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
- **Impeccable Circuits**
  - Protection against DFA
  - Follow-Up work offers protection against SIFA
  - 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.”

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

---

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**

Diagram showing the flow of plaintext and key through a circuit, with operations like SC, AC, ART, SR, MC, RK, and State. The diagram includes arrows indicating the flow and transformations between different components.
Impeccable Circuits – Full Redundancy

plaintext

64

State

rst

Ciphertext

64

Key

64

S

64

State’

rst

64

RK

C

64

C’

64

RK’

C

C’

SC

AC

ART

SR

MC

SC’

AC’

ART’

SR’

MC’

P

P’
<table>
<thead>
<tr>
<th>SKINNY core</th>
<th>Area [GE]</th>
<th>Crit. Path [ns]</th>
<th>Power [μW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>unprotected</td>
<td>2670.00</td>
<td>3.95</td>
<td>154.75</td>
</tr>
<tr>
<td>duplication</td>
<td>4997.25</td>
<td>4.82</td>
<td>279.26</td>
</tr>
<tr>
<td>RED 1</td>
<td>4130.00</td>
<td>4.30</td>
<td>206.15</td>
</tr>
<tr>
<td>RED 1 multivariate</td>
<td>4405.75</td>
<td>6.73</td>
<td>213.63</td>
</tr>
<tr>
<td>RED 3</td>
<td>5738.75</td>
<td>4.32</td>
<td>290.38</td>
</tr>
<tr>
<td>RED 3 multivariate</td>
<td>6849.75</td>
<td>6.99</td>
<td>315.94</td>
</tr>
<tr>
<td>RED 4</td>
<td>6878.75</td>
<td>4.52</td>
<td>334.37</td>
</tr>
<tr>
<td>RED 4 multivariate</td>
<td>8305.75</td>
<td>7.95</td>
<td>366.92</td>
</tr>
</tbody>
</table>
### Impeccable Circuits – Post Layout Implementation Details

<table>
<thead>
<tr>
<th>SKINNY core</th>
<th>Area [GE]</th>
<th>Crit. Path [ns]</th>
<th>Power [μW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>unprotected</td>
<td>2670.00</td>
<td>3.95</td>
<td>154.75</td>
</tr>
<tr>
<td>duplication</td>
<td>4997.25</td>
<td>4.82</td>
<td>279.20</td>
</tr>
<tr>
<td>RED</td>
<td>4230.00</td>
<td>4.52</td>
<td>200.41</td>
</tr>
<tr>
<td>RED 1 multivariate</td>
<td>4405.75</td>
<td>6.73</td>
<td>213.63</td>
</tr>
<tr>
<td>RED 3</td>
<td>5738.75</td>
<td>4.32</td>
<td>290.38</td>
</tr>
<tr>
<td>RED 3 multivariate</td>
<td>6243.75</td>
<td>4.70</td>
<td>314.94</td>
</tr>
<tr>
<td>RED 4</td>
<td>6520.75</td>
<td>4.12</td>
<td>334.37</td>
</tr>
<tr>
<td>RED 4 multivariate</td>
<td>8305.75</td>
<td>7.95</td>
<td>366.92</td>
</tr>
</tbody>
</table>

**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: $5.6 \times 5.6 \mu m$
  
  $28 \times 28 \mu m$
- 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

<table>
<thead>
<tr>
<th>SKINNY Core</th>
<th>Laser Spot Size</th>
<th>Inform. Faults/Attempt</th>
<th>Key Extraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>unprotected</td>
<td>28.0 μm</td>
<td>57.5758%</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>8.0994%</td>
<td>✓</td>
</tr>
<tr>
<td>duplication</td>
<td>28.0 μm</td>
<td>0.0000%</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>0.0000%</td>
<td>✗</td>
</tr>
<tr>
<td>RED 1</td>
<td>28.0 μm</td>
<td>0.3141%</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>0.4123%</td>
<td>✓</td>
</tr>
<tr>
<td>RED 1 multivariate</td>
<td>28.0 μm</td>
<td>0.9110%</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>0.5030%</td>
<td>✓</td>
</tr>
<tr>
<td>RED 3</td>
<td>28.0 μm</td>
<td>0.0298%</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>0.0817%</td>
<td>✓</td>
</tr>
<tr>
<td>RED 3 multivariate</td>
<td>28.0 μm</td>
<td>0.0570%</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>0.0586%</td>
<td>✓</td>
</tr>
<tr>
<td>RED 4</td>
<td>28.0 μm</td>
<td>0.0000%</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>0.0000%</td>
<td>✗</td>
</tr>
<tr>
<td>RED 4 multivariate</td>
<td>28.0 μm</td>
<td>0.0000%</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>5.6 μm</td>
<td>0.0000%</td>
<td>✗</td>
</tr>
</tbody>
</table>
## Overview

<table>
<thead>
<tr>
<th>SKINNY Core</th>
<th>Laser Spot Size</th>
<th>Inform. Faults/Attempt</th>
<th>Key Extraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>unprotected</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>duplication</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>RED 1</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RED 1 multivariate</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RED 3</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RED 3 multivariate</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RED 4</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>RED 4 multivariate</td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

DURATION 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 ?!