IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 7, July 2015.
www.ijiset.com
ISSN 2348 – 7968

Implementation of secure elliptic curve cryptography against side channel attacks

Miss. Anuja S. Deoghare
IV sem, M.tech (CSE)
Dept .Of CSE, PBCOE, Nagpur

K. N. Hande
Assistant Professor
Dept .Of CSE, PBCOE, Nagpur

Abstract:

Elliptic curve cryptography have become the secure system, widely use and more trusted system. But, sometimes the recent approach of utilizing side channel information poses powerful threat to the system, in such cases system is not ready for the exact type of attack. Side channel attacks are easy to implement but powerful attack against the cryptographic implementation. It reveals the secret key and extracts the secret data of the system. Their targets range from primitives, protocols, modules, and devices to even systems. This paper investigates the ECSM technique of an elliptic curve as a step towards resistance against such attacks in the context of elliptic curve cryptography. The idea is to use the same procedure to compute the addition, the doubling or the subtraction of points. The side channel attacks fall in to three main categories: fault analysis, timing attacks, and power attacks. We mainly focus on the power analysis attack by using the Montgomery ladder algorithm with ECSM technique.

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

1 Introduction:

1.1 Elliptic curve cryptography:

In computation and communication system, security is the major concern. Various cryptographic algorithms like symmetric ciphers, public-key ciphers, and hash functions, form a set of primitives that helps as building blocks to construct security mechanisms that target specific objectives. For example, network security protocols, such as SSH and TLS, combine these primitives to provide authentication between communicating entities, and ensure the confidentiality and integrity of communicated data. In practice, these security mechanisms only specify what functions are to be performed, irrespective of how these functions are implemented. Mathematical structure of an additive group is presented by the elliptic curve. elliptic curves particularly attractive for cryptographic applications. As a result, with shorter key lengths, comparable levels of security can be attained.

An elliptic curve over a field K is formed by the point *O* 'at infinity' and the set of points *P=(x, y) € k*k* satisfying non-singular equation:

E/k: $yy2 + a1xy + a3y = x3 + a2x2 + a4x + a6$

In elliptic curve cryptography the scalar multiplication is the basic operation. Given a point p € E(K), so as to compute Q= kP , where, kP = P+P+P…….(k times). The discrete logarithm problem consists in finding the value of *k* from the values of P and Q = kP.

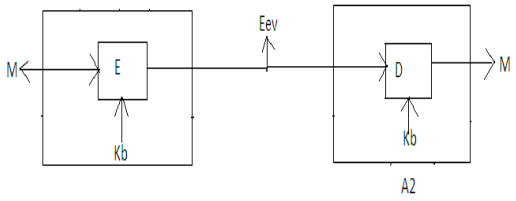

Fig1. Traditional cryptographic model

1.2 Side Channel Attacks:

There are two point of view of cryptographic primitive, first is, it can be viewed as an abstract mathematical object like a transformation, turning some input into output i.e classical cryptanalysis. Second is this primitive will in fine have to be implemented in a program that

ISSN 2348 – 7968

will run on a given processor, in a given environment, and will therefore present specific characteristics i.e side channel cryptanalysis. Side-channel cryptanalysis takes advantage of implementation-specific characteristics to recover the secret parameters involved in the computation. Therefore it becomes much less general and it is specific to a given implementation, but often much more powerful than classical cryptanalysis, and is considered very seriously by cryptographic devices implementers.

Generally, in cryptanalysis, when assessing the security of a cryptographic protocol, it is assumes that the opponent has a complete description of the protocol, is in possession of all public keys, but less knowledge about secret keys. In addition, the opponent can be intercepted some data exchanged between the participants, and may even have some control over the nature of this data (e.g., by selecting the messages in a chosen-message attack on a signature scheme, or by selecting the cipher text in a chosen-cipher text attack on a public-key encryption scheme). The opponent then attempts to compromise the protocol goals by either solving an underlying problem assumed to be intractable, or by exploiting some design flaw in the protocol. Side Channel attacks categories into two main categories in to passive attacks and active attacks. In passive attacks to those that do not noticeably interfere with the operation of the target system; the attacker gains some information about the target system's operation, but the target system behaves exactly as if no attack occurs. In active attack, the opponent exerts some influence on the behavior of the target system. In Side channel attack includes timing attacks, fault attacks, power analysis attack, EM attacks etc. We mainly focus on the Power analysis attack.

1.3 Power analysis attack:

The power consumption of a cryptographic device may provide much information about the system operations that take place and the involved parameters. Power analysis attack is applicable only to hardware implementation of the cryptosystems. Power analysis attack is particularly effective and proven successful in attacking smart cards or other dedicated embedded systems which storing the secret key. Very powerful attacks for most straightforward implementations of symmetric and public key ciphers, Power analysis attacks have been demonstrated. Power analysis attack can be divided into Simple and Differential Power Analysis (referred to as SPA and DPA, respectively). In SPA attacks, the aim is essentially to guess from the power trace which particular instruction is being executed at a certain time and what values the input and output have . Therefore, the adversary needs an exact knowledge of the implementation to mount such an attack. On the other hand, DPA attack does not need the knowledge of the implementation details and alternatively exploiting statistical methods in the analysis process.

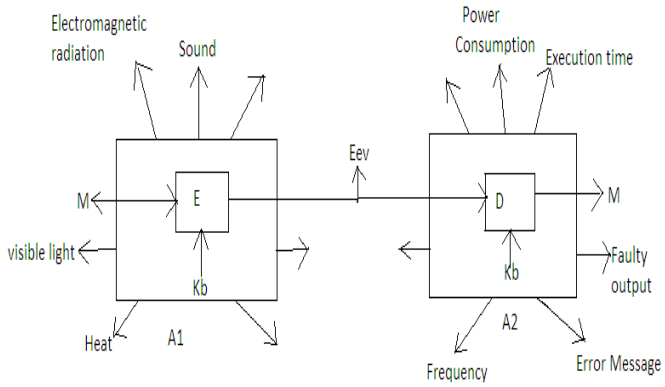

Fig2. Cryptographic model including side channel

For example, the opponent may be able to monitor the power consumed or the electromagnetic radiation emitted by a smart card while it performs private-key operations such as decryption and signature generation. The opponent may also be able to measure the time it takes to perform a cryptographic operation, or analyze how a cryptographic device behaves when certain errors are encountered. It should be emphasized that a particular side-channel attack may not be a realistic threat in some environments. For example, attacks that measure power consumption of a cryptographic device can be considered very plausible if the device is a smart card that draws power from an external source. On the other hand, if the device is a workstation located in a

ISSN 2348 – 7968

secure office, then power consumption attacks are not a significant threat.

2. Related Work

Farooq Anjum have proposed an initial approach for detection of intrusions in ad hoc networks. Anand Patwardhan have display a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol independent Intrusion Detection and Response system for adhoc networks.

Kamal Deep Meka have proposed a trust based framework to enhance the security of adhoc network routing protocols. They have selected the Ad hoc on demand Distance Vector (AODV) for constructing their trust framework which used widely. Making minimum changes for implementing AODV and attaining increased level of security and reliability is their goal. Their schemes are based on incentives & penalties depending on the behavior of network nodes.

Marc Joye and Jean-Jacques Quisquater investigates the Hessian parameterization of an elliptic curve as a step towards resistance against such attacks in the context of elliptic curve cryptography. The idea is to use the same procedure to compute the addition, the doubling or the subtraction of points.

Elena Trichina and Antonio Bellezza presents a study of software counter measures against side channel attacks for elliptic curve cryptosystems.They introduce two new counter measures. The first is a new implementation technique, namely, homogeneous group operations, which has the property that addition and doubling on elliptic curves cannot be distinguished from side channel analysis. Being inexpensive time-wise, this technique is an alternative to a well-known Montgomery ladder. The second is a non-deterministic method of point exponentiation with precomputations. Although requiring rather large ROM, it provides an effective resistance against high-order power analysis attacks for the price of index re-computations and ROM accesses.

YongBin Zhou, DengGuo Feng present and surveys the methods and techniques employed in various side channel attacks, the destructive effects of such attacks, the countermeasures against such attacks and evaluation of their feasibility and applicability. Finally, the necessity and feasibility of adopting this kind of physical security testing and evaluation in the development of FIPS 140-3 standard are explored.

3. Methodology

Methodology concentrates on devising a scheme which will address the successful denial of attack in order to protect the system from being extracting the secret key to the attacker. We mainly focus on the power analysis attack. The scheme focuses on generation of ECSM (Elliptic curve scalar multiplication) using Montgomery ladder algorithm. For making the elliptic curve scalar multiplication more secure and speeding up against the various side channel attack such as power attack and timing analysis attack. Since various methods have been invented using particularly chosen elliptic curves. We show that both goals can be achieved simultaneously even for conventional elliptic curves over Fp. This result shown via two facts first is that every elliptic curve over Fp admit scalar multiplication by using Montgomery ladder algorithm. This is the resistant against the power analysis attack. In an elliptic curve cryptosystems, basically target for side-channel attacks are the algorithms that are used for the elliptic curve scalar multiplication(ECSM).In this multiplication one is given a positive integer k, a point P on a curve C over a finite field Fq and the task is to add k times the point P to itself, which is usually denoted as
k× P, generally the elliptic curves are known to be abelian additive groups with respect to the addition of points. In this case point p is public which is chosen by an attacker and the scalar k kept secret that attacker wants to extract from the system. As power analysis attacks are mainly differentiate in to differential and non differential attacks. An attack relying on a differential analysis guesses unknown (hardware or software) internal bits and then correlates this guessing over a large number of runs.
This attack is normally controlled well known randomization technique which is concerning elliptic curves.
The Montgomery ladder solves the various problem, as it leads to a uniform execution pattern, as it always performs an addition and a doubling independently of the scalar k.
It exploits the fact that if the difference of two points is known, it is easier to compute their sum. The Montgomery ladder was originally introduced to accelerate the scalar multiplication on a certain restricted class of curves defined over Fp. The Montgomery ladder algorithm for non differential side channel attacks works as follows. Let k be a positive integer and (kn-1,……,Ko) its binary representation where we may assume that kn-1 =1.To

ISSN 2348 – 7968

compute kP we start with the pair (P; 2P). At the beginning of each step i we have the pair (P1; P2) = (mP; (m+1)P) where m = (kn-1; : : : ; kn-1-i) and at the end we eventually have (kP; (k + 1)P).
Input: An integer K>=1 and a point P on the curve C.
Output: kP.
1.P1 ← P and P2 ←2P.
2. For i from n- 2 down to 0 do
if ki = 1 then
P1← P1 + P2 and P2 ←2P2
else
P2 ←P1 + P2 and P1←2P1.
3. Return P1.
Montgomery ladder algorithm

3.1 Implementation Performance

3.1.1. Topology formation and neighbor discovery phase:

In this phase, constructing project design in NS2 should take place, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous neighbor establishment. 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. In network formation we create 49(0-48) number of mobile nodes. Set the value of X co-ordinates and Y co-ordinates and set routing protocol as DSR(dynamic source routing) protocol. In our simulation channel capacity of mobile hosts is set to the same value. In simulation we use IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the link breakage. In our simulation path is elected based on the simulation. . The simulated traffic is Constant Bit Rate (CBR). Propagation/Two Ray Ground , these models are used to predict the received signal power of each packet. At the physical layer of each wireless node, there is a receiving threshold. When a packet is received, if its signal power is below the receiving threshold, it is marked as error and dropped by the MAC layer. Basically, Base node sends the discovery packet to the every node and performs the energy level analysis. For sending the hello packets neighbors calculation is done on the basis of X and Y parameters. According to the X and Y parameters value, the node having values in particular range, base node send discovery packets to it. In Elliptic curve cryptography we use Elliptic curve scalar multiplication. We have developed a mechanism that efficiently performs power control according to packet type. This mechanism adds only a flag (usePtFlag_) into the physical layer. This flag is set by MAC layer to indicate that a packet must be sent using Pt_, otherwise the packet has to be sent with Pmax. Then the Power transmission is calculated at network layer and must be set at physical layer, a trivial solution is to directly access (in cross layer) and update Pt_ whenever its value changes. Transmission power adjustment after sending RTS and before completely transmitting data, at the transmitter: Transmission power adjustment after receiving RTS and before completely sending ACK, at the receiver: Then after energy model monitors how energy is spent based on user's definition of various energy parameters, such as the power levels when operating in different modes. NS-2 implements a very simple energy model defined by class Energy Model. The model represents energy level in a mobile node. It considers four radio states: transmit, receive, idle and sleep which could be parameterized.

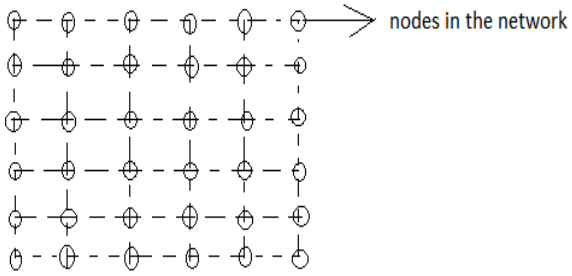

Fig3. Network formation

3.1.2. 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. In this phase we include multiplication algorithms, Montgomery Power Ladder, In this algorithm for every bit of k, stores both an addition and a doubling. In this algorithm conditional branches are not present, the algorithm dose not relay on the actual bits of d and is thus SPA-secure. This method is especially nice since it doesn't even reveal the Hamming weight (number of 1's) of the key, as opposed to other blinding techniques which might.

ISSN 2348 – 7968

In SPA attack, attacker directly observes a system's power consumption. Different attacks are possible depending on the capabilities of the attacker. Some cases where the attacker may be allowed to run only a single encryption or decryption operation. Other attackers may have unlimited access to the card. The most powerful attackers not only have unlimited access, but also have detailed knowledge of the software and hardware running in the card. If an attacker can determine exact location, where certain instructions are being executed, it can be relatively simple to extract important data. A more powerful attack can result if the attacker can see Hamming weight information about the key bytes and also attacker know the information about shifted versions of the key bytes. A DPA attack is more powerful than an SPA attack. In DPA attack, the attacker does not need to know as many details about how the algorithm was implemented. The technique also gains strength by using statistical analysis to help recover side channel information.

3.1.3. ECC attack detection

The source node broadcast the RREQ message to neighbors for establishing the path to destination. The malicious nodes 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

Update its block table that node is a malicious node. After detecting the malicious node it will eliminated from the network. In the network 0-49 nodes are present. Nodes 10,31,34,48 are detected malicious nodes.

3.1.4. Data Transmission and Graph Design Based Result

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.

Graph is an essential part of display a result, so we plot a graph to show a various result comparison with packets, throughput, energy efficient and etc. Figure 4 shows the energy consumption graph according to the nodes in the network. It shows how much energy requires to each node for performing the operation. Figure 5 shows the graph data transfer versus time. It shows the data transfer rate of nodes in the network. Figure 6 and 7 shows the packet delivery ratio and packet drop ratio respectively versus time.

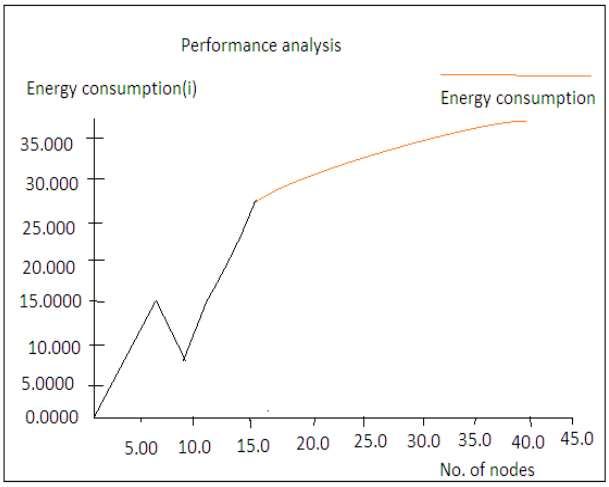

Fig.4 Energy consumption graph

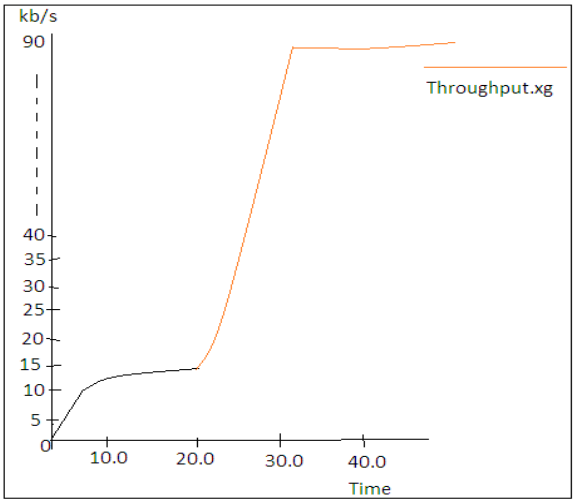

Fig5. Throughput analysis graph

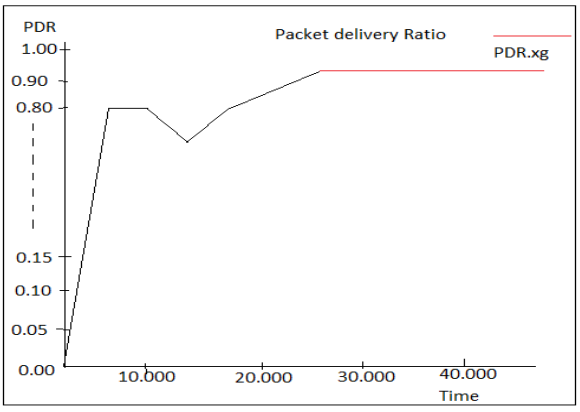

Fig6. Packet delivery Ratio

ISSN 2348 – 7968

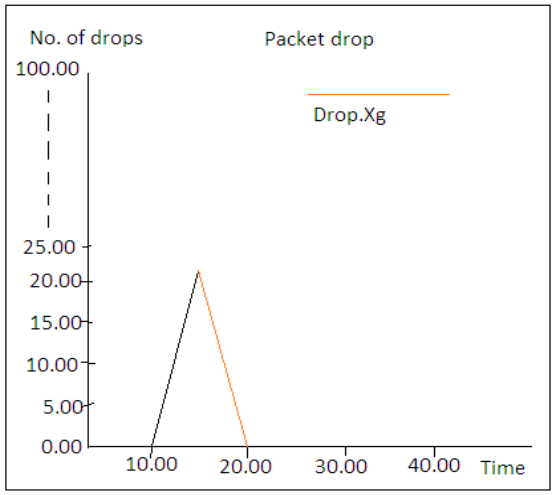

Fig7. Packet drop ratio

4. Conclusion

We introduce a method elliptic curve scalar multiplication that provides immunity against the power analysis attack. The algorithm is the Montgomery ladder algorithm, to ensure point addition and point doubling. , we introduce a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. Then the node is extracted from the network. We have shown that the proposed MAC-layer security protocol achieves high packet delivery ratio while attaining low delay and overhead.

5. References:

[1] J. Fan, X. Guo, et al., State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures. IEEE, 2010.

[2] L. Goubin, A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems, CP8 Crypto Lab, SchlimbergerSema, pp. 207-208, 2003.

[3] J. Fan, X. Guo, et al., State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures. IEEE, 2010.

[4] C.H. Lim. *A New Method for Securing Elliptic Scalar Multiplication Against Side-Channel Attacks*. ACISP 2004, LNCS 3108, pp.289-300, 2004.

[5] M. O. Pervaiz, M. Cardei, and J. Wu, " Routing Security in Ad-hoc Wireless Networks" Network Security , S. Haung, D. Maccallum, Springer, 2008.

[6] S. Kadir, A. Sasongko, et al, Simple Power Analysis Attack against ECC Processor on FPGA Implementation.

[7] 2011 International Conference on Electrical Engineering and Informatics, 17-19 July 2011.

[8] H. Cohen, G. Frey, et al, Handbook of Elliptic and Hyperelliptic Curve Cryptography, chapter 28. Chapman and Hall/CRC, 2005.

[9] M. Medwed and E. Oswald, Template Attacks on EDCSA. Information Security Applications, WISA, vol. 5379, 2008, pp. 14-27, 2008.

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

[11] L.C. Brown, P.M. Berthouex, et al, Statistics for Environmental Engineers, 2nd Ed., chapter 31. CRC Press,2002.

[12] Joye, M., Quisquater, J-J.,: Hessian elliptic curves and side-channel attacks. Proc.*Cryptographic Hardware and Embedded Systems (CHES 2001)*, LNCS **2162** (2001) 402–410

[13] Izu, T., Takagi, T.: A fast parallel elliptic curve multiplication resistant against side channel attacks. Proc. Public Key Cryptography (PKC 2002), LNCS **2274** (2002) 280–296

[14] Hankerson, D., Hernandez, J. L., Menezes, A.: Software implementation of elliptic curve cryptography over binary fields. Proc. Cryptographic Hardware and Embedded Systems (CHES 2000), LNCS **1965** (2000)