Proceedings of IEEE Computer Society Annual Symposium on VLSI (IEEE ISVLSI'10),
Kefalonia, Greece, July 5-7, 2010.

Side Channel Attacks Cryptanalysis Against Block Ciphers Based on FPGA Devices

Anestis Bechtsoudis
Computer Engineering and Informatics Department (CEID)
University of Patras, GREECE
mpechtsoud@ceid.upatras.gr

Nicolas Sklavos
Informatics & MM Dept., Branch of Pyrgos
Technological Educational Institute of Patras
Pyrgos, ZIP 27100, GREECE
e-mail: nsklavos@ieee.org

***Abstract* — The block cipher designers assume that the secret information will be manipulated in close and reliable computing environments. Unfortunately, this isn't feasible because actual computing units and chips have implementation information leakage during their operation. Side channel cryptanalysis exploits this implementation data, in order to extract cipher's secret information. In this paper, we discuss the current state-of-art of side channel cryptanalysis. We also analyze the different categories of side channel attacks and examine how concrete attacks against FPGA devices leads to secret information reveal.**

Keywords: side channel, cryptanalysis, block ciphers, FPGA

I. INTRODUCTION

There are two different points of view that we can consider a cryptographic primitive, such as a block cipher or a digital signature algorithm [1]. On the one hand, it can be viewed as an abstract mathematical object, typically a transformation parameterized by a key, turning some input into some output. On the other hand, this primitive will actually have to be implemented in a program that will run on a given processor, in a given environment, and therefore present specific characteristics. Namely the mathematical object is necessarily implemented to a concrete system which presents specific behavior and characteristics. Traditionally, cryptanalysis efforts have been directed solely against the mathematical object, and the resultant attacks necessarily apply to any concrete implementation. Statistical attacks against block ciphers (such differential and linear cryptanalysis) are good examples of this, and they work against ciphers regardless of which implementation of them is being attacked.

The first point of view is what so called "classical" cryptanalysis, while the second one is the side-channel cryptanalysis. Side-channel cryptanalysis is taking advantage of implemented specific characteristics in order to recover the secret parameters involved in the computation. Therefore is much less general (since it is specified to a given implementation) but often much more powerful than the classical cryptanalysis. It is under great consideration by implementers of cryptographic devices.

We now understand that a strong mathematical algorithm is not enough to define a "safe" cryptosystem. Designers must take under great consideration, the side channel data leakage of the device, and ensure that this leakage will not lead to the reveal of secret information.

II. SASEBO FPGA DEVICES

Since Kocher et al. introduced side-channel attacks [2], [3], many new attacks and countermeasures have been studied. But the scientific community tries to formulate international standards for security evaluation against side-channel attacks. In order to contribute to the standardization process, the Research Center for Information (RCIS) of AIST and Tohoku University have developed the Side-channel Attack Standard Evaluation Board (SASEBO) [4]. SASEBO boards were designed focusing on the power consumption factor which is in the foreground nowadays. Five types of SASEBO exist, based on both Xilinx and Altera FPGAs. Fig. 1 shows the standard version of the board & Table 1 its basic features [3].

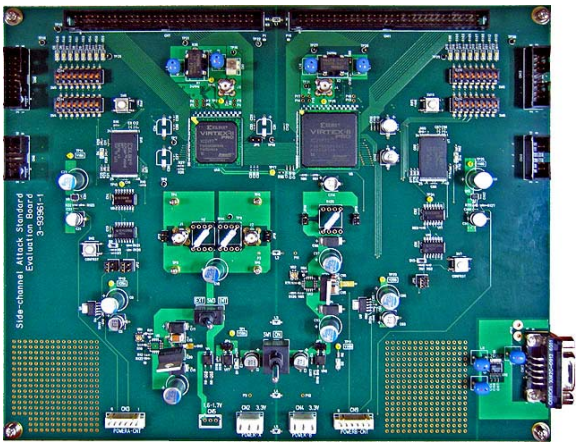

Figure 1. Side-channel Attack Standard Evaluation Board (SASEBO)

TABLE 1. BASIC FEATURES OF SASEBO

Size	250 x 200 x 1.6 mm^3, FR-4, eight layers
FPGAs	Xc2vp7-5FG456C (cryptographic circuit) Xc2vp30-5FG676C (control circuit)
Power Supply	Two 3.3V DC power supply lines. 2.5V, 1.8V, and 1.6V internal regulators
Monitor points	Shunt resistors are inserted at the VDD and GND lines
Clocks	24MHz oscillator for each FPGA
Local bus	32-bit bus between the FPGAs

Fig. 2 shows the SASEBO block diagram and in Fig. 3 we illustrate the structure of the interface hardware and software.

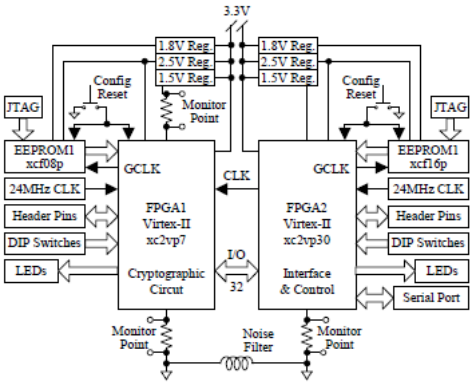

Figure 2. Block diagram of SASEBO

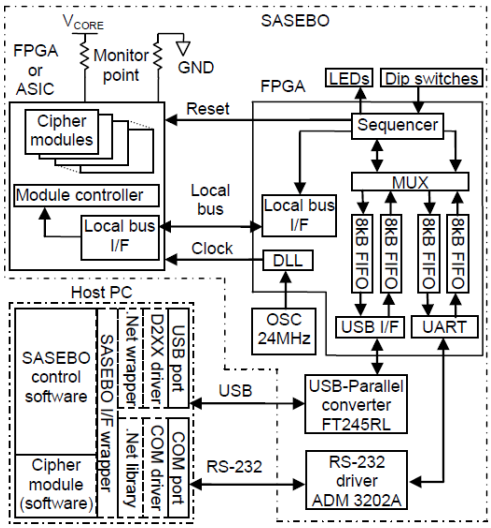

Figure 3. Power analysis experimentation environment

III. Experiments using SASEBO

Using SASEBO boards engineers are trying to automatize the procedure by developing testing software, which controls the encryption process in SASEBO, capture power traces and performs power analysis attacks. This testing procedure results will be a safety criterion for ciphers' hardware implementations. Although such a test automaton model, is difficult to be achieved, because each implementation and its internal architecture, has differences with the other ones and introduces new parameters.

In our paper we examine and present the experimental results so far [5] [6], and try to release our own power analysis attacks based on SASEBO. In Fig. 4 we can see a power trace of an AES implementation and the segments that the attack can be released [5]. Our goal is to go one step further and try to reveal all the vulnerabilities of the cryptosystems in less time and with an automatic procedure. By carefully studying the previous work, we see where the previous researches faced difficulties and barriers in their measurement techniques. We try to overtake these obstacles and through our experiments present a sufficient enough model, in order to evaluate the safety of concrete implementation of block ciphers.

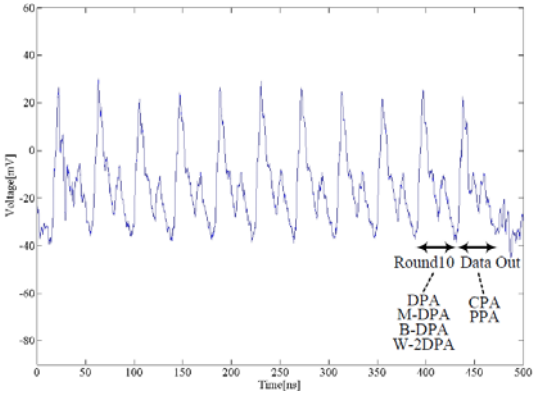

Figure 4. Power trace segments targeted by attack methods in an AES implementation in SASEBO

IV. On progress & future work

In future work we plan to go a step further and investigate the resistance characteristics of concrete implementations and try to develop a side-channel attack model that will automatize the procedure of testing the cryptosystems. We will release modified-optimized power analysis attacks against product block ciphers and see how effective some countermeasures, that have been proposed, are. Also we will examine approaches that reduce the number of needed measurements and time of attack. We will make a statistic of all these data and propose an overall evaluation model and techniques.

V. Conclusion

We release power analysis attacks against SASEBO boards in which block ciphers have been implemented. We examine and analyze the behavior of each implementation and present the side-channel information leakage and how this kind of information is capable to reveal the cipher's secret information to the attacker. Finally through statics we see how easy (how many power traces do we need to obtain) and with what level of access can we break the cryptosystem and gain access to secret parameters (not always the key itself but these parameters eventually lead to key reveal).

References

[1] N. Sklavos, X. Zhang, Wireless Security & Cryptography: Specifications and Implementations, CRC-Press, A Taylor and Francis Group, ISBN: 084938771X, 2007.

[2] Paul C. Kocher, "Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and other Systems," In CRYPTO '96, LNCS 1109, pp. 104-113, 1996.

[3] P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in CRYPTO '99, LINCS 1666, pp. 188-387, 1999.

[4] Side-channel attack standard evaluation board, http://www.rcis.aist.go.jp/special/SASEBO/

[5] "Power Analysis Attacks on SASEBO", RCIS, NIAIST January 2010

[6] J. Kesley, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers", *Journal of Computer Security*, v. 8, n. 2-3, 2000, pp. 141-158.

[7] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Investigations of Power Analysis Attacks on Smartcards," Proc. USENIX Workshop S,nartcard Technology, pp. 151-161, May 1999.