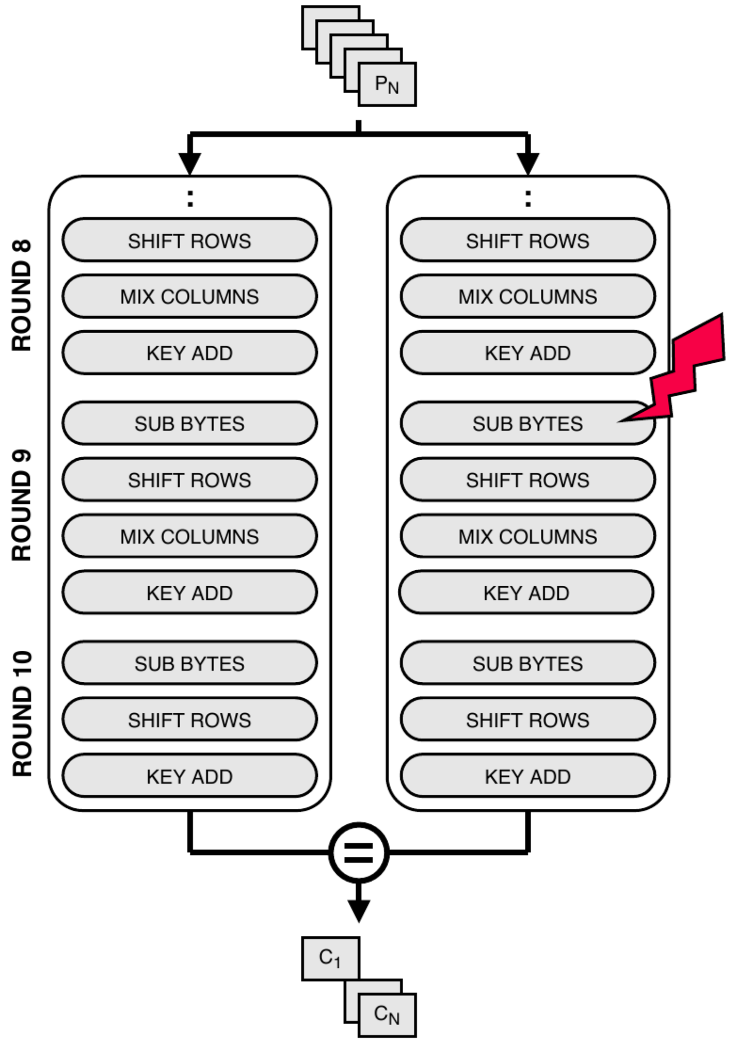
  # Faulty encryptions: 1200

Statistical Ineffective Fault Attacks [DEK+18]



- Redundant computation was supposed to fix the problem!

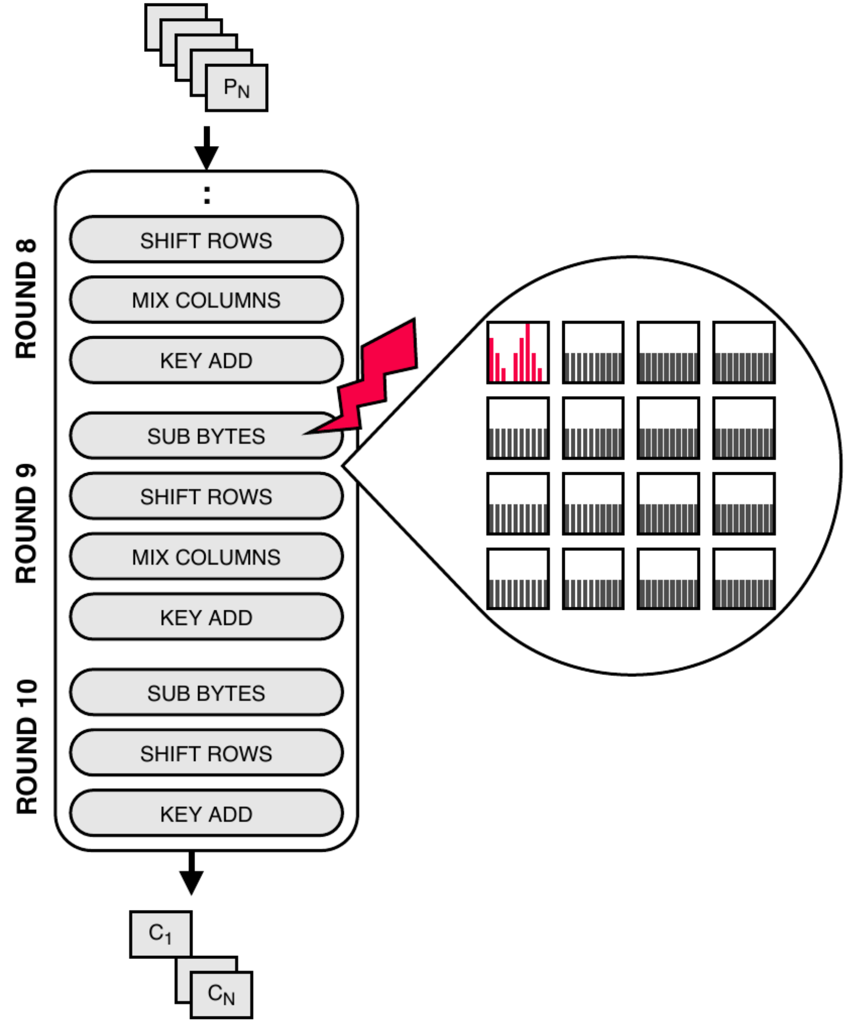
Statistical Ineffective Fault Attacks [DEK+18]



- Redundant computation was supposed to fix the problem!
- Except it doesn't

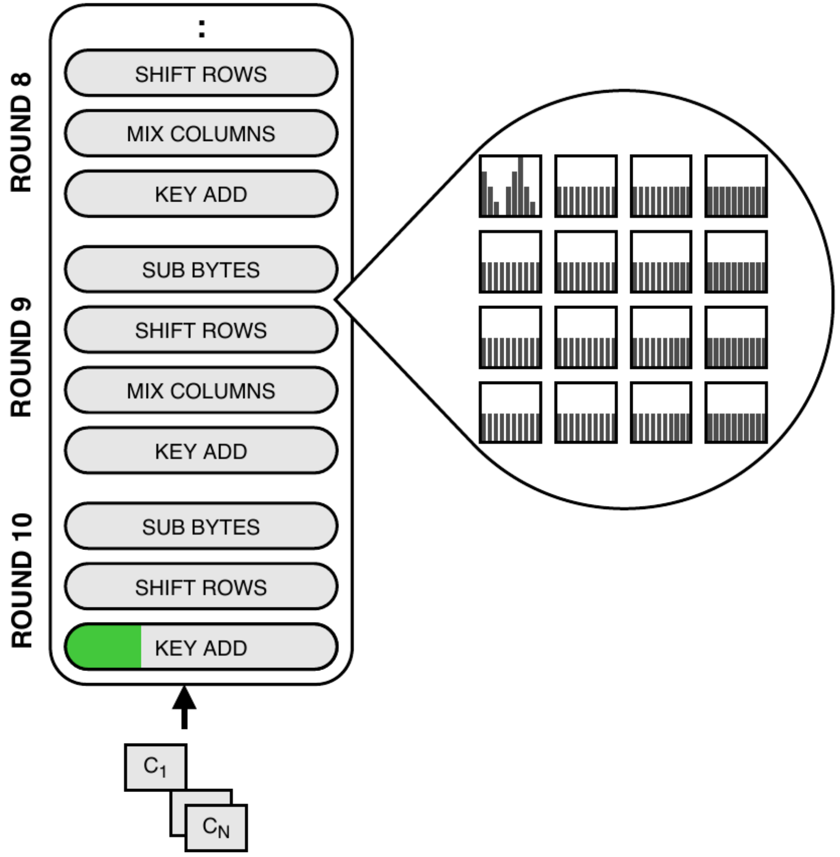
Statistical Ineffective Fault Attacks [DEK⁺18]

- For simplicity, assume stuck-at zero fault (others work as well)
- *Effective* faults are filtered out
- Correct ciphertexts still show a bias in round 9



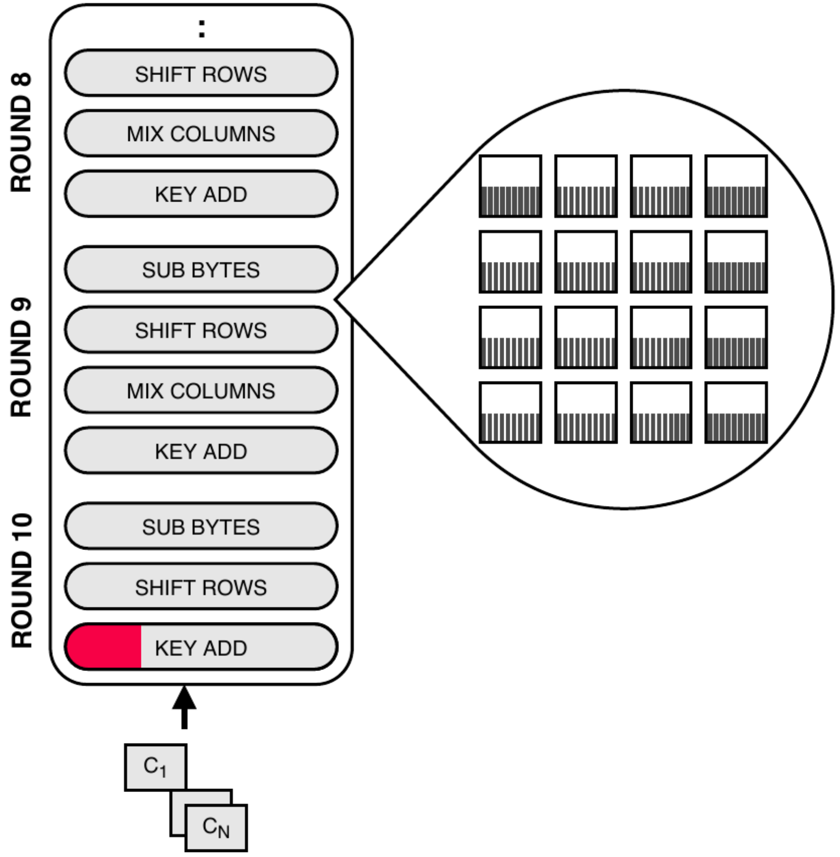
Statistical Ineffective Fault Attacks [DEK+18]

- For simplicity, assume stuck-at zero fault (others work as well)
- *Effective* faults are filtered out
- Correct ciphertexts still show a bias in round 9
- Exploitation works same as before



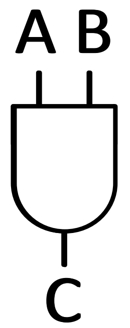
Statistical Ineffective Fault Attacks [DEK+18]

- For simplicity, assume stuck-at zero fault (others work as well)
- *Effective* faults are filtered out
- Correct ciphertexts still show a bias in round 9
- Exploitation works same as before



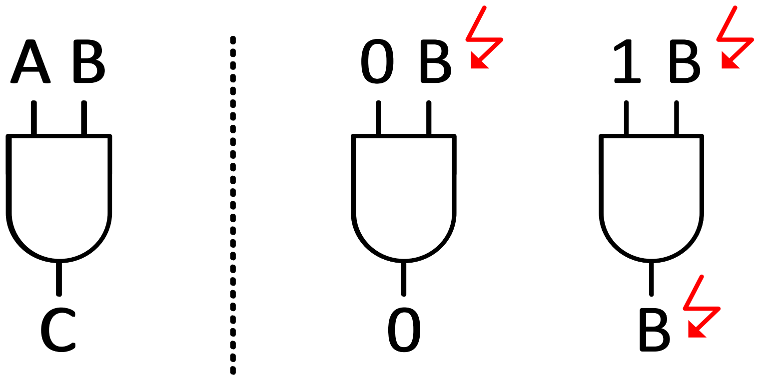
Ineffective Faults on AND-gate

- Example (AND-gate)



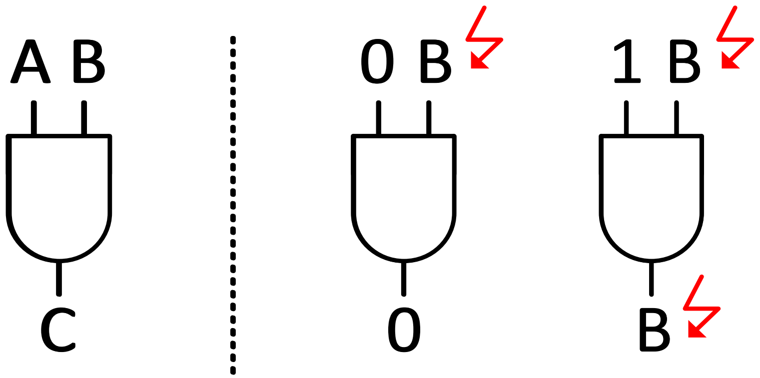
Ineffective Faults on AND-gate

- Example (AND-gate)



Ineffective Faults on AND-gate

- Example (AND-gate)



- If we get an alarm then we know that A=1 otherwise A=0 with high probability (>0.5)

Ineffective Faults on AND

- **Stuck-at fault:** If we get an alarm then we know that A=1 otherwise A=0 with probability 2/3

A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

⇨

A	B ↯	C
0	0	0
0	0	0
1	0	0
1	**0**	**0**

} alarm

Ineffective Faults on AND

- **Bit-flip fault:** If we get an alarm then we know that A=1 otherwise A=0 with probability 1

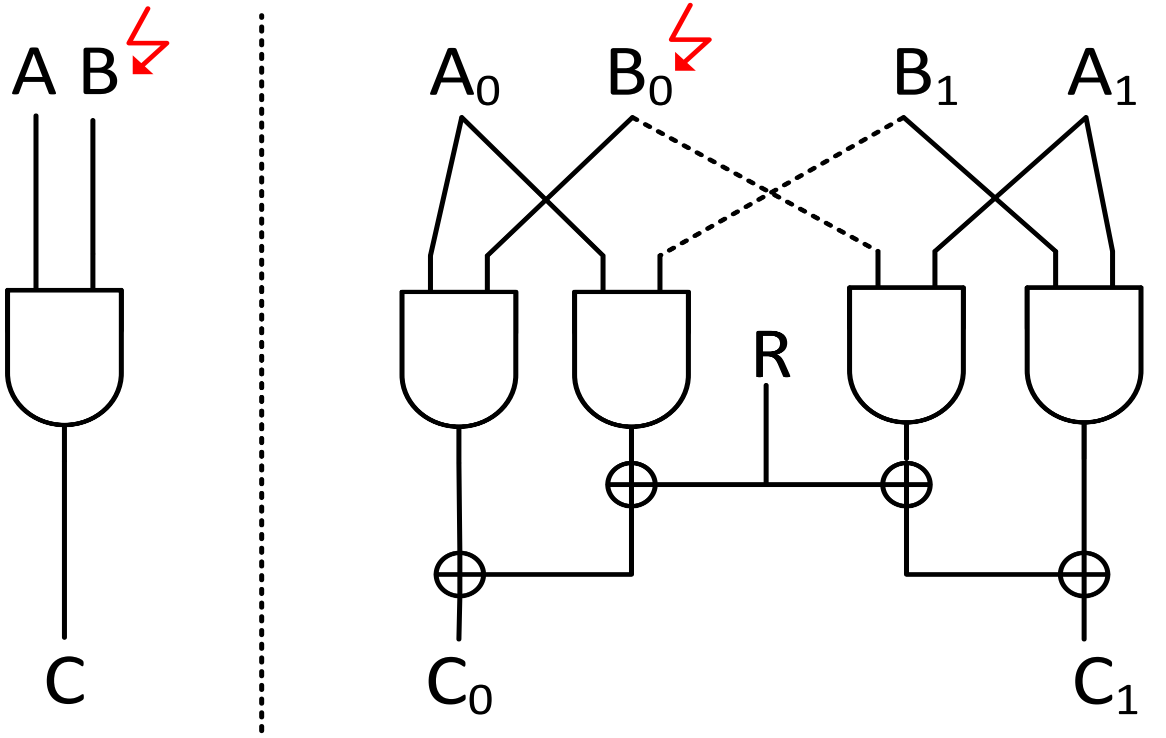
A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

⇨

A	B ↯	C	
0	1	0	
0	0	0	
1	**1**	**1**	alarm
1	**0**	**0**	alarm

Masking does not prevent the Attack [DEG+18]

- Example (AND-gate)



AND-gate

Masked AND-gate

Other Masking Schemes

- Similar results for other masking schemes
  - ISW masking scheme + Improvements
  - TI masking scheme
  - DOM masking scheme
  - …

Other Masking Schemes

- Similar results for other masking schemes
  - ISW masking scheme + Improvements
  - TI masking scheme
  - DOM masking scheme
  - …
- Works in a similar way for S-Boxes

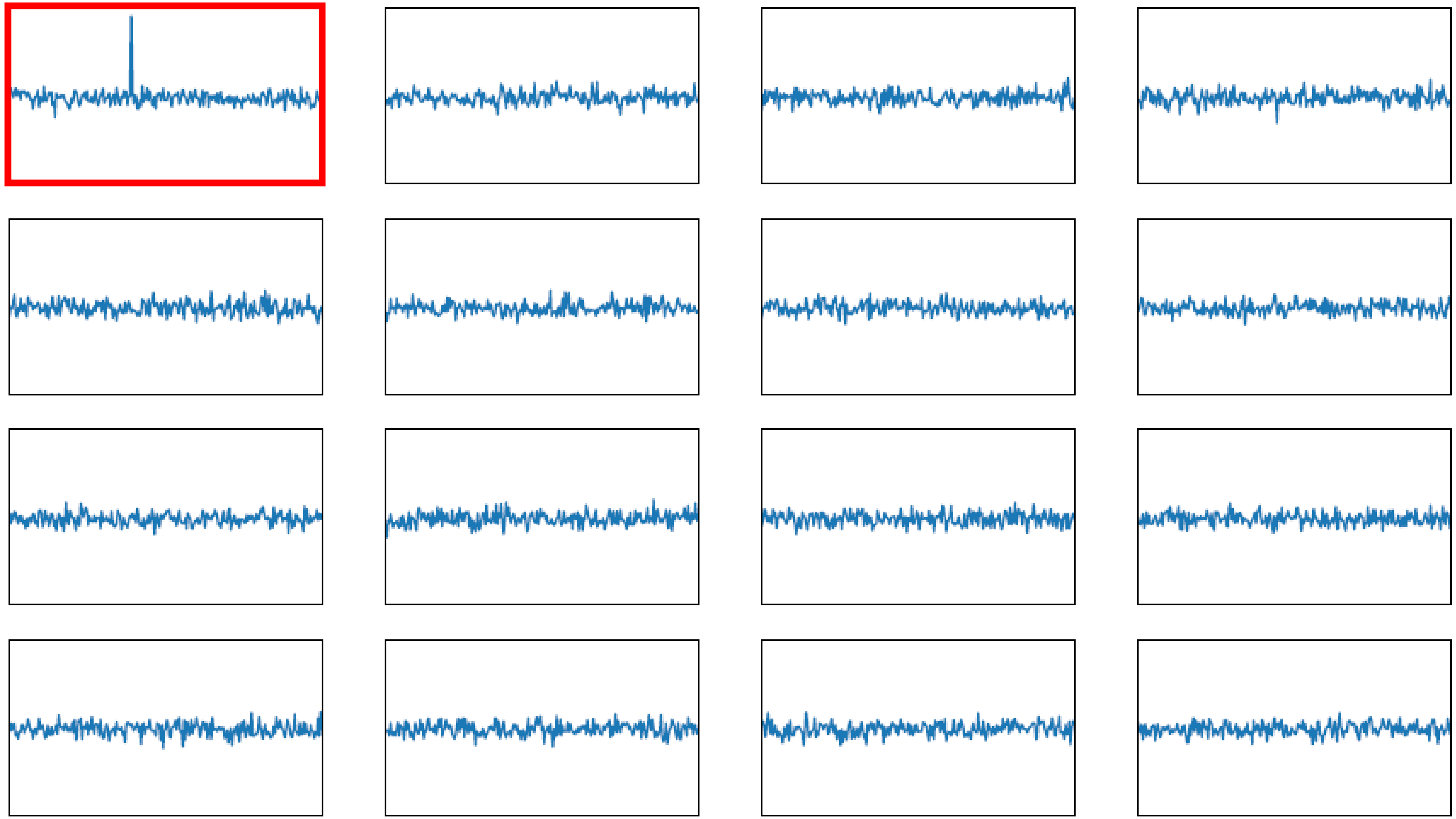
Practical Evaluation/Results [DEG+18]

- Higher Order Masked AES by Rivain et al. with time redundancy

- Implementation by Coron
  - ATXmega 128D4
  - 10^{th}-order masked AES
  - arbitrary time redundancy

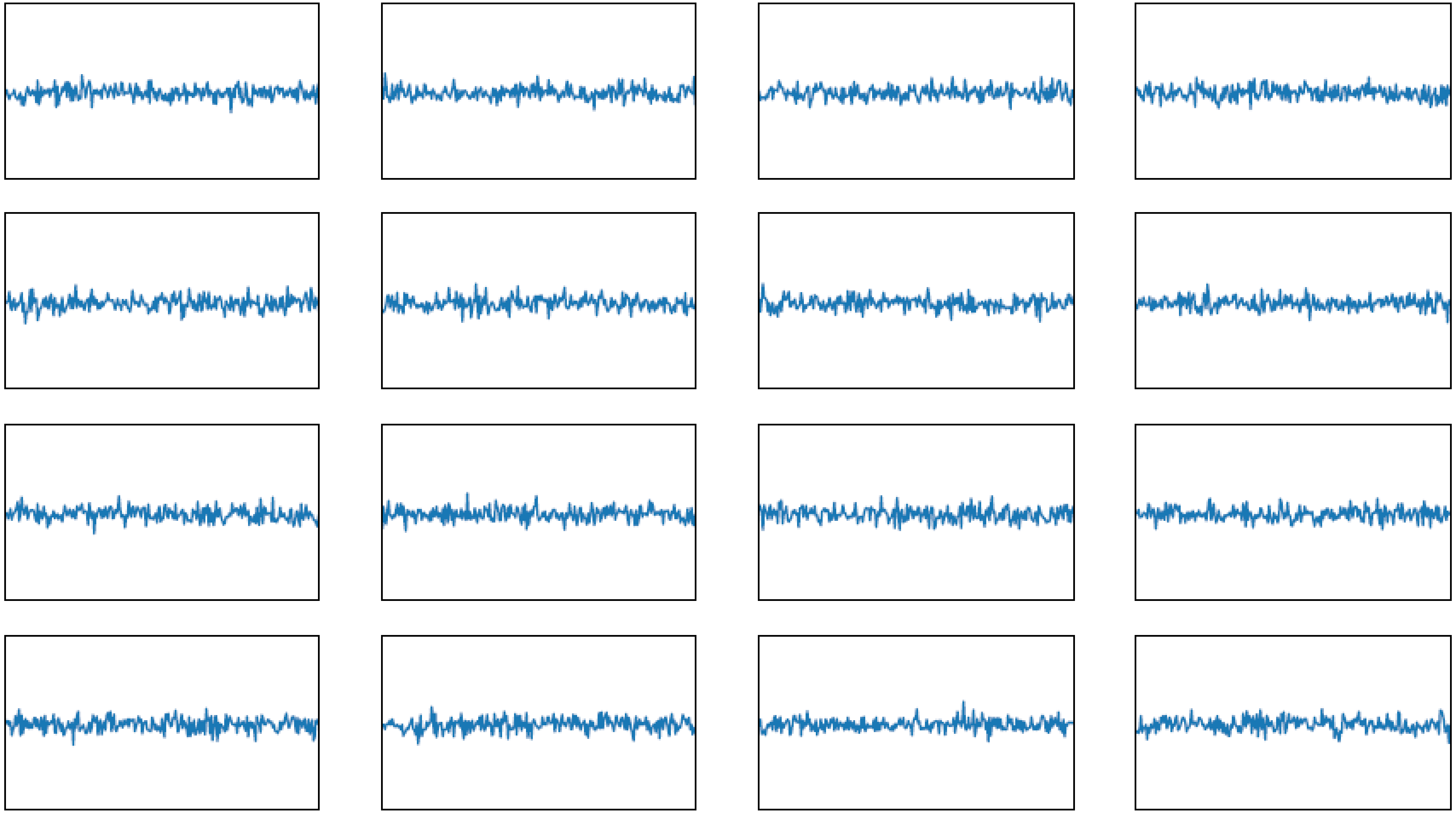
- Fault Injection
  - Target: S-box in the 9^{th}-round
  - Method: clock glitches

Results SFA: Correct Key



25 000 faulty encryptions (ciphertexts)

Results SFA: Wrong Key

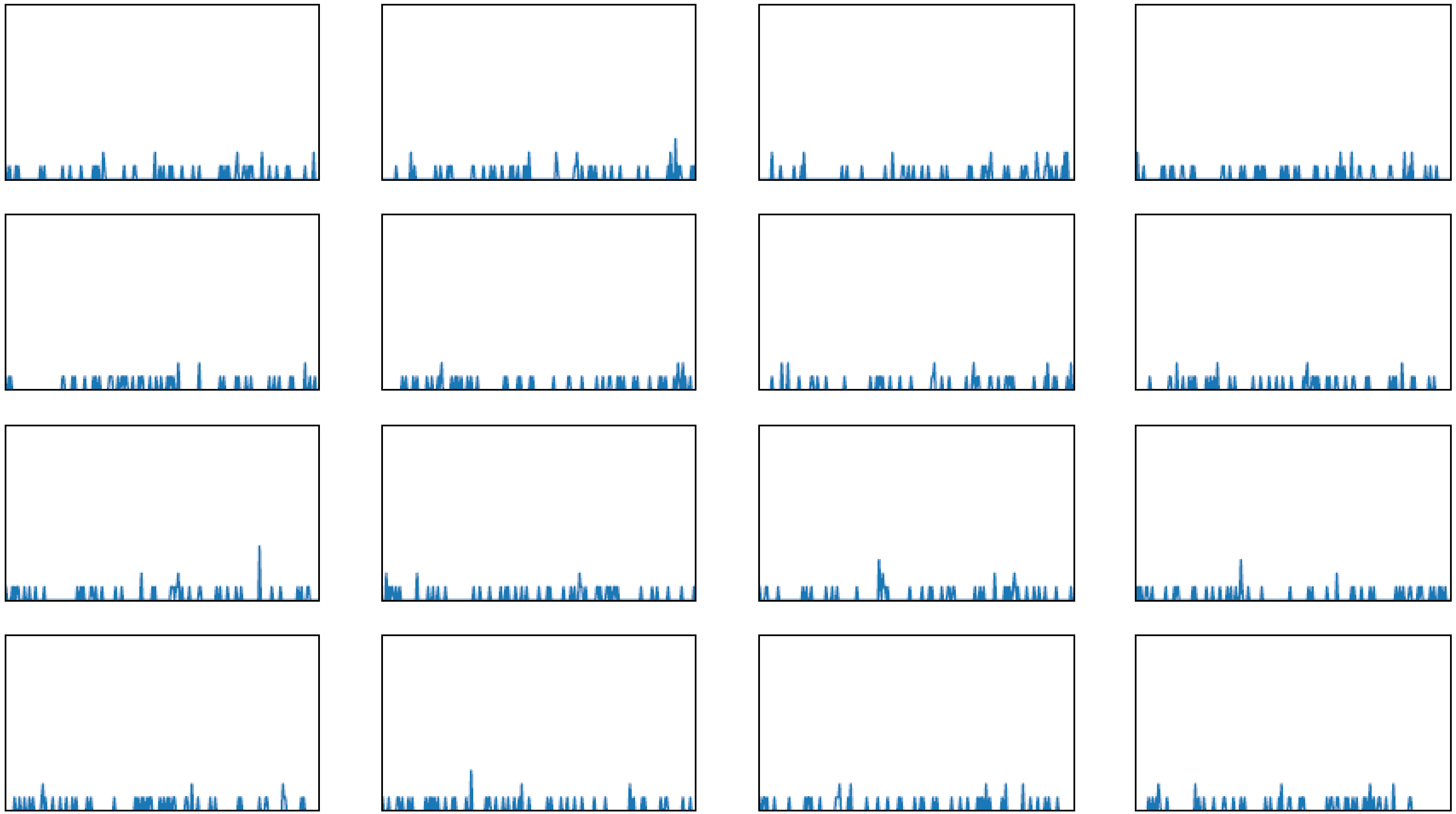


25 000 faulty encryptions (ciphertexts)

Results SIFA: Correct Key

2 000 faulty encryptions

Results SIFA: Wrong Key



2 000 faulty encryptions

Statistical Ineffective Fault Attacks

- SIFA is a quite powerful attack
- Can break both fault and power analysis countermeasures
- Requires only one fault per computation
- Attacker does not need to hit specific bits/bytes
- Attacker does not need know how the faults influence the computation

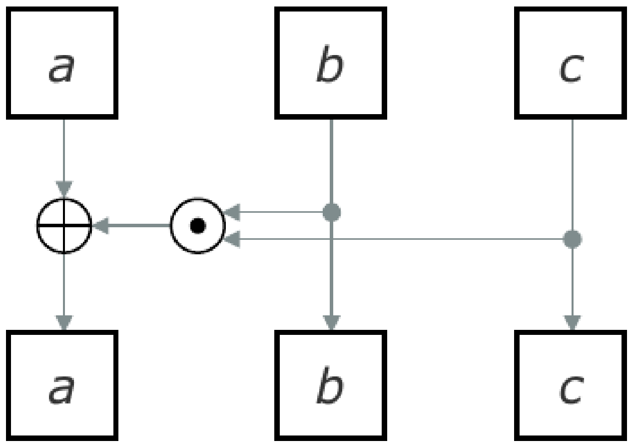
Countermeasures

- Sensors to detect tampering
- Adding noise (hiding)
- Limit number of outputs (e.g. fault counters)
- Error Correction
- ...

Basic Idea – Protecting against SIFA [DDE+20]

- Build a masked and redundant circuit from some basic circuits such that *critical* faults will always be detected
- Each basic circuit operates only on a incomplete set of shares and is a permutation
- Permutation can either be a linear function or a variant of the Toffoli-gate (simplest invertible non-linear function)

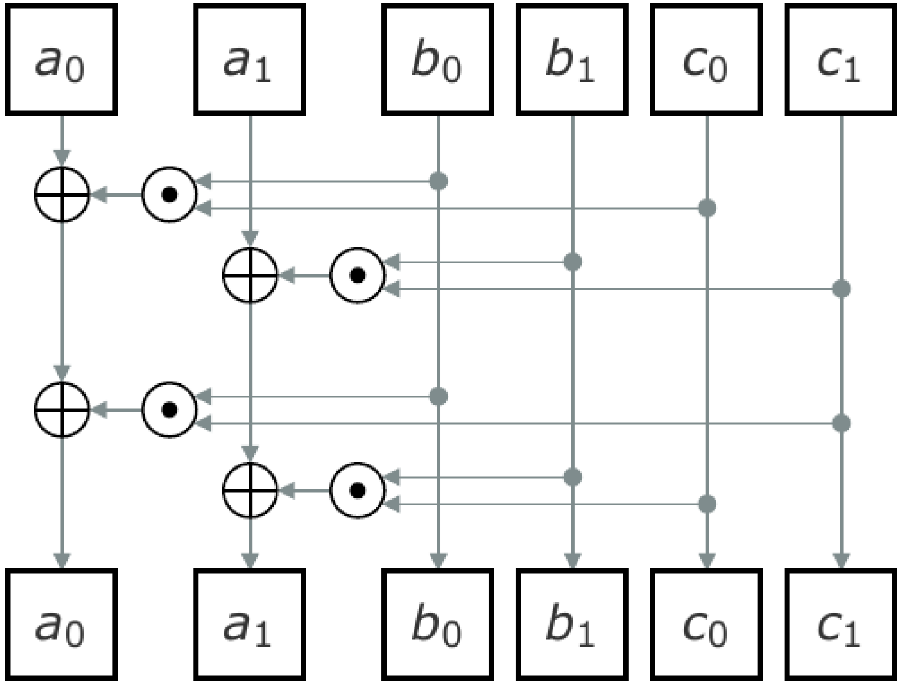
Toffoli-gate



- Simplest invertible non-linear function
- Any bit-flip fault /difference at input will propagate to the output and detected
- But stuck-at faults might not be detected and will leak information

→ Masked Toffoli-gate

Masked Toffoli-gate



- Constructed from 4 Toffoli-gate
- Is an invertible function → bit-flip fault will be detected
- Each Toffoli-gate only operates on incomplete set of shares → a single stuck-at fault will not leak information about the actual value

→ Singel-fault SIFA robustness

Application to S-boxes [DDE+20]

- This approach can be implemented quite efficiently
- Shown to work for all 3-bit and many 4-bit S-boxes
- No noticeable performance difference to regular masked S-boxes
- Approach can even be extended to larger fields (e.g. AES S-boxes)

Application to S-boxes [DDE+20]

- This approach can be implemented quite efficiently
- Shown to work for all 3-bit and many 4-bit S-boxes
- No noticeable performance difference to regular masked S-boxes
- Approach can even be extended to larger fields (e.g. AES S-boxes)

- Construction has been formally verified [HPB21]

Summary

- SIFA is a quite powerful attack
- Works for many ciphers and encryption schemes
- Can break both detection and infection fault countermeasures
- In practice the complexity of the attack depends on many factors
  - Fault setup, fault method, ...
- Dedicated countermasueres against SIFA are important and an interessting area of research

Thank you for your attention!

Questions?

References

[BS97] E. Biham, A. Shamir: **Differential Fault Analysis of Secret KeyCryptosystems**. CRYPTO 1997

[C07] C. Clavier: **Secret External Encodings Do Not Prevent Transient Fault Analysis**. CHES 2007

[DDE+20] J. Daemen, C. Dobraunig, M. Eichlseder, H. Groß, F. Mendel, R. Primas: **Protecting against Statistical Ineffective Fault Attacks**. CHES 2020

[DEG+18] C. Dobraunig, M. Eichlseder, H. Groß, S. Mangard, F. Mendel, R. Primas: **Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures**. ASIACRYPT 2018

[DEK+16] C. Dobraunig, M. Eichlseder, T. Korak, V. Lomné, F. Mendel: **Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes**. ASIACRYPT 2016

[DEK+18] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel, R. Primas: **SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography**. CHES 2018

[FJLT13] T. Fuhr, E. Jaulmes, V. Lomné, A. Thillard: **Fault Attacks on AES with Faulty Ciphertexts Only**. FDTC 2013

[HPB21] V. Hadzic, R. Primas, R. Bloem: **Proving SIFA Protection of Masked Redundant Circuits**. ATVA 2021