IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

Chosen message strategy to improve the correlation power analysis

ISSN 1751-8709
Received on 15th May 2018
Revised 26th November 2018
Accepted on 31st January 2019
E-First on 20th February 2019
doi: 10.1049/iet-ifs.2018.5103
www.ietdl.org

Maamar Ouladj[1] ✉, Phillipe Guillot[1], Farid Mokrane[1]

[1]LAGA, UMR 7539, CNRS, Université de Paris VIII, 2 Rue de la liberté, 93200 Saint Denis, France

✉ *E-mail: maamar.ouladj@etud.univ-paris8.fr*

Abstract: Nowadays cryptographic circuits are subject to attacks that no longer focus on the algorithm but on its physical implementation. Attacks exploiting information leaked by the hardware implementation are called side-channel attacks (SCA). In particular, the popular correlation power analysis (CPA) is known by its effectiveness. This paper presents a new method for an original optimisation of the CPA to recover secret keys with less power consumption traces than what is expected from the standard CPA. This improvement is done by choosing appropriate plaintexts, both non-adaptively and adaptively. A mathematical proof of the proposed procedure is provided for any cryptographic device with any known leakage model. The proposed technique is tested on the advanced encryption system (AES) S-box input (resp. output) implemented in an ATMega 163 smartcard, with hamming weight leakage model.

1 Introduction

The correlation power analysis (CPA) is a method that allows to recover the secret information (usually the secret key) embedded in the silicon of an electronic device [1–3]. It has been introduced in 2004 by Eric Brier, Christhophe Calavier, and Francis Olivier, in [3]. This attack follows the work of Paul Kocher proposed in 1999 [4]. The principle of CPA is to recover secret information through the power consumption measurements, while the device performs a computation that involves a secret subkey and a message. The message can be only known by the adversary or can also be chosen by him. The goal of this work is to minimise the number of measurements by choosing appropriate ones.

Two attack strategies (non-adaptive and adaptive) are presented in this work. The adaptive adversary can choose his queries with the knowledge of previously revealed side-channel information. Unlikely, a non-adaptive adversary does not have access to the system's responses until the end of the attack. Thus, when choosing a message, he cannot take into account the outcomes of the previous queries [5].

Chosen-message adversaries, known-message adversaries, and unknown message adversaries form a strict hierarchy in terms of the information that they can extract from a given side-channel [6]. In classical cryptanalysis, the adaptive selection of the cryptographic primitive inputs is known to be a powerful ability for the adversaries. Quite surprisingly, and although it is frequently suggested as a possible improvement, very few related works have been presented in the context of side-channel attacks (SCA) [7]. That is, in most experimental settings, one generally considers attacks with random input messages [7].

Several attacks among the most frequently used by the side channel community are asymptotically equivalent, when the adversary attacks one intermediate computation. In particular, in [8], the authors prove that most univariate attacks proposed in the literature can be expressed as CPA with different leakage models. Indeed, both differential power analysis (DPA), partitioning power analysis (PPA), and CPA attacks can be reformulated to reveal a correlation coefficient computation. They only differ in the involved model [8]. In [9], the authors show that the amount of information leaked by a cryptographic device measured with an information theoretic metric is connected to the correlation coefficient. Recently, in [10], the authors show that the CPA is almost optimal when the leakage model is known up to an affine transformation and under the Gaussian noise assumption.

Here, a new method to improve CPA over any cryptographic device with known leakage model is presented. This method allowed us to improve the CPA success rate, by choosing appropriates plaintexts both non-adaptively and adaptively. To lead a CPA with a minimum number of measurements, we choose a set of messages with the most pairwise decorrelated subkeys consumption model. We present two algorithms to find this set of plaintexts.

Operations involved in a symmetric block cipher, such as AES and DES, are usually reinforced by a non-linear function, called SBox. The input of the SBox involves both a plain data and a secret subkey [11, 12]. To attack through a side channel, the choice of an intermediate computation and leakage model have a significant impact on the success of the attack. In order to assess our strategies, they have been tested on the AES first round SBox input (resp. output). The target device is an ATMega 163 smartcard.

This article is organised as follows. In Section 2, some related works are given. In Section 3, some preliminaries of the CPA are presented. In Section 4, the chosen strategy is presented together with a mathematical model in a general setting. The presented principle may be applied to any leakage model. Sections 5 explains the practical implementation of both non-adaptive and adaptive strategies. Finally, some future works are proposed in the conclusion.

2 Related works

The measurement of the resistance to chosen-message attacks has been defined in [5]. In [13], an information-theoretic metric is defined. It captures multiple measurements, with respect to chosen-message adversaries. In [7], the authors propose an adaptive chosen-message strategy that can be applied to improve the efficiency of any distinguisher, particularly in template and correlation attacks. Unlikely to our strategy, the method here is entropy based. Their method is first designed for template attacks and is later just approximated by heuristics in the context of CPA. Our method is proven and designed especially for CPA. In [14], authors propose a method to enhance CPA by choosing a suitable normalisation. In [15], the authors propose an enhanced CPA on smart card. It is based on probability distribution of Hamming distance. In [16], a collision-based power analysis of modular exponentiation using chosen-message pairs have been proposed. Recently, a first-order chosen-plaintext DPA attack especially on

the third round of DES is proposed in [17]. All these paper do not have an obvious relationship with our work.

3 Preliminaries of the correlation power analysis (CPA)

The circuits that performs the computation in the processor are built by using a technology known as CMOS (Complementary Metal Oxide Semiconductor). Power analysis attacks are based on the general principle that the instantaneous power consumption depends on the data it processes and on the operation it performs [18]. In particular, CPA is based on the Pearson correlation coefficient between the power samples and the theoretical consumption given by a model (Hamming weight, Hamming distance of the handled data or any other model) [3].

Let K be the set $\{0,1\}^n$ of possible subkeys and also X be the set $\{0,1\}^n$ of possible messages, where n is the machine word size. In practice, K and X are often set of byte $\{0,1\}^8$.

Let Enc be the encryption function which involves a secret subkey k and a message x:

$$Enc: \begin{array}{ccc} K \times X & \to & \{0,1\}^n \\ (k,x) & \mapsto & Enc(k,x) \end{array}$$

The leakage model represents the power consumption of the circuit while it computes the encryption function. It is modelled as a function:

$$L: \begin{array}{ccc} K \times X & \to & \mathbb{R} \\ (k,x) & \mapsto & L(k,x) \end{array}$$

We assume that the adversary can send a set $\mathbb{S}$ of m messages with the same unknown subkey k: $\mathbb{S} = \{x_i; i = 1, \ldots, m\} \subseteq X$.

For k in K and $i = 1$ to m, let $CM_{k,i} \in \mathbb{R}$ denotes the consumption measurement corresponding to the unknown subkey k and the message x_i.

For short, let $L_{k',i} = L(k', x_i)) \in \mathbb{R}$ where k' is a candidate subkey, and x_i is the message.

Let us denote: $M_{k,i} = CM_{k,i} - E(\boldsymbol{CM}_k)$ the centred known consumption, where $E(\cdot)$ is the mean function, and denote $V_{k',i} = L_{k',i} - E(\boldsymbol{L}_{k'})$ the centred consumption model.

For the set $\mathbb{S}$ of messages, the unknown subkey k and any candidate subkey k', the Pearson correlation coefficient [19] between the power consumption measurement and the consumption given by the leakage model is defined as:

$$\rho_{\mathbb{S}}(\boldsymbol{CM}_k, \boldsymbol{L}_{k'}) = \frac{\sum_{i=1}^{i=m} M_{k,i} V_{k',i}}{\sqrt{\sum_{i=1}^{i=m} M_{k,i}^2} \sqrt{\sum_{i=1}^{i=m} V_{k',i}^2}}. \quad (1)$$

The CPA principle states that the subkey which lead to the highest correlation between the measured consumption and the leakage model consumption is the most probable one [3].

The Pearson correlation coefficient we can expressed by mean of scalar products [10, 20].

Let $\Phi_{\mathbb{S}}$ denote the set of real-valued functions over the set $\mathbb{S}$ of n -dimensional binary messages:

$$\Phi_{\mathbb{S}} = \{\boldsymbol{\varphi}: \mathbb{S} \to \mathbb{R}\}$$

For any two functions $\boldsymbol{f}$ and $\boldsymbol{g}$ in $\Phi_{\mathbb{S}}$, we define their scalar product with respect to $\mathbb{S}$ by:

$$\langle \boldsymbol{f} \cdot \boldsymbol{g} \rangle_{\mathbb{S}} = \sum_{x \in \mathbb{S}} \boldsymbol{f}(x) \boldsymbol{g}(x).$$

This scalar product is a symmetric positive definite bilinear form which induce to $\Phi_{\mathbb{S}}$ a structure of a m -dimensional Euclidean vector space over $\mathbb{R}$.

The norm associated to this scalar product is:

$$\| \boldsymbol{f} \|_{\mathbb{S}} = \sqrt{\langle \boldsymbol{f} \times \boldsymbol{f} \rangle_{\mathbb{S}}} = \sqrt{\sum_{x \in \mathbb{S}} \boldsymbol{f}(x)^2}.$$

The well-known Cauchy–Schwarz inequality holds:

$$\forall \boldsymbol{f}, \boldsymbol{g} \in \Phi_{\mathbb{S}}, |\langle \boldsymbol{f} \times \boldsymbol{g} \rangle_{\mathbb{S}}| \leq \| \boldsymbol{f} \|_{\mathbb{S}} \times \| \boldsymbol{g} \|_{\mathbb{S}}.$$

where $|\cdot|$ stands for the absolute value.

For any subkey k in K, let us define the centred measurement function $\boldsymbol{M}_k$ as:

$$\boldsymbol{M}_k: \begin{array}{ccc} \mathbb{S} & \to & \mathbb{R} \\ x_i & \mapsto & M_{k,i} \end{array}$$

Similarly, the centred leakage model $\boldsymbol{V}_k$ is defined as:

$$\boldsymbol{V}_k: \begin{array}{ccc} \mathbb{S} & \to & \mathbb{R} \\ x_i & \mapsto & V_{k,i} \end{array}$$

The Pearson correlation coefficient given by (1) can be rewritten as:

$$\rho_{\mathbb{S}}(\boldsymbol{CM}_k, \boldsymbol{L}_{k'}) = \frac{\langle \boldsymbol{M}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{M}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} \quad (2)$$

The CPA succeeds if the consumption given by the leakage model applied to the unknown subkey k is correlated to the physical observations more than the leakage model corresponding to any other candidate subkey. Thus, let k be the unknown subkey to recover, CPA succeeds if and only if:

$$\forall k' \in K,\ k' \neq k \Rightarrow \rho_{\mathbb{S}}(\boldsymbol{CM}_k, \boldsymbol{L}_k) > \rho_{\mathbb{S}}(\boldsymbol{CM}_k, \boldsymbol{L}_{k'}) \quad (3)$$

We now deal with chosen messages strategy in order to improve the CPA success rate.

4 Chosen messages strategy principle

If the adversary does not have access to the system's responses during the attack, he should choose from the beginning a non-adaptive set of messages. A more powerful scenario is when the adversary can adaptively select the plaintexts, depending on the prior knowledge about the secret subkey and a hypothetical leakage model [5, 7].

In this section, we first show an example to illustrate our chosen messages principle and we proof it in the Section 4.1. Then, two algorithms are presented in order to find plaintexts that would be used to improve the CPA success rate. These algorithms present, respectively, a non-adaptive strategy (Section 4.2) and an adaptive strategy (Section 4.3).

4.1 Attack idea and modelling

The same notations as in preliminaries are used. Before introducing our analysis, we fix the following assumptions which are very usual and realistic. First, recall that it is assumed that the adversary can send a set $\mathbb{S}$ of m messages involving the same unknown subkey k; $\mathbb{S} = \{x_1, x_2, \ldots, x_m\} \subseteq X$.

We do as in [9] the following assumption which is standard in SCAs [21]:

Assumption 1: (additive noise): The leakage sample $CM_{k,i}$ can be written as the sum of a deterministic part $L_{k,i}$ and a random part N_i. Moreover, the random part is assumed to be independent from the deterministic part and is identically distributed for all messages and subkeys.

When the leakage model is perfectly known, the model is said to be idealised. When the leakage model is partially unknown, the model is said to be noisy or non-idealised. We now deal with chosen messages strategy in order to improve the CPA success rate, both in idealised and non-idealised model.

Table 1 AddRoundKey leakage model

$Hw(k \oplus x)$	000	001	010	011	100	101	110	111
$k = 000$	0	1	1	2	1	2	2	3
$k = 001$	1	0	2	1	2	1	3	2
$k = 010$	1	2	0	1	2	3	1	2
$k = 011$	2	1	1	0	3	2	2	1
$k = 100$	1	2	2	3	0	1	1	2
$k = 101$	2	1	3	2	1	0	2	1
$k = 110$	2	3	1	2	1	2	0	1
$k = 111$	3	2	2	1	2	1	1	0

As in [22], an important property of the Pearson correlation coefficient will be used:

Property 1: The Pearson correlation coefficient is invariant under any increasing affine transformation applied to one of its input random variables.

In order to explain the idea behind our method, let us consider the simple example of the exclusive or operator $(k \oplus x)$ over the set of 3-dimensional binary vectors in the idealised model.

4.1.1 Example: Let K and X be the set of 3-dimensional binary vectors and consider the following subset of three messages: $\mathbb{S} = \{000, 001, 010\}$. Let us consider the Hamming weight leakage model:

$$L: \begin{array}{ccc} K \times X & \rightarrow & \mathbb{R} \\ (k, x) & \mapsto & Hw(k \oplus x) \end{array},$$

where $Hw(\cdot)$ denotes the Hamming weight function.

In Table 1, the leakage values are illustrated as a function of k and x.

The subkey k can be recovered if the chosen set of messages shows different computation profiles. This property holds for the three first columns, so one could theoretically consider the three messages 000, 001, and 010 to recover the unknown subkey. Whereas according to the Property 1, subkey 0 and subkey 4 cannot be distinguished with the Pearson correlation coefficient, as they are related by an affine relationship. Thus, this subset of messages is not suitable.

From this idea, messages should be chosen such that components in the lines of Table 1 form vectors as most as possible pairwise orthogonal.

Let us define the leakage model estimation errors function (or noise function) by: $\boldsymbol{N} = \boldsymbol{M}_k - \boldsymbol{V}_{k'}$, where the functions $\boldsymbol{M}_k$ and $\boldsymbol{V}_{k'}$ are defined as above.

Let us also define *SNR* (signal to noise ratio) for the m measurements given by the set of messages ($\mathbb{S}$) as follows:

Definition 1: For m measurements involving the same unknown subkey k and the m messages in $\mathbb{S}$, the signal to noise ratio is defined as:

$$\mathrm{SNR}_{\mathbb{S}} = \frac{\| \boldsymbol{V}_k \|_{\mathbb{S}}}{\| \boldsymbol{N} \|_{\mathbb{S}}}.$$

Recall that $\boldsymbol{V}_k$ denotes the centred leakage model involving the right unknown subkey k.

Proposition 1: : Let k be the unknown subkey to recover and $\mathbb{S}$ be a set of messages involving the same unknown subkey k.

In the idealised model (*i.e.* $\| \boldsymbol{N} \|_{\mathbb{S}} = 0$), the CPA applied to $\mathbb{S}$ succeeds if and only if:

$$\forall k' \in K, k' \neq k \Rightarrow 1 - \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} > 0$$

In the noisy model ($\| \boldsymbol{N} \|_{\mathbb{S}} \neq 0$), this condition is satisfied if:

$$\forall k' \in K,\ k' \neq k \Rightarrow 1 - \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} > \frac{2}{SNR_{\mathbb{S}}}$$

Proof: From (2), the CPA success condition given by inequality (3) is written as:

$$\forall k' \in K,\ k' \neq k \Rightarrow \frac{\langle \boldsymbol{M}_k, \boldsymbol{V}_k \rangle_{\mathbb{S}}}{\| \boldsymbol{M}_k \|_{\mathbb{S}} \| \boldsymbol{V}_k \|_{\mathbb{S}}} > \frac{\langle \boldsymbol{M}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{M}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}}$$

Since $\boldsymbol{M}_k$ corresponds to the correct subkey k and the noise is assumed to be additive ($\boldsymbol{M}_k = \boldsymbol{V}_k + \boldsymbol{N}$), the CPA succeeds if and only if, for all k' in K different from k, one has:

$$\begin{aligned} &\frac{\langle \boldsymbol{V}_k + \boldsymbol{N}, \boldsymbol{V}_k \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}}} > \frac{\langle \boldsymbol{V}_k + \boldsymbol{N}, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} \\ &\frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_k \rangle_{\mathbb{S}} + \langle \boldsymbol{N}, \boldsymbol{V}_k \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}}} > \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}} + \langle \boldsymbol{N}, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} \\ &\frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_k \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}}^2} - \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} > \frac{\langle \boldsymbol{N}, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} - \frac{\langle \boldsymbol{N}, \boldsymbol{V}_k \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}}^2} \end{aligned}$$

So, from condition (3), the CPA succeeds if and only if, for all k' in K different from k;

$$1 - \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} > \left\langle \frac{\boldsymbol{N}}{\| \boldsymbol{V}_k \|_{\mathbb{S}}}, \frac{\boldsymbol{V}_{k'}}{\| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} - \frac{\boldsymbol{V}_k}{\| \boldsymbol{V}_k \|_{\mathbb{S}}} \right\rangle_{\mathbb{S}} \quad (4)$$

Thus, if $\| \boldsymbol{N} \|_{\mathbb{S}} = 0$, then the CPA succeeds if and only if, for all k' in K different from k, the following inequality holds:

$$1 - \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} > 0 \quad (5)$$

According to Cauchy–Schwarz and triangular inequalities, for all k' in K different from k, one has:

$$\begin{aligned} \frac{2}{SNR_{\mathbb{S}}} &= \frac{\| \boldsymbol{N} \|_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}}} \left(\| \frac{\boldsymbol{V}_{k'}}{\| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} \|_{\mathbb{S}} + \| \frac{\boldsymbol{V}_k}{\| \boldsymbol{V}_k \|_{\mathbb{S}}} \|_{\mathbb{S}} \right) \\ &\geq \left\langle \frac{\boldsymbol{N}}{\| \boldsymbol{V}_k \|_{\mathbb{S}}}, \frac{\boldsymbol{V}_{k'}}{\| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} - \frac{\boldsymbol{V}_k}{\| \boldsymbol{V}_k \|_{\mathbb{S}}} \right\rangle_{\mathbb{S}} \end{aligned}$$

From condition (4), if $\| \boldsymbol{N} \|_{\mathbb{S}} \neq 0$, the CPA success condition is satisfied if:

$$\forall k' \in K,\ k' \neq k \Rightarrow 1 - \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} > \frac{2}{SNR_{\mathbb{S}}} \quad (6)$$

This completes the proof. □

From this condition, it can be seen that a suitable choice of the messages can improve the CPA success rate more than the number of traces by itself.

Indeed, more the leakage model applied to the guessed subkey is correlated with the leakage model applied to correct subkey, more it is difficult to distinguish the guessed subkey from the correct one. So, the success rate can be improved by choosing messages who lead as less as possible the correlations between the

```
procedure NON-ADAPTIVE-STRATEGY(L[2^n][2^n], SNR)
                ▷ SNR or the maximum number of measurements
    𝕊 ← choose_any_message(X)
    x, current_quality = 0
    while (current_quality < 2/SNR) do
                ▷ Or the maximum number of measurements
        x ← look_for_greater_quality(X)
        add_to(𝕊, x)
        current_quality ← quality(𝕊)
    end while
    return 𝕊
end procedure
```

Fig. 1 *Algorithm 1: Non-adaptive chosen messages algorithm*

```
procedure ADAPTIVE-STRATEGY(L[2^n][2^n], 𝕊_m, Keys[ℓ])
                ▷ Keys[ℓ]:The ℓth most correlated subkey
    quality(𝕊_{m+1}) ← 0
    for (x in X) do
        max_corr ← −1                    ▷ maximum correlation
        for (key1 ← 1 to ℓ − 1) do
            for (key2 ← key1 + 1 to ℓ) do
                if (max_corr < ρ_{s_m ∪ {x}}(key1, key2)) then
                    max_corr ← ρ_{s_m ∪ {x}}(key1, key2)
                end if
            end for
        end for
        if (quality(𝕊_{m+1}) < 1 − max_corr) then
            quality(𝕊_{m+1}) ← 1 − max_corr
            x_{m+1} ← x
        end if
    end for
    return x_{m+1}
end procedure
```

Fig. 2 *Algorithm 2: Adaptive chosen messages algorithm*

leakage model applied to the correct subkey and leakage model applied to all other candidates. As the adversary does not know the key k, this property must be fulfilled for all pair of possible subkeys.

We now deal with two strategies.

4.2 Non-adaptive chosen messages strategy

According to inequality (6) and since the adversary does not know necessarily the *SNR*, we define the quality of a set $\mathbb{S}$ of messages by the worst possible case as:

Definition 2: Let $\mathbb{S}$ be a set of messages:

$$\text{quality}(\mathbb{S}) = 1 - \max_{\substack{k,k' \in K \\ k \neq k'}} \left\{ \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} \right\}$$

The goal is to find the best set $\mathbb{S}$ of m messages. It is the set which maximise the quality:

$$\begin{aligned} \text{best}(m) &= \underset{\mathbb{S};\#\mathbb{S}=m}{\text{ArgMax}} \{\text{quality}(\mathbb{S})\} \\ &= \underset{\mathbb{S};\#\mathbb{S}=m}{\text{ArgMin}} \left\{ \max_{\substack{k,k' \in K \\ k \neq k'}} \left\{ \frac{\langle \boldsymbol{V}_k, \boldsymbol{V}_{k'} \rangle_{\mathbb{S}}}{\| \boldsymbol{V}_k \|_{\mathbb{S}} \| \boldsymbol{V}_{k'} \|_{\mathbb{S}}} \right\} \right\} \\ &= \underset{\mathbb{S};\#\mathbb{S}=m}{\text{ArgMin}} \left\{ \max_{\substack{k,k' \in K \\ k \neq k'}} \{\rho_{\mathbb{S}}(\boldsymbol{V}_k, \boldsymbol{V}_{k'})\} \right\} \end{aligned}$$

where $\#\mathbb{S}$ denotes the cardinality of the set $\mathbb{S}$.

If the adversary does not have access to the system responses during the attack, he should find the smallest set of messages satisfying condition (6). So, the adversary should find the smallest messages set with a quality greater than $2/SNR_{\mathbb{S}}$. The complexity of the exhaustive research of this set is exponential. In order to address this problem, a greedy heuristic is presented to find an acceptable solution. We propose to choose messages one after the other. In each step, the chosen message is those that maximise the quality of the set, as presented in the sequel.

Let us denote the set of the chosen messages during the first m steps by $\mathbb{S}_m = \{x_1, \ldots, x_m\}$.

The $(m+1)$ th message is chosen to maximise the quality of $\mathbb{S}_{m+1} = S_m \cup \{x_{m+1}\}$:

$$\begin{aligned} x_{m+1} &= \underset{x \in X}{\text{ArgMax}} \{\text{quality}(\mathbb{S}_m \cup \{x\})\} \\ &= \underset{x \in X}{\text{ArgMin}} \left\{ \max_{\substack{k,k' \in K \\ k \neq k'}} \{\rho_{s_m \cup \{x\}}(\boldsymbol{V}_k, \boldsymbol{V}_{k'})\} \right\} \end{aligned}$$

The advantage of this algorithm is threefold. First, its complexity is much better than the exhaustive research. Second, the iterative construction of the set of messages allows to conduct the attack with success even if the $SNR_{\mathbb{S}}$ is unknown.

Third, this iterative construction allows to compute the Pearson correlation coefficient efficiently by an incremental procedure as proposed in [23].

The Algorithm 1 (see Fig. 1) presents the non-adaptive chosen messages strategy, where n denotes the machine word size.

4.3 Adaptive chosen messages strategy

When the adversary can adaptively select the plaintexts, depending on the prior knowledge about the secret subkey, a second algorithm is proposed. It consists in choosing the $(m+1)$ th message by taking adaptively of the knowledge of the m th previously revealed side-channel information.

This algorithm chooses the message x_{m+1} which builds $\mathbb{S}_{m+1}$ from $\mathbb{S}_m$ with respect to the best possible quality similarly to the Algorithm 1 (Fig. 1). The difference is that this adaptive method computes the quality of $\mathbb{S}_{m+1}$ with respect to a most likely subkeys set K_ℓ (10% of the possible subkeys set K e.g.).

Recall that the non-adaptive algorithm computes the quality of $\mathbb{S}_{m+1}$ with respect to all possible subkeys ($k \in K$).

$$x_{m+1} = \underset{x \in X}{\text{ArgMin}} \left\{ \max_{\substack{k,k' \in K_\ell \\ k \neq k'}} \{\rho_{s_m \cup \{x\}}(\boldsymbol{V}_k, \boldsymbol{V}_{k'})\} \right\}$$

K_ℓ is the set of the ℓ subkeys for which the leakage model applied to them is the most correlated to the measurements, at the m th step. This adaptive chosen messages strategy is based on the principle that the likelihood of the guessed subkeys is proportional to its leakage model correlation with the physical measurements at the m th step.

Indeed, by definition, the *quality* depends to all pairwise subkeys. Whereas up to noise, the CPA analysis should only compute the correlation coefficient between the leakage model applied to the correct subkey k and the leakage model applied to all other guessed subkeys. The knowledge of the m th previously revealed side-channel information allows us to focus our research, for the next query, on the most likely subkeys.

Since the appropriate plaintexts is chosen only with respect to the subset of the most likely subkeys, this algorithm is more efficient both in the success rate, time complexity, and memory complexity. It is a significant improvement of the standard CPA. Algorithm 2 (see Fig. 2) presents the adaptive chosen message strategy of the the $m+1$ th plaintext.

To avoid to sort all subkeys after each step, in order to select the ℓ th most correlated subkeys during the m th previous queries, the maximum correlation (*MaxC*) and the minimum correlation (*MinC*) are stored. To choose the $(m+1)$th plaintext, one considers only the keys for which the leakage model applied to it are more

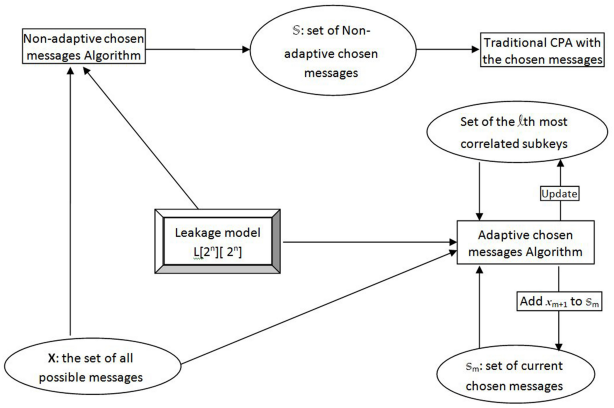

Fig. 3 *Schematic description of our adaptive and non-adaptive chosen messages algorithms*

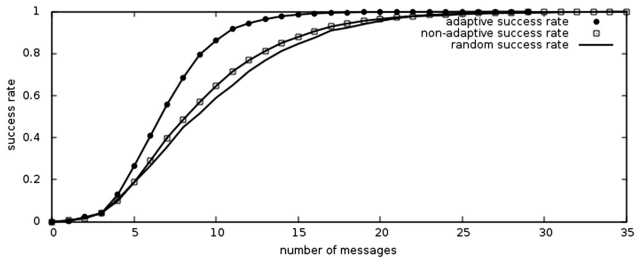

Fig. 4 *Attack on the Sbox input: This figure shows the success rate evolution with the number of measurements*

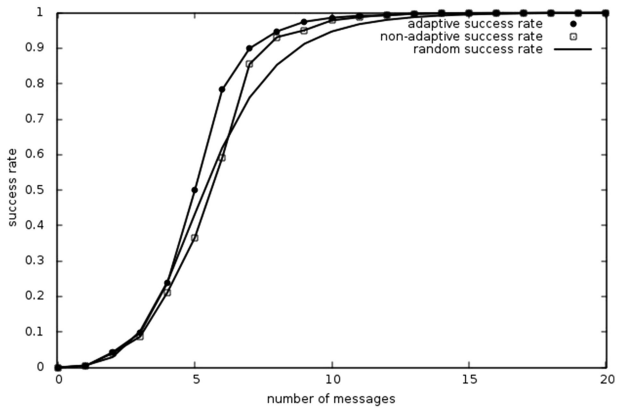

Fig. 5 *Attack on the Sbox output: This figure shows the success rate evolution with the number of measurements*

correlated to the measurement then the last decile for example $(\mathrm{Max}C - 0.1(\mathrm{Max}C - \mathrm{Min}C))$.

A schematic description of our adaptive and non-adaptive chosen messages algorithms shown in Fig. 3. The next section presents practical results of our idea in comparison with the standard CPA.

5 Experiments

In order to assess our strategy on practical implementation, experiments was performed by taking power measurements of an ATMega 163 smartcard. We used a Picoscope 3204A and a modified smart card reader to measure power consumption.

We selected two points of interest of an AES Rijndael software implementation. One corresponds to a first round S-box input $(x \oplus k)$ computation (3rd S-box but clearly not definitive) and the other corresponds to its output $(SBox(x \oplus k))$. The Hamming weight leakage model is assumed in our attacks as in [3]. The choice of the leakage model is not restrictive. We can straightforward adapt our chosen plaintexts strategy to other target architecture leakage model. It is worth noting that many papers

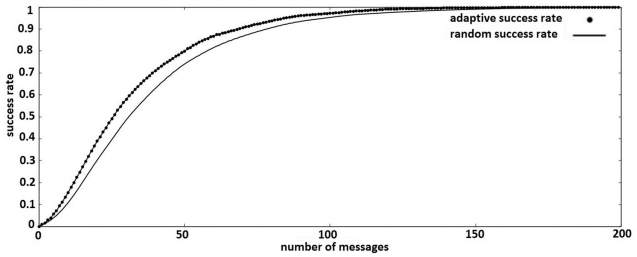

Fig. 6 *Attack on the Sbox input with standard deviation $\sigma_1 = 2$ noise: This figure shows the success rate evolution with the number of measurements*

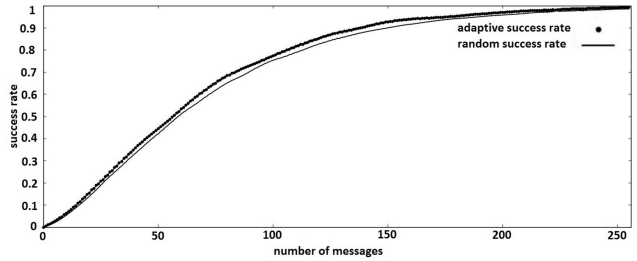

Fig. 7 *Attack on the Sbox input with standard deviation $\sigma_2 = 3$ noise: This figure shows the success rate evolution with the number of measurements*

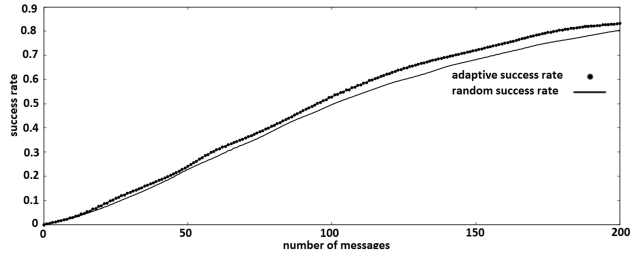

Fig. 8 *Attack on the Sbox input with standard deviation $\sigma_3 = 4$ noise: This figure shows the success rate evolution with the number of measurements*

investigate new power models, but the optimal choice of the leakage model is out of the scope of this paper.

In addition, we estimated the success rates over all possible key recoveries (256 keys). For each possible key, the attack was performed 100 times. The attack is considered as successful if and only if the correct subkey has been recovered. For each attack, the success rate is attributed according to this criterion.

Three situations are compared: random messages, non-adaptive chosen messages, and adaptive chosen messages. The results are posted in Fig. 4 for the S-Box input and in Fig. 5 for the S-Box output.

Notes and Comments: Fig. 4 shows that on the S-box input, the no-adaptive strategy is more efficient than choosing messages randomly. The adaptive strategy is the most efficient for any number of traces.

Fig. 5 shows that on the S-box output the no-adaptive strategy is more efficient than choosing messages randomly, after some number of traces. The adaptive strategy is the most efficient for any number of traces. There is a better distinguishability of the subkeys at the outputs of the first round Sbox than on its inputs, as presented in [24].

5.1 Adding noise

In order to assess this strategy in presence of noise, we added a normally distributed random noise with zero mean and three different standard deviation values $(\sigma_1 < \sigma_2 < \sigma_3)$. The results of these experiments for random-messages and adaptive chosen attacks are posted in Figs. 6–8 for the S-Box input and in Figs. 9–11 for the S-Box output.

Notes and Comments: These figures show that this chosen messages strategies keep a good results even in a noisy environment. As already known, analysing the outputs of the S-

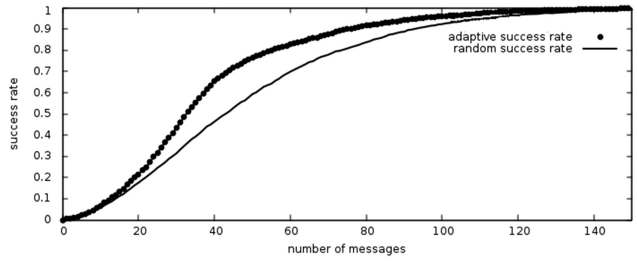

Fig. 9 *Attack on the Sbox output with standard deviation $\sigma_1 = 2.5$ noise: This figure shows the success rate evolution with the number of measurements*

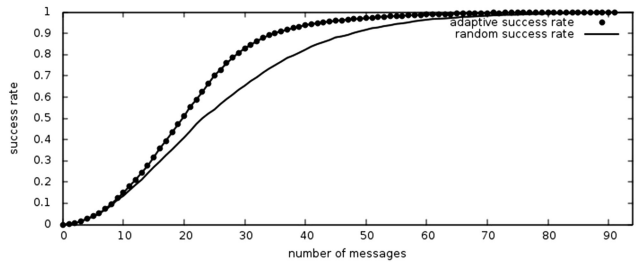

Fig. 10 *Attack on the Sbox output with standard deviation $\sigma_2 = 4$ noise: This figure shows the success rate evolution with the number of measurements*

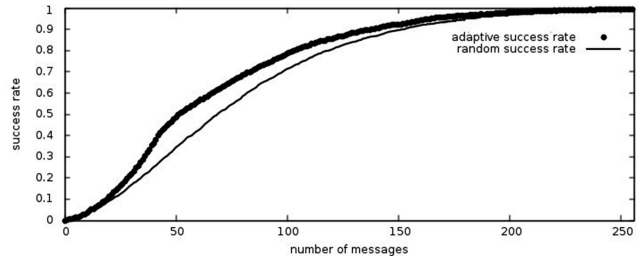

Fig. 11 *Attack on the Sbox output with standard deviation $\sigma_3 = 5.5$ noise: This figure shows the success rate evolution with the number of measurements*

boxes distinguishes the subkeys better than analysing their inputs [24], and our strategy is more efficient at this intermediate computation.

5.2 Discussion

The efficiency of our strategy only depends on the accuracy of the leakage model used. This technique is built in such a way that it does not assume anything about the linearity of the leakage model. Since the CPA is tolerant to any scaling of the leakage function [10], our strategy holds again if the leakage model is only known up to a linear transformation.

Complexity: Usually, CPA attacks rely on statistical analysis and has a quadratic complexity compared to the number of guessed subkeys $((2^n)^2)$, when resorting to Pearson correlation coefficient computation [25, 26]. In the non-adaptive chosen messages algorithm, the adversary should choose at most (m) messages. In each message choice, he should look for the greater quality by computing the Pearson correlation coefficient between all pair of leakage model applied to a pair of possible subkeys. Since the number of possible subkey pairs equals $((2^n)^2)$, then the non-adaptive chosen messages algorithm has the complexity of $(m \times (2^n)^2)$.It can be performed prior to the attack.

The advantage of the adaptive chosen messages algorithm is that the number of the considered subkeys is smaller in comparison with the non-adaptive one. For example, if we consider 1/10 of subkeys to choose the next plaintext, the success rate of the adaptive chosen messages algorithm increases and the complexity decrease. This complexity is $(m \times (2^n/10)^2)$ instead of $(m \times (2^n)^2)$ in the non-adaptive chosen messages algorithm.

When the machine word size is larger (16 or 32 bits), the contrast between the guesses is relatively enhanced [3]. So one can consider less than 1/10 of subkeys to choose adaptively the next plaintext. The complexity decreases again. We began tests with varying percentage of subkeys to consider, and the first results does not show direct influence of the success rate to this percentage. The good trade-off is to study.

Finally, the adaptive strategy requires access to the device, but this strategy can be done incrementally as in [23], and for a small subset of subkeys. A strategy is optimal if the adversary can expect to have less uncertainty about the subkey than with any other strategy of the same number of messages [5]. Our strategy is not necessarily optimal.

6 Conclusion

This paper presents two new chosen messages strategies to improve the CPA, namely non-adaptive and adaptive. The proposed strategies has been tested on the AES first round S-box input (resp. output). The adaptive strategy is the most efficient both in idealised and non-idealised models. It is based on the choice of the next message which distinguish as much as possible the most likely subkeys in the previous traces.

Since adaptive strategies require to take larger security margins than for random-message attacks [7], the efficiency of our adaptive strategies should be considered when reasoning about CPA countermeasures.

Finally, we hope that our work will be followed by some interesting further research works. Among them, experiments should be performed on protected implementation and on different machine architectures [27–31]. The principal component analysis (PCA) could also be used to enhance our strategies [32].

7 References

[1] Mayer-Sommer, R.: 'Smartly analysing the simplicity and the power of simple power analysis on smartcards'. Cryptographic Hardware and Embedded Systems – CHES, Worcester, MA, USA, 2000 (LNCS, **1965**), pp. 78–92

[2] Brier, E., Clavier, C., Olivier, F.: 'Optimal statistical power analysis'. Cryptology ePrint Archive, Report 2003/152, 2003. Available at http://eprint.iacr.org/2003/152

[3] Brier, E., Clavier, C., Olivier, F.: 'Correlation power analysis with a leakage model'. Cryptographic Hardware and Embedded Systems – CHES 2004: 6th Int. Workshop, Cambridge, MA, USA, 11–13 August 2004, pp. 16–29

[4] Kocher, P., Jaffe, J., Jun, B.: 'Differential power analysis'. Advances in Cryptology – CRYPTO '99, 19th Annual Int. Cryptology Conf., Santa Barbara, California, USA, 15–19 August 1999 (LNCS, **1666**), pp. 388–397

[5] Köpf, B., Basin, D.: 'An information-theoretic model for adaptive side-channel attacks'. Proc. 14th ACM Conf. on Computer and Communication Security (CCS 2007), Alexandria, Virginia, USA, 2007, pp. 286–296

[6] Backes, M., Köpf, B.: 'Formally bounding the side-channel leakage in unknown-message attacks'. Proc. 13th European Symp. on Research in Computer Security (ESORICS 2008), Málaga, Spain, 2008 (LNCS, **5283**), pp. 517–532

[7] Veyrat-Charvillon, N., Standaert, F.X.: 'Adaptive chosen-message side-channel attacks'. ACNS 2010, Beijing, China, 2010 (LNCS, **6123**), pp. 186–199

[8] Doget, J., Prouff, E., Rivain, M., *et al.*: 'Univariate side channel attacks and leakage modeling'. *J Cryptogr Eng*, 2011, **1**, pp. 123–144, doi: 10.1007/s13389-011-0010-2

[9] Mangard, S., Oswald, E., Standaert, F.-X.: 'One for all, all for one: unifying standard DPA attacks', Cryptology ePrint Archive, Report 2009/449, *IET Inf. Secur.*, 2011, **5**, (2), pp. 100–110, doi: 10.1049/iet-ifs.2010.0096, 2010

[10] Heuser, A., Rioul, O., Guilley, S.: 'Good is not good enough, deriving optimal distinguishers from communication theory'. Cryptographic Hardware and Embedded Systems – CHES 2014, Busan, South Korea, 2014 (LNCS, **8731**), pp. 55–74

[11] NIST AES: Fips publication 197 – 'advanced encryption standard', 1998

[12] NIST DES: Fips publication 46-3 – 'data encryption standard', 1977

[13] Standaert, F.-X., Malkin, T.G., Yung, M.: 'A unified framework for the analysis of side-channel key recovery attacks-extended version – version 3.0', 23 February 2009

[14] Le, T.-H., Clédière, J., Canovas, C., *et al.*: 'A proposition for correlation power analysis enhancement'. Cryptographic Hardware and Embedded Systems – CHES, Yokohama, Japan, 2006, pp. 174–186

[15] Li, H., Wu, K., Peng, B., *et al.*: 'Enhanced correlation power analysis attack on smart card'. The 9th Int. Conf. for Young Computer Scientists, Zhang Jia Jie, Hunan, China, 2008, doi: 10.1109/ICYCS.2008.230

[16] Homma, N., Miyamoto, A., Aoki, T., *et al.*: 'Collision-based power analysis of modular exponentiation using chosen-message pairs'. Cryptographic Hardware and Embedded Systems – CHES, Washington, D.C., USA, 2008, pp. 15–29

[17] Reparaz, O., Gierlichs, B.: 'A first-order chosen-plaintext DPA attack on the third round of DES'. Cryptology ePrint Archive, Report 2017/1257, December 2017. Available at http://eprint.iacr.org/2017/1257
[18] Messerges, T.S., Dabbish, E.A., Sloan, R.H.: 'Examining smart-card security under the threat of power analysis attacks', *IEEE Trans. Comput.*, 2002, **51**, (5), pp. 541–552
[19] Pearson, K.: 'On lines and planes of closest fit to systems of points in space', *Philosophical Magazine Series*, 1901, **2**, (6), pp. 559–572
[20] Guillot, P., Millerioux, G., Dravie, B., *et al.*: 'Spectral approach for correlation power analysis, In proceeding of the second international conference of codes'. Cryptology and Information Security (C2SI2017), Rabat, Morocco, 10–12 April 2017, Proceedings – In Honor of Claude Carlet, (LNCS 10194), pp. 238–253
[21] He, W., Bhasin, S., Otero, A., *et al.*: 'Sophisticated security verification on routing repaired balanced cell-based dual-rail logic against side channel analysis', *IET Inf. Sec.*, 2015, **9**, (1), pp. 1–13
[22] Prouff, E., Rivain, M., Bevan, R.: 'Statistical analysis of second order differential power analysis'. IACR Cryptology ePrint Archive, 2010, p. 646
[23] Bottinelli, P., Bos, J.W.: 'Computational aspects of correlation power analysis', *In J. Cryptogr Eng.*, 2016, doi: 10.1007/s13389-016-0122-9, pp. 167–181
[24] Prouff, E.: 'DPA attacks and S-boxes'. Fast Software Encryption – FSE 2005, Paris, France, 2005 (LNCS, **3557**), pp. 424–442
[25] Schimmel, O., Duplys, P., Bohl, H.E.J., *et al.*: 'Correlation power analysis in frequency domain'. First Int. Workshop on Constructive Side-Channel Analysis and Secure Design COSADE, Darmstadt, Germany, 2010
[26] Prouff, E. (Ed.): 'Constructive side-channel analysis and secure design-4th international workshop'. COSADE 2013, Paris, France, 6–8 March 2013, Revised Selected Papers, LNCS7864. Available at http://dx.doi.org/10.1007/978-3-642-40026-1, ISBN 978-3-642-40025-4
[27] Marzouqi, H., Al-Qutayri, M., Salah, K.: 'Review of gate-level differential power analysis and fault analysis countermeasures', *IET Inf. Sec.*, 2014, **8**, (1), pp. 51–66, doi:10.1049/iet-ifs.2012.0319
[28] Mahanta, H.J., Khan, A.K.: 'Securing RSA against power analysis attacks through non-uniform exponent partitioning with randomisation', *IET Inf. Sec.*, 2018, **12**, (1), pp. 25–33, doi:10.1049/iet-ifs.2016.0508
[29] Zhou, X., Whitnall, C., Oswald, E., *et al.*: 'Categorising and comparing cluster-based DPA distinguishers'. Report 2017/764, 2017. Available at http://eprint.iacr.org/
[30] Lerman, L., Veshchikov, N., Picek, S., *et al.*: 'On the construction of side-channel attack resilient S-boxes'. COSADE, Paris, France, 2017 (LNCS, **10348**), pp. 102–119. Available at http://dx.doi.org/10.1007/978-3-319-64647-3_7
[31] Lerman, L., Veshchikov, N., Picek, S., *et al.*: 'Higher order side-channel attack resilient S-boxes'. Cryptology ePrint Archive, Report 2018/006, 2018. Available at https://eprint.iacr.org/2018/006
[32] Batina, L., Hogenboom, J., Woudenberg, J.G.J.V.: 'Getting more from PCA: first resultats of using principal component analysis for extensive power analysis'. CT-RSA, San Francisco, CA, USA, 2012 (LNCS, **7178**), pp. 383–397