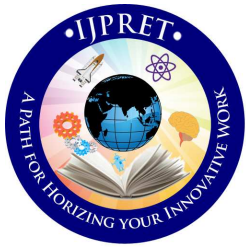
Research Article *ISSN: 2319-507X*
Nischal Puri, IJPRET, 2013; Volume 1(8): 58-71 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SURVEY OF SIDE CHANNEL ATTACKS ON ECC

NISCHAL PURI[1], HARSHAD KUBADE[1], PRAFUL BAREKAR[2]

1. **Asst. Prof in Dept. of I.T, Priyadarshini Institute of Engineering & Technology, Nagpur.**
2. **Asst. Prof in Dept. of C.S.E, Priyadarshini Institute of Engineering & Technology, Nagpur.**

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

ECC

Analyze

Electro Magnetic

Radiation

Corresponding Author

Mr. Nischal Puri

Abstract

Side-channel analysis is a powerful technique discovered by P. Kocher. The principle consists in monitoring some side-channel information like the running time, the power consumption, or the electromagnetic radiation. From the monitored data, the attacker tries to deduce the inner-workings of the algorithm and thereby to retrieve some secret information. This survey is aimed to analyze the performance of elliptic curve cryptosystem under side channel attacks. The main advantage of Elliptic curve cryptography is smaller key size, it is mostly used for public key infrastructure, but the side channel analysis is now well understood by the implementer.

INTRODUCTION

Provable security becomes more and more popular in the cryptographic community. It is now common to see it as an attribute of a cryptosystem. Provable security is at the protocol level, a harder task may be to evaluate the security of a cryptosystem at the implementation level. Rather than considering a cryptosystem as a black-box, we may assume that some sensitive data can leak during the course of the execution of a (naively implemented) crypto-algorithm. Side-channel analysis is a powerful technique re-discovered by P. Kocher in 1996. The principle consists in monitoring some side-channel information like the running time, the power consumption, or the electromagnetic radiation. Next, from the monitored data, the attacker tries to deduce the inner-workings of the algorithm and thereby to retrieve some secret information. When there is a single measurement, the process is referred to as a simple side channel analysis; and when there are several measurements handled together with statistical tools, the process is referred to as differential side-channel analysis.

ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography.

The mathematical operations of ECC is defined over the elliptic curve $y2 = x3 + ax + b$, where $4a3 + 27b2 \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the

elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead. The addition operation in ECC is the counterpart of modular multiplication in RSA, and multiple additions are the counterpart of modular exponentiation. To form a cryptographic system using elliptic curves, we need to find a "hard problem". All systems rely on the difficulty of a mathematical problem for their security. To explain the concept of difficult mathematical problem, the notion of an algorithm is required. To analyze how long an algorithm takes, computer scientists introduced the idea of polynomial time algorithms and exponential time algorithms. An algorithm runs quickly if it is polynomial time algorithm, and slowly if it is exponential time algorithm. Therefore, easy problems equate with polynomial time algorithms, and difficult problems equate with exponential time algorithms. When looking for a mathematical problem on which to base a public key cryptographic system, cryptographers search for a problem for which the fastest algorithm takes exponential time. The longer it takes to compute the best algorithm for a problem, the more secure a public key cryptosystem based on that problem will be. Three types of systems are considered secure and efficient: the Integer Factorization Systems (RSA), the Discrete Logarithm Systems (DSA), and the Elliptic Curve System (Elliptic Curve Discrete Logarithm System). In RSA, given an integer n which is the product of two large primes p and q such that,

$$n = pxq. \qquad (1)$$

It is easy to calculate n given p and q but it is difficult to determine p and q given n for large values of n. The U.S. government's Digital Signature Algorithm (DSA) is based

on discrete logarithm problem modulo a prime p. Given an integer g between 0 and p-1, and y which is the result of exponentiation of g, we have

$$y = g^x (\mathrm{mod} p) \text{ for some } x. \quad (2)$$

The discrete logarithm problem modulo p is to determine the integer x for a given pair g and y. The Elliptic Curve Cryptosystem (ECC), whose security rests on the discrete logarithm problem over the points on the elliptic curve. The main attraction of ECC over RSA and DSA is that the best known algorithm for solving the underlying hard mathematical problem in ECC (the elliptic curve discrete logarithm problem (ECDLP) takes full exponential time. RSA and DSA take sub-exponential time. This means that significantly smaller parameters can be used in ECC than in other systems such as RSA and DSA, but with equivalent levels of security. A typical example of the size in bits of the keys used in different public key systems, with a comparable level of security (against known attacks), is that a 160-bit ECC key is equivalent to RSA and DSA with a modulus of 1024 bits. The lack of a sub-exponential attack on ECC offers potential reductions in processing power and memory size. These advantages are especially important in applications on constrained devices. In practical terms, the performance of ECC depends mainly on the efficiency of finite field computations and fast algorithms for elliptic scalar multiplications. In addition to the numerous known algorithms for these computations, the performance of ECC can be increased by selecting particular underlying finite fields and/or elliptic curves. For ECC, we are concerned with a restricted form of elliptic curve that is defined over a finite field. Of particular interest for cryptography is what is referred to as the elliptic group mod p, where p is a prime number. This is defined as follows. Choose two nonnegative integers, a and b, less than p that satisfy:

$$4a3 + 27\, b2 \ (\mathrm{mod}\ p) \neq 0. \quad (3)$$

Then Ep(a, b) denotes the elliptic group mod p whose elements (x, y) are pairs of nonnegative integers less than p, satisfying:

$$y2 = x3 + ax + b \ (\mathrm{mod}\ p) \quad (4)$$

Together with the point at infinity O. The elliptic curve discrete logarithm problem

can be stated as follows. Fix a prime p and an elliptic curve.

$$Q = xP \quad (5)$$

Where xP represents the point P on elliptic curve added to itself x times. Then the elliptic curve discrete logarithm problem is to determine x given P and Q. It is relatively easy to calculate Q given x and P, but it is very hard to determine x given Q and P.

III SIDE CHANNEL ATTACKS ON ECC

Side-channel analysis is a powerful technique re-discovered by P. Kocher in1996. The principle consists in monitoring some side-channel information like the running time, the power consumption, or the electromagnetic radiation. Next, from the monitored data, the attacker tries to deduce the inner-workings of the algorithm and thereby to retrieve some secret information. When there is a single measurement, the process is referred to as a simple side channel analysis; and when there are several measurements handled together with statistical tools, the process is referred to as differential side-channel analysis [1] [3]. Side channel attacks based on following Parameters

Time Analysis

Power Analysis

Electromagnetic analysis

On the basis of these parameters, there are two types of attacks on ECC

Simple Side Channel Analysis

When there is a single parameter measurement.

Differential Side Channel Analysis

When there are several parameter measurements handled together with statistical tools.

IV ATTACKS ON IMPLEMENTATIONS

Several classes of attacks can be distinguished. The most straightforward attack is a physical attack directly to the silicon. This is a powerful method if a probing point is available. For instance, it is easy to retrieve secret information by probing the data on a bus. The fault induction attack is a well-known technique

that works by disturbing the device to induce errors in the computation. These attacks are named active attacks after the technique. A possibly more dangerous type of attack, undetectable for the embedded system, is called passive attacks. These attacks are based on measuring physical characteristics leaking from side-channels of the embedded system. Timing Analysis (TA) checks the computation time. If the execution time varies with the data or the key used in the computations, this can be detected by the attacker. Simple Power Analysis (SPA) measures the power consumption during cryptographic operations and guesses the actual types of computations. In, Kocher et al. introduced Differential Power Analysis (DPA) that also considers effects correlated to data values. Electromagnetic Analysis (EMA) and Acoustic Analysis (AA) were also introduced as effective SCA examples

V THE ATTACKER'S TASK

The attacker has the ability to observe a sequence of elliptic curve operations, thus, the attacker's aim is to calculate and exploit the probabilities of certain sequences of bits given an observed sequence of elliptic curve operations. Using the information of such conditional probabilities, the key-space that has to be searched to find the correct ephemeral key, can be significantly reduced. This is because certain combinations of patterns in the power trace and certain combination of digits are less likely than the others (or even not possible at all). The attacker's task can be stated in a more formal way. Let X be a random variable that denotes a sequence of elliptic-curve operations and |X| the length of X (i.e. the number of elliptic-curve operations in this sequence). For example, X="DDD" (i.e. the realization of the random variable X consists of three consecutive elliptic-curve point-double operations) thus |X| = 3, or X="DAD" (i.e. the realization of the random variable X consists of an elliptic-curve point-double operation, an elliptic-curve point-addition operation and an elliptic-curve point-double operation) thus |X| = 3. Let Y be a random variable that denotes a sequence of digits in the digit representation of k and |Y | the length of Y (i.e. the number of digits). For example Y = "000" (i.e. the realization of the random

variable Y consists of three consecutive zeros) thus |Y | = 3, or Y = "01" (i.e. the realization of the random variable Y consists of a zero and a one digit) thus |Y | = 2. Then the attacker's goal is to calculate and exploit the conditional probability

For many different realizations x of X and y and Y. Equation 1 is the mathematical definition for the conditional probability. Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems, It is an important observation that the calculation of the right hand side of (1) requires the knowledge of the probability to be in a specific state of the point multiplication algorithm (the terminology used here will be explained in the next section). This is because in order to calculate the probabilities P(X = x), one has to calculate the sum of the probabilities of all possible sequences of digits that lead to the pattern x. Since such a sequence can basically start from any state of the algorithm, the probabilities are dependent on the probability of the starting-state.

The basic principles of how to apply power analysis attacks on elliptic curve cryptosystems have been discussed. To counteract both simple power analysis attacks and (first order) differential power-analysis attacks there are basically two things that have to be done. Firstly, one has to randomize the expressions (i.e. the coordinates) of calculated points. This can be done by using randomized projective coordinates (DPA countermeasure). Secondly, one has to conceal the ephemeral key. It would be optimal if there would be no statistical relationship between the sequence of elliptic-curve operations and the bits of the ephemeral key (SPA countermeasure). Countermeasures applicable to arbitrary curves fixing the sequence of elliptic-curve operations have been presented by Coron, Moller and Izu . Countermeasures applicable to arbitrary curves not fixing the sequence of elliptic-curve operations have been presented by Oswald and Brier. Countermeasures applicable to special curves fixing the sequence of elliptic-curve operations have been presented by Hasan and by Okeya. Countermeasures applicable to special curves not fixing the sequence of elliptic-

curve operations have been presented by Liardet and Joye.

VI VARIOUS PARAMETRIC ATTACKS ON ECC

Time Analysis Attack

Kocher presented the timing-attacks: Attackers carefully measure the amount of time required to perform the private key operations, so that they might be able to decide fixed Diffie-Hellman exponents [11]. This attack could be applicable to the elliptic curve cryptosystems including ECDSA. Time required to perform the conventional scalar multiplication algorithm based on the Weierstrass-form depends on the bit-patterns (and on the ratio between the number of zeros and the number of one's) of the secret value [3]. Where as we show that the scalar multiplication on the Montgomery-form elliptic curve does not depend on the bit-patterns (nor on the ratio between the number of zeros and the number of one's) of the secret value. It has exactly seven multiplications and four square-multiplications on Fp per bit. This is due to the specific algorithm for computing scalar multiplication nP from P, which repeatedly calculates either (2mP, (2m + 1)P) or ((2m + 1)P, (2m + 2)P) from (mP, (m + 1)P) in the Montgomery-form elliptic curves. The computation via by choosing a representive in the projective coordinates randomly is also useful for making it more difficult to measure the amount of time required. We compute the scalar d multiplications on the a.ne coordinates (x, y) via a corresponding projective coordinates (kx, ky, k), where k is randomly choosed. Thus, Montgomery-form elliptic curves are shown to be useful for public-key cryptosystems from the point of view of not only efficient implementation but also protection against timing-attacks.

Power Analysis Attack

Power attacks arise from the actual implementation of the cryptosystems, which differ from the ideal cryptosystems. There are leakages of information in addition to input and output data while the cryptographic devices (e.g. smart card) execute cryptographic transactions (e.g. signature, encryption, and decryption) [11]. An attacker may use the leakages for his estimate. In 1996, Kocher proposed timing attack. Timing attack is one of the power

attacks in which an attacker uses timing of execution for his estimate of the secret key. Recently, Kocher et al. proposed DPA (Differential Power Analysis) and SPA (Simple Power Analysis) DPA is a power attack in which an attacker uses power consumption and analyzes such data statistically, and SPA is an attack without statistical analysis [7]. Coron generalized DPA to elliptic curve cryptosystems with the following SPA-immune scalar multiplication algorithm. for the purpose of constructing cryptosystems with immunity to DPA, we explain characteristics of DPA how an attacker estimates the secret key in the attack. The point of this attack is "a difference between executing procedures (non-symmetry)" and "an appearance of a predicted special value". First, the executing procedure of typical cryptographic transaction depends on the secret key. Consequently, the executing procedure of cryptographic transaction differs from secret key to secret key. If an attacker finds the difference of the executing procedure from leakages, he is able to derive the information on the secret key. Actually, since it is hard to find the difference of executing procedure as it is, he treats it statistically and makes its bias big, and finally he finds the difference of the executing procedure. Next, if an appearance of some specific value on the cryptographic transaction depends on the secret key, an attacker is able to detect the secret key by whether the value appears on the execution or not.

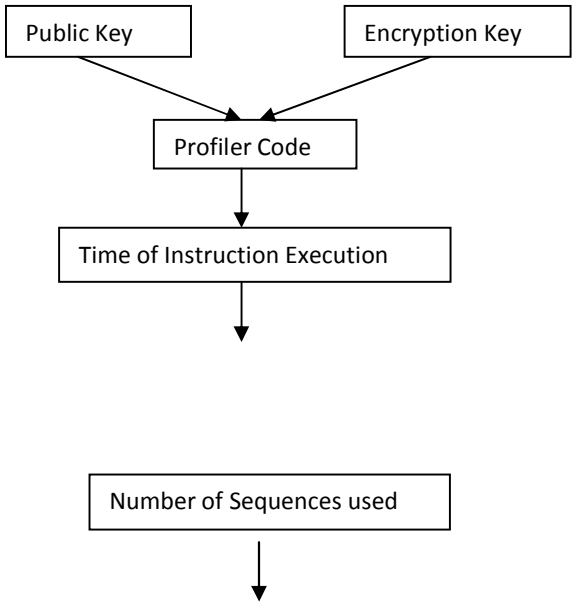
Electromagnetic Analysis Attack

Nowadays, CMOS is by far the most commonly used technology to implement digital integrated circuits. A CMOS gate consists of a pull-up network with p-MOS transistors and a pull-down network with n-MOS transistors. Those networks are complementary: when the input is stable, only one of the two networks conducts. The most simple logic gate is an inverter; its power consumption is representative for all logic ports and gives a general image of the power consumption in a CMOS circuit. During the functioning of the inverter, 3 types of power consumption can be distinguished. The leakage current, the current that flows from the power source to the ground during the switching from 0 to 1

(short-circuit current) and the current used to charge and discharge the different capacitors in a digital network (dynamic power consumption). The last one causes the biggest power consumption in present designs. Important to note is that these capacitors are necessary to maintain the two different logic levels. In addition, all capacitors for each gate differ, which results in a different power consumption of the different gates according to the data being processed [23]. The sudden current pulse that occurs during the transition of the output of a CMOS gate causes a variation of the electromagnetic field surrounding the chip; this can be monitored for example by inductive probes which are particularly sensitive to the related impulsion.

Two types of electromagnetic analysis attacks are distinguished. In a simple electromagnetic analysis (SEMA) attack, an attacker uses the information from one electromagnetic radiation measurement directly to determine (parts of) the secret key [11]. In a differential electromagnetic analysis (DEMA) attack, many measurements are used in order to filter out noise and the key is derived using a statistical analysis. While SEMA exploits the relationship between the executed operations and the electromagnetic radiation, DEMA exploits the relationship between the processed data and the electromagnetic radiation [23]. A SEMA attack is typically used when there is a conditional branch in the algorithm, whichresults in a different radiation pattern whenever the branch is taken. A DEMA attack uses the property that processing different data needs a distinct amount of power and radiates a different field.

VII DESIGN FLOW OF TIME ANALYSIS ATTACK



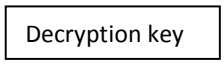


Figure1: Design flow of Time Analysis Attack

Scalar point-multiplication consists of a sequence of point-addition, point-subtraction and point-doubling operations. The attacker's goal is to learn the key using the information obtained from carefully observing the running Time required for a complete scalar point-multiplication. Every elementary field-operation has its unique running time required. The sequence of elementary field-operations that form the point-addition operation has a different running Time required than the sequence of elementary field operations that form the point-doubling operation. Profiler code analyses the time required to execute the set of instructions written under it.

VIII CONCLUSION

We have studied different parametric Attacks, like time analysis Attack, Power Analysis Attack, Electromagnetic Analysis Attack. The different parameters used are Time consumption, power consumption, and electromagnetic radiations to produce result. Finally describes the design flow of timing attack on Elliptic curve cryptography in public key Infrastructure scheme.

IX REFERENCES

1. Ekambaram Kesavulu Reddy, "Elliptic Curve Cryptosystems and Side-channel Attacks", Published in international Journals of Network Security, 2009.

2. Kazuo Sakiyama, Elke De Mulder, Bart Preneel, and Ingrid Verbauwhede "Side-channel Resistant System-level Design Flow for Public-key Cryptography" GLSVLSI'07, March 11–13, 2007, Stresa-Lago Maggiore, Italy.

3. Marc Joye, "Elliptic curves and side channel analysis", published in ST Journal of System Research, 2003.

4. Zhang Tao, Fan Mingyu & Zheng Xiaoyu " Secure and efficient elliptic curve cryptography resists side-channel attacks" published in Journal of Systems Engineering and Electronics Vol. 20, No. 3, 2009, pp.660–665

5. Werner Schindler1, Kerstin Lemke, and Christof Paar, "A Stochastic Model for Differential Side Channel Cryptanalysis", International Association for Cryptologic Research, 2005.

6. Elisabeth Oswald, "Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems", Springer-Verlag Berlin Heidelberg, 2003.

7. Katsuyuki Okeya and Kouichi Sakurai, "Power Analysis Breaks Elliptic Curve Cryptosystems Even Secure against the Timing Attack", Springer-Verlag Berlin Heidelberg, 2000.

8. Katsuyuki Okeya, Hiroyuki Kurumatani, and Kouichi Sakurai, " Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications", Springer-Verlag Berlin Heidelberg, 2003

9. Bodo M¨oller, "Securing Elliptic Curve Point Multiplication against Side-Channel Attacks", Springer-Verlag Berlin Heidelberg, 2003.

10. An Implementation Tutorial on " Elliptic Curve Cryptography", By Anoop MS.

11. Dimitrios L. Delivasilis and Sokratis K. Katsikas, "Side Channel Analysis on Biometric-based Key Generation Algorithms on Resource Constrained Devices", International Journal of Network Security, Vol.3, No.1, PP.44–50, July 2006.

12. Ernie Brickell, Gary Graunke, Michael Neve and Jean-Pierre Seifert, "Software mitigations to hedge AES against cache-based software side channel vulnerabilities"

13. Eric Brier and Marc Joye, "Weierstraß Elliptic Curves and Side-Channel Attacks", [Published in D. Naccache and Pascal Paillier, Eds., Public Key Cryptography,vol. 2274 of Lecture Notes in Computer Science, pp. 335–345,Springer-Verlag, 2002.]

14. Marc Joye and Christophe Tymen "Protections against Di_erential Analysis for Elliptic Curve Cryptography An Algebraic Approach", [Published in C_ .K. Ko_c, D. Naccache, and C. Paar, Eds., Cryptographic Hardware and Embedded Systems, CHES 2001, vol. 2162 of Lecture Notes in Computer Science, pp. 377, Springer-Verlag, 2001.]

15. Marc Joye and Jean-Jacques Quisquater, "Hessian Elliptic Curves and Side-Channel Attacks", [Published in C. K. Koc D. Naccache, and C. Paar, Eds., Cryptographic Hardware and Embedded Systems– CHES 2001, vol. 2162 of Lecture Notes in Computer Science, pp. 402–410, Springer-Verlag, 2001.]

16. Jean-Sebastien Coron and_Ecole Normale Superieure, "Resistance Against Di_erential Power Analysis for Elliptic Curve Cryptosystems", [Published in C_ .K. Ko_c and C. Paar, Eds., Cryptographic Hardware and Embedded Systems, vol. 1717 of Lecture Notes in Computer Science, pp. 292 Springer-Verlag, 1999.]

17. Tetsuya Izu, Bodo M¨oller, and Tsuyoshi Takagi, "Improved Elliptic Curve Multiplication Methods Resistant against Side Channel Attacks", [Appears in A. Menezes, P. Sarkar (Eds.): Progress in Cryptology INDOCRYPT 2002, Springer-Verlag LNCS 2551, pp296–313, ISBN 3-540-00263-4.]

18. Benoıt Chevallier-Mames, Mathieu Ciet, and Marc Joye, "Low-Cost Solutions for Preventing Simple Side-Channel Analysis: Side-Channel Atomicity", [Published in IEEE Transactions on Computers 53(6):760–768, 2004.]

19. Katsuyuki Okeya and Kouichi Sakurai, "On Insecurity of the Side Channel Attack Countermeasure Using Addition-Subtraction Chains under Distinguishability between Addition and Doubling", [L. Batten and J. Seberry (Eds.): ACISP 2002, LNCS 2384, pp. 420–435, 2002. c Springer-Verlag Berlin Heidelberg 2002]

20. Katsuyuki Okeya and Tsuyoshi Takagi, "A More Flexible Countermeasure against Side Channel Attacks Using Window Method", [C.D. Walter et al. (Eds.): CHES 2003, LNCS 2779, pp. 397–410, 2003. c Springer-Verlag Berlin Heidelberg 2003]

21. Katsuyuki Okeya and Tsuyoshi Takagi, " The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks", [M. Joye (Ed.): CT-RSA 2003, LNCS 2612, pp. 328–343, 2003. c Springer-Verlag Berlin Heidelberg 2003]

22. Werner Schindler, Kerstin Lemke, and Christof Paar, "A Stochastic Model for

Differential Side Channel Cryptanalysis", [J.R. Rao and B. Sunar (Eds.): CHES 2005, LNCS 3659, pp. 30–46, 2005.c International Association for Cryptologic Research 2005]

23. "Electromagnetic Analysis Attack on a FPGA Implementation of an Elliptic Curve Cryptosystem".