A Novel and Efficient countermeasure against Power Analysis Attacks using Elliptic Curve Cryptography

M.Prabu
Research Scholar,
Anna University Coimbatore,
Tamil Nadu, India
prabu_pdas@yahoo.co.in ,

R.Shanmugalakshmi
Assistant Professor/CSE,
Government College of Technology,
Tamil Nadu, India
shanmuga_lakshmi@yahoo.co.in

Abstract- **Recently, there is a leakage in the communication channel information by the cryptographic processors. It is the major chore to overcome the pouring out or spreading out of the secure data. In this paper, a new level of security analysis model is constructed in power analysis using Elliptic Curve Cryptography. And so many side channel attacks and their countermeasures are explained undeniably. An algorithm design based on power analysis is also described and it makes our countermeasure more secure against simple power analysis, differential power analysis and other attacks. The theoretical analysis based on these result has been shown and it represents how the algorithm design should fluctuate from the facade side channel attacks.**

Keywords-component Simple Power Analysis, Differential Power Analysis, Security Analysis Model, Algorithm design, Side Channel Attacks

I. INTRODUCTION

Data are poured out by the cryptographic processors, as power consumption, electromagnetic emission and during the computing time of an encryption/decryption operation. These information leakages are known as side channel information. Side channel attacks are based on these side channel information.

In customary, cryptographic attacks are based on the cipher text, by choosing the accurate key for capturing the plain text, but now a days side channel attacks are focused in a different manner such as VLSI based on implementation of the cryptographic algorithm.

This paper gives a brief introduction about the side channel attacks and their countermeasures. Then, as the base of proposed basic security analysis model, the levels of analysis attacks are compared to security levels. Finally a brief case study of power analysis attacks and a special design based on countermeasure are explained clearly.

II. ATTACKS

Normally attacks can be categorized as passive and active attacks. Based on the observation of side channel information the two attacks can be explained as follows. The passive attacks are used to gain the information on the particular event and receive all the information including key values and the power consumption of the key events. Active attacks make many changes and create an abnormal behavior and erroneous computation on results while tracing out the information from the particular event.

A.Fault Attacks

Fault attacks and agitate on electronic devices have been examined since 1970's in an aerospace industry. The first embedded cryptographic implementation has been finalized in 1997, when D.Boneh, R.Demillo and R.Lipton [18] published the first theoretical attacks. This attack is called bellcore attack. After the first theoretical attack, lenstra wrote new and short notes [23] to listen and know about the attacks.

The note has been supported to develop an improved version of the attacks. According to computation error, the bellcore researchers showed how to recover the secret prime factors p and q of modulo n from two different signatures for the single message. Again Lenstra showed only one fault signature is required where the message is also known. I.Biham and A. Shamir [6] were developed the first Different Fault Analysis (DFA) on symmetric algorithm applies to DES in 1997. These types of attacks are basic things to identify and design the products secure and at the same time it is essential to find the analysis based on these attacks.

III. ROLE OF POWER ANALYSIS

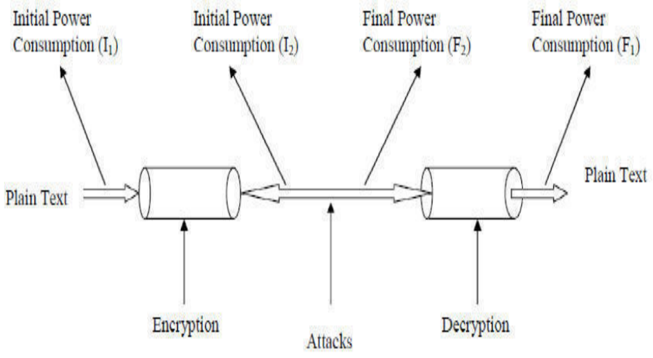
Initial Power Consumption (I_1)
Initial Power Consumption (I_2)
Final Power Consumption (F_2)
Final Power Consumption (F_1)
Plain Text
Plain Text
Encryption
Attacks
Decryption

Figure 1. Role of Power Analysis

IV. SIDE CHANNEL ATTACKS

The detection of an encryption key is mainly based on side channel signal; the signal -to-noise ratio (SNR) may significantly influence the key guess accuracy [7]. While some of the early side channel attacks targeted the hardware implementation, it also targets software implementation equally, if not more vulnerable. Early side channel attack techniques are based on analyzing the chip's functional characteristic for retrieving information. The side channel information is used to analyses the leakage of unintended information from an unprotected device while implementing the cryptographic algorithms.

V. COUNTERMEASURES

Two general countermeasures are obfuscation and tamper-proofing. Obfuscation technique is used to conceal the meaning of certain computation by making it obscure and harder to understand .Code obfuscation [14, 21, and 22] has been proposed previously as a technique to limit side channel information leakage.

A. Nature of Obfuscation

It propose an algorithm consisting of so many line coding, each and every instructions coding can be executive depending on their input values [14]. The side channel information hack the instruction coding and fetch an unrelated coding to the particular hacked part .To solution for this problem is to create the code in which the different path of the execution path over different execution cycles takes different amount of time. This solution is used to avoid the fake instruction codes. Some of the techniques can be classified as follows.

1). Independent Data Performance

Each and every data is being proceeded independently to calculate the amount of time for performing the operation.

2). Blinding

This technique is stirred from blind signature [23]. It is the best method to prevent the electromagnetic side channel attacks.

B.Tamper –Proofing

This technique is used to cover the data from the side channel attack. The main obstruct factor of building sensor nodes in tamper proof bodies is its cost. It is used to avoid the environmental factor attack, by increasing the overall performance of the data [1].The side channel attacks can be classified as Power analysis attack, electromagnetic attack, timing attack, fault analysis attack and traffic analysis attack [19].

VI. POWER ANALYSIS ATTACKS

Power analysis attacks are inspired from side channel attacks. It is an implementation attack, depending on the physical aspects such as mathematical implementation and hardware implementation [2]. Normally the power analysis techniques try to solve the power based problems in different views, such as hardware design and interaction between instructions set process architecture. Kocher has been [3] introduced the concepts of power attacks in the examples of SPA and DPA

A. Simple Power Analysis Attack

It is a key technique to measure a single value to gain the secret key information of the device. It scans each and every cryptographic execution [15, 16]. Especially, it calculates or trace out the individual encryption/decryption operation's power consumption. Even if an algorithm is protected against SPA, it may be vulnerable to DPA.DPA is similar to SPA, but it consists of so many analysis techniques.

B. Differential Power Analysis Attack

DPA attacks can be classified as two modules namely data collection and statistical analysis phase.

1). Data Collection

Discrete power signals are the basis for a DPA attacks. The signal Pi,j is the execution encryption algorithm for N different random input Mi The index i corresponds to the execution number of the algorithm and the index j to the execution time. [7]

2). Statistical Data Analysis

A key dependent partition function D is chosen for analyzing the statistical data. The function D is chosen such that it represents a specific bit x of an intermediate value of the algorithm which is directly dependent on a part of the message Ms and on a part of the secret key Kb. [7] x = D (Ms, Kb)

VII. NOISE ANALYSIS ATTACK

The DPA attack is used to reduce the noise performance [10], but it is important to investigate other strategies leading to further reduction in the amount of noise. Noise can be classified as External, Internal, and Quantization.

A. External & Internal

External is generated by external source. Intrinsic is due to the random movement of charge carrier within conductions.

B.Quantization

Due to quantization the analog to digital conversion is used to sample the power analysis. The result presented in this paper confirms that power analysis attacks can be quite powerful and need to be addressed.

VIII. FAULT ANALYSIS ATTACKS

An error occurs when a cryptographic device is in progress, this type of attack is called fault analysis attack. Errors are produced due to non-malicious agents such as hardware failures, software bugs and the external noise.

A malicious process, which has access to the physical device in reverse to Non- Malicious Agents. Non-malicious agents and the fault analysis attacks don't create any significant work. A malicious process is a process in which any data before computation will be verified thoroughly and errors are detected using error control techniques in internal memory [4, 5]. These types of precaution are used to avoid the fault analysis attacks.

A.EC Digital Signature Generation

Let p be a prime (or) a power of two and let E be an elliptic curve defined over Fp[20].Let A be a pint on E having prime order q.Such that the discrete logarithm problem in (A) is in infeasible.

Let P= {0,1} * A=Zq* X Zq*
And define k={(p,q,E,A,m,B); B=mA}

Where 0≤m≤ q-1, the values p,a,E,A and B are the public key and m is the private key for k=(p,a,E,A,m,B) and a random number k,1≤ k≤q-1 ,define
Sig k(x,k)=(r,s)
KA=(u,v)
R=u mod q
s=k-1 (SHA-1(x)+mr)mod q

Before entering the parameter, it is necessary to verify each and every signature generation parameters. For example p, a, E, A, m, B and the input parameter and input message are verified before entering through the computation. These types of precautions are used to avoid the fault analysis attacks[24].

IX. ELECTROMAGNETIC ATTACKS

This type of attack is purely based on hardware generated emissions especially emission from modules of cryptographic algorithms. Electromagnetic attacks are more powerful than power analysis attacks. Similar to power analysis the electromagnetic attacks can be classified as Simple Electromagnetic Analysis (SEMA) and Differential Electromagnetic Analysis (DEMA).To trounce electromagnetic attacks is to use masking methods [11, 13]. Masking method is a scheme, which is an intermediate variable .It doesn't support dependent access of secret keys. The countermeasures are implemented by preventing or complicating the power analysis attacks. With tamper resistant body it can be achieved in so many ways.

A. Embedded the module in chip

These types of techniques built the modules in chip which increases the noise to the power consumption. This countermeasure is easily implemented but it is not efficient. It adds the manufacture cost of the device.

B. Obfuscation

Is a good solution to prevent SPA, but is susceptible to DPA

X. TRAFFIC ANALYSIS ATTACK

Traffic analysis is purely based on network topological information. Hub plays a major role to activate the traffic analysis attack [17]. Hub is used to gather information and pre process them before relaying. This makes aggregator nodes an attractive target of side channel attacks. To identify the valid node through the high probability of occurrence during computation activates at a node.

XI. TIMING ATTACK

This attack incorporates the variance in execution time at different levels in cryptosystem .It utilize the slow processors [18]. The slow processors will enhance even small difference in computation time over different levels. The countermeasures for the timing attacks, is to use more clock cycles for each and every execution independent level and doesn't affect the execution time.

XII. POWER ANALYSIS ATTACKS- A CASE STUDY

A. Elliptic Curve Scalar Multiplication

An elliptic curve is a set of points P which denotes the solution for the cubic equation over a field [11]. These fields are called as finite fields. The finite fields can be classified as prime finite field and binary finite field.

In Elliptic Curve Cryptography, the secret key d is engaged in the scalar multiplication operation, where scalar multiplication is comprehend completely by recurring addition of the same point. If d is a positive integer and P is a point on an elliptic curve, the scalar multiplication dP is the result of adding d copies of P [12, 13]

$$dP = \underbrace{P+P+\ldots+P}_{d}$$

There are two implementations of scalar multiplication algorithm, namely Binary Method [14] shown in algorithm 1 and Montgomery method [9] shown in Algorithm 2. Scalar Multiplication (Binary Method)

```
Algorithm 1:
Input d= (dn-1………d0) (dn-1=1)
Q ←P
For i from n-2 to 0 to…
     Q←2Q
If di=1 then Q←Q+P
Return (Q)
Out put dP
```

Scalar Multiplication (Montgomery Method)

```
Algorithm 2
Input d=(dn-1………d0) (dn-1=1)
Q([0] ← P.Q[1] ←2P
For i= n-2 to 0…..
Q[1-di] ←Q[0]+Q[1]
Q[di] ←2Q[di]
Return (Q[0])
Output dP
```

The scalar multiplication implementation contains both point addition and point doubling. The key d determines the procedure for doubling and addition operation. [9]

1). Binary Method

If key bit = 0, then it accepts and activates the point doubling operation If key bit = 1, then it accepts and activates the point addition operation

2).Montgomery Method

This method doesn't consider the key bit sizes [16]. Whatever the key size may be both the point doubling and point addition are executed. By measuring the power consumption during the ECC operation, the attackers can retrieve the secret key.

XIII. BASIC SECURITY ANALYSIS MODEL

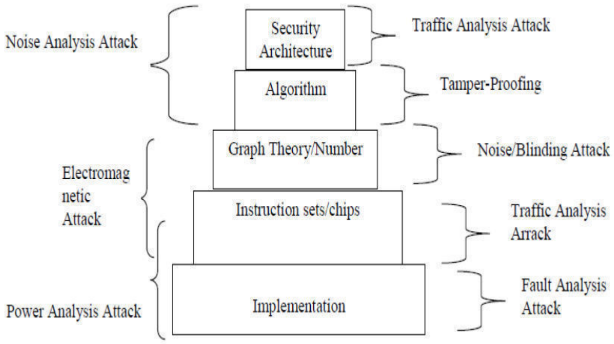

Figure 2.Basic Security Analysis Model

XIV. CONCLUSION

In this paper, we have shown a new level of security analysis model and explained a case study for power analysis attacks based on algorithm design. The paper proposed a countermeasure for ECC against simple power analysis attacks, with balanced operation procedure for point doubling and addition during a scalar multiplication implementation. And this paper also suggests, what are the countermeasures are used to solve the design based power analysis attacks. The further study of the algorithm design and the side channel attack information will help to improve the level of security to implement hardware based designs.

ACKNOWLEDGEMENT

I would like to thank Dr.R.Shanmugalakshmi for her fruitful comments and suggestion on the preliminary version of this paper.

REFERENCES

[1]. Thomas S.Messerges, Zzat A.Dabbish, Robert H.Sloan, "Examing Smart-card Security under the threat of Power Analysis", IEEE Transactions on Computers, Vol 51, and No: 5, May 2002, Page No: 541-552

[2]. Girish.B.Ratanpal,Ronald ,D.Williams, Travis N.Blalock, " An On-Chip Signal Suppression Countermeasures the power Analysis Attacks", IEEE Transactions on Dependable and Secure computing, Vol:1,No:3,July-September 2004, Pg No:179- 189

[3] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," ser. Lecture Notes in Computer Science, M. J. Wiener, Ed., vol. 1666. Springer, 1999, pp. 388–397.

[4]. Keke Wu ,Huiyun Li, Tingding Chen, Fengqi Yu "Simple Power Analysis on Elliptic Curve Cryptosystems and Countermeasures: Practical Work", 2009Second International Symposium on Electronic Commerce and Security, DOI 10.1109/ISECS.2009.7

[5] Francois-xavier standert,Eric peters, Gael Rouvroy & Jean-Jacques Quisquater, "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays", Proceedings of the IEEE, Vol. 94, No. 2, Feb 2006, DOI 10.1109/JPROC.2005.862437

[6]. Thomas Popp,Stefan Mangard,Elisabeth Oswald "Power Analysis Attacks and Countermeasures" IEEE Design & Test of Computers 2007,Pg No:535-544

[7] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems In Burton S. Kaliski Jr., editor, Advances in Cryptology - CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pages 513–525. Springer, 1997.

[8] Jens R¨udinger, Adolf Finger, "Key Dependent Operation and Algorithm Specific cryptographic protocols for faults (extended abstract). In EUROCRYPT, pages 37–51, 1997.

[9] P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods for Factorizations," Mathematics of Computation, vol. 48, pp. 243- 264, 1987.

[10]. Radu Muresan, Member, IEEE, and Stefano Gregori, Senior Member, IEEE "Protection Circuit against Differential Power Analysis Attacks for Smart Cards", IEEE Transactions on Computers, Vol. 57, No. 11, Nov 2008, DOI 10.1109/TC.2008.107, Pg No:1540-1549

[11] A. J. Menezes, "Elliptic Curve Public Key Cryptosystems," Kluwer Academic Publishers, Norwell, 1993.

[12] IEEE Std-1363-2000: Standard Specifications for Public Key Cryptography, January 2000.

[13] X. F. Tang, "The VLSI Implementation of Elliptic Curve Cryptography IP," Master Thesis, Circuits and Systems of Department of Electric Engineering of Zhejiang University, China, February 2004.

[14] J. Wang, "A Dual-Field Algorithm for Elliptic Curve Cryptosystem and Its Hardware Implementation," PhD Thesis, In PhD Thesis, microelectronics and Solid State electronics of Peking University, China, June 2008.

[15]. Da-Zhi Sun, Jin-Peng Huai, Ji-Zhou Sun, Zhen-Fu Cao "An Efficient Modular Exponentiation Algorithm against Simple Power Analysis Attacks" , IEEE Transactions on Consumer Electronics, Vol. 53, No. 4, Nov 2007, Pg .No:1718- 1723

[16]. M. Bucci L. Giancane R. Luzzi M. Marino G. Scotti,A. Trifiletti, "Enhancing power analysis attacks against cryptographic devices" IET Circuits Devices System., 2008, Vol. 2, No. 3, pp. 298–305, doi: 10.1049/iet-cds:20070166

[17]. A. Zadali mohammad kootiani,A. Golabpour,M. Doostari,M. Broujerdian, "Differential Power Analysis in the Smart card by Data simulation" DOI 10.1109/MMIT.2008.192,Pg No:817-821

[18]. M. Joye and J. Quisquater, "Hessian Elliptic Curves and Side-channel Attacks", CHES 2001, Lecture Notes in Computer Science 2162, 402-410.

[19] Amir Moradi a,*, Mohammad Taghi Manzuri Shalmani a, Mahmoud Salmasizadeh , "Dual-rail transition logic: A logic style for counteracting power analysis attacks" Computers and Electrical Engineering 35 (2009) 359–369, Elsevier, doi:10.1016/j.compeleceng.2008.06.004

[20]. Santosh Ghosh *, Monjur Alam, Dipanwita Roy Chowdhury, Indranil Sen Gupta," Parallel crypto-devices for GF(p) elliptic curve multiplication resistant against side channel attacks", Computers and Electrical Engineering 35 (2009) 329–338, doi:10.1016/j.compeleceng.2008.06.009

[21]. Ning Zhang a,*, Zhixiong Chen a,b, Guozhen Xiao, "Efficient elliptic curve scalar multiplication algorithms resistant to power analysis", An International Journal of Information Science, doi:10.1016/j.ins.2006.12.016

[22]. JeongChoon Ryoo, Dong-Guk Han, Sung-Kyoung Kim, and Sangjin Lee, "Performance Enhancement of Differential Power Analysis Attacks With Signal Companding Methods", IEEE Signal Processing Letters, Vol. 15, 2008, DOI : 10.1109/LSP.2008.2002930, Pg No:625-628

[23] A.K. Lenstra. Memo on RSA signature generation in the presence of faults. 1996.

AUTHORS PROFILE

M.Prabu is working as a Lecturer in the Department of Computer Science and Engineering in Adhiyamaan college of Engineering, Hosur, Tamil Nadu, India. He is presently doing his Ph.D in Anna University, Coimbatore, India. He has published more than 5 International/National journals. His area of interest are computer Networks, Information Security and Cryptography. He is a life member of ISTE,IE, IACSIT and IAENG.

Dr. R.Shanmugalakshmi is working as an Assistant Professor in the Department of Computer Science and Engineering in Government College of Technology, Coimbatore, India. She has published more than 40 International/National journals. Her research areas include Image Processing, Neural Networks, Information Security and Cryptography. She has received Vijya Ratna Award from Indian International Friendship Society in the year 1996, Mahila Jyothi Award from Integrated Council for Socio-Economic Progress in the year 2001 and Eminent Educationalist Award from International Institute of Management, New Delhi in the year 2008.She is a member of Computer Society of India,{
ISTE and FIE.