KU LEUVEN

The Random Fault Model

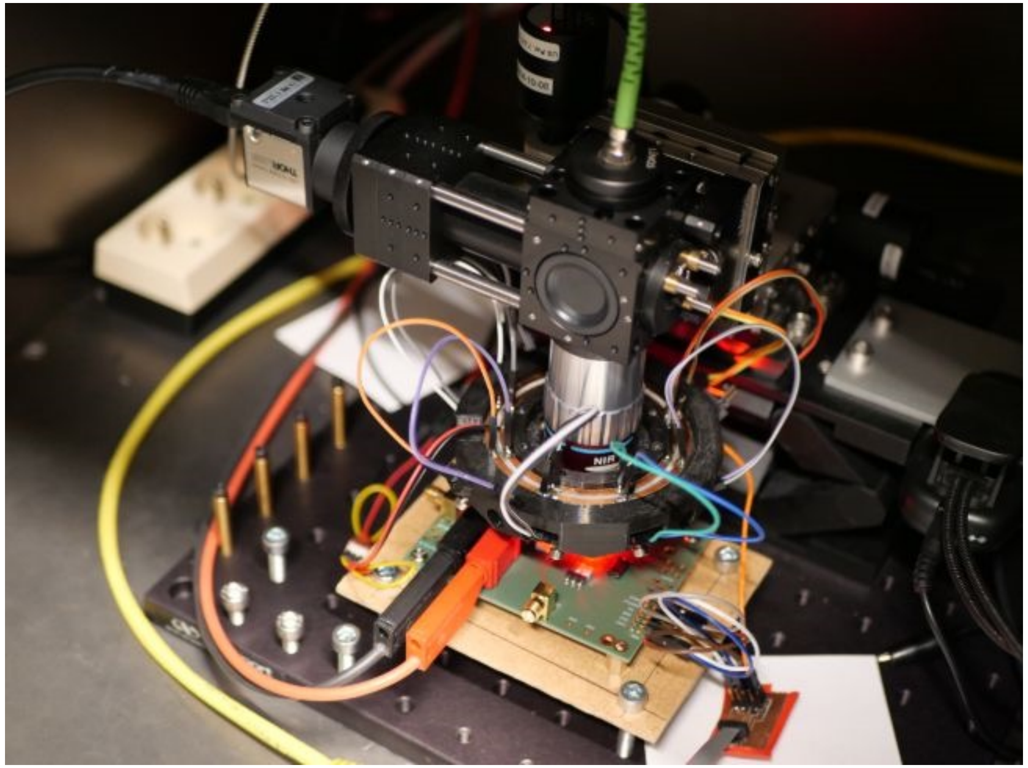
Siemen Dhooghe & Svetla Nikova
SAC 2023

COSIC

Fault Attacks & Adversary Models

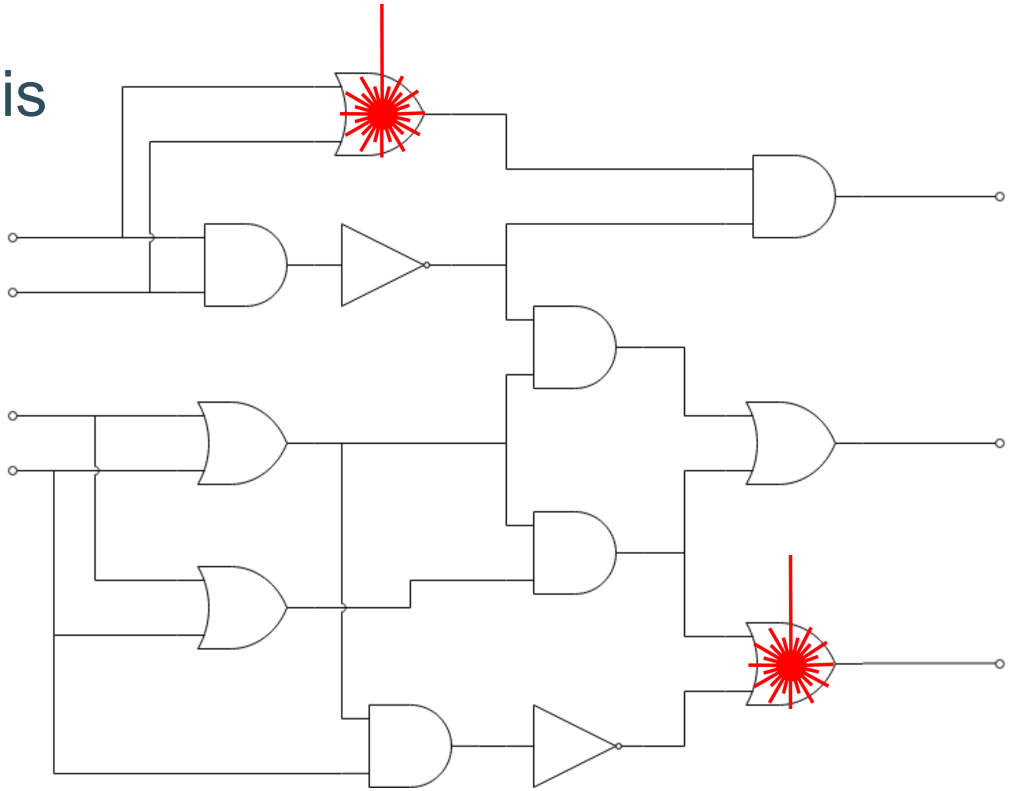
- Protection of embedded device's against physical attacks

- A need to algorithmically secure implementations
  - Platform-independent
  - Quantifiable security



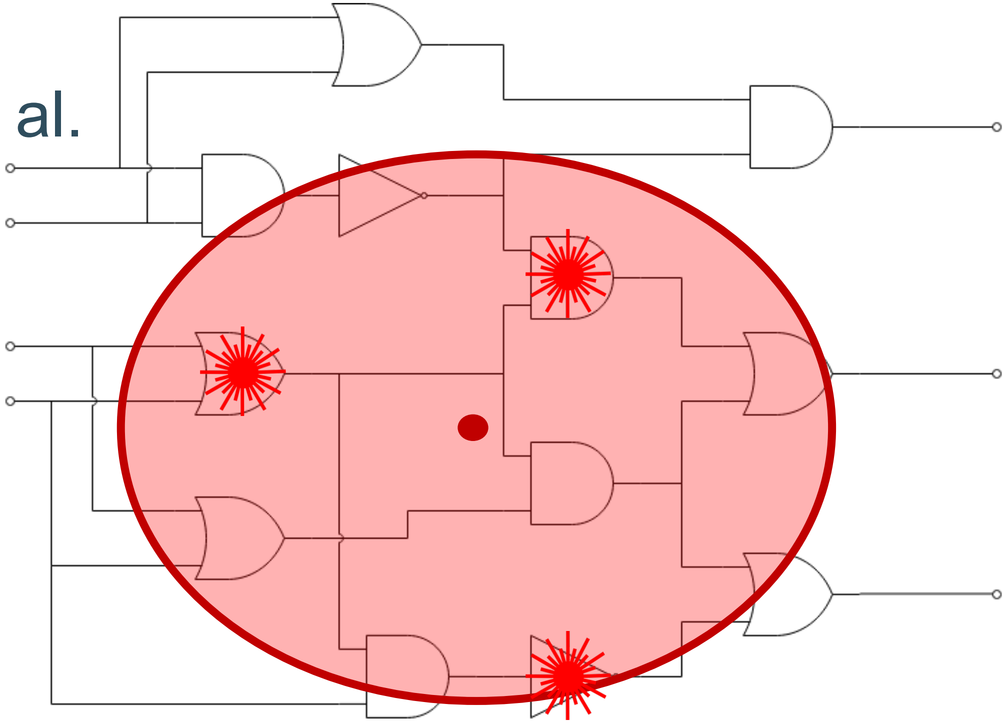
The Threshold Fault Model

- Current most-used model
- Allows for a theoretical analysis



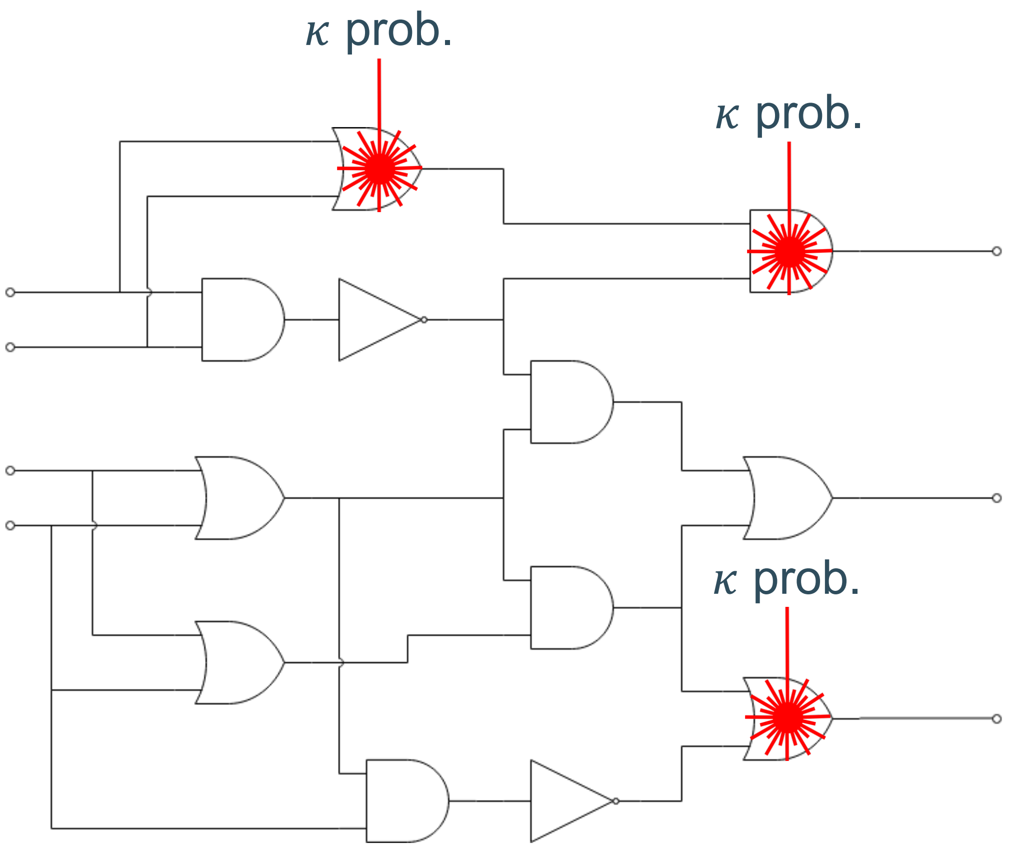
The Threshold Fault Model

- Not how real attacks work
- Mismatch has real effects
  - Examples by Bartkewitz et al. in CHES 2022
- Real modelling requires more details than what algorithms give



The Random Fault Model

- The new model
  - An adversary can target all gates/wires but each fault has a limited prob. to succeed
- A little closer to practice
  - Not fully there
- Still allows for theoretical analysis



KU LEUVEN

Correctness and Privacy Models

- Correctness: Advantage to get an incorrect ciphertext (not abort)
  - Can be related to DFA-like attacks

- Privacy: Advantage to guess some secret only given whether the circuit aborts or not
  - Can be related SIFA-like attacks

Results: Masking

- For n shares, the security decreases n times

$$\mathrm{Adv}(\mathcal{A}) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i+1} \kappa^{2i+1} (1-\kappa)^{n-2i-1} = \frac{1}{2}\left(1 - (1-2\kappa)^n\right) \leq n\kappa$$

Results: Error Detection

- For duplication, the security increases exponentially with the number of duplicates
- For linear codes, we repeat Bartkewitz's experiments

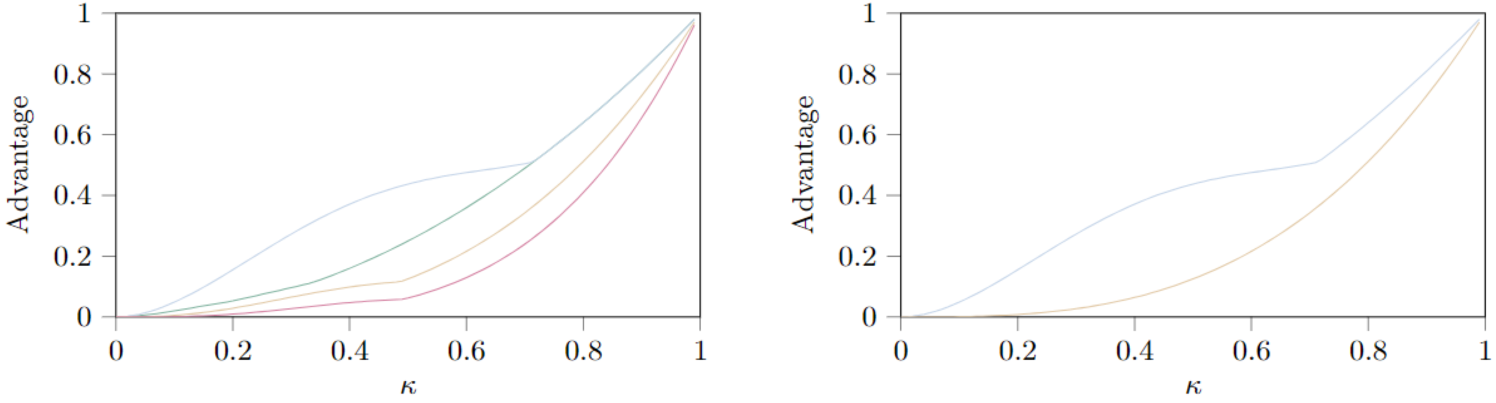


Fig. 5. The advantage of a random fault adversary against encoded values on the left and on the right when only the message bits are attacked. Blue depicts the $[5, 4, 2]$ code, green $[8, 4, 2]$, yellow $[7, 4, 3]$, and red $[8, 4, 4]$. For the right figure, the $[8, 4, 2]$ and $[8, 4, 4]$ codes have advantage zero.

Results: Error Correction

- The security of triplication is lower if the state size increases versus duplication

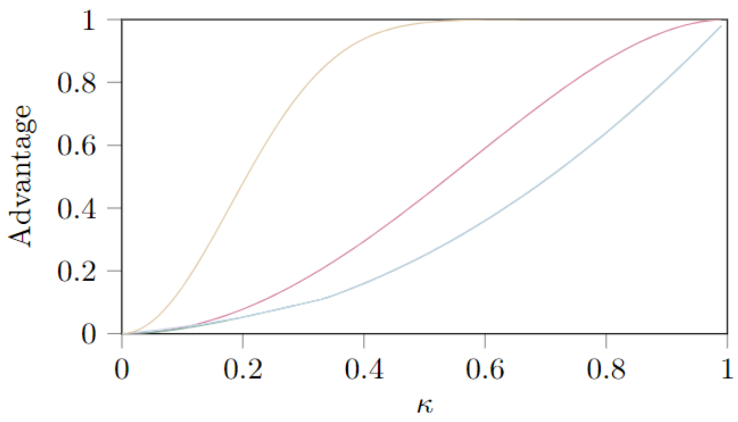


Fig. 6. The advantage against error correction (with three duplicates) is shown in red (for $m = 2$) and yellow ($m = 16$). The advantage against error detection (with two duplicates) is shown in green (for $m = 2$) and blue ($m = 16$).

Results: Shuffling

- The Rocky countermeasure by Miteloudi et al. considers shuffling values to resist fault attacks
- We show that both in correctness and privacy models there are weak inputs which do not give an improvement in protection
- For some values of κ, shuffling no additional protection
- Currently, we have no formal argument showing shuffling’s security against fault attacks

Conclusions & Open Problems

- The work also considered random probing
  - Showed that shuffling provides no significant protection in the random probing model
- Several countermeasures are not yet studied (random probing or fault)
  - Multiplicative masking
  - Arithmetic masking
  - Prime field masking
- Study combined security or the security of operations

Thank you!