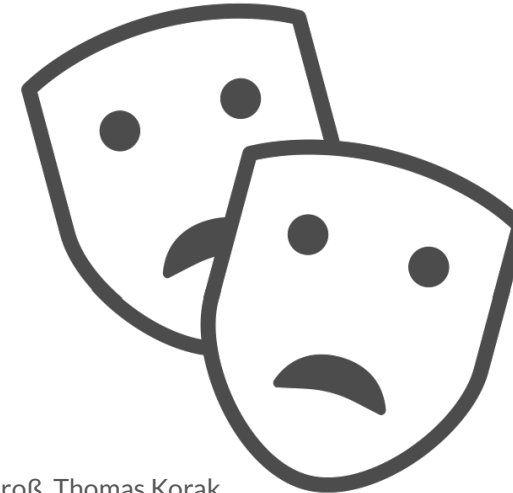
# SIFA

Statistical Ineffective Fault Attacks



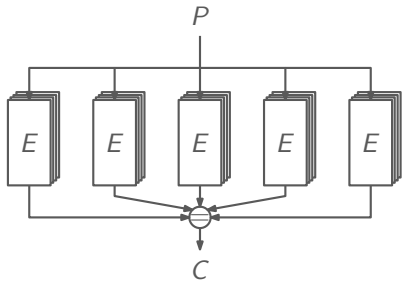
**Rump Session at CHES 2018**

Based on work of:
Christoph Dobraunig, Maria Eichlseder, Hannes Groß, Thomas Korak,
Stefan Mangard, Florian Mendel, Robert Primas

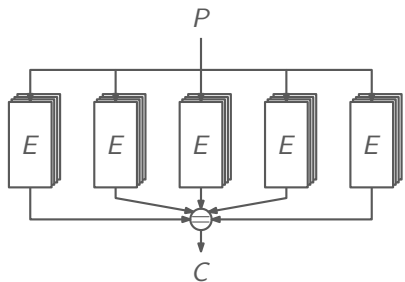
# Are Protected Implementations Hard to Attack?

# Are Protected Implementations Hard to Attack?

# Are Protected Implementations Hard to Attack?

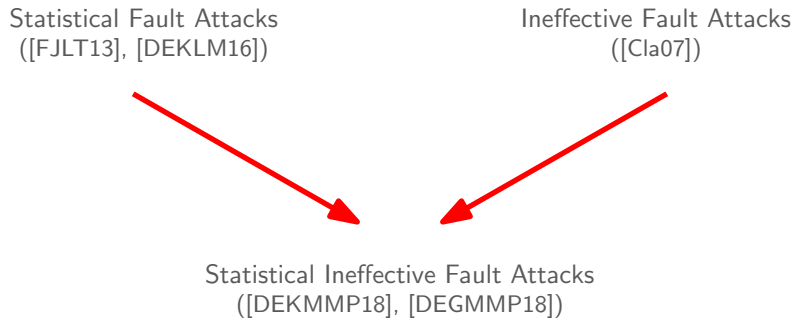


# Are Protected Implementations Hard to Attack?

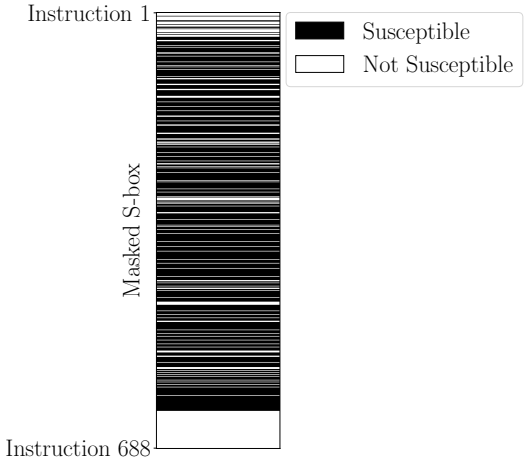



- SIFA can attack masked implementations of arbitrary order and with arbitrary error detection capabilities
  - single fault per execution of the primitive
  - typically effort does not significantly increase with higher protection order

# Path to SIFA


Statistical Fault Attacks
([FJLT13], [DEKLM16])
Ineffective Fault Attacks
([Cla07])
Statistical Ineffective Fault Attacks
([DEKMMP18], [DEGMMP18])

# Where to Fault?




- Example of masked AES in Software [SS16] and byte-stuck-at-0

# Which Fault Models?

- Successful attacks when we:
  - Flip one bit
  - Set one bit to zero
  - Randomize one bit
  - Flip one byte
  - Set one byte to zero
  - Randomize one byte
  - Skip an instruction
  - …

# Which Fault Models?

- Successful attacks when we:
  - Flip one bit
  - Set one bit to zero
  - Randomize one bit
  - Flip one byte
  - Set one byte to zero
  - Randomize one byte
  - Skip an instruction
  - …

# Which Fault Models?

- Successful attacks when we:
  - Flip one bit
  - Set one bit to zero
  - Randomize one bit
  - Flip one byte
  - Set one byte to zero
  - Randomize one byte
  - Skip an instruction
  - …

# Which Fault Models?

- Successful attacks when we:
  - Flip one bit
  - Set one bit to zero
  - Randomize one bit
  - Flip one byte
  - Set one byte to zero
  - Randomize one byte
  - Skip an instruction
  - …

# Which Fault Models?

- Successful attacks when we:
  - Flip one bit
  - Set one bit to zero
  - Randomize one bit
  - Flip one byte
  - Set one byte to zero
  - Randomize one byte
  - Skip an instruction
  - …

# Which Fault Models?

- Successful attacks when we:
  - Flip one bit
  - Set one bit to zero
  - Randomize one bit
  - Flip one byte
  - Set one byte to zero
  - Randomize one byte
  - Skip an instruction
  - …

# Which Fault Models?

- Successful attacks when we:
  - Flip one bit
  - Set one bit to zero
  - Randomize one bit
  - Flip one byte
  - Set one byte to zero
  - Randomize one byte
  - Skip an instruction
  - …

# Thank you

https://eprint.iacr.org/2018/071
https://eprint.iacr.org/2018/357

# Bibliography I


[Cla07] C. Clavier
Secret External Encodings Do Not Prevent Transient Fault Analysis
Cryptographic Hardware and Embedded Systems – CHES 2007

[DEGMMP18] C. Dobraunig, M. Eichlseder, H. Gross, S. Mangard, F. Mendel, and R. Primas
Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures
To appear at ASIACRYPT 2018, 2018

[DEKLM16] C. Dobraunig, M. Eichlseder, T. Korak, V. Lomné, and F. Mendel
Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes
Advances in Cryptology – ASIACRYPT 2016

[DEKMMP18] C. Dobraunig, M. Eichlseder, T. Korak, S. Mangard, F. Mendel, and R. Primas
SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography
IACR Transactions on Cryptographic Hardware and Embedded Systems 2018:3, 2018

# Bibliography II


[FJLT13] T. Fuhr, É. Jaulmes, V. Lomné, and A. Thillard
Fault Attacks on AES with Faulty Ciphertexts Only
Fault Diagnosis and Tolerance in Cryptography – FDTC 2013

[SS16] P. Schwabe and K. Stoffelen
All the AES You Need on Cortex-M3 and M4
Selected Areas in Cryptography – SAC 2016