Power Analysis Attack: A Vulnerability to Smart Card Security

Hridoy Jyoti Mahanta
Department of Information Technology
Assam University
Silchar, India
E-mail: hridoy69@gmail.com

Abul Kalam Azad
Department of Information Technology
Assam University
Silchar, India E-mail:
abul.chosen821@gmail.com

Ajoy Kumar Khan
Department of Information Technology
Assam University
Silchar, India
E-mail: ajoyiitg@gmail.com

***Abstract*—A major breakthrough in side channel attacks came up when analysis of power consumption by a cryptographic device led to discovery of the secret key. This analysis technique popularly known as Power Analysis Attack is now one of the most volatile and successful side channel attacks. This technique uses the power consumed by a cryptographic system as the main parameter to identify the cryptographic algorithms as well as the secret key used. The power traces of the system are statistically analyzed and the correlation between these traces and the cryptographic technique is explored to break the security. This attack has been successfully carried out on various cryptographic algorithms like DES, AES, RSA and ECC which are implemented on cryptographic devices such smart cards, FPGA, DSP, ASIC etc. In this paper we present a review on the power analysis attack and its techniques. Also, a brief detail on some of the power analysis attacks on smart card and FPGA have been presented. Couple of methods to improve such attacks has also been mentioned**

Keywords—cryptosystem, power analysis, SPA, DPA, CMOS, smart cards

I. INTRODUCTION

Side channel attacks as the name suggests, uses the additional physical information like noise, power, fault, time etc. of a cryptographic device known as side channel information for breaking the security of that system. This information may be the power consumption, electromagnetic radiation, sound, time, fault etc. that can be easily traced from the system. Power analysis attack is one of the most popular and volatile side channel attacks. For this kind, the power consumed by the system to execute its operations is used to identify the cryptographic technique used and the secret key. The power traces are collected and then analyzed to find a correlation among them and finally detect the key from it. Encryption techniques like DES, RSA, AES etc. are already vulnerable to this kind of attack. The popularity of smart cards has a major impact on the attackers to use this new technique and break the security of a cryptosystem.

The rest of the paper is organized in five sections. The next section gives a detail on power analysis attack and smart cards. Section 3 explains the two types by which power analysis can be done. Section 4 and 5 elaborates some of the existing power analysis and methods to improve such attack. Section 6 states some of the common countermeasures on various devices available on literature. Finally a conclusion is formulated.

II. SMART CARD AND POWER ANALYSIS ATTACK

Smart cards are primary mode of authentication and secure transactions in today's scenario. They use some cryptographic algorithms which may be symmetrical or asymmetrical like AES, RSA, triple DES etc. for their purpose of security [14]. Even though these algorithms and protocols are highly secured, but the smart cards uses additional external devices to operate which are prone to side channel attacks.

Smart card consists of circuits containing microprocessor, which are mainly based on CMOS gates. CMOS gates have mainly three power sources, first is the leakage currents in transistors, second the short-circuit currents during the switching of a gate during simultaneous conduction of NMOS and PMOS and lastly, the dynamic power consumption which is due to the charge and discharge of the load capacitance [2]. The dotted paths as shown below in figure 1 represent the load capacitance C_L.

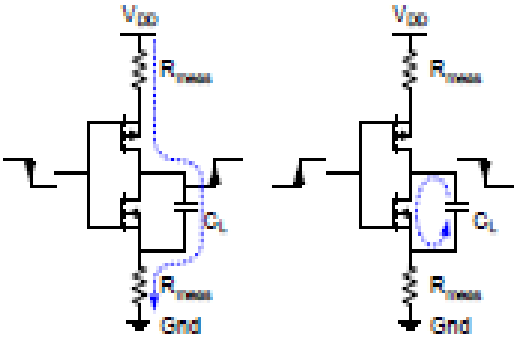

Fig 1: Charge and discharge of capacitor in CMOS[2]

Equation 1 here represents the dynamic power consumed by the CMOS gates [2]:

$$P_{dyn} = C_L V^2_{DD} P_{0\rightarrow1} f \quad (1)$$

where $P_{0\rightarrow1}f$ is called the switching activity with $P_{0\rightarrow1}$ being the probability of 0→1 transition, f and V_{DD} are the working frequency and voltage of the power supply of the particular device. Figure 2 shows the circuit for monitoring the power dissipation by the device at the ground pin V_{ss} of the smart card by connecting a small resistor R_1 in series between the V_{ss} pin and the ground. Current monitoring through R_1 creates a time varying voltage, which can be sampled with the help of a digital oscilloscope. The same current is responsible for charging and discharging of the capacitors C_1, C_2 and C_{load} which flows out of the smart card through a bond wire I_{bond} that acts like an inductor. For every smart card the values of inductor and the capacitors are different and will determine the shape of the power signal that is observed at the V_{scope} [5]. In a typical smart card microprocessor, the gates attached to internal buses dissipates a larger portion of the power. These internal buses have large capacitive loads that can readily leak information to attackers making the smart cards vulnerable to power analysis attack.

III. TYPES OF POWER ANALYSIS ATTACK

Power analysis attacks are classified into two type's viz. simple power analysis (SPA) and differential power analysis attack (DPA). Further differential power analysis is enhanced to high order differential power analysis for greater accuracy [11]. Below we explain these both techniques in detail.

A. *Simple Power Analysis*

Simple Power Analysis (SPA) implements direct interpretation of the power consumption measurements collected during cryptographic operations [1] from a device. SPA can depict information about the device`s operation as well as secret key material. It involves providing some random inputs to the cryptographic device and then visually inspecting its power consumption throughout.

The attacker could measure the power consumption waveforms of the device and store the data using a digital Oscilloscope and later process the information to extract the secret key [2]. The waveforms can be seen in figure 3 showing the 16 rounds of DES are clearly visible and figure 4 showing details of the rounds in the DES.

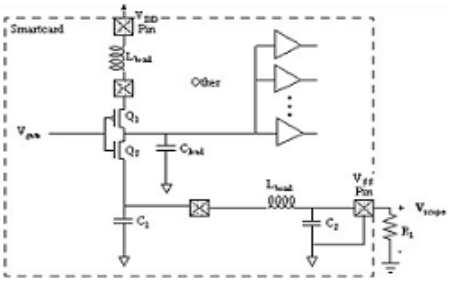

Fig 2: Circuit for measuring power consumption of a smart card [5]

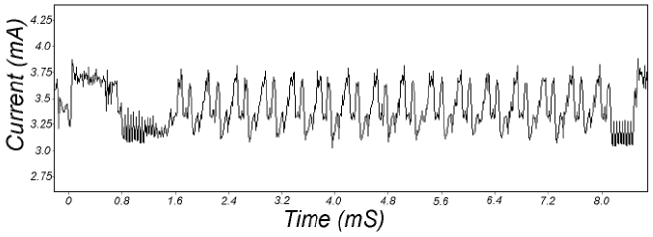

Fig 3: SPA showing trace of DES [3]

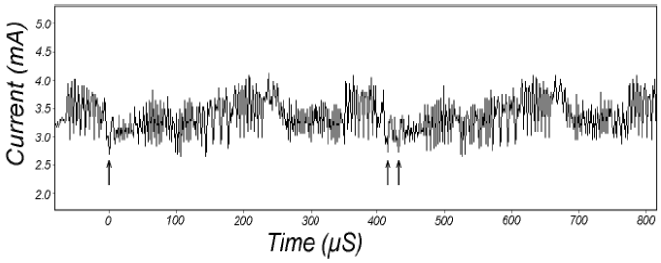

Fig 4. SPA showing trace of round 2 and 3 of DES [3]

B. *Differential Power Analysis*

Differential power analysis (DPA) attack passively performs external observation of the power consumed by a circuit performing cryptographic computations. Unlike SPA, DPA is based on the theory that the power consumption of a computational logic is statistically correlated with the internal bit transition [7]. An important factor leading to successful DPA attack is use of correct power model. If the power model is well described, the number of traces required may be substantially less with the noise involved. There are different power models for DPA, however most commonly used are Hamming-Distance model and Hamming–Weight model [6] as the correlation between the distance and weight can easily depict the key used.

Hamming-Distance model counts the number of 1→0 and 0→1 transitions that occur in the cryptographic device while executing the cryptographic algorithm. Number of transition occurred describes the power consumption of the cryptographic device at a particular time interval. Whereas, Hamming-Weight model is much simpler than Hamming-Distance model. Here the only number of 1's in a set of data needs to be examined to find the power traces [6]. Figure 5 below shows the DPA trace from a typical smart card

showing the power consumption difference from selecting one input bit to a DES encryption technique.

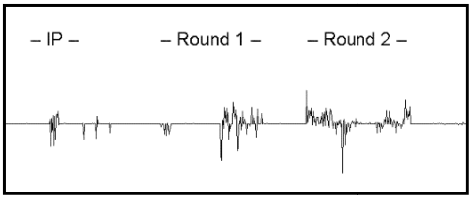

Fig 5: DPA traces from a typical smart card [2]

IV. REVIEW ON POWER ANALYSIS ATTACKS

A DPA attack can be more perilous than SPA, as it can be performed with little details on how the algorithm was actually implemented. The technique can gain more strength if some statistical analysis method is used to recover the side channel information [11]. Below some of the DPA techniques that have been implemented on smart cards and FPGA that are available in literature have been reviewed.

A. DPA Attack on Smart Card Running DES algorithim

A DPA attack starts by running the encryption algorithm for N random plaintext inputs. Song Sun et. al. in [6] explained a DPA attack where they record N random plaintexts and their corresponding power in a matrix represented as PT [N][M]. The voltage value on power trace PT [i] at particular time j can be given by PT [i][j]. The attacker can determine the values of N and M. The accuracy in guessing the final extracted key depends on the value of N i.e. the higher is N, the more is the accuracy. The value of M influences the power-sampling rate. A larger M implies a higher power-sampling rate [6]. After that the attackers choose an output bit of the first round S-box, say it be the first output bit b_0 which depends on the other six bits of the secret key and plaintext. The attacker makes an initial guess of those key bits based on which one can compute the guessed value of b_0. Since b_0 can be either 0 or 1, the entire power traces samples can be grouped into two sets. Those traces whose theoretical value of b_0 is 0 they are assigned into the first set otherwise it is assigned into the second set [6][17]. Figure 6 shows a typical S-box for DES algorithm. Once all the power trace values or the inputs have been collected, the average power is calculated using the following equations [6]:

$$P^j A = \frac{1}{|A|}\sum_{i=1}^{|A|} P[i][j] \quad (2)$$

$$P^j B = \frac{1}{|B|}\sum_{i=1}^{|B|} P[i][j] \quad (3)$$

If the attacker makes correct guess of the key bit then the computed value of bit b_0 will be same as the actual value with a probability of 1 else it will be different with probability 0.5 [5][6].

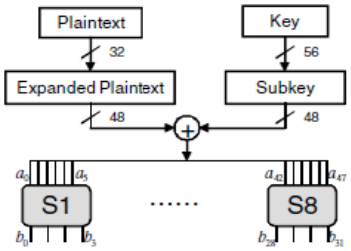

Fig 6: Structure of the S-box in a round of DES [6]

B. Differential Power Analysis Attack on FPGA running AES

The AES takes up 128-bit plain text and 128-bit key to produce 128-bit cipher text. Each round has a round key say K_{11} computed from the original key. Attacker attacks the last round key K_{11} as the original key can be calculated from this round because of its reversible nature [15]. In [10], Velegalati et. al. have performed the attack on AES in Output Feedback (OFB) mode where the output from the previous encryption was given as input for the next encryption. The power consumption for the last round was compared to a measurement of the power consumption in the 11^{th} clock cycle. They considered that for some plain text P_{11} of the 11^{th} round with key K_{11} the cipher text was obtained by,

$$C_{11} = K_{11} \text{ XOR (Shift row (sub byte } (P_{11}))) \quad (4)$$

With unknown plaintext and key, guesses were made using the known cipher text C_{11}. Different values of K_{11} were guessed and using equation 5, the plain text P_{11} was computed.

$$P_{11} = \text{sub byte}^{-1} (\text{shift rows}^{-1}(K_{11(guess)} \text{ XOR } C_{11})) \quad (5)$$

Hamming distance model was then used to depict the hypothetical power.

The correlation between the powers measured by the attacker using guessed keys (P_{guess})and actual power consumed by the system ($P_{measured}$)was found using some correlation function based on cross-covariance as in equation 6.

$$\text{Max } f_{Cor}(K_{11}) = \text{correlation coefficient } (P_{guessed}, P_{measured}) \quad (6)$$

The maximum value of the correlation is the correct key of the last round. However, the correlation may not give the correct key, due to lots of noise in the measured current. The effect of noise can be removed using thousands of combinations of plaintext-cipher text for the same key are measured. The method is repeated until the complete key round was found. After obtaining the round key the actual key can be obtained as in [10].

C. Correlation Power Analysis Attack on Smart Card

DPA has an issue of "ghost peaks" where peaks occurs even at wrong guess of the attacker. Correlation Power Analysis (CPA), addresses this issue by correlating and analyzing the coefficient between power and hamming weight of the data instead of only analyzing the data. CPA hence offered more robust and efficient analysis than DPA [8].

Huiyun Li et. al. in [8] proposed a new enhanced power model based on correlation analysis. Their model used the probability distribution of the intermediate data and correlates it with the hamming distance and hamming weight of the same. The correlation coefficient used in this model between any set of variables X and Y is stated in equation 7.

$$corr(X,Y) = \frac{E(X.Y) - E(X).E(Y)}{\sqrt{D(X)}.\sqrt{D(Y)}} \quad (7)$$

Where, E(X) and D(X) denotes the expectation and variance of X. Correlation coefficient represents the linear association between two sets of variables. Instead of using this correlation directly, its square root shifted by 1 was used.

To verify this new improved model CPA analysis was carried on a smart card running DES encryption. The correlation between the probability distribution of Hamming distance and Hamming weight used previously was found 10% less than the correlation obtained by this new improved model making it more efficient. This model was also compared with the classical hamming weight model which resulted to produce 10% better correlation coefficient as compared to the classical model [8]. Hence, CPA can give a higher success in power analysis attack.

V. IMPROVING DIFFERENTIAL POWER ANALYSIS

Although DPA has been a mainstream in making power analysis attack successful, it needs to be improved for higher robustness and efficiency. In DPA, efficiency can be termed as making the correct guess with minimum number of power traces.

One of the important factor which hurdles in the success of DPA is the noise that accompanies the power traces. Due to which it is difficult to measure the actual power consumptions. Kocher et. al. performed DPA by averaging to reduce the noise however many other strategies can exist. In [5] Messerges et. al. have stated that there can be five different types of noise which may be present during like external, intrinsic, algorithmic, quantization and sampling which appears from different sources. Filtering may remove noise but with care that, it doesn't hamper the components creating power traces. Messerges et. al. have developed a signal-to-noise ratio (SNR) model for DPA which explores the noise present in the bias signal. The SNR was considered for both a single as well as all the bias signals. They referred them as *intrasignal* SNR and *intersignal* SNR respectively. The model used mean and variance of the the distribution to describe the *intrasignal* SNR [5]. The *intrasignal* SNR was described as in equation 8 below.

$$SNR = \frac{\varepsilon\sqrt{N}}{\sqrt{8\sigma^2 + \varepsilon^2(\alpha n + n - 1)}} \quad (8)$$

Where, N is the number of signals of an n-bit processor with signal size □, σ^2 the average non algorithmic variance and ∞ the percentage of algorithmic noise. The *intersignal* SNR is dependent on the algorithm and function used for the attack. The *intersignal* SNR was as like the *intrasignal* SNR in the model. It was large enough whenever the *intrasignal* SNR was large.

The typical assumption of power leakage information is mainly focused on leakage at logic level and instruction levels. This is because most of the cryptographic algorithms are directly implemented in hardware [7]. However, the fact that the leakage of power can be controlled at early stages of design is completely ignored. In [7], Kreig et. al. have proposed a power emulation hardware which is capable of tracing power at reasonable level. Their work contributes with a semi-automatic switching activity-aware power characterization process and a data dependent power model for hardware accelerated security evaluations [7]. Their approach used power emulation methodology which could speed up the power estimation and faster generation of power traces highly supportive for DPA. The model mainly had two phases: profiling phase and analysis phase. In profiling phase, the power profile was traced using run time tracing with help of a power emulation unit or using some RTL simulations. One the traces were available they were analyzed in the second phase using some analysis toolkit.

For acceptability they tested their model in AES algorithm which resulted in less than 7% average and 20% root mean square (RMS) error [7].

VI. COUNTERMEASURES FOR POWER ANALYSIS ATTACKS

Smart card used for secure and reliable transaction is under the web of power analysis attack leading to failure of security and confidentiality of the cryptographic algorithms and systems. Thus, some countermeasures have to be introduced to prevent the cryptographic systems from such attacks.

It has been found that avoidance of procedures which uses secret intermediate or key for conditional branching can limit the expose of many SPA characteristics. Conditional branching can be avoided by using AND,OR and XOR operation in place of "if" clause [1].

Balancing of power consumption into a constant value with the use of dummy register and gate prevents power analysis attack. Dummy registers are the places where useless operations are made to assure that the total power of the unit remain constant when a useful operation is performed [12].

Addition of noise into power consumption measurement acts as another countermeasure for such attacks. When an extra amount of noise is introduced, the number of sample required for an attack increases possibly to an unfeasibly large number [5].

Modification of algorithm is also an approach to prevent the power analysis attack. When some modification is invoked it prevents the correlation among the power traces. Modification like non-linear key updating destroys the partial information of the key collected by the attacker [1].

Also the aggressive use of exponent and modulus multiplication processes in public key schemes prevents collecting data from large number of operations [1].

Introducing randomized elements into the instruction at the cost of small performance degradation can be a simple and easily implemented countermeasure for DPA [8].

VII. CONCLUSION

This paper presents a review on power analysis attack, which is one of the most powerful and volatile attacks in today's security aspects. Power analysis attack challenges the vulnerability of most of the encryption techniques used to maintain security. Use of smart cards has given attackers a medium to perform such attacks as smart cards can easily leave traces of the power used to execute its operations. The two most common ways of power analysis, SPA and DPA are briefly explained here. Also, a review on some of the power analysis attacks on smart cards and FPGA have been explained in brief. Methods to improve the existing DPA have also been stated in brief. Finally, some of the popular countermeasures for such attack, which can prevent a cryptographic system from being attacked, have been formulated.

Acknowledgement

The research presented in the paper have been supported by Department of Electronics and Information Technology (DeitY), Government of India

REFERENCES

[1]. Hagai Bar-El "Introduction to side channel attacks." *Discretix Technologies Ltd* 43 (2003).

[2]. Francois-Xavier Standaert. "Introduction to side-channel attacks." *Secure Integrated Circuits and Systems*. Springer US. pp-27-42.2010

[3]. Paul Kocher, Joshua Jaffe, and Benjamin Jun. "Differential power analysis."*Advances in Cryptology—CRYPTO'99*. *Springer Berlin/Heidelberg*, 1999.

[4]. Shuo Chen, Rui Wang, Xiao Feng Wang, Kehuan Zhang "Side-channel leaks in web applications: A reality today, a challenge tomorrow." In *Security and Privacy (SP), IEEE Symposium on* (pp. 191-206). IEEE*2010*.

[5]. Thomas S. Messerges, Ezzat A. Dabbish and Rober H. Sloan "Examining Smart-Card Security under the Threat of Power Analysis Attacks." *IEEE TRANSACTION ON COMPUTERS*. Vol. 51 No.5. IEEE, 2002.

[6]. Song Sun, Zijun Yan and Joseph Zambreno, "Experiments in Attacking FPGA-Based Embedded Systems using Differential Power Analysis."*IEEE*. 2008.

[7]. Armin Krieg, Christian Bachmann, Johannesv Grinschgl, Christian Steger, Reinhold Weiss and Josef Haid, "Accelerating Early Design Phase Differential Power Analysis using Power Emulation Techniques."*IEEE*. 2011.

[8]. Huiyun Li, Keke Wu, Bo Peng, Yiwei Zhang, Xinjian Zheng and Fengqi Yu, "Enhanced Correlation Power Analysis Attack on Smart Card.."*The 9th international Conference for Young Computer Scientists*. IEEE, 2008.

[9]. Thomas S. Messerges, EzzyA. Dabbish, Robert H. Sloan. "Power Analysis Attacks of Modular Exponentiation in Smart Cards."*CHES`99,LNCS 1717,pp.144-157*. 1999.

[10]. Rajesh Velegalati and Panasayya SVVK Yalla. "Differential power analysis attack on FPGA implementation of AES." *George Mason University publisher*, 2008.

[11]. Thomas S. Messerges, Ezzat A. Dabbish and Rober H. Sloan "Investigations of Power Analysis Attacks on Smart Cards." *Prc USENIX workshop Smartcard Technology,*pp.151-161,May 1999

[12]. Thomas S. Messerges and Robert Adviser-Sloan. "Power analysis attacks and countermeasures for cryptographic algorithms."*University of Illinois at Chicago*, 2000.

[13]. Louis Goubin and Jacques Patarin. "DES and differential power analysis the "duplication" method." *Cryptographic Hardware and Embedded Systems*. Springer Berlin Heidelberg, 1999

[14]. R. Mayer-Sommer. "Smartly analyzing the simplicity and the power of simple power analysis on smartcards." In *Cryptographic Hardware and Embedded Systems—CHES 2000,* pp. 78-92. Springer Berlin Heidelberg, 2000.

[15]. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. "Power analysis attacks: Revealing the secrets of smart cards."*Vol. 31. Springer,* 2008.

[16]. Eli Biham and Adi Shamir. "Differential cryptanalysis of the full 16-round DES."*Springer New York*, 1993.

[17]. Eli Biham and Adi Shamir. "Differential cryptanalysis of DES-like cryptosystems." *Journal of CRYPTOLOGY* 4.1 pp:3-72, 1991.