SURVEY ON "SECURITY ARCHITECTURE BASED ON ECC (ELLIPTIC CURVE CRYPTOGRAPHY) IN NETWORK"

Mrs. Sweta Nigam, Mr. K.N. Hande

[1]*M. Tech (CSE), Priyadarshini Bhagwati College of Engineering Nagpur (M.S.),*
Shwetawhite13@rediffmail.com
[2]*Asst. Professor, Priyadarshini Bhagwati College of Engineering Nagpur (M.S)*

Abstract

Cryptography is the technique of hiding message in some unintelligible format so that the message lies hidden in plain sight of an unintended person. Public key cryptography offers a wide range of security over the various modes of transferring data, especially over Internet. Countermeasures against these attacks should be considered during cryptosystem design. Side channel attacks allow an attacker to retrieve secret keys with far less effort than other attacks. The main aim of this paper is to introduce ECC to implement an efficient and secure networks with high speed as compared to current standards by using various techniques and algorithms

***Keywords**: Elliptic Curve Cryptography, Side Channel Attack, Running Time, Power Consumption, Electromagnetic Radiation.*

I. Introduction

Elliptic curves as algebraic geometric entities have been studied extensively for the past 150 years, and from these studies have emerged. They allowed establishment of generation of asymmetric cryptographic algorithms. A 2048-bit RSA key and a 210-bit ECC key are equivalent .The use of an ECC can be done to prepare the network which can defend against attackers who can attack on them. No better data can be leaked or any other information can retrieved from another place. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

In 1985, Koblitz and Miller introduced the use of elliptic curves in public key cryptography called Elliptic curve Cryptography (ECC). Basically, the main operation of elliptic curves consists of multiplying a point by a scalar in order to get a second point; the complexity arises from the fact that, given the initial point and the final point, the scalar could not be deduced, leading to a very difficult problem of reversibility, or cryptanalysis, called also the elliptic curve discrete logarithm problem.

ECC was developed by certicom a mobile business security provider. Elliptical Curve Cryptography (ECC) is a public key encryption technique based on elliptic curve Theory that can be used to create more efficient and smaller Cryptographic keys. ECC helps to establish equivalent security with lower computing power and battery resource usage. ECC is based on properties of particular type of Equation created from mathematical group. There is a set which is large but finite. There is a Group Operator is typically denoted by the symbol .Every user has a public and private key. Public key is used for Encryption/digital Signature verification. Private Key is used for Decryption/ Digital Signature Generation.

"Side channel attacks" are attacks that are based on "Side Channel Information". Side channel information is information that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the ciphertext resulting from the encryption process.

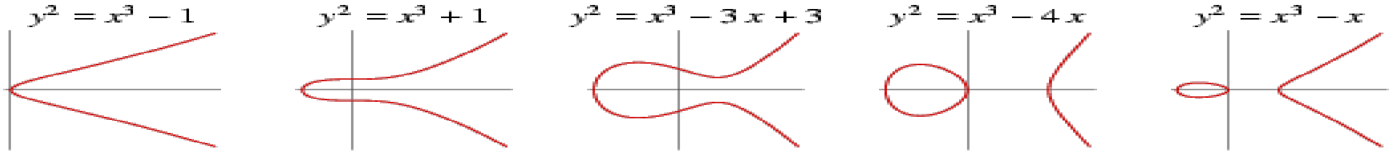
In the past, an encryption device was perceived as a unit that receives plaintext input and produces ciphertext output and vice-versa. Attacks were therefore based on either knowing the ciphertext (such as ciphertext-only attacks), or knowing both (such as known plaintext attacks) or on the ability to define what plaintext is to be encrypted and then seeing the results of the encryption (known as chosen plaintext attacks).

BASICS OF ELLIPTIC CURVE

An elliptic curve is a plane curve defined by an equation of the form

$$y^2 = x^3 + ax + b$$

Examples



Side Channel Attack

Side-channel analysis is a powerful technique re-discovered by P. Kocher in1996.Side Channel Attacks" are attacks that are based on Side "Channel Information." Side channel information is information that can be retrieved from the encryption device. This information is neither the plaintext nor the ciphertext. Side channel analysis techniques are a concern because the attacks can be mounted quickly and cheaply.

In cryptography, a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Depending on the type of attack, it can take a short amount of time to attack a card. For example, with a Simple Power Analysis attack, attacks on smartcards take a few seconds per card.

Side channel attacks based on following Parameters

Time Analysis
Power Analysis
Electromagnetic analysis

Types of attacks in ECC

TIMING ATTACKS

Timing attacks are based on measuring the time it takes for a unit to perform operations. This information can lead to information about the secret keys. For example: By carefully measuring the amount of time required to perform private key operations, an attacker might find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems If a unit is vulnerable, the attack is computationally simple and often requires only known ciphertext.

POWER CONSUMPTION ATTACKS

These attacks are based on analyzing the power consumption of the unit while it performs the encryption operation. By either simple or differential analysis of the power the unit consumes, an attacker can learn about the processes that are occurring inside the unit and gain some information that, when combined with other cryptanalysis techniques, can assist in the recovery of the secret key. It can also be categorised into following:

Simple Power Analysis (SPA) Attacks
Differential Power Analysis (DPA) Attacks

II. RELATED WORK

An efficient implementation of point multiplication on Koblitz curves for extremely-constrained applications such as RFIDs and sensor networks. We have represented the field elements by GNB over and used bit-level multiplications. One main advantage of these multipliers is their cheap squaring's in hardware and providing low area complexity suitable for resource-constrained and secure environments. Through sharing the addition/accumulation part of the bit-level multiplier to perform other field additions, lower area complexities have been achieved. We have also proposed a new technique for computing point addition in affine coordinate. This approach needs fewer registers for storing the intermediate variables compared to the traditional schemes. Comparing the results of our ASIC implementation using a CMOS library to the previously presented works shows that our work has lower energy consumption and requires less than half of the clock cycles to compute point multiplications. Consequently, the proposed efficient implementation of point multiplication on Koblitz curves is suitable for extremely-constrained environments.

Next, we analyze and discuss two possible directions for future research. Implementation attacks are cryptanalytic attacks that utilize information obtained from a physical implementation of a cryptographic algorithm through a side-channel, e.g., timing, tower, or electromagnetic radiation or by analysing results from the implementation after deliberately injected faults. They form a serious threat for cryptosystems in practice. Countermeasures against these attacks typically come with significant costs in area and latency which makes their use challenging in extremely-constrained applications. As a consequence, the most appropriate countermeasures must be selected based on a careful risk analysis of the application. Because our target was to minimize the resource requirements and to propose a general processor architecture that could be useful in a large variety of applications (perhaps after small modifications), our processor does not implement any specific countermeasures. However, certain simple countermeasures could be added with small overheads. These include, e.g., blinding the sign of by using dummy additions for point additions and blinding the positions of nonzero by using dummy maps. More generally, developing and applying low-cost countermeasures for our processor and other extremely-constrained processors is an important.

In many applications, it is possible to use cryptosystems where conversions can be avoided by generating representations at random or by pre-computing and hardwiring them. Extremely-constrained applications typically require careful fine-tuning (e.g., by fixing certain parameters, of the cryptosystems that are used in the application and these aspects should be taken into account when considering different cryptosystems for the application.

Nevertheless, techniques for computing conversions with minimal resources and with resources shared with the architecture computing point multiplications.

Bit-level multiplication using normal basis provides cheap squaring's and, comparably, low area complexity, making it suitable for resource-constrained environments. The main contributions of this paper can be summarized as follows:

- In addition/accumulation part of the bit-level multiplier to perform other field additions, resulting in lower area complexities. Moreover, employing normal basis representation provides cheap squaring's which can be achieved by rewiring on hardware.

•A new technique to compute point additions in affine coordinates. This technique is based on applying a recently introduced inversion algorithm [and it requires fewer registers to store intermediate variables than the traditional schemes.

III. METHODOLOGY

1. Choosing a Curve

For each of the cryptographic methods depended on the difficulty of the EC discrete log problem, we must begin by choosing an elliptic curve that is not susceptible to the known fast attacks on the discrete log problem, such as the MOV attack described in the previous section. The curve must therefore satisfy the following restrictions:

There exists a large prime p dividing #E(Fq), so that the problem is not susceptible to the Pollard attack.
#E(Fq)=6q (i.e. the curve is not anomalous). This prevents the problem from being susceptible to the Semaev Smart SatohAraki attack.

2. Setup for Encryption Algorithms

Consider the following problem of cryptography:
Alice wants to send Bob a message m, usually assumed to be an integer. However, she does not want the eavesdropper Eve to be able to read the message as well. Therefore, Alice uses and encryption key to encrypt the message, and sends the resulting ciphertext (rather then the plaintext) to Bob. Bob then uses a decryption key to decrypt they message. Obviously, Eve must be prevented from finding the decryption key, as otherwise she would also be able to decode the message.

There are two possibilities in this scenario. Perhaps Alice and Bob were able to communicate secretly in advance and agree on a key, and perhaps they were not. If they were, the encryption and decryption keys may be the same. If they were not, they must establish a public encryption key that allows Alice to encode the message and a different private decryption key that allows Bob to decrypt the message.

3. ECPM Encryption

Elliptic curve point multiplication (ECPM) is one of the most critical operations in elliptic curve cryptography. In this brief, a new hardware architecture for ECPM over GF(p) is presented, based on the residue number system (RNS). The proposed architecture encompasses RNS bases with various word-lengths in order to efficiently implement RNS Montgomery multiplication. Two architectures with four and six pipeline stages are presented, targeted on area-efficient and fast RNS Montgomery multiplication designs, respectively. The fast version of the proposed EC architecture achieves higher speeds and the area efficient version achieves better area–delay tradeoffs compared to state of- the-art implementations.

4. Key Exchange module

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible: this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem.

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key: for example, a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public k**ey.**

5. Topology Formation

Constructing project design in NS2 should takes place. In this phase, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous neighbor establishment.

6. 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.

7. Timing attack

A timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Every logical operation in a node takes time to execute, and the time can differ based on the input; with precise measurements of the time for each operation, an attacker can work backwards to the input. Information can leak from a system through measurement of the time it takes to respond to certain queries sent by source node.

ECC attack detection

The source node broadcast the public key based RREQ message to neighbors for establishing the path to destination. The timing attacker nodes node forwards the rreq message continuously to unreached destination 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.

8. Power analysis attack and its detection

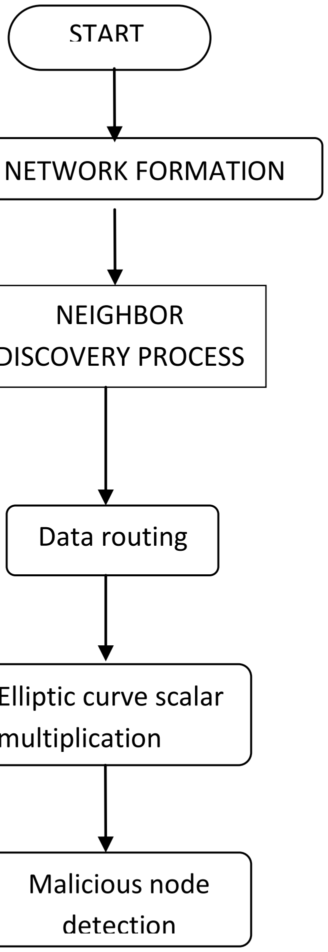
Power analysis attack is a side-channel attack which involves visual examination of graphs of the current used by a device over time. Variations in power consumption occur as the device performs different operations. For example, different instructions performed by processing node will have differing power consumption profiles. So by analyzing the energy consumption of all nodes, we can detect the timing attack as node which consumes more energy.

9. 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.

Graph Design Based Result

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.


START
NETWORK FORMATION
NEIGHBOR DISCOVERY PROCESS
Data routing
Elliptic curve scalar multiplication
Malicious node detection

IV. Conclusion

An efficient implementation of point multiplication on Koblitz curves for extremely-constrained applications such as RFIDs and sensor networks .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. Techniques for computing conversions with minimal resources and with resources shared with the architecture computing point multiplications should be studied in the future.

References

[1] R. Azarderakhsh and A. Reyhani-Masoleh, "Low-complexity multiplier architectures for single and hybrid-double multiplications in Gaussian normal bases," IEEE Trans. Compute., vol. 62, no. 4, pp.744–757, 2013.

[2] S. Kumar, T. Wollinger, and C. Paar, "Optimum digit serial multipliers for curve-based Cryptography""IEEE Trans. Compute., vol.55, no. 10, pp. 1306–1311, 2006.

[3] M. Mozaffari Kermani and A. Reyhani-Masoleh, "A low-power high-performance concurrent fault detection approach for the com-positefield S-box and inverse S- box,"IEEE Trans. Compute., vol.60, no. 9, pp. 1327–1340, 2011.

[4] M. Mozaffari Kermani and R. Azarderakhsh, "Efficient fault diagnosis schemes for reliable lightweight Cryptographic ISO/IEC standardCLEFIA benchmarked on ASIC and FPGA,"IEEE Trans. Ind. Electron., vol. 60, no. 12, pp. 5925–5932, Dec. 2013.

[5] S. Kumar and C. Paar, "Are standards compliant elliptic curve crypto systems feasible on RFID," in Proc. Workshop RFID Security (RFIDSec 2006), 2006.

[6] L. Batina, N. Mentens, K. Sakiyama, B. Preneel, and I. Verbauwhede,"Low-cost elliptic curve Cryptography for wireless sensor networks,"inProc. Security and Privacy in Ad-Hoc and Sensor Networks, 2006,pp. 6–17.

[7] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic-curve-base security processor for RFID,"IEEE Trans. Compute, vol.57, no. 11, pp. 1514–1527, 2008.

[8] D. Hein, J. Wolkerstorfer, and N. Felber, "ECC is ready for RFID-Aproof in silicon," in Proc. Workshop on Selected Areas in Cryptography(SAC 2009), 2009, pp. 401–413, Springer.

[9] U. Kocabas, J. Fan, and I. Verbauwhede, "Implementation of binary Edwards curves for very-constrained devices," in Proc. 21st Int. Conf.Application-Specific Systems Architectures and Processors (ASAP 2010), 2010, pp. 185–191.

[10] V. Dimitrov and K. Järvinen, "Another look at inversions over binary fields," in Proc. 21st IEEE Int. Symp. Computer Arithmetic (ARITH-21), 2013, pp. 211–218.

[11] R. Azarderakhsh and A. Reyhani-Masoleh, "A modified low complexity digit-level Gaussian normal basis multiplier," in Proc. 3rd Int.Workshop Arithmetic of Finite Fields (WAIFI 2010), 2010, vol. 6087,pp. 25–40.

[12] A. Reyhani-Masoleh, "Efficient algorithms and architectures for field multiplication using Gaussian normal bases,"IEEE Trans. Comput.,vol. 55, no. 1, pp. 34–47, 2006.

[13] A. Reyhani-Masoleh, "A new bit-serial architecture for field multiplication using polynomial bases," in Proc. Cryptographic Hardware and Embedded Systems— CHES 2008 E.Oswald, and P.Rohatgi,Eds.,2008, vol. 5154, ser. Lecture Notes in Computer Science, pp. 300–314.

[14] N. Koblitz, "CM-curves with Good Cryptographic Properties," in Advances in Cryptology (CRYPTO 1991).NewYork,NY,USA:Springer, 1992, pp. 279–287.

[15] B. B. Brumley and K. U. Järvinen, "Conversion algorithms and implementations for Koblitz curve Cryptography,"IEEE Trans. Compute.vol. 59, no. 1, pp. 81–92, 2010.

[16] J. Adikari, V. Dimitrov, and K. Järvinen, "A fast hardware architecture for integer to -NAF conversion for Koblitz curves,"IEEE Trans.Comput., vol. 61, no. 5, pp. 732–737, May 2012.

[17] E. Al-Daoud, R. Mahmod, M. Rushdan, and A. Kilicman, "Anew addition formula for elliptic curves over ,"IEEE Trans. Compute.,vol. 51, no. 8, pp. 972–975, 2002.

[18] C. Rebeiro and D. Mukhopadhyay, "High speed compact elliptic curve cryptoprocessor for FPGA Platforms," in Progress in Cryptology, IN- DOCRYPT 2008 . New York, NY, USA: Springer-Verlag, 2008, vol. 5365, ser. Lecture Notes in Computer Science, pp. 376–388.

[19] C. Rebeiro, S. S. Roy, D. S. Reddy,and D. Mukhopadhyay, "Revisiting the Itoh-Tsujii inverions algorithm for FPGA platforms,"IEEE Trans.Very Large Scale Integer. (VLSI) Syst., vol. 19, no. 8, pp. 1508–1512, 2011.

[20] S. S. Roy, C. Rebeiro, and D. Mukhopadhyay, "Theoretical modeling of the Itoh-Tsujii inversion algorithm for enhanced performance on -LUT based FPGAs," in Proc. Design, Automation & Test in Europe (DATE 2011), 2011, pp. 1–6.