Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes

C. Dobraunig[1], M. Eichlseder[1], T. Korak[1], V. Lomné[2], F. Mendel[1]

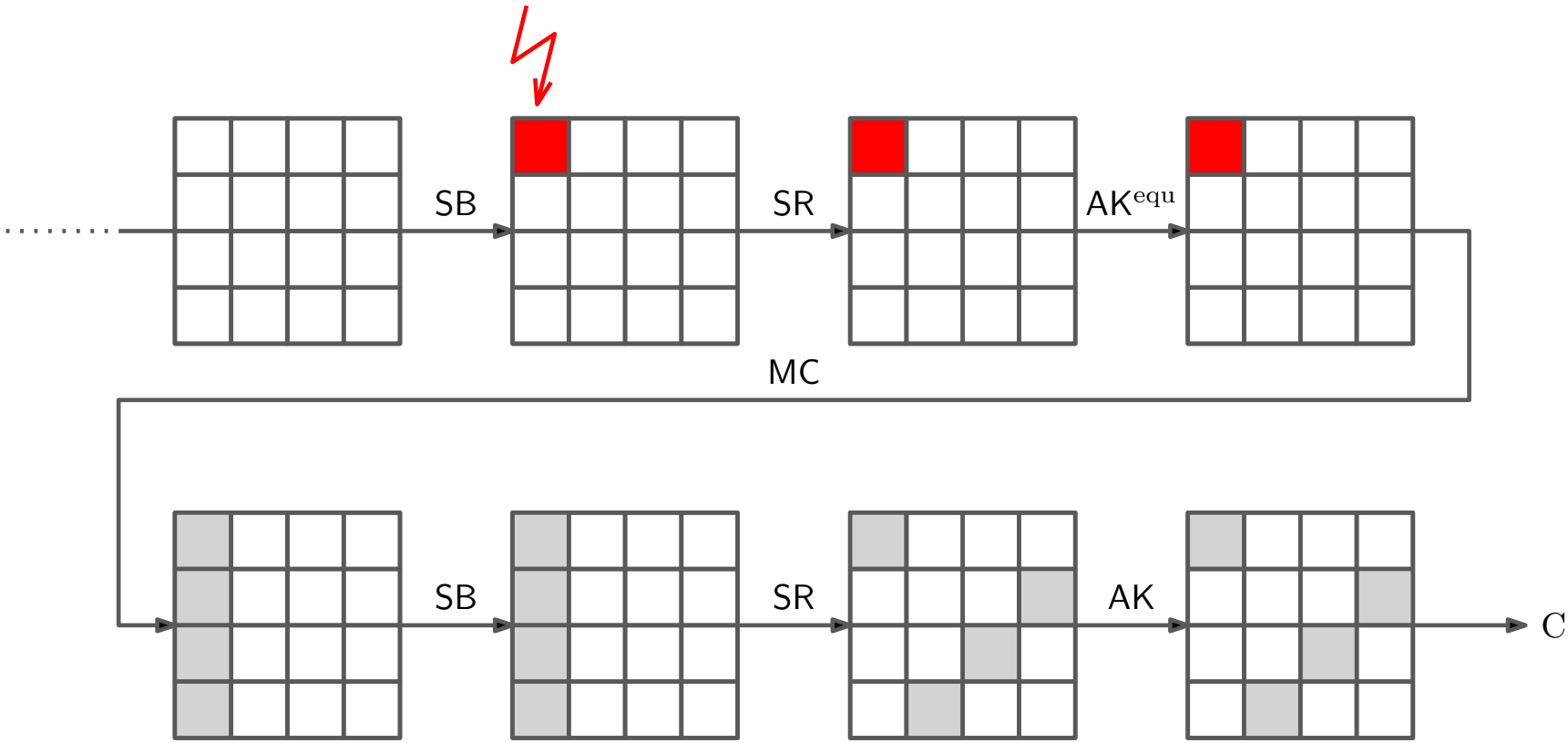
AsiaCrypt 2016

[1] Graz University of Technology, Austria
[2] ANSSI, Paris, France

Overview

- Fault attacks on AES-based AE-schemes
  - Nonce does not preclude fault attacks
  - Based on Fuhr et al. (FDTC 2013)
  - Faults influence distribution
- Experiments to show practical relevance

Statistical Fault Attack



Application to Authenticated Encryption

Requirements for the Attack

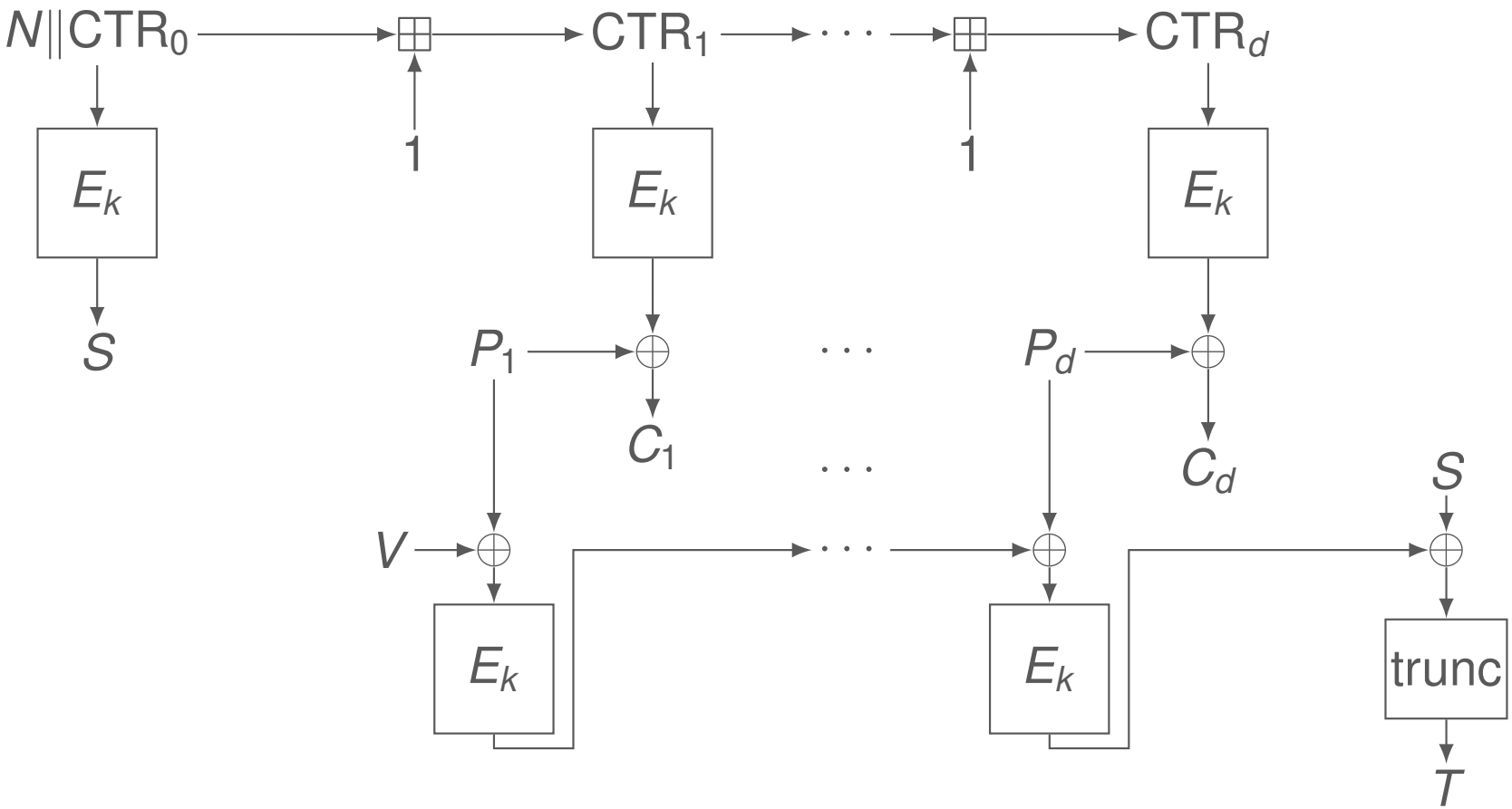
1. The inputs need to be different for each fault
2. The block cipher output needs to be known

Application to Authenticated Encryption

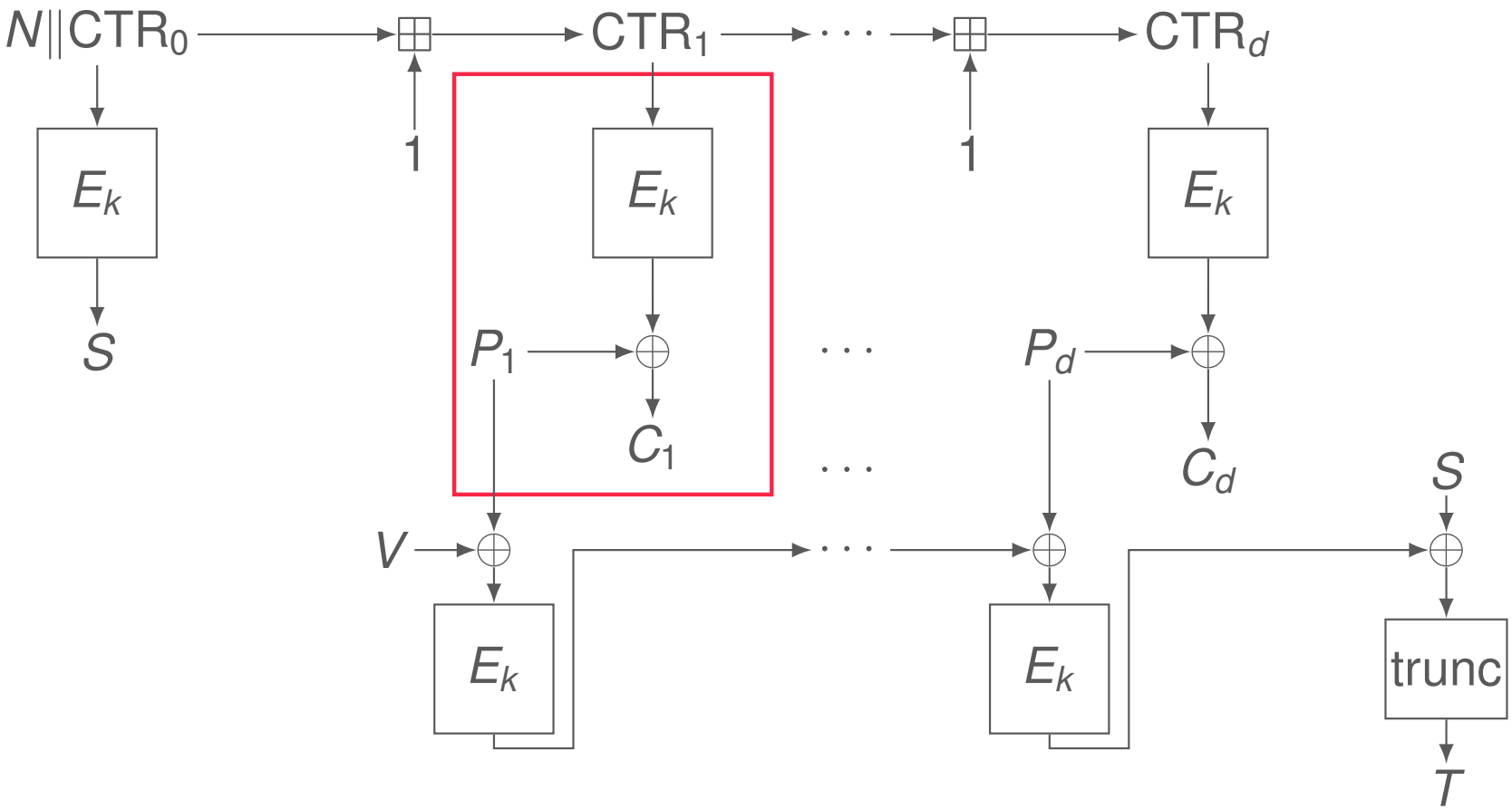
Authenticated encryption modes for block ciphers (ISO/IEC)

- CCM
- EAX
- GCM
- OCB

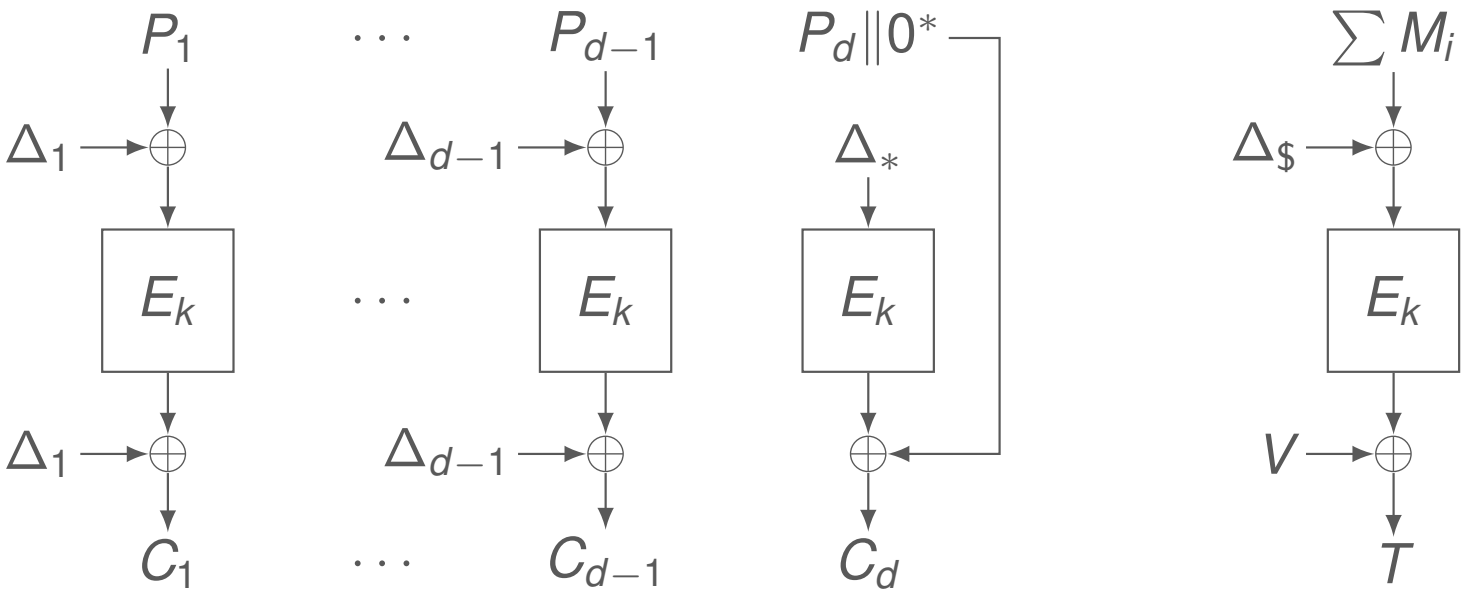
Attack on CCM



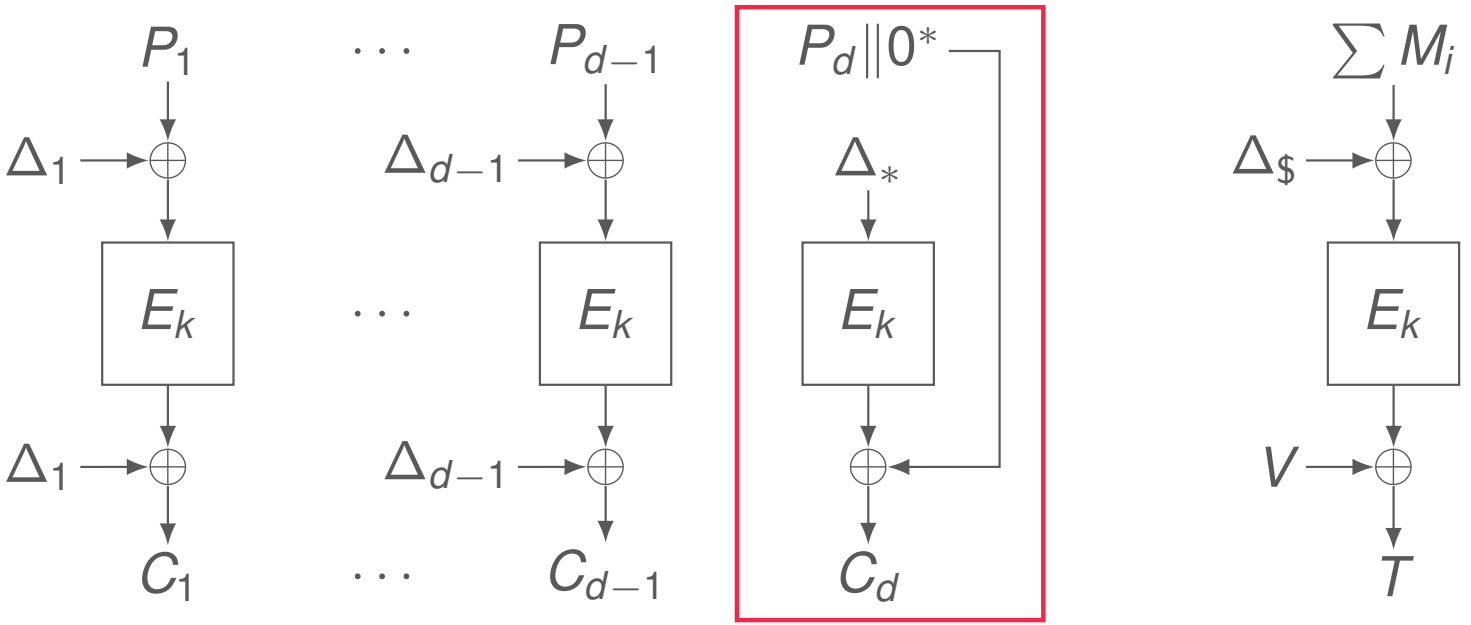
Attack on CCM



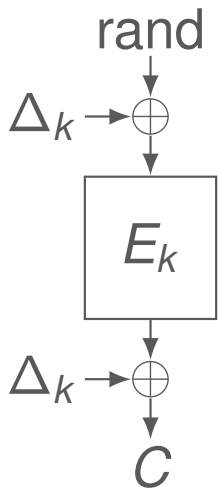
Attack on OCB

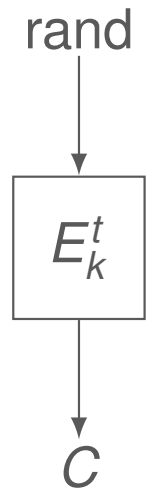


Attack on OCB



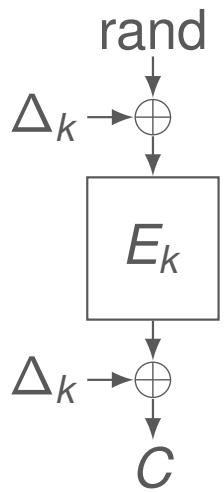
Application to other schemes



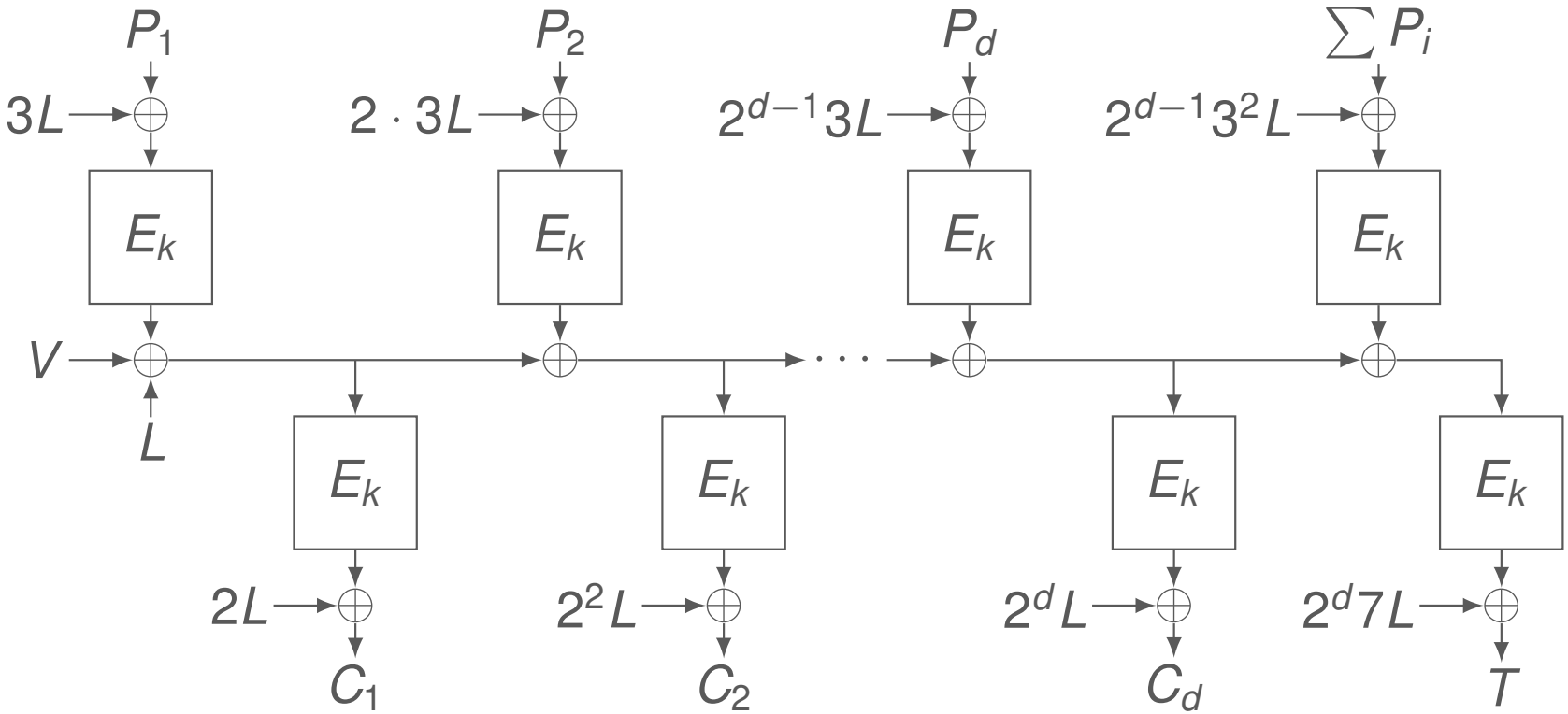


XEX-like Construction

- Output masked by Δ_k
  - $\Delta_k := \delta_k$
  - $\Delta_k := \delta_k + \delta_n$
  - $\Delta_k := \delta_{k,n}$
- Example: COPA

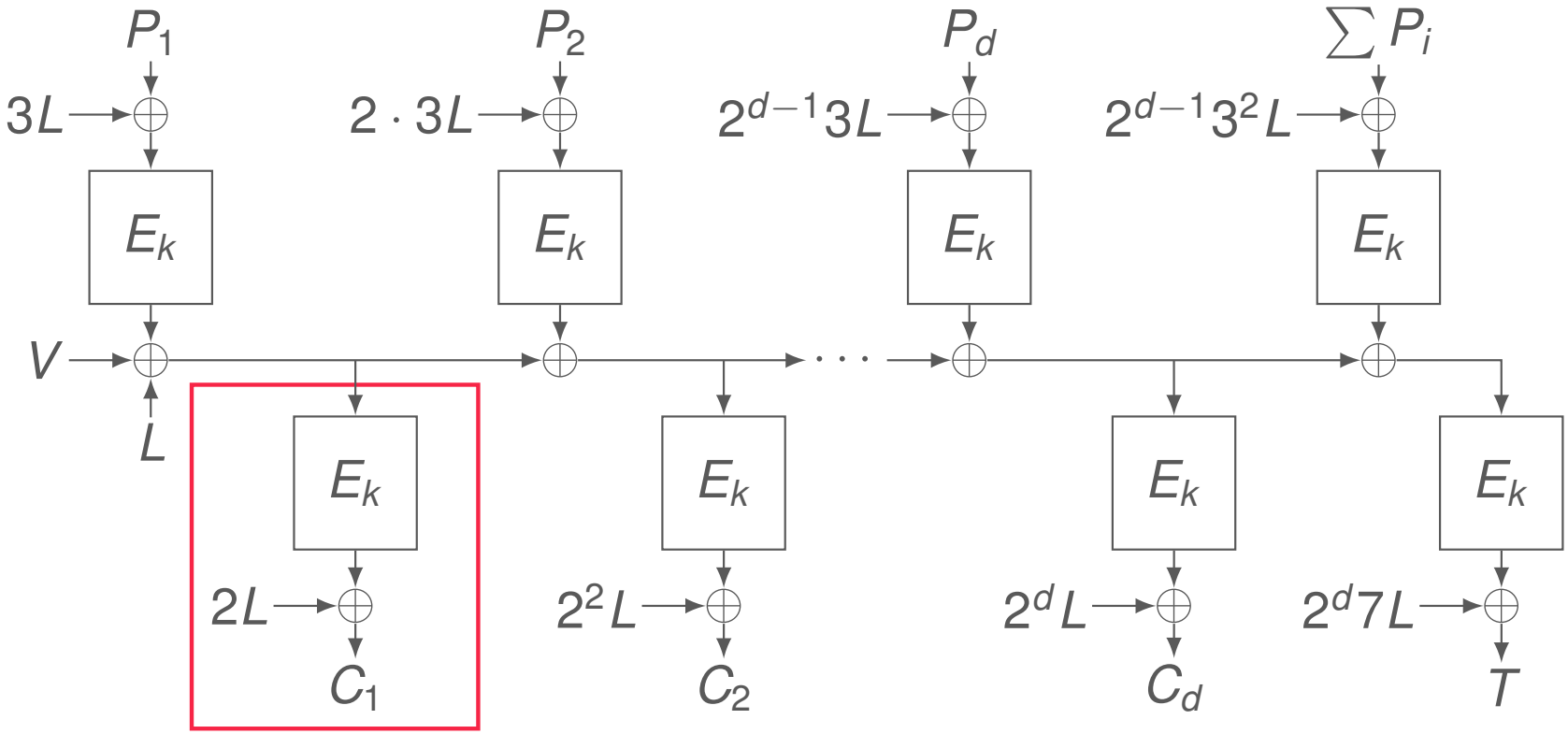


Attack on COPA



- $L = E_k(0)$

Attack on COPA



- $L = E_k(0)$

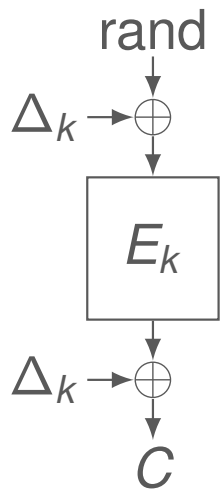
Attack on COPA

- Idea: Consider $2L$ as part of the last subkey
  - $SK'_{10} := SK_{10} \oplus 2L$
- Apply SFA to recover SK'_{10}
- Repeat attack to either recover
  - SK_9 (in round 9) or
  - $SK''_{10} := SK_{10} \oplus 2^2 L$ of the next block the get SK_{10}

$\Rightarrow$ Attack complexity (number of needed faults) is doubled

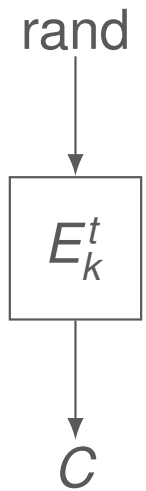
XEX-like Construction

- Output masked by Δ_k
  - $\Delta_k := \delta_k$
  - $\Delta_k := \delta_k + \delta_n$
  - $\Delta_k := \delta_{k,n}$

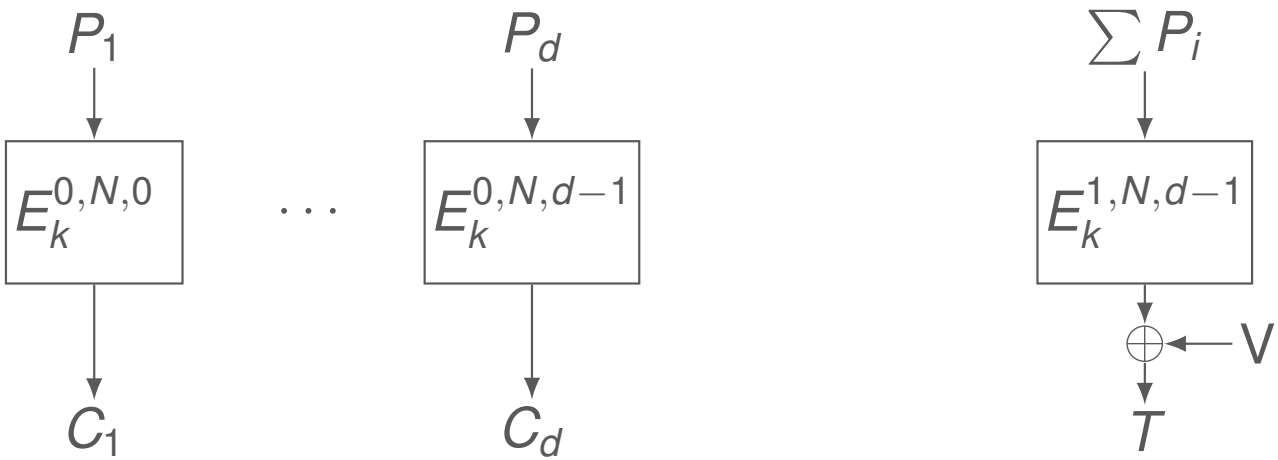


Tweakable Block Cipher

- TWEAKEY framework
  - Deoxys
  - KIASU
  - ...

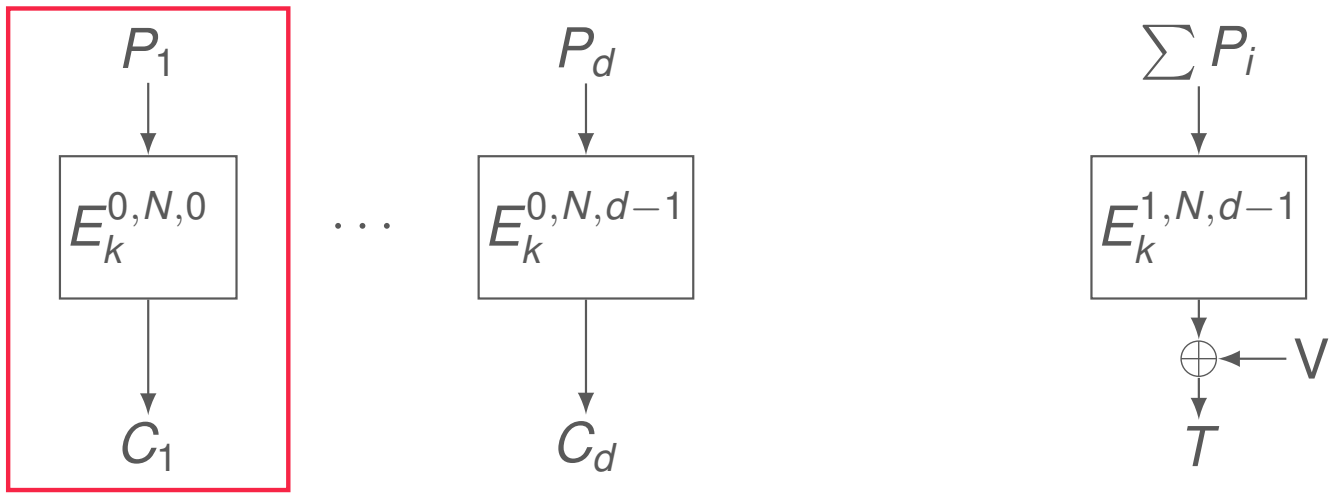


Attack on Deoxys$^{\neq}$



- Similar to OCB

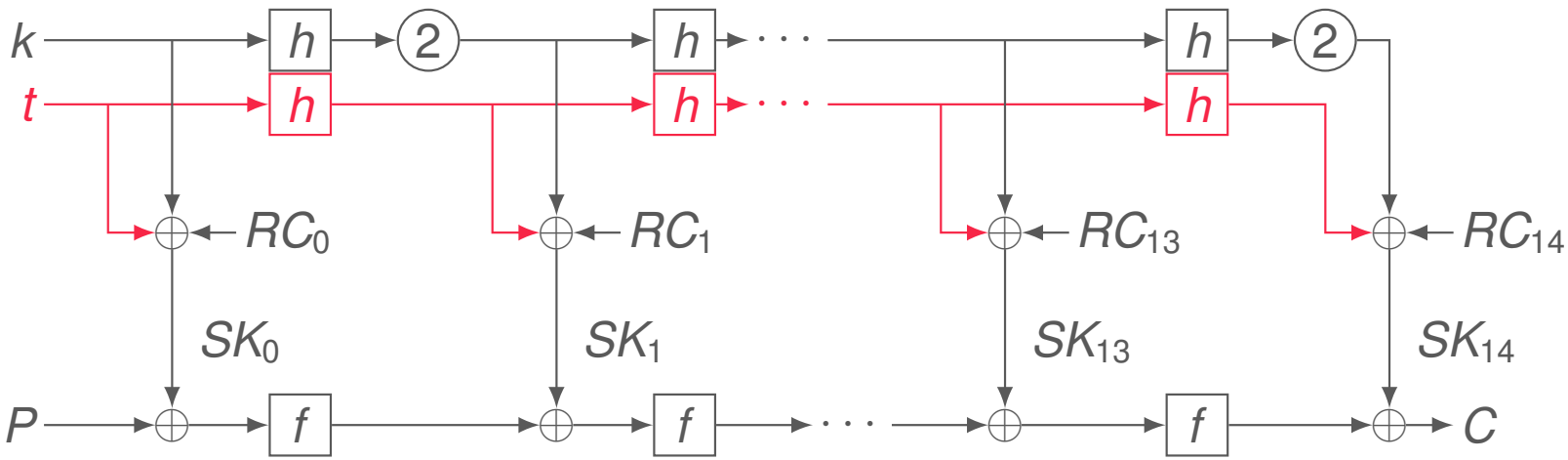
Attack on Deoxys$^{\neq}$



- Similar to OCB

Attack on Deoxys$^{\neq}$

- Deoxys-BC-256



Summary of Results

Primitive	Classification	Comments
CCM	basic	CTR
GCM	basic	CTR
EAX	basic	CTR
OCB	basic	XE
Cloc/Silc*	basic	CFB
OTR*	basic	XE
COPA*	XEX	
ELmD*	XEX	
SHELL*	XEX	
KIASU*	TBC	
Deoxys*	TBC	

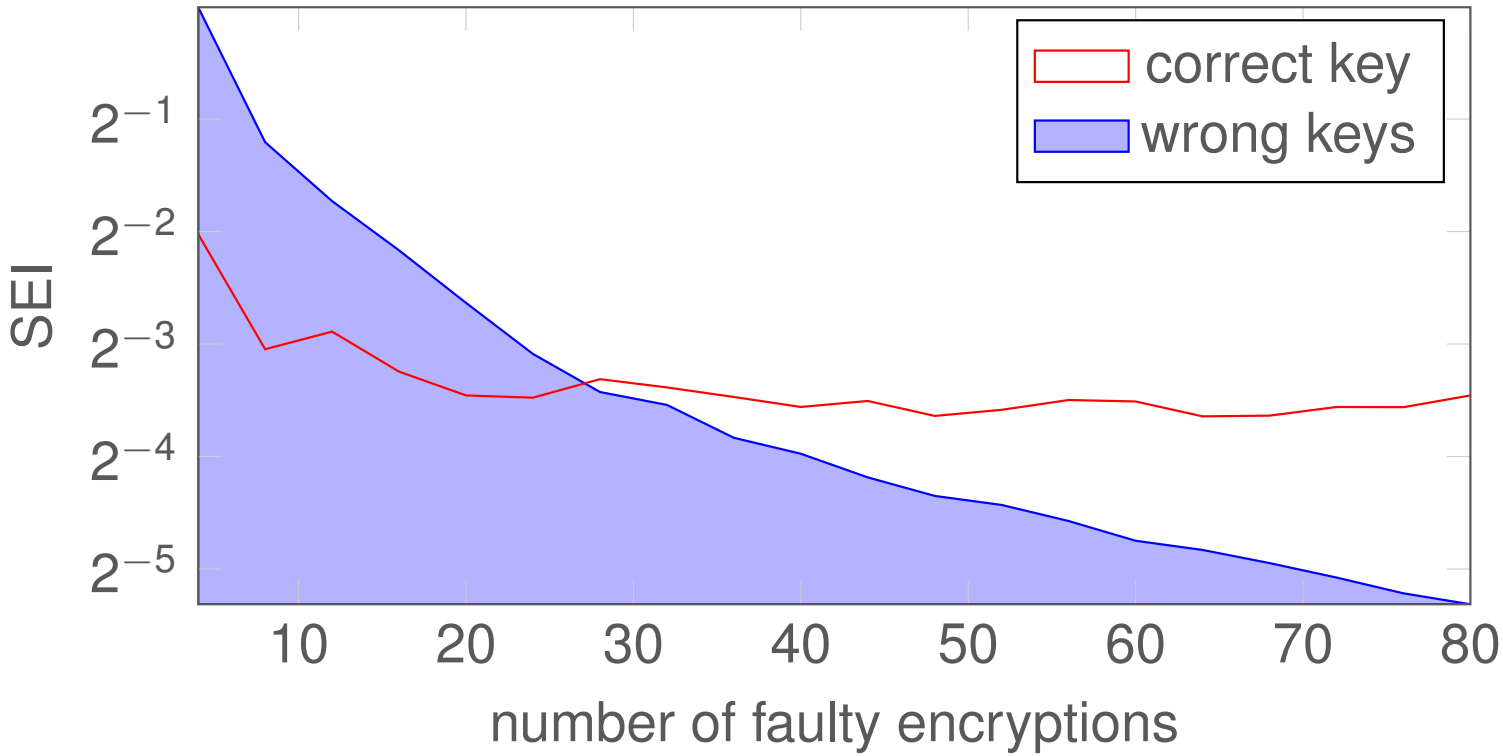
* CAESAR candidates

Practical Verification/Implementation

- Clock glitches
  - General-purpose microcontroller
  - AES software implementation
  - AES hardware co-processor
- Laser fault injection
  - Smartcard microcontroller
  - AES hardware co-processor

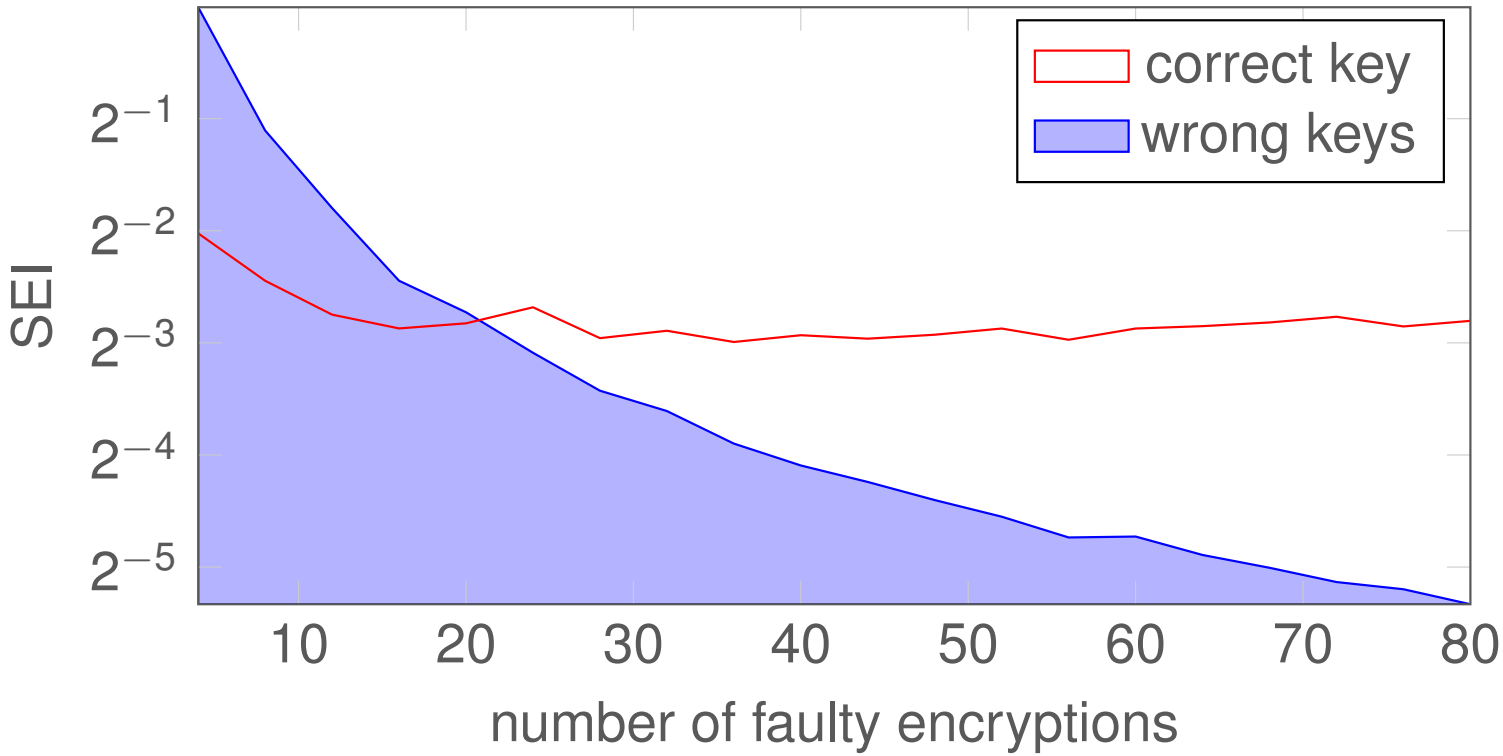
$\Rightarrow$ Key-recovery with a small number of faulty ciphertexts

ATxmega 256A3



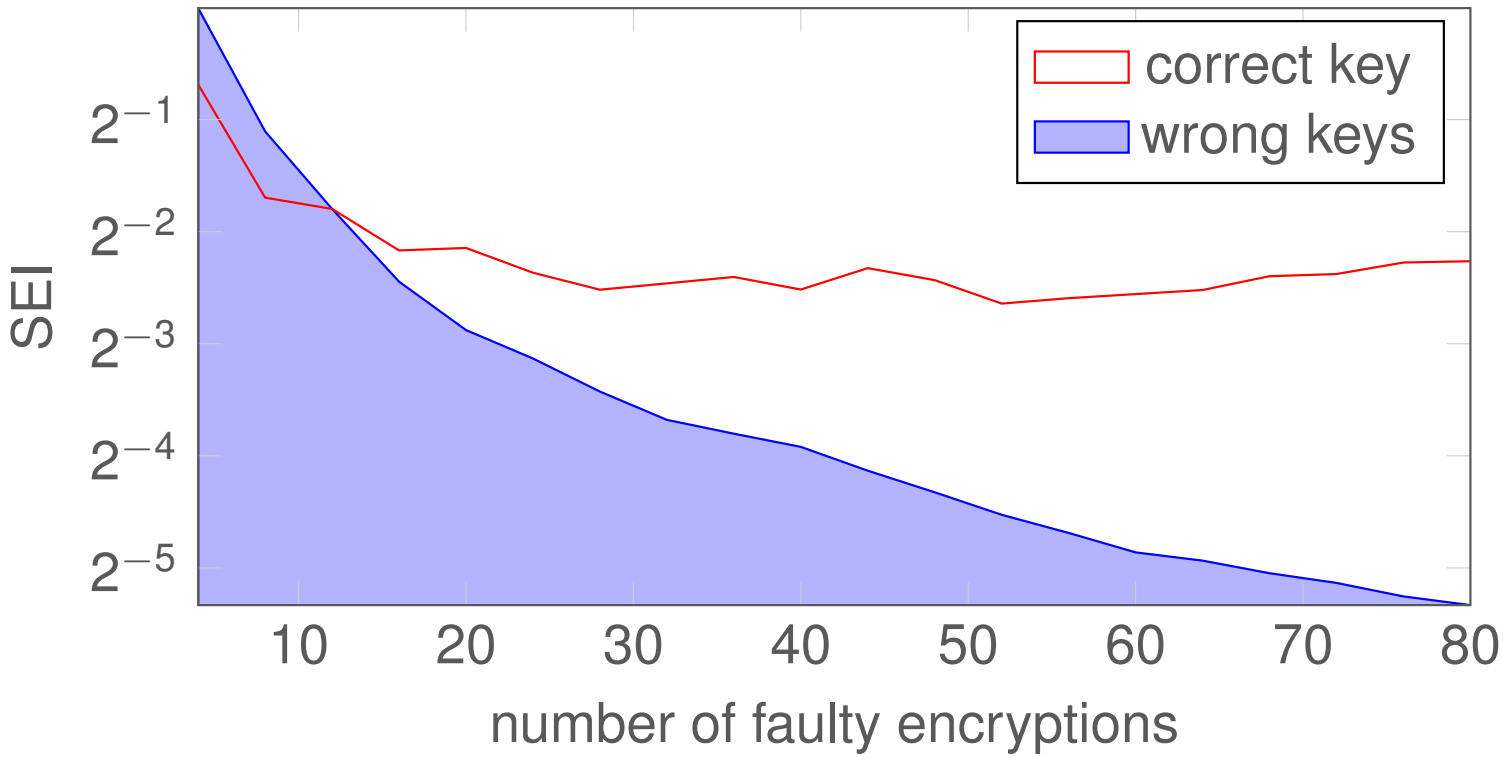
- Software implementation
- Single clock glitch

ATxmega 256A3



- Software implementation
- Multiple clock glitches

Smartcard Microcontroller



- AES co-processor
- Laser

Summary

- SFA is a powerful tool
- Nonce is not enough
- Attacks are not limited to AES-based modes

Thank you

http://eprint.iacr.org/2016/616

References

E. Biham and A. Shamir
Differential Fault Analysis of Secret Key Cryptosystems
CRYPTO 1997

D. Boneh, R. A. DeMillo, and R. J. Lipton
On the Importance of Checking Cryptographic Protocols for Faults
EUROCRYPT 1997

J. Blömer and V. Krummel
Fault Based Collision Attacks on AES
FDTC 2006

T. Fuhr, É. Jaulmes, V. Lomné, and A. Thillard
Fault Attacks on AES with Faulty Ciphertexts Only
FDTC 2013

C. Dobraunig, M. Eichlseder, T. Korak, V. Lomné, and F. Mendel
Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes
ASIACRYPT 2016