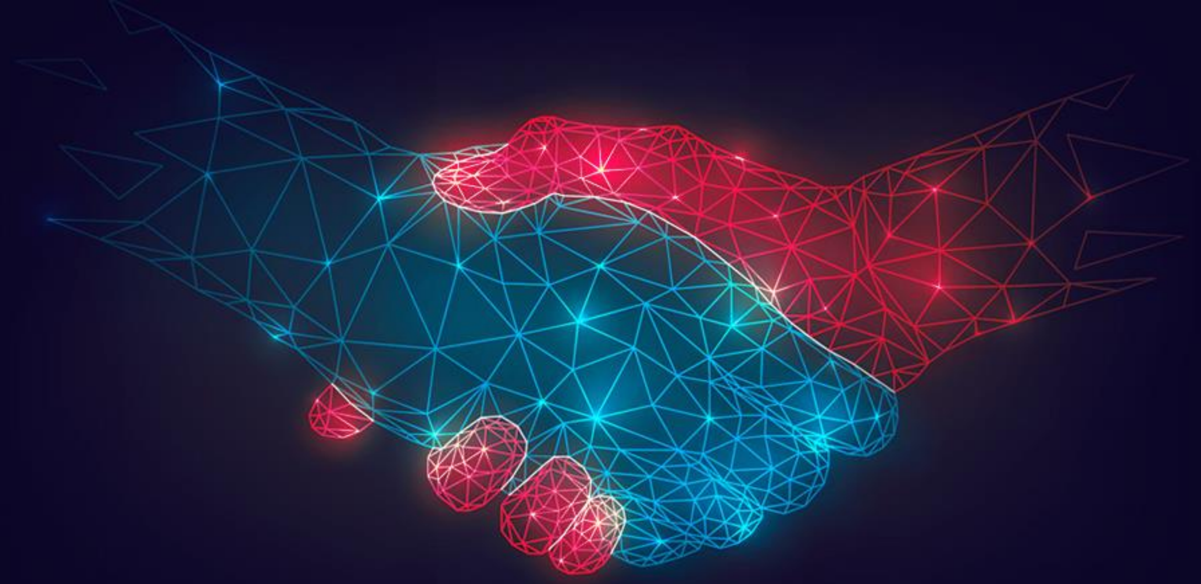


Beware of Insufficient Redundancy

An Experimental Evaluation of Code-based FI Countermeasures

Timo Bartkewitz, Sven Bettendorf, Thorben Moos, Amir Moradi, Falk Schellenberg

TÜViT, UCLouvain, University of Cologne, MPI for Security and Privacy

What‘s that all about?

- Internet Of Things
    - Access to cheap hardware
    - Optimized for low area and fast execution times
    - Lightweight Ciphers (SKINNY)

- Fault injection pose a serious threat (DFA, SIFA)
- Any unprotected cryptographic implementation is vulnerable
- Standard countermeasures are :
    - Shields, Sensors
    - Redundancy in various forms

What‘s new?

- *Impeccable Circuits*[1]
  - Protection against DFA
  - Follow-Up work offers protection against SIFA[2, 3]
  - Concurrent-Error-Detection (CED) based on Error-Correction-Code (ECC)
  - Focused on Fault Propagation
  - Security is reliant to the underlying adversary model

“[…] guarantees the detection of any fault in a hardware circuit that is covered by the underlying EDC[1].“

- How hard is it to inject fault that are not covered by the underlying EDC ?

[1] Aghaie, et. al., Impeccable Circuits. *IEEE Trans. Computers*, 69(3):361–376, 2020.
[2] Rezaei Shahmirzadi, et. al., Impeccable Circuits II. In DAC 2020, pages 1–6. IEEE, 2020.
[3] Rasoolzadeh, et. al., Impeccable Circuits III. In ITC 2021, pages 163–169. IEEE, 2021.

Impeccable Circuits – Variants

RED1 [5,4,2]:

- Parity bit (1 bit redundancy/nibble)
- Guaranteed 1 bit fault detection over entire encryption

RED3 [7,4,3]:

- Hamming code (3 bits redundancy/nibble)
- Guaranteed 2 bits fault detection over entire encryption

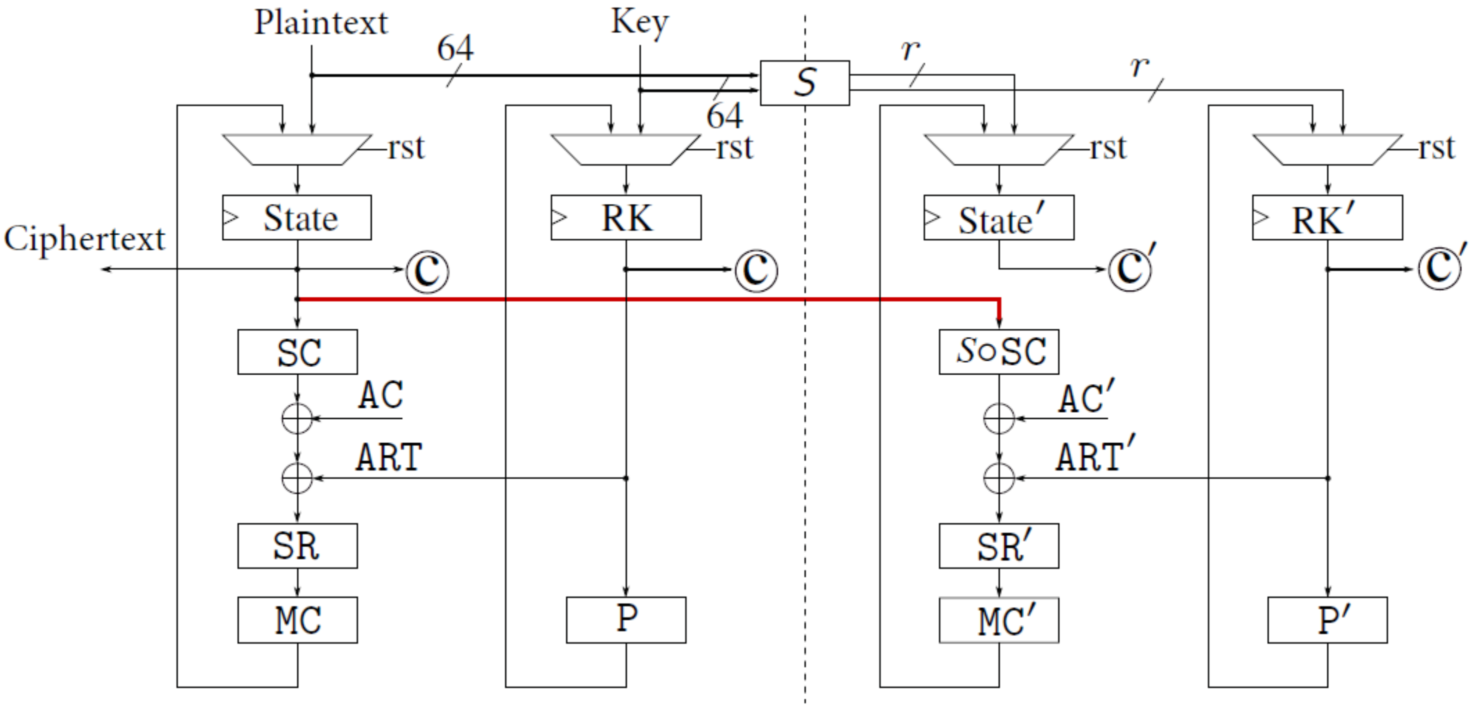
RED4 [8,4,4]:

- Extended Hamming code (4 bits redundancy/nibble)
- Guaranteed 3 bits fault detection over entire encryption

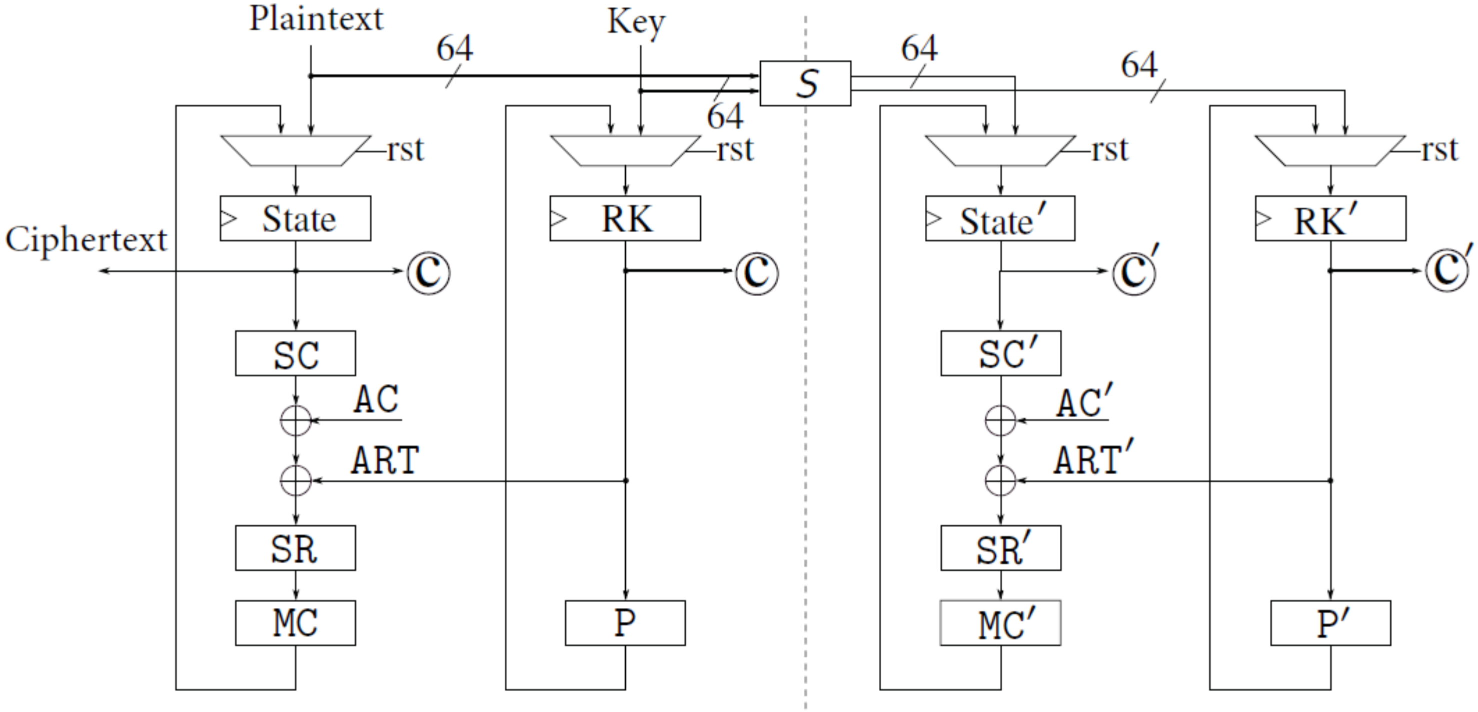
Multivariate Adversary Model:

- Extension to detect faults injected over multiple clock cycles
- Example: RED4: Guaranteed 3 bits fault detection at every clock cycle

Impeccable Circuits – No Full Redundancy



Impeccable Circuits – Full Redundancy



Impeccable Circuits – Post Layout Implementation Details

SKINNY core	Area [GE]	Crit. Path [ns]	Power [µW]
unprotected	2670.00	3.95	154.75
duplication	4997.25	4.82	279.26
RED 1	4130.00	4.30	206.15
RED 1 multivariate	4405.75	6.73	213.63
RED 3	5738.75	4.32	290.38
RED 3 multivariate	6849.75	6.99	315.94
RED 4	6878.75	4.52	334.37
RED 4 multivariate	8305.75	7.95	366.92

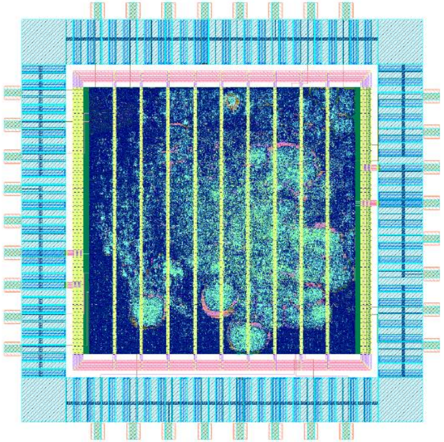
Impeccable Circuits – Post Layout Implementation Details

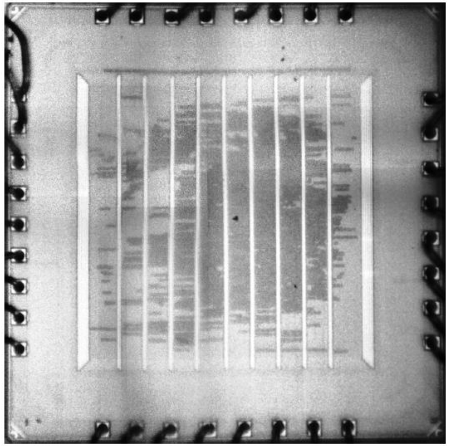
SKINNY core	Area [GE]	Crit. Path [ns]	Power [µW]
unprotected	2670.00	3.95	154.75
d[illegible]lication	4997.25	4.82	279.2[illegible]
R[illegible]	[illegible]	[illegible]	[illegible]
RED 1 multivariate	4405.75	6.73	213.63
RED 3	5738.75	4.32	290.38
RED 3 multiva[illegible]	[illegible]	[illegible]	31[illegible].94
RED 4	[illegible]	[illegible]	3[illegible]4.37
RED 4 multivariate	8305.75	7.95	366.92

Based on reasonable assumptions?

Experimental Proof

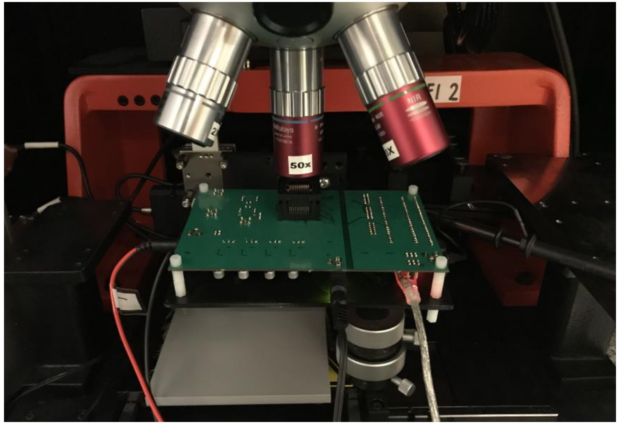
- ASIC in a 40nm low power CMOS technology
- LFI on backside
- Neodymium-doped Yttrium Aluminum Garnet (Nd:YAG)
- Spot-Size: 5.6 x 5.6 µm
  28 x 28 µm
- Detect-and-suppress principle

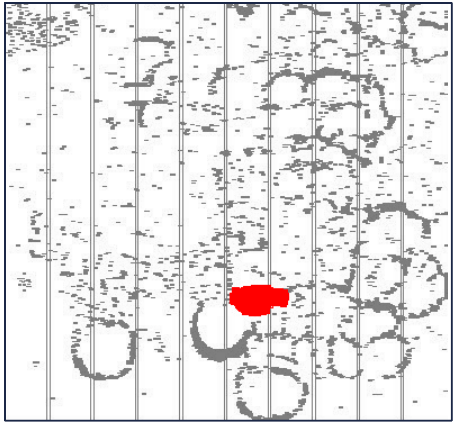


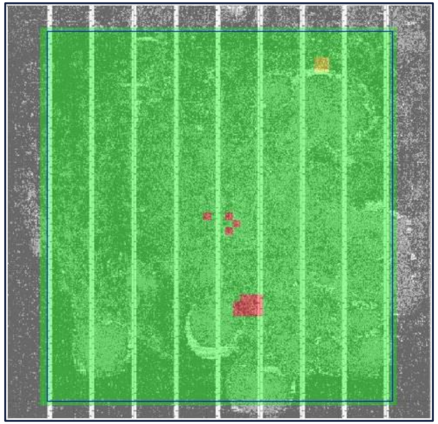


Preparation

1. Package opening
2. Thin the silicon on the backside
3. Polishing the ASIC
4. Laser Fault Attack







Experimental Results

Unprotected implementation:
- Possible to receive faulty output
- **Successful DFA**
- Success in ~60% of the attempts

Duplication:
- Not possible to receive faulty output
- **Unsuccessful DFA**
- Only suppressed responses (0x0)

Experimental Results

Unprotected implementation:
- Possible to receive faulty output
- **Successful DFA**
- Success in ~60% of the attempts

Duplication:
- Not possible to receive faulty output
- **Unsuccessful DFA**
- Only suppressed responses (0x0)

Everything as expected

Experimental Results

RED1 :
- Possible to receive faulty output
- **Successful DFA**
- **Success in 0.3% - 0.9%** of the attempts

RED3:
- Possible to receive faulty output
- **Successful DFA**
- **Success in 0.02% - 0.09%** of the attempts

RED4:
- Not possible to receive faulty output
- **Unsuccessful DFA**
- Only suppressed responses (0x0)

Overview

SKINNY Core	Laser Spot Size	Inform. Faults/Attempt	Key Extraction
unprotected	28.0 µm	57.5758%	✓
	5.6 µm	8.0994%	✓
duplication	28.0 µm	0.0000%	✗
	5.6 µm	0.0000%	✗
RED 1	28.0 µm	0.3141%	✓
	5.6 µm	0.4123%	✓
RED 1 multivariate	28.0 µm	0.9110%	✓
	5.6 µm	0.5030%	✓
RED 3	28.0 µm	0.0298%	✓
	5.6 µm	0.0817%	✓
RED 3 multivariate	28.0 µm	0.0570%	✓
	5.6 µm	0.0586%	✓
RED 4	28.0 µm	0.0000%	✗
	5.6 µm	0.0000%	✗
RED 4 multivariate	28.0 µm	0.0000%	✗
	5.6 µm	0.0000%	✗

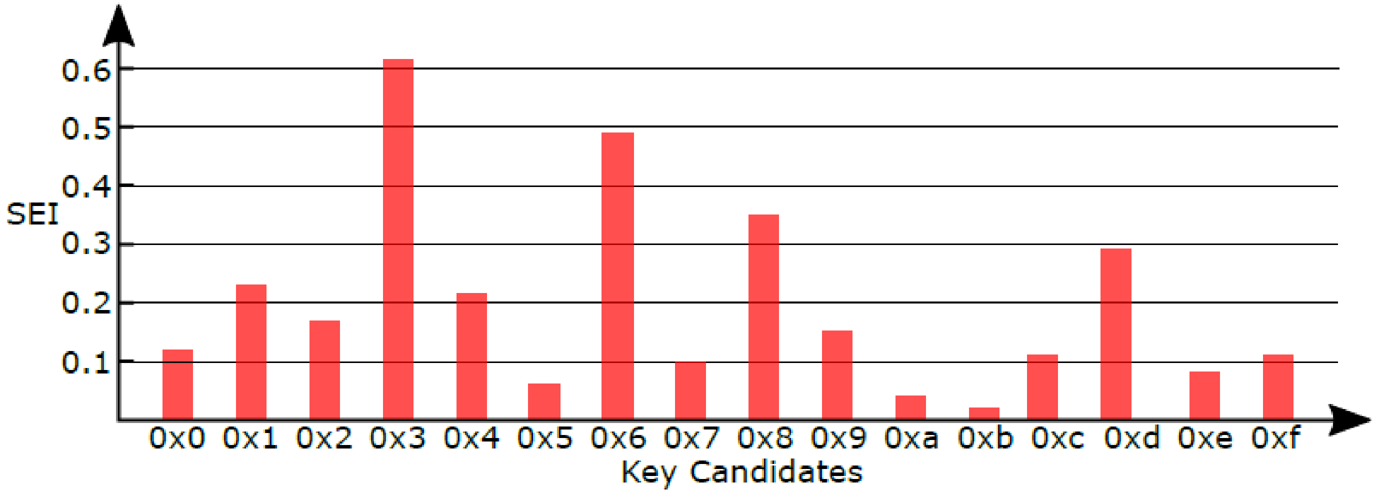
Overview

SKINNY Core	Laser Spot Size	Inform. Faults/Attempt	Key Extraction
unprotected	28.0 µm	57.5758%	✓
	5.6 µm	8.0994%	✓
duplication	28.0 µm	0.0000%	✗
	5.6 µm	0.0000%	✗
RED 1	28.0 µm	0.31[illegible]%	✓
	5.6 µm	0.412[illegible]%	✓
RED 1 multivariate	28.0 µm	0.9110%	✓
	5.6 µm	0.5030%	✓
RED 3	28.0 µm	0.0298%	✓
	5.6 µm	0.08[illegible]7%	✓
RED 3 multivariate	28.0 µm	0.05[illegible]0%	✓
	5.6 µm	0.05[illegible]%	✓
RED 4	28.0 µm	0.0000%	✗
	5.6 µm	0.0000%	✗
RED 4 multivariate	28.0 µm	0.0000%	✗
	5.6 µm	0.0000%	✗

Duplication sufficient to resist fault attacks?

Threats to Simple Duplication

- Double Laser Attack
- Attacks against detect-and-suppress principle exist
    - Statistic Ineffective Fault Attack



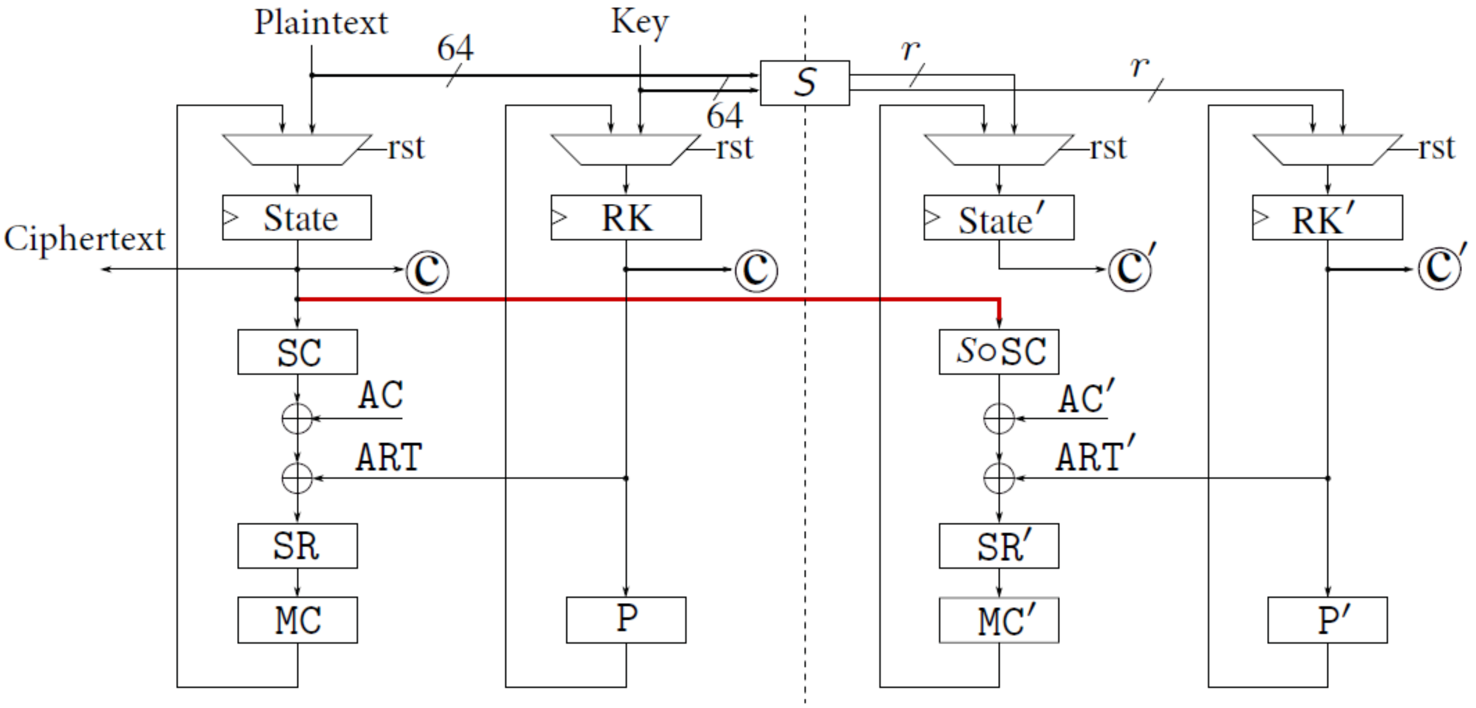
Conclusions

- 1-bit and 3-bit redundancy is not sufficient per nibble
- Simple redundancy can offer better results as complex codes
- It is easier to inject multiple bit faults than single bit faults

- The adversary assumptions are only realistic for RED4
    - Offers more security than simple redundancy
    - Expensive in area

"We would like to stress the importance of verifying the assumptions and hypotheses [...] in real-world experiments."

Conclusions – No Full Redundancy



Conclusions

- 1 bit and 3 bit redundancy is not sufficient per nibble
- Simple redundancy can offer better results as complex codes
- It is easier to inject multiple bit faults than single bit faults

- The adversary assumptions are only realistic for RED4
    - Offers more security than simple redundancy
    - Expensive in area

"We would like to stress the importance of verifying the assumptions and hypotheses [...] in real-world experiments."

Questions ?!