Une approche spectrale pour l'analyse de corrélation sur la consommation

BRANDON DRAVIE
Centre de Recherche en Automatique de Nancy (CRAN)

Supervisor	:	GILLES MILLERIOUX
Co-supervisor	:	PHILIPPE GUILLOT

Crypto'Puces 2017

29 *Mai* – 2 *Juin* 2017

Introduction

Side Channel Attack

When running an electronic device, it emits signals due to power consumption or waves due to electromagnetic radiations.

Observe and exploit these emanations can help to extract informations within the device at a precise running time.

Introduction

Side Channel Attack

When running an electronic device, it emits signals due to power consumption or waves due to electromagnetic radiations.

Observe and exploit these emanations can help to extract informations within the device at a precise running time.

A cryptographic device (smart card, FPGA device...) performs operations on secret data that are hold inside the circuit of the devices:

- running the cryptographic algorithm $\Longrightarrow$ physical emanations or leakage due to functions that operate on secret data (ex. non-linear function)
- exploiting physical leakage $\Longrightarrow$ physical attacks that reveal the secret data

This kind of attack is called Side Channel Attack or SCA for short.

Contents

Table of contents

Correlation Power Analysis (CPA)

Side Channel Attack

- Simple Power Analysis (SPA) [Koc96]
- Differential Power Analysis [PJB99]
- Correlation Power Analysis (CPA) [BCO04]

Correlation Power Analysis (CPA)

Side Channel Attack

- Simple Power Analysis (SPA) [Koc96]
- Differential Power Analysis [PJB99]
- Correlation Power Analysis (CPA) [BCO04]

Test Bench:

- smart card (containing the cryptographic algorithm to attack)
- oscilloscope (to perform measurement when the smart card is working)
- Personal Computer (to drive the smart card and the oscilloscope).

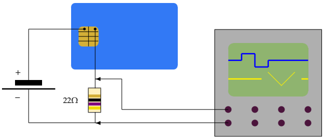


Figure : Test bench.

Correlation Power Analysis

A CPA establishes correlation between :

- real power consumption values obtained by measuring the power consumption when running the smart card

  and

- hypothetical power consumption values obtained from a leakage model.

Table of contents

Function on binary words

$\varphi : \{0,1\}^n \mapsto \mathbb{R}$: Function on binary words. $\Phi = \{\varphi : \{0,1\}^n \to \mathbb{R}\}$

Scalar product

$\varphi, \psi \in \Phi$:

$$\langle \varphi, \psi \rangle = \sum_{x \in \{0,1\}^n} \varphi(x)\psi(x).$$

Norm

$$\|\varphi\| = \sqrt{\langle \varphi, \varphi \rangle} = \sqrt{\sum_{x \in \{0,1\}^n} \varphi(x)^2}$$

The norm of $\varphi \in \Phi$ is called energy of φ.

Function on binary words

$\varphi : \{0,1\}^n \mapsto \mathbb{R}$: Function on binary words. $\Phi = \{\varphi : \{0,1\}^n \to \mathbb{R}\}$

Scalar product

$\varphi, \psi \in \Phi$:

$$\langle \varphi, \psi \rangle = \sum_{x \in \{0,1\}^n} \varphi(x)\psi(x).$$

Norm

$$\|\varphi\| = \sqrt{\langle \varphi, \varphi \rangle} = \sqrt{\sum_{x \in \{0,1\}^n} \varphi(x)^2}$$

The norm of $\varphi \in \Phi$ is called energy of φ.

Fourier Transform

$$\begin{array}{rccl} \widehat{\varphi}(u) : & \{0,1\}^n & \mapsto & \mathbb{R} \\ & u & \mapsto & \widehat{\varphi}(u) = \dfrac{1}{\sqrt{2^n}} \displaystyle\sum_{x \in \{0,1\}^n} \varphi(x)(-1)^{u \cdot x} \end{array}$$

Function on binary words

$\varphi : \{0,1\}^n \mapsto \mathbb{R}$: Function on binary words. $\Phi = \{\varphi : \{0,1\}^n \to \mathbb{R}\}$

Scalar product

$\varphi, \psi \in \Phi$:

$$\langle \varphi, \psi \rangle = \sum_{x \in \{0,1\}^n} \varphi(x)\psi(x).$$

Norm

$$\|\varphi\| = \sqrt{\langle \varphi, \varphi \rangle} = \sqrt{\sum_{x \in \{0,1\}^n} \varphi(x)^2}$$

The norm of $\varphi \in \Phi$ is called energy of φ.

Fourier Transform

$$\begin{array}{rccl} \widehat{\varphi}(u) : & \{0,1\}^n & \mapsto & \mathbb{R} \\ & u & \mapsto & \widehat{\varphi}(u) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \varphi(x)(-1)^{u \cdot x} \end{array}$$

Isometry of Fourier Transform

$$\langle \varphi, \psi \rangle = \langle \widehat{\varphi}, \widehat{\psi} \rangle.$$

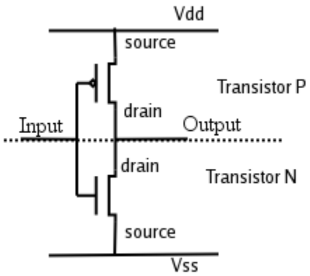
Energy conservation law

$$\|\varphi\| = \|\widehat{\varphi}\|$$

Table of contents

Physical principles

Circuit CMOS (Complemantary Metal-Oxyde Semiconductor):



Hypothesis

The power consumption of a CMOS circuit is proportional to the number of logic gates that switch.

Target of the attack

The target of the CPA attack is an S-Box function implemented as Look Up Table (LUT) in the circuitry of the device.

S-Boxes performed essentially non-linear operations of the encryption algorithm.

S-Box

$$f : \{0,1\}^n \mapsto \{0,1\}^m$$

it computes a quantity (within the cryptographic device)

$$y = f(x + k^\star)$$

where x is a known value (by the adversary) and $k^\star$ is an unknown value (by the adversary)

$\Longrightarrow$ aim of the CPA attack on the S-Box: recover the value $k^\star$.

Example $n = m = 4$, $f : \{0,1\}^4 \mapsto \{0,1\}^4$

0	1	9	14	13	11	7	6	15	2	12	5	10	4	3	8

Leakage model and estimation of the power consumption φ

Leakage model (Hamming weight)

$$\varphi(x) = \mathrm{WH}(f(x+k^\star)) + \varepsilon(x) + C$$

$$\varphi(x) = \sum_{i=1}^{m} f_i(x+k^\star) + \varepsilon(x) + C \qquad (1)$$

- $\sum_{i=1}^{m} f_i(x+k^\star)$ is the Hamming weight of f
- $\varepsilon(x)$ is a random noise that depends on x
- C is a constant related to the power consumption of the smart card that does not depend on the value x.

Leakage model and estimation of the power consumption φ

Leakage model (Hamming weight)

$$\varphi(x) = \mathrm{WH}(f(x+k^\star)) + \varepsilon(x) + C$$

$$\varphi(x) = \sum_{i=1}^{m} f_i(x+k^\star) + \varepsilon(x) + C \qquad (1)$$

- $\sum_{i=1}^{m} f_i(x+k^\star)$ is the Hamming weight of f
- $\varepsilon(x)$ is a random noise that depends on x
- C is a constant related to the power consumption of the smart card that does not depend on the value x.

The adversary needs to guess the value of $k^\star$ and then assume a value k that is not equal to $k^\star$.
For this value k (with $g(x+k) = \sum_{i=1}^{m} f_i(x+k)$:= power consumption model):

$$\varepsilon_k(x) = \varphi(x) - g(x+k) - C. \qquad (2)$$

Leakage model and estimation of the power consumption φ

Leakage model (Hamming weight)

$$\varphi(x) = \mathrm{WH}(f(x+k^\star)) + \varepsilon(x) + C$$

$$\varphi(x) = \sum_{i=1}^{m} f_i(x+k^\star) + \varepsilon(x) + C \qquad (1)$$

- $\sum_{i=1}^{m} f_i(x+k^\star)$ is the Hamming weight of f
- $\varepsilon(x)$ is a random noise that depends on x
- C is a constant related to the power consumption of the smart card that does not depend on the value x.

The adversary needs to guess the value of $k^\star$ and then assume a value k that is not equal to $k^\star$.
For this value k (with $g(x+k) = \sum_{i=1}^{m} f_i(x+k)$:= power consumption model):

$$\varepsilon_k(x) = \varphi(x) - g(x+k) - C. \qquad (2)$$

likelihood value of $k^\star$

The value of $k^\star$ is the value of k for which the energy of the noise ε_k is minimal:

$$k = k^\star \Leftrightarrow \|\varepsilon_k(x)\| \text{ minimal for } k$$

Steps of the CPA attack

Let f an S-Box of the encryption algorithm. The CPA attack is performed in 3 steps:

Steps of the CPA attack

Let f an S-Box of the encryption algorithm. The CPA attack is performed in 3 steps:

1. choose the values of x and run the algorithm that computes $y = f(x + k^{\star})$

Steps of the CPA attack

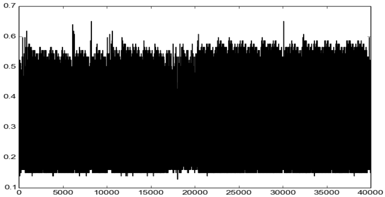
Let f an S-Box of the encryption algorithm. The CPA attack is performed in 3 steps:

1. choose the values of x and run the algorithm that computes $y = f(x + k^{\star})$
2. measure and record power consumption values denoted by φ:
   - for all value of x is associated a power consumption curve called a trace
   - each trace admits a number NBSAMPLES of samples where each sample corresponds to a power consumption at a given time t of the execution time of the algorithm

Steps of the CPA attack

Let f an S-Box of the encryption algorithm. The CPA attack is performed in 3 steps:

1. choose the values of x and run the algorithm that computes $y = f(x + k^{\star})$
2. measure and record power consumption values denoted by φ:
   - for all value of x is associated a power consumption curve called a trace
   - each trace admits a number NBSAMPLES of samples where each sample corresponds to a power consumption at a given time t of the execution time of the algorithm



Steps of the CPA attack

Let f an S-Box of the encryption algorithm. The CPA attack is performed in 3 steps:

1. choose the values of x and run the algorithm that computes $y = f(x + k^\star)$
2. measure and record power consumption values denoted by φ:
    - for all value of x is associated a power consumption curve called a trace
    - each trace admits a number NBSAMPLES of samples where each sample corresponds to a power consumption at a given time t of the execution time of the algorithm
3. analyse the traces by applying Fourier transform to find the probable value of $k^\star$

Estimation of the likelihood value of $k^\star$

Energy conservation law $\Longrightarrow$ $\|\varepsilon_k\| = \|\widehat{\varepsilon_k}\| = \sqrt{\sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2} = E(k)$

find $k^\star$ $\Longrightarrow$ find $\arg\min_k \sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2 = \arg\min_k E(k)^2$

Estimation of the likelihood value of $k^\star$

Energy conservation law $\Longrightarrow$ $\|\varepsilon_k\| = \|\widehat{\varepsilon_k}\| = \sqrt{\sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2} = E(k)$

find $k^\star$ $\Longrightarrow$ find $\arg\min_k \sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2 = \arg\min_k E(k)^2$

$$\text{Equation (2)} \Rightarrow \qquad \widehat{\varepsilon_k}(u) = \widehat{\varphi_t}(u) - (-1)^{u\cdot k}\widehat{g}(u) - C\sqrt{2^n}\delta_0(u). \tag{3}$$

The constant value C can be discarded by considering the functions:

$$\widehat{\varphi_t^\star}(u) = \begin{cases} \widehat{\varphi_t}(u) & \text{if } u \neq 0 \\ 0 & \text{else} \end{cases} \text{ and } \widehat{g}^\star(u) = \begin{cases} \widehat{g}(u) & \text{if } u \neq 0 \\ 0 & \text{else} \end{cases} \tag{4}$$

Estimation of the likelihood value of $k^\star$

Energy conservation law $\Longrightarrow \|\varepsilon_k\| = \|\widehat{\varepsilon_k}\| = \sqrt{\sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2} = E(k)$

find $k^\star \Longrightarrow$ find $\arg\min_k \sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2 = \arg\min_k E(k)^2$

$$\text{Equation (2)} \Rightarrow \qquad \widehat{\varepsilon_k}(u) = \widehat{\varphi_t}(u) - (-1)^{u\cdot k}\widehat{g}(u) - C\sqrt{2^n}\delta_0(u). \tag{3}$$

The constant value C can be discarded by considering the functions:

$$\widehat{\varphi_t^\star}(u) = \begin{cases} \widehat{\varphi_t}(u) & \text{if } u \neq 0 \\ 0 & \text{else} \end{cases} \text{ and } \widehat{g}^\star(u) = \begin{cases} \widehat{g}(u) & \text{if } u \neq 0 \\ 0 & \text{else} \end{cases} \tag{4}$$

$$E(k)^2 = \sum_{u\in\{0,1\}^n} \widehat{\varphi_t^\star}(u)^2 + \sum_{u\in\{0,1\}^n} \widehat{g}^\star(u)^2 - 2\sum_{u\in\{0,1\}^n} \widehat{\varphi_t^\star}(u)\widehat{g}^\star(u)(-1)^{u\cdot k} \tag{5}$$

Estimation of the likelihood value of $k^\star$

Energy conservation law $\Longrightarrow \|\varepsilon_k\| = \|\widehat{\varepsilon_k}\| = \sqrt{\sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2} = E(k)$

find $k^\star \Longrightarrow$ find $\arg\min_k \sum_{u\in\{0,1\}^n} \widehat{\varepsilon_k}(u)^2 = \arg\min_k E(k)^2$

$$\text{Equation (2)} \Rightarrow \quad \widehat{\varepsilon_k}(u) = \widehat{\varphi_t}(u) - (-1)^{u\cdot k}\widehat{g}(u) - C\sqrt{2^n}\delta_0(u). \tag{3}$$

The constant value C can be discarded by considering the functions:

$$\widehat{\varphi_t^\star}(u) = \begin{cases} \widehat{\varphi_t}(u) & \text{if } u \neq 0 \\ 0 & \text{else} \end{cases} \text{ and } \widehat{g}^\star(u) = \begin{cases} \widehat{g}(u) & \text{if } u \neq 0 \\ 0 & \text{else} \end{cases} \tag{4}$$

$$E(k)^2 = \sum_{u\in\{0,1\}^n} \widehat{\varphi_t^\star}(u)^2 + \sum_{u\in\{0,1\}^n} \widehat{g}^\star(u)^2 - 2 \sum_{u\in\{0,1\}^n} \widehat{\varphi_t^\star}(u)\widehat{g}^\star(u)(-1)^{u\cdot k} \tag{5}$$

$\Longrightarrow$ **minimize** $E(k)^2$ amounts to **maximize** $F_t(k) = \sum_{u\in\{0,1\}^n} \widehat{\varphi_t^\star}(u)\widehat{g}^\star(u)(-1)^{u\cdot k}$

The theoretical value of $k^\star$ is then given by:

$$\arg\max_k F_t(k) \tag{6}$$

Estimation of the reliability of the value k that is found

The reliability of the value k that is found can be estimated by:

$$r_t(k) = \frac{F_t(k)}{\|\widehat{\varphi}_t^\star\| \cdot \|\widehat{g}^\star\|} = \frac{\langle \widehat{\varphi}_t^\star, \widehat{g}_k{}^\star \rangle}{\|\widehat{\varphi}_t^\star\| \cdot \|\widehat{g}_k{}^\star\|}$$

This coefficient is the Pearson correlation coefficient of φ_t (the real consumption value) and g (the hypothetical consumption value):

$$r_t(k) = \rho(\varphi_t, g) \qquad \text{with} \qquad \rho(\varphi, \psi) = \frac{\langle \varphi - m_\varphi, \psi - m_\psi \rangle}{\|\varphi - m_\varphi\| \cdot \|\psi - m_\psi\|}$$

Estimation of the reliability of the value k that is found

The reliability of the value k that is found can be estimated by:

$$r_t(k) = \frac{F_t(k)}{\|\widehat{\varphi}_t^\star\| \cdot \|\widehat{g}^\star\|} = \frac{\langle \widehat{\varphi}_t^\star, \widehat{g}_k{}^\star \rangle}{\|\widehat{\varphi}_t^\star\| \cdot \|\widehat{g}_k{}^\star\|}$$

This coefficient is the Pearson correlation coefficient of φ_t (the real consumption value) and g (the hypothetical consumption value):

$$r_t(k) = \rho(\varphi_t, g) \qquad \text{with} \qquad \rho(\varphi, \psi) = \frac{\langle \varphi - m_\varphi, \psi - m_\psi \rangle}{\|\varphi - m_\varphi\| \cdot \|\psi - m_\psi\|}$$

Pearson correlation coefficient

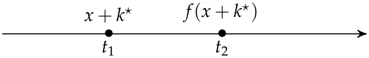
Let two random variables X and Y:

$$\rho(X,Y) = \frac{\mathrm{cov}(X,Y)}{\sigma_X \cdot \sigma_Y} = \frac{\sum_{i=1}^n (X_i - \bar{X}) \cdot (Y_i - \bar{X})}{\sqrt{\sum_{i=1}^n (X_i - \bar{X})^2 \cdot \sum_{i=1}^n (Y_i - \bar{Y})^2}}$$

- $\rho(X,Y) \in [-1,1]$
- $|\rho| = 1 \Longrightarrow$ high correlation
- $\rho = 0 \Longrightarrow$ low correlation

the correlation coefficient measures statistical relationship (”proportionnality”) between two random variables.

Multidimensional attack



multidimensional attack $\Longrightarrow$ attack that takes into account consumption at several instants

time		computed value	consumption	leakage model	error
t_1	$\rightarrow$	$f^1(x+k^\star)$	φ^1	g^1	E^1
t_2	$\rightarrow$	$f^2(x+k^\star)$	φ^2	g^2	E^2

Multidimensional attack

$$\xrightarrow[\quad t_1 \quad\quad\quad t_2 \quad]{x+k^\star \quad\quad f(x+k^\star)}$$

multidimensional attack $\Longrightarrow$ attack that takes into account consumption at several instants

time		computed value	consumption	leakage model	error
t_1	$\rightarrow$	$f^1(x+k^\star)$	φ^1	g^1	E^1
t_2	$\rightarrow$	$f^2(x+k^\star)$	φ^2	g^2	E^2

The most likely value of $k^\star$: minimize $\|\overrightarrow{E}\| = \|(E^1, E^2)\|$

$\Longleftrightarrow$ maximize $F(k) = \sum_{u \neq 0} \left(\widehat{\varphi^1}(u)\widehat{g^1}(u) + \widehat{\varphi^2}(u)\widehat{g^2}(u)\right)(-1)^{u \cdot k}$

$$\Phi_2 : \{\overrightarrow{\varphi} : \{0,1\}^n \to \mathbb{R}^2\}$$

$$\forall \overrightarrow{\varphi} = (\varphi^1, \varphi^2) \in \Phi_2$$
$$\forall \overrightarrow{\psi} = (\psi^1, \psi^2) \in \Phi_2$$

Euclidean scalar product in Φ_2

$$\langle \overrightarrow{\varphi}, \overrightarrow{\psi} \rangle = \langle \varphi^1, \psi^1 \rangle + \langle \varphi^2, \psi^2 \rangle$$

Euclidean norm in Φ_2

$$\|\overrightarrow{\varphi}\|^2 = \|\varphi^1\|^2 + \|\varphi^2\|^2$$

reliability coefficient $\Longrightarrow r_t(k) = \dfrac{\langle (\widehat{\varphi_t^1}^\star, \widehat{\varphi_t^2}^\star), (\widehat{g_k^1}^\star, \widehat{g_k^2}^\star) \rangle}{\|(\widehat{\varphi_t^1}^\star, \widehat{\varphi_t^2}^\star)\| \cdot \|(\widehat{g^1}^\star, \widehat{g^2}^\star)\|}$,

Experimental Results

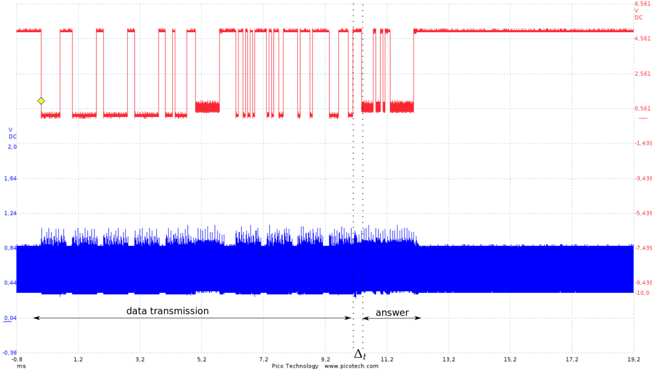
AES S-box (size of the S-box $n = 8$)

compute sequentially 4 times the S-box with different 8-bit keys k_1, k_2, k_3, k_4

record 256 traces of 40.000 samples

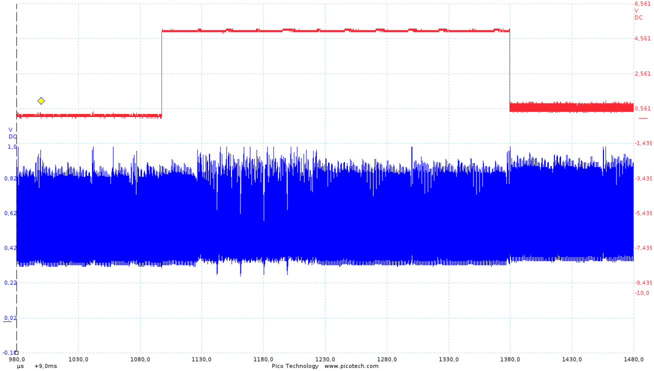
Experimental Results

power consumption and et I/O signal when running the encryption algorithm:



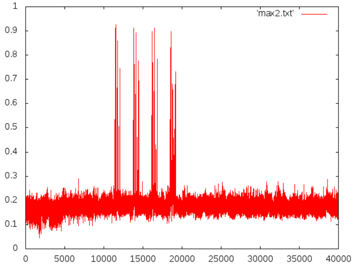
Experimental Results

power consumption and et I/O signal when running the encryption algorithm:

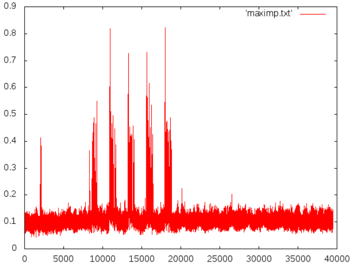


Experimental Results

Correlation between the real power consumption φ_t and the hypothetical power consumption g



One dimensional attack



Multidimensional attack

Conclusion

- we performed a CPA attack based on a Fourier Transform
- the approach allows multidimensional attack
- improvement: reduce the number of traces required to recover the right key

Thank you for your attention

Eric Brier, Christophe Clavier, and Francis Olivier.
Correlation power analysis with a leakage model.
In *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, pages 16–29, 2004.

Paul C. Kocher.
Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems.
In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer, 1996.

Kocher P., Jaffe J., and Jun B.
Differential power analysis.
In *Advances in Cryptology (CRYPTO'99)*, pages 388–397, 1999.