Power-based Side-Channel Analysis Against AES Implementations: Evaluation and Comparison

Noura Benhadjyoussef, Mouna Karmani and Mohsen Machhout

Faculty of Sciences of Monastir, Electronics and Micro-Electronics
Laboratory (E.µ.E.L),
University of Monastir, Tunisia

Summary

From an information security perspective, protecting sensitive data requires utilizing algorithms which resist theoretical attacks. However, treating an algorithm in a purely mathematical fashion or in other words abstracting away from its physical (hardware or software) implementation opens the door to various real-world security threats. In the modern age of electronics, cryptanalysis attempts to reveal secret information based on cryptosystem physical properties, rather than exploiting the theoretical weaknesses in the implemented cryptographic algorithm. The correlation power attack (CPA) is a Side-Channel Analysis attack used to reveal sensitive information based on the power leakages of a device. In this paper, we present a power Hacking technique to demonstrate how a power analysis can be exploited to reveal the secret information in AES crypto-core. In the proposed case study, we explain the main techniques that can break the security of the considered crypto-core by using CPA attack. Using two cryptographic devices, FPGA and 8051 microcontrollers, the experimental attack procedure shows that the AES hardware implementation has better resistance against power attack compared to the software one. On the other hand, we remark that the efficiency of CPA attack depends statistically on the implementation and the power model used for the power prediction.

***Keywords*:**

Power analysis (CPA); Advanced Encryption Standard (AES); correlation coefficient; power model; AES implementation.

1. Introduction

Encryption systems have become essential for the security-critical applications such as military, government, and banking systems. These encryption systems are designed to scramble data and keep them safe from prying eyes, but the implementation of such systems is more complicated than the theory itself. In the traditional model of cryptography, cryptographic algorithms provide security against a hacker who has no access to cryptographic devices. However, such model does not always match to the physical implementations realities.

Over the past two decades, new forms of attacks were introduced where a passive hacker observes platform side-channel information in order to recover the key. In fact, software and hardware implementations of these devices leak sensitive correlated information in the form of power consumption, electromagnetic (EM) emissions, time execution, allowing hackers to extract the secret key from cryptographic devices [1]-[4],[21]-[23]. These types of attacks are called Side Channel Analysis (SCA).

In this paper, we explore the power side-channel analysis as a case study. Such attacks, usually, involve demonstrating the relationship between the data being manipulated by a cryptographic device and its instantaneous power consumption.

Simple power analysis (SPA) [5], differential power analysis (DPA) [2],[4], and correlation power analysis (CPA) [7] are three fundamental techniques of power-based SCA attacks. The SPA attack is applicable when the leak is so evident that simple analysis techniques such as visual inspection can disclose the secret information, however the DPA method employs statistical analysis using many power measurements. This work studies the power-based side channel analysis and precisely CPA attack [3], [8], [9],[10]. The CPA analysis uses a set of power measurements of a cryptographic device under attack in order to reveal the secret information by exploiting the correlation with the internal data or internal operations. Indeed, the measured power traces have different statistical distributions that can be exploited because it depends on the operands or the operations. A hacker can reveal secret information by analysing these distributions.

The main contributions of this paper are as follows:

- We firstly present a power based Hacking technique to demonstrate how a power analysis can be used in order to reveal the secret information which is the AES algorithm private key. In our proposed case study, we explain the main methods that can break the security of the AES algorithm by exploiting the CPA Hacking technique.
- We start by illustrating a CPA Hacking technique against AES algorithm using simulated power traces in order to evaluate the CPA Hacking technique difficulty using real measurements.
- We conduct a CPA Hacking technique against software and hardware implementations of the AES algorithm are deeply studied. The representative devices used are the Field Programmable Gate Arrays (FPGA) and the 8051-microcontroller for the hardware and the software implementations respectively.

Manuscript received April 5, 2021
Manuscript revised April 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.4.32

- Finally, based on the needed power traces number and the correlation coefficient values, we elaborate a comparison between the efficiency of CPA Hacking technique against hardware and software implementations.

This paper is organized as follows. In section II, we describe the background knowledge. In Section III, we describe the CPA Hacking technique and existing power model. Section IV presents the CPA Hacking technique on simulated power measurement. The same attacks using real power measurements is then presented in Section V. section VI discuss the results and comparison are discussed in.

2. BACKGROUND

2.1 Advanced Encryption Standard

In 2001, the Advanced Encryption Standard was selected by the National Institute for Standard and Technology (NIST) as the new Encryption standard [11]. This algorithm takes place of the DES algorithm, which had been used since 1976. The AES is a symmetric block cipher and round-based encryption algorithm where the number of rounds depends on the key length: 14 rounds for 256-bit keys, 12 rounds for 192-bit keys and 10 rounds for 128-bit keys. The AES algorithm takes a block with 128 bits' lengths and every data block consists of 4 × 4 array of bytes called the state.

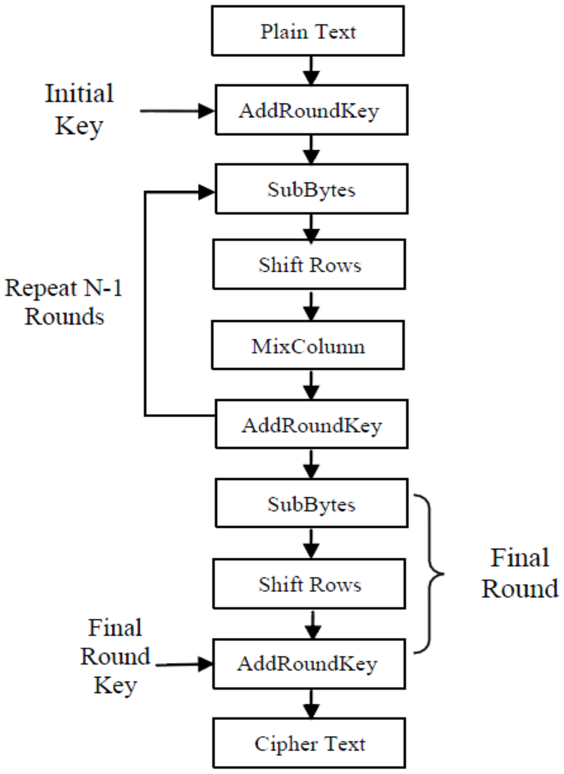

Fig. 1. Simplified block diagram of AES

In this paper, the AES-128-bit (with 128-bit Keys) is used as a case study. The AES-128 bits starts with a single AddRoundKey transformation followed by nine identical rounds. evry round contains 4 different transformations: SubBytes, ShiftRows, MixColumn, and AddRoundKey. The tenth and final round has no MixColumns transformation.

- The SubBytes transformation: is a non-linear substitution operation that replaces each byte with another according to a LUT.
- The ShiftRows transformation: is a linear operation that shifts cyclically the bytes in each row of a state by a certain offset.
- MixColumns: is a linear operation that operates on the state columns in order to combine the 4 bytes in each column.
- AddRoundKey: each byte of the state is combined with the round key derived from the original cipher key using a key expander.

2.2 AES implementations

The AES algorithm may be implemented in hardware or software implementation. The hardware implementation is designed using hardware description languages, like Verilog or VHDL, to run AES on physical technology like FPGAs and ASICs. Typical software implementations such embedded microcontrollers or microprocessors, are designed using programming language.

Generally, AES hardware implementations offer a higher security level compared to their software equivalents. In fact, instructions in the programming language are executed out one by one, this is why the software implementation leakage is very time-dependent and power measurements are less interfered [13, 14] . This makes it relatively easy to extract sensitive information from traces using power models. On the other hand, AES hardware implementations carry out instructions concurrently. Therefore, power measurement from hardware implementations overlap correlation with the secret information, which makes power based side-channel analysis inherently more difficult, especially in advanced technology [15,16].

3. The CPA Hacking techniques

This section presents the CPA hacking techniques overview and describes how to perform such attack in order to retrieve the AES secret key. This considered power-based side channel analysis is presented in Fig.2.

3.1 The CMOS platform power Consumption model

The CMOS still the dominant hardware solution for SoC approach due to its many advantages, including low power requirements, high operating clock speed, density, cost, performance, and manufacturing designer experience

The dynamic power consumption is the dominating part for CMOS gate power consumption [8]. The power consumption (P_D) is expressed as follows:

$$P_D = C_L V_{DD}^2 \, P_{0\rightarrow 1} f \qquad (1)$$

where CL presents the gate load capacitance, P0-->1 denotes probability of data switching from 0 to 1, VDD the supply voltage and f presents the clock frequency

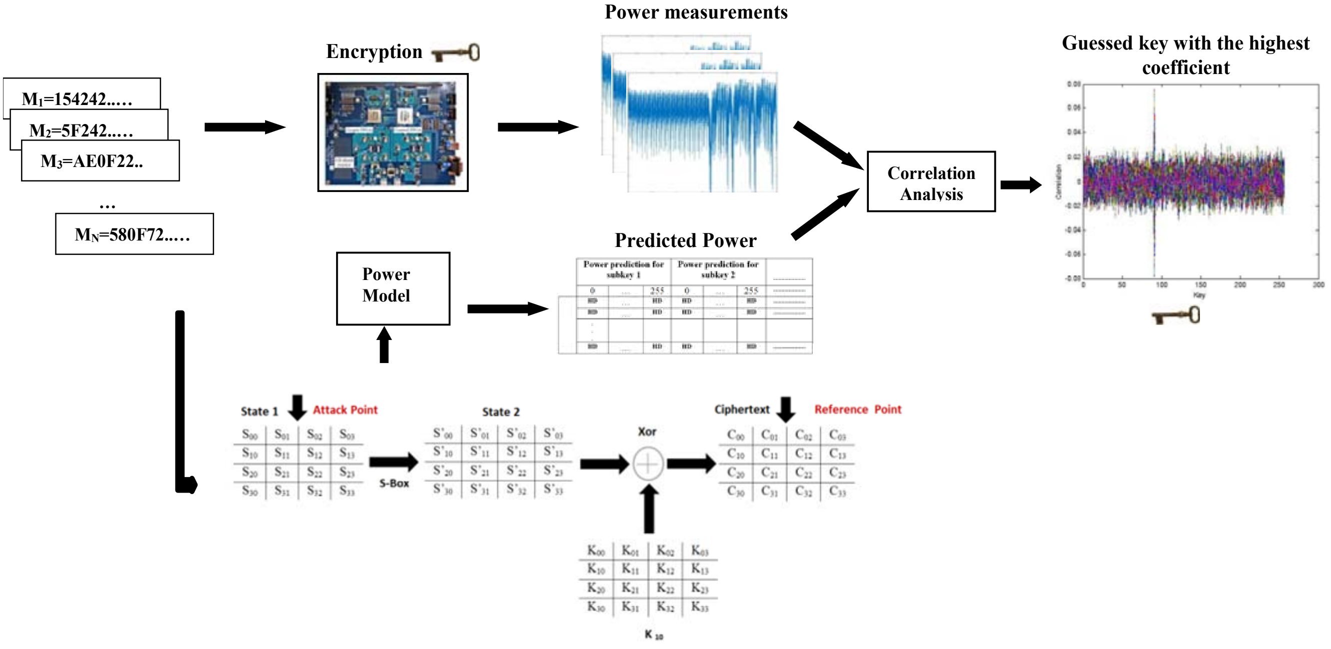

Fig. 2. Power-based- Side-Channel attack on 128-AES

Equation 1 demonstrates that, for CMOS technologies, the power dissipation of a gate depends on its output switches.

After choosing the point attack of the AES algorithm, the CPA attack exploits the information dependency of cryptographic devices power consumption and analyse this power consumption using a large number of power measurements. For example, choosing an 8- bits register as a point attack with R a reference value and X the target data value to be deployed. The power-consumption Y needed to switch from the value R to another value X in this register may be expressed by the equation [17]:

$$Y = \alpha \, H(X \oplus R) + \beta \qquad (2)$$

where $H(X \oplus R)$ is the estimated power consumption when on bit transits from 0 to 1 as from 1 to 0. This estimated power is calculated by the Hamming distance between X and R. β s a term for everything like static power dissipation and α is

scaling factor between the power consumed and the Hamming distance. Considering that the considered 8- bits register has a reference value R equal zero (initial state), the equation (2) will enclose the Hamming weight model as expressed bellow.

$$Y = \alpha \, H(X) + \beta \qquad (3)$$

In this prediction Step, to perform the CPA attack, a hacker selects the point attack (that must depend on the target secret information), and predicts the Y value (i.e. the number of bit switches in the target node). This step is performed for N random AES inputs/outputs and k possible key guesses.

3.2 The power-consumption measurement step

In the second step of the CPA hacking technique, the hacker uses a computer to send known plaintexts to the target cryptographic device, and record the corresponding power measurements. This step must re-uses the same N inputs of the prediction step with the target secret key. The obtained power measurements are normalized using a pre-amplifier and collected by oscilloscope during the AES encryption process.

3.3 The Correlation analysis step

Finally, the hacker analyses the correlation between the theoretical predictions of the power consumption (calculated by the power model) with power measurements of the cryptographic device manipulating the secret key.

The CPA hacking technique uses a Pearson coefficient ρ_{WH} given by Eq.4[6].

$$\rho_{WH} = \frac{\mathrm{cov(W,H)}}{\sigma_W \sigma_H} \tag{4}$$

where W is the power measurement and H denote the power prediction by the power model. This equation satisfies the property: $-1 \leq \rho_{WH} \leq +1$. We consider that we have a high similarity when the correlation value is close to ±1 and a feeble similarity when this coefficient is close to 0. Therefore, the CPA hacking technique is successful when only a unique value, corresponding to the correct sub-key assumption, has the highest correlation coefficient.

4. The Simulated CPA Hacking techniques

The simulated CPA attack, against AES algorithm, uses a simulated power measurement. This simulated attack evaluates the CPA attack difficulty before exploiting real power measurements. To perform this simulated attack, we firstly made N simulated power consumption. To perform this step, we used 100 random AES plain-text and one fixed secret 128-key. These simulated power-measurements are saved in a matrix denoted S.

Secondly, the power consumption of the target 128-AES implementation is predicted using 256 sub-key assumptions. In this simulated attack, we used the initial s-box output as a target point attack. The predicted power consumption calculated by the power model depends on corresponding secret sub-key assumption ranges from 0 to 255 and the plaintext.

In fact, the initial AES round of AES begins by the RoundKey transformation followed by the Subbytes transformation. The Subbytes transformation divides the 128-bit RoundKey output [128-key ⊕ 128-bit plain-texts] into 16 substitution boxes (S-box). Every S-box receipts one byte at input and products one byte at output. Consequently, the assumption of one byte of the key (sub-key) is easy to calculate.

Therefore, using the same AES inputs of the simulated power measurements, we compute predicted power consumption of the target point attack for 256 sub-key guess (256 assumptions: 2^8). While the AES-128bits is used as a case study, this step is repeated 16 times because it must be performed for the 16 S-box (see Fig. 3). At the end, we obtain a predicted power matrix of size N x 256 x 16.

In this step, the Hamming weight model is used where suppose that the point attack is equal zero at the initial moment.

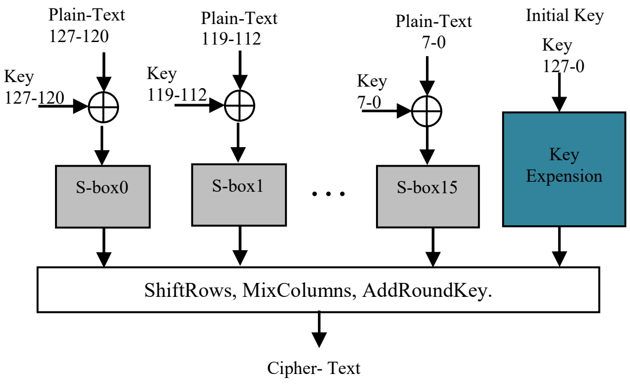

Fig. 3. Simplified diagram of AES

Finally, to reveal the secret key, we compute the correlation coefficients between the predicted power consumption P and the simulated power consumption S. The correlation coefficient obtained by this simulated attack is sown in Fig.4. As shown the highest correlation value corresponds to the first byte of the correct key (first sub-key=66 in our case study) while the correlation coefficient corresponding to the incorrect sub-key assumption remain low.

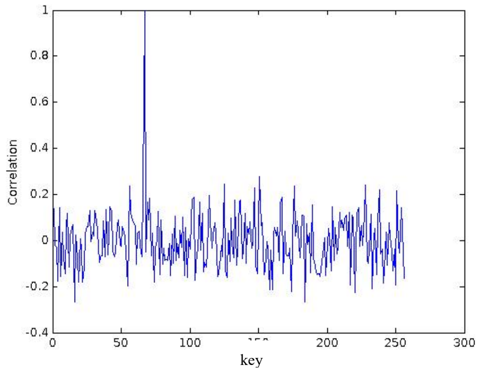

Fig. 4. The correlations trace of the simulated Attack

As presented in Fig.4, the correlations trace demonstrates that the hamming weight model predicts correctly the physical power-consumption

5. The CPA hacking techniques using the measured data

In this section we perform the CPA hacking technique against software and hardware implementations of the AES crypto-core.

5.1 The CPA attack against Software implementation

In this section, we demonstrate the efficiency of the CPA-based side-channel attacks against software implementation of the AES-128bit. The cryptographic devise used as a case study is a 0.18 µm CMOS technology based 8051 8-bit microcontroller [12]. To elaborate the CPA statistical analysis, N plaintexts and their corresponding power traces are exploited. As a first step, we estimate the AES implementation power consumption by the hamming weight power model. The point attack chosen in this attack is the SubBytes output of the first round as demonstrated in Fig. 5.

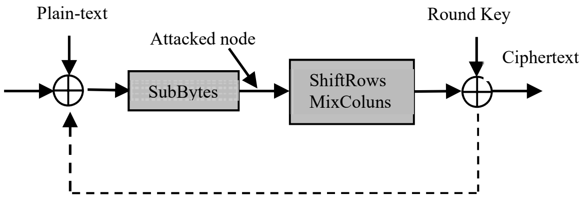

Fig. 5. The CPA Attack point selection step

Secondly, we record the power consumption measurements of the target microcontroller while processing the same plain-texts exploited by the prediction step.

In this CPA attack, the power-measurements were accomplished by the IAIK Institute (Applied Information Processing and Communications).

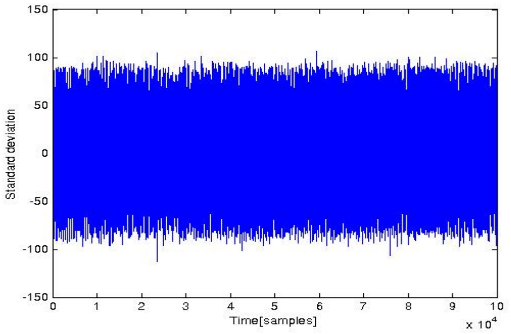

Fig. 6. Power-consumption of the 8051 microcontroller during AES encryption

The 8051 microcontroller power-measurement during the AES encryption process is presented in Fig. 6.

Finally, we calculate the similarity between the real power measurements and predicted power consumption for all 256 sub-key guesses. The experimental result with 200 power measurements is presented in Fig.7. This figure presents the 256 correlation traces between predicted power consumption and real measurements. As indicated, a unique correlation value, corresponding to the correct sub-key assumption (in our case 106), have to a high correlation value. Besides, the correct key assumption regularly stands out with a notable difference leading to a sure verdict of a successful attack.

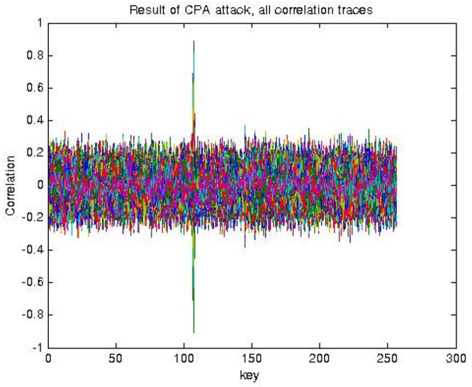

Fig. 7. Correlation coefficient values of CPA against software implementation

The correlation coefficient between predicted power consumption with the correct sub-key assumption (166) and the reel power-measurements is close to '1' as indicated in Fig.7. Therefore, we can assume that these CPA hacking techniques against microcontroller based software implementation can break the security of cryptographic device by revealing secret information like secret key. On the other hand, the hamming weight used as a case study in this attack proves its effectiveness to predict devices power consumption.

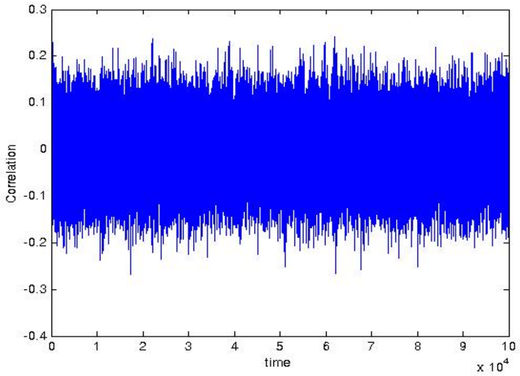

Fig. 8. The Correlation coefficient of an incorrect sub-key assumption.

Fig. 8 corresponds to the correlation of the in-correct sub-key assumption. As shown, the correlation power traces do not reveal the correct secret-key. Indeed, there is no high correlation value in the obtained trace.

5.2 The CPA attack against Hardware implementation

We present in this section how we perform a successful CPA on the FPGA based AES implementation using the Side-channel Attack Standard Evaluation Board (SASEBO). The embedded FPGA is the Xilinx Virtex TM-5 FPGA (XC5VLX30) [19].

The power measurements of this attack were performed by the "DPA contest v2" competition from the COMELEC

Telecom department. Fig. 9 shows the power measurement of the target FPGA during the AES encryption process.

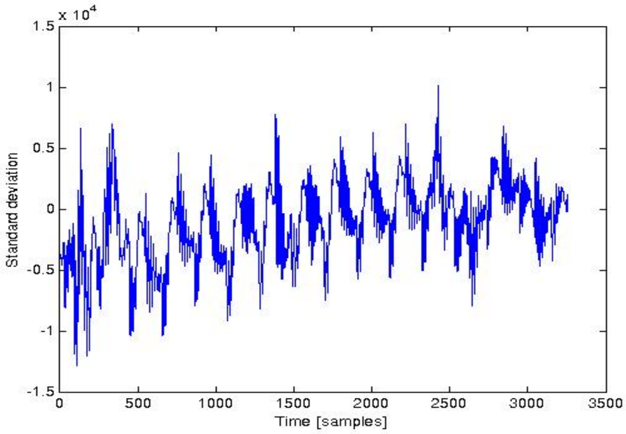

Fig. 9. Average curve of AES

In order to perform CPA attack against the AES hardware implementations, 3000 power measurements are used in a fist experience. The corresponding 3000 AES plain-texts/cipher-text couple are exploited for the statistical analysis.

Contrary to the CPA attack against Microcontroller, the FPGA based attack do not reveal secret key with few measurements number. Indeed, we predict the AES implementation power for all possible attack points. We choose, firstly, the hamming weight power model for the initial and final round, and we compute the similarity between the obtained power predictions and the real power measurement by the correlation procedure. Secondly, the distance Hamming model was used to predict FPGA power consumption. Unluckily, these attempts failed to reveal the secret key. Fig. 10 displays correlation traces with 3000 power measurements.

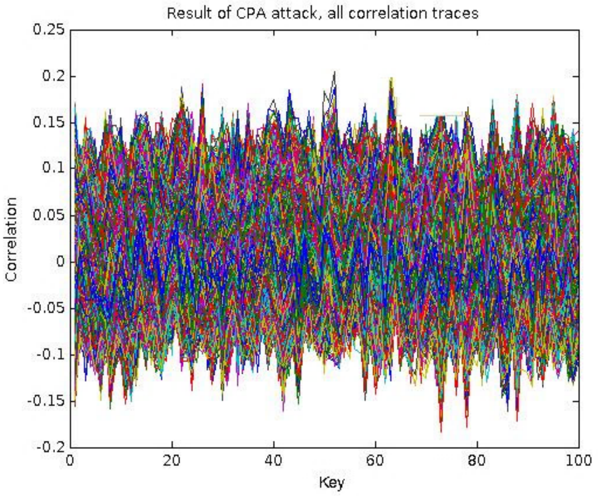

Fig. 10. Correlation values of FPGA based CPA with 3000 traces

As shown in this figure, the correlation power traces do not reveal the correct secret-key. Indeed, there is no high correlation value in the obtained trace. Therefore, we conclude that the CPA attack against hardware implementation using 3000 power measurement is unsuccessful.

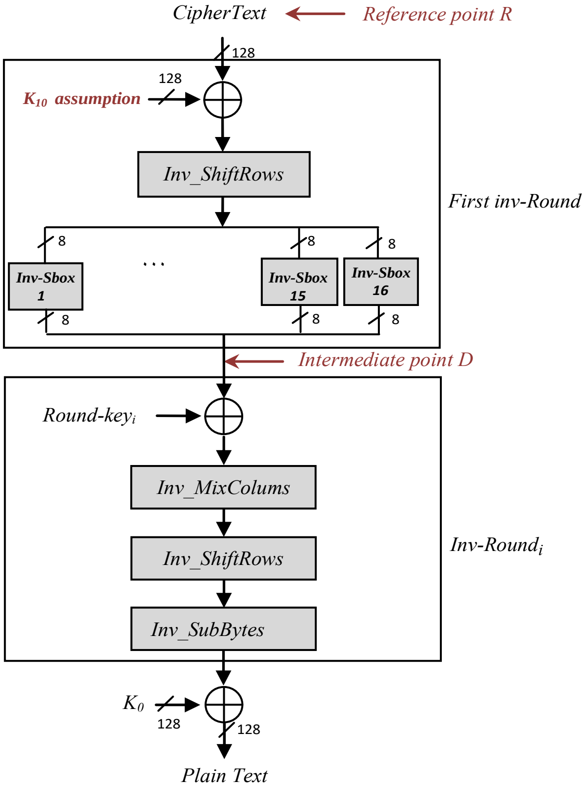

Fig. 12. The CPA Attack point selection at the final round

In the second experience, the same correlation coefficient is calculated for the 256 sub-key assumption using 20000 power measurements. We choose an attack point depend on both the known variable (e.g. the output of S-box) and secret keys K. (see Fig. 11). In fact, the tenth round-encryption is isolated from the other nine rounds and is generally different power signals.

Since the Key schedule of the AES algorithm is invertible, it is easy to calculate the original secret key K0 going backwards. Fig.11 shows the selected intermediate node D defined as the Subbytes transformation output and the reference node R defined as the corresponding Cipher-text. As shown, a unique correlation value, corresponding to the true sub-key assumption, have have the highest correlation coefficient. Therefore, a good decision of the secret key valus may be take unambiguously.

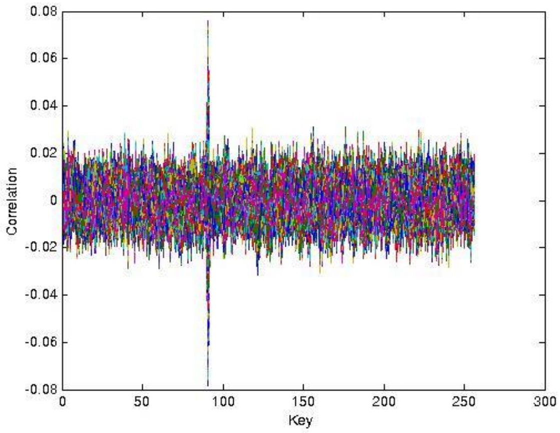

Fig. 13. The CPA attack with 20000 messages

In Fig.14 the maximum correlation coefficient, for all the sub-key assumption, in term of the power traces number was presented. This correlation trace presents the correlation coefficient between the power measurements and predicted power consumption for 20000 numbers of traces.

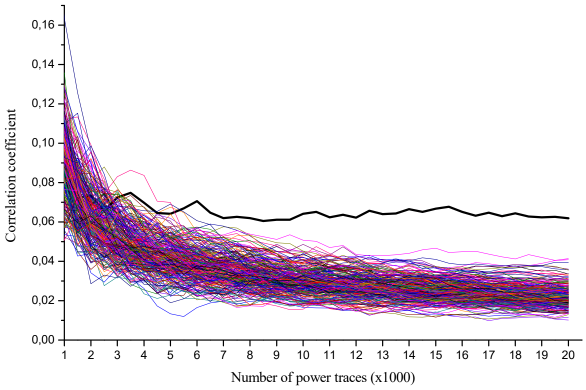

Fig. 14. The correlation values for different number of traces

As shown, the correct sub-key assumption (plotted in black) is distinguished after approximately 6000 traces. This experimental result proves that CPA attack is an efficient power side-channel attack technique to extract the secret key.

6. Results and Comparison

For the 8051-microcontroller based software implementation, usually, few hundred suffice to extract secret key. We guess that between 100 and 200 power measurements are needed to perform a successful attack. However, for the hardware implementation based CPA attack, 3000 traces do not lead to reveal the secret key. Table1 presents the correlation coefficient values for the successful CPAs against Microcontroller and FPGA based AES implementation.

This table gives the highest correlation value and the power measurements number needed to ensure successful CPA attacks against both software and hardware based AES implementations.

Table. 1. CPA Attack on Microcontroller and FPGA: Result and comparison

	Hardware Implementation	*Software Implementation*
Cryptographic Embedded System	*FPGA*	*8051-compatible microcontroller*
Number of power traces	6000	200
Number of samples	5003	5000
correlation coefficient value	0,08	0.916

As illustrated in this table, the FPGA based hardware implementation reduces the probability of successful CPA attacks. In fact, the CPA attack against Microcontroller based AES implementation can reveal the secret sub-key using only 200 power measurements whereas the CPA attack against FPGA based AES implementation reveal the secret sub-key using 6000 power-measurements. Therefore, we conclude that the attack success depends on the device used for the implementation and the number of power measurements as well.

7. Conclusions and future work

Power based side channel attacks become a realistic threat for hardware and software implementations of cryptographic algorithms. In this paper, we present a detailed power based Hacking technique to demonstrate how the power analysis can be exploited to reveal the AES secret key. In the proposed case study, we explain the main techniques that can break the security of the considered AES design by using the powerful CPA attack.

The obtained CPA results show that by analysing the correlation coefficient value and the power measurement number needed to retrieve the secret key, the FPGA based hardware implementation of the AES has less data-dependent power leakages compared to ITS software implementation. In our future work, we aim to enhance CPA hacking techniques by exploiting new techniques like deep-learning models.

References

[1] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering, IEEE J. Solid-State Circuits, 54(2) , (2019), pp. 569–583.

[2] D. Das and S. Sen, Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach,"Cryptography, 4(4), p. 30,(2020).

[3] P. Kocher, J. Jaffe, B. Jun, Differential Power Analysis, Crypto 1999, LNCS, 1666, Santa-Barbara, CA, USA, (1999), pp 398-412.

[4] D. Agrawal, B. Archambeault, J. Rao, P. Rohatgi, The EM Side-Channel(s), CHES 2002, LNCS, 2523, , Redwood City, CA, USA, August (2002), pp 29-45.

[5] N. Benhadjyoussef, M. Karmani, and H. Mestiri, Power Analysis for

Smartcard's Authentication-Protocol, 2019 International Conference on Advanced Systems and Emergent Technologies (IC_ASET), Hammamet, Tunisia, (2019), pp. 268-272.

[6] J. Kundrata, D. Fujimoto, Y. Hayashi and A. Barić, "Comparison of Pearson correlation coefficient and distance correlation in Correlation Power Analysis on Digital Multiplier," 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, (2020), pp. 146-151,

[7] Brier, C. Clavier, and F. Olivier, Correlation Power Analysis with a Leakage Model BT - Cryptographic Hardware and Embedded Systems - CHES 2004, (2004), pp. 16–29.

[8] Yongdae Kim, Takeshi Sugawara and Naofumi Homma. Biasing power traces to improve correlation in power analysis attacks, First International Workshop on Constructive Side-Channel Analysis and Secure Desig, COSADE (2010).

[9] Neil Hanleyy, Robert McEvoyy and Michael Tunstally, Correlation Power Analysis of Large Word Sizes. ISSC (2007).

[10] N. Benhadjyoussef, M. Machhout and R. Tourki, "Optimized power trace numbers in CPA attacks," Eighth International Multi-Conference on Systems, Signals & Devices, Sousse, Tunisia, (2011), pp. 1-5,

[11] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), FIPS Publication 197, (2001).

[12] Stefan Mangard, Elisabeth Oswald, Thomas Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards", (2007)

[13] Wang, H. and E. Dubrova. "Tandem Deep Learning Side-Channel Attack Against FPGA Implementation of AES." IACR Cryptol. ePrint Arch. 2020 (2020).

[14] H. Maghrebi, T. Portigliatti, and E. Prouff, "Breaking cryptographic implementations using deep learning techniques," in International Conference on Security, Privacy, and Applied Cryptography Engineering, pp. 3–26, (2016)

[15] F.-X. Standaert, E. Peeters, G. Rouvroy, J.-J. Quisquater, An Overview of Power Analysis Attacks against field programmable gate arrays, 94(2), (2006).

[16] F.-X. Standaert, S.B. Ors, B. Preneel, Power Analysis of an FPGA Implementation of Rijndael: is Pipelining a DPA Countermeasure? in the proceedings of CHES 2004, Lecture Notes in Computer Science, vol 3156, Boston, USA, (2004) , pp 30-44.

[17] Eric Brier, Christophe Clavier and Francis Olivier. Optimal statistical power analysis. Cryptology ePrint Archive, Report 2003/152, 2003.

[18] P.Holambe, H.D. Zodpe, Cryptanalysis of AES using FPGA Implementation, International Journal of Engineering Trends and Technology (IJETT), 31(2), January (2016), Page 54.

[19] Research Center for Information Security, "Sidechannel Attack Standard Evaluation BOard (SASEBO),"

[20] "DPA Contest v2, http://www.dpacontest.org /v2.

[21] D. Das, J. Danial, A. Golder, S. Ghosh, A. R. Wdhury and S. Sen, "Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS," IEEE Custom Integrated Circuits Conference (CICC), Boston, MA, USA, (2020), pp. 1-4.

[22] N. Benhadjyoussef, H. Mestiri, M. Machhout and R. Tourki, "Implementation of CPA analysis against AES design on FPGA," 2012 International Conference on Communications and Information Technology (ICCIT), Tunisia, (2012), pp. 124-128.

[23] Turki F. Al-Somani, M. K. Ibrahim, High Performance Elliptic Curve GF(2m) Cryptoprocessor Secure Against Timing Attacks, IJCSNS International Journal of Computer Science and Network Security, Vol. 6 No. 1 pp. 177~183, 2006

[24] M. Petrvalsky, M. Drutarovsky and M. Varchola, "Differential power analysis attack on ARM based AES implementation without explicit synchronization," 2014 24th International Conference Radioelektronika, Bratislava, Slovakia, (2014), pp. 1-4

Noura Benhadjyoussef received his engineering degree in electrical engineering from the National Engineering School of Sousse, Tunisia, in 2008, the Master degree in Electronic Engineering from National Engineering School of Sousse, Tunisia, in 2010 and the Ph.D. degrees in electrical engineering from National Engineering School of Monastir, Tunisia, in 2016. Dr Benhadjyoussef is currently Associate Professor in electronics and microelectronics at the Faculty of Sciences of Monastir, University of Monastir, Tunisia. His research interests include Architectural Synthesis for the Crypto-systems, physical cryptanalysis, and smartcard security.

Mouna Karmani received his engineering degree in electrical engineering from the National Engineering School of Sfax, Tunisia, in 2005, the Master degree in safety and security of industrial systems from the Higher Institute of Applied Sciences and Technology of Sousse, Tunisia, in 2007 and the Ph.D. degree in electronics from the Faculty of Sciences of TUNIS, Tunisia, in 2015. Dr Karmani is, currently, an Associate Professor in electronics and microelectronics at the Faculty of Sciences of Monastir, University of Monastir, Tunisia. His research interests include digital, analog and mixed signal circuit VLSI design and testing, fault-Tolerant and secure embedded systems.

Mohsen Machhout received MS and Ph.D. degrees in electrical engineering from University of Tunis II, Tunisia, in 1994 and 2000 respectively. Dr Machhout is currently Full Professor at University of Monastir, Tunisia. His research interests include implementation of standard cryptography algorithm, key stream generator and electronic signature on FPGA and ASIC, security of smart card and embedded system with resource constraints.