

Controlled Fault Injection: Wishful Thinking, Thoughtful Engineering, or just LUCK?

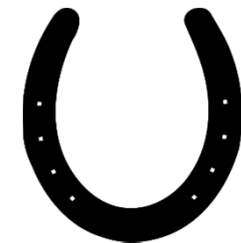


FDTC 2017 Panelists:

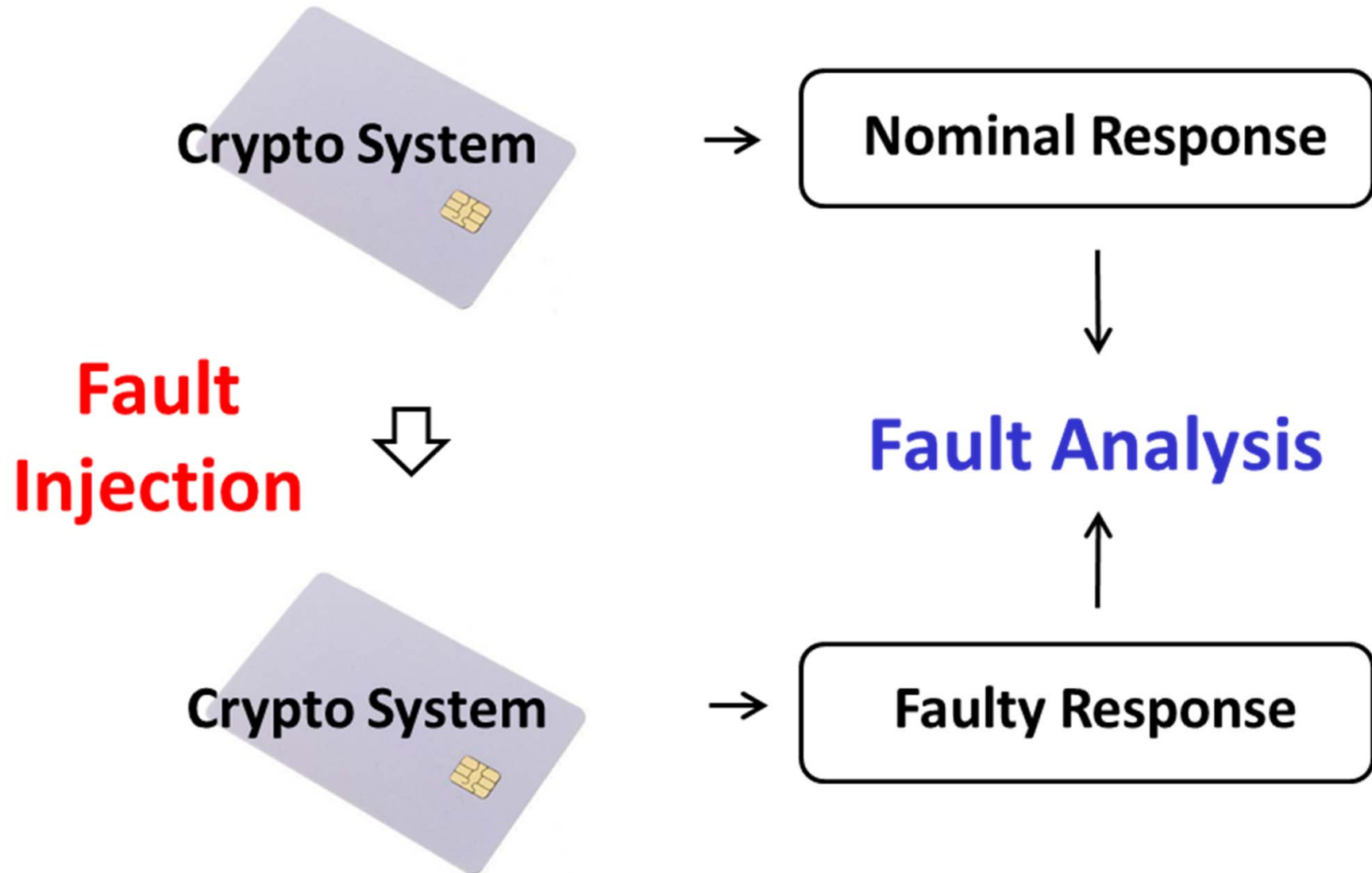
Ilia Polian,

Marc Joye, Ingrid Verbauwhede

Marc Witteman, Johann Heyszl



The Fault Attack Process



The Fault Attack Process

1999 Bellcore

....

2010 Single Fault AES

2012 Optimal Fault Attacks

Well understood
Solid Methodologies
DFA, Safe Error, ...

Nominal Response

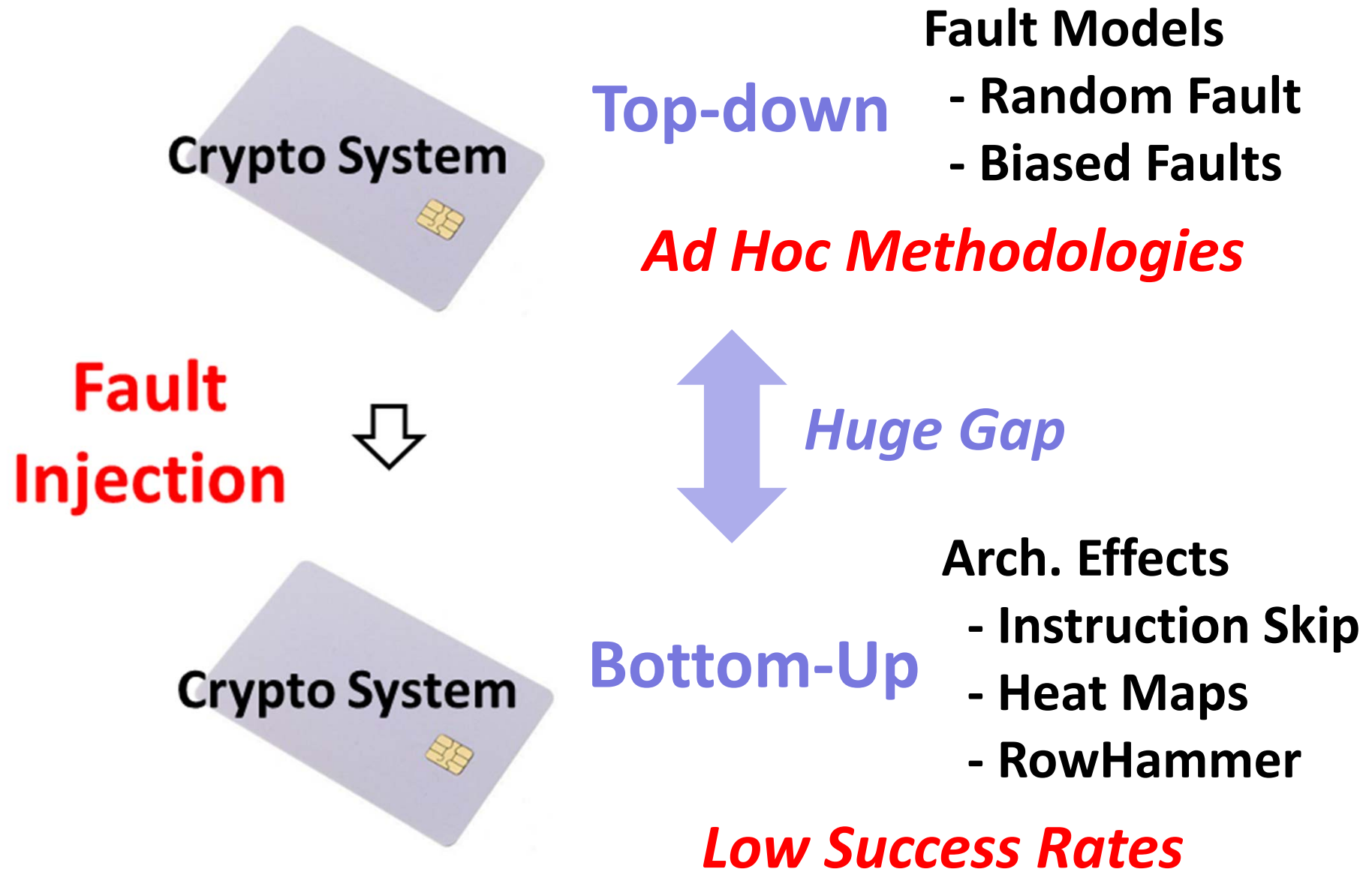


Fault Analysis



Faulty Response

The Fault Attack Process



Kick-off Questions

- 1. If side-channel attacks are driven by science and reason, fault attacks seem to look like **black magic**. Do we really understand fault attacks?**
- 2. What is the significance of fault attacks over time? Are they becoming more or less relevant?**
- 3. ...**

Panelist Statements



**Ilia
Polian**
Professor
Uni Passau



**Marc
Joye**
NXP Fellow



**Ingrid
Verbauwhede**
Professor KUL



**Marc
Witteman**
CEO Riscure



**Johann
Heszl**
Fraunhofer
AISEC



Panelist Statements



**Ilija
Polian
Professor
Uni Passau**



**Marc
Joye
NXP Fellow**



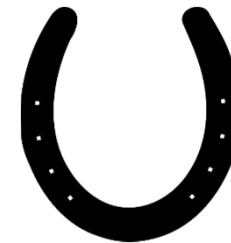
**Ingrid
Verbauwhede
Professor KUL**



**Marc
Witteman
CEO Riscure**



**Johann
Heszl
Fraunhofer
AISEC**



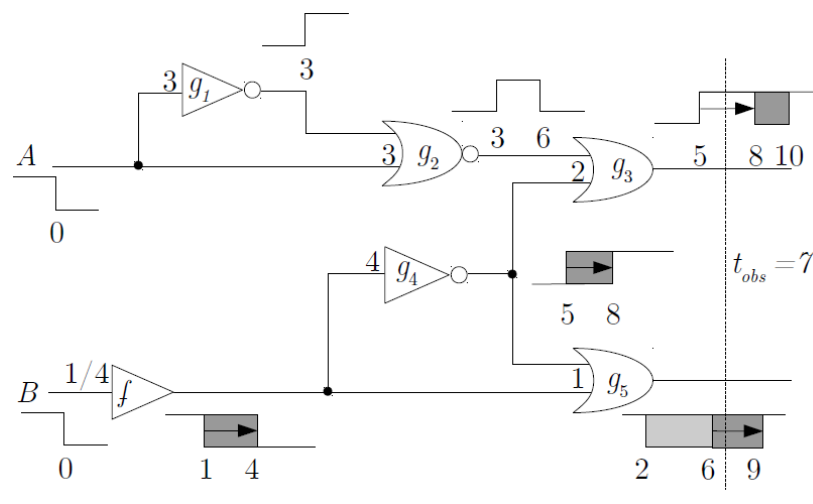
Ilia Polian

University of Passau

CONTROLLED FAULT INJECTION:
WISHFUL THINKING, THOUGHTFUL
ENGINEERING, OR JUST LUCK?

Do we really understand fault attacks?

- Yes, to some extent, but we could do better!
 - Observation-based, large amount of trial-and-error.
 - Detailed understanding is not considered essential.
 - Even a simple glitch can have complex implications.



Need for more accurate models?

- **Glitch: Which paths to outputs are sensitized?**
 - Influenced by parasitics, power-supply noise, reconvergencies, etc.
- **Laser, EM, ... Even more complex.**
 - Multiphysics modeling.
- **We cannot have full predictive power.**
 - Process variability, ambient parameters, unknown inputs.
- **There is vast amount of models from test, diagnostics, and reliability domain which seem to work.**

Significance of fault attacks over time?

- If we had better models, will they lead to more effective attacks?
 - „First-time right“ injection in presence of detectors.
- Or can we design better countermeasures, if we know exactly what fault-injections are possible?
 - E.g., special error-detecting codes?
- Models must balance accuracy against scalability.
- Apart from „application-oriented“ benefits, better understanding of malicious failures can be a valuable intellectual result in itself.

Panelist Statements



**Ilia
Polian
Professor
Uni Passau**



**Marc
Joye
NXP Fellow**



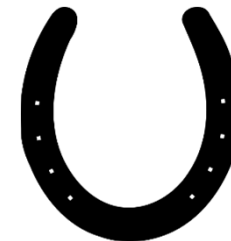
**Ingrid
Verbauwhede
Professor KUL**




**Marc
Witteman
CEO Riscure**



**Johann
Heszl
Fraunhofer
AISEC**





Marc Joye, NXP Semiconductors
Panel discussion @ FDTC 2017 -- Taipei, Taiwan
09/24/2017

Fault Attacks: Science or Black Magic?



Fault Attacks: Science or Black Magic?

Depends who you ask!

Fault attacks are not black magic

Semiconductor devices are sensitive to light by nature

Side-channel analysis (SCA) may appear more driven by science

More knowledge is needed to apply an exploitable attack using SCA

General attacker does not really care what is really happening in the chip if the fault attack is working

Vulnerability analysis teams have of course to understand the root cause

Significance/Relevance of Fault Attacks?

Security is a moving target

Implementation attacks (incl. side channels and faults) are evolving and keep their relevance

Analysts (hackers) have access to a variety of fault-injection techniques that greatly improved over time

Security certification requires products to comply to security targets

Fault Attacks: Today and Tomorrow

Fault attacks: science vs. black magic

Side-channel attacks vs. fault attacks

Crypto community is very diverse

Future of fault attacks

Combined attacks can unleash the full power of fault attacks

Deep understanding helps designing the best protection methods

Panelist Statements



**Ilia
Polian
Professor
Uni Passau**



**Marc
Joye
NXP Fellow**



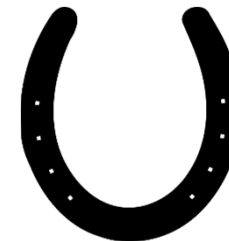
**Ingrid
Verbauwhede
Professor KUL**



**Marc
Witteman
CEO Riscure**



**Johann
Heszl
Fraunhofer
AISEC**





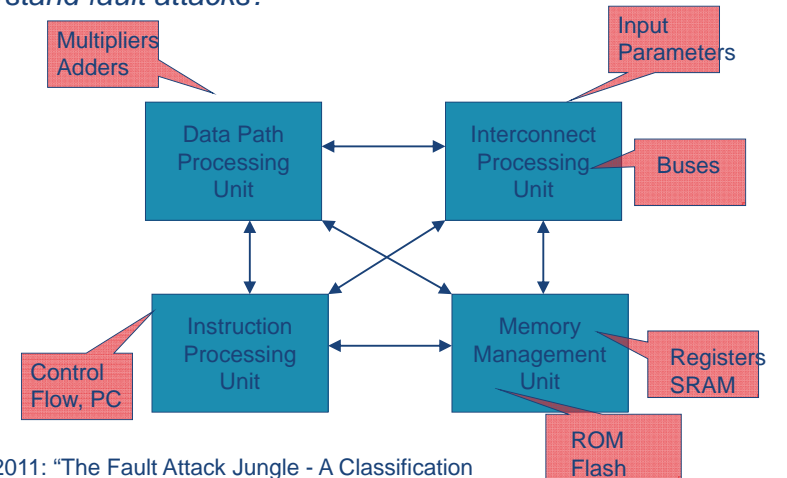
Panel on Fault Attacks

3 slides

Ingrid Verbauwhede
COSIC, KU Leuven



If side-channel attacks are driven by science and reason, fault attacks seem to look like black magic. Do we really understand fault attacks?

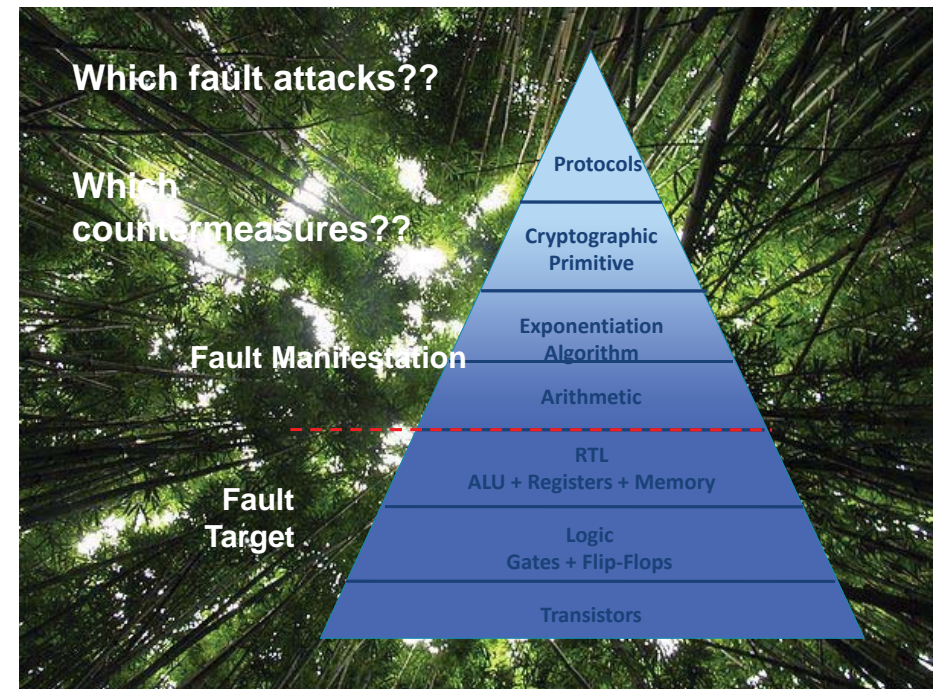


[FDTG 2011: "The Fault Attack Jungle - A Classification Model to Guide You" I. Verbauwhede]

What is the significance of fault attacks over time? Are they becoming more or less relevant?

- Become more relevant: attacker always looks for the weakest link. If good protection against side channel attacks, then try fault attacks
- IOT devices more and more in the hand of the end-user (= attacker). Thus much more opportunity to try attacks
- Fault attacks = active attacks
 - So, I can detect them with sensors! Clock/power glitch, EM attack, laser attack, temperature attack
- Challenge: **COMBINED** fault and side-channel attack AND countermeasures

21



Panelist Statements



**Ilia
Polian
Professor
Uni Passau**



**Marc
Joye
NXP Fellow**



**Ingrid
Verbauwhede
Professor KUL**



**Marc
Witteman
CEO Riscure**



**Johann
Heszl
Fraunhofer
AISEC**



The logo for RISCURE, featuring the word in a bold, lowercase, sans-serif font. The background is a light green gradient with a large, dark green curved shape on the right side.

riscure

Controlled Fault Injection

*wishful thinking, thoughtful
engineering, or just luck?*

FDTC

September 25, 2017

Fault Injection

Science

~~or~~

Skill

AND

DFA on RSA CRT

Inject a fault during CRT that corrupts S_q :

S'_q is a corrupted result of S_q computation

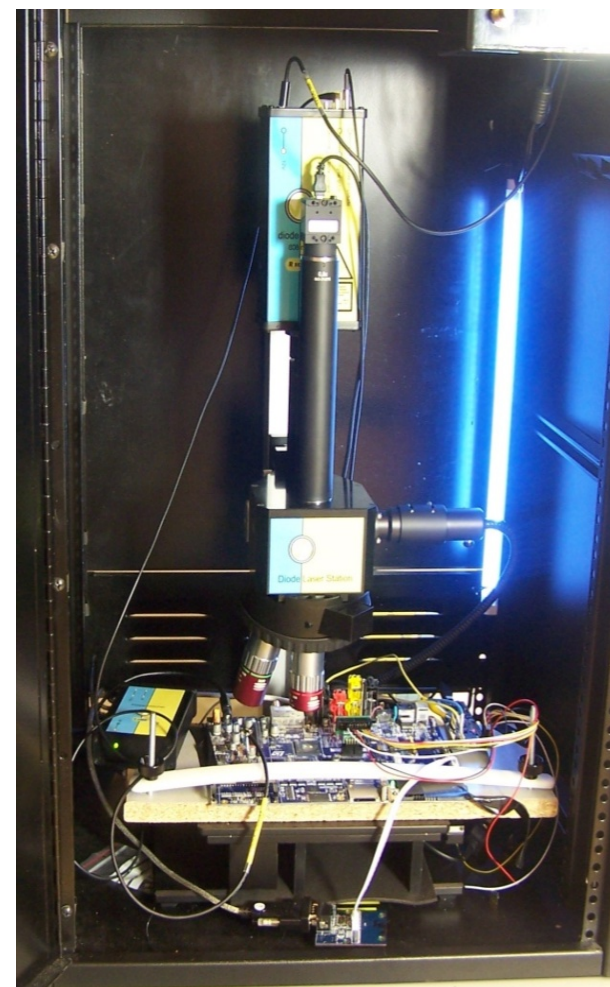
$$S' = (((S'_q - S_p) * K) \bmod q) * p + S_p$$

Subtract S' from S :

$$\begin{aligned} S - S' &= (((S_q - S_p) * K) \bmod q) * p - (((S'_q - S_p) * K) \bmod q) * p \\ &= (x_1 - x_2) * p \bmod N \end{aligned}$$

compute $\text{Gcd}(S - S', n) = \text{Gcd}((x_1 - x_2) * p, p * q) = p$

compute $q = n / p$



How to succeed in Fault Injection?



“I injected a zillion faults and nothing happened”

“I destroyed all my targets while testing”

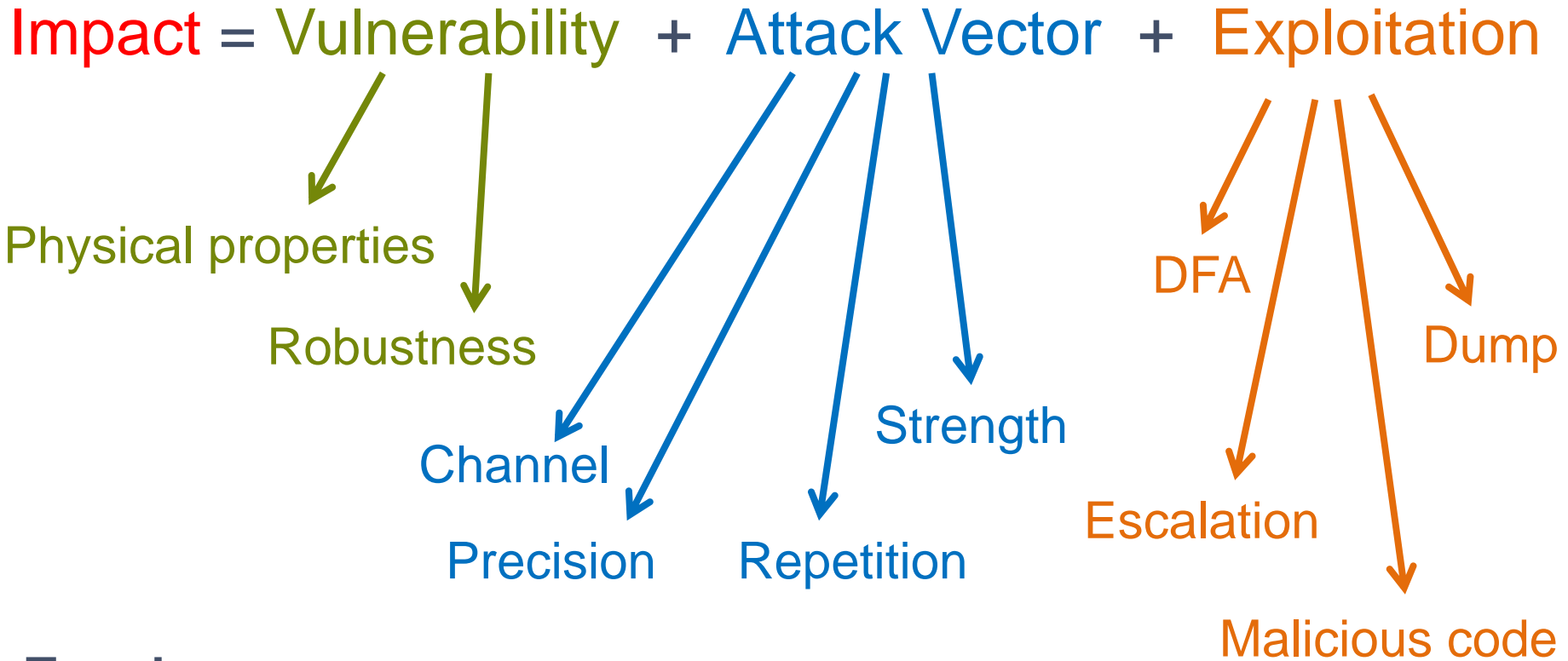
What goes wrong here?

- Lack of understanding – what is really happening?
- Lack of control

FI is no black magic, but **thoughtful engineering**

- Science: understand target and attack opportunities
- Skill: precision & perseverance

Fault Injection success



Trends

- Robustness increases
- But attack tools and exploitation grow faster
- **Overall FI relevance only growing**

riscure

Challenge your security

Contact: Marc Witteman
witteman@riscure.com

Riscure B.V.

Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America

550 Kearny Street, Suite 330
San Francisco CA 94108
USA
Phone: +1 650 646 99 79

inforequest@riscure.com

Panelist Statements



**Ilia
Polian
Professor
Uni Passau**



**Marc
Joye
NXP Fellow**



**Ingrid
Verbauwhede
Professor KUL**



**Marc
Witteman
CEO Riscure**



**Johann
Heszl
Fraunhofer
AISEC**



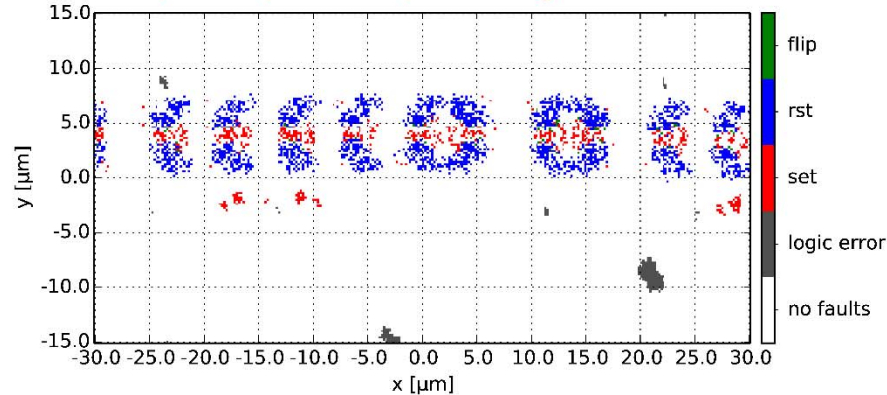
Controlled fault injection: Wishful thinking, thoughtful engineering, or just luck?

Dr. Johann Heyszl, Head of Hardware Security Department
Fraunhofer-Institute for Applied and Integrated Security | FhG AISEC

25th September 2017

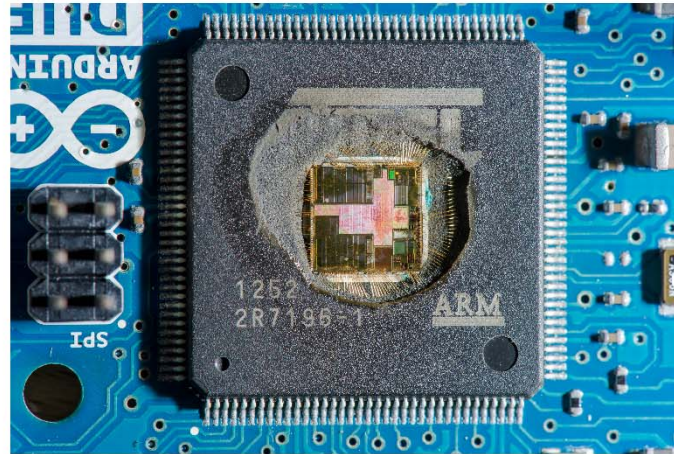
Fault attacks seem to look like black magic. Do we really understand fault attacks?

- Laser FI - Very powerful fault model - Requires precise profiling



- Target single FFs in 45 nm Xilinx Spartan-6 → Dual LFI breaks duplicated AES
- Significant efforts for setup, automation, calibration, debugging
- SCA: Not (m)any provably secure CMs - Use Countermeasures - Confirm on real device
- FA: Derive fault model (e.g. LFI see above) - More chance for reasoning / emulation?
 - IMHO not realistic for EM FI / glitching etc. (similar to *local EM*)
- FI CMs (e.g. redundancy, signatures) seem more effective → High attack complexity (multiple hits, high location / time precision)

What is the significance of fault attacks over time? Are they becoming more or less relevant?



1. High-precision, semi-invasive - Laser FI

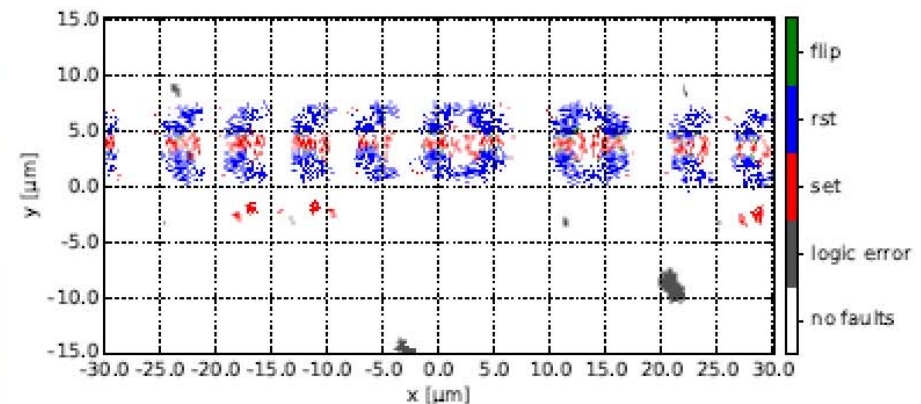
- IMO best method for systematic analysis of high-sec devices (simply worst-case FM)
- Less relevant for IoT embedded systems - Many other attacks paths

2. Low-precision, non-invasive, low-cost - EM FI, Glitching, ...

- Highly relevant (only?) for IoT devices!
- Example: (*) 1st Paper today Glitch vs. unprotected CPU / Linux
- (*) BADFET, Cui & Hoursley, WOOT / Usenix, 2017: Simple EM FI on DRAM
- IMHO not helpful for evaluation. Instead estimate FM and reason / emulate

Laser FI

- Biggest issues with LFI: Calibration of energy output, mechanical drift / uncertainty of positioning, calibration of z-height, profiling



- Setups very different - Comparison difficult
- Small misconfigurations / miscalibrations - Huge impact
- Deriving security guarantees from LFI measurement campaigns seems difficult
- Benchmark LFI setups on open (e.g. FPGA-based) designs → Get better comparability

Contact Information



Dr.-Ing. Johann Heyszl

Hardware Security Department

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Parkring 4
85748 Garching (near Munich)
Germany

Internet: <http://www.aisec.fraunhofer.de>

Phone: +49 89 3229986-172

Fax: +49 89 3229986-299

E-Mail: johann.heyszl@aisec.fraunhofer.de