Differential Power Analysis on FPGA board: Boundaries of Success

Lukáš Mazur and Martin Novotný
Faculty of Information Technology
Czech Technical University in Prague
Thákurova 9, 160 00 Prague, Czech Republic
{mazurluk, novotnym}@fit.cvut.cz

Abstract— **Differential Power Analysis (DPA) is a contemporary method able to break cryptographic device via measuring and analyzing its power consumption. The success rate of the DPA method strongly depends on the measurement setup. We have investigated and evaluated the influence of measurement setup on the success rate of DPA attack against FPGA board running AES encryption. From our findings it follows that removing decoupling capacitors plays major role in success rate of the DPA attack. Replacing standard switched-mode power supply with accumulators and linear stabilizers simplifies the attack, however, its effect is not that significant.**

***Keywords**- Side Channel Attacks, Differential Power Analysis, DPA, Advanced Encryption Standard, AES*

I. Introduction

The cryptanalysis can be divided into three types: classical cryptanalysis, social engineering attacks, and side channel attacks [1]. Even the cryptographic systems based on mathematically strong ciphers may be vulnerable to side-channel attacks, as these attacks are mounted on the implementation rather than the cipher itself. Differential power analysis (DPA), introduced by Paul Kocher et al. in 1999 [2], is based on the idea that power consumption of the cryptographic device is linked to the data being processed [3]. By measuring the power consumption we can reveal the secret key.

The success rate of the DPA method strongly depends on the measurement environment – e.g., switched-mode power supply may generate noise hiding the power consumption trace, decoupling capacitors may remove power consumption peaks, etc. To investigate and evaluate the influence of measurement setup on the success rate of the DPA attack on FPGA board, we created an implementation of AES cipher for Spartan 3E Starter Board [4]. We experimented with two such boards, one standard and one with removed decoupling capacitors. For power supply we used either standard switched-mode power supply delivered with board, or the accumulators and linear stabilizers. In this paper we present results of our observations.

A. Differential Power Analysis

The DPA attack takes two steps. At first, we capture the power traces from the cryptographic device, and then we run the analysis on those traces. In the first step, we are sending different plaintexts to the cryptographic device, capturing the power traces, and storing the received ciphertexts from the cryptographic device. It is necessary to have ciphertext for each trace to successfully perform the attack [5].

In the second step, we run the analysis. The analysis begins by creation of the key hypothesis. During the creation of the key hypothesis we compute the hypothetical consumption for each value of the given byte of a key. Different consumption models can be used. The most commonly used models are Hamming weight and Hamming distance [6]. The key hypothesis is then correlated with obtained traces. From the result, we should be able to get the correct key and also the number of sample where the encryption operation took place in. The correct key hypothesis does not necessarily need to have the highest (or the lowest) value of correlation coefficient from all the key hypotheses, but its plot should be somewhat different from the others. Visual inspection of the result of the analysis is thus necessary.

DPA can be used against any block cipher. In our experiment we used the AES encryption algorithm [7, 8] with 128 bit key. We can mount the attack either against the first round or the last round in the case of AES. We tried both options, and we were successful with the attack against the last round.

II. AES Design

We implemented iterative design which performs one round of AES algorithm per one clock cycle. The encryption takes 11 clock cycles (1 clock cycle is used for the initial preparation, and 10 clock cycles are used for the actual encryption). The design is clocked at the frequency 1.5625 MHz. The diagram of the design can be seen in Fig. 1. To simplify alignment of power traces, the AES controller generates additional triggering pulse on dedicated pin prior the encryption.

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).

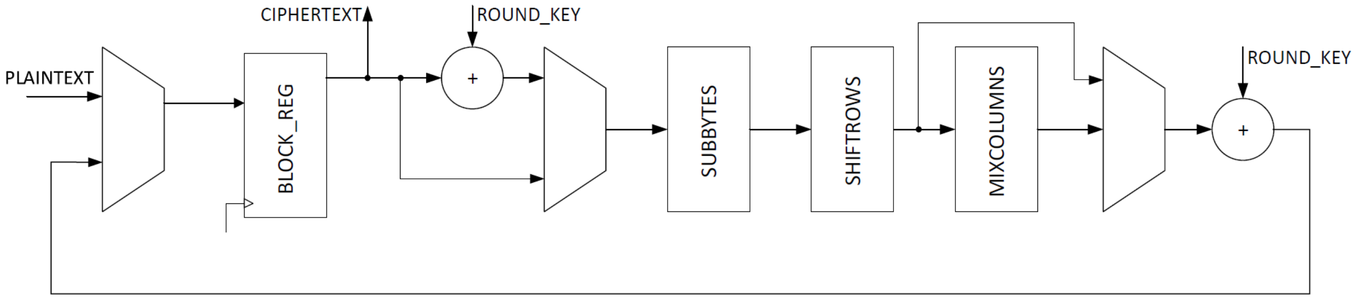

Figure 1. Diagram of AES design.

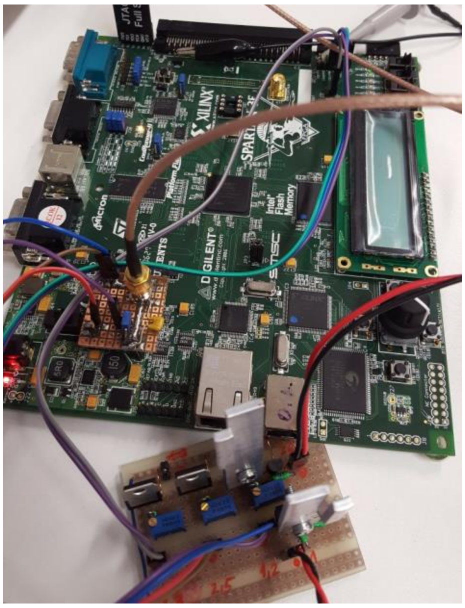

Figure 2. FPGA board powered by accumulators via linear stabilizers.

III. FPGA Board Modifications

We have decided to use the Spartan 3E Starter Board [4] as a device under attack. We made two modifications of the board with the aim to investigate the resistance of different board configurations against DPA – a) we removed decoupling capacitors on the 1.2 V power supply of the FPGA core and b) we replaced the switched-mode power supply with accumulators.

We removed capacitors C158-C175 as proposed in [9]. The capacitors are located around the FPGA chip, or next to the connector JP7. When powering the board from accumulators, we used linear stabilizers providing all the necessary voltages (i.e. 1.2 V, 2.5 V, and 3.3 V). The photo of the connection can be seen in Fig. 2.

IV. Measurement Setup

We used Agilent MSO7104A [10] oscilloscope having four channels, bandwidth 1 GHz and sampling frequency 4 GSa/s. Lately, we found out that we did not need such a high sampling frequency, because the more samples, the slower the key computation is. We were able to recover the correct key with just 16400 samples per trace. We used an AC preamplifier PA 303 BNC by Langer EMV-Technik (with gain 30 dB) [11]. The diagram of the measurement setup with the AC preamplifier can be seen in Fig. 3. The oscilloscope settings used for the successful attack were as follows: input: DC coupling, 50 Ω (this was required by the AC preamplifier), bandwidth limit: on, resolution: 360 mV per division.

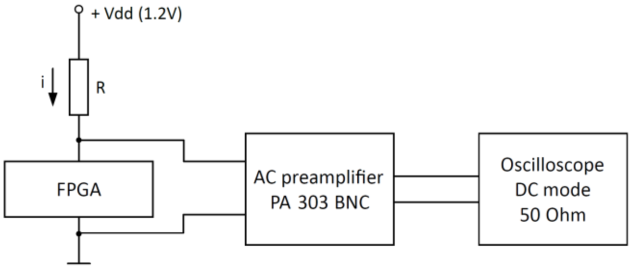

Figure 3. Diagram of the measurement setup with AC preamplifier.

TABLE I. FPGA board configurations for DPA attack

Decoupling Capacitors	Power Source	# traces needed for successful attack
Removed	Accumulators	5,000
Removed	Switched-mode power supply	30,000
Removed	Accumulators	30,000

Note that the measurement setup plays major role in the success of the attack. For instance, we were not able to reveal the key using a differential probe Hameg HZO41 [12] (instead of the AC preamplifier), as the probe attenuates the signal at the 10:1 ratio and introduces additional noise to the signal.

V. DPA Attack

Having proper measurement setup we performed the DPA attack against three different configurations of the FPGA board (see Table I). We mounted the attack against the last round and we were using a Hamming distance as a power consumption model. Attacking the first round and/or using Hamming weight as a power model did not lead to successful attack on FPGA implementation of AES (however, attacking the first round and/or using Hamming weight is applicable to MCU implementation of AES). The correct key hypothesis is

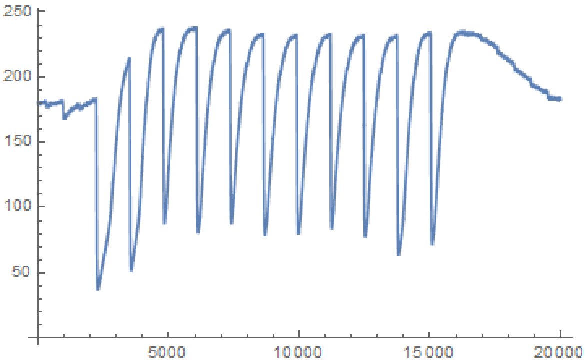

Figure 4. Power trace. Configuration: removed capacitors, accumulators.

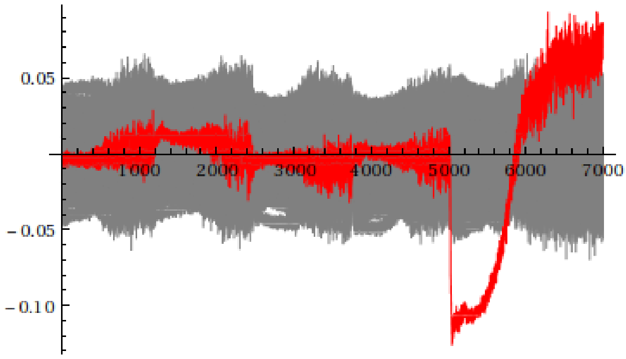

Figure 5. Plots of correlation coefficients (correct key in red), samples 10,000–17,000, 5,000 traces. Configuration: removed capacitors, accumulators.

identifiable by the lowest correlation coefficient because we were measuring an increase in current flow as a voltage drop.

A. *Capacitors: Removed; Power Source: Accumulators*

Board with removed decoupling capacitors and powered from accumulators via linear stabilizers provides ideal attack environment. As can be seen from Figure 4, the captured power trace is noiseless and perfectly shaped. Obtaining and analyzing just 5,000 traces was sufficient to reveal the correct key. Figure 5 shows the plots of correlation coefficients for all key hypotheses. The plot for the correct key hypothesis is significantly different from the others. There is an easily recognizable spike around the sample where the operation took place in.

B. *Capacitors: Removed; Power Source: Switched-Mode Power Supply*

We replaced the accumulators with the standard switched-mode power supply delivered with the board. The power trace from this measurement can be found in Fig. 6. As the switched-mode power supply generates small, but not negligible noise on power line, analyzing just 5,000 traces was insufficient for revealing the correct key. As can be seen on Fig. 7, the plot of correlation coefficient for correct key is indistinguishable from other plots.

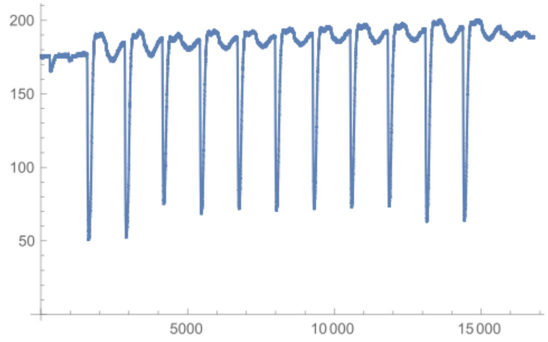

Figure 6. Power trace. Configuration: removed capacitors, switched-mode power supply.

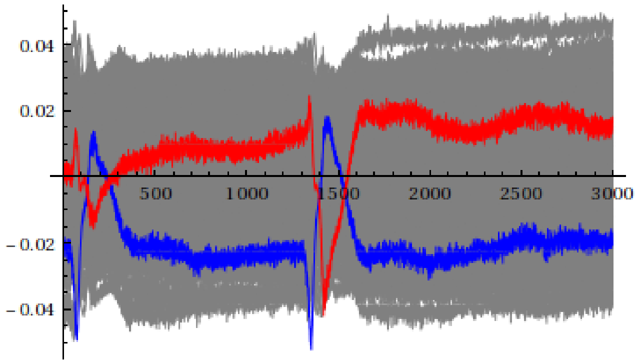

Figure 7. Plots of correlation coefficients (correct key in red, key hypothesis with lowest correlation coefficient in blue), samples 13,000–16,000, 5,000 traces. Configuration: removed capacitors, switched-mode power supply

We repeated the analysis for 30,000 traces. The plot of the correlation coefficient of the correct key hypothesis is similar to the plot for 5000 traces, but the correlation coefficient of the correct key hypothesis is easily distinguishable now (see Fig. 8).

C. *Capacitors: Present; Power Source: Accumulators*

For investigation of influence of decoupling capacitors we used standard non-modified board, powered from accumulators via linear stabilizers. As can be seen from Fig. 10, analyzing just 5,000 traces is again insufficient to reveal the correct key. Moreover, the plot of correlation coefficient looks differently than the plot of correlation coefficient obtained on the board with removed decoupling capacitors – there is a wave with multiple peaks instead of one spike.

We repeated the analysis for 30,000 traces. The plot of the correlation coefficient of the correct key hypothesis is similar to the plot from the attack with 5,000 traces (see Fig. 11), and the correlation coefficient of the correct key hypothesis is the lowest one. However, in comparison with previous two measurements, there is no spike in the correlation coefficient plot. Even though the correlation coefficient of correct key hypothesis was the lowest one, the shape of the plot was not easily distinguishable from correlation coefficients of other key hypotheses.

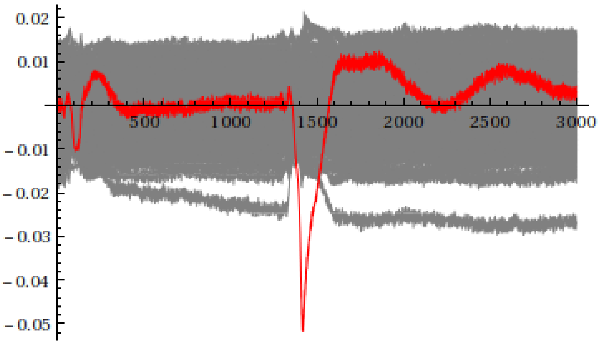

Figure 8. Plots of correlation coefficients (correct key in red), samples 13,000–16,000, 30,000 traces. Configuration: removed capacitors, switched-mode power supply.

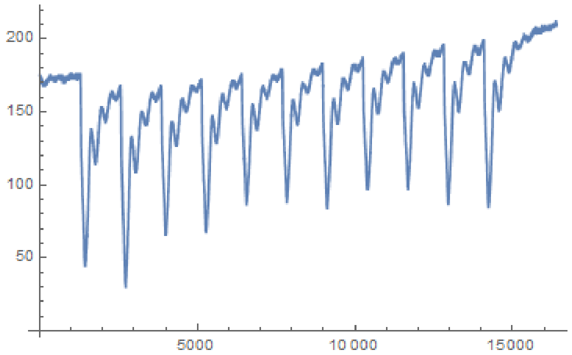

Figure 9. Power trace. Configuration: present capacitors, accumulators.

VI. Conclusions

We mounted the DPA attack against FPGA running AES algorithm. We focused on the last round and used Hamming distance as a power model, as attacking first round and/or using Hamming weight does not lead to success in case of FPGA implementation. Proper measurement setup plays major role in the success of the attack – while using differential probe disables the attack, using differential amplifier enables it. We studied the role of decoupling capacitors. Surprisingly, their presence does not disable the attack, however, as expected, their removal enables the attack significantly. We also studied the influence of noise in power source. We found out that even the circuit powered from (noisy) switched-mode power supply can be successfully attacked, however, noiseless power supply (accumulator) simplifies the attack in terms of number of traces necessary for successful attack on the FPGA implementation.

Acknowledgment

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).

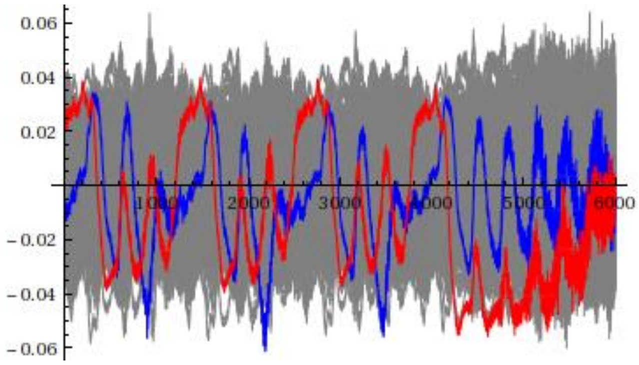

Figure 10. Plots of correlation coefficients (correct key in red, key hypothesis with lowest correlation coefficient in blue), samples 10,000–16,000, 5,000 traces. Configuration: present capacitors, accumulators.

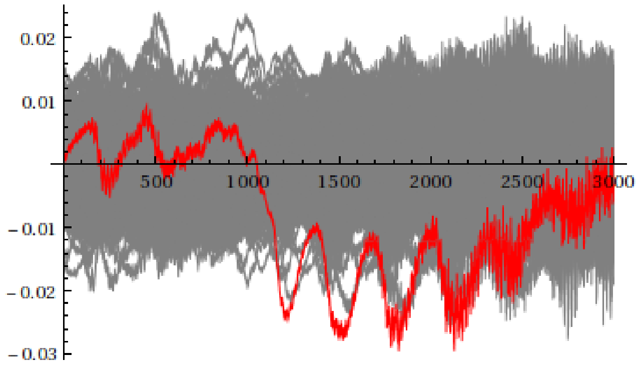

Figure 11. Plots of correlation coefficients (correct key in red), samples 13,000–16,000, 30,000 traces. Configuration: present capacitors, accumulators.

References

[1] C. Paar and J. Pelzl, *Understanding Cryptogtaphy*, 2nd ed. Berlin Heidelberg: Springer-Verlag, 2010.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology – CRYPTO '99*, M. Wiener, Ed. Springer Berlin Heidelberg, aug 1999, pp. 388–397.

[3] T. Caddy, "Differential Power Analysis," in *Encyclopedia of Cryptography and Security*. Springer US, 2005, pp. 152–154.

[4] *Spartan-3E Starter Kit Board User Guide*, [cit. 2017-02-04]. [Online]. Available: https://reference.digilentinc.com/ media/s3e:s3estarter ug.pdf

[5] C. Paar, *Implementation of Cryptographic Schemes 1*. Ruhr University Bochum, 2015.

[6] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York: Springer US, 2007.

[7] National Institute of Standards and Technology, *FIPS PUB 197: Advanced Encryption Standard (AES)*. Gaithersburg: National Institute of Standards and Technology, Nov. 2001.

[8] J. Daemen and V. Rijmen, The Design of Rijndael: *AES – The Advanced Encryption Standard*. Berlin Heidelberg: Springer-Verlag, 2002.

[9] R. Velegalati and P. Yalla, "Differential Power Analysis Attack on FPGA Implementation of AES," [cit. 2017-02-04]. [Online]. Available: https://cryptography.gmu.edu/team/download.php?docid=2082

[10] *Agilent Technologies InfiniiVision 7000A Series Oscilloscopes*, USA, 2012, [cit. 2016-02-04]. [Online]. Available: http://literature.cdn.keysight.com/litweb/pdf/5989-7736EN.pdf?id=1373609

[11] *Langer EMV-Technik PA 303 BNC preamplifier*, [cit. 2017-02-04]. [Online]. Available: https://www.langer-emv.de/en/product/preamplifier/37/pa-303-bnc-set-preamplifier-100-khz-up-to-3-ghz/519

[12] *Hameg Probes Datasheet*, [cit. 2017-02-04]. [Online]. Available: http://www.farnell.com/datasheets/1806004.p