www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 10018-10022

“ECC Based Prevention for Side Channel Attack: A Survey”

Miss. Anuja S. Deoghare , K. N. Hande

IV sem, M.tech (CSE)

Dept .Of CSE, PBCOE, Nagpur

anuja.deoghare@gmail.com

Assistant Professor

Dept .Of CSE, PBCOE, Nagpur

kapilhande@gmail.com

Abstract

Elliptic curve cryptography has many advantages like it is used for data encryption as well as digital signature. Also it gives efficiency for both software and hardware implementation. Despite of its security level the elliptic curve cryptography is affected by various types of attacks like side channel attacks. In side channel attack basically the attacker retrieve the secret key with less effort and affect the implementation of the cryptosystem and exploit the information leakage. We introduce the most effective side channel attack is the power analysis attack. This attack categories into simple power analysis attack (SPA) that reveals the secrete key by analyzing operation sequence that depend on the key value using power consumption trace and differential power analysis ie.(DPA) it uses statistical tool for analyzing the correlation between consumption and processing operation which depend on secrete key. Basically the Power analysis attack exploits the power consumption of the cryptosystem and break the ECC.

Keyword: Elliptic curve cryptography, side channel attacks, power analysis attacks, ECSM.

1. Introduction

1.1) Elliptic curve cryptography

Elliptic curve cryptography is known for an efficient and secure encryption scheme. As compare to RSA and DSA Elliptic curve cryptography is more effective and efficient due to its smaller key size for security. Security of elliptic curve cryptosystem is depends upon discrete logarithm problem over the points on elliptic curve. The elliptic curve cryptography has the best known algorithm for solving the underlying hard problems in ECC that takes full exponential time. This means ECC requires much smaller system parameters, which leads to faster computation and less storage requirements and gives equal security. The ECC mainly used for three common fields like secure communication while the confidential data transferred by two systems, key exchange and digital signature generation which are important facts in secure data transfer. Though ECC provides good security level, some faults occurs due to natural and artificial reasons which creates the problems like data corruption and security leakage of system. The lack of sub-exponential attacks on ECC offers potential reduction in processing power and memory size. Elliptic curve cryptography used in networks and electronic cash. In electronic cash smart cards are very common but some cases the current technologies are not so much capable to resist the powerful attacks.

The Elliptic curve cryptography has most computationally intensive operation is the ECSM (Elliptic curve Scalar multiplication), it computes kp where p is the base point and k is scalar kept secret. ECSM performs two basic operations which are point addition and point doubling. In point addition adds two different points and point doubling add point to itself. These two operations are defined geometrically on the elliptic curve E. They involve computation of co-ordinates of points.

The security of ECC is directly related to the difficulties of elliptic curve discrete logarithm problems. The most effective side channel attack is power analysis attacks. There are various types of side channel attacks:

1.2) Power analysis attacks

Power analysis attacks has the main target on smart cards, other embedded system where the secret key is importantly store. It is applicable on the hardware implementation. It has two categories simple power analysis attack(SPA) and Differential power analysis attack (DPA).In Simple power analysis attack ,thing is guess from the power trace of particular instruction which being executed at a specific time and what input and output values have Simple power analysis (SPA)involves visually interpreting power *traces*, or graphs of electrical activity over time. The goal of SPA attacks is to reveal the secret key when given only a few power traces (That is, for a small number of input or output values).Attacker must be able to monitor the power consumption of the device under attack. In the attacked device, Secret key must have (Directly or indirectly) a significant impact on the power consumption. Differential power analysis (DPA)is a more advanced form of power analysis which can allow an attacker to compute the intermediate values within cryptographic computations by statistically analyzing data collected from multiple cryptographic operations. It requires many power traces need physical possession of the device. It visually checks the power traces of the system.

1.3) Fault Attack

The fault attacks deliberately creates fault during operation of cryptosystem due to this the faulty output is generate. Due to hardware fault it affects the security of the system. There are two kinds of fault side channel. First one is the fault occur during the operation of the system or computation of the cryptographic module. This computation fault regards the most effective side channel attacks. Second type is that sending incorrect or corrupted input data to the attack module.

1.4) EM Attack

Simple electromagnetic analysis can be categories into two parts, first is simple electromagnetic analysis and second is differential electromagnetic analysis .The countermeasures of this attack are single strength reduction and simple information reduction. Acoustic Attack: The main attacks where side channel attack focused on power consumption diffuse visible light from CRT displays, but the oldest over dropping channels caused acoustic emanation has a very important.

2. Literature Survey

Fault attacks manipulate the computation of an algorithm and get information about the private key from the erroneous result. for the cryptographic device It is the most powerful attack. Currently, the research on error detection methods and fault attacks has been studied widely. S. Pontarelli et al. introduced an error detection method in 2009. It can detect an error that occurs during Elliptic Curve Scalar Multiplication (ECSM). They elaborate a new fault attack. Attack can avoid the error detection method introduced by S. Pontarelli et al. They apply a bit flip error in the 0 Addition Chain (EAC) on the private key in ECSM and retrieve the private key. They provide countermeasures which are secure against this attack using the different methods.

Johannes Blomer, Martin Otto, Jean-Pierre Seifert present a new type of fault attacks on (ECSM), Sign Change Attacks. This attack does not change the original curve E and works with points on the curve E. They show how sign changes of intermediate points can be used to recover the secret scalar factor. This attack leads to a faulty output that is a valid point on the original elliptic curve. Then they can use an algorithm similar to the one presented for RSA in [BDL01] to recover the secret scalar factor in expected polynomial time. They present the attack for the NAF based left-to-right repeated doubling algorithm, because here Sign Change Faults seem to be easier to realize than for other repeated doubling variants.

Bhandari, A. K. given basic information to Elliptic Curve Cryptography. They introduced the discrete log integral problem, then gave a general, but slow method of attack on this problem. There exist methods that take constant rather than √N space, but there are no know general methods that run faster than √N time. This means that the EC discrete log problem is difficult. It is known to be easy only for specific classes of elliptic curves, such as super singular curves (due to the MOV attack).

Abdulaziz Mohammad Alkhoraidly In their 1976 paper titled “New Directions in Cryptography”, Whitfield Diffie and Martin Hellman introduced a method, based on the hard problem of finding discrete logarithms in a prime field, by which parties that have no shared secrets can establish a shared secret over an insecure channel, finding the secret key. Since then, many public-key cryptosystems have been invented, but few have stood the tests of time and eager cryptanalysts. Among those are the Rivest-Shamir- Adleman (RSA) cryptosystem and the Rabin cryptosystem, both based on the hard factoring integers with large prime factors.

3. Revive of Methods for side channel Attacks

3.1) There are different types fault and attacks occurs on the system.

3.1.1) Statistical Modeling of Faults:

For estimating the fault frequency effect modeling the occurrence of faults in a system is important. Reliability is usually applicable for single components in a system, and then the results are used to determine the reliability of the whole system. Following are the known fault attack on elliptic curve cryptosystem and there countermeasure.

3.1.2) Biehl-Meyer-M¨uller Invalid Curve Attacks:

In the attacks presented the representation of a point P on a strong elliptic curve E can be modified, e.g. by a register fault, to move P to a different, often weaker, curve E′. This gives the faulty output & varies the result. Which revels the faulty result

Usually, the attack has to be repeated since in many cases the value guessed are not unique.

3.1.3) Exploiting early random register faults:

Consider the device checks whether P lies on E before starting the computation, and assume a single bit fault in an unknown position can be introduce right between the test and the computation. Exploiting random faults during computation Assume that E is defined over an extension field Fq such that E(Fq) contains a subgroup of prime order p with p > q/ log q, and that the binary algorithm is used to perform the scalar multiplication. It will give the correct result Q=kp.

3.1.4) Ciet-Joye Invalid Curve Attacks:

In the attacks representing in the consideration that only a single or few bit errors can be injected into the representation of P is relaxed. It also demonstrates how random errors in the representation of P, the curve parameters or the field representation can allow for the recovery of secret key either fully or partially.

3.1.5) Sign change fault Attack:

By changing the base point, an intermediate point or parameter on the curve, it will move the computation to the different curve. Basically it gives the faulty result in the original curve. After collecting the faulty result, secret is revel in polynomial time.

3.1.6) Fault in digital system:

It is important that every system will be fault free. There are so many reasons like natural and artificial that fault can occur. Due the fault the secret key and important data will be extracting from the system, so it is very important to recover the system from this attack. For this various counter measures can be available.

3.1.7) Invalid Curve Fault Attack:

In this case the attacker can move the computation from the secure curve to a weaker. In this the target is the system parameter and the running computation. The counter measure of this fault is to detect and recover it by the special system

3.2) There are some countermeasures for these attacks are presented and effectiveness and limitations.

3.2.1) Checksums: The checksums are mostly used in detecting errors in data while stored or transit, but it cannot be used to detect the errors injected during the computations. They are not strong against the invalid curve attacks and sign-change attacks.

3.2.2) Hardware and/or time redundancy: This process is easier to detect faults since the attacker has to inject some error twice to pass the comparison test. Hardware dependency used to detect permanent fault in the computation area of the system. The disadvantage of this scheme is that it is very costly.

3.2.3) Scalar multiplication using Montgomery's ladder: The Montgomery scalar multiplication algorithm works using only x-co-ordinates of particular point, it is naturally protect the system against the sign change fault attack and invalid curve attacks. However Montgomery ladder is not enough by itself to counter a general invalid curves attacks that does not use the y-co-ordinate.

3.2.4) Randomized encoding: Randomization helps in elliptic curve scalar multiplication in different ways while encoding the scalar, base point or curve parameters. But Randomization technique does not help in investigating invalid curve attacks since its effect will be reserved by the decoding the result.

3.2.5) Computation on a combined curve: Computation on combined curve is an effective countermeasure against sign change fault attacks, but it is not effective against invalid curve attacks.

3.2.6) Information Redundancy: The simplest solution, and the cheaper in terms of overhead, is validating the resulting point before giving it exact output. The point validation can be performed using the same field arithmetic units used in the scalar multiplication operation. It can also be performed by an independent module and takes around 80-200% of the time of an average point operation depending on the implementation.

4. Prevention Techniques

One of the strong prevention technique against the side channel attacks is the LOADER scheme ie. Low cost error detection and recovery scheme. In this scheme, exploits the invariance among the results produced by the algorithm, to detect errors. The error detection is done periodically during the elliptic curve scalar multiplication for the purpose of verifying the data correctness. and will recover the cryptosystem back to the latest checkpoint during elliptic curve scalar multiplication upon detecting errors**.** The time overhead of this scheme depends on how many times the Error detection and recovery process is performed. The main disadvantages of this scheme are that, it takes so much time while performing the operation step by step. Frequent validation is another technique for detecting the attacks and its recovery. In this scheme analyze new designs for fault-tolerant scalar multiplication structures. The main goal of this technique is to address the problem of random transient faults and design more efficient and reliable elliptic curve scalar multiplication structures. Here the parallel validation is done ie, the validation perform sequentially related to the main computation of ECSM. Researchers have invent the special techniques for the purpose of increasing the efficiency and the security such that Double and add algorithm, Montgomery ladder algorithm, ECSM based on Euclidean Addition Chain (EAC), Euclid's addition chains can provide secure and efficient technique of exponentiation by computing the EAC for a scalar k. It is possible to fast implementation by using the Co-Z addition method, the x-coordinate method based on ECSM with the EAC. These systems are proven to be secure with mathematical tools, they could be vulnerable to physical attacks using additional information via side channels. In chain randomization two techniques two schemes are present scalar randomization and random addition chain generations.

The error detection in elliptic curve cryptosystem involves the detection of error from both natural and artificial faults, it doesn't matter whether it transient or permanent. The natural errors are caused by an attacker to move a point to an invalid curve, with the exception being errors caused by a sign change attack where the points stay on the original curve. The error detection solutions for elliptic curve cryptography are information redundancy, time redundancy, hardware redundancy, or their combination.

5. Methodology

The proposed work focuses on devising a scheme which will address the successful denial of fault attack in order to protect the cryptosystem from being revealing the secret keys to the attacker. The scheme focuses on generation of ECSM (Elliptic curve scalar multiplication) .Then we make efforts to try to find out the errors which may incur during attack and recover from them. During an encryption process, the initialization step initializes the register in the data path and then ECSM step performs scalar multiplication in projective form.

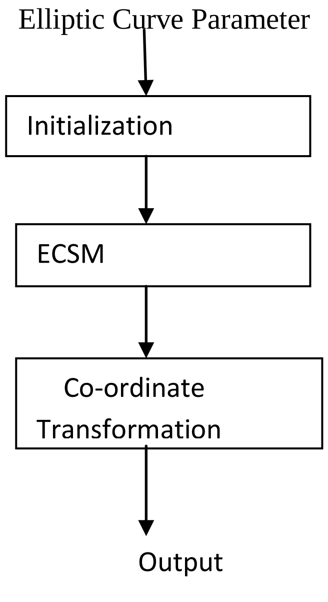

Fig1. Computation flow

Elliptic curve scalar multiplication is performed by repeating point addition (ECADD) operation and point doubling (ECDBL) operations over the curve. Elliptic curve point addition and point doubling operations in turn rely on finite field (FF) operations such as addition/subtraction, multiplication and inversion. One way to achieve parallel and pipelined scalar multiplication is to decompose ECADD and ECDBL operations into FF operations, which results in a sequence of FF inversion addition squaring and doubling operations. Grouping of finite field operations is a key factor in the implementation of parallel and/or pipelined algorithms. Among the finite field operations, the execution time of a squaring operation varies considerably depending on the type of fields– prime field or extension field. For field GF(p), where p is prime, the complexity of squaring is comparable to the complexity of multiplication. However, in binary extension field GF(2m), when the irreducible polynomial defining the field is known in advance, the complexity of squaring is significantly lower than that of multiplication and generally becomes comparable to that of addition. After a secure network formation data transformation can be done. We focused mainly on the power analysis attacks. There are some techniques to avoid or minimize the power analysis attack are protocol hiding and masking. In protocol, power analysis attacks become more difficult by using session key. In hiding user's can remove the power consumption's data dependency. In masking the intermediate value process by the cryptographic devices are randomize.

It is not necessary the fault occurs in a sequential manner; fault will occur anywhere in the computation system and can affect any area. The computation flow is shown in above figure. In this we perform Topology Formation, in this phase, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous neighbor establishment._.Second is Neighbor discovery phase. This phase is neighbor discovery phase, each source node identifies its neighbor nodes through broadcasting hello packets, through this process each node detects its neighbor nodes corresponding to location and distance. Based on the neighbor discovery phase each node forms a stable path to destination. Third is side channel attack**,** In this section we concentrate on side channel attack of power analysis, so to prove our detection mechanism these three attackers participate in the network as malicious nodes Then in ECC attack detection, The source node broadcast the RREQ message to neighbors for establishing the path to destination. The malicious nodes node sends the false RREP message continuously faster than its first source neighbors, at this point source node checks its routing table and performs ECC scalar multiplication process and identifies it's a malicious node and updates its block table that node is a malicious node. Then in Data Transmission, after the source node S successfully finds out a route to the destination source node S successfully finds out a route to the destination node D, S can start data transmission under the security factor.

The aim and proposed system is to provide source sharing of information over the network. It also provide the different attacks prevention methods. The main objective is to gives the secure environment to share the information. The Following are the aims and objective.

4.1) To device protective methods during every stage of Elliptical Curve Scalar Multiplication computation: The most time consuming and vulnerable operation to attacks in practical implementation of ECC Cryptosystems is Elliptical Curve Scalar Multiplication (ECSM). The aim will be to find methods that will protect this operation from attacks.

4.2) To design a secure system mechanism for Side Channel Attacks: The ECC Cryptosystems are found to be more susceptible to Side channel Attacks where the attacker can reveal the secrete keys used in the cryptosystem. The aim is to design a mechanism which will detect errors caused due to these attacks and makes an effort to recover from them.

4.3) To optimize the above mechanism to provide low cost scheme: The cost incurred in implementing such a system may go on higher side. So efforts will be made to make the system a low cost one. To achieve this aim, following work will done. The work focuses on devising a scheme which will address the successful denial of fault attack in order to protect the cryptosystem from being revealing the secret keys to the attacker. The scheme focuses on generation of ECSM (Elliptic curve scalar multiplication) using a Montgomery Ladder Algorithm. Then we make efforts to try to find out the errors which may incur during fault attack and recover from them.

6. Conclusion

The algorithm implemented will improve the Scalar Multiplication process which is the most integral part of ECC and which consumes more system resources. The proposed scheme helps in achieving low cost approach for detection of errors and their recovery in Elliptical Curve Cryptography. Analysis shows that it has strong fault detection capability against deliberately-induced faults as well as environment-induced faults. It is also compatible with most of existing countermeasures against power-analysis attacks.

References

[1] P Banik, S. Maitra, S. Sarkar. “A Differential Fault Attack on the Grain Family of Stream Ciphers”, CHES 2012, pp. 122–139, 2012

[2]K. Järvinen, C. Blondeau, D. Page, M. Tunstall, “Harnessing Biased Faults in Attacks on ECCBased Signature Schemes”, FDTC 2012, pp. 72-84, 2012.

[3] Karmakar, S.Roy Chowdhury, “Fault analysis of Grain-128 by targeting NFSR”, AFRICACRYPT 2011, pp.298–315, 2011.

[4] K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter. Public keys. In R. Safavi-Naini and R. Canetti, editors, CRYPTO, volume 7417 of LNCS, pages 626{642. Springer, 2012.

[5] Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous distributed E-Cash from Bitcoin. In IEEE Symposium on Security and Privacy, pages 397{411. IEEE Computer Society, 2013.}

[6] Dominguez-Oviedo and M. A. Hasan, “Algorithm-level error detection for ECSM,” Centre Appl. Crypto. Res., Univ. Waterloo, ON, Canada, Tech. Rep., TR-2009-05, 2009.

[7] Blömer, M. Otto, and J. Seifert, "Sign Change Fault Attacks on Elliptic Curve Cryptosystems," *Fault Diagnosis and Tolerance in Cryptography 2006 (FDTC ’06), volume 4236 of Lecture Notes in Computer Science*, Prentice Hall, 2004, pp. 36--52.

[8] M. Ciet and M. Joye, "Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults," *Designs, Codes and Cryptography*, vol. 36, 2005, pp. 33-43.

[9] Domínguez-Oviedo and M.A. Hasan, "Error Detection and Fault Tolerance in ECSM using Input Randomization," *IEEE Transactions on Dependable and Secure Computing*, vol. 6, 2009, pp. 175-187. N. Meloni, “New point addition formulae for ECC Applications”, WAIFI 2007, pp.189-201, 2007.

[10] Byrne, F. Crowe, W.P. Marnane, N. Meloni, A. Tisserand, and E. Popovici, “SPA resistant elliptic curve cryptosystem using addition chains”, International Journal of High Performance Systems Architecture, vol. 1, no. 2, pp. 133–142, 2007.

[11] Blömer, M. Otto, J. Seifert, “Sign change fault attacks on elliptic curve cryptosystems”, Cryptology ePrint Archive, vol. 4236, pp 36-52, 2006.

[12] Kim, J. Ha, S. Moon, S.-M. Yen, W.-C. Lien, and S.-H. Kim. (2005). “An improved and efficient countermeasure against power analysis attacks,” [Online]. Available: http://eprint.iacr.org/2005/022.

[13] H. Mamiya, A. Miyaji, and H. Morimoto, “Efficient Countermeasures against RPA, DPA, and SPA,” in *Proc. CHES*, vol. 3156, 2004, pp. 343–356.

[14] P. Fouque, D. Real, F. Valette, and M. Drissi, “The carry leakage on the randomized exponent countermeasure,” in *Proc. CHES*, 2008, pp. 198–213.

[15] S. M. Shohdy, A. El-Sisi, and N. A. Ismail, “FPGA Implementation of Elliptic Curve Point Multiplication over GF(2∧191),” in *Proc. 3rd Int. Conf. Workshops Adv. ISA*, 2009, pp. 619–634.