ISSN:0975-9646

Implementation of Power Analysis Attack using SASEBO-W

Deevi Radha Rani[#], S. Venkateswarlu[*]

[#] *Women Scientist, Department of CSE, KL University*
Vaddeswaram, AP, 522502, India
[*] *Mentor & Professor, Department of CSE, KL University*
Vaddeswaram, AP, 522502, India

***Abstract*—Side Channel Attacks exploit information that leaks from a cryptographic device. Power Analysis is a kind of side channel attack which reveals the key of cryptographic device by analyzing its power consumption. Power analysis attack causes serious threat to the security of cryptographic devices. Differential Power Analysis Attack is most widely used against embedded devices but suffers from few defects. In this paper, SASEBO-W is used for implementing power analysis attack. The correlation power attack is used to recover secret key based on power consumption of the device.**

***Keywords*—Side Channel Attack, Power Analysis Attack, Differential Power Analysis, Correlation Power Analysis.**

I. 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*.

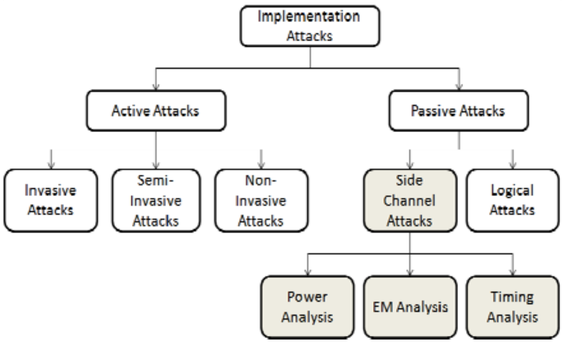


Fig. 1 Classification of Implementation Attacks

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

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.

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-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. This paper mainly focuses on power-analysis attack.

This paper is organized as follows: section II presents the power analysis attack and various methods existing, section III presents the SASEBO-W and its components, section IV presents the experimental setup and results, section V presents the conclusion.

II. Power Analysis Attack

Power Analysis is a kind of attack which reveals the key of cryptographic device by analyzing its power consumption. Power consumption of a device depends on data processed and operations performed in it. Power analysis attack causes serious threat to the security of cryptographic devices. Simple example for power analysis attack: Cryptographic device is programmed to perform any encryption algorithm. It receives a plaintext from PC, encrypts it and sends the ciphertext to PC. During encryption, power consumption of the device is measured. To measure power consumption a 1Ohm resistor is inserted into the ground line of the device, voltage drop across the resistor is recorded using digital oscilloscope. Voltage drop is proportional to power consumption of the device. So voltage drop is considered as power consumption and the voltage trace is referred as power trace.

In [4] a platform is presented to automatically perform DPA on a real-world FPGA board which gives a systematic view on how to successfully perform the DPA attack in a practical sense. It was obtained that DPA attack being difficult and expensive to perform on this kind of system. [7] presented a classical model for the power consumption of cryptographic devices based on the Hamming distance of the data handled and highlights the defects in DPA. Power Analysis Attack is implemented in many platforms like Spartan 6, Virtex II Pro FPGA but SASEBO-W and smartcard is highly suitable for side channel attack experiments [5].

III. Side-Channel Attack Standard Evaluation Board-W (SASEBO-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.

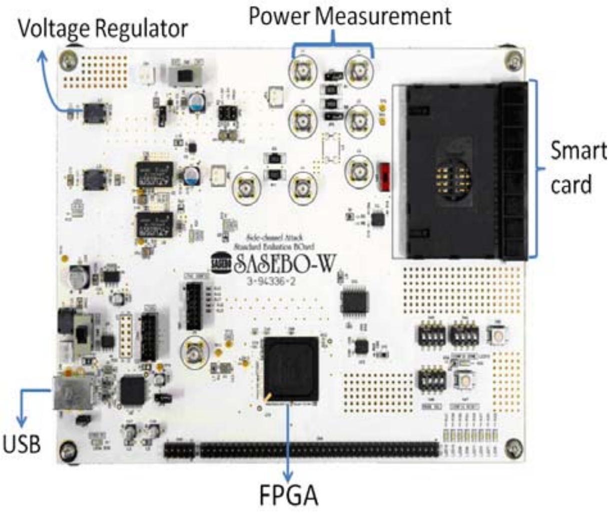
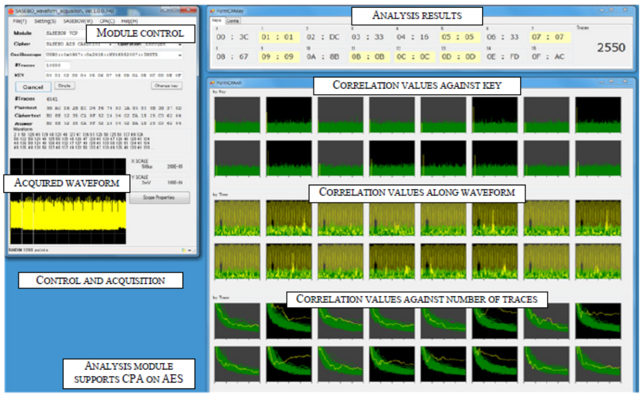


Fig. 2 Main components of SASEBO-W

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. Power supply to the board is through USB connector. 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, 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].


Module control
Acquired waveform
Control and acquisition
Analysis module supports CPA on AES
Analysis results
Correlation values against key
Correlation values along waveform
Correlation values against number of traces

00 : 3C 01 : 01 02 : DC 03 : 33 04 : 16 05 : 05 06 : 33 07 : 07
08 : 67 09 : 09 0A : 8B 0B : 0B 0C : 0C 0D : 0D 0E : FD 0F : AC
2550

Fig 3. User Interface of side channel attack evaluation software

IV. Experimental Setup

The aim of the experiment is to measure the power consumption of entire AES [8] processing sequence and record the power traces. Our total experimental setup consists of SASEBO-W, Host PC, Experimental smartcard and Digital Oscilloscope.

The experimental smartcard is an ATMega 163 microcontroller with 8-bit architecture and 1KB of data and instruction memory. This operates at 3.57MHz and supports AES function shown in the figure 4.

```
AES128( ){
SETPORTHIGH;
ADDROUNDKEY( );
FOR(I=0; I<9; I++){
  SUBBYTE( );
  SHIFTROWS( );
  MIXCOLUMNS( );
  KEYEXPANSION( );
  ADDROUNDKEY( );
}
SUBBYTE( );
SHIFTROWS( );
KEYEXPANSION( );
ADDROUNDKEY( );
SETPORTLOW;
}
```

Fig. 4 AES Function

The power consumption of entire AES encryption sequence on smartcard is captured using Tektronix DPO4032 digital phosphor oscilloscope with sampling rate 2.5G/s. One probe of oscilloscope is connected to the trigger output of AES on FPGA. The other probe is connected to ground output of the board. The leakage current flow through resistor load whose 2 ends are connected to oscilloscope. The voltage measured varies with the operations inside the board. The signal of the power consumption was amplified with amplifier. The figure 5 shows power consumption waveforms during AES processing at the beginning.

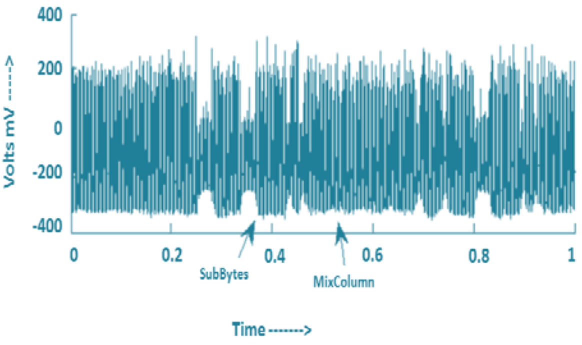


Fig. 5 Power consumption waveforms during AES processing

Power consumption waveforms were collected using any 2 cryptographic keys and the collected waveforms are analysed using Correlation Power Analysis. The power consumption H_{ij} of CPA was set to the Hamming weight of SubBytes output. The correlation coefficients $corr_k(t)$ between H_k and $W_i(t)$ were calculated for all k and t. The 8-bit partial key k with the largest value $corr_k(t)$ is retrieved as secret key. The figure 6 shows number of partial keys that were estimated correctly by CPA from the power consumption waveforms. It also shows that secret key can be extracted from 150 power consumption waveforms.

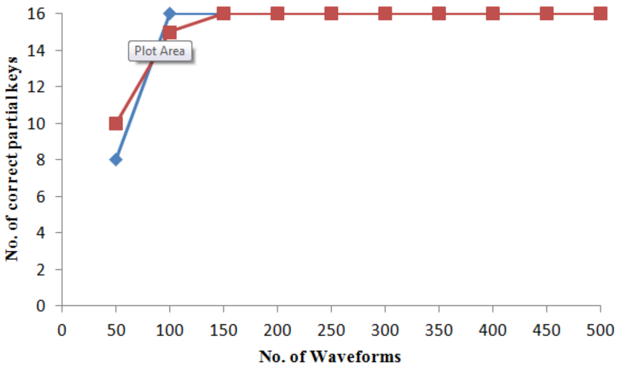


Fig. 6 Partial keys estimated from power consumption waveforms

V. Conclusion

In this paper, SASEBO-W and experimental smartcard is used for implementing power analysis attack which is highly efficient. Correlation Power Analysis for Power Analysis Attack can retrieve the key by using the relationship between data and power. It is faster and more accurate than compared to Differential Power Analysis Attack. The result shows that CPA requires less noise and less number of traces to guess the correct key.

Acknowledgement

This research is supported by DST WOS-A File No. SR WOS-A/ET-78/2011. 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*, in the Proceedings of Crypto 1996, LNCS, vol 1109, pp 104–113, Santa Barbara, CA, USA, August 1996.

[2] P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, in the Proceedings of Crypto 1999, LNCS, vol 1666, pp 398–412, Santa-Barbara, CA, USA, August 1999.

[3] D. Agrawal, B. Archambeault, J. Rao, P. Rohatgi, *The EMSide-Channel(s)*, in the proceedings of CHES 2002, LNCS, vol 2523, pp 29–45, Redwood City, CA, USA, August 2002.

[4] Song Sun; Zijun Yan; Zambreno, J., “Experiments in attacking FPGA-based embedded systems using differential power analysis,” Electro/Information Technology, 2008. EIT 2008. IEEE International Conference on vol.7, no.12, pp. 18-20, May 2008.

[5] Katashita, T., Hori, Y., Sakane, H. and Satoh, A.: Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing, NIST 2012.

[6] Rajesh Velegalati, Panasayya S V V K Yalla, “Differential Power Analysis Attack on FPGA Implementation of AES”, In ECE 746 Statistical Signal Processing, 2008.

[7] Eric Brier, Christophe Clavier and Francis Olivier, “Correlation Power Analysis with a Leakage Model”, CHES 2004, published by Springer, Volume 3156/2004.

[8] National Institute of Standards and Technology (U.S.). Advanced Encryption Standards (AES) FIPS Publication.

[9] Omar Choudary, "Breaking Smartcards Using Power Analysis", University of Cambridge, 2005

[10] “Side-channel Attack Standard Evaluation BOard (SASEBO),” AIST. http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html.