Fault Injection Resilience

Sylvain GUILLEY, Laurent SAUVAGE,
Jean-Luc DANGER, Nidhal SELMANE.

Institut TELECOM / TELECOM-ParisTech
CNRS – LTCI (UMR 5141)

FDTC (Santa Barbara, CA, USA),
Saturday August 21st, 2010.

Presentation Outline

1. Context
   - Fault Injection Attacks
   - State-of-the-Art in Protections for Asymmetric Cryptography
   - State-of-the-Art in Protections for Symmetric Cryptography
2. Detection versus Fault Injection Resilience (FIR)
   - Features of Detection
   - Features of FIR
3. Case-Study #1: Protocol-Level Resilience
   - Against Faults
   - Against Leakage
4. Case-Study #2: Netlist-Level Resilience
   - Against Asymmetric Faults
   - Against Symmetric Faults
5. Conclusions

Presentation Outline

1. Context
   - Fault Injection Attacks
   - State-of-the-Art in Protections for Asymmetric Cryptography
   - State-of-the-Art in Protections for Symmetric Cryptography
2. Detection versus Fault Injection Resilience (FIR)
   - Features of Detection
   - Features of FIR
3. Case-Study #1: Protocol-Level Resilience
   - Against Faults
   - Against Leakage
4. Case-Study #2: Netlist-Level Resilience
   - Against Asymmetric Faults
   - Against Symmetric Faults
5. Conclusions

Fault Attacks in Cryptography

Harmfulness

- 1 fault suffices to break unprotected CRT-RSA
- 1 fault suffices to break unprotected AES-128

Fault Injection Techniques

- **Global faults**:
  - are low cost,
  - often asymmetrical,
  - can break real-world implementations.
- **Local faults**:
  - require sample preparation,
  - can be symmetrical (arbitrary),
  - can break real-world implementations.

Observation attacks are easily thwarted by masking:

- $\forall r_1, r_2, \left(M^{d+r_1 \times \phi(N)} \mod r_2 \times N\right) \mod N = M^d \mod N$, hence multiple degrees of freedom to mask cryptographic parameters.

Perturbation attacks are fought thanks to similar properties:

- Randomness can also be injected within the algorithm, so as to enable verifications afterwards [BHT09].

This paper by Jean-Sébastien CORON (@ AsiaCrypt 2009) [CM09] proves that RSA with PSS is provably secure against random fault injection attacks in the random oracle model.

Algorithm 1: RSA implementation protected against SCA and FIA.

Input : $x \in \mathbb{G}, d = (d_{n-1}, \cdots, d_0)_2$
Output: $x^d \in \mathbb{G}$ or "Error"

1 Generate a random $r \in \mathbb{G}^*$
2 $R[0] \leftarrow r$
3 $R[1] \leftarrow r^{-1}$
4 $R[2] \leftarrow x$
5 **for** $i \in [0, n-1]$ **do**
6 $\quad R[1 - d_i] \leftarrow R[1 - d_i] \cdot R[2]$
7 $\quad R[2] \leftarrow R[2]^2$
8 **end**
9 **if** $R[0] \cdot R[1] \cdot x = R[2]$ **then**
10 $\quad$ **return** $r^{-1} \cdot R[0]$
11 **else**
12 $\quad$ **return** "Error"
13 **end**

Disclaimer

All this is very challenged by recent attacks:

- Attack of Berzati *et al.* at CHES'2010 [BCDG10]
- Attack on Vigilant's CT-RSA of CHES'2008 to come...

In symmetric cryptography:

Detection seems to be the only research effort.

It involves redundancy, such as:

- Space
- Time
- Information
- Algorithm

Objective of this talk:

We tackle other ways to protect symmetric cryptography against fault injection attacks.

Presentation Outline

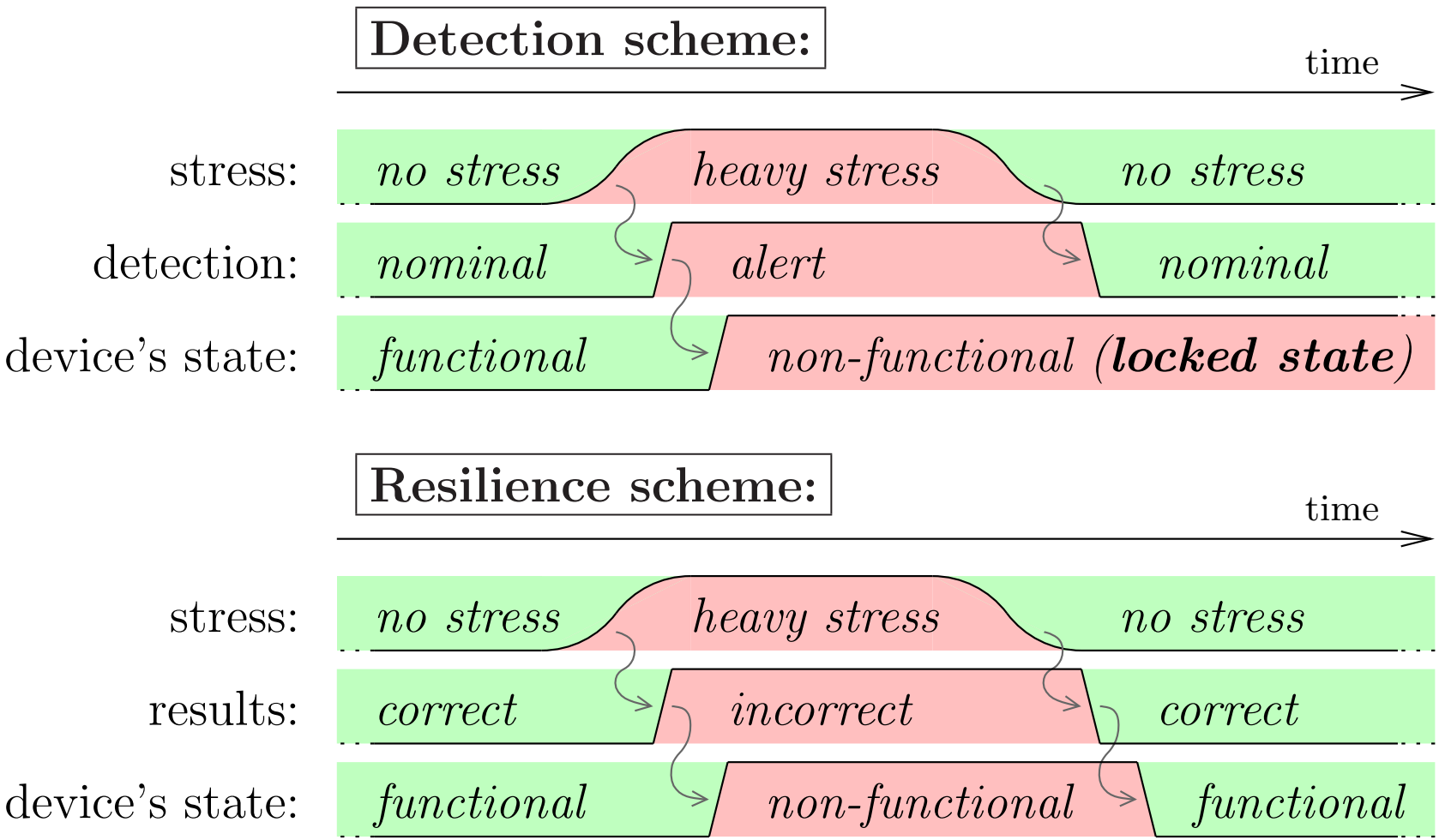
1. Context
   - Fault Injection Attacks
   - State-of-the-Art in Protections for Asymmetric Cryptography
   - State-of-the-Art in Protections for Symmetric Cryptography
2. Detection versus Fault Injection Resilience (FIR)
   - Features of Detection
   - Features of FIR
3. Case-Study #1: Protocol-Level Resilience
   - Against Faults
   - Against Leakage
4. Case-Study #2: Netlist-Level Resilience
   - Against Asymmetric Faults
   - Against Symmetric Faults
5. Conclusions

Reminder about the characteristics of detection

		Ciphertext incorrect?	
		Yes	**No**
Alarm raised?	**Yes**	Safe	Problem of **availability**
	No	Problem of **security**	Safe

- **Undetected faults**: fatal... and inexistent in resilience
- **Unnecessary detections**: inconvenience (*that does not exist in side-channel resilience*)

Virtues of Resilience also against Perturbation Attacks



Presentation Outline

1. Context
   - Fault Injection Attacks
   - State-of-the-Art in Protections for Asymmetric Cryptography
   - State-of-the-Art in Protections for Symmetric Cryptography
2. Detection versus Fault Injection Resilience (FIR)
   - Features of Detection
   - Features of FIR
3. Case-Study #1: Protocol-Level Resilience
   - Against Faults
   - Against Leakage
4. Case-Study #2: Netlist-Level Resilience
   - Against Asymmetric Faults
   - Against Symmetric Faults
5. Conclusions

Algorithm 2: Probabilistic Encryption Algorithm built on top of AES, non-protected against FIAs.

Input : A plaintext x to be encrypted with the key k.

Output: A ciphertext along with a random number.

1 Determine a random number r of the same size as x; `/* This number will whiten` x `*/`.

2 Return the couple $(y = \mathrm{AES}_k(x \oplus r), r)$.

Algorithm 3: Deterministic Decryption Algorithm matching algorithm (2).

Input : A ciphertext under the form $(y = \mathrm{AES}_k(x \oplus r), r)$ to be decrypted by the AES key k.

Output: The plaintext x.

1 Decrypt y with key k: $z = \mathrm{AES}_k^{-1}(y)$.

2 Return the demasked input: $z \oplus r = x$.

Suggestion of resolution for the asymmetry encryption/decryption

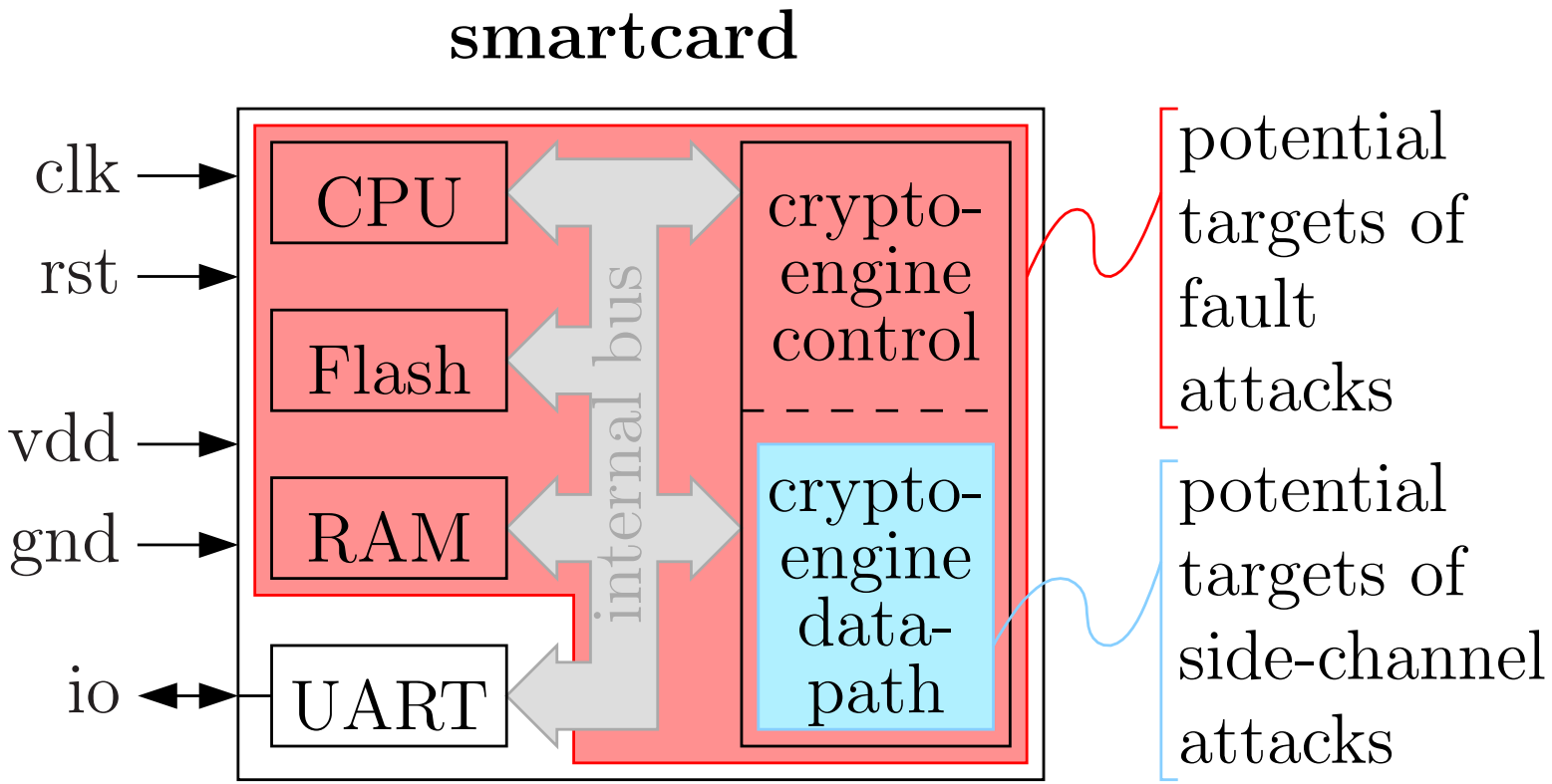
Easy to protect:
$\Rightarrow$ Algorithm (3)

Difficult to protect:
$\Rightarrow$ Algorithm (2)

Deterministic decryption, in a tamper-proof and tamper-evident reader

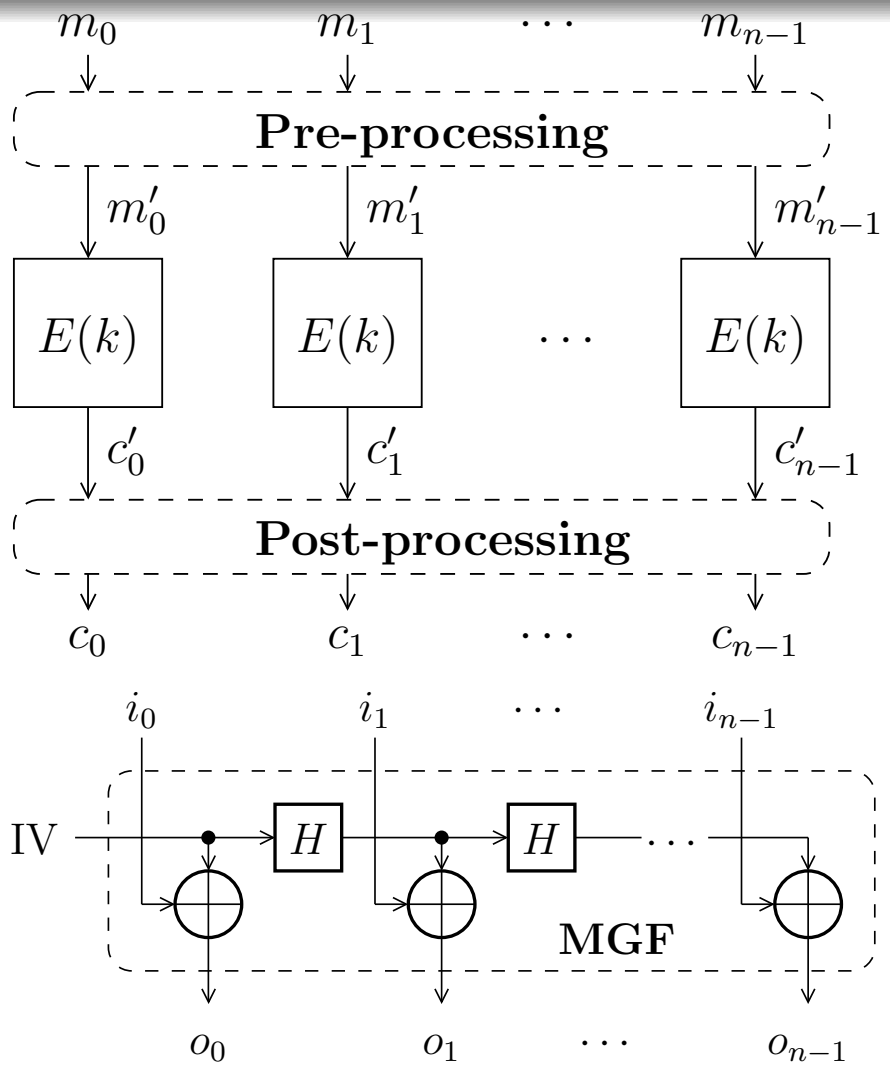
Probabilistic encryption, with blinding at the input & at the output

Cryptography is the most demanding resource



Susceptible organs of a smartcard in two representative sensitive operations (`EXTERNAL` and `INTERNAL AUTHENTICATE`).
Typically, the cryptography will be either **RSA** or **3DES**.

Blinding inputs ... and outputs!



The initialization vector (IV) is:

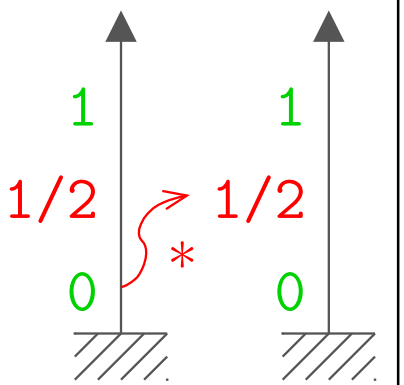
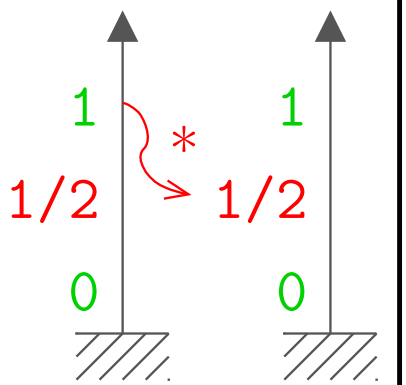
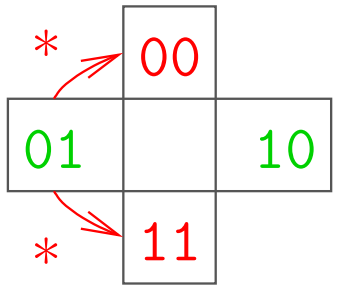
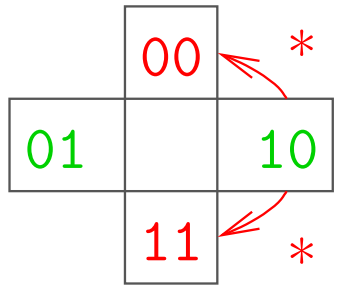
- a **random number** for the input, and
- a **secretly exchanged nonce** for the output.

MGF = **M**ask **G**eneration **F**unction.

Presentation Outline

1. Context
   - Fault Injection Attacks
   - State-of-the-Art in Protections for Asymmetric Cryptography
   - State-of-the-Art in Protections for Symmetric Cryptography
2. Detection versus Fault Injection Resilience (FIR)
   - Features of Detection
   - Features of FIR
3. Case-Study #1: Protocol-Level Resilience
   - Against Faults
   - Against Leakage
4. Case-Study #2: Netlist-Level Resilience
   - Against Asymmetric Faults
   - Against Symmetric Faults
5. Conclusions

When we cannot trust the external TRNG

Multi-valued logic		Redundant logic	
Case #1	Case #2	Case #1	Case #2
			

Two kinds of faults (in red), namely $\{0,1\} \xrightarrow{*} 1/2$ for 3-valued logic and $\{01,10\} \xrightarrow{*} \{00,11\}$, *i.e.* $\{\texttt{VALID0}, \texttt{VALID1}\}$ for DPL, after which the initial value (in green) has been forgotten.

Vocabulary

- **DPL**: **D**ual-rail with **P**recharge **L**ogic
- **EPE**: **E**arly **P**ropagation (in evaluation or in precharge) **E**ffect

- **DPL w/ EPE**: $\exists a$ VALID, $f(a, \text{NULL}) = \text{VALID}$;
- **DPL w/o EPE**: $\forall a$ VALID, $f(a, \text{NULL}) = \text{NULL}$.

DPL w/ EPE is Protected against Multiple *Asymmetrical* Faults [SBG+09]

b \ a	VALID0	VALID1	NULL0
VALID0	VALID0	VALID0	VALID0 (**EPE**)
VALID1	VALID0	VALID1	NULL0
NULL0	VALID0 (**EPE**)	NULL0	NULL0

b \ a	'0'	'1'	'U'
'0'	'0'	'0'	'0'
'1'	'0'	'1'	'U'
'U'	'0'	'U'	'U'

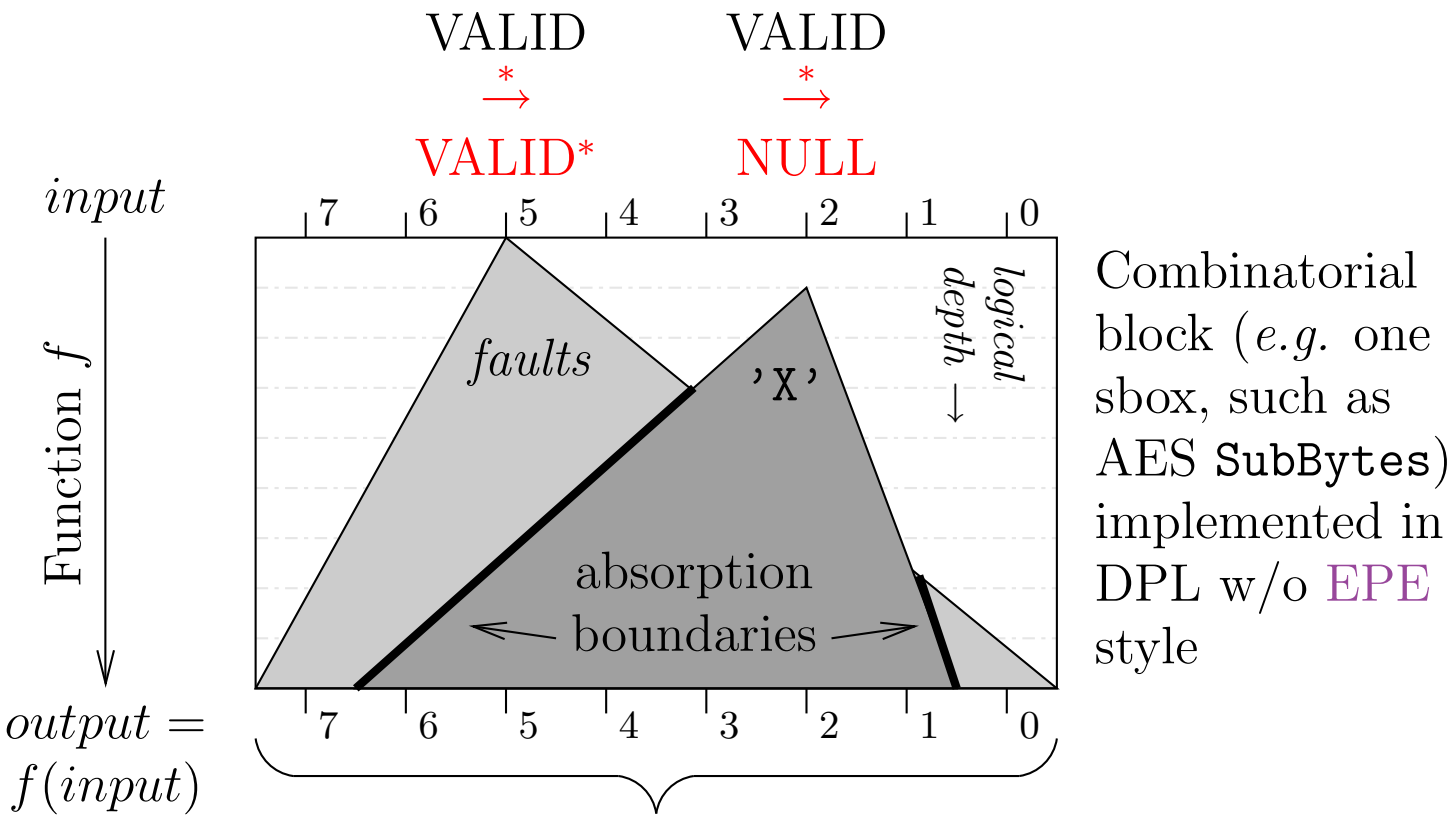
where the tokens $\{\text{VALID0}, \text{VALID1}, \text{NULL0}\}$ implement respectively the items $\{\text{'0'}, \text{'1'}, \text{'U'}\}$.

DPL w/o EPE is Protected in front of Multiple *Symmetric* Faults [BDF+09]

b \ a	VALID0	VALID1	NULL0	NULL1
VALID0	VALID0	VALID0	NULL0	NULL1
VALID1	VALID0	VALID1	NULL0	NULL1
NULL0	NULL0	NULL0	NULL0	NULL1
NULL1	NULL1	NULL1	NULL0	NULL1

Remark that if we call: '0': VALID0, '1': VALID1, 'X': NULL = {NULL0, NULL1}, then we have the same behavior (*i.e.* "*propagate always*") as VHDL. This is illustrated below:

b \ a	'0'	'1'	'X'
'0'	'0'	'0'	'X'
'1'	'0'	'1'	'X'
'X'	'X'	'X'	'X'



Combinatorial block (*e.g.* one sbox, such as AES `SubBytes`) implemented in DPL w/o EPE style

The output is mixed NULL and VALID*

Multiple faults, where the false valid is not completely hidden by the `'X'` wave. The `'X'` avalanche absorbs most, if not all, the valid faults.

Performance overhead of different SCA+FIA countermeasures.

Strategy	**Detection + DPL**	**Resilience = DPL**	
Countermeasure	[KKT04] + [THH+05]	DRSL [CZ06]	IWDDL [MMMT09]
Area	5.49 ×	2.56 ×	4.34 ×
Throughput	4.49 ×	2.00 ×	1.53 ×

Presentation Outline

1. Context
   - Fault Injection Attacks
   - State-of-the-Art in Protections for Asymmetric Cryptography
   - State-of-the-Art in Protections for Symmetric Cryptography
2. Detection versus Fault Injection Resilience (FIR)
   - Features of Detection
   - Features of FIR
3. Case-Study #1: Protocol-Level Resilience
   - Against Faults
   - Against Leakage
4. Case-Study #2: Netlist-Level Resilience
   - Against Asymmetric Faults
   - Against Symmetric Faults
5. Conclusions

Conclusions

- Asymmetric crypto *seems* easier to protect than symmetric crypto
- We demonstrate both a **protocol-level** and an **implementation-level** fault injection resilience (FIR) scheme
- Those techniques combine nicely with leakage resistance techniques.

- **FIPS-140** requires detection schemes...
- whereas **CC** are open to any kind of countermeasures.

[BCDG10] Alexandre Berzati, Cécile Canovas-Dumas, and Louis Goubin.
Public Key Perturbation of Randomized RSA Implementations.
In *CHES*, volume 6225 of *Lecture Notes in Computer Science*, pages 306–319. Springer, August 17-20 2010.
Santa Barbara, CA, USA.

[BDF+09] Shivam Bhasin, Jean-Luc Danger, Florent Flament, Tarik Graba, Sylvain Guilley, Yves Mathieu, Maxime Nassar, Laurent Sauvage, and Nidhal Selmane.
Combined SCA and DFA Countermeasures Integrable in a FPGA Design Flow.
In *ReConFig*, pages 213–218. IEEE Computer Society, December 9–11 2009.
Cancún, Quintana Roo, México, DOI: 10.1109/ReConFig.2009.50, http://hal.archives-ouvertes.fr/hal-00411843/en/.

[BHT09] Arnaud Boscher, Helena Handschuh, and Elena Trichina.
Blinded Fault Resistant Exponentiation Revisited.
In *FDTC*, pages 3–9. IEEE Computer Society, September 6 2009.
Lausanne, Switzerland.

[CM09] Jean-Sébastien Coron and Avradip Mandal.
PSS Is Secure against Random Fault Attacks.
In *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 653–666. Springer, December 6-10 2009.
Tokyo, Japan.

[CZ06] Zhimin Chen and Yujie Zhou.
Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage.
In *CHES*, volume 4249 of *LNCS*, pages 242–254. Springer, 2006.
Yokohama, Japan, http://dx.doi.org/10.1007/11894063_20.

[KKT04] Mark G. Karpovsky, Konrad J. Kulikowski, and Alexander Taubin.

Robust Protection against Fault Injection Attacks on Smart Cards Implementing the Advanced Encryption Standard.

In *DSN*, pages 93–101. IEEE Computer Society, June 28 – July 01 2004.

Florence, Italy.

[MMMT09] Robert P. McEvoy, Colin C. Murphy, William P. Marnane, and Michael Tunstall.

Isolated WDDL: A Hiding Countermeasure for Differential Power Analysis on FPGAs.

ACM Trans. Reconfigurable Technol. Syst. (TRETS), 2(1):1–23, 2009.

[SBG+09] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, Tarik Graba, and Jean-Luc Danger.

WDDL is Protected Against Setup Time Violation Attacks.

In *FDTC*, pages 73–83. IEEE Computer Society, September 6th 2009.

In conjunction with CHES'09, Lausanne, Switzerland. DOI: 10.1109/FDTC.2009.40; Online version: http://hal.archives-ouvertes.fr/hal-00410135/en/.

[THH+05] Kris Tiri, David Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, and Ingrid Verbauwhede.

A side-channel leakage free coprocessor IC in 0.18 μm CMOS for Embedded AES-based Cryptographic and Biometric Processing.

In *DAC*, pages 222–227. ACM, June 13-17 2005.

San Diego, CA, USA.