

Combined countermeasures against perturbation & observation attacks

Shivam BHASIN, Taoufik CHOUTA, Guillaume DUC, Jean-Luc DANGER,
Aziz EL AABID, Florent FLAMENT, Philippe HOOGVORST,
Tarik GRABA, **Sylvain GUILLEY**, Housseem MAGHR'EBI,
Olivier MEYNARD, Maxime NASSAR, Renaud PACALET,
Laurent SAUVAGE, **Nidhal SELMANE** and Youssef SOUISSI.

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



PASTIS workshop (ENSMSE, CMP-GC), June 16th, 2010.

Presentation Outline

- 1 Context
- 2 Asymmetric Cryptography
- 3 Symmetric Cryptography
 - Leakage-Resiliency
 - Perturbation-Resiliency
 - SCA+FIA Formally Provable Solutions
 - SCA+FIA Implementation-Level Solutions
- 4 Conclusion

Presentation Outline

- 1 Context
- 2 Asymmetric Cryptography
- 3 Symmetric Cryptography
 - Leakage-Resiliency
 - Perturbation-Resiliency
 - SCA+FIA Formally Provable Solutions
 - SCA+FIA Implementation-Level Solutions
- 4 Conclusion

Attacks Context

Attacks out there

- **Observation** attacks: passive
- **Perturbation** attacks: active and non-permanent
- **Manipulation** attacks: active and permanent

Worse: they are combined...

- **Sequentially**: complex attack paths
 - Observation attacks help prepare perturbation attacks.
 - EMA cartography guides EMI.
- **In parallel**:
 - Optically enhanced position-locked DPA [19].
 - PACA (tomorrow's presentation by Benoît FEIX [1, 5]).

Countermeasures Context

In this presentation, I talk about...

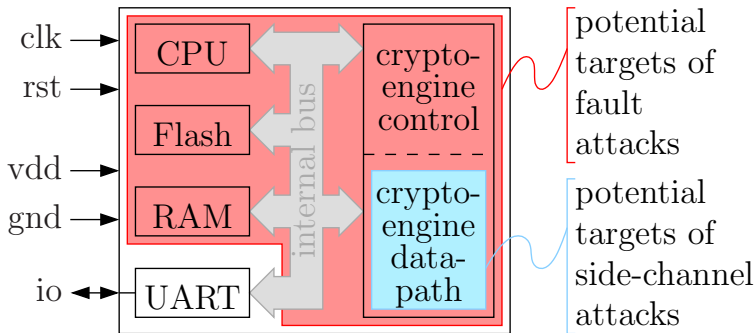
- **Observation** attacks: *aka* Side-Channel Leakage (**SCA**).
- **Perturbation** attacks: *aka* Fault-Injection Attacks (**FIA**).

Cost and risk: integrated countermeasures are better

- **Worst case**: the cost of each countermeasure multiplies.
 - The countermeasure to **one** attack facilitates **another** attack [22].
 - The combination of **two** countermeasures yields a weaker countermeasure [17].
- **Best case**: one single countermeasure is universal.
 - No risk of security paradigm **bias**.
 - No risk of **interference**.

Cryptography is the most demanding resource

smartcard



Susceptible organs of a smartcard in two representative sensitive operations (EXTERNAL and INTERNAL AUTHENTICATE).

Typically, the cryptography will be either **RSA** or **3DES**.

Presentation Outline

- 1 Context
- 2 Asymmetric Cryptography
- 3 Symmetric Cryptography
 - Leakage-Resiliency
 - Perturbation-Resiliency
 - SCA+FIA Formally Provable Solutions
 - SCA+FIA Implementation-Level Solutions
- 4 Conclusion

Observation attacks are easily thwarted by masking:

- $\forall r_1, r_2, (M^{d+r_1 \times \phi(N)} \bmod r_2 \times N) \bmod N = M^d \bmod N$, 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 [3].

This paper by Jean-Sébastien CORON (@ AsiaCrypt 2009) [6] proves that RSA with PSS is provably secure against random fault injection attacks in the random oracle model, and side-channel attacks.

Algorithm 1: RSA implementation protected against SCA and FIA.

Input : $x \in \mathbb{G}, d = (d_{n-1}, \dots, d_0)_2$ **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    $R[1 - d_i] \leftarrow R[1 - d_i] \cdot R[2]$ 
7    $R[2] \leftarrow R[2]^2$ 
8 end
9 if  $R[0] \cdot R[1] \cdot x = R[2]$  then
10   return  $r^{-1} \cdot R[0]$ 
11 else
12   return “Error”
13 end
```

Presentation Outline

- 1 Context
- 2 Asymmetric Cryptography
- 3 Symmetric Cryptography
 - Leakage-Resiliency
 - Perturbation-Resiliency
 - SCA+FIA Formally Provable Solutions
 - SCA+FIA Implementation-Level Solutions
- 4 Conclusion

Context in Symmetric Cryptography

Similar results would be welcomed in symmetric cryptography. However, the **malleability** of asymmetric crypto does not exist in symmetric crypto.

Let's start with observation attacks. Provable countermeasures [18] are rather **protocole-level**:

- if we cannot operate formally **within**,
- we operate **around**.

The main step has been to:

- resign from **leakage-proof** solutions, but instead
- resort to **leakage-resilient** solutions.

Leakage-resilient crypto

Traditional approaches: “within”

- Constant execution: DPL [12, Chp. 7]
- Random execution: masking [12, Chp. 9]
- Unpredictable execution: “glitch-ful” [2]
- Unexploitable execution: encrypted leakage [7]

Idea: “around”

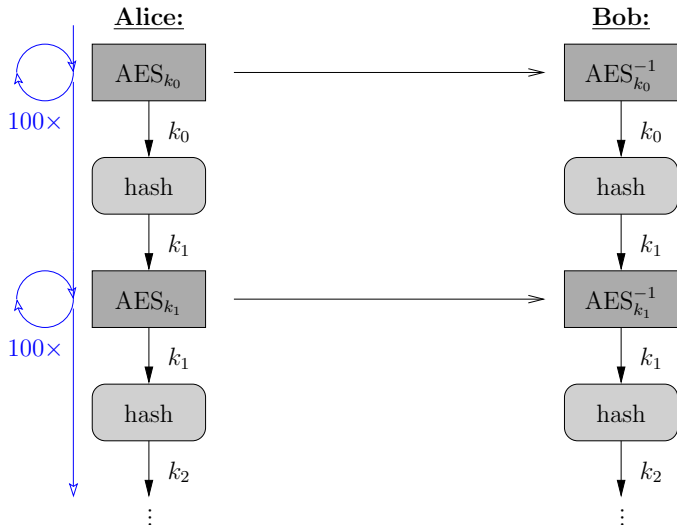
- It does not matter if the circuit leaks,
- as far as the leak is unexploitable.

Leakage-resilient crypto

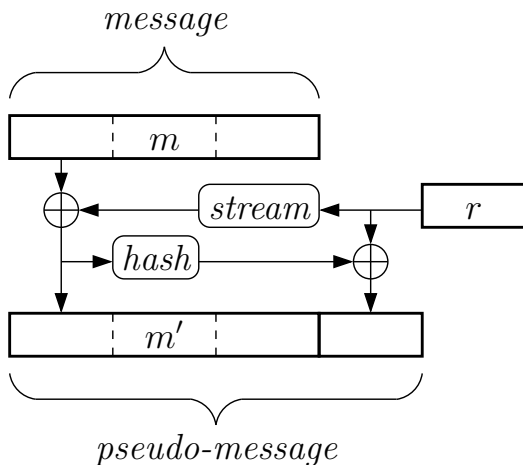
Two approaches

- 1 Renew the key on a regular basis:
 - Kocher's patent "Leak-resistant cryptographic indexed key update" [10, 11],
 - republished by UCL under title "Fresh rekeying" [16].
- 2 Have the input plaintext remain unexpected, when the output is kept secret:
 - Robert McEvoy's patent about "All-Or-Nothing Transforms" [14, 15],

Protocol level: if ≈ 1 bit is leaked per 100 encryptions...



All-Or-Nothing Transform (AONT)



AONT is an unkeyed probabilistic transform.

Leakage-Resilient Solutions

Pros and Cons

1 Rekeying:

- pros: no need for randomness.
- cons: keeping the synch / hashing overhead.

2 Random encryption:

- pros: no synchro since dynamic.
- cons: need for randomness / what about decryption?

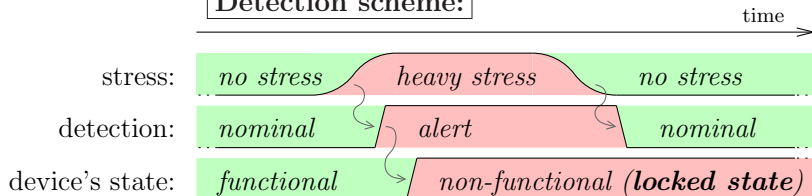
Let's try to apply the same methodology to fault attacks.

Reminder about the characteristics of detection:

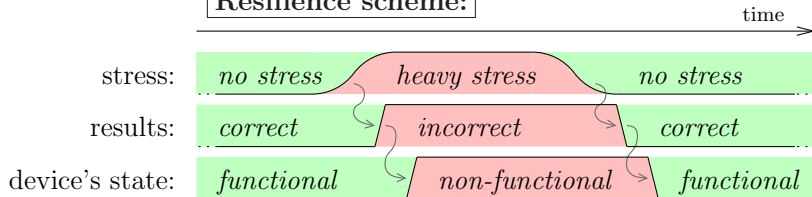
		Ciphertext incorrect?	
		Yes	No
Alarm raised?	Yes	Safe	Problem of availability
	No	Problem of security	Safe

Virtues of Resilience also against Perturbation Attacks [8]

Detection scheme:



Resilience scheme:



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 $(y = \text{AES}_k(x \oplus r), r)$.
-

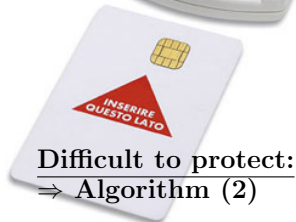
Algorithm 3: Deterministic Decryption Algorithm matching algorithm (2).

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

Output: The plaintext x .

- 1 Decrypt y with key k :
 $z = \text{AES}_k^{-1}(y)$.
 - 2 Return the demasked input:
 $z \oplus r = x$.
-

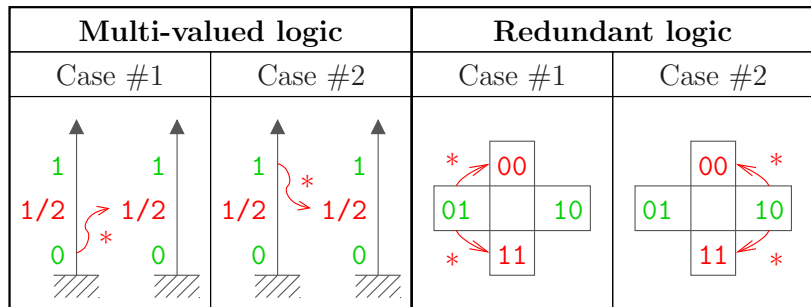
Suggestion of resolution for the dissymmetry encryption/decryption



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

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

When we cannot trust the external TRNG



Two kinds of faults (in red), namely $\{0, 1\} \xrightarrow{*} 1/2$ for 3-valued logic and $\{01, 10\} \xrightarrow{*} \{00, 11\}$, i.e. $\{\text{VALID0}, \text{VALID1}\}$ 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**: $\exists a \text{ VALID}, f(a, \text{NULL}) = \text{VALID}$;
- **DPL w/o EPE**: $\forall a \text{ VALID}, f(a, \text{NULL}) = \text{NULL}$.

DPL w/ EPE is Protected against Multiple Asymmetrical Faults

$b \backslash a$	VALID0	VALID1	NULL0
VALID0	VALID0	VALID0	VALID0 (EPE)
VALID1	VALID0	VALID1	NULL0
NULL0	VALID0 (EPE)	NULL0	NULL0

$b \backslash a$	'0'	'1'	'U'
'0'	'0'	'0'	'0'
'1'	'0'	'1'	'U'
'U'	'0'	'U'	'U'

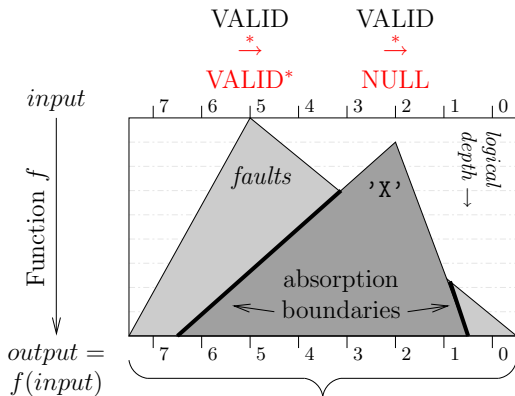
where the tokens {VALID0, VALID1, NULL0} implement respectively the items {'0', '1', 'U'}.

DPL w/o EPE is Protected in front of Multiple Symmetric Faults

$b \backslash a$	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:

$b \backslash a$	'0'	'1'	'X'
'0'	'0'	'0'	'X'
'1'	'0'	'1'	'X'
'X'	'X'	'X'	'X'



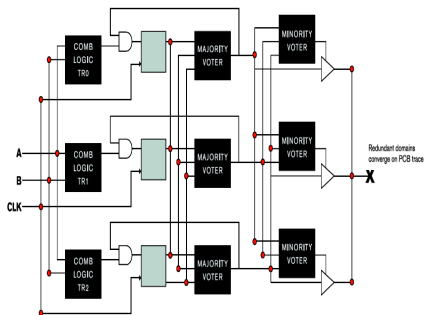
Combinatorial block (e.g. one sbox, such as AES SubBytes) implemented in DPL w/o EPE style

The output is mixed **NULL** and **VALID***

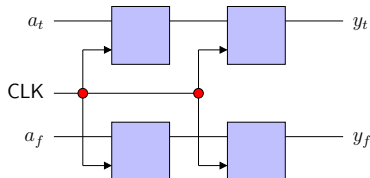
Multiple faults, where the false valid is not completely hidden by the 'X' wave. The 'X' avalanche absorbs most, if not all, the valid faults.

Performance overhead of different SCA+FIA countermeasures.

Strategy	Detection + DPL	Resilience = DPL	
Countermeasure	[9] + [21]	DRSL [4]	IWDDL [13]
Area	5.49 ×	2.56 ×	4.34 ×
Throughput	4.49 ×	2.00 ×	1.53 ×



Memorization element in triple modular redundancy as implemented in Xilinx “XTMR” solution [20].



Memorization element in DPL; although four times larger than an unprotected flip-flop, this structure is nevertheless much smaller than that involved in TMR logic.

Presentation Outline

- 1 Context
- 2 Asymmetric Cryptography
- 3 Symmetric Cryptography
 - Leakage-Resiliency
 - Perturbation-Resiliency
 - SCA+FIA Formally Provable Solutions
 - SCA+FIA Implementation-Level Solutions
- 4 Conclusion

Conclusions

- Asymmetric crypto is easier to protect than symmetric crypto
- Some solutions exist for asymmetric crypto
- Resilience seems to be the key
- Some reflex must be overcome...

- 2nd edition of the DPA contest is on-going
- Visit <http://www.DPAcontest.org/v2/>

- [1] Frédéric Amiel, Karine Villegas, Benoît Feix, and Louis Marcel.
Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis.
In *FDTC*, pages 92–102. IEEE Computer Society, 10 September 2007.
Vienna, Austria.
- [2] Shivam Bhasin, Sylvain Guilley, Laurent Sauvage, and Jean-Luc Danger.
Unrolling Cryptographic Circuits: A Simple Countermeasure Against Side-Channel Attacks.
In *RSA Cryptographers' Track, CT-RSA*, volume 5985 of *LNCS*, pages 195–207. Springer, March 1-5 2010.
San Francisco, CA, USA. DOI: 10.1007/978-3-642-11925-5_14.
- [3] 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.
- [4] 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.
- [5] Christophe Clavier, Benoît Feix, Georges Gagnerot, and Mylène Roussellet.
Passive and Active Combined Attacks on AES.
In *FDTC*. IEEE Computer Society, 21 August 2010.
Santa Barbara, CA, USA.
- [6] 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.

- [7] Sylvain Guilley and Jean-Luc Danger.
Protection des modules de cryptographie contre les attaques sur les canaux cachés par chiffrement Vernam des fuites d'information, May 11 2009.
Brevet Français, FR09/50342.
- [8] Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, and Nidhal Selmane.
Fault Injection Resilience.
In *FDTC*. IEEE Computer Society, August 21 2010.
Santa Barbara, CA, USA. Complete version: <http://hal.archives-ouvertes.fr/hal-00482194/en/>.
- [9] 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.
- [10] Paul C. Kocher.
Leak-resistant cryptographic indexed key update, March 25 2003.
United States Patent 6,539,092 filed on July 2nd, 1999 at San Francisco, CA, USA.
- [11] Paul C. Kocher.
From Proof to Practice: Real-World Cryptography (invited talk).
In *CHES*, volume 3156 of *Lecture Notes in Computer Science*. Springer, August 11-13 2004.
Cambridge, MA, USA.
- [12] Stefan Mangard, Elisabeth Oswald, and Thomas Popp.
Power Analysis Attacks: Revealing the Secrets of Smart Cards.
Springer, December 2006.
ISBN 0-387-30857-1, <http://www.dpabook.org/>.

- [13] 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.
- [14] Robert P. McEvoy, Michael Tunstall, Claire Whelan, Colin C. Murphy, and William P. Marnane. A differential side-channel analysis countermeasure. Filled in 27.01.2010.
- [15] Robert P. McEvoy, Michael Tunstall, Claire Whelan, Colin C. Murphy, and William P. Marnane. All-or-Nothing Transforms as a Countermeasure to Differential Side-Channel Analysis. Cryptology ePrint Archive, Report 2009/185, 2009. <http://eprint.iacr.org/>.
- [16] Marcel Medwed, François-Xavier Standaert, Johann Großschädl, and Francesco Regazzoni. Fresh Re-Keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. In *AFRICACRYPT*, volume 6055 of *LNCS*. Springer, May 03-06 2010. Stellenbosch, South Africa.
- [17] Elke De Mulder, Benedikt Gierlichs, Bart Preneel, and Ingrid Verbauwhede. Practical DPA Attacks on MDPL. In *First International Workshop on Information Forensics and Security (WIFS)*. IEEE Signal Processing Society, December 6-9 2009. London, United Kingdom. Also <http://eprint.iacr.org/2009/231>.
- [18] Workshop on “Provable Security against Physical Attacks”, February 10-19 2010. Amsterdam, Netherlands. <http://www.lorentzcenter.nl/lc/web/2010/383/program.php?wsid=383>.
- [19] Sergei P. Skorobogatov. Optically Enhanced Position-Locked Power Analysis. In *CHES*, volume 4249 of *LNCS*, pages 61–75. Springer, October 10-13 2006. Yokohama, Japan.

- [20] The "Xilinx TMR Tool". Features description at this web page:
http://www.xilinx.com/ise/optional_prod/tmrtool.htm.
- [21] 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.
- [22] Sung-Ming Yen and Marc Joye.
Checking Before Output May Not Be Enough Against Fault-Based Cryptanalysis.
IEEE Trans. Computers, 49(9):967–970, 2000.
DOI: 10.1109/12.869328.