Randomness as countermeasures against Side Channel Attacks

Nadia El Mrabet

nadia.el-mrabet@emse.fr

Mines St Etienne

WRACH'2019, April 17, 2019

Presentation given here

Houssem Maghrebi, Underwriters Laboratories.

Deep Learning based Side Channel Attacks in Practice. See abstract

Damien Robissout, Université Jean Monnet de Saint-Etienne.

Improved Deep-Learning Side-Channel Attacks using Normalization laye

Ramtine Tofighi, Trusted Labs / Univ. Grenoble Alpes.

Using Machine Learning to defeat software protection.

Eleonora Cagli, Univ. Grenoble Alpes / CEA LETI.

Classifying Side-Channel desynchronized signals with convolutional neural ne

Annelie Heuser, CNRS IRISA.

Profiled side-channel analysis revisited. See abstract

Thomas Plantard, Univ. Wollongong.

SPA resistant Exponentiation based on Brun's GCD alg

Thomas Espitau, Sorbonne universite.

Physical Attacks on Lattice based Signat

Jean-Luc Danger and Sylvain Guilley, ENST/SecureIC.

Analysis of Mixed PUF-TRNG Circuit Based on SR-Latches in FD-SOI Technology. See abstract

Nicolas Bruneau, Sylvain Guilley and Adrien Facon, ENST/SecureIC.

Automatic derivation of optimal side-channel attacks rounded at a given order. See abstract

Timo Zijlstra, Karim Bigou and Arnaud Tisserand, Univ. Bretagne Sud.

Countermeasures against physical attacks on ring-LWE encryption schemes. See abstract

Philippe Elbaz-Vincent, Cyril Hugounenq and Sebastien Riou, Univ. Grenc

SPAE: An authenticated encryption algorithms for low-cost embedded systems

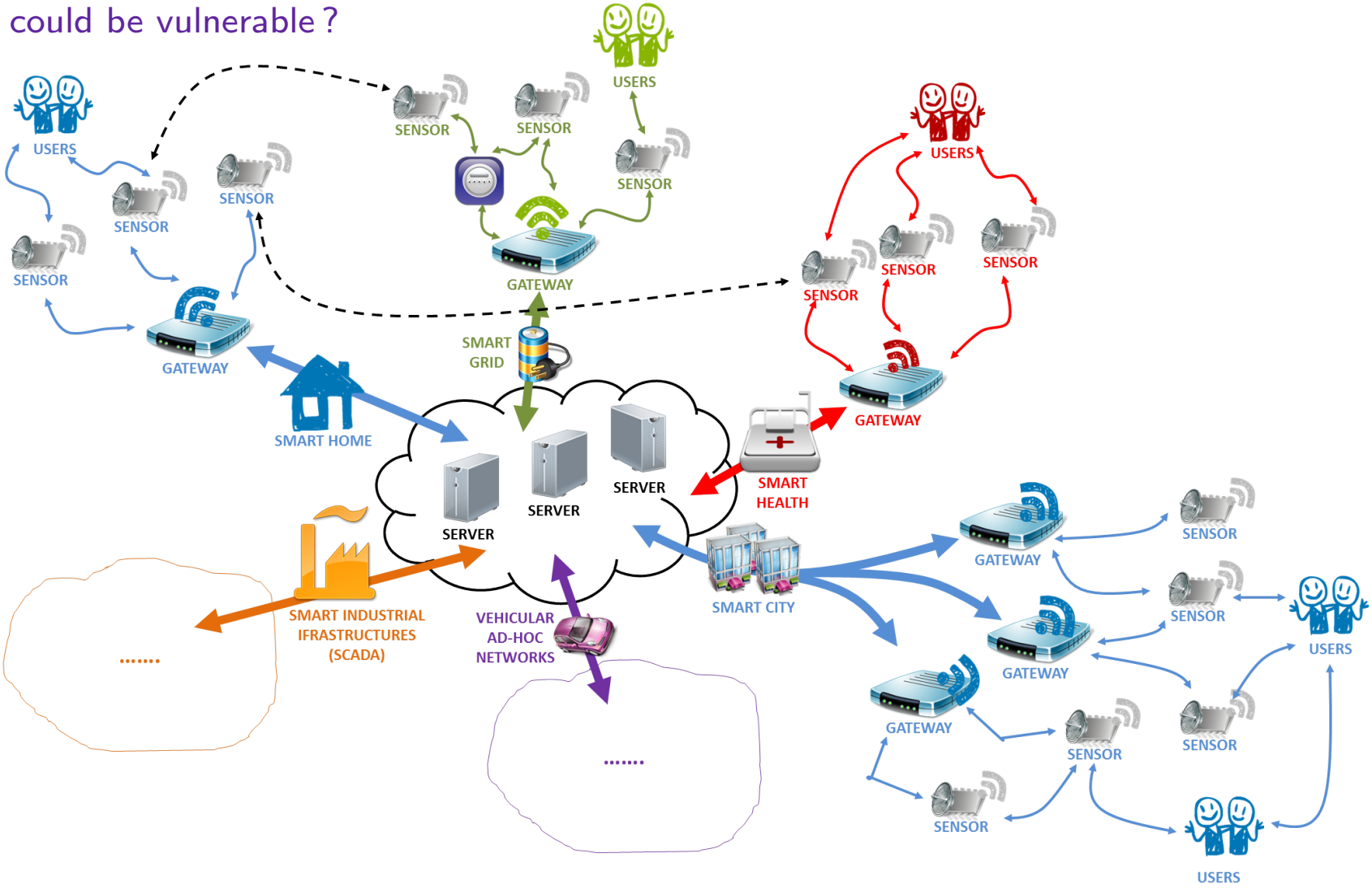
Titouan Coladon, Philippe Elbaz-Vincent and Cyril Hugounenq, Univ. Grenoble

MPHELL: a fast and robust library with unified arithmetic for elliptic curves cryptog

MINES Saint-Étienne

In real life

What could be vulnerable ?

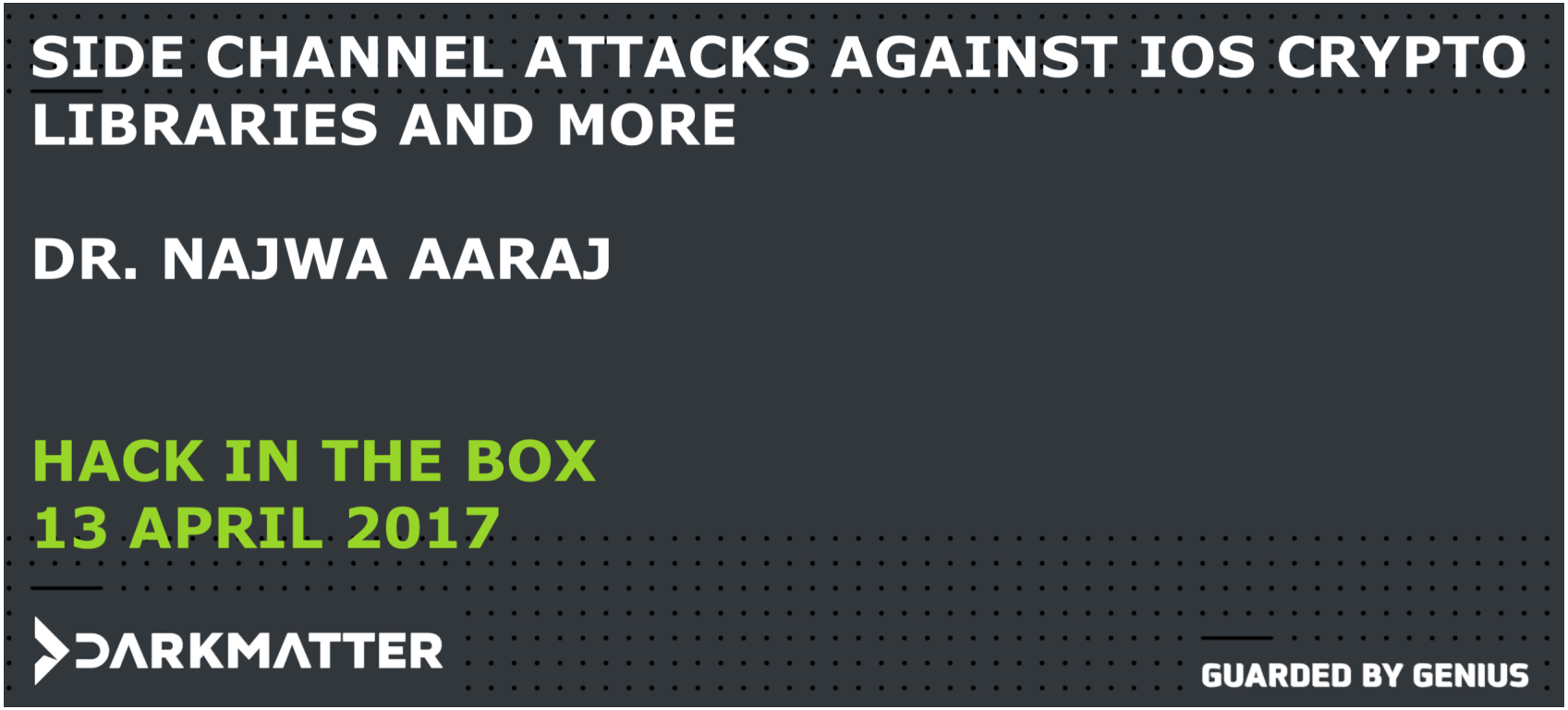


In real life

Existing attacks

In real life

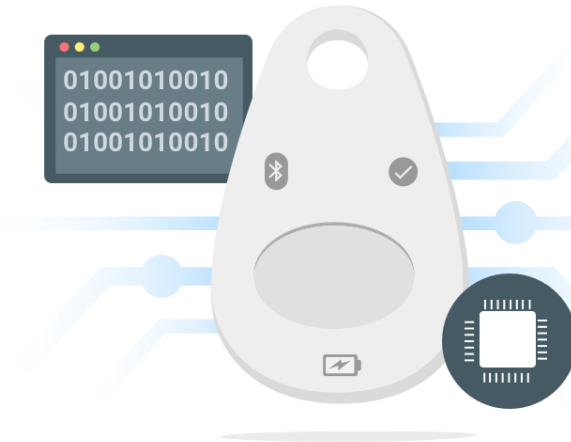
Existing attacks



In real life

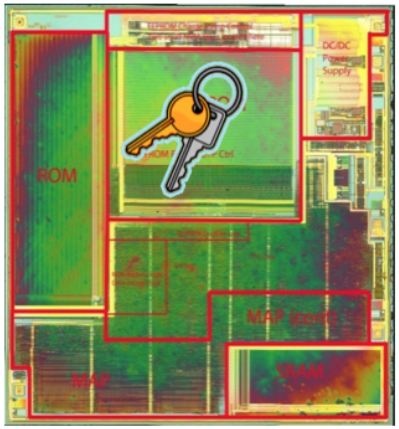
Un matériel de confiance

Les clés de sécurité Titan intègrent une puce matérielle incluant un micrologiciel conçu par Google qui valide l'intégrité de la clé. Cela permet de garantir que les clés n'ont pas été altérées.



- Industrials are building teams to protect their product (Apple, Google, Wawai...)

Attacks on Device



Cryptanalysis

Software attacks

Physical cryptanalysis

Combined attacks

Hardware attacks

Observation

Power
Electromagnetic emission
Duration of computation
Internal signal
Light, etc.

Inspection

Imaging
Retro- engineering

Perturbation

Under/over powering
Over clocking
Temperature
Electromagnetic
Laser, etc.

The most important point

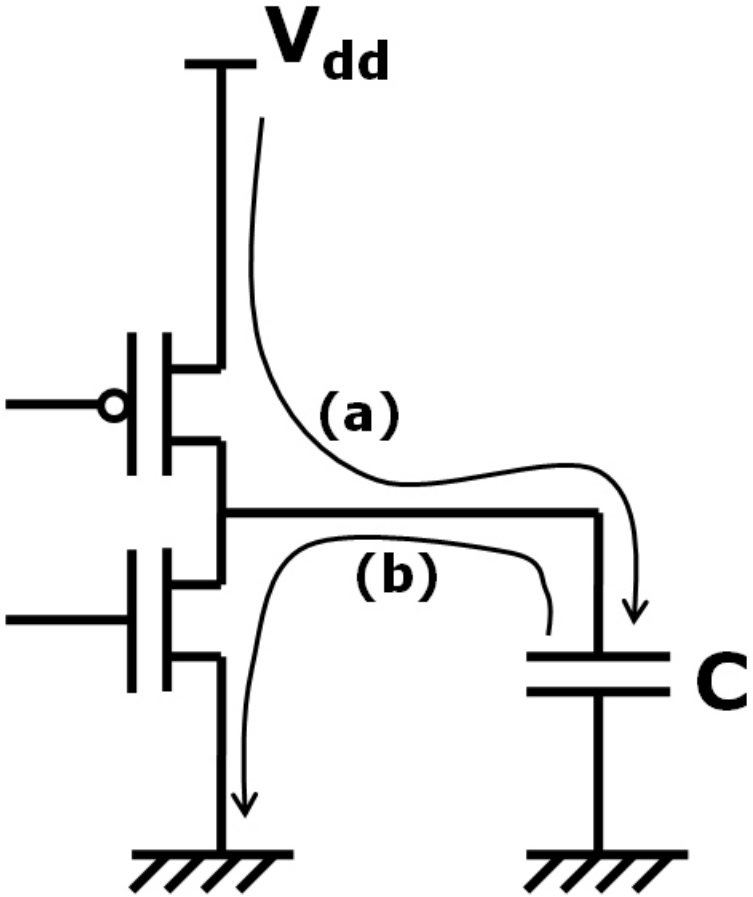


Figure – High level explanation of SCA

The most important point

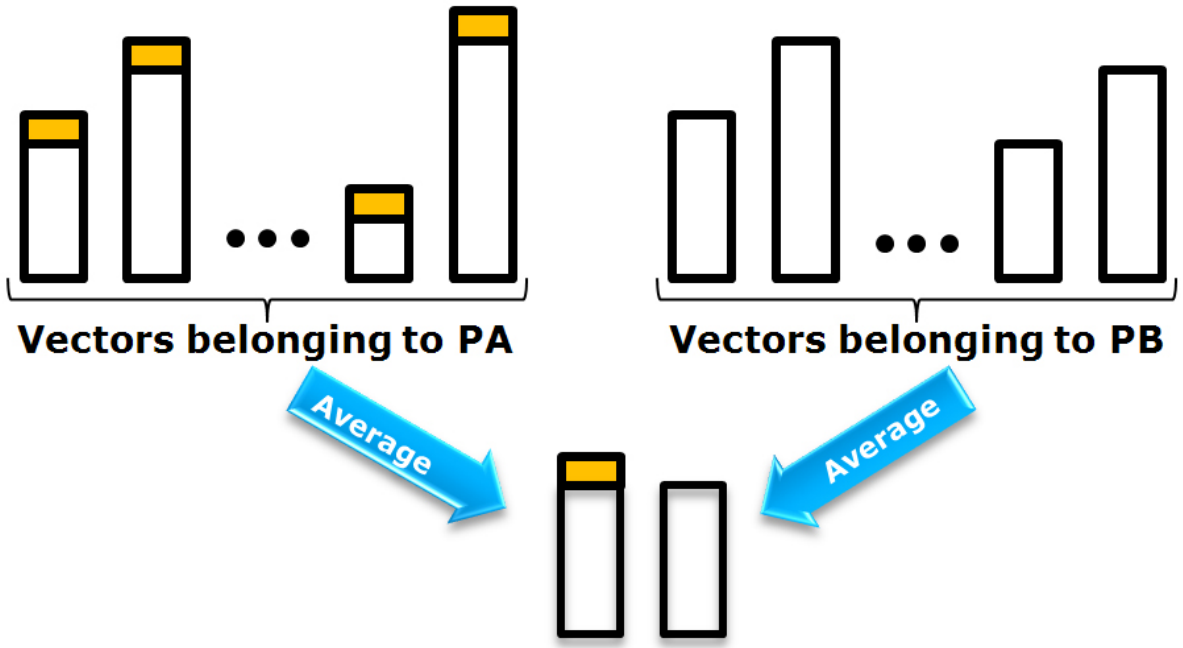


Figure – Selection according to guesses on the key

The most important point

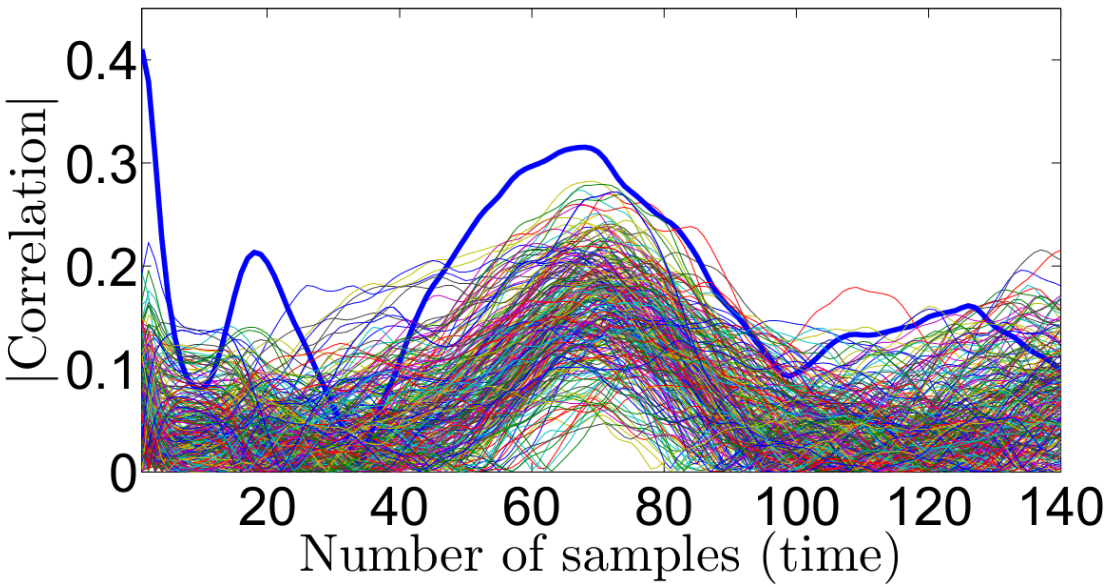


Figure – Real curve attack

The Countermeasures

- Physical

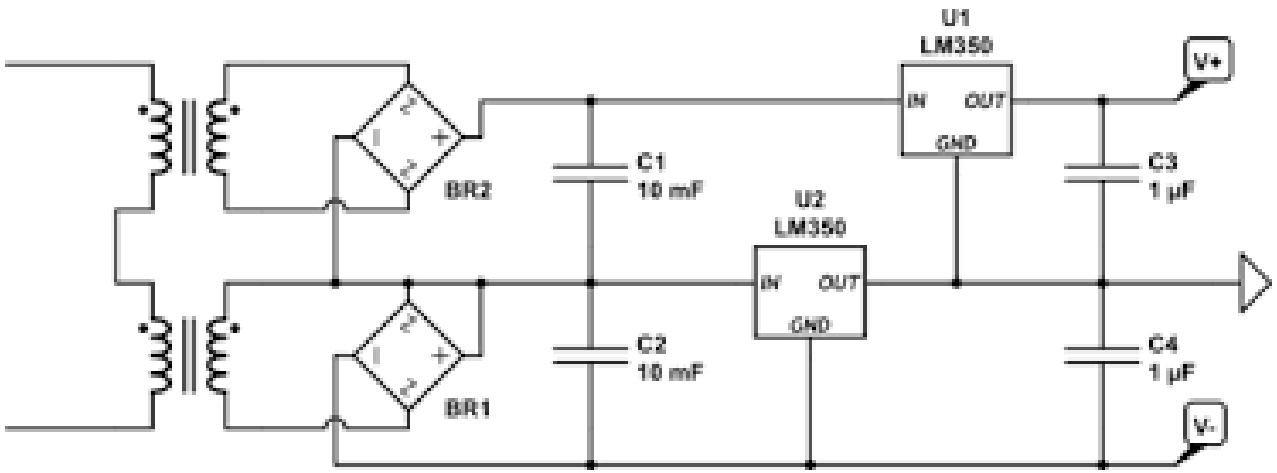
The Countermeasures

- Physical
- Algorithmic
- Arithmetical

Physical countermeasures

Duplication of the circuit

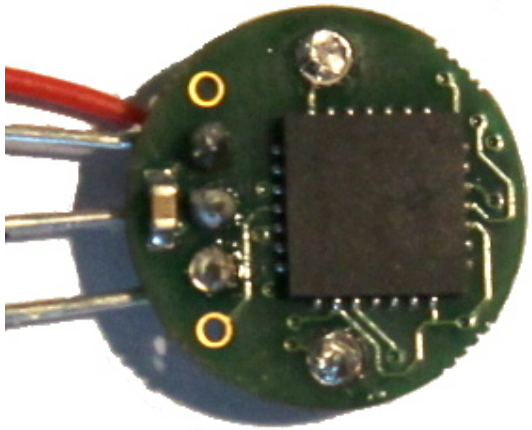
Dual rail technology



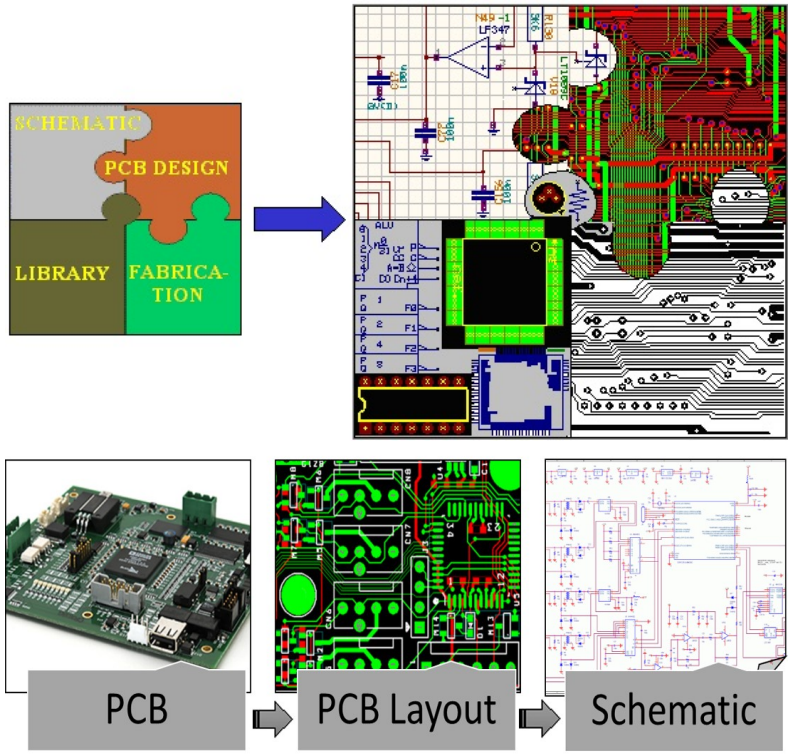
Physical countermeasures

Protection of the circuit

Shield



Randomisation of the circuit



First arithmetical countermeasures

Double and add algorithm

Data: $r = (r_N \dots r_0)_2$, $P \in E$
Result: rP
$T \leftarrow P$;
for $i = N - 1$ **to** 0 **do**
  $T \leftarrow [2]T$;
  if $r_i = 1$ **then**
    $T \leftarrow T + P$;
  end
end
return $T = [r]P$
Algorithm 1: Double and add

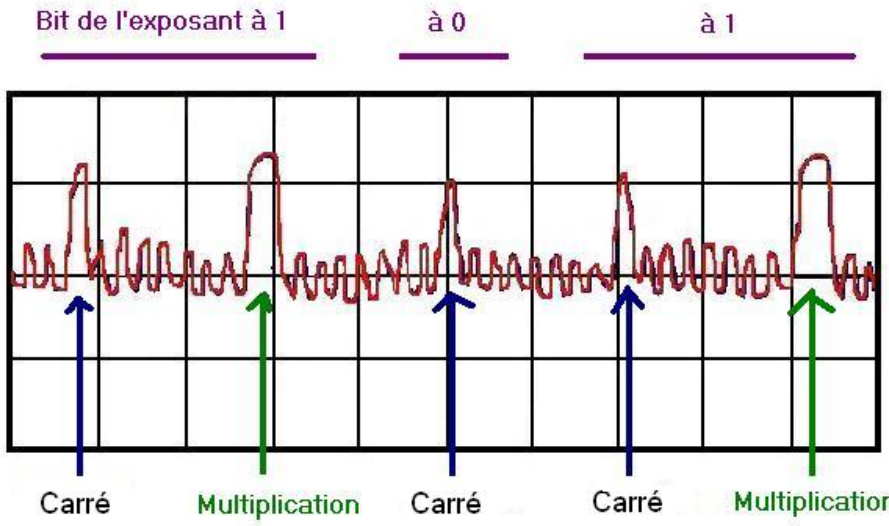


Figure – SPA

First arithmetical countermeasures

Handle the leakages

$T \leftarrow P$;
for $i = N - 1$ **to** 0 **do**
  $T \leftarrow 2T$;
  if $r_i = 1$ **then**
    $T \leftarrow T + P$;
  else $U \leftarrow T + P$;
end
return $T = rP$

Algorithm 2: Double and add always

First arithmetical countermeasures

Handle the leakages

$T \leftarrow P$;
for $i = N - 1$ **to** 0 **do**
  $T \leftarrow 2T$;
  if $r_i = 1$ **then**
    $T \leftarrow T + P$;
  else $U \leftarrow T + P$;
end
return $T = rP$

Algorithm 4: Double and add always

FAULT ATTACK STRIKES

First arithmetical countermeasures

Handle the leakages

$T \leftarrow P$;
for $i = N - 1$ **to** 0 **do**
  $T \leftarrow 2T$;
  if $r_i = 1$ **then**
    $T \leftarrow T + P$;
  else $U \leftarrow T + P$;
end
return $T = rP$

Algorithm 6: Double and add always

FAULT ATTACK STRIKES

$T_0 \leftarrow P, T_1 \leftarrow 2P$;
for $i = N - 1$ **to** 0 **do**
  if $r_i = 1$ **then**
    $T_0 \leftarrow T_0 + T_1, T_1 \leftarrow 2T_1$
  else
    $T_1 \leftarrow T_0 + T_1, T_0 \leftarrow 2T_0$
  end
end
return T_0

Algorithm 7: Montgomery ladder

MINES Saint-Étienne

First arithmetical countermeasures

The Montgomery ladder is not sufficient

- Goubin's attack : uses a special point (several variants, same method).
- Walter's attack : uses leakage from the conditional branch.
- Correlation collision attack (vertical and horizontal).

  Template, deep learning attacks...

Generic protection

- Constant time implementation : necessary but not sufficient.
- The less conditional branches is the better.

MINES Saint-Étienne

First arithmetical countermeasures

Behind Montgomery ladder

- Joye's double-add
- Add-Only
- Square Only (Remember Thomas presentation)
- Zero-less signed digit expansion
- Atomic block

First arithmetical countermeasures

Behind Montgomery ladder

- Joye's double-add [Still safe]
- Add-Only [Correlation collision attacks]
- Square Only (Remember Thomas presentation) [Correlation collision attacks]
- Zero-less signed digit expansion [Still safe]
- Atomic block [Horizontal correlation collision attacks]

The property of the cryptosystem

ECC : representation of the curve

- Edwards curves, inverted Edwards curves
- Huff model, Hessian curves
- Jacobi curves

MINES Saint-Étienne

The property of the cryptosystem

ECC : representation of the curve

- Edwards curves, inverted Edwards curves [Template attacks]
- Huff model, Hessian curves
- Jacobi curves

MINES Saint-Étienne

The property of the cryptosystem

ECC : representation of the curve

- Edwards curves, inverted Edwards curves [Template attacks]
- Huff model, Hessian curves
- Jacobi curves

ECC : representation of the points

- Unified formulaes for Weieirstrass

$\Rightarrow$ Goubin's, Izu-Takagi's attacks (special point)

$\Rightarrow$ Amiel et al's attack : uses SCA to distinguish a S from a M

$\Rightarrow$ Horizontal attacks

MINES Saint-Étienne

The property of the cryptosystem

ECC : randomisation of the scalar

- Coron's countermeasure
- Exponentiation splitting
- Trichina-Bellezza's countermeasure : $kP = (kr^{-1})rP$
- Regular representation of the scalar
- Euclidien chain (Remember Christophe, Jean-Marc, Nicolas presentations)
- Chevallier-Mames Self-Randomised Exponentiation

MINES Saint-Étienne

The property of the cryptosystem

ECC : randomisation of the scalar

- Coron's countermeasure [Big attack]
- Exponentiation splitting [Big Mac attack]
- Trichina-Bellezza's countermeasure : $kP = (kr^{-1})rP$ [Still safe]
- Regular representation of the scalar [Correlation collision attacks]
- Euclidien chain (Remember Christophe, Jean-Marc, Nicolas presentations) [Big Mac attack]
- Chevallier-Mames Self-Randomised Exponentiation [Still safe]

MINES Saint-Étienne

The property of the cryptosystem

ECC : randomisation of the scalar

- Coron's countermeasure [Big attack]
- Exponentiation splitting [Big Mac attack]
- Trichina-Bellezza's countermeasure : $kP = (kr^{-1})rP$ [Still safe]
- Regular representation of the scalar [Correlation collision attacks]
- Euclidien chain (Remember Christophe, Jean-Marc, Nicolas presentations) [Big Mac attack]
- Chevallier-Mames Self-Randomised Exponentiation [Still safe]

ECC : A lot of counter measures, but much more attacks !

MINES Saint-Étienne

The property of the cryptosystem

Pairing based cryptography

- Bilinear function, non degenerate.
- Very great for key schedule, hierarchical encryption, several signatures schemes...
- Natively sensitive to SCA.
- Counter measures for ECC can be used.
- $e(P, Q) = e(aP, bQ)$, for a and b such that $ab = 1 \mod r$.
- $$e(P, Q) = \frac{e(P + R, Q)}{e(R, Q)}.$$

The property of the cryptosystem

AES

Masking and masking or masking

The graal

White box cryptography

- The method is somehow an obfuscation of the algorithm.
- There is a contest organized within CHES.
- As far as I know, no resistant scheme is existing.
- I see one major drawback : the contradiction with Kerchoffs rules.
- Luca will maybe find a nice asymmetric protocole.

MINES Saint-Étienne

Random multiplication flow

- For a given protocol, the instruction flow for the multiplication is different for each product.
- Somewhat, it comes back to a random circuit for each device.
- Could be resistant to reverse engineering,
- BUT very hard to deploy in practice.
- There is no guarantee that it would resist to SCA.

MINES Saint-Étienne

Randomisation of the representation

Projectives coordinates for ECC

Let P be a point of an elliptic curve E, λ a scalar then we have

$$(X_P, Y_P, Z_P) = (\lambda X_P, \lambda Y_P, \lambda Z_P).$$

MINES Saint-Étienne

Randomisation of the representation

Projectives coordinates for ECC

Let P be a point of an elliptic curve E, λ a scalar then we have

$$(X_P, Y_P, Z_P) = (\lambda X_P, \lambda Y_P, \lambda Z_P).$$

$\Rightarrow$ Special point attacks

Figure – Big Mac attack

Randomisation of the arithmetic

Smart-Oswald-Page randomised representation

Instead of working modulo m within the range $\{0, \ldots, m-1\}$ you work modulo $C = c \times m$, for c a coprime integer to m in the range $\{0, \ldots, C-1\}$.

The ultimate solution

Randomisation of the arithmetic

PMNS : the ultimate solution

- $a \in \mathbb{F}_p$, $a = \sum_0^n a_i \gamma^i$ for a given γ and $a_i \leq \rho$.
- This representation is highly redondant, a admits ρ^{n-1} representations.
- PMNS allows efficient arithmetic over $\mathbb{F}_p$ and extensions of $\mathbb{F}_p$, where p is a prime number.

MINES Saint-Étienne

Randomisation of the arithmetic

PMNS : the ultimate solution

- $a \in \mathbb{F}_p$, $a = \sum_0^n a_i \gamma^i$ for a given γ and $a_i \leq \rho$.
- This representation is highly redondant, a admits ρ^{n-1} representations.
- PMNS allows efficient arithmetic over $\mathbb{F}_p$ and extensions of $\mathbb{F}_p$, where p is a prime number.
- In "Randomization of Arithmetic over Polynomial Modular Number System" with Didier, Dosser, Marrez and Véron :
- we defined a random expression in PMNS ;
- we defined a random multiplication in $\mathbb{F}_p$ based on PMNS.
- For the description of our work pay attention to the two following presentations by Yssouf Dosso and Jérémie Marrez ! !

MINES Saint-Étienne