International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 11-18
http://dx.doi.org/10.14257/ijsia.2015.9.6.02

Securing Embedded Systems from Power Analysis Attack

Deevi Radha Rani[1], S. Venkateswarlu[2], Venkata Naresh Mandhala[3] and Tai-hoon Kim[4,*]

[1]*Women Scientist, Department of CSE, KL University, Vaddeswaram, AP, 522502, India*
[2]*Department of CSE, KL University, Vaddeswaram, AP, 522502, India*
[3]*Department of Information Technology, VFSTR University, Vadlamudi-522213, Guntur, India*
[4]*Department of Convergence Security, Sungshin Women's University, 249-1, Dongseon-dong 3-ga, Seoul, 136-742, Korea*
[1]*radharani_cse@kluniversity.in*, [2]*somu23@kluniversity.in*, [3]*mvnaresh.mca@gmail.com*,[4]*taihoonn@daum.net*
(Corresponding Author)

Abstract

Power Analysis Attack is a type of side-channel attack that uses power consumption of a cryptographic device to reveal the sensitive information. Power Analysis Attack is causing a serious threat to the embedded systems like smart cards. So there is a need to secure embedded systems from power analysis attack. In this paper, various methods of power analysis attack are addressed. The power analysis attack experimental setup using SASEBO-W is depicted and the various countermeasures are proposed. Performance comparison of counter measures are analyzed and tabulated.

Keywords: *Side channel attack, Power Analysis Attack, SASEBO-W, Countermeasures*

1. Introduction

The rapid use of communication systems increased the need for securing the information that communicating between them. The use of cryptographic algorithms secure the information by using cryptographic keys but still many issues exists in physical implementation. Now-a-day's these cryptographic algorithms are embedded in devices such as smart cards and cell phones. Implementation attacks aim at implementation of cryptographic system to retrieve secret information but not on cryptographic algorithm. The implementation attacks can be classified as 2 types: active attacks and passive attacks. Active attacks aim at physical security of the devices. Passive attacks do not damage cryptographic device but observe leakage of cryptographic device. Securing hardware devices requires an assessment of various attacks on those devices. Side channel attack is a passive attack which is an attack on cryptographic algorithm that determines bits of unknown key. Kocher introduced the use of side channels to break a cryptosystem [1, 2]. Attacks involving passive observation of external characteristics of a device are termed eavesdropping attacks, also sometimes called side-channel attacks.

There are many different types of side channel attacks including timing, electromagnetic and power.

Timing attack is the type of side-channel attack involves the time taken to complete critical operations. Kocher [1] provides a detailed attack strategy for timing crypto-

* Corresponding Author

ISSN: 1738-9976 IJSIA

analysis of several commonly used algorithms. He notes that by measuring the time taken to perform private key operations, attackers can recover the input to those operations, thereby determining the private key. Implementations of cryptographic algorithms often perform computations in non-constant time, due to performance optimizations. If such operations involve secret parameters, these timing variations can leak some information and, provided enough knowledge of the implementation is at hand, a careful statistical analysis could even lead to the total recovery of these secret parameters. Timing attack of DES based on hamming weight is described in [8].

Electromagnetic analysis [3] exploits information that leaks through the electromagnetic field that is produced by a device. EM emanation can also exploit local information and, although more noisy, the measurements can be performed from a distance. There are 2 types of emanations: intentional and unintentional. The first type results from direct current flows. The second type is caused by various couplings, modulations etc.

Power analysis attacks [2] exploit the dependence between the instantaneous power consumption of a cryptographic device and the data it processes and/or the operation it performs. The overall power consumption of a cryptographic device can be divided into a static and dynamic part. Since the dynamic power consumption is connected directly with the processed data, it is a potential target to detect the dependency between these two parameters. For that reason, power traces can be used to obtain secret information. There are mainly two attacks using this approach, the simple power analysis and the differential power analysis. In a simple power-analysis, the attacker uses detailed knowledge of the device to identify which instructions are being executed based on their power signatures. In a differential power analysis, the attacker uses a hypothetical model of the device, and refines this model with statistical analysis of the power usage of the device.

The rest of the paper is organized as follows. In Section 2 we present the background of power analysis attack. In Section 3 we discuss SASEBO-W and its components. Section 4 describes the implementation setup for power analysis attack. Section 5 describes the countermeasures of power analysis attack and in Section 6 compares the performance of countermeasures for power analysis attack. Section 7 summarizes the paper.

2. Background

2.1. Power Analysis Attacks

Power Analysis Attacks are a type of Side Channel Attack where the power consumption of an executing implementation is used to reveal secret key information [2]. The power consumption of an implementation can be measured and recorded as it executes. This is referred to as the instantaneous power consumption. Power Analysis Attacks exploit a relationship between the instantaneous power consumption and the changing internal state of a cryptographic implementation.

There are three important steps required for any successful Power Analysis Attack [4]. Each step represents a part of the overall process which allows secret information to be identified based on the instantaneous power consumption:

- *Identify*: Find relationship between secret key information and instantaneous power consumption.
- *Extract*: Develop method of extracting the state of the relationship information.
- *Evaluate*: Use this information to determine all or part of the secret key information.

There are several specific types of Power Analysis Attacks described in research. The three main types of power analysis techniques are Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA). SPA usually involves the visual inspection of power traces for large scale differences. DPA utilizes statistical techniques in order to identify very subtle variations in power consumption due to differences in the data values being manipulated. CPA correlates a power model of the unit under test to the actual instantaneous power consumption. Related attacks include using emitted electromagnetic radiation. DPA can be performed with both single and multiple target bits. CPA uses a power model of the unit under test which can be developed using either Hamming Weight or Hamming Distance to estimate power consumption.

2.2. Hamming Distance Model

The basic idea of Hamming-distance model is to count number of 1→0 and 0→1 transitions that occur in the crypto processor when it is implementing the cryptographic algorithm. This number of transitions is the used to describe the power consumption of the processor at that time interval. But when we are using a Hamming-distance model to simulate the power consumption in the circuit assumption must be made that all 1→0 and 0→1 transitions have same amount of power consumption, also the transitions 0→0 and1→1 also consume same amount of power .therefore it assumes that all the gates contribute equally to the power consumption of the circuit and it neglects the parasitic capacitance between the transistors or wires. Since this model is neglecting the parasitic capacitances it provides a rough estimation of the power consumed .the Hamming–distance model is well suited to describe the power consumption on a data buses and the registers present in the crypto processor. Usually in order to apply the hamming distance model one should the consecutive values of data that are being processed. Also the Hamming distance model assumes that 1→0 and 0→1 consume same amount of power which in most of the cases is not true.

2.3. Hamming Weight Model

Compared to Hamming distance model, Hamming weight is much simpler. This models used when the attacker does not know the consecutive values of data for some part of the process. The basic idea of this model is that the number of Bits set in a processed data or a bit string is proportional to the power consumption of the circuit. The bit strings that are processed before and after this step are ignored. Hence this model is not well suited for the simulation of a digital circuit in CMOS technology. Attackers only resort to this model when Hamming distance model cannot be applied.

3. Side-Channel Attack Standard Evaluation Board-W

Side channel attack is a physical attack which exploits measurable parameters of cryptographic devices to extract the key. There is a need for standard platform to compare attacking algorithms and the efficiency of countermeasures. To contribute to these standardization efforts, National Institute of Advanced Industrial Science & Technology, Japan and National Institute of Standards & Technology, USA, have developed SASEBO, Cryptographic Circuits, IP macros, software and distributed to over 100 government, industry and academic research laboratories. There are different types of SASEBO platforms: SASEBO-G, SASEBO-B, SASEBO-R, SASEBO-GII, SASEBO-W, all of which use FPGA and custom ASIC LSIs to implement experimental cryptographic circuits.

SASEBO-W and the smartcard are highly suitable for side-channel attack experiments. Figure 2 shows the main component of SASEBO-W Board. The board is equipped with a

USB interface and an RS-232 serial port for communication with a host computer. The FPGA used in this board is Xilinx Spartan-6 LX150 which acts as control device. It is connected to digital volume of regulator and smartcard signals. Capacitors are not mounted on FPGA to allow monitoring of small fluctuations in power consumption. Also noise from control circuits are suppressed by separating power supply circuits of control FPGA and Cryptographic FPGA[5]. Power supply to the board is through USB connector.

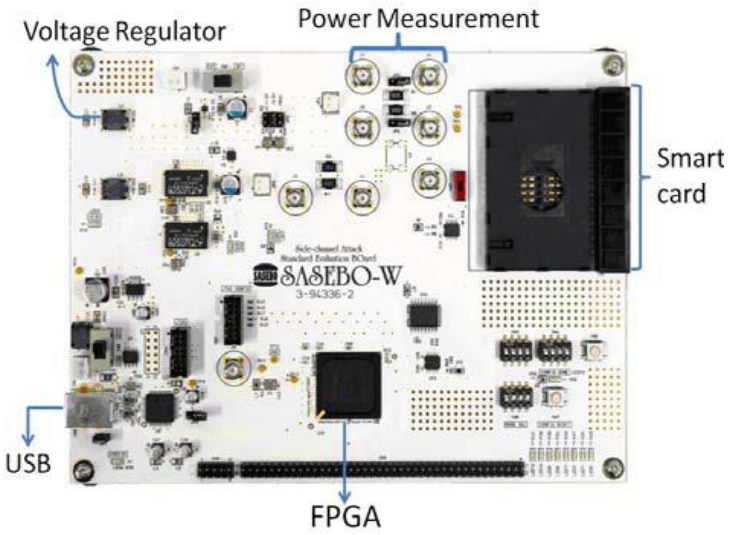

Figure 1. Main Components of SASEBO-W

The voltage of the power supply is adjusted through control FPGA. SubMiniature Version A (SMA) connectors are placed on VCC and GND to measure power consumption.

Along with Board, software is also available which consist of tool for waveform acquisition and analysis of power traces. The Figure 3 shows the user interface of the side channel attack evaluation software. The cryptographic modules [7], the controllers and the interface circuits were implemented in Verilog HDL, and the control software for operation check was developed in C#. The complete source code and all support documentation are available in [10].

4. Power Analysis Attack Setup

In order to measure a power traces from a cryptographic devices like smartcard, the following components are used, SASEBO-W is the main component in our experimental setup to measure the power consumption of AES implementation.

- *SASEBO-W*: The device under attack which takes in a plain text and computes an cryptographic algorithm and deliver cipher text. It should also interface with an PC as it receives data from the PC and send out the cipher text back to the PC. It has inbuilt experimental Smartcard.
- *Current Probe*: Used to measure the power consumption of the FPGA.
- *Digital oscilloscope*: TektronixDPO4032 digital phosphor oscilloscope with sampling rate 2.5G/s is used to obtain power traces
- *Personal computer*: Control the measurement setup and to store and compare the traces obtained.

The total experiment setup to measure the power consumption for AES using the experimental setup described above and the results obtained are described in [6]. Figure 2 shows the first two rounds of AES implementation. The two rounds look different.

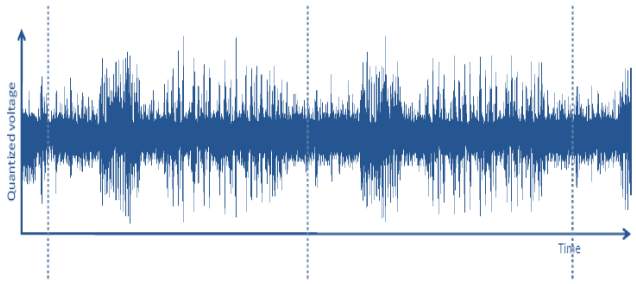

Figure 2. Two Rounds of AES Implementation

For Power Analysis Attack there are several options which we can use in the attack scenario. We can use:

- The peak of the power consumption.
- The integral of the power consumption over some number of power trace points.
- The sum of squares of the power consumption over some number of points.
- The sum of absolute values of the power consumption over a certain number of points.

While all of these choices may work, one may slightly reduce the number of traces required for a successful attack over the others.

5. Countermeasures for Power Analysis Attacks

Several Power Analysis Attack countermeasures were proposed over the years. Some of them are:

- Adding a noise generating circuit to the crypto processor
- Using specialized standard cell libraries which do not exhibit data dependent function
- Modifying the algorithm
- Providing additional circuits to prevent Power Analysis Attack

Adding noise generating circuit to the crypto processor in order to hide the power consumption looks promising but in reality it only increases the number of power traces. The designs of specialized cell libraries for Power Analysis Attack tamper resistant are still in research. Modifying the algorithm itself by introducing a randomly generated bit strings in between the execution of the devices if done correctly provides a good resistance against the Power Analysis attack.

At a high level [9], general categories of countermeasures to Power Analysis Attack include:

Leakage Reduction: These procedures make the set or sequence of operations less subject to the key or mystery intermediates. Adjusting systems to reduce variety in the power utilization can likewise be utilized, albeit utilizing these strategies on FPGAs may oblige additional care because of asymmetries inside the routing infrastructure. The general objective of leakage reduction methods is to decrease the leakage signal-to-noise

proportion, expanding the quantity of power measurements an adversary would require for a successful attack.

Noise introduction: These strategies include diverse sorts of noise into the power utilization estimations accessible to the aggressor, reducing the leakage-signal to noise ratio. Noise can be produced in the amplitude domain (*e.g.*, by consuming random measures of power) or in the temporal domain (*e.g.*, by randomizing operation timing). Similarly as with leakage reduction, these countermeasures expand the quantity of power follows needed by an adversary.

Obfuscation: By keeping algorithms mystery, the attacker is compelled to perform reverse engineering alongside power analysis. Such countermeasures normally don't give any security once a foe comprehends the operation of the obscure function; however can expand the initial effort needed for an attack. Since the cost of ensuing attacks is not expanded, obfuscation based countermeasures ought to be utilized with alert, yet at the same time may be superior to having no protection by any means.

Incorporating Randomness: These classifications incorporate a broad range of strategies for randomizing the information controlled by the device in ways that still create the right result. For public key systems, strategies for masking or blinding of information and keys can be particularly effective. Correspondingly, for symmetric algorithms, for example, AES, strategies for masking intermediates and tables can be viable. These systems constrain the attacker to utilize more complex attacks, for example, higher order Power Analysis Attack that requires a large number of estimations.

Protocol level countermeasures: These approaches involve designing the cryptographic protocols to preserve security even if some information leaks from each cryptographic operation. Secrets are continually refreshed and updated during cryptographic operations, so that an attacker is never able to get sufficient information to solve for any particular value. Variants of these constructions are applicable to both on-line applications (such as challenge-response authentication to a server) and off-line applications (such as firmware loading), and can accommodate both interactions with trusted servers as well as fully peer-to-peer protocols. While these methods cannot be used with legacy protocols lacking integrated protocol-level protections, designers who have the flexibility in the protocols can use these methods to achieve the highest level of security against power analysis attacks. Because power analysis attacks use signal processing to amplify leaked information, systems generally benefit from using multiple countermeasures. So combination of countermeasures would benefit.

6. Performance Comparison of Countermeasures

The countermeasures discussed above are implemented in our proposed experimental setup against AES implementation in SASEBO-W. The performance was analyzed using the number of cycle. The performance comparisons of countermeasures are tabulated in Table 1.

Comparing the countermeasures shows Noise reduction makes the attacks impossible and there is very little overhead. Furthermore this countermeasure can be implemented on all platforms.

Table 1. Performance Comparison of Countermeasures

Countermeasures	No. of Cycles	Performance Comparison
Leakage Reduction	3,765	~15 x slower
Noise Introduction	1,398	~2.02 x slower
Obfuscation	8,232	~4.7 x slower
Incorporating randomness	1,543	~2.05 x slower

7. Conclusion

In this paper, we reviewed the side-channel attacks against smart cards and presented power analysis attack. Side-channel Analysis Evaluation Board-W components are highlighted with our proposed experimental setup. The experimental setup implements the AES and the power traces are drawn. The various countermeasures described in research are discussed and these countermeasures are implemented in our proposed experimental setup. The performance comparison shows noise reduction makes the power analysis attack impossible. A combination of the countermeasures mentioned in this article should give enough security for next generation smart cards.

Acknowledgements

This research work is supported by DST WOS-A File No. SR WOS-A/ET-78/2011 dated 18.11.2011. I would like to thank DST for sponsoring me to do this research work. I would also thank KL University for their support and facilities to carry out my research work.

References

[1] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems", Proceedings of Crypto 1996, LNCS, Santa Barbara, CA, USA, vol. 1109, **(1996)** August, pp. 104-113.
[2] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis", Proceedings of Crypto 1999, LNCS, Santa-Barbara, CA, USA, vol. 1666, **(1999)** August, pp. 398-412.
[3] D. Agrawal, B. Archambeault, J. Rao and P. Rohatgi, "The EMSide-Channel(s)", Proceedings of CHES 2002, LNCS, Redwood City, CA, USA, vol. 2523, **(2002)** August, pp. 29-45.
[4] K. J. Smith Jr, "Methodologies for Power Analysis Attacks on Hardware Implementations of AES", MSc thesis, Rochester Institute of Technology, Rochester, New York, **(2009)** August.
[5] R. Velegalati and S. V. V. K. Yalla Panasayya, "Differential Power Analysis Attack on FPGA Implementation of AES", ECE 746 Statistical Signal Processing, **(2008)**.
[6] D. Radha Rani and S. Venkateswarlu, "Implementation of Power Analysis Attack using SASEBO-W", International Journal of Computer Science and Information Technologies, vol. 5, no. 3, **(2014)**, pp. 3994-3997.
[7] A. Satoh, T. Katashita and H. Sakane, "Secure implementation of Cryptographic modules", Development of a standard evaluation environment for side channel attacks, Synthesiology-English, vol. 3, no. 1, **(2010)** July, pp. 86-95.
[8] D. Radha Rani and S. Venkateswarlu, "Timing Analysis Attack based on Hamming Weight", International Journal of Applied Engineering Research, vol. 9, no. 18, **(2014)**, pp. 5161-5169.
[9] R. Whitepaper, "Protecting fpgas from power analysis. Cryptography", Cryptography Research, Tech. Rep., **(2010)**.
[10] "Side-channel Attack Standard Evaluation BOard (SASEBO)", AIST. http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html.