Laser Attack Benchmark Suite

Burin Amornpaisannon, Andreas Diavastos, Li-Shiuan Peh, Trevor E. Carlson

39th IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2020

Tuesday, November 3, 2020

Presenter Bio

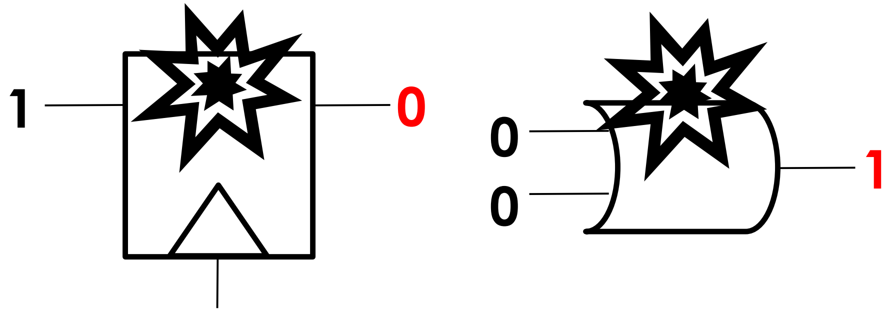
Burin Amornpaisannon
Second year Ph.D. student
National University of Singapore

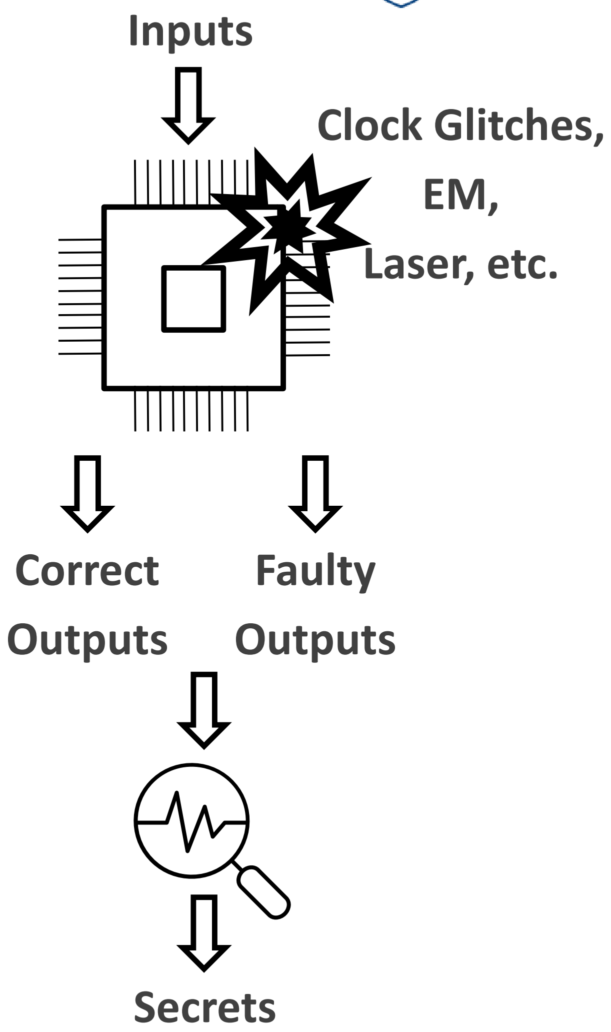
Interests:

- Physical Attacks
- Neuromorphic Computing
- Computer Architecture

Fault Attacks

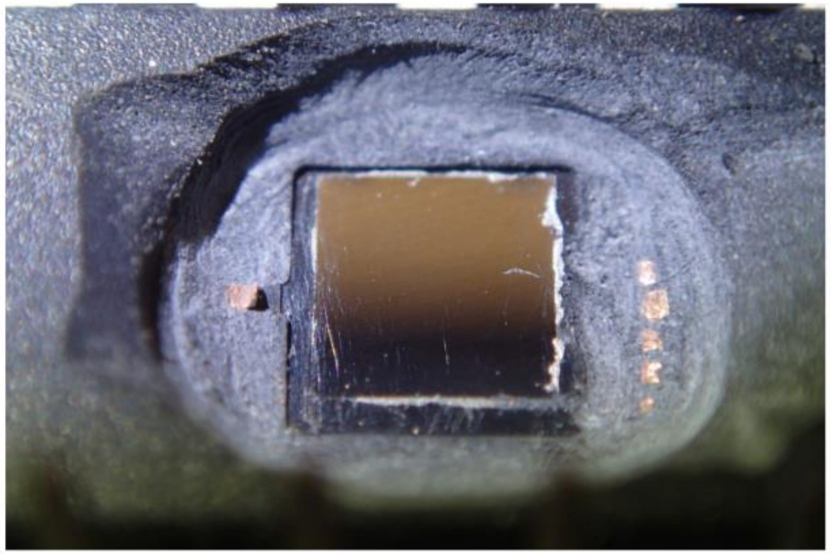
- Try to directly inject faults to electronic devices
  - Cryptographic algorithms, neural networks, etc.
- Electronic devices are subject to faults
- Faults can become errors that can be exploited
  - To retrieve secrets, decrease neural network accuracy, etc.





Laser Fault Injection

- One of the most effective methods to generate fault attacks
  - Accurate timing
  - High precision
- Can be tested only after chip fabrication
  - Too late!
  - Restarting the complete silicon design cycle is required.

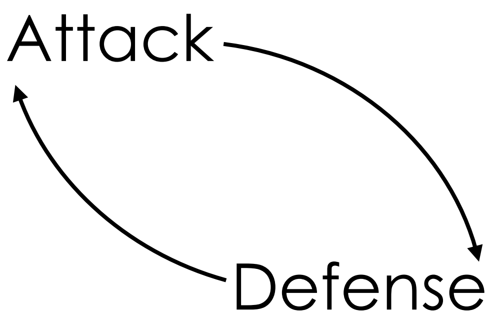


ATmega328P de-packaged from the back side [1].

1. Jakub, Breier & Jap, Dirmanto & Chen, C.-N. 2015. Laser Profiling for the Back-Side Fault Attacks: With a Practical Laser Skip Instruction Attack on AES. In CPSS.

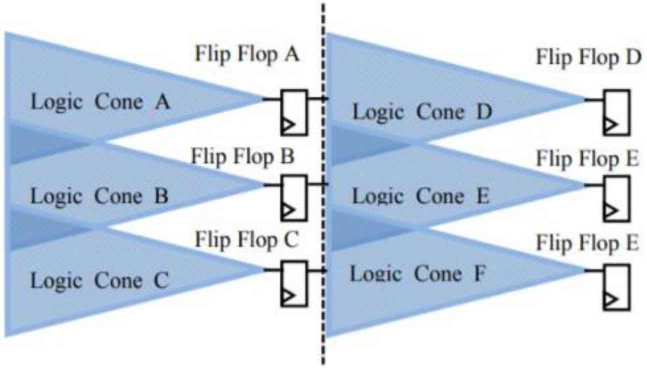
Goals

- To allow circuit designer to evaluate their design against precise laser attacks during the early design stage.
- To automatically integrate a protection to the design.



Related Work

- RTL Laser Fault Modeling Based on Cone Partitioning

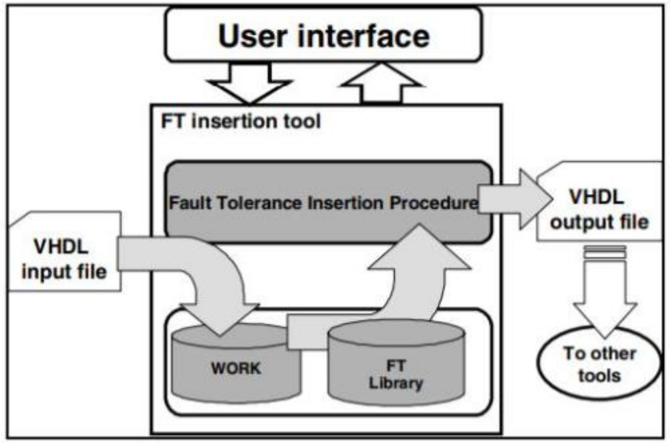


Logic Cone Partitioning [1]

1. Athanasios Papadimitriou, David Hély and Vincent Beroulle, Paolo Maistri, and Régis Leveugle. 2014. A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks. In DATE
2. Kais Chibani, Adrien Facon, Sylvain Guilley, Damien Marion, Yves Mathieu, Laurent Sauvage, Youssef Souissi, and Sofiane Takarabt. 2019. Fault Analysis Assisted by Simulation. Springer International Publishing
3. Luis Berrojo, Fulvio Corno, Luis Entrena, Isabel Gonzalez, Celia López, Matteo Sonza Reorda, and Giovanni Squillero. 2002. An industrial environment for high-level fault-tolerant structures insertion and validation. In VTS.

Related Work

- RTL Laser Fault Modeling Based on Cone Partitioning
- Physical Attack Simulation (Virtualyzr®)

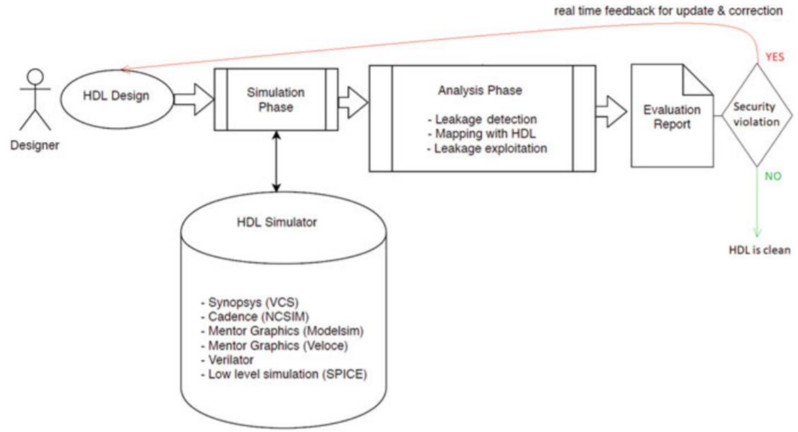


Overview of the framework [3]

1. Athanasios Papadimitriou, David Hély and Vincent Beroulle, Paolo Maistri, and Régis Leveugle. 2014. A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks. In DATE
2. Kais Chibani, Adrien Facon, Sylvain Guilley, Damien Marion, Yves Mathieu, Laurent Sauvage, Youssef Souissi, and Sofiane Takarabt. 2019. Fault Analysis Assisted by Simulation. Springer International Publishing
3. Luis Berrojo, Fulvio Corno, Luis Entrena, Isabel Gonzalez, Celia López, Matteo Sonza Reorda, and Giovanni Squillero. 2002. An industrial environment for high-level fault-tolerant structures insertion and validation. In VTS.

Related Work

- RTL Laser Fault Modeling Based on Cone Partitioning
- Physical Attack Simulation (Virtualyzr®)
- Automatic Insertion of Fault Tolerant Structures

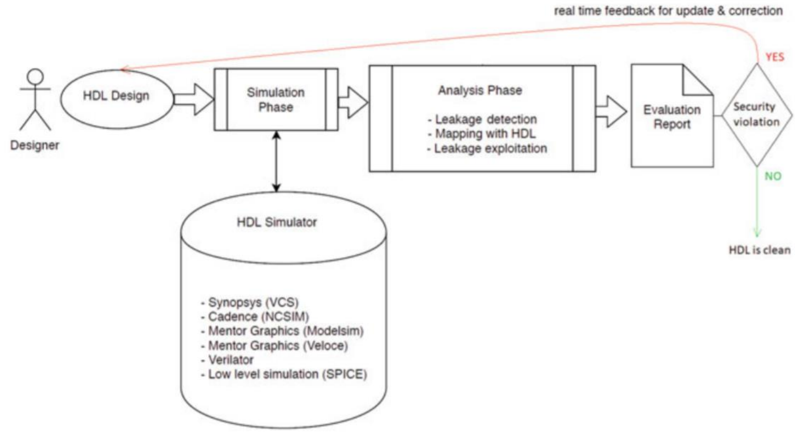


General Workflow [2]

1. Athanasios Papadimitriou, David Hély and Vincent Beroulle, Paolo Maistri, and Régis Leveugle. 2014. A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks. In DATE
2. Kais Chibani, Adrien Facon, Sylvain Guilley, Damien Marion, Yves Mathieu, Laurent Sauvage, Youssef Souissi, and Sofiane Takarabt. 2019. Fault Analysis Assisted by Simulation. Springer International Publishing
3. Luis Berrojo, Fulvio Corno, Luis Entrena, Isabel Gonzalez, Celia López, Matteo Sonza Reorda, and Giovanni Squillero. 2002. An industrial environment for high-level fault-tolerant structures insertion and validation. In VTS.

Related Work

- RTL Laser Fault Modeling Based on Cone Partitioning
- Physical Attack Simulation (Virtualyzr®)
- Automatic Insertion of Fault Tolerant Structures
- There exists no prior laser attack benchmark suite

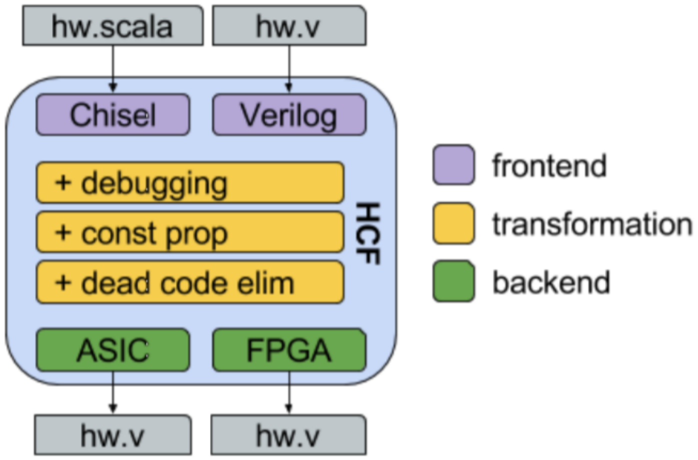


General Workflow [2]

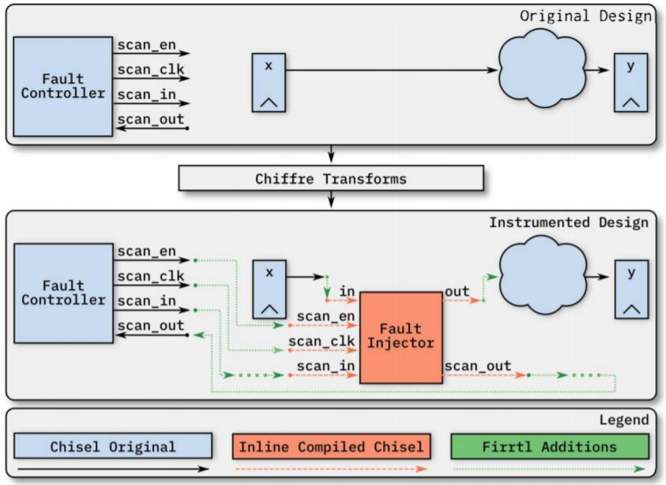
1. Athanasios Papadimitriou, David Hély and Vincent Beroulle, Paolo Maistri, and Régis Leveugle. 2014. A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks. In DATE
2. Kais Chibani, Adrien Facon, Sylvain Guilley, Damien Marion, Yves Mathieu, Laurent Sauvage, Youssef Souissi, and Sofiane Takarabt. 2019. Fault Analysis Assisted by Simulation. Springer International Publishing
3. Luis Berrojo, Fulvio Corno, Luis Entrena, Isabel Gonzalez, Celia López, Matteo Sonza Reorda, and Giovanni Squillero. 2002. An industrial environment for high-level fault-tolerant structures insertion and validation. In VTS.

Foundational Work

- Flexible Intermediate Representation for RTL (FIRRTL) and its hardware compiler framework (HCF) FIRRTL
- A configurable hardware fault injection framework for RISC-V systems (Chiffre)



The hardware compiler framework [1].

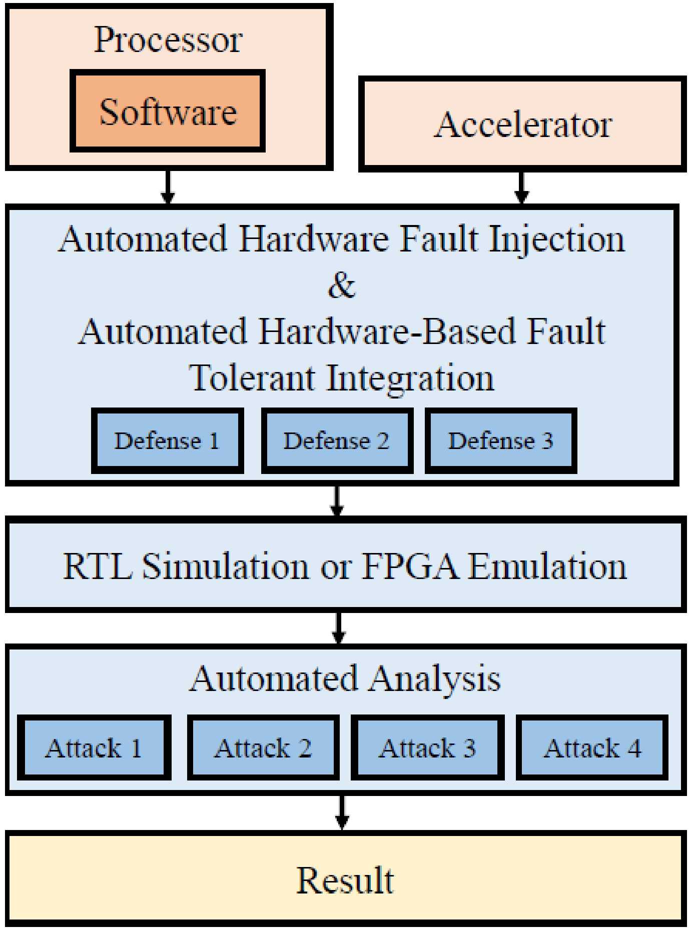


Chiffre's Instrumentation [2].

1. Adam Izraelevitz, Jack Koenig, Patrick Li, Richard Lin, Angie Wang, Albert Magyar, Donggyu Kim, Colin Schmidt, Chick Markley, Jim Lawson, and Jonathan Bachrach. 2017. Reusability is FIRRTL ground: Hardware construction languages, compiler frameworks, and transformations. In ICCAD.
2. Schuyler Eldridge, Alper Buyuktosunoglu, and Pradip Bose. 2018. Chiffre: A Configurable Hardware Fault Injection Framework for RISC-V Systems. In CARRV'18.

Overview

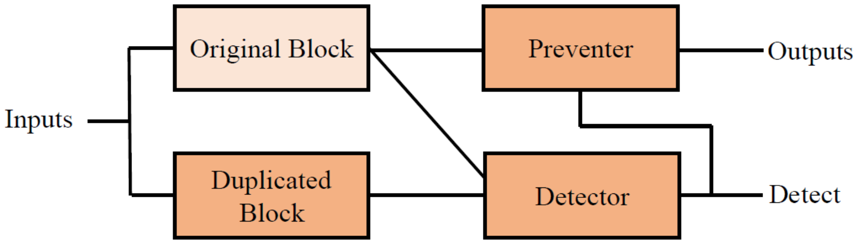
- Simulates laser fault injection attacks on an RTL simulator or FPGA
- Supports logical level faults
- Integrates hardware-based defenses
- Analyzes outputs from attacks



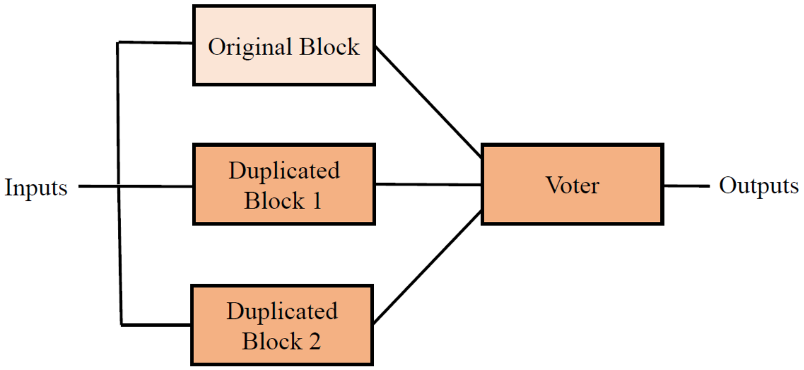
Overview of LABS

Overview: Supported Attacks and Defenses

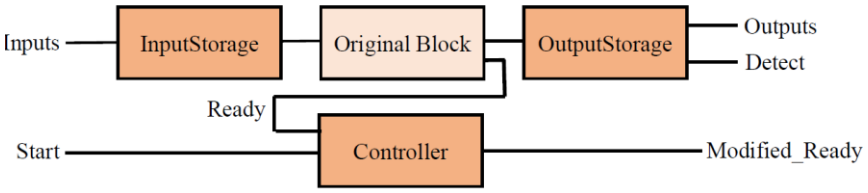
Application	Target	Description
AES	Processor	Skip the last round *Addroundkey*
AES	Processor Accelerator	Inject one-bit fault into input of the last round
RSA-CRT	Processor	Inject faults into one of two parts of signature
Neural Network	Processor	Skip a computation of the activation functions



Double Modular Redundancy

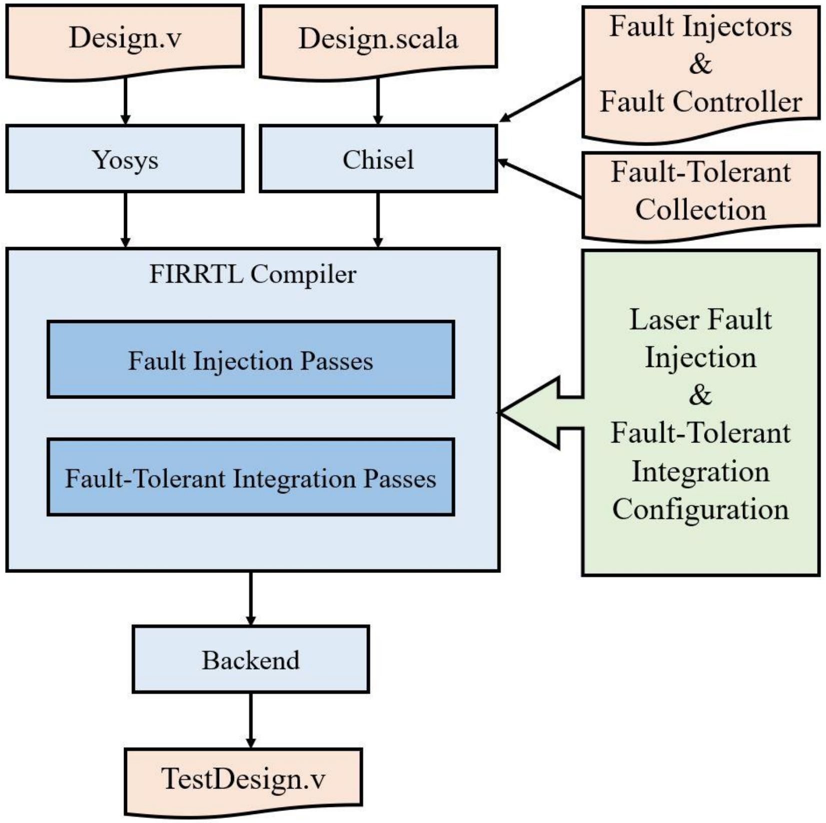


Triple Modular Redundancy

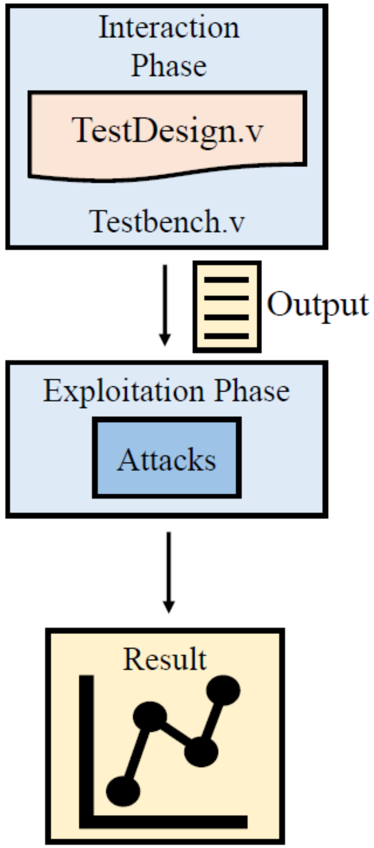


Temporal Redundancy

Methodology



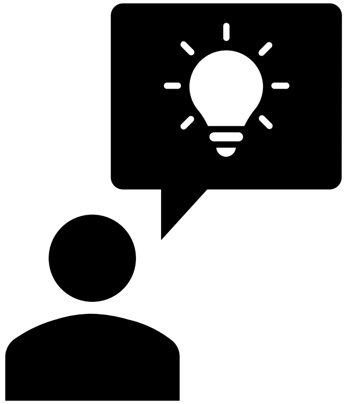
LABS's automated hardware fault injection and hardware-based fault-tolerant integration flow



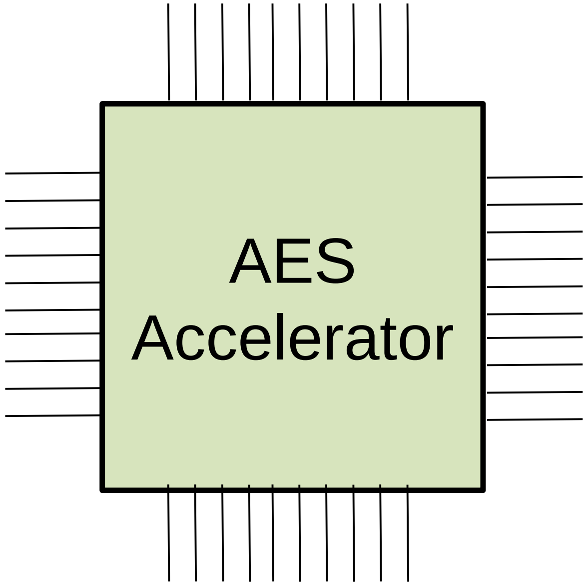
LABS's Simulation and Analysis Flow

A Use-case Scenario

Scenario

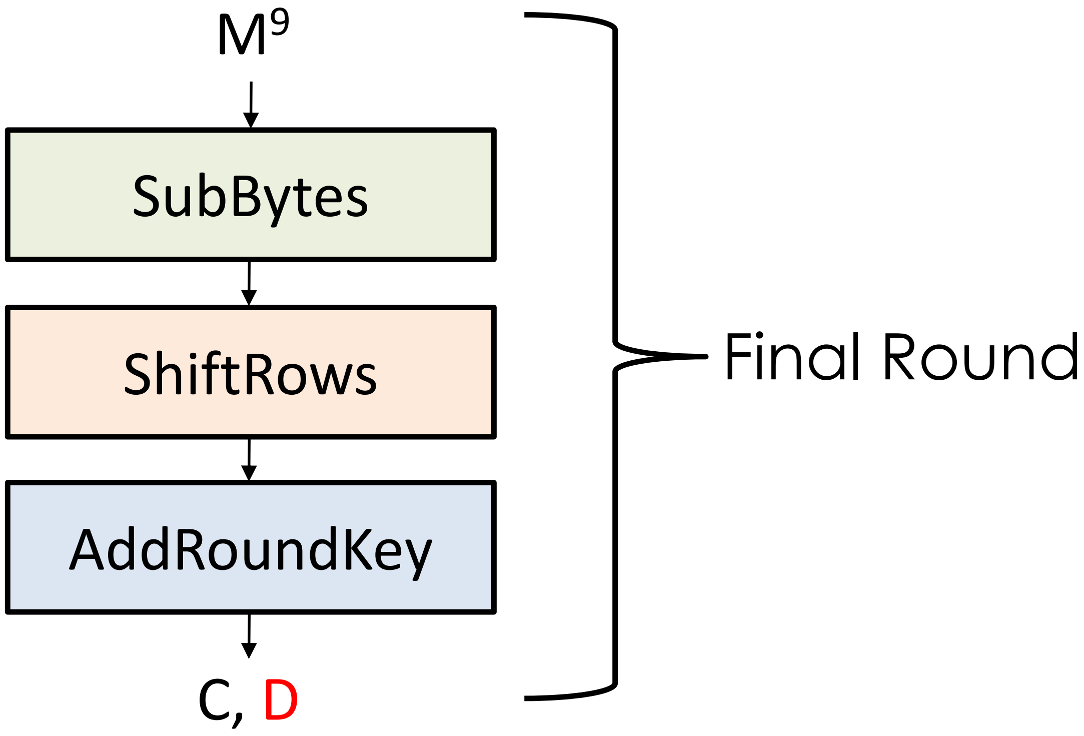


Circuit Designer



AES Attack by Giraud et al.

- Inject a one-bit fault to the intermediate data during the start of the final round of the AES algorithm (M^9).



$$C_{ShiftRows(j)} \oplus D_{ShiftRows(j)} = SubBytes(M^9_j) \oplus SubBytes(M^9_j \oplus e_j)$$

AES Attack by Giraud et al.

- The attack can be generated by sending a configuration file to LABS.

```
[{"class":"chiffre.passes.FaultInjectionAnnotation",   (a)
  "target":"aes.aes_encipher_block.block_w3_reg",
  "id":"main",
  "injector":"chiffre.inject.FaultInjector" },
 {"class":"chiffre.passes.ScanChainAnnotation",         (b)
  "target":"aes.FaultController.scan",
  "ctrl":"master",
  "dir":"scan",
  "id":"main" },
 {"class":"labs.passes.FaultControllerAnnotation",     (c)
  "target":"aes.aes_encipher_block.round_ctr_reg",
  "data_target":"h_a",
  "max_number_of_fires": 1,
  "target_bits": [1] },
```

(a) Fault Location, Fault Type

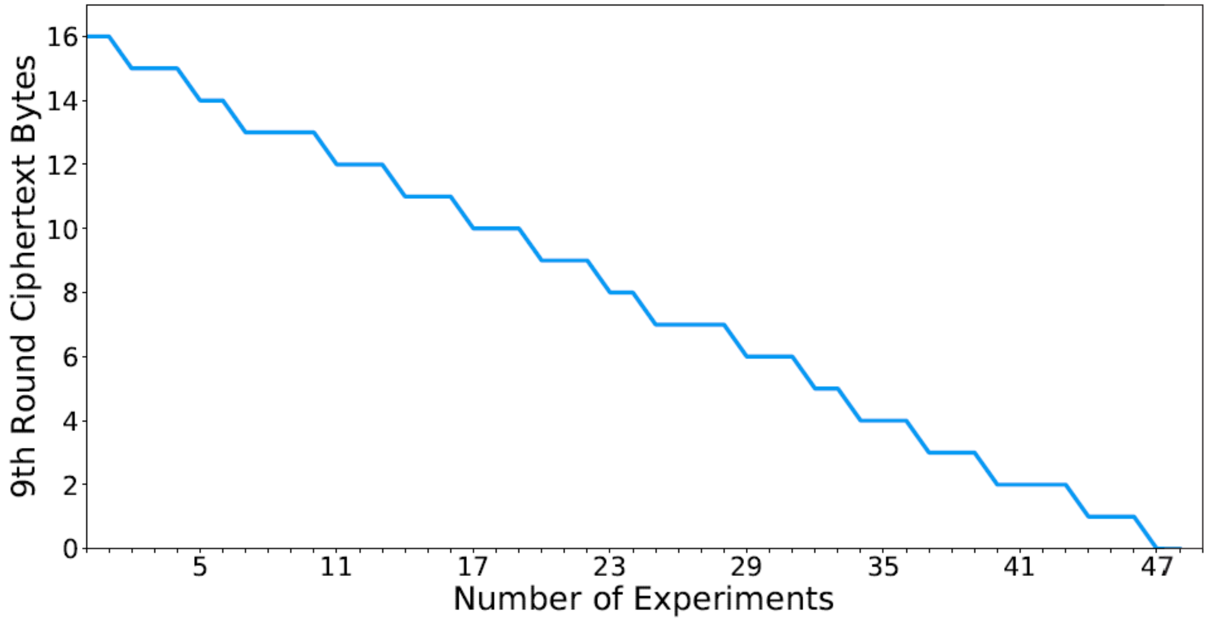
(b) Fault Controller

(c) Fault Controller Configuration

LABS Configuration Example

AES Attack by Giraud et al.

- From the automated fault analysis, 47 experiments are needed to successfully reveal the entire M^9.

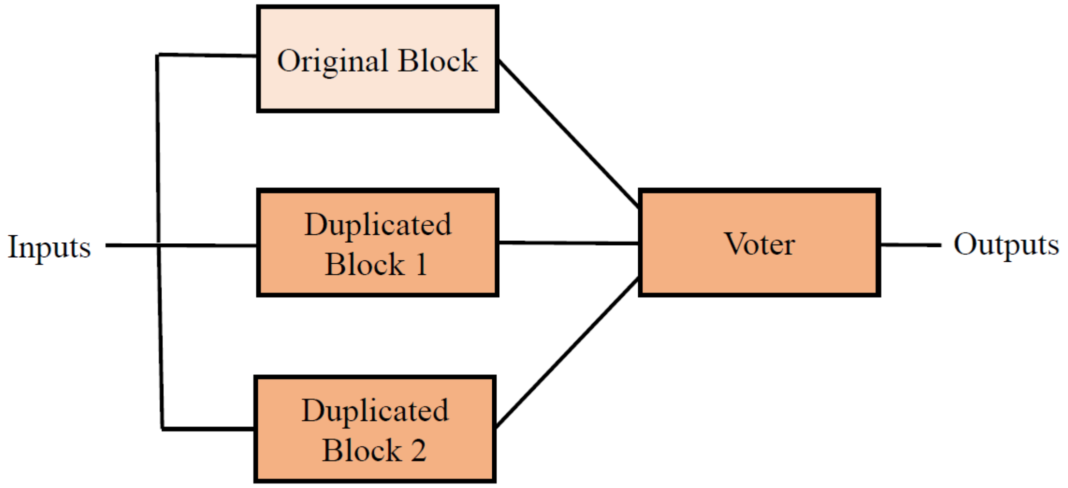


The result of the AES attack by Giraud et al.

Hardware Redundancy Integration

- Integrate a hardware-based redundancy technique to protect against the attack.
- It is automatically done by LABS.

```
{"class":"labs.passes.FaultTolerantTMRAnnotation",
 "target":"aes.aes_encipher_block.None"}]
```



Triple Modular Redundancy.

Hardware Redundancy Results

Design	#Combs (Cells)	#Seqs (Cells)	Area (μm^2)	Power (mW)	Freq (GHz)
Original	17973	2472	10661	6.26	1.03
DMR	35973	4947	21526	12.63	1.03
Temporal	18843	2865	11478	7.70	1.03
TMR	53729	7416	32170	18.92	1.03
Hybrid	57228	8066	34353	20.54	1.03

Overheads of the supported defenses.

```
Correct:   0x3ad77bb40d7a3660a89ecaf32466ef9
Faulty:    0x3ad77bb40d7a3697a89ecaf32466ef9
DMR:       0x00000000000000000000000000000000
Temporal:  0x00000000000000000000000000000000
TMR:       0x3ad77bb40d7a3660a89ecaf32466ef9
```

An example of the outputs of the AES accelerator being attacked by Giraud et al. with hardware countermeasures at module level

Framework Evaluation

Attacks	(m:ss)
AES by Breier et al.	8:30
AES by Giraud et al.	:27
RSA-CRT by Boneh et al.	2:26
NN by Breier et al.	6:09

Elapsed time for behavioral simulation for all use-case scenarios

Steps	(m:ss)
Fault-Tolerant Integration	:07
Hardware Fault Injection	:09
Simulation Compilation	:04
Behavioral Simulation	:01
Fault Analysis	:01

Elapsed time per step (AES accel.)

Thank you

LABS is modular open-source software, and open for extensions.

https://github.com/nus-labs/labs