State-of-the-art of international standardisation of side-channel analysis test methodologies and calibration of acquisition tools

Sylvain GUILLEY
sylvain.guilley@TELECOM-ParisTech.fr

September 10, 2015, PARIS

Overview on the workshop topic

Workshop on Implementation: Security and Evaluation

Overview on the workshop topic

tactic

Workshop on Implementation: Security and Evaluation

strategy

Overview on the workshop topic

Overview on the workshop topic

reality !!!

painful experience

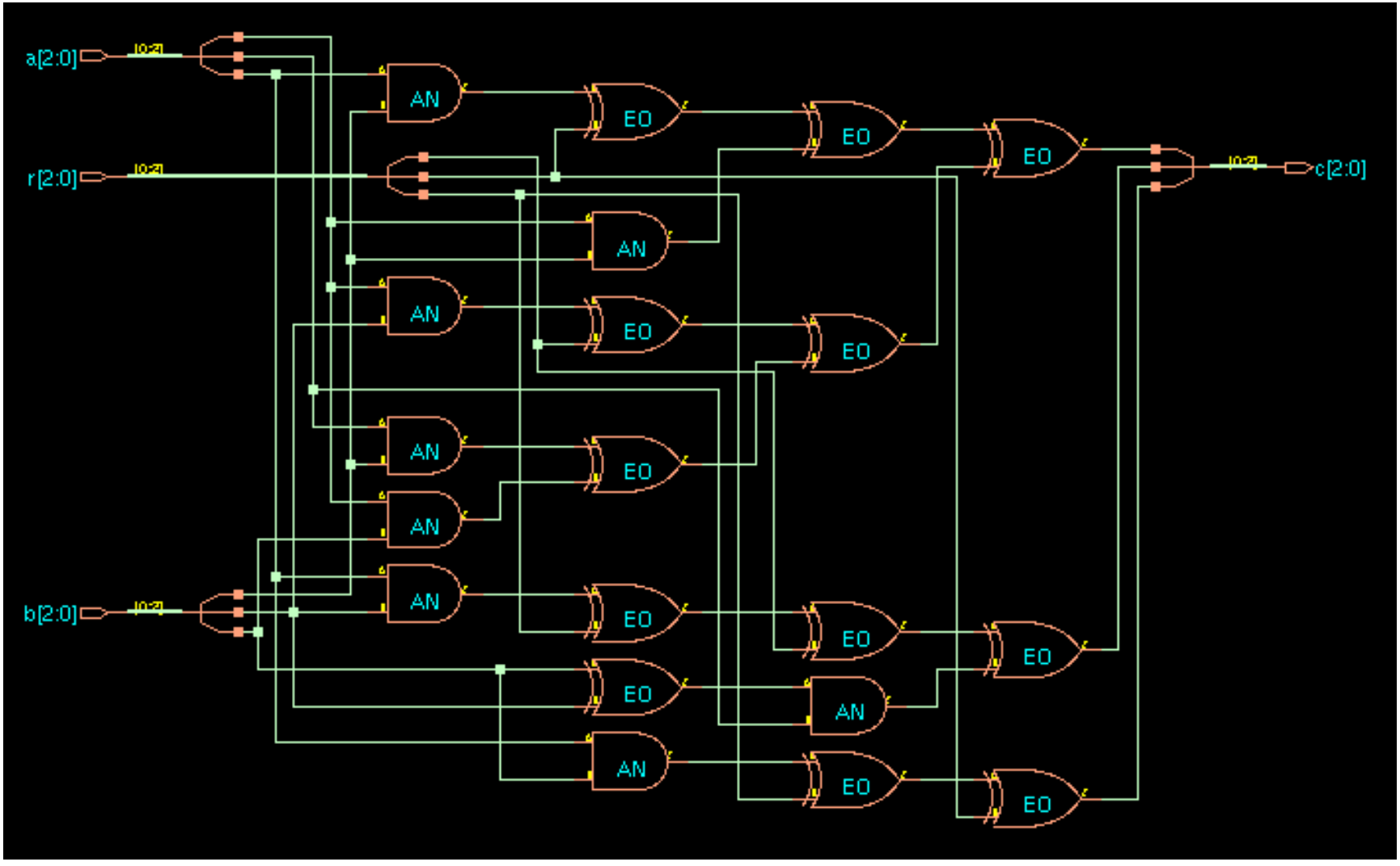
Workshop on Implementation: Security and Evaluation

silicon proven + various certifs.

Problem #1 Gap btw theory & practice

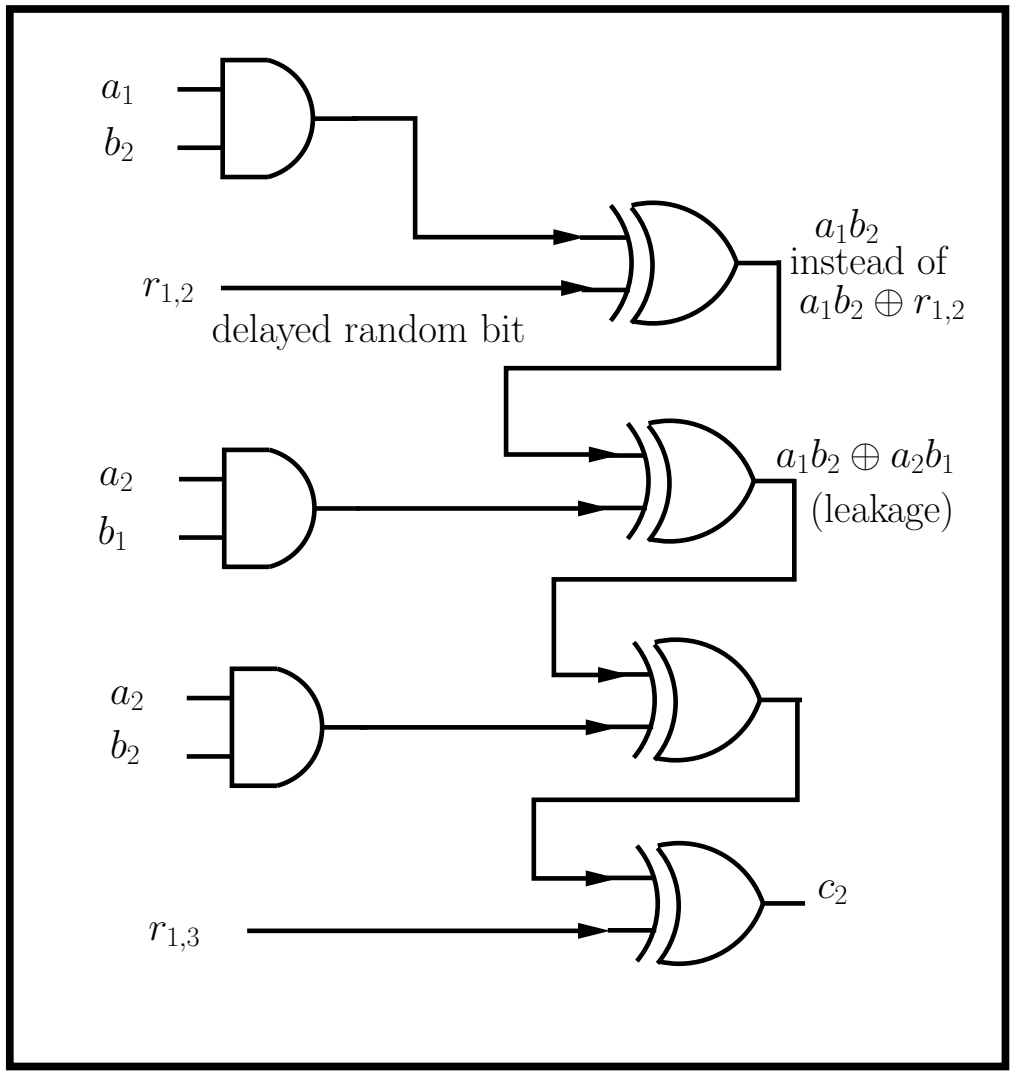
- In practice, it does not work
  - Assumptions may be invalid...
  - Errors while implementing implementation-level protections...
- Modelization with the same accuracy of *important* parts & *tiny* parts
- How to implement theoretical requirements: e.g., random numbers generation?

Warning for optimizations (Cadence) [ISW03]



Caption: AN = `and`, EO = `xor`.

In practice, it does not work [RBG+15]



Algorithm: CRT-RSA with Vigilant's countermeasure

Input: Message M, key (p, q, d_p, d_q, i_q) **Output:** Signature $M^d \mod N$, or a random value in $\mathbb{Z}_N$

1 Choose a small random integer r. $N = p \cdot q$
2 $p' = p \cdot r^2$
3 $i_{pr} = p^{-1} \mod r^2$
4 $M_p = M \mod p'$
5 $B_p = p \cdot i_{pr}$; $A_p = 1 - B_p \mod p'$
6 $M'_p = A_p \cdot M_p + B_p \cdot (1 + r) \mod p'$ // CRT insertion of verification value in M'_p

8 $S'_p = {M'_p}^{d_p} \mod \varphi(p') \mod p'$ // Intermediate signature in $\mathbb{Z}_{pr^2}$
9 $c_p = M'_p + N - M + 1 \mod p$
10 $S_{pr} = 1 + d_p \cdot r$ // Checksum in $\mathbb{Z}_{r^2}$ for S'_p
11 $q' = q \cdot r^2$
12 $i_{qr} = q^{-1} \mod r^2$
13 $M_q = M \mod q'$
14 $B_q = q \cdot i_{qr}$; $A_q = 1 - B_q \mod q'$
15 $M'_q = A_q \cdot M_q + B_q \cdot (1 + r) \mod q'$ // CRT insertion of verification value in M'_q

17 $S'_q = {M'_q}^{d_q} \mod \varphi(q') \mod q'$ // Intermediate signature in $\mathbb{Z}_{qr^2}$
18 $c_q = M'_q + N - M + 1 \mod q$
19 $S_{qr} = 1 + d_q \cdot r$ // Checksum in $\mathbb{Z}_{r^2}$ for S'_q

21 $S_r = S_{qr} + q \cdot (i_q \cdot (S_{pr} - S_{qr}) \mod p')$ // Recombination checksum in $\mathbb{Z}_{r^2}$
22 $S' = S'_q + q \cdot (i_q \cdot (S'_p - S'_q) \mod p')$ // Recombination in $\mathbb{Z}_{Nr^2}$
23 $c_S = S' - S_r + 1 \mod r^2$

25 **return** $S = S' c_p c_q c_S \mod N$ // Retrieve result in $\mathbb{Z}_N$

Problem #2 Gap btw test & evaluation

- Test: reproducible
- Evaluation: possibility to innovate, but outcome depends on the skill of the evaluator

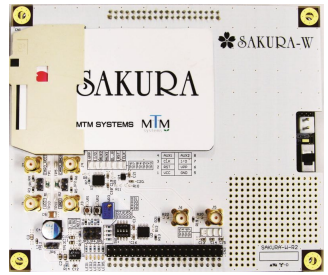
Test	*versus*	Evaluation
CMVP Conformance through Testing		Common Criteria
ISO/IEC 19790:2012		ISO/IEC 15408:2009

Problem #3 Education

Our discipline is not yet mainstream...

But let's mention those interesting dissemination activities:

- Liran Lerman: ..... R for SCA
- Elisabeth Oswald: ..... Matlab for SCA (OpenSCA)
- Guillaume Duc: ..... DPAcontest v4
- Akashi Satoh: ..... SASEBO + SAKURA



- Colin O'Flynn; ChipWhisperer

CHIP WHISPERER™
Listen to your Inner Hardware™

Problem #4 Heterogeneous community

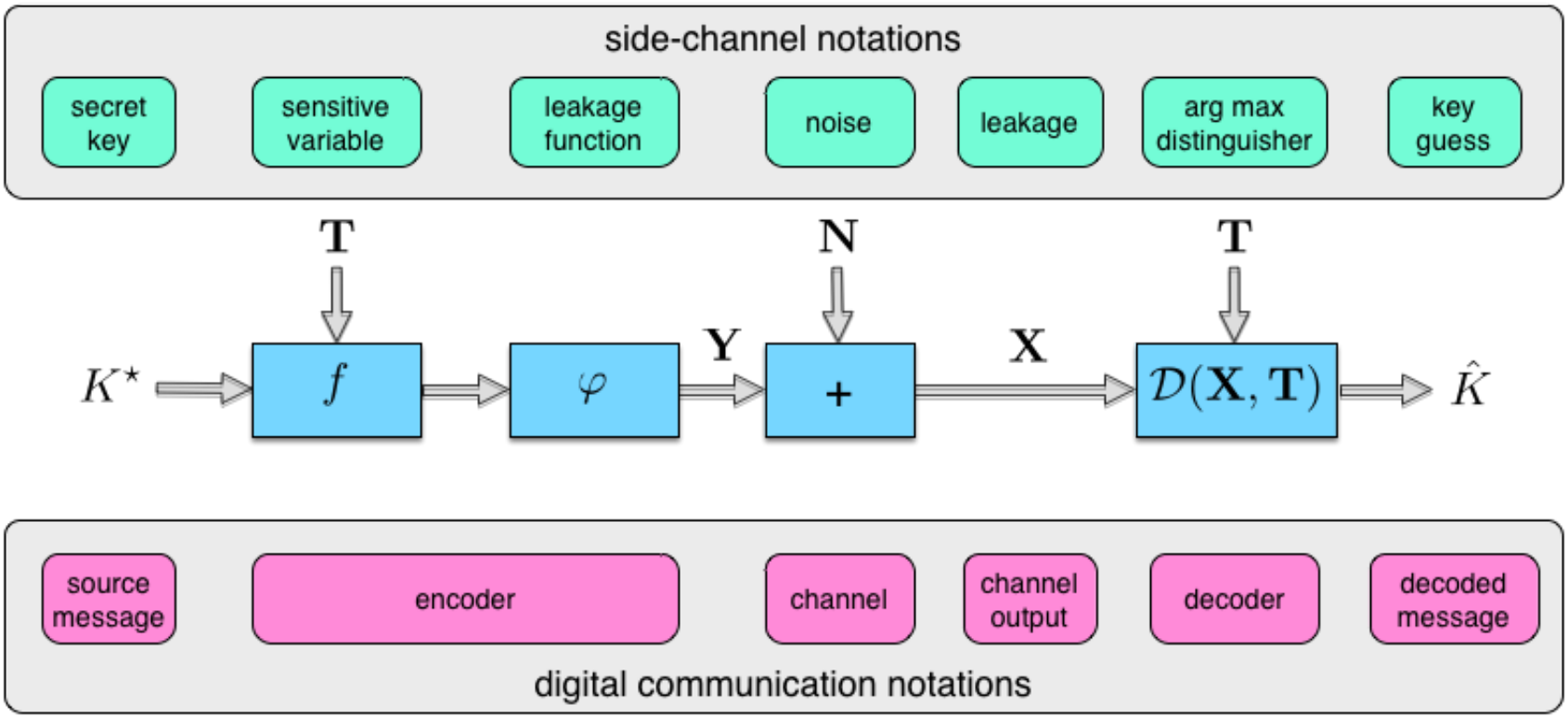
We are a mix of various *academic* & *technical* skills, in:

- Signal processing
- Stats
- Data analysis
- Crypto

Design & evaluation people do not often meet formally.

One example [HRG14]

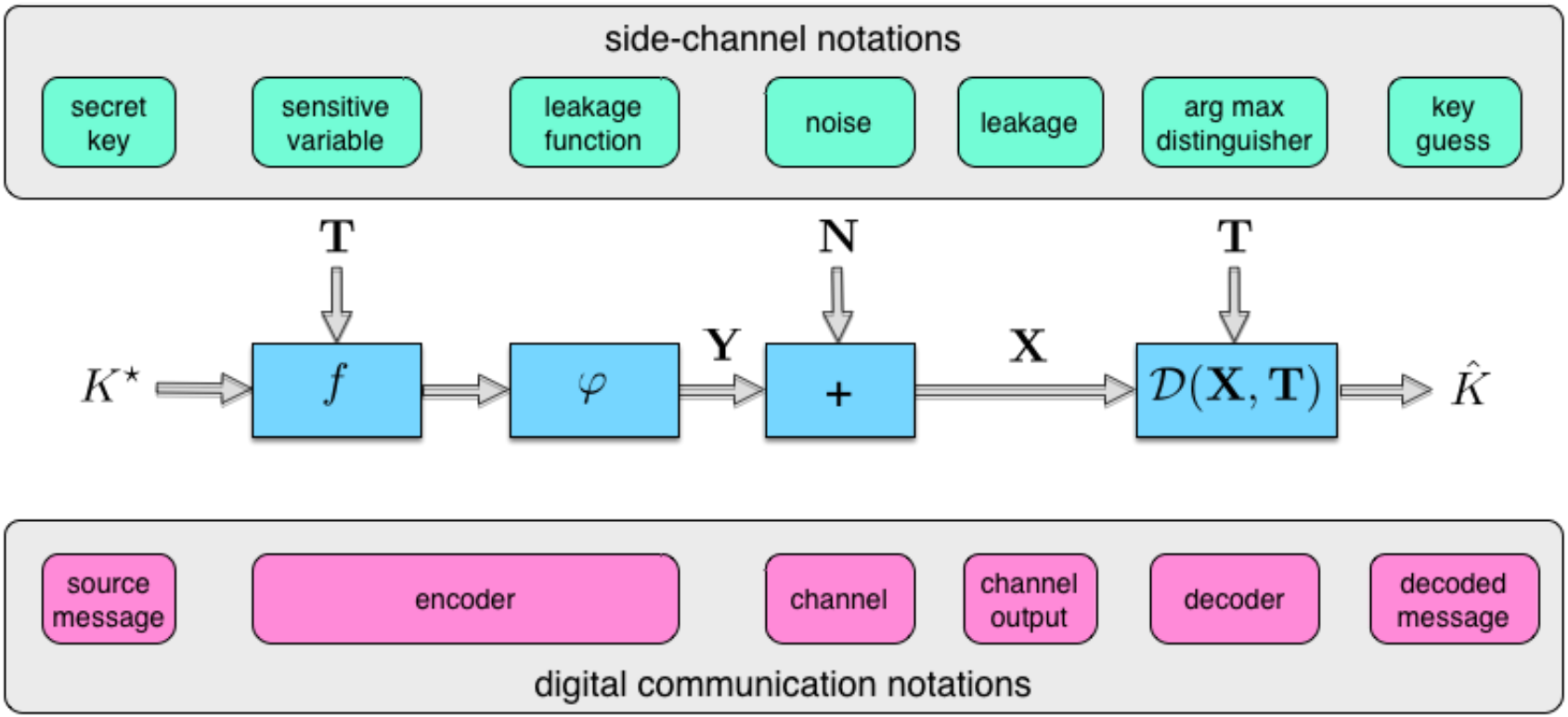
: Annelie Heuser, proficient in SCA



: Olivier Rioul, proficient in stats & info theory

One example [HRG14]

: Annelie Heuser, proficient in SCA

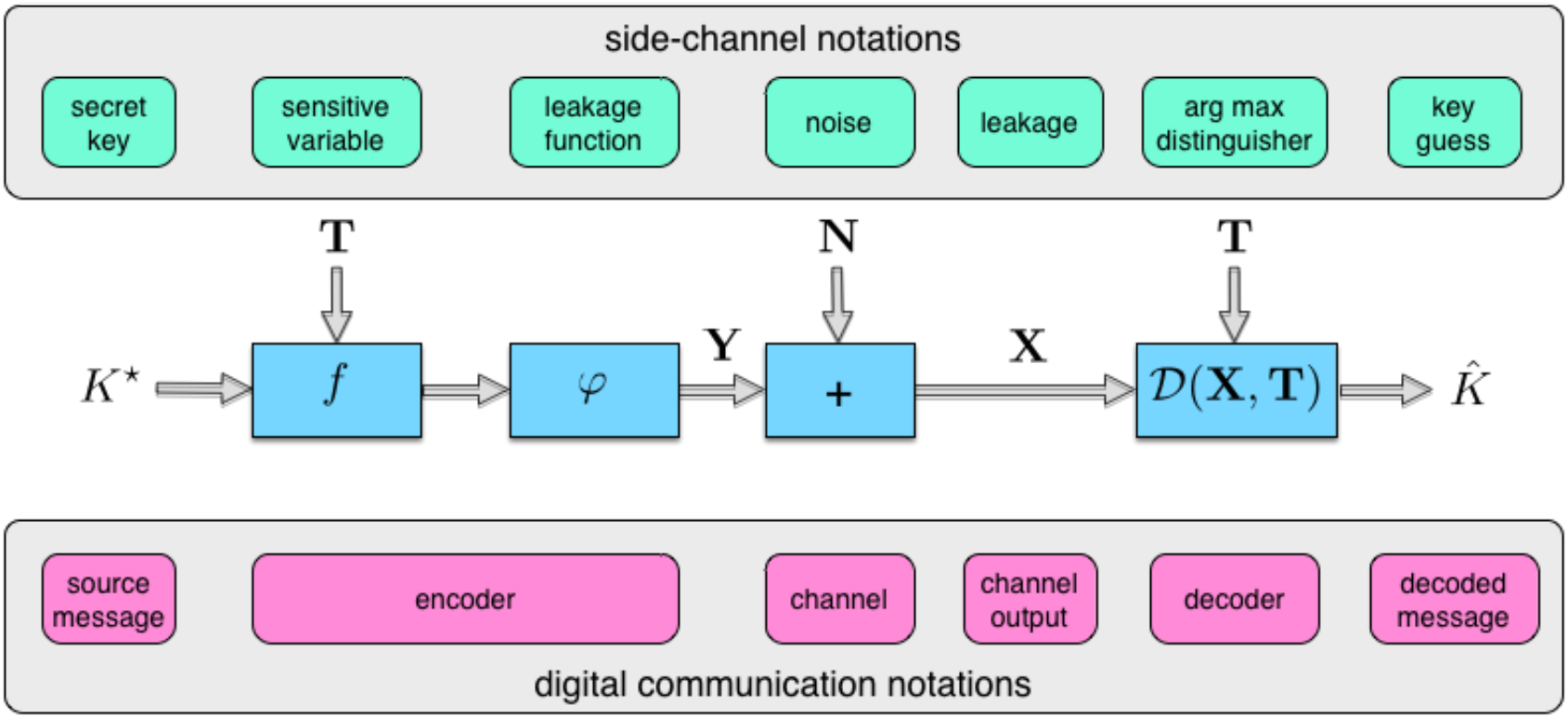


: Olivier Rioul, proficient in stats & info theory

→ CPA is the optimal attack in the affine stochastic setup... [HRG14]

One example [HRG14]

: Annelie Heuser, proficient in SCA

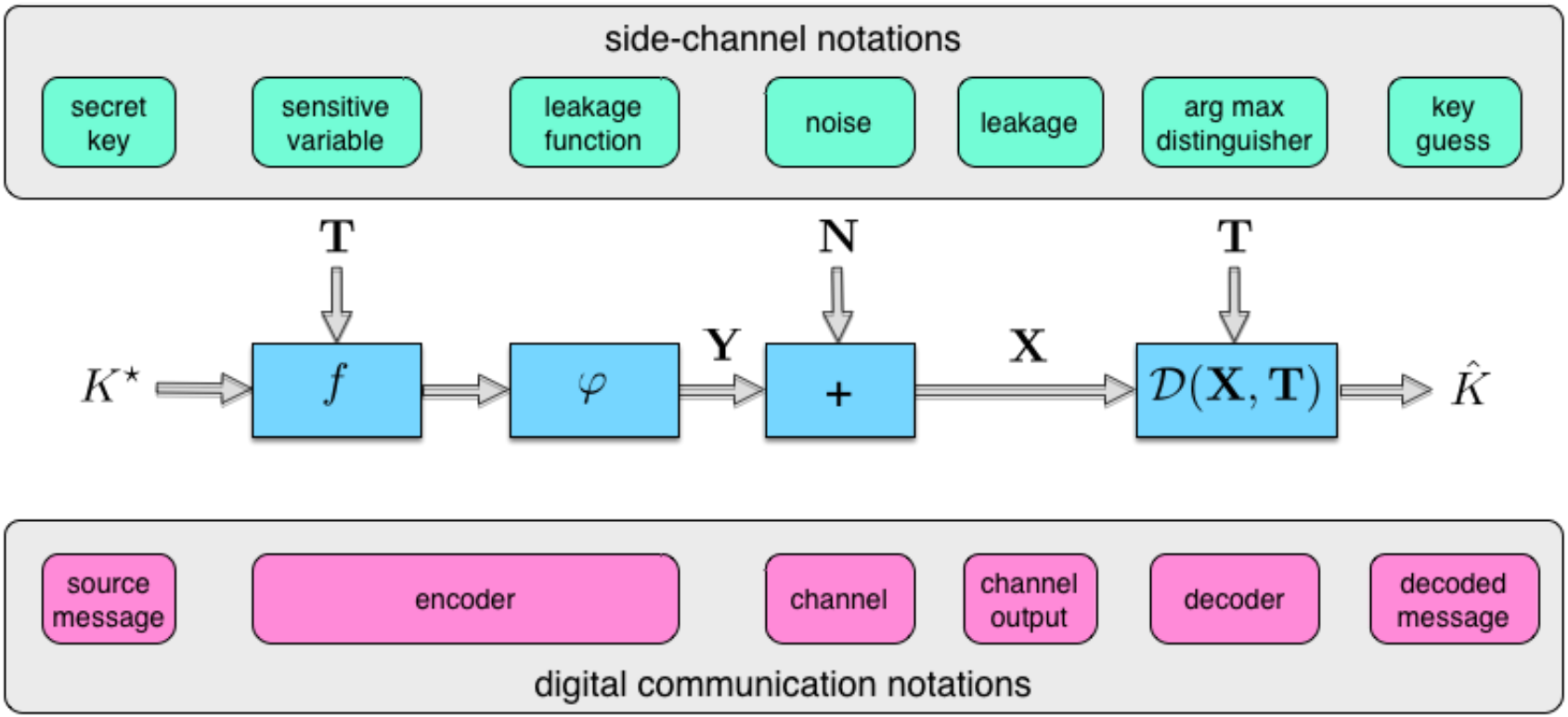


: Olivier Rioul, proficient in stats & info theory

→ HO-CPA is optimal in case of masking *and* high noise... [BGHR14]

One example [HRG14]

: Annelie Heuser, proficient in SCA



: Olivier Rioul, proficient in stats & info theory

→ Dimensionality reduction doesn't decrease success rate... [BGH+15]

Problem #5

Security as a whole

- Secure boot
- Key derivation and transport (whole life cycle)
- Faults & reverse-engineering attacks
- etc.

Standardization in embedded security

De facto

One example:

WORLD DEFACTO STANDARD for side-channl attack evaluation

SAKURA boards are **WORLD DEFACTO STANDARD** for side-channl attack evaluation because they are used as a substrate for evaluation in the DPA contest and the research area.

Consensus driven, in committees

- `ISO/IEC JTC 1/SC 27`: IT Security techniques
- `WG3`: Security evaluation, testing and specification

Standardization at ISO

Objective

- Agree on **common** definitions and methods
- For a **better** and **wider** development of technologies

How does it work?

- **ISO**: International Standard Organization (non profit)
- **Open** participation, through the "**national bodies**"
- Process: **Study Period** $\rightarrow$ **Work Item** $\rightarrow$ **Int'l Standard**

Current **study periods** → **NWIP**

PUF

- SC 27 N13700, "Physically Unclonable Functions for non-stored security parameter generation"
- Function, and performance figures

TRNG for RFID

- 20543, "Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408"
- Rapporteurs: FR, GE, USA.

Current **work items**

Calibration of non-invasive attack testing platforms

- 20085: Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules -
  - 20085-1: Part 1: Test tools and techniques
  - 20085-2: Part: 2 Test calibration methods and apparatus

$\Rightarrow$ To contribute, please contact your national body

- Next ISO meeting, Oct. 26–30, 2015, at Jaipur, INDIA.

BUREAU OF INDIAN STANDARDS

WG MEETINGS OF ISO/IEC JTC 1/SC 27

State-of-the-art of international standardisation of side-channel analysis test methodologies and calibration of acquisition tools

Sylvain GUILLEY
sylvain.guilley@TELECOM-ParisTech.fr

September 10, 2015, PARIS

[BGH+15] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, and Olivier Rioul.
Less is more - dimensionality reduction from a theoretical perspective.
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 22–41. Springer, 2015.

[BGHR14] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, and Olivier Rioul.
Masks Will Fall Off: Higher-Order Optimal Distinguishers.
In *ASIACRYPT*, volume 8874 of *LNCS*, pages 344–365. Springer, December 2014.
P. Sarkar and T. Iwata (Eds.): ASIACRYPT 2014, PART II.

[HRG14] Annelie Heuser, Olivier Rioul, and Sylvain Guilley.
Good Is Not Good Enough - Deriving Optimal Distinguishers from Communication Theory.
In 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*, pages 55–74. Springer, 2014.

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner.
Private Circuits: Securing Hardware against Probing Attacks.
In *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, August 17–21 2003.
Santa Barbara, California, USA.

[RBG+15] Debapriya Basu Roy, Shivam Bhasin, Sylvain Guilley, Jean-Luc Danger, and Debdeep Mukhopadhyay.
From Theory to Practice of Private Circuit: A Cautionary Note.
In *The 33rd IEEE International Conference on Computer Design (ICCD '15)*, October 18-21 2015.
New York City, USA.

Welcome to PROOFS '15

September 17, 2015, at Saint-Malo (France)