Experiments and Hardware Countermeasures on Power Analysis Attacks

ManKi Ahn[1] and HoonJae Lee[2]

[1] Defense Agency for Technology and quality Assurance,
Kyungpook National University,
Daegu, 706-020, Korea
mkahn@dqaa.mil.kr
[2] Dongseo University, Busan, 617-716, Korea
hjlee@dongseo.ac.kr

Abstract. Security is a concern in the design of smartcards. It is possible to leak much side channel information related to secret key when cryptographic algorithm runs on smartcards. Power analysis attacks are a very strong cryptanalysis by monitoring and analyzing power consumption traces. In this paper, we experiment Exclusive OR operation. We also analyze the tendency of state-of-the-art regarding hardware countermeasures and experiments of Hamming-Weights on power attacks. It can be useful to evaluate a cryptosystem related with hardware security technology.

Keywords: Side Channel Attacks, Power Analysis, SPA/DPA, Countermeasure, SmartCard.

1 Introduction

The power consumption of a cryptographic device such as smartcard may provide much information about the operations that take place and the involved parameters. In 1999, P.Kocher introduced the so-called side channel attacks based on *simple power analysis*(SPA) and *differential power analysis*(DPA) to recover the secret key[1]. A smartcard, based on the idea of embedding an integrated circuit chip within a ubiquitous plastic card, can execute cryptographic operations and provide high reliability and security. Recently, however, this had been a target of the side channel attacks.

This paper[1] analyzes the tendency of state-of-the-art regarding hardware countermeasures and experiments of Hamming-Weights on power attacks, and experiments Exclusive OR operation in smartcards. It will be discussed in detail in section 3. The remainder of this paper is organized as follows: Section 2 overviews power attacks, while section 3, We experiment on power analysis attacks. Section 4 analyzes state-of-the-art regarding hardware countermeasures. Conclusion is presented in section 5.

[1] This research was supported by University IT Research Center Project.

M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3982, pp. 48–53, 2006.

2 Power Analysis Attacks

The power consumption of hardware circuit is a function of the switching activity at the wires inside it. Since the switching activity is data dependent, it is not surprising that the key used in a cryptographic algorithm can be inferred from the power consumption statistics gathered over a wide range of input data. these attacks have been shown to be very effective in breaking smartcards. These attacks are called power analysis attacks which are non-invasive attacks.

Simple power analysis(SPA) consists of observing the variations in the global power consumption of the chip and retrieving from it some information which can help to identify any secret key or value. A special kind of SPA, the so called Hamming-weight attacks exploit a strong relations between the Hamming-weight and the power consumption trace.

Differential power analysis(DPA) is more sophisticated than the SPA. The attacker identifies some intermediate value in the cryptographic computation that is correlated with the power consumption and dependent on the plaintext and the key. The attacker divides the traces into groups according to the intermediate value predicted by current guess at the key and the traces corresponding plaintext. If the averaged power trace of each group differs noticeably from the other, it is likely that the current key guess is correct. Incorrect key guesses should result in all groups having very similar averaged power traces, since incorrectly predicted groups having very similar averaged power traces.

Recently, there are many open questions regarding reconfigurable hardware devices, such as Field Programmable Gate Arrays(FPGAs), as a module for security functions. The use of FPGAs is highly attractive for a variety of reasons that include algorithm upload or modification, architecture efficiency, and costs. However, FPGAs will be targeted of the one-to-one copy, reverse-engineering, and physical attacks. Therefore, many people discuss and experiment vulnerabilities of modern FPGAs against the threat[2][3][4][5][6][7][8][9]. They used either a microchip PIC 16F84A microcontroller, ATMEL AT89S8252, a Xillinx XCV800, Virtex-E FPGA, or ARM CM7TDMI core and used MATLAB, C-programs as statistical analysis tool etc.

A PINPAS(Program INferred Power Analysis in Software) tool supports the testing of algorithms for vulnerability to SPA/DPA. The tool is especially useful as an aid in the design of both cards(hardware) and algorithms(software)[10][11].

The masking method is the usage of masked logic. However, that does not prevent DPA attacks, because Glithes occur in every CMOS circuit. The Glithes are that the transitions at the output of a gate that occur before the gate switches to the correct output[12].

3 Experiments of Power Attacks on Smartcard

3.1 Experiments of Hamming-Weights

Now, we will carry out the experiments of Hamming-Weights[1] using data transition in smartcard. The instruction takes the Exclusive OR operation(XOR) of

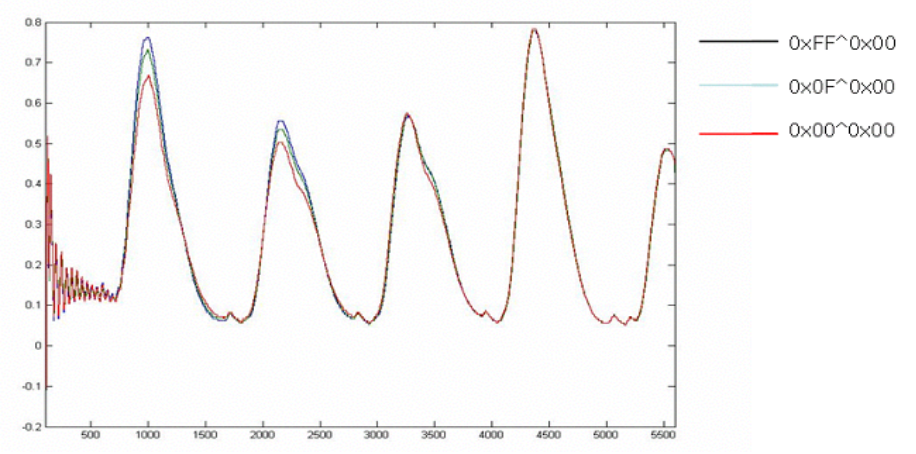

Fig. 1. Power traces of several XOR operations over 1,000 traces

two 8-bit values. The experimental results are shown in figure 1. As the below results, the plot confirms the assumption about the measurability of Hamming-Weights leakage. we need approximately 1,000 measurements to identify the correct plot.

3.2 Experiments of DPA

The plaintexts are prepared that only the data at the output of the 1st S-Box would be different in the first round of block cipher. Further details of the S-Boxes are omitted, but it handles the main ingredients of an algorithm like block ciphers(DES,AES). The smartcard is assumed to leak information about secret values transported on the memory bus. The potential power source for SPA/DPA is the value of a operand XOR secret key which can be calculated from the known operand and a guessed secret key.

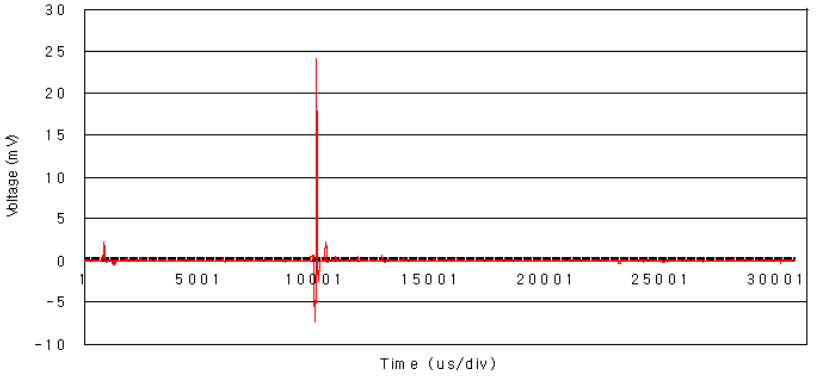

Fig. 2. The differential power traces for the correct key guess

In the criterion, we generated power traces and be split into two groups with Hamming-weights larger and smaller than 4.

By performing several XOR operations with S-Boxes, A difference trace was obtained by subtracting the average traces for each of the two groups. We gather approximately 5,000 measurements. Figure 2 show that the correlation could be observed.

4 Hardware Countermeasures on Power Analysis Attacks

The advantages of software implementations are the ease of use, the ease of upgrade, the portability, low development costs, low unit price and flexibility. Software implementations offers moderate speed, slow the execution process compared to hardware system. Hardware implementations are more secure because they cannot as easily be read or modified by an attackers as software. Hardware countermeasures offer deal either with some form of power trace smoothing or with transistor-level changes of the logic[4]. The goal of countermeasures against DPA attacks is to completely remove or at least to reduce this correlation, i.e. the addition of noise with noise-generators of the filtering of the power traces[13], the insertion of random delays[14], the use of capacitor or dummy bus, internal clock generator including random clock jittering, static complementary CMOS logic[15], or the usage of masked logic, but that does not prevent DPA attacks, because of Glithes occur in every CMOS circuit[12].

4.1 Countermeasures of Logic Level

We summarize security problems produced by attacks against hardware implementations. To be resistant against the SPA/DPA, various countermeasures have already been proposed. The protection against power analysis attacks involved implementing hardware based on a power attacks resistant logic with constant power consumption[16]. It depends on both the values and transitions, i.e. the Hamming-weights between consecutive data values, yet this is quite expensive to implement. Therefore, we analyze another power attack resistant hardware-type and state-of-the-art skill.

Dual-rail method is to render information about Hamming-weights of secret values completely useless, dual-rail logic provide attackers with the meanless Hamming-weights of values, because these values are always the same. An implementation of this method in hardware can be efficient and transparent to the algorithm running on smartcard. This method used precharge logic. Every signal transition is represented with a switching event, in which the logic gate charges a capacitance. But at a price, the hardware resources have to be doubled in size[10]. Dual-rail encoding can be similarly used to pass data and an alarm signal by using the 11 value to indicate an alarm (00 is used to pass a clear signal; 01 and 10 representing logical-0 and logical-1 respectively). Asynchronous logic(the self-timed circuits) can be made far less susceptible to power attacks, simply slowing down when the supply voltage dips rather than malfunctioning. By contrast, the

self-timed circuits are consumed considerable silicon area(nearly three times the area of the synchronous one) and slower than the synchronous one[17][18][19].

A dynamic and differential CMOS logic is presented in which a gate always uses a fixed amount of power. Sense Amplifier Based Logic (SABL)[16] uses advanced circuit techniques to guarantee that the load capacitance has a constant value. SABL completely controls the portion of the load capacitance that is due to the logic gate. The intrinsic capacitances at the differential in and output signals are symmetric and additionally it discharges and charges the sum of all the internal node capacitances. A major disadvantage is the non-recurrent engineering costs of a custom designed cell library development. SABL also suffers from a large clock load, as is common to all clocked dynamic logic styles and uses two times the area and power of other CMOS logic.

4.2 Countermeasures of Operation Level

Secure instruction based on a pipeline architecture execute sequences of instruction(i.e. fetch, decode, execute, write). This is implemented by the electronics of the microcontroller rather than by software addition. However, this countermeasure is only implemented with RISC(Reduced Instruction Set Computer) architecture in which the instructions are read and executed in parallel. RISC architectures using a so called "pipeline" method make it possible to interleave several instructions by several instructions in the same clock cycle. Therefore, the waiting time is introduced randomly between the sequences of instruction. In other words, there is instruction set architecture of pipelined smart card processor with secure instructions to mask the power differences due to key-related data[20].

5 Conclusion

We have experiments of Hamming-Weights using Exclusive OR operation(XOR) on power attacks. Experimental results have demonstrated that the instruction with the different value of Hamming-Weights can make different power traces. Therefore, at the part of hardware countermeaure, A logic designer must consider DPA-resistant CMOS logic in smartcard. Besides, we also analyze the tendency of state-of-the-art regarding hardware countermeasures. Side-channel resistance cannot be isolated at one abstraction level. It can be useful to evaluate a cryptosystem related with hardware security technology.

References

1. P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *In Proceedings of Advances in Cryptology-CRYPTO '99,* LNCS 1666, pp. 388-397, Springer-Verlag, 1999.
2. Larry T. MaDaniel III, " An Investigation of Differential Power Analysis Attacks on FPGA-based encryption Systems", available to scholar.lib.vt.edu, *Master of Science in Electrical Engineering*, May, 2003.
3. Siddika Berna Ors, Elisabeth Oswald and Bart Preneel, " Power-Analysis Attacks on an FPGA-First Experimental Results", *In Proceedings of CHES 2003*, LNCS 2779, Springer-Verlag, pp. 35-50. 2003

4. Thomas Wollinger and Christof Paar, "How Secure Are FPGAs in Cryptographic Applications(Long version)", Report 2003 /119, IACR, 2003. available on http://eprint.iacr.org
5. Chin Chi Tiu, "A New Frequency-Based Side Channel Attack for Embedded Systems", *A Master thesis, in the University of Waterloo*, 2005
6. Ryan Junee, "POWER ANALYSIS ATTACKS :: A Weakness in Cryptographic Smart Cards and Microprocessors", *Bachelor of Computer Engineering & Bachelor of Commerce*, November, 2002
7. Elisabeth Oswald, "On Side-Channel Attacks and the Application of Algorithmic Countermeasures", *A PhD Thesis in Graz University of Technology*, IAIK, May, 2003
8. Stefan Mangard, " Calculation and simulation of the Susceptibility of Cryptographic Devices to Power-Analysis Attacks", *A Diploma Thesis, in Graz University of Technology*, IAIK, 2003
9. KULRD & SCARD Consortium, "Side Channel Analysis Resistant Design Flow", IST-2002-507270, SCARD-KULRD-D4.1, 2005, available on http://www.scard-project.org.
10. J. den Hartog and others, "PINPAS : a tool for power analysis of smartcards", *in SEC 2003, IFIP WG 11.2 Small Systems Security*, pp. 447-451, 2003
11. J.I den hartog, and E.P. de Vink, " Virtual Analysis and Reduction of Side-Channel Vulnerabilities of Smartcards", available on http://www.win.tue.nl/ecss, 2005.
12. Stefan Mangard, Thomas Popp, and Berndt M. Gammel, "Side-Channel Leakage of Masked CMOS Gates", *Topics in Cryptology - CT-RSA2005*, LNCS 3376, pp. 351-365, Springer-Verlag, 2005.
13. Kris Tiri and Ingrid Verbauwhede. "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation.", *In DATE 2004*, pp. 246-251. IEEE Computer Society, 2004.
14. Stefan Mangard. "Hardware Countermeasures against DPA. A Statistical Analysis of Their effectiveness. *In proceedings of Cryptology-CT-RSA 2004*, LNCS 2964, pp. 222-235. Springer-Verlag, 2004.
15. Kris Tiri and Ingrid Verbauwhede, "A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs" *In Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE05)*, 2005.
16. Kris T., Moonmoon A., and Ingrid V., "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to withstand Differential power Analysis on Smart Cards" *In 28th European Solid-State Circuits Conference,* 2002.
17. K. J. Kulikowski, Ming Su, A.Smirnov, A. Taubin, M. G. Karpovsky, and Daniel M., "Delay Insensitive Encoding and Power Analysis: A Balancing Act", *In 11th IEEE International Symposium on Asynchronous Circuits and Systems: ASYNC'05*, pp. 116-125, 2005.
18. S. Moore and others, "Improving SmartCard Security using Self-timed Circuits", available on $http://actes.sstic.org/SSTIC03/Rump_sessions$, 2003.
19. Simon Moore, Ross Anderson, Robert Mullins and George Taylor, "Balanced self-checking asynchronous logic for smart card applications" *in the Microprocessors and Microsystems Journal*,2003
20. Feyt, "Countermeasure method for a microcontroller based on a pipeline architecture", *US PATENT 20030115478 A1*, 2003
21. Elisabeth Oswald, Stefan Mangard, Norbert Pramastaller, Vincent Rijmen, "A Side-Channel Analysis Resistant Description of the AES S-Box.", *FSE 2005, Revised Selected Papers*, LNCS 3557, pp. 413-423, Springer-Verlag , 2005.
22. Kris Tir and Ingrid Verbauwhede, "Simulation Models for Side-Channel Information Leaks" *ACM 1-59593-058-2/05/0006, DAC 2005*