An Overview of Side Channel Attacks and Its Countermeasures using Elliptic Curve Cryptography

M.Prabu
Research Scholar
Anna University Coimbatore
Tamil Nadu, India

R.Shanmugalakshmi
Assistant Professor/CSE
Government College of Technology
Tamil Nadu, India

Abstract **In order to provide security the electronic devices and their execution systems contain implementations of cryptographic algorithms. This paper explains basic level of side channel attacks and their countermeasure. These countermeasures show the way, how to trounce the side channel attacks and describe an efficient approach to overcome the side channel attacks. Based on this approach, the paper analyzes functions over many other countermeasures such as Simple Power Analysis, Differential Power Analysis; Data bit Differential Power Analysis and Zero Value Attacks.**

Key -components
Cryptographic algorithms, Differential Power Analysis, Zero Value Attacks, Countermeasures

I. INTRODUCTION

In 1996, Paul Kocher introduced the power analysis procedure. And in 1999 he introduced types of side channel attacks. These attacks have become a major threat against tamper resistant devices [1]. Fault Attacks (FA) [2] and Single Power Analysis (SPA) [3] are the most effective power consumption techniques to disclose the secret keys. Kocher et al. [1] initially introduced the two kinds of power analysis attacks: simple power analysis (SPA) attack and differential power analysis (DPA) attack. SPA attack tries to recover the information about the secret key by simply measuring the power consumption trace of the computing device during an execution process. DPA [6],an attacker performs a statistical power analysis, which involves a secret key, taking a large number of measurement of power traces

II. TRADITIONAL ATTACKS

The traditional attacks frequently require the acquisition and manipulation of extremely large amounts of data.

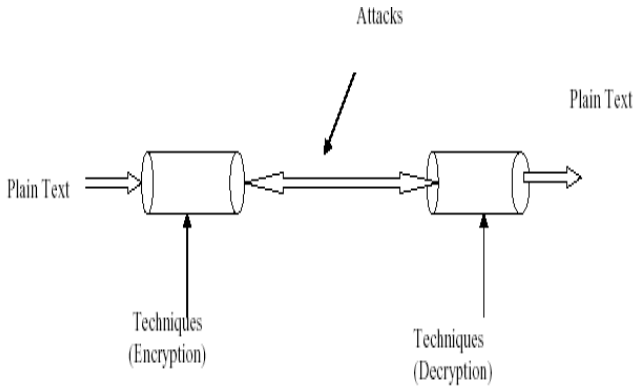

Figure.1 Traditional Attacks

III. SIDE CHANNEL ATTACKS

SCA attacks utilize the information poured out during the computation process. The side-channel attacks [7] [10], which target the security of the cryptographic devices with alarming efficiency. SCA attacks use power consumption information from the cryptosystem to extract the secret key stored in the cryptosystem, thus effectively breaking the cryptosystem.

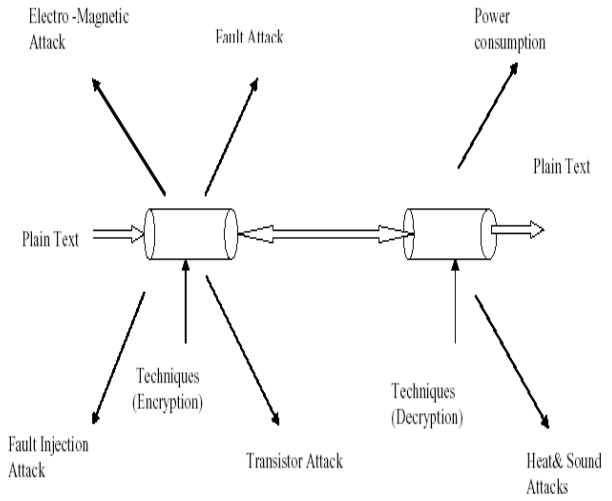

Figure 2. Side Channel Attacks

The Side Channel Attacks can be classified at three levels, Such as Actions over computation process, accessing the modules and methods used in analysis process.Actions over computation processes can be classified as two ways, such as passive attack and active attack.

3.1.Passive attack:

Passive attacks are based on the observation of side channel information such as the power consumption of the chip [12]. This is used to gain the information on the operation handled by the attackers.

3.2.Active attack:

Active attack consists in perturbing the chip processing to obtain in abnormal behavior. With the help of information the attackers can make alter or modifying the originality.

IV. SIDE CHANNEL ATTACKS

A. Differential Power Analysis

DPA is a more powerful attack than SPA. DPA attacks uses statistical analysis and Error correction Techniques to extract information correlated to keys. Two distinct steps are used to implement DPA attacks

Data Collection

Data Analysis

Data Collection for DPA may be performed as described previously by sampling the devices power consumption during Cryptographic operation in finite time[21]. The attackers directly observe the systems power consumption. With this information, the hackers may easily interrupt the system. It is difficult to sketch out the statistical and information correlated works.

B. Simple Power Analysis

SPA generally represents the visual view of the particular event's power consumption, which may be an encryption function (or) Decryption function. It observes the power consumption of one single execution of a cryptographic algorithm [21]. The power consumption varies depending on the microprocessor instruction performed. The level of SPA implementation is somewhat difficult when compared to DPA implementation.

C. Data Bit Differential Power Analysis

Data-Bit DPA (DDPA) – analyzes a relation between the secret key and the changed/not changed data of registers[17]. Consider an implementation of the Add-and-double-always Method (Algorithm 4.3). The data of register H will change only (in lines 6-10) if di = 1.

Algorithm 4.3: Add-and-double-always Method
Input: d = (dn−1. . . d0), P □ E(Fq)
Output: dP
H = P
Q = O
for i = n − 2 to 0 do
H = 2H
Q = H + P
if di = 1 then
H = Q
else
H = H
end
return H
end

D Address Bit Differential Power Analysis (ADPA)

ADPA analyzes a relation between the secret key and the addresses of registers [5]. We consider an implementation of the e.g. Add-and double- always Method (Algorithm 2.3). If di = 1, we have H Q otherwise we get H H. So if d_i changes, the register that is assigned to H will also change. This correlation draws a conclusion about the value of di.

E.Goubin's Power Analysis (GPA)

GPA is also called as Refined Power Analysis (RPA) in [17][18]. It specializes DPA to reveal the secret key by using a special elliptic curve point with a zero value defined as (x, 0) or (0, y) as described in[4]. Even after conversion, such points (rx, r·0, r) and (r·0, ry, r) (in projective coordinates) will still have a zero value. An adversary can take advantage by analyzing the computations on such a point.

F. Zero Value Attacks (ZPA)

Zero-value Point Attack (ZPA)– The previously described RPA can be generalized to ZPA,which makes use of any zero-value register computed in EC-addition or EC doubling formulas as proposed in [11]. If an attacker can choose a base point ˆ P such that a zero-value register appears during an EC-operation, he can conclude on the bit-values of the secret key starting from most significant bit (MSB).

V. ACCESSING THE MODULE

A.Invasive attack

Repackaging to get direct access to the internal components of cryptographic modules.

B. Semi-invasive attack

It involves access to the device, but without damaging the passivation layer

C. Non-invasive

It involves close observation of the devices's operation incompletely.

D. Simple Side Channel Attacks

The attack exploits the side channel output mainly depending on the performed operations[15]. It maintains single trace only. Related to the attacked instructions needs to be larger than the side channel information related to unrelated instructions. SSCA exploits in the relationship between the executed instructions and the side channel output.

E. Differential Side Channel Attacks

DSCA contains many traces, the attack exploits in the correlation between the processed data and the side channel output[15]. It is more powerful than SSCA. DSCA can be categorized by the level of actions performed namely Single output value and more (multiple) output value.

VI. EXISTING COUNTERMEASURE

- ✓ Noise Adding
- ✓ Algorithm Based

A. Noise Adding

This countermeasure adds the noise in power measurements [3]. The noise is a white noise. This noise can be easily removed in reverse operation using filters and it finds the original power rate. Several techniques are used to improve the Signal to noise Ratio of DPA trace**.**

B. Algorithm Based

The algorithm based can be classified as masking and Duplication method. The main idea behind masking is to minimize correlation between key and value. Masking introduces the noise into power consumption measurements. The countermeasure for masking needs more number of measurements to obtain the secret key. The Duplication Method in which the secret key involves interaction on both sides and independently activates partly. Duplication method develops redundant logic to inverse the hardware optimal implementation [9]. The work on masking techniques has been presented by [16][17][18][19].

VII. COUNTERMEASURE AGAINST POWER ANALYSIS ATTACKS

A. Power balancing

Power balancing techniques should be applied whenever and wherever possible. Here some dummy registers and gates are added to the main port. Normally it is a dummy operation. This operation is used to produce power balancing constant value. The same operation is performed in hardware[12], a complementary operation should be performed on a dummy element to assure that the total power consumption of the unit remains balanced according to some higher value. Each and every gate had some power consumption level, whenever added to the dummy registers (or) gates, the power consumption level is increased. It is one of the disadvantages. The same disadvantage can be overcome with the help of reduction of gates.

Size

One approach to prevent power analysis attacks is by reducing signal sizes, using the following,

Constant execution path code
Balancing hamming weights
State Transitions

B. Noise Based

An approach against power analysis involves introducing noise into power consumption measurements. Like signal size reductions[3][14], adding noise increase the number of samples required for an attack, possibly to an unfeasible large number. In addition, execution timing and order can be randomized to generate a similar effect.

C. Design

Approaches against power analysis attacks involve designing cryptosystems with realistic assumptions about the underlying hardware[13]. Non-linear key updates procedure can be employed to ensure that power traces and it can't be correlated between transitions. This approach may solve the problem, but it does require design changes in the algorithm and protocols themselves, which are likely to make the resulting product non-compliant with standards and specifications.

VIII. CONCLUSION

This paper discussed a countermeasure of elliptic curve against side channel attacks. The side channel attacks results in the leakage of information. Therefore it is vital role to take extra attention during the implementation of a crypto-

device so that it can resist different side channel attacks and that may little bit degrade the overall performance of the design.

REFERENCES

[1] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology, Proc. CRYPTO '96, N. Koblitz, ed., pp. 104-113, 1996.

[2] D. Boneh, R. DeMillo, and R. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," Advances in Cryptology, Proc. EUROCRYPT '97, W. Fumy, ed., pp. 37-51, 1997.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Advances in Cryptology, Proc. CRYPTO '99, M. Wiener, ed., pp. 388-397, 1999.

[4] Louis Goubin. A refined power-analysis attack on elliptic curve cryptosystems. In PKC '03: Proceedings of the 6th International Workshop on Theory and Practice in Public Key Cryptography, pages 199–210, London, UK, 2003. Springer-Verlag

[5]. Kouichi Itoh, Tetsuya Izu, and Masahiko Takenaka. A practical countermeasure against address-bit differential power analysis. In Cryptographic Hardware and Embedded Systems - CHES 2003, Lecture Notes in Computer Science, pages 382–396. Springer-Verlag, 2003.

[6]. P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proceedings of 19th International Advances in Cryptology Conference. CRYPTO'99*, pages 388-397, 1999

[7] P. Kocher, J. Jaffe, anad B. Jun, "Differential Power Analysis, Lecture Notes in Computer Science, vol. 16667 pp. 388-397, 1999

[8] Paul Kocher, Joshua Jaffe, and Benjamin Jun. "Differential power analysis". In M. Wiener, editor, Advances in Cryptology - CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pages 388-397.Springer-Verlag, 1999.

[9]. Vijay Sundaresan, Srividhya Rammohan and Ranga Vemuri," Defense against Side-Channel Power Analysis Attacks on Microelectronic Systems "Proceeding of IEEE, 978-1-4244-2616-4/08

[10] KUL1RD and SCARD Consortium "Intermediate report side- attacks, SCARD, Tech. Rep., January 2005.

[11] Toru Akishita and Tsuyoshi Takagi. Zero-value point attacks on elliptic Curve cryptosystem. In Information Security, 6th International Conference, volume 2851 of Lecture Notes in Computer Science, pages 218–233, Bristol, UK, 2003. Springer-Verlag

[12] M.-L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, "Power Analysis, What Is Now Possible," Proc. Sixth Int'l Conf. the Theory and Application of Cryptology and Information Security, Advances in Cryptology (ASIACRYPT 2000), pp. 489-502, 2000.

[13] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential Power Analysis in the Presence of Hardware Countermeasures," Proc. Second Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES 2000), pp. 252-263, 2000.

[14] S.B.Ors, E.Oswald, and B.Preneel, "Power-analysis attacks on an FPGA - First experimental results," *Cryptographic Hardware and Embedded Systems - CHES*, vol. 2279 of Lecture Notes in Computer Science, pp. 35–50, 2003

[15]. J. S. Coron, "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems," *Cryptographic Hardware and Embedded Systems - CHES*, vol. 1717 of Lecture Notes in Computer Science, pp. 292–302, 1999.

[16] T. Messerges, "Securing the AES Finalists Against Power Analysis Attacks," Proc. Seventh Int'l Workshop Fast Software Encryption (FSE 2000), pp. 150-164, 2001.

[17] J.-S. Coron and L. Goubin, "On Boolean and Arithmetic Masking against Differential Power Analysis," Proc. Second Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES 2000), pp. 231- 236, 2000.

[18] L. Goubin, "A Sound Method for Switching between Boolean and Arithmetic Masking," Proc. Conf. Cryptographic Hardware and Embedded Systems (CHES 2001), pp. 3-15, 2001.

[19] M. vonWillich, "A Technique with an Information-Theoretic Basis for Protecting Secret Data from Differential Power Attacks," Proc. Conf. Cryptography and Coding 2001, pp. 44-62, 2001.

[20] A. Shamir, "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies," Proc. Second Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES 2000), pp. 71-77, 2000.

[21]. Itoh, Yajima, Takenaka, and Torii. DPA countermeasures by improving the window method. In CHES: International Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, 2002.

[22] P. Rakers, L. Connell, T. Collins, and D. Russell, "Secure Contactless Smartcard ASIC with DPA Protection," IEEE J. Solid-State Circuits, vol. 36, no. 3, pp. 559-565, Mar. 2001.

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 has published more than 8 International/National journals and presented the 15 International/ National Conferences.He is presently doing his Ph.D in Anna University, Coimbatore, India. His area of interest are computer Networks, Information Security and Cryptography. He is life member of ISTE.

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 area includes Image Processing, Neural Networks, Information Security and Cryptography. She has received Vijya Ratna Award from India International Friendship Society in the year of 1996, she has received Mahila Jyothi Award from Integrated Council for Socio-Economic Progress in the year of 2001 and she has received Eminent Educationalist Award from International Institute of Management, New Delhi in the year of 2008.She is member of Computer Society of India, ISTE and FIE.