POLITECNICO DI TORINO
Repository ISTITUZIONALE

Side-channel analysis of SEcube™ platform

Original
Side-channel analysis of SEcube™ platform / Bollo, M., Carelli, A., Di Carlo, S., Prinetto, P.. - ELETTRONICO. - (2017), pp. 1-5. (2017 IEEE East-West Design & Test Symposium (EWDTS) Novi Sad, (Serbia) 29 Sept.-2 Oct. 2017) [10.1109/EWDTS.2017.8110067].

Availability:
This version is available at: 11583/2692798 since: 2017-11-20T10:44:27Z

Publisher:
IEEE

Published
DOI:10.1109/EWDTS.2017.8110067

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

13 June 2026

Side-channel analysis of SEcube™ platform

Matteo BOLLO*, Alberto CARELLI†, Stefano DI CARLO†, Paolo PRINETTO*†
*CINI Cyber Security National Lab, Rome, Italy
matteo.bollo@Consorzio-CINI.it
†Politecnico di Torino, Turin, Italy
{alberto.carelli, stefano.dicarlo, paolo.prinetto}@polito.it

***Abstract*—Cryptography provides techniques to cypher and de-cypher sensitive information through a token called key in order to store and transmit it across insecure networks. The goal of cryptography is to protect information from potential attackers and to enable access to authorized users only. Several hardware cryptographic devices are entering the market. However, these devices can be subject to passive attacks that consist in retrieving secret data by observing the side-channel behaviour of the device (i.e. execution time, power consumption, electromagnetic field). This work studies the robustness of SEcube™, an innovative secure hardware product against Differential Power Analysis attacks. SEcube™ is a system-on-chip equipped with three devices interconnected and embedded in a single chip: an ARM Cortex M4 low-power processor, a Lattice MachXO2-7000 FPGA and a SmartCard SLJ52G (EAL5+ certified). Moreover, in order to examine the security enhancement of this platform, we perform the same analysis with a similar board equipped with the same microprocessor and then compare the results.**

Experimental results show that the number of correct bits is similar between the two platform.

***Index Terms*—Side-channel power analysis DPA**

1. Introduction

CRYPTOGRAPHY provides techniques to cypher and de-cypher sensitive information through a token called key in order to store and transmit it across insecure networks. The goal of cryptography is to protect information from potential attackers and to enable access to authorized users only.

In contrast to the cryptography principles, the cryptanalysis techniques are used to acquire knowledge of cyphered information without using the de-cypher key. Cryptanalysis attacks often exploit hardware and/or software physical properties of the implementation of the cryptographic algorithms (i.e. execution time, power consumption, electromagnetic field, glitches and fault sensitivity).

Cryptanalysis attacks can be distinguished in four categories: (1) active, (2) passive, (3) invasive and (4) non-invasive. In case of the active attacks the malicious user acts directly on the device trying to alter its behaviour (e.g., injecting faults) while in passive attacks the attacker does nothing other than to observe the normal behaviour of the device. When the attack alters physically the device, for example exposing access to its internal components and connections, it is defined as invasive, instead non-invasive attacks do not require physical alteration of the device because they exploit external information, i.e., physical quantities.

Side-channel analysis is among the most effective passive and non-invasive type of attack [1]. It exploits the fact that all cryptographic devices leak physical data during the encryption process. The leakage (e.g., electromagnetic radiation, power dissipation, etc.) can be measured, collected and analyzed in order to discover the encryption key monitoring the behavior of the circuit. To succeed in the attack, the observed physical quantities must be somehow correlated with the secret key used to cypher the information. The most effective property of side-channel attacks is its black-box approach that only requires the knowledge of the encryption algorithm but not its specific implementation. Among the physical leakages, the most easy to acquire is the power consumption. It is sufficient to place a resistor between the power supply line and the circuit in order to collect measurements of the voltage required by the device.

Simple Power Analysis (SPA) and Differential Power Analysis (DPA) belong to the category of side-channel attacks focusing on power consumption [1]. SPA is a technique that focuses on the performed operations of a device to acquire knowledge of information. Inspecting the leakage traces it is possible to understand which operations are performed, provided that the operations have different power consumption. Also the sequence of operations might provide useful information, when the operations performed depend on the processed data. Instead, in DPA, the focus is on the data itself. It considers the dependencies among power consumption traces for different data processed. Depending on the considered leakage model, different number of transitions lead to different power consumption values.

This work studies the robustness of SEcube™, an innovative secure hardware product, against DPA attacks. SEcube™ is a system-on-chip. It is equipped with three devices interconnected and embedded in a single chip: an ARM Cortex M4 low-power processor, a Lattice MachXO2-7000 FPGA and a SmartCard SLJ52G

(EAL5+ certified). The platform is available either as SEcube™ Development Board for development purposes or as USB stick (USEcube™) to be employed as security token. In both cases, the interface adopted between the SEcube™ device and the host system is the USB bus.

While the board is commonly used for development, the USB token can be used in a variety of fields and applications (e.g., home banking) where security cannot be neglected. For this reason, the purpose of this paper is to analyze the robustness of the SEcube™ device. Moreover, in order to examine the security enhancement of this platform, we perform the same analysis with a similar board equipped with the same microprocessor and then compare the results.

The paper is organized as follows: Section 2 supplies a short overview regarding the Differential Power Analysis technique. Section 3 explains the tools and the methodology adopted to carry out the experiment. Section 4 reports and discusses the obtained results. Finally, Section 5 concludes this paper.

2. Differential Power Analysis

Differential Power Analysis is a side-channel attack which considers the power consumption of a circuit. It is a non-invasive attack that requires physical access to the security device. More precisely it must be possible to act on the device supply line. This technique can be employed to identify the key used for the encryption. It can be helpful to identify just a part of the key when this technique is adopted together with a brute-force attack. This can be simplified avoiding unnecessary combinations already assessed with DPA leading to a faster attack.

The basic idea of the DPA is to find a correlation among different sets of data to be processed with a cryptographic algorithm through a statistical analysis of the power consumption values [2]. It exploits the fact that, different data will lead to a different power consumption when the operations performed are the same.

First, several sets of power consumption measurements have to be collected avoiding as much as possible noise that will impact negatively the analysis leading to incorrect results. Second, the DPA takes place: all collected power measurements are partitioned in two different sets according to a selection function and with an assumption on the value of a bit belonging to the key. The difference of the average of power traces in each group is computed. This is repeated for every bit of the key.

The selection function determines how to group power traces. It depends on the power consumption model. Several models are possible, in this paper we consider only the following:

- Hamming Distance - one set contains the traces that are considered to generate the transition of the bit value 0 to 1 and 1 to 0. The other set contains the remaining traces;
- Hamming Weight - one set contains the traces that are considered to generate the transition of the bit value 0 to 1 and 1 to 1. The other set contains the remaining traces;
- Rising - one set contains the traces that are considered to generate the transition of the bit value 0 to 1. The other set contains the remaining traces;

By construction, one of the two sets will contain a power consumption component not present in the other set. The difference of the averages will approach zero for an increasing number of traces when there is no correlation, while it will present a peak in the opposite case. It has to be noted that even in presence of noise affecting the measurements, given enough traces it can be possible to detect small correlations [2]. The choice of the selection function will change the components of the two sets, and as consequence also the averages change. In general, this will lead to different results in term of correct bits.

3. Setup

The security device we use in our experiments is the SEcube™ platform. It is an open-source security platform which provides both hardware schematic and software source code. Even though the SEcube™ platform is provided with its open-source firmware and the implementation of its cryptographic algorithms is known, in order to better analyze the strength of its security, we decided to employ a black-box approach based on the sampling of the power consumption. Also, we want to compare the efficacy of the DPA attack with a normal device, to verify the security improvement brought by SEcube™ comparing it with a similar device. To make the experiment meaningful, we picked a ST Microelectronics Nucleo board [3] equipped with the same microprocessor [4] of SEcube™. All these devices are powered through the USB interface, where we act to precisely measure the power consumption.

The commercial USB token USEcube™ does not allow direct access to the internal circuitry. This already partially prevents the usage of probes to capture the power supply signal, unless invasive attacks are employed. For our experiments we adopted the Development Board version. With this device, having direct access to the V_{dd} pins, we could sample the power consumption very easily and with low noise. Nevertheless, to emulate a real attack, for both Nucleo board and SEcube™ board, we decided to use a custom connector to sample the power signal from the power supply line between the platform and the host PC. This special custom device is tailored for a generic USB device, so it can be employed also for other types of devices. To build it, we used an electronic prototyping board (i.e., a stripboard), where an USB male socket and a USB female connector have been soldered and linked together. The connection between the two ports is voluntarily left exposed, allowing the probes to be attached easily without introducing distortion. Moreover, a BNC connector is inserted in parallel between the supply line (+5V) and ground line (GND) (see Figure 1). In this way, this device can be connected directly to an oscilloscope avoiding the noise introduced by probes ohmic contacts,

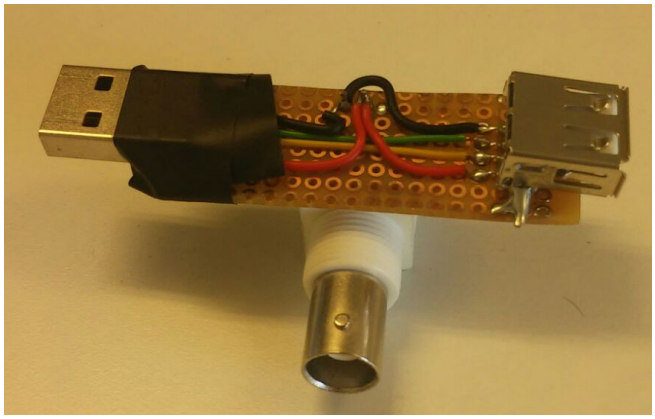

Figure 1. Custom handmade USB-USB/BNC connector

thus leading to more accurate measurements of the input voltage. Also, it allows us to perform the attack without physically modifying the security device, hence maintaining a non-invasive approach. To perform measurements, we employed an oscilloscope. The used device is a Tektronix TDS5052B [5] with 500 MHz bandwidth, 5 GS/s real-time sample rate and 2 acquisition channels. It embeds a General Purpose Interface Bus (GPIB) controller, which we use to manage the measurement process. In order to collect and store the power traces in an automated way, we setup a LabView module, which interfaces with and command the oscilloscope through the GPIB interface. Also the data is collected through the same physical interface.

Another requirement to perform a DPA attack is to know what algorithm is involved. Being the SEcube™ firmware open-source we can see that the available encryption algorithm is the AES-256 implemented using a software routine.

To verify the security solely of the hardware platform we created a custom firmware. This firmware includes low-level drivers for the microprocessor but it only executes the encryption algorithm instead of the whole SEcube™ open-source firmware. By employing this new firmware, we can better isolate the encryption process, which lead us to more accurate measurements without spurious transitions due to other operations performed in the original firmware that are not directly related to the encryption. The implemented AES algorithm is coded in C language, like the rest of the firmware. The implementation uses the simplest operation mode, i.e., Electronic Codebook (ECB). Both the used plaintext and the encryption key have size equal to 128 bits and are hard-coded in the firmware. The encryption process is repeated multiple times: it ciphers the plaintext with the same key, but in every round the last byte of the plaintext is changed, in order to have data dependence. The voltage drop at the power supply pins is measured during this process. To simplify the data trace acquisition procedure we added a trigger signal to highlight the beginning of the encryption process.

Finally, the acquired tracks are parsed and edited to be compliant with the software for the DPA analysis realized by the authors of [6].

Figure 2 shows the whole workflow just described.

TABLE 1. CIPHER KEY OF 128 BIT FROM [7] - CASE A

0x2b	0x7e	0x15	0x16	0x28	0xae	0xd2	0xa6
0xab	0xf7	0x15	0x88	0x09	0xcf	0x4f	0x3c

TABLE 2. PLAINTEXT OF 128 BIT FROM [7] - CASE A

0x32	0x43	0xf6	0xa8	0x88	0x5a	0x30	0x8d
0x31	0x31	0x98	0xa2	0xe0	0x37	0x07	0x00 .. 0xFF

4. Results

In order to test the security improvement introduced by SEcube™ platform, we adopted a comparative method. We take as a reference design the Nucleo board which embeds the same microprocessor of the SEcube™. The AES encryption algorithm is executed on both development boards against the same input data. The power traces are sampled with the same experimental setup. The attacks are performed separately and the results are compared. The difference in terms of effort (number of power traces required, number of guessed bits, ...) gives a quantitative estimation of the security enhancement of the SEcube™ platform with respect to the Nucleo board.

The test-bench algorithm is a software implementation of the AES algorithm. We adopt the same key and the same plaintext (both of 128 bits) proposed in the NIST standard specifications presented in FIPS PUB 197 [7]. However in our experiments, we limit the attack to the last byte of the key. The key and the plaintext used are reported respectively in Table 1 and Table 2.

The encryption process consists into cypher the block of data with the specified key. This is repeated 256 times and in every cycle we vary the plaintext altering the last byte for every possible configuration, from 0x00 to 0xFF. We control and force the changes into the plaintext in order to generate on purpose data-correlation among the sets of measurements. The encryption process is then repeated a modest number of times, in order to have statistical relevance.

The measurements acquired with the oscilloscope amount to 2.713 traces for Nucleo Board and to 15.872 for SEcube™. The traces are collected during the encryption routine. We decided to acquire more measurements on the SEcube™ platform since it should be more secure. In total, the encryption sessions are 16 for the Nucleo board, against 62 for SEcube™. Every power consumption trace contains 10.000 samples.

The robustness of the SEcube™ platform against side-channel analysis has been verified through a real DPA attack experience. Both configurations, Nucleo and SEcube™ Development Board, while encrypting test data are analyzed in order to collect the power consumption traces. To relax the time required for running the data acquisition, the attack was limited to a specific byte, thus only 256 traces in every encryption session.

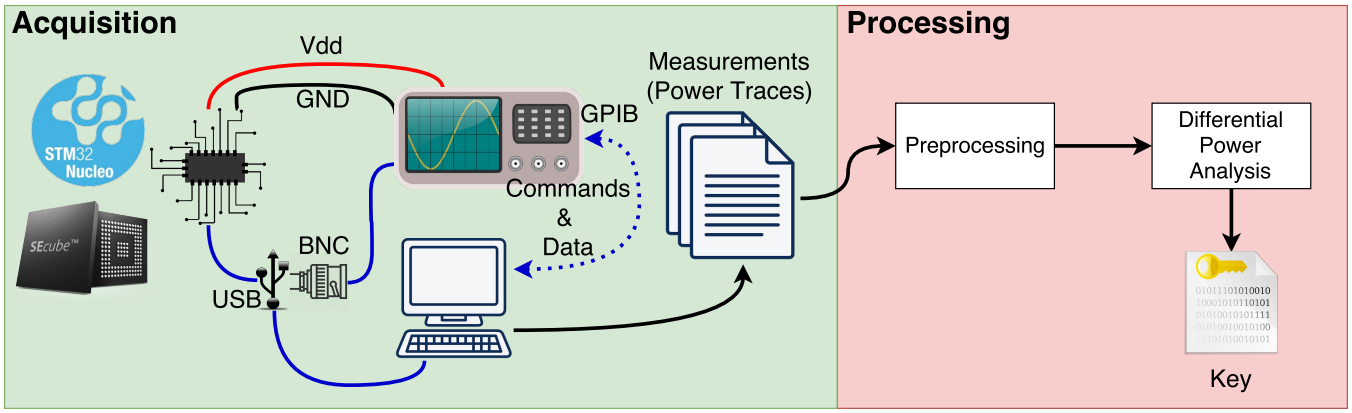

Figure 2. Overview of the workflow adopted

TABLE 3. NUCLEO RESULTS - WRONG BITS IN THE KEY

Nucleo

	No. of Samples	2500	3333	5000	10000
SboxAES	*Hamming Distance*	4	2	2	3
	Hamming Weight	5	3	5	6
	Rising	3	4	4	3
	Average	4	3	4	4
AES	*Hamming Distance*	4	2	5	3
	Hamming Weight	5	3	5	6
	Rising	6	4	6	5
	Average	5	3	5	5

TABLE 4. SECUBE RESULTS - WRONG BITS IN THE KEY

SEcube

	No. of Samples	2500	3333	5000	10000
SboxAES	*Hamming Distance*	4	3	4	4
	Hamming Weight	6	4	3	4
	Rising	1	2	1	5
	Average	4	3	3	4
AES	*Hamming Distance*	5	5	5	5
	Hamming Weight	6	4	3	4
	Rising	5	4	3	2
	Average	5	4	4	4

After the acquisition phase, the traces are preprocessed, parsed and fed to the DPA tool. The analysis has been carried out considering variations on the following parameters:

- Number of samples of each trace: we considered 25%, 30%, 50% and 100% with respect to the full number of samples.
- Type of the Algorithm: we considered the whole AES encryption algorithm and the single S-Box (*SboxAES*).
- Selection Function: Hamming weight (*hweight*), Hamming distance (*hdistance*), Rising

Table 3 and Table 4 present the results from the analysis. Each columns represent the number of samples in every trace. On the rows there are the selection functions considered. Moreover, the results are divided considering whole AES encryption and the single S-Box. The results presented in the various configurations of the parameters state the number of incorrect bits in the last byte of the encryption key. The average of incorrect bits is rounded up and is computed considering the previous configurations. An higher number of bits indicates an unsuccessful attack, which can be interpreted as an enhancement in security.

The reference configuration was attacked first. The results are reported in Table 3. It can be noticed that attacking only the Sbox of the AES the results are slightly better. However, in most cases, just half of last byte of the key is correct. Considering the whole AES, the number of wrong bits increases.

The same attack is performed on the SEcube™ configuration. The results of the analysis are shown in Table 4. Also considering the SEcube™ platform the results are similar. The same considerations applies also.

5. Conclusions

From the results of our analysis it can be seen that on average both platforms provide the same level of security. We can state that after analysing several power consumption traces we were able to discover roughly only half byte of the whole key. This result might lead to improvements when DPA is combined with a brute-force attack. Although the results are similar, in this paper several simplifications are considered. It must be pointed out that the number of traces acquired for the SEcube™ platform is much higher than the one acquired for the Nucleo board. Further investigation is required to achieve more significant results.

6. Acknowledgments

The authors would like to thank Gianfranco Albis and Giuseppe Romano for manufacturing of the measurement circuits presented in this work, professor Alberto Vallan, Riccardo Gassino and Luigi Spagnolo for having provided the measurements equipment.

The present work has been partially supported by CINI Cybersecurity National Laboratory within the project FilieraSicura: Securing the Supply Chain of Domestic Critical Infrastructures from Cyber Attacks (www.filierasicura.it) funded by CISCO Systems Inc.

References

[1] F.-X. Standaert, *Introduction to Side-Channel Attacks*. Boston, MA: Springer US, 2010, pp. 27–42. [Online]. Available: https://doi.org/10.1007/978-0-387-71829-3_2

[2] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5–27, Apr 2011. [Online]. Available: https://doi.org/10.1007/s13389-011-0006-y

[3] *STM32 Nucleo-144 board Data brief*, ST Microelectronics, 3 2017, rev. 6.

[4] *STM32F427xx STM32F429xx Datasheet - production data*, ST Microelectronics, 7 2016, rev. 9.

[5] *TDS5000B Series Digital Phosphor Oscilloscopes - Quick Start User Manual*, Tektronix.

[6] G. D. Natale, M. L. Flottes, and B. Rouzeyre, "An integrated validation environment for differential power analysis," in *4th IEEE International Symposium on Electronic Design, Test and Applications (delta 2008)*, Jan 2008, pp. 527–532.

[7] "Fips pub 197, advanced encryption standard (aes)," 2001, u.S.Department of Commerce/National Institute of Standards and Technology.