Sécurité des systèmes embarqués contre les phases d'identification et d'exploitation

Sylvain GUILLEY
sylvain.guilley@secure-ic.com

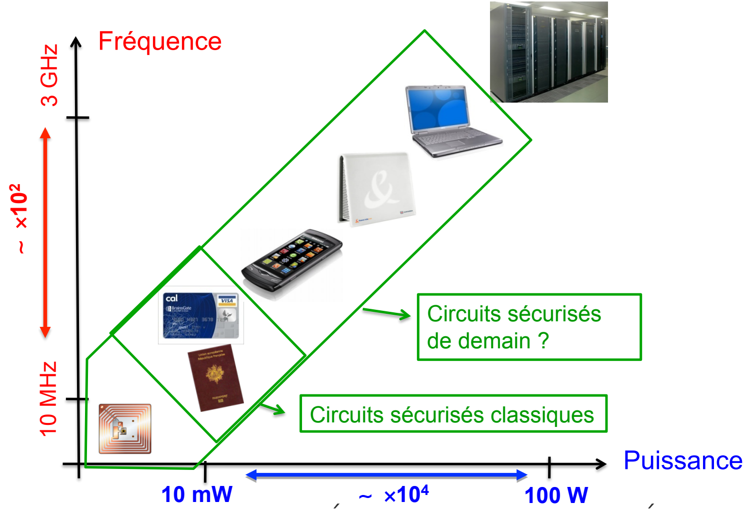
COGITO workshop, Dec. 3rd, 2015.

SECURE IC
THE TRUSTED COMPUTING COMPANY

TELECOM ParisTech

❑ Contexte et motivations – Sécurité matérielle

- Circuits sécurisés

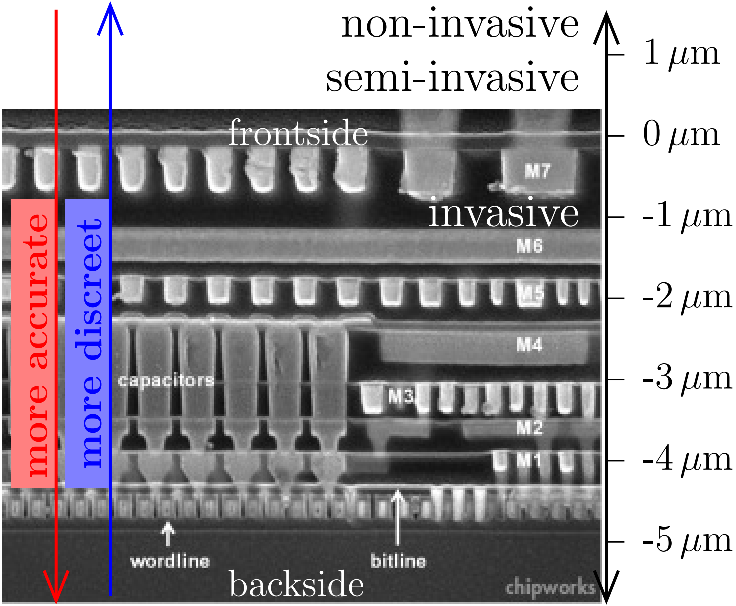


Courtesy of Jean-Max Dutertre, École des Mines de Saint-Étienne.

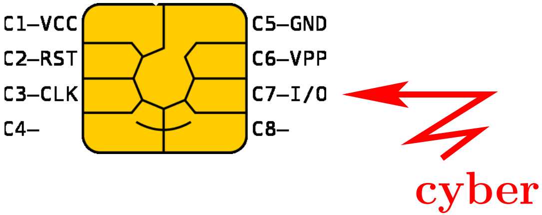
Outline

Outline

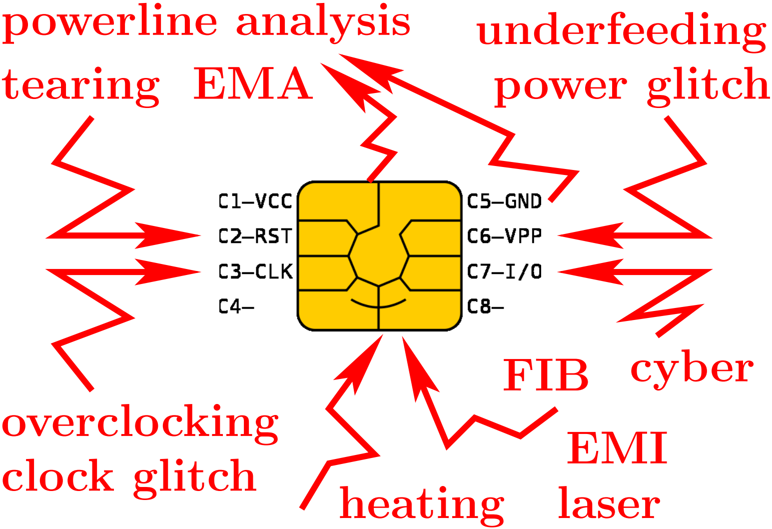
Physical attacks



Cyber attacks



Cyber-physical attacks



Defense bricks

- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Defense bricks

- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Security / perf tradeoffs, with formal guarantees

Defense bricks

- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Provably secure key generation resistant to harmonic fault injection

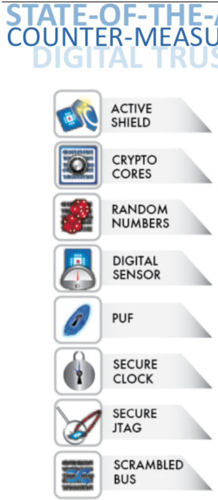
Defense bricks

- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Non-stored keys, with large reliability and aging resistance

Defense bricks



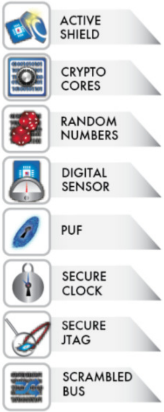
- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

All-in-one 360° protection against fault injection attacks

Defense bricks

STATE-OF-THE-ART
COUNTER-MEASURES
DIGITAL TRUST



- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Cryptographic protection against FIB and probing invasive attacks

Defense bricks

- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Various levels of user programmable jittered clock, against fault and side-channel attacks

Defense bricks

- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Crypto-grade combinational (< 1 clock latency) bus and memory encryption & decryption

Defense bricks

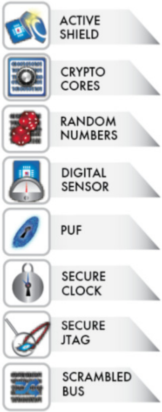
- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Tamper-proof circuit debugging interface, with cryptographic authentication

Defense bricks

STATE-OF-THE-ART COUNTER-MEASURES
DIGITAL TRUST



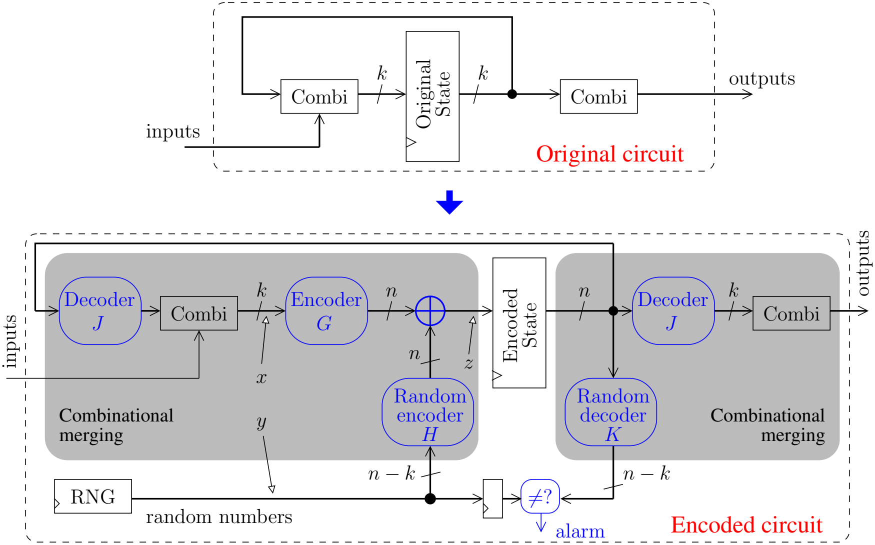
- **Secure IP cores that leverage patents / know-how in security**
  - Tunable Cryptography
  - True Random Number Generator
  - Physically Unclonable Function
  - Digital Sensor
  - Active Shield
  - Secure Clock
  - Scrambled Bus
  - Secure JTAG
  - CyberCPU

Details:

Real-time hardware-level detection of data & instruction corruption

Defense against attackers inside the chips

FIB and Hardware Trojan Horses [BCC+14, NBD+15, CDD+15]



Defense against attackers inside the chips

FIB and Hardware Trojan Horses

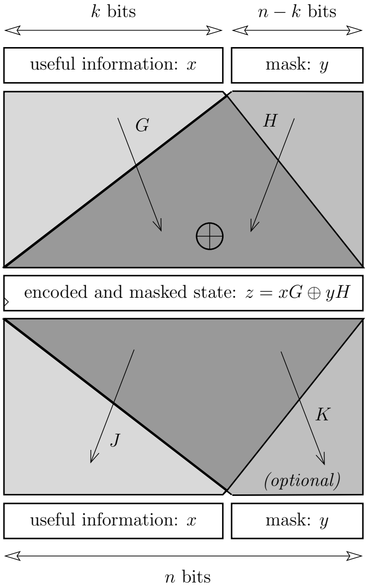
Theory [CG14, CG15]

In general:

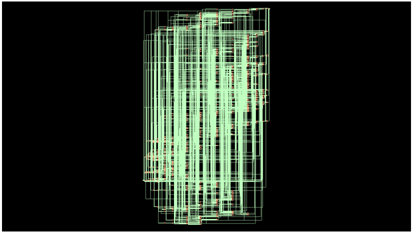
$$\begin{pmatrix} G \\ H \end{pmatrix}^{-1} = \begin{pmatrix} J & K \end{pmatrix} .$$

If $GH^{\mathsf{T}} = 0$,

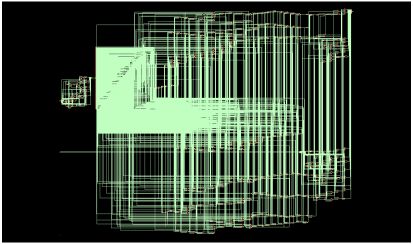
- $z \Rightarrow x$ using
  $J = G^{+} = G^{\mathsf{T}}(GG^{\mathsf{T}})^{-1}$,
- $z \Rightarrow y$ using
  $K = H^{+} = H^{\mathsf{T}}(HH^{\mathsf{T}})^{-1}$.



AES S-Box



Original



Encoded

Outline

Evolution of attacks and defense techniques

Analysis of attack / defense
- Generic protections
- Role of SNR in side-channel attacks
- Link between SNR and probability of success

From SmartCards to System-on-Chips

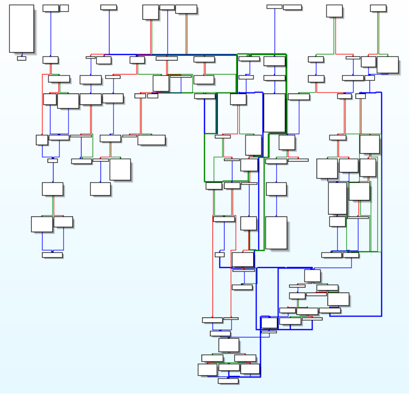
Conclusions

Vision of Common Criteria

Attack / Defense	**Identification**	**Exploitation**
Obscurity	xxx	
Clarity		xxx

Application to cyber-attacks

Identification



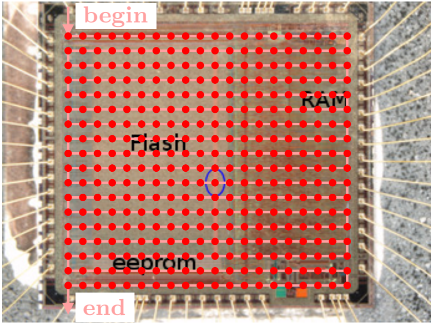
Exploitation

```
shellcode:
  jmpl %o2+%o3,%o7    ! like a call
  add  %o5,%o3,%o0    ! addr of secret buffer
  jmpl %o2+%o4,%l7    ! jump to prev address
  and %i7,0x1FFF,%g0  ! nop
```

(16 bytes)

Application to physical-attacks

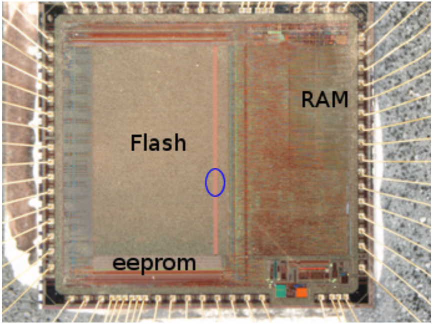
Identification



Exploitation

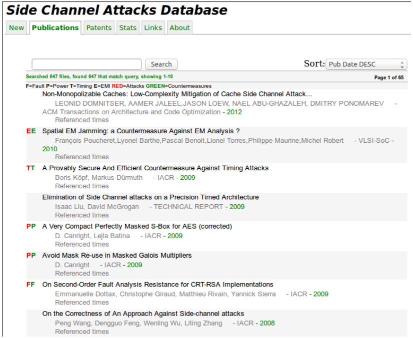
Application to physical-attacks

Identification



Exploitation

How to handle **all** attacks?



Countermeasures must be aware of **all** attacks

- "*Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing*" by YongBin Zhou and DengGuo Feng [ZF05],
- "*700+ Attacks Published on Smart Cards: The Need for a Systematic Counter Strategy*" by Mathias Wagner [Wag12].

Generic protections against SCA + FIA

Against SCA

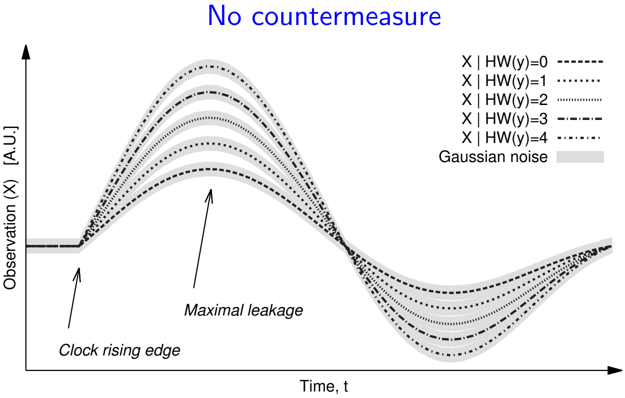
- Randomize
  - Data: with masks
  - Control: with shuffling
- Balance
- Tolerate: resilience

Against FIA

- Verification
  - Data: with codes
  - Control: with check-points
- Tolerate:
  - denial of exploitation
  - infective countermeasures

Example: protection against SCA

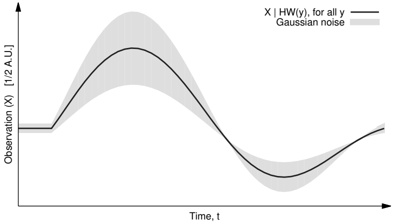
Reduce the SNR!



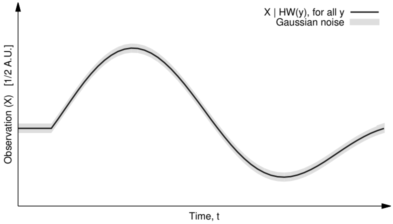
Example: protection against SCA

Reduce the SNR!

Masking (randomization)



Hiding (balancing)



Some definitions

Definition (Signal-to-Noise Ratio [MOP06])

$$\text{SNR} = \frac{\text{Var}[\mathbb{E}[X|Y]]}{\mathbb{E}[\text{Var}[X|Y]]} \ . \tag{1}$$

Definition (Normalized Inter-Class Variance)

$$\text{NICV} = \frac{\text{Var}[\mathbb{E}[X|Y]]}{\mathbb{E}[X]} = \frac{1}{1 + \frac{1}{\text{SNR}}} \ . \tag{2}$$

Remark

NICV is also named: coefficient of determination, F-test, coefficient of non-linear correlation, etc.

Relationship to correlation power attacks [BDGN14]

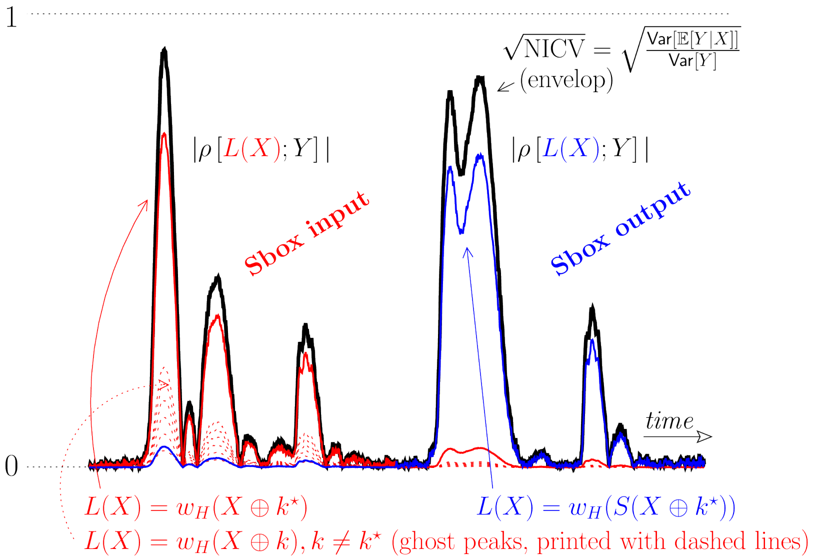
Proposition

$$\forall L : \mathbb{F}_2^n \to \mathbb{R} \ ,$$

$$\boxed{0 \ \leq \ \rho^2 \left[X; L(Y)\right] \ \leq \ \frac{\mathrm{Var}[\mathbb{E}[X|Y]]}{\mathrm{Var}[X]} \ = \ NICV \ \leq \ 1} \ . \qquad (3)$$

Proof.

It is a direct application of the Cauchy-Schwarz theorem.
There is equality if and only if L is proportional to the actual leakage. □


1
0
$\sqrt{\text{NICV}} = \sqrt{\frac{\text{Var}[\mathbb{E}[Y|X]]}{\text{Var}[Y]}}$
(envelop)
$|\rho[L(X);Y]|$
$|\rho[L(X);Y]|$
Sbox input
Sbox output
time
$L(X) = w_H(X \oplus k^\star)$
$L(X) = w_H(S(X \oplus k^\star))$
$L(X) = w_H(X \oplus k), k \neq k^\star$ (ghost peaks, printed with dashed lines)

Probability of success

Definition

$$\mathbb{P}_S = \mathbb{P}(\hat{K} = K^\star) \ .$$

Proposition (Characterization [HRG14])

When the keys are equiprobable and the model $\phi \circ f$ is known, maximizing $\mathbb{P}_S$ is equivalent to maximizing:
$p(\mathbf{x}|\mathbf{y}(k^\star)) = p_{\mathbf{N}}(\mathbf{x} - \mathbf{y}(k^\star)) = \prod_{i=1}^{m} p_{N_i}(x_i - y_i(k^\star))$.

Corollary

The optimal distinguisher when the noise is Gaussian is:

$$k^\star \in \mathcal{K} \qquad \mapsto \qquad -\|\mathbf{x} - \phi(f(k^\star, \mathbf{t}))\|^2 \ .$$

Success Rate: Goal

- Compute the exact probability of success $\mathbb{P}_S$
- Rigorous mathematical computation of its first order exponent of success rate:

$$\mathbb{P}_S \approx 1 - e^{-mE} \quad \text{for some } E \ . \tag{4}$$

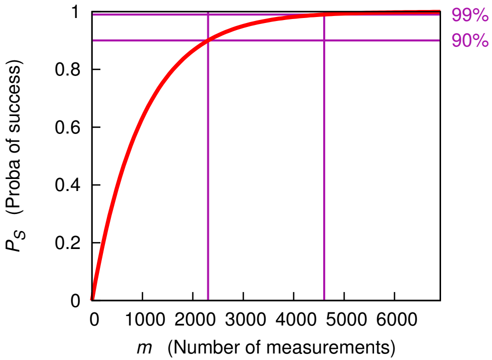
Definition (First-Order Exponent Equivalence)

A sequence p_m of positive numbers admits a first-order exponent E_m if $\epsilon_m = E_m + \frac{1}{m} \ln p_m$ tends to zero as $m \to +\infty$. In this case we write:

$$p_m \approx e^{-mE_m} \ .$$

Example *where E_m does not depend on m*

- By Eq. (4), if $\mathbb{P}_S = 90\%$, then $m = \frac{\ln(10)}{E}$;
- Doubling the number of measurements
  $m \longrightarrow 2m \implies \mathbb{P}_S = 99\%$.



$(E = 10^{-3})$

Result for Gaussian noise & optimal distinguisher (norm-2)

Proposition (CHES '14 poster & INDOCRYPT '15 [GHR15])

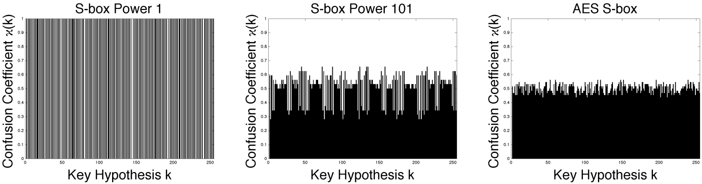
When $X = \alpha Y(k^\star) + N$, with $N \sim \mathcal{N}(0, \sigma^2)$ is the noise:

$$E = \frac{1}{8\sigma^2} \min_{k \neq k^\star} \mathbb{E}(Y(k) - Y(k^\star))^2 \quad (5)$$

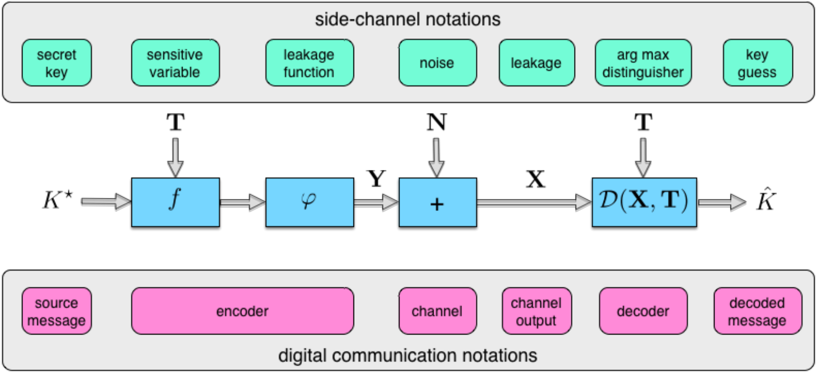
$$= \frac{1}{2} SNR \min_{k \neq k^\star} \kappa_{k,k^\star} \quad , \quad (6)$$

where:

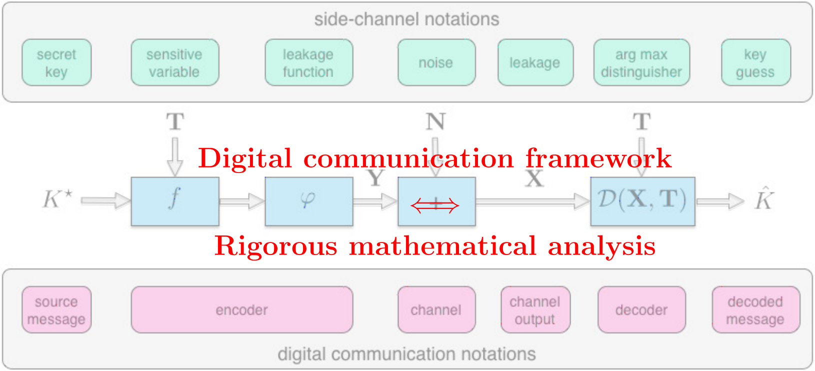
- $SNR = \frac{\alpha^2}{\sigma^2}$, *and*
- $\kappa_{k,k^\star} = \frac{1-\rho(Y(k),Y(k^\star))}{2}$ *is the confusion coefficient [FLD12].*



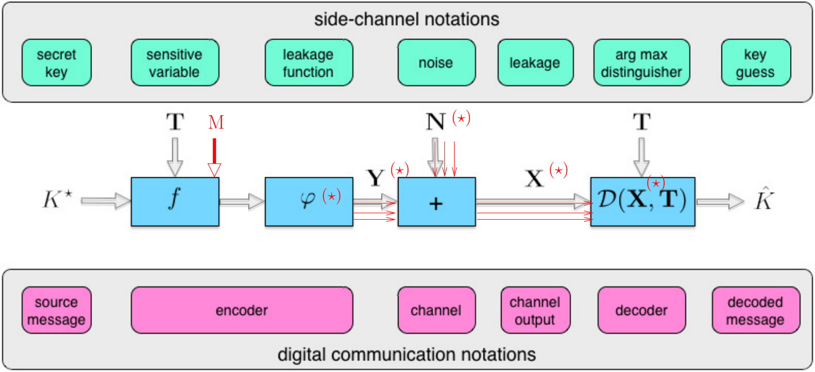
Side-Channel Analysis as a Digital Com. Problem (CHES '14 [HRG14])



Side-Channel Analysis as a Digital Com. Problem (CHES '14 [HRG14])



Side-Channel Analysis as a Digital Com. Problem (CHES '14 [HRG14])



Explicit Derivations for Masking [BGHR14]

Theorem (Second-order HOOD)

If the model (i.e., $\phi^{(\omega)}$) is known to the attacker for all ω, then the second-order HOOD is:

$$\mathcal{D}^2_{opt}(\mathbf{x}^{(\star)}, \mathbf{t}^{(\star)}) = \underset{k \in \mathcal{K}}{\arg\max}\ p_k(\mathbf{x}^{(\star)} | \mathbf{t}^{(\star)})$$

$$= \underset{k \in \mathcal{K}}{\arg\max} \prod_{i=1}^{q} \sum_{m^{(\star)} \in \mathcal{M}^{(\star)}} \mathbb{P}(m^{(\star)}) \prod_{\omega=0}^{1} p_k(x_i^{(\omega)} | t_i^{(\omega)}, m^{(\omega)}).$$

Explicit Derivations for Masking [BGHR14]

Theorem (High-order HOOD)

If the model (i.e., $\phi^{(\omega)}$) is known to the attacker for all ω, then the high-order HOOD is:

$$\mathcal{D}_{opt}^{d+1}(\mathbf{x}^{(\star)}, \mathbf{t}^{(\star)}) = \arg\max_{k \in \mathcal{K}} \ p_k(\mathbf{x}^{(\star)} | \mathbf{t}^{(\star)})$$

$$= \arg\max_{k \in \mathcal{K}} \prod_{i=1}^{q} \sum_{m^{(\star)} \in \mathcal{M}^{(\star)}} \mathbb{P}(m^{(\star)}) \prod_{\omega=0}^{d} p_k(x_i^{(\omega)} | t_i^{(\omega)}, m^{(\omega)}).$$

Explicit Derivations for Masking [BGHR14]

Theorem (High-order HOOD — is *additive*)

If the model (i.e., $\phi^{(\omega)}$) is known to the attacker for all ω, then the high-order HOOD is:

$$\mathcal{D}_{opt}^{d+1}(\mathbf{x}^{(\star)}, \mathbf{t}^{(\star)}) = \underset{k \in \mathcal{K}}{\arg\max}\; p_k(\mathbf{x}^{(\star)} | \mathbf{t}^{(\star)})$$

$$= \underset{k \in \mathcal{K}}{\arg\max} \sum_{i=1}^{q} \log \sum_{m^{(\star)} \in \mathcal{M}^{(\star)}} \mathbb{P}(m^{(\star)}) \prod_{\omega=0}^{d} p_k(x_i^{(\omega)} | t_i^{(\omega)}, m^{(\omega)}).$$

Taylor expansion of attacks, in the SNR (denoted as γ)

Theorem (Mixed order attack)

$$\log \mathbb{E} \exp\left(-\gamma \|x - y(t,k,M)\|^2\right) = \sum_{\ell=1}^{+\infty} \frac{\kappa_\ell}{\ell!} (-\gamma)^\ell \ .$$

Theorem (Two order attack)

Assuming the masking implementation is perfect at order L, the next order successful attack is the one at order $L+2$ which maximizes LL_{L+2}. This is equivalent to summing

$$\mu_{L+1}(1+\gamma\mu_1) - \gamma \frac{\mu_{L+2}}{L+2}$$

over all traces and

- *maximize the result over the key hypothesis, if L is odd;*
- *minimize the result over the key hypothesis, if L is even.*

Taylor expansion of attacks, in the SNR (denoted as γ)

Theorem (Mixed order attack)

$$\log \mathbb{E} \exp\big(-\gamma \|x - y(t, k, M)\|^2\big) = \sum_{\ell=1}^{+\infty} \frac{\kappa_\ell}{\ell!} (-\gamma)^\ell \ .$$

Here, κ_ℓ is a cumulant [LB10]! Such notion is related to moments μ_ℓ...

Theorem (Two order attack)

Assuming the masking implementation is perfect at order L, the next order successful attack is the one at order $L+2$ which maximizes LL_{L+2}. This is equivalent to summing

$$\mu_{L+1}(1 + \gamma\mu_1) - \gamma \frac{\mu_{L+2}}{L+2}$$

over all traces and

- *maximize the result over the key hypothesis, if L is odd;*
- *minimize the result over the key hypothesis, if L is even.*

Concrete results + comparison with [PRB09, BGNT15]

Algorithm 1: Shuffled Table re-computation

input : Genuine SubBytes $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$

output : Masked SubBytes $S' : \mathbb{F}_2^n \to \mathbb{F}_2^n$

1 $m \leftarrow_{\mathcal{R}} \mathbb{F}_2^n$, $m' \leftarrow_{\mathcal{R}} \mathbb{F}_2^n$ `// Draw of random input and output masks`

2 $\varphi \leftarrow_{\mathcal{R}} \mathbb{F}_2^n \to \mathbb{F}_2^n$ `// Draw of random permutation of` $\mathbb{F}_2^n$

3 **for** $\omega \in \{0, 1, \ldots, 2^n - 1\}$ **do** `// S-Box masking`

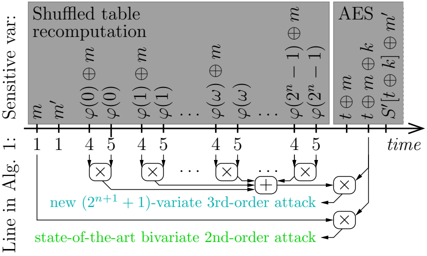
4 $\quad z \leftarrow \varphi(\omega) \oplus m$ `// Masked input`

5 $\quad z' \leftarrow S[\varphi(\omega)] \oplus m'$ `// Masked output`

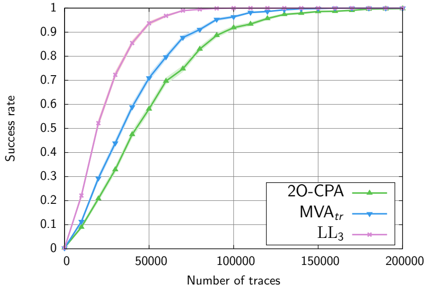
6 $\quad S'[z] = z'$ `// Creating the masked S-Box entry`

7 **end**

8 **return** S'



Attack on shuffled table recomputation: medium noise, $\sigma = 7$:



Outline

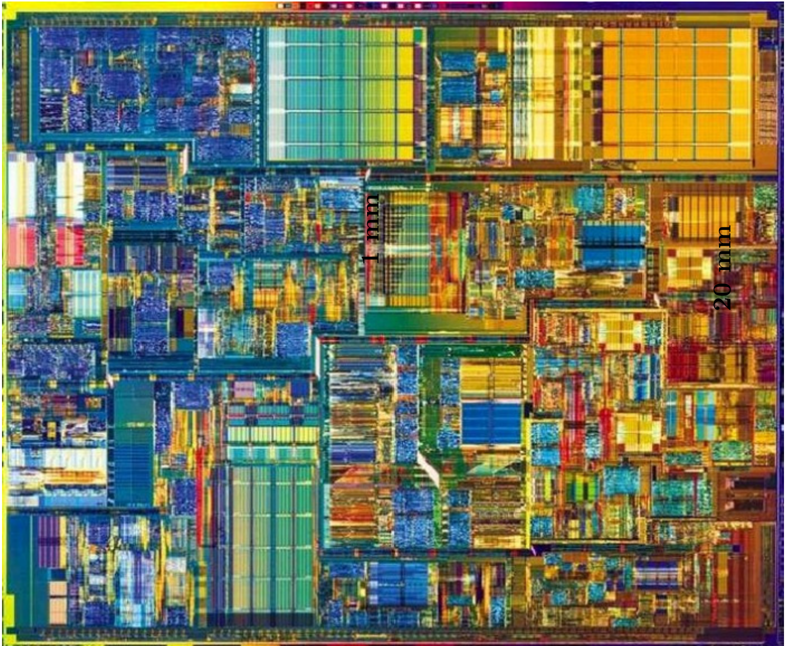
Evolution of attacks and defense techniques

Analysis of attack / defense

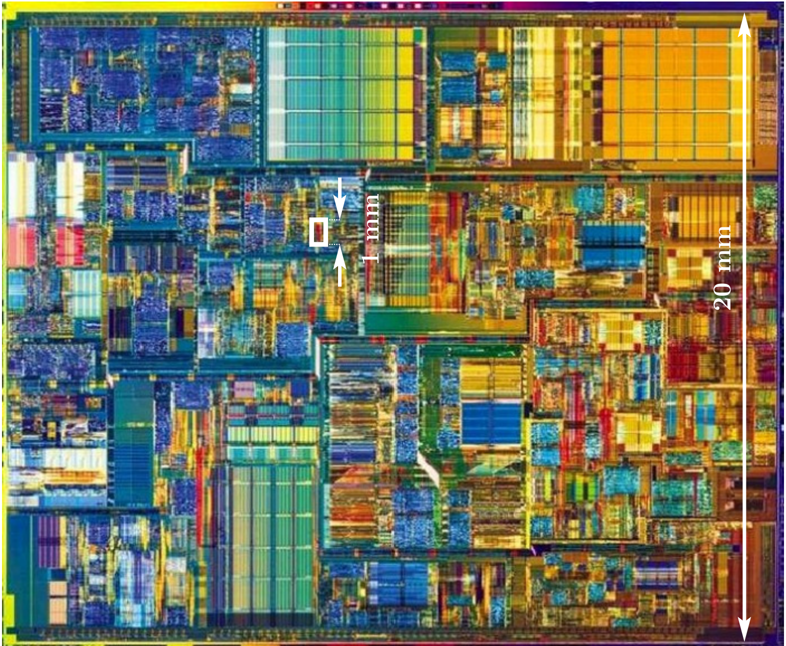
From SmartCards to System-on-Chips

Conclusions

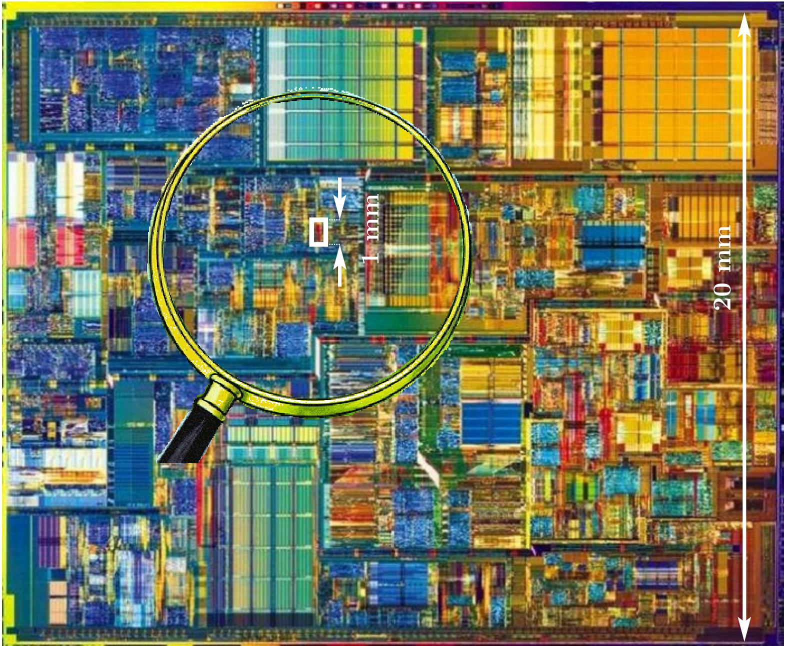
SmartCard to System-on-Chip



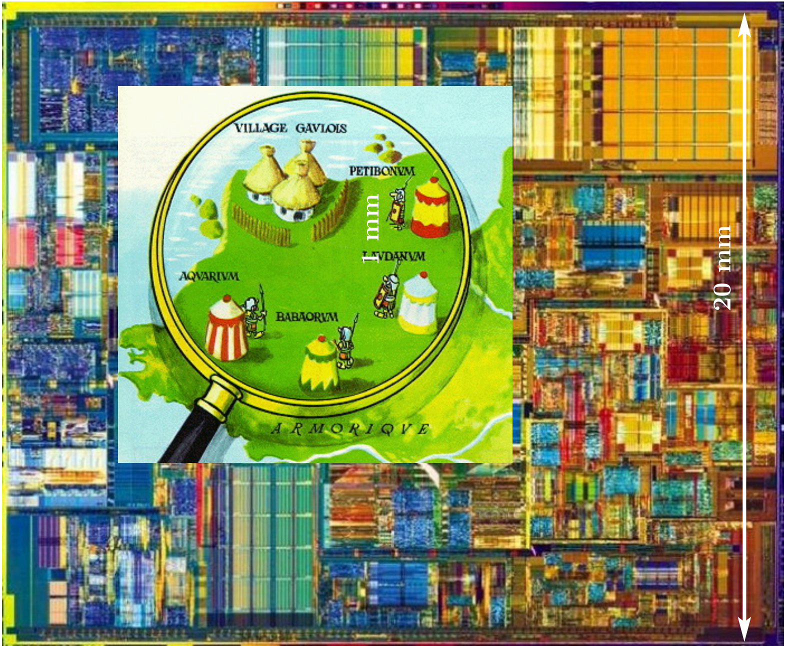
SmartCard to System-on-Chip



SmartCard to System-on-Chip



SmartCard to System-on-Chip



Discussion about pros/cons of security of SC vs SoC

Feature	Secure SmartCard	Secure System-on-Chip
Size	small	large
Techno	90 nm	$<$ 28 nm
Ports	$<$ 8	$>$ 500
API	ISO 7816	Proprietary
Red/Black	Yes	No

Discussion about pros/cons of security of SC vs SoC

Against invasive attacks good / bad

Feature	Secure SmartCard	Secure System-on-Chip
Size	small	large
Techno	90 nm	$<$ 28 nm
Ports	$<$ 8	$>$ 500
API	ISO 7816	Proprietary
Red/Black	Yes	No

Discussion about pros/cons of security of SC vs SoC

Against fault injection attacks good / bad

Feature	Secure SmartCard	Secure System-on-Chip
Size	small	large
Techno	90 nm	$<$ 28 nm
Ports	$<$ 8	$>$ 500
API	ISO 7816	Proprietary
Red/Black	Yes	No

Discussion about pros/cons of security of SC vs SoC

Against side-channel attacks good / bad

Feature	Secure SmartCard	Secure System-on-Chip
Size	small	large
Techno	90 nm	$<$ 28 nm
Ports	$<$ 8	$>$ 500
API	ISO 7816	Proprietary
Red/Black	Yes	No

Outline

Evaluation: three philosophies for an effective defense

- **1. Defense in depth**:
  - Multiple layers
- **2. Security by obscurity**:
  - Customize the protections
- **3. Software patches**:
  - Enrich the API

Opportunities for SoCs

- More defense in depth:
  - System-level protections
- Powerful CPUs:
  - Crazy countermeasures become realistic!
- Hardware countermeasures can be unleashed!
  - Do not forget hardware is the root of trust!

Standardization

CC [Cri13]

Common Criteria

Supporting Document
Mandatory Technical Document

Application of Attack Potential to Smartcards

May 2013

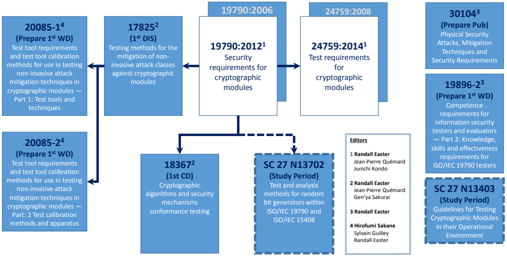
Version 2.9

CCDB-2013-05-002

ISO [Eas12]

ISO International Organization for Standardization

Cryptographic Module Testing – ISO Standards



Sécurité des systèmes embarqués contre les phases d'identification et d'exploitation

Sylvain GUILLEY
sylvain.guilley@secure-ic.com

COGITO workshop, Dec. 3rd, 2015.

SECURE IC
THE TRUSTED COMPUTING COMPANY

TELECOM ParisTech

[BCC+14] Julien Bringer, Claude Carlet, Hervé Chabanne, Sylvain Guilley, and Houssem Maghrebi.
Orthogonal Direct Sum Masking – A Smartcard Friendly Computation Paradigm in a Code, with Builtin Protection against Side-Channel and Fault Attacks.
In *WISTP*, volume 8501 of *LNCS*, pages 40–56. Springer, June 2014. Heraklion, Greece.

[BDGN14] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm.
Side-channel Leakage and Trace Compression Using Normalized Inter-class Variance.
In *Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy*, HASP '14, pages 7:1–7:9, New York, NY, USA, 2014. ACM.

[BGHR14] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, and Olivier Rioul.
Masks Will Fall Off – Higher-Order Optimal Distinguishers.
In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 344–365. Springer, 2014.

[BGNT15] Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, and Yannick Teglia.
Multi-variate high-order attacks of shuffled tables recomputation.
In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, volume 9293 of *Lecture Notes in Computer Science*, pages 475–494. Springer, 2015.

[BR14] Lejla Batina and Matthew Robshaw, editors.
Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings, volume 8731 of *Lecture Notes in Computer Science*. Springer, 2014.

[CDD+15] Claude Carlet, Abderrahman Daif, Jean-Luc Danger, Sylvain Guilley, Zakaria Najm, Xuan Thuy Ngo, and Cédric Tavernier.
Optimized Linear Complementary Codes Implementation for Hardware Trojan Prevention.
In *22nd European Conference on Circuit Theory and Design, ECCTD2015*, pages Trondheim, Norway, August 24-26 2015.

[CG14] Claude Carlet and Sylvain Guilley.
Complementary Dual Codes for Counter-measures to Side-Channel Attacks.
In Springer, editor, *ICMCTA, 4th International Castle Meeting on Coding Theory and Applications*, CIM-MS, September 15-18 2014.
Palmela, Portugal. URL: `http://icmcta.web.ua.pt`. (article #9). ISBN 978-3-319-17295-8. `http://www.springer.com/978-3-319-17295-8`.

[CG15] Claude Carlet and Sylvain Guilley.
Complementary Dual Codes for Counter-measures to Side-Channel Attacks.
Advances in Mathematics and Communications (AMC), 2015.

[Cri13] Common Criteria.
Application of Attack Potential to Smartcards, Mandatory Technical Document, Version 2.9, Revision 2, CCDB-2013-05-002, May 2013.
http://www.commoncriteriaportal.org/files/supdocs/CCDB-2013-05-002.pdf.

[Eas12] Randall J. Easter.
Text for ISO/IEC 1st WD 17825 – Information technology – Security techniques – Non-invasive attack mitigation test metrics for cryptographic modules, January 19 2012.
Prepared within ISO/IEC JTC 1/SC 27/WG 3. (Online).

[FLD12] Yunsi Fei, Qiasi Luo, and A. Adam Ding.
A Statistical Model for DPA with Novel Algorithmic Confusion Analysis.
In Emmanuel Prouff and Patrick Schaumont, editors, *CHES*, volume 7428 of *LNCS*, pages 233–250. Springer, 2012.

[GHR15] Sylvain Guilley, Annelie Heuser, and Olivier Rioul.
A Key to Success - Success Exponents for Side-Channel Distinguishers.
In Alex Biryukov and Vipul Goyal, editors, *Progress in Cryptology - INDOCRYPT 2015 - 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings*, volume 9462 of *Lecture Notes in Computer Science*, pages 270–290. Springer, 2015.

[HRG14] Annelie Heuser, Olivier Rioul, and Sylvain Guilley.
Good Is Not Good Enough - Deriving Optimal Distinguishers from Communication Theory.
In Batina and Robshaw [BR14], pages 55–74.

[LB10] Thanh-Ha Le and Maël Berthier.
Mutual Information Analysis under the View of Higher-Order Statistics.
In Isao Echizen, Noboru Kunihiro, and Ryôichi Sasaki, editors, *IWSEC*, volume 6434 of *Lecture Notes in Computer Science*, pages 285–300. Springer, 2010.

[MOP06] 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/.

[NBD+15] Xuan Thuy Ngo, Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm.
Linear complementary dual code improvement to strengthen encoded circuit against hardware trojan horses.
In *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2015, Washington, DC, USA, 5-7 May, 2015*, pages 82–87. IEEE, 2015.

[PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan.
Statistical Analysis of Second Order Differential Power Analysis.
IEEE Trans. Computers, 58(6):799–811, 2009.

[Wag12] Mathias Wagner.
700+ Attacks Published on Smart Cards: The Need for a Systematic Counter Strategy.
In Werner Schindler and Sorin A. Huss, editors, *COSADE*, volume 7275 of *LNCS*, pages 33–38. Springer, 2012.

[ZF05] YongBin Zhou and DengGuo Feng.
Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing.
Cryptology ePrint Archive, Report 2005/388, 2005.
http://eprint.iacr.org/2005/388.