Attacking AES Implementations Using Correlation Power Analysis on ZYBO Zynq-7000 SoC Board

Petr Socha, Jan Brejník, Matěj Bartík
Czech Technical University in Prague
Faculty of Information Technology
{sochapet,brejnjan,bartimat}@fit.cvut.cz

***Abstract*—Differential power analysis (DPA) and its enhanced variant, correlation power analysis (CPA), are one of the most common side channel attacks today. A dedicated hardware platform is often used when performing this kind of attack for experimental purposes. In this paper, we present the modifications of a common ZYBO board, that are necessary to perform the CPA attack. We illustrate the whole process of attacking both software and hardware implementations of AES-128 and we present our experimental results.**

Keywords-side channel attack; AES; differential power analysis; correlation power analysis; ZYBO; Zynq; SoC

I. INTRODUCTION

Cryptography has been evolving for thousands of years now, as a way to secure confident information against third party. We are surrounded by computers and communication networks in today's world, and cryptography is an essential part of our lives. Nowadays cryptographic systems include many diverse embedded devices, such as smartcards used e.g. for identification or for prepaid services, various IoT applications or even smart cars. Cryptanalysis developed alongside cryptography, analyzing existing cryptosystems and attempting to reveal secret information without appropriate privileges (e.g. without knowledge of the decryption key).

While many ciphers currently in use (such as AES) are considered mathematically secure, their implementations may be vulnerable to side channel attacks, such as differential power analysis [1] or its enhanced variant, correlation power analysis [2,3]. This kind of attack exploits the fact that an intermediate value is processed in the implementation, that correlates with power consumption of the device, and with some other known information (e.g. plaintext or ciphertext).

We would like to compare various AES implementations on the Xilinx Zynq-7000 SoC platform regarding their side channel attack resistance using correlation power analysis. The used Zynq chip contains Xilinx 7-Series FPGA logic (equivalent to Artix-7) and a dual-core ARM Cortex-A9 processor. The architecture of the Zynq platform allows to explore cryptographic behavior on several levels of (programming) abstraction.

II. THEORETICAL BACKGROUND AND RELATED WORK

A. AES/Rijndael Symmetric Block Cipher

Rijndael algorithm has been adopted as a new Advanced Encryption Standard (AES) by the government of the United States of America when DES (Data Encryption Standard) has been found insecure and obsolete. AES was standardized by the National Institute for Standards and Technology (NIST) as the FIPS-197 standard [4].

The 128-bit AES encryption consists of the *Key expansion* (where a cipher key is expanded into 11 round keys, first one being the cipher key) and the initial (zero) round, followed by 10 rounds. In the initial round, the *AddRoundKey* operation is performed, i.e. the plaintext is xored with the first round key, which is equal to the cipher key. This value becomes the cipher state. After the initial round, ten rounds follow, altering the current cipher state. Each round consists of four operations: *SubBytes* (i.e. a non-linear 8-bit substitution, so-called S-Box), *ShiftRows* (i.e. a circular shift), *MixColumns* (i.e. a linear transformation) and *AddRoundKey*. In the last round, the *MixColumns* operation is skipped.

Moreover, 192-bit and 256-bit key length variants of AES exist, consisting of 12 or 14 rounds respectively.

B. Correlation Power Analysis

A side channel attack does not exploit the mathematical properties of the cipher. Instead, it targets the implementations, where processed data may be leaked e.g. through power consumption or electromagnetic radiation. Differential power analysis (DPA) was introduced in [1] and [5], as a side channel attack applicable to many block ciphers including DES or AES. Enhanced variant of DPA, called correlation power analysis (CPA), was presented in [2,3,6]. While DPA focuses on attacking a single (or multiple) bit of a cipher key at a time, CPA attacks a larger portion of a key (e.g. a byte).

The correlation power analysis (CPA) attack is based on measuring power consumption of the device. It depends on the fact, that an intermediate value is processed in the implementation, that correlates with power consumption, with the plaintext or ciphertext used, and with a part of the cipher key. Fig. 1 shows a possible power measurement setup when performing the CPA attack.

This research has been partially supported by the grant GA16-05179S of the Czech Grant Agency, "Fault-Tolerant and Attack-Resistant Architectures Based on Programmable Devices: Research of Interplay and Common Features" (2016-2018) and CTU project SGS17/213/OHK3/3T/18.

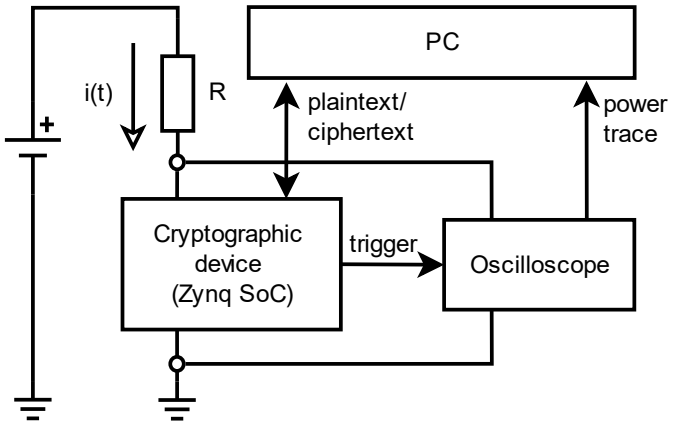

Figure 1. Measurement setup when performing the CPA attack. The shunt resistor R works as a current measuring device.

We sample power consumption of the device during the whole encryption, since we typically do not know the precise time when power consumption correlation appears. To trigger the measurement, a dedicated signal is often implemented. We call the collection of *m* samples obtained during one encryption a power trace.

The attacked cryptographic device is fed with *n* random plaintexts, capturing the ciphertexts if needed. Let us assume that we attack 128-bit AES, where the CPA attack focuses on attacking a byte of the key at a time. For every plaintext/ciphertext used during measurement, there are *256* possible power consumption candidates, based on one of the *256* possible values of the byte of the cipher key. We call these $n \times 256$ values, for every measurement done, a power model.

Obtaining the power model based on the implementation and plaintexts or ciphertexts used is discussed later in Section III.

Let us assume that power consumption of the device, at a single sampling time, is a random variable *X*. The measurements, as described earlier, then give us *m* random variables, one for each sample point in the power trace: $\{X_i(j) \mid \forall i, j: 0 \le i < m, 0 \le j < n\}$. Let us assume that the power model, as described earlier, is a set of *256* random variables representing the expected power consumption, one variable for each key candidate: $\{Y_i(j) \mid \forall i, j: 0 \le i < 256, 0 \le j < n\}$.

Computing the Pearson correlation coefficient between each *X* variable (every sample point in the trace) and each *Y* variable (every key candidate) gives us a correlation matrix *C* with dimensions $m \times 256$. Searching for the maximum or minimum Pearson correlation coefficient in the matrix *C* should reveal the right key candidate, according to the maximum likelihood principle. This search may fail if the number of obtained power traces (*n*) is insufficient.

Practical approach to the CPA attack and various aspects of side channel attacks are discussed in [7,8,10,11].

C. Xilinx Zynq & Digilent ZYBO Platform

The platform selected for our experimental work is the Digilent ZYBO development board [12], featuring Xilinx Zynq-7000 SoC [19]. This chip integrates Xilinx 7-series programmable FPGA logic, dual-core ARM Cortex-A9 processor, on-chip memory, external memory interfaces or I/O peripherals. The integrated feature-rich dual-core ARM processor also provides support for SIMD and vector floating-point instruction set Cortex-A9 NEON, useful for the AES encryption acceleration.

III. Proposed Experiment

We focused on AES (128-bit variant) implemented in embedded systems, using CPA for attacking a byte of the AES cipher key at a time. We selected the Digilent ZYBO [12] development board for performing our experiments. The ZYBO board had to be modified to provide support for side channel attacks. The features of the Zynq platform allow us to compare many various implementations on different levels of abstraction in the matter of their side channel attack resistance:

- native VHDL implementation,
- AXI4 peripheral block,
- native C software implementation using Xilinx SDK,
- optimized software implementation using the ARM NEON instruction set.

Our approach has the advantage of the results being directly comparable to each other, since all the implementations, both hardware and software, run in the same packaged chip and the same environment; unlike existing experiments done on various chips from various vendors [13].

A. Modifications of ZYBO Board

The Digilent ZYBO Zynq-7000 ARM/FPGA SoC Trainer Board is not intended for cryptanalysis applications. Therefore, certain changes to the board must be done in order to successfully perform the CPA attack on the deployed Zynq chip.

The difference in power consumption of the device, for different plaintext and key values, may be very subtle. Any decoupling capacitors near the chip need to be removed. Namely, capacitors C121-C124, C148-C162 were all removed.

As depicted in Fig. 1, a shunt resistor needs to be deployed in order to measure power consumption (i.e. the electrical current) of the device. This is done by replacing original 0 Ω resistor R265 with the resistor 0.1 Ω.

Approximately 10 Ω resistor is used when attacking a pure FPGA chip (e.g. Spartan-3E or Artix-7) [14,15]. In our case, the Zynq SoC, with both FPGA logic and dual-core processor, has much bigger static power consumption, therefore only 0.1 Ω resistor is used.

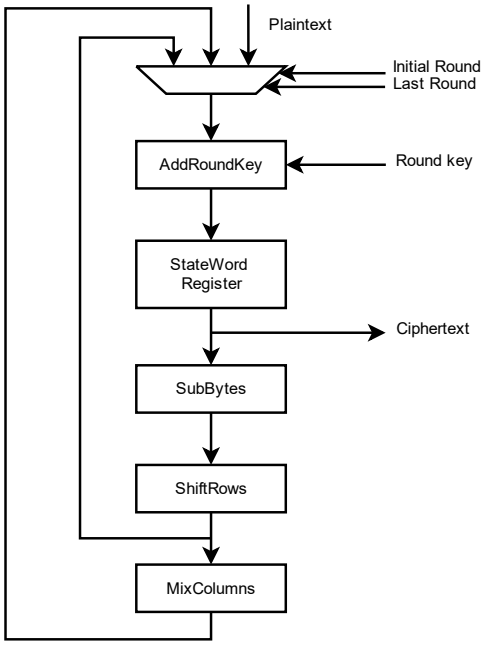

Figure 2. Hardware architecture of the AES encryption.

B. SW Implementation Power Consumption Model

As mentioned earlier, 128-bit AES encryption consist of the initial round, where *AddRoundKey* (i.e. a bitwise xor) is performed, followed by ten rounds consisting of these four operations: *SubBytes* (i.e. a non-linear 8-bit substitution, so-called S-Box), *ShiftRows* (i.e. a circular shift), *MixColumns* (i.e. a linear transformation). In the last round, the *MixColumns* operation is skipped [4].

Attacking the software implementation of 128-bit AES exploits the knowledge of the cipher implementation and the knowledge of the plaintext used [16,17]. With the knowledge of the plaintext, one can easily perform the initial *AddRoundKey* operation on a single byte (giving out *256* possibilities) and the first *SubBytes* operation. The *SubBytes* operation is performed for each byte separately (which is why the CPA attacks a byte at a time) and is usually implemented as a memory look-up table. The **Hamming weight** of this result is assumed to correlate with power consumption of the device, since we presume that consumption of the memory buses is dominant.

C. HW Implementation Power Consumption Model

Attacking the FPGA implementation of 128-bit AES is more difficult. This is because power consumption of the CMOS circuit depends on the transitions made (0 to 1, or 1 to 0), rather than on the immediate value of the signal. The RTL architecture of the AES round is depicted in Fig. 2.

In this case, the CPA attack focuses on the *StateWord Register* at the time of the last round and is based on the knowledge of the ciphertext [7,17]. The ciphertext represents the value of the *StateWord Register* after the last round. As mentioned earlier, in the last round, the *MixColumns* operation is skipped. Performing the inverse *ShiftRows* and the inverse *SubBytes* operations on the selected byte and guessing a byte of the key, one receives *256* possible values, that were in the *StateWord Register* in the previous round. Computing the **Hamming distance** between the value that was in the register after the last round (the cipher text), and the guessed *256* values from the previous round, we obtain the expected power consumption model based on the transitions made on the *StateWord Register*.

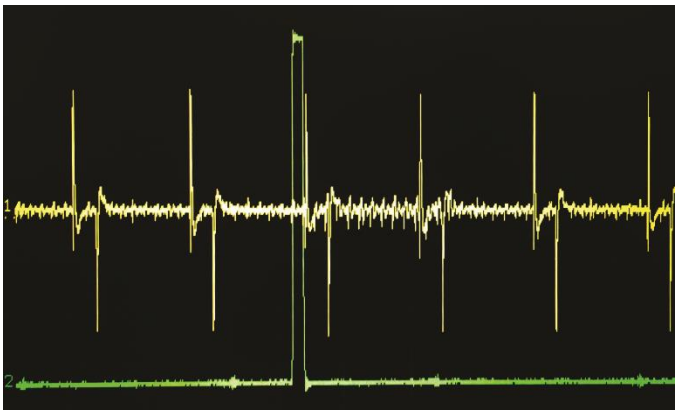

Figure 3. Input signals of the oscilloscope. The yellow line (1) is power consumption of the Zynq chip, with a visible noise. The green line (2) is a trigger signal, signaling the beginning of the encryption.

IV. Experimental Results

The measurement setup is depicted in Fig. 1, with cryptographic device being the ZYBO Zynq board, modified as described in Section III-A, and shunt resistor placed in the Vdd path.

We placed a 30dB wideband signal amplifier BGA2869 [18] at the input of the oscilloscope, since the power consumption differences may be very subtle. The oscilloscope used was Agilent DSOX3012A, set in DC 50Ω mode, with sampling frequency 2 GSa/s.

A. Signal Noise

While capturing the power traces, we have experienced an unwanted noise in a form of voltage spikes with frequency approximately 660 kHz. Unfortunately, we have not conclusively identified the source of this noise and we have not been able to eliminate it. This noise can be seen in Fig. 3.

B. Attacking FPGA Implementation

Our AES implementation in the Zynq SoC FPGA runs at 5 MHz. With 11 clock cycles needed, the whole encryption is done within 2200 ns. Due to that, approximately two asynchronous noise spikes (as described earlier) occur per a power trace. Performing the attack with these power traces without any further processing lead to a failure.

Identifying the position of the last round, which we aim to attack with our power model, we have been able to crop the power traces and filter out the traces containing the unwanted

noise. From 40,000 originally measured power traces, we have algorithmically selected 15,000 power traces with the last round unspoiled. From these, only 5,000 power traces were necessary to successfully perform the attack and recover the last round key. From a last round key, the original cipher key can be easily derived.

C. Attacking ARM Implementation

The software implementation written in C using Xilinx SDK, which we run on the ARM processor inside the Zynq SoC, takes approximately 2 ms to encrypt the plaintext, which means it is approximately 900× slower, than the FPGA implementation. This also means that the number of power spikes present in the power trace is approximately 900× bigger.

We have not managed to recover any bytes of the cipher key using these power traces. Our attempts were not successful even when using a simple spike detection method and a selective correlation computation, where disturbed samples were not taken into the account.

V. Future Work

To give a sound comparison of all the implementations we have prepared, a more suitable development board is necessary. Such a development board should preferably feature low-noise power supplies and a minimum of unnecessary components capable of producing noise.

VI. Conclusion

We have presented steps necessary to perform a side channel attack, namely the correlation power analysis, on a generic hardware platform such as Digilent ZYBO board. We have also designed the AES implementations on different levels of abstraction, including both hardware and software implementations, in order to compare their side channel attack resistance. All these implementations are capable of running on the same Zynq SoC chip, making the results of the CPA side channel attack directly comparable to each other.

We have successfully managed to recover the cipher key when attacking the last round of the FPGA implementation. This attack was successful even using the ZYBO board as a deployment platform, with minimal modifications made, and despite the present noise.

Unfortunately, we have not recovered any bytes of the key when attacking the software implementation run on the ARM in the Zynq SoC. This was due to the massive noise present in the measured power traces, possibly caused by the power supply.

References

[1] P. Kocher, J. Jaffe, and B. Jun, Differential Power Analysis. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[2] B. den Boer, K. Lemke, and G. Wicke, "A dpa attack against the modular reduction within a crt implementation of rsa," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2002, pp. 228–243.

[3] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2004, pp. 16–29.

[4] J. Daemen and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[5] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of power analysis attacks on smartcards." Smartcard, vol. 99, pp. 151–161, 1999.

[6] T.-H. Le, J. Clédière, C. Canovas, B. Robisson, C. Servière, and J.-L. Lacoume, "A proposition for correlation power analysis enhancement," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2006, pp. 174–186.

[7] V. Miškovský, H. Kubátová, and M. Novotný, "Influence of fault-tolerant design methods on differential power analysis resistance of aes cipher: Methodics and challenges," in Embedded Computing (MECO), 2016 5th Mediterranean Conference on. IEEE, 2016, pp. 14–17.

[8] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A statistics-based fundamental model for side-channel attack analysis." IACR Cryptology ePrint Archive, vol. 2014, p. 152, 2014.

[9] F.-X. Standaert, P. Bulens, G. de Meulenaer, and N. Veyrat-Charvillon, "Improving the rules of the dpa contest." IACR Cryptology ePrint Archive, vol. 2008, p. 517, 2008.

[10] F.-X. Standaert, T. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks." in Eurocrypt, vol. 5479. Springer, 2009, pp. 443–461.

[11] A. Moradi, "Advances in side-channel security," Habilitation, Ruhr-Universität Bochum, 2015

[12] Digilent, "Reference manual, zybo rev," 2014.

[13] N. Bochard, C. Marchand, O. Pet'ura, L. Bossuet, and V. Fischer, "Evariste iii: A new multi-fpga system for fair benchmarking of hardware dependent cryptographic primitives," in Workshop on Cryptographic Hardware and Embedded Systems, CHES 2015, 2015.

[14] M. Bartik and J. Buček, "A low-cost multi-purpose experimental fpga board for cryptography applications," in Advances in Information, Electronic and Electrical Engineering (AIEEE), 2016 IEEE 4th Workshop on. IEEE, 2016, pp. 1–4.

[15] L. Mazur and M. Novotný, "Differential power analysis on fpga board: Boundaries of success," in Embedded Computing (MECO), 2017 6th Mediterranean Conference on. IEEE, 2017, pp. 1–4.

[16] A. Schuster and E. Oswald, "Differential power analysis of an aes implementation," Institute for Applied Information Processing and Communications, Graz University of Technology, Tech. Rep. IAIK-TR, vol. 6, p. 25, 2004.

[17] M. Alioto, M. Poli, and S. Rocchi, "A general power model of differential power analysis attacks to static logic circuits," IEEE transactions on very large scale integration (VLSI) systems, vol. 18, no. 5, pp. 711–724, 2010.

[18] NXP Semiconductors, "Bga2869 product datasheet," 2015.

[19] Xilinx, "Zynq-7000 all programmable soc technical reference manual.," 2017.

.