POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Executive Summary of the Thesis

# Performing SCA Against Block Ciphers Using Closest and Furthest Leakage Models

Laurea Magistrale in Computer Science and Engineering - Ingegneria Informatica

**Author:** Costantino Vincifori

**Advisor:** Prof. Gerardo Pelosi

**Co-advisor:** Prof. Alessandro Barenghi

**Academic year:** 2020-2021

## 1. Introduction

Nowadays, cryptographic implementations on physical system are subject to *side-channel* attacks (or SCAs). Side-channel attacks are used to exploit physical properties of a device, with the aim of retrieving the secret key employed in a cryptographic encryption/decryption. The first side-channel attacks that were developed used to define as accurately as possible the leakage model of the target device. This process would also exploit the information about the physics on which such cryptographic algorithms were implemented on. The most famous attack that models as accurately as possible the physics of a device is *Correlation Power Analysis* (or CPA). Then, a side-channel attack is mounted by making key guessing, and by observing to which key guess it is associated to the highest score through a *distinguisher*. A distinguisher is a function that associates a score to each key guess. The higher the score of a key guess, the more probable it is that specific key guess is actually the secret key employed for that cryptographic encryption/decryption.

Only recently, in the last decade, it was developed a new class of side-channel attacks that were defined as *generic*. Generic side-channel attacks do not require to define a leakage model as accurately as possible; instead, it used a suitable function executed within the cryptographic algorithm as leakage model. As the definition of the leakage model is more relaxed, it must be used a distinguisher that is capable to extract more information from such simpler models. In this project it is studied the properties of mutual information as a key distinguisher for side-channel attacks. Side-channel attacks exploiting mutual information as key distinguishing tool fall under the name of mutual information analysis (MIA)[2] attacks.

An advantage on performing side-channel attacks with generic side-channel attacks as MIA with respect to SCAs that model as accurately as possible the target device for the leakage model as CPAs, is that they do not require any particular knowledge of the target device, but only what type of algorithm is it run on it. Thus, in a scenario where an attacker has limited information about a target device, MIA may help to mount a successful attack[1]. The trade off is paid in terms of physical measurements that must required from the device under attack.

A MIA attack is performed by making key hypothesis $k_{hyp}$, and observing the maximum of mutual information estimation $I(\mathbf{O}|\mathbf{L}_{k_{hyp}})$ between side-channel measurements $\mathbf{O}$ extracted from a target device, and values computed by the hypothetical leakage model $\mathbf{L}_{k_{hyp}}$. Then, an attack is successful if it is defined as hypothetical leakage model that model that is the "closest" possible to the real (but unknown) target model. This model is able to justify the physical observations only when it is interrogated with the correct key hypothesis, as the estimation of the mutual information hits its maximum.

## 2. Project's Goal

Cryptographic algorithms encrypt/decrypt data by means of a secret key and the application of several encrypting/decrypting *rounds*. Each round is composed of a set of fixed operations: each operation modifies the state of a datum, and such modification can only be reverted when it is used the correct secret key.

Leakage models for side-channel attacks are usually built from non-linear functions, also known as substitution boxes. These boxes are usually implemented as look-up tables that take as argument a key hypothesis $k_{hyp}$, a known datum $m$, and outputs a value with no apparent relation with both inputs.

In this project it is chosen to analyze the performance of MIA attacks on leakage models $L_{k_{hyp}} := f(k_{hyp})$, where $f(\cdot)$ is a suitable substitution box of a cryptographic algorithm. Since there is a lot of flexibility in the choice of leakage models, the choice of the best leakage model is still an open problem.

However, in this project, it is chosen to analyze leakage models defined as $L_{k_{hyp}} := mask_{out} \& f(mask_{in}, k_{hyp})$ by means of exhaustive search of variables $mask_{in}$ and $mask_{out}$.

Up to now, in literature, it has never been shown such a fine grained analysis on leakage models for generic side-channel attacks. In addition to it, it was also chosen to analyze substitution boxes generated from genetic algorithms, presented in the paper "On the Construction of Side-Channel Attack Resilient S-boxes" by Lerman et al.[3]. in this paper it was presented a set of substitution boxes that claim to be more resilient to CPA and *Template Attacks* (or TA) attacks. Thus, in this work it analyzed the behaviour of MIA attacks when leakage models are built from such substitution boxes. The first objective of this work is to investigate if it could be found out substitution boxes that are resilient to MIA attacks when it is used the closest leakage models.

Moreover, while exploring leakage models by exhaustive search of variables $mask_{in}$ and $mask_{out}$, it was also observed a particular behaviour of mutual information on particular leakage models. It was observed that for some values of variable $mask_{in}$ and $mask_{out}$, it was possible to perform successful MIA attacks when it is observed the minimum of mutual information.

Intuitively, the minimum of mutual information would observed in correspondence to that hypothetical leakage model that is the most distant possible from the real (and unknown) target model only when it is tested with the correct key hypothesis. If this model exists, it is then (one) of the furthest model possible, capable to perform badly in a systematic way (only under the correct key assumption).

Then, the second challenge of this work is to observe if it is possible to find further leakage models built on substitution boxes presented in Lerman et al.[3], and study when it is possible to use these leakage models to perform successful side-channel attacks.

Again, in literature there is no previous work that investigates the existence of furthest leakage models for generic side-channel attacks. Then, the second objective of this work is to find out if it is possible to attack with the furthest leakage models those substitution boxes that were resilient to MIA with the closest leakage models.

## 3. Experimental Results

The first experiment that was conducted it was on the substitution box of AES cipher (an 8-to-8 bits substitution box), and it was observed that MIA attacks with furthest leakage models were successful with *Success Rate* equal to 1.00 only when it was used ideal measurements (without noise). The success rate is a metric used for side-channel attacks that measures the amount of successful attacks, each performed with the key guess with the highest scores (estimated from the distinguisher), averaged over all the attacks that were performed[1].

### AES S-Box

Table 1: Success Rate with the first most probable key guess

| SNR | max MI | min MI |
|---|---|---|
| $\infty$ | ✓ | ✓ |
| 10dB | ✓ | ✗ |
| 1dB | ✓ | ✗ |
| -10dB | ✓ | ✗ |

A success rate of 1.00 means that for each secret key, the distinguisher would associate the highest score to the correct key guess when a particular leakage model is used.
However, for the experiment it was also simulated side-channel measurements with different SNR profiles, but it could not be possible to find furthest leakage models for such profiles. The higher the SNR, then the better it is the quality of the measurements with respect to simulated noise; the lower the SNR, then the worse it is the quality of measurements w.r.t. the simulated noise.

## 3.1. 4-to-4 Bits S-Box

However, when it was studied the performance of 4-to-4 bits substitution boxes generated from genetic algorithms discussed in Lerman et al.[3], it was observed some interesting behaviours.
It was observed that for those substitution boxes that are actually implemented in ciphers used in real applications (such as PRINCE, PRIMATE, Klein), it was possible to find at least one furthest leakage model when with noiseless measurements, and it was possible only for Klein cipher to find a furthest leakage model with measurements with 10dB of SNR. In this case, the success rate was observed by looking at the first two most probable keys estimated from the distinguisher.

### PRESENT/PRINCE/Klein S-Box

Table 2: Success Rate with the first two most probable key guesses

| SNR | max MI | min MI |
|---|---|---|
| $\infty$ | ✓/✓/✗ | ✓/✓/✓ |
| 10dB | ✓/✓/✓ | ✗/✗/✓ |
| 1dB | ✓/✓/✓ | ✗/✗/✗ |
| -10dB | ✓/✓/✓ | ✗/✗/✗ |

While for the substitution boxes generated to be resilient to CPA attacks, it was observed that the substitution box *evolved_k* designed to be the most exploitable to CPA attacks, was actually the most resilient to MIA attacks, as it couldn't be found a furthest leakage model for SNR equal to 10dB.

### evolved_sr1/evolved_sr2/evolved_k S-Box

Table 3: Success Rate with the first two most probable key guesses

| SNR | max MI | min MI |
|---|---|---|
| $\infty$ | ✓/✓/✓ | ✓/✓/✓ |
| 10dB | ✓/✓/✓ | ✓/✓/✗ |
| 1dB | ✓/✓/✓ | ✗/✗/✗ |
| -10dB | ✓/✓/✓ | ✗/✗/✗ |

While for substitution boxes designed to be resilient to TAs it was observed they were way more resilient than CPA resilient S-Boxes to MIA attacks. In fact, it can be observed that for some substitution boxes it was not even possible to find a furthest leakage model for noiseless measurements.

### evolved_ta_sr1/evolved_ta_sr2/ evolved_ta_sr3/evolved_ta_sr4 S-Box

Table 4: Success Rate with the first two most probable key guesses

| SNR | max MI | min MI |
|---|---|---|
| ∞ | ✓/✓/✓/✓ | ✓/✗/✓/✗ |
| 10dB | ✓/✓/✓/✓ | ✓/✗/✗/✗ |
| 1dB | ✓/✓/✓/✓ | ✗/✗/✗/✗ |
| -10dB | ✓/✓/✓/✓ | ✗/✗/✗/✗ |

## 3.2. 5-to-5 Bits S-Box

Again, starting from substitution boxes of renowned ciphers (such as ASCON and PRIMATE), it was observed that only for ideal measurements it is possible to find furthest leakage models that would lead to successful MIA attacks with the highest success rate.

### ASCON/PRIMATE S-Box

Table 5: Success Rate with the first two most probable key guesses

| SNR | max MI | min MI |
|---|---|---|
| ∞ | ✗/✓ | ✓/✓ |
| 10dB | ✓/✓ | ✗/✗ |
| 1dB | ✓/✓ | ✗/✗ |
| -10dB | ✓/✓ | ✗/✗ |

For what concerns CPA resilient S-Boxes, on the other hand, it were spotted some substitution boxes that were attackable with furthest leakage models even with measurement with 10dB SNR.

### evolved_sr1/evolved_sr2/evolved_sr3/ evolved_sr4/evolved_sr5/evolved_sr6/ evolved_sr7/evolved_sr8/evolved_sr9 S-Box

Table 6: Success Rate with the first two most probable key guesses

| SNR | max MI |
|---|---|
| ∞ | ✓/✗/✓/✓/✗/✗/✓/✗/✓ |
| 10dB | ✓/✗/✓/✓/✗/✗/✓/✓/✓ |
| 1dB | ✓/✓/✓/✓/✓/✓/✓/✓/✓ |
| -10dB | ✓/✓/✓/✓/✗/✗/✓/✓/✓ |

### evolved_sr1/evolved_sr2/evolved_sr3/ evolved_sr4/evolved_sr5/evolved_sr6/ evolved_sr7/evolved_sr8/evolved_sr9 S-Box

Table 7: Success Rate with the first two most probable key guesses

| SNR | min MI |
|---|---|
| ∞ | ✓/✓/✓/✓/✓/✓/✓/✓/✓ |
| 10dB | ✓/✓/✓/✗/✓/✓/✗/✗/✗ |
| 1dB | ✗/✗/✗/✗/✗/✗/✗/✗/✗ |
| -10dB | ✗/✗/✗/✗/✗/✗/✗/✗/✗ |

While for TA resilient substitution boxes it was impossible to find a furthest leakage model for 10dB SNR measurements.

### evolved_ta_sr1/evolved_ta_sr2/ evolved_ta_sr3/evolved_ta_sr4/ evolved_ta_sr5/evolved_ta_sr6 S-Box

Table 8: Success Rate with the first two most probable key guesses

| SNR | max MI | min MI |
|---|---|---|
| ∞ | ✓/✓/✗/✗/✗/✓ | ✓/✓/✓/✓/✓/✓ |
| 10dB | ✓/✓/✓/✓/✓/✓ | ✗/✗/✗/✗/✗/✗ |
| 1dB | ✓/✓/✓/✓/✓/✓ | ✗/✗/✗/✗/✗/✗ |
| -10dB | ✓/✓/✓/✓/✓/✓ | ✗/✗/✗/✗/✗/✗ |

## 4. Conclusions

In this project it was observed that for some substitution boxes, it was possible to identify some furthest leakage model that would lead to successful attack with MIA. Specifically, it was possible to find such models from 5-to-5 bits CPA resilient substitution boxes introduced in Lerman et al.[3]. However, these models are reasonable to be used by a highly motivated actor that owns high quality sampling measurements, capable to obtain extract exceptional side-channel measurements.

However, despite the requirements may be a bit demanding, the attack surface exploiting furthest leakage models does still exist, and thus it must not be taken lightly.

In fact it can be observed that 5-to-5 bits substitution box $evolved\_sr2$, $evolved\_sr5$ an $evolved\_sr6$ it could be found furthest leakage models for 10dB SNR measurements, while it could not be found any closest leakage model for the same SNR.

## References

[1] Éloi Chérisey, Sylvain Guilley, Annelie Heuser, and Olivier Rioul. On the optimality and practicability of mutual information analysis in some scenarios. *Cryptography Commun.*, 10(1):101–121, 01 2018.

[2] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis. In *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, 2008.

[3] Liran Lerman, Nikita Veshchikov, Stjepan Picek, and Olivier Markowitch. On the construction of side-channel attack resilient s-boxes. In Sylvain Guilley, editor, *Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers*, volume 10348 of *Lecture Notes in Computer Science*, pages 102–119. Springer, 2017.