Body biasing fault injection: Enhancements, analysis, modeling, and simulation

PhD thesis defense

Geoffrey Chancel

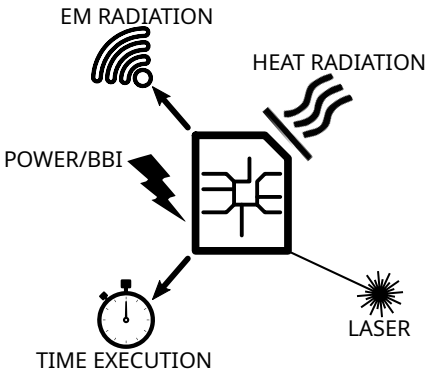
2024/01/29

Jean-Luc Danger Giorgio Di Natale Pascal Nouet

Jean-Max Dutertre Jean-Marc Gallière Philippe Maurine

Context: hardware security

- Electronics are found in every economic sector
- In IoT, CPS, debit cards, phones, bank systems
- They embed cryptographic algorithms to ensure security
- These algorithms are fallible, they leak data and can be disturbed



Side-channel and fault injection.

Fault injection attacks

Fault injection objectives:

- Denial of service (DoS) → Stop circuit operations and the related services
- Verification bypass → Modify data on the fly to fake authenticity
- Confidential data extraction → Modify data to perform differential fault analysis

Thanks to a fault injection platform:

- Power Glitch Fault Injection (PW-GFI)
- Clock Glitch Fault Injection (CK-GFI)
- Laser Fault Injection (LFI)
- Electromagnetic Fault Injection (EMFI)
- Body Biasing Fault Injection (BBI)

Body biasing injection: state-of-the-art

- "Yet another fault injection technique : by forward body biasing injection (2011)": Introducing the new technique and a Bellcore attack
- "Voltage spikes on the substrate to obtain timing faults (2012)": Timing faults
- "Body biasing injection attacks in practice (2016)": Lumped model for dual-well substrates

Six days after the beginning of my thesis:

- "Low-cost body biasing injection (BBI) attacks on WLCSP devices. (2020)":Low-cost tool, fault analysis, hardware attack

Limited information in the literature at the beginning of my thesis

Body biasing injection: industrial and academic platforms

Langer

Current source:

- 4 *A in* 1 Ω
- ± 1 *ns* jitter
- 2 *ns* rise time

Riscure

Voltage source:

- Probe 64 *A*
- 450 *V* ± 45 *V*
- Max. PW 50 *ns*

ChipSHOUTER

Voltage source:

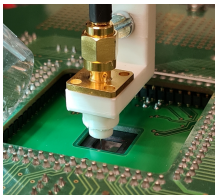
- 150 V to 450 V
- PW: 15 ns to 480 ns
- 220 ps jitter

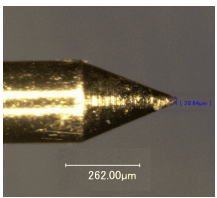
Pico-EMP

Voltage source (AC):

- Up to 250 V
- PW: 85 ns in 50 Ω
- Up to 200 mW

Body biasing injection: LIRMM BBI platform





- Custom BBI probe;
  - Spring-loaded metal probe;
  - Custom 3D printed housing;
  - SMA connector;
- AVTECH AVRK-4-B high voltage pulse generator.
- Ajouter caractéristiques plateforme

Body Biasing Injection: thesis objectives

- What is the spatial resolution of BBI?
- What is the time resolution of BBI?
- Is thinning the substrate useful in any way?
- How faults occur in a BBI context?
- How to model BBI?

Thesis agenda

- Body Biasing Injection platform enhancements;
- Integrated circuits modeling for BBI;
- Enhanced simulation flow;
- Substrate thinning analysis in a BBI context.
- Conclusion and perspectives