www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13187-13191

On Improving Side channel Attack defence mechanism using ECPM technique under Elliptic curve Cryptography

[1]Mrs. Sweta Nigam, [2]Mr. K.N. Hande
Priyadarshini Bhagwati college Of Engineering,
Nagpur(M.S.)
Shwetawhite13@rediffmail.com

, Priyadarshini Bhagwati College Of Engineering,
Nagpur(M.S.)

Abstract:In recent years, elliptic curve cryptography (ECC) has gained widespread exposure and acceptance, and has already been included in many security standards. Engineering of ECC is a complex, interdisciplinary research field encompassing such fields as mathematics, computer science, and electrical engineering. In this paper, we survey ECC implementation issues as a prominent case study for the relatively new discipline of cryptographic engineering. In particular, we show that the requirements of efficiency and security considered at the implementation stage affect not only mere low-level, technological aspects but also, significantly, higher level choices, ranging from finite field arithmetic up to curve mathematics and protocols.

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

1. Introduction

Encryption is the process of transforming plaintext data into cipher text in order to conceal its meaning and so preventing any unauthorized recipient from retrieving the original data. The main task of encryption is to ensure secrecy. Companies usually encrypt their data before transmission to ensure that the data is secure during transit.

The encrypted data is sent over the public network and is decrypted by the intended recipient. ECC is an public key cryptography system.

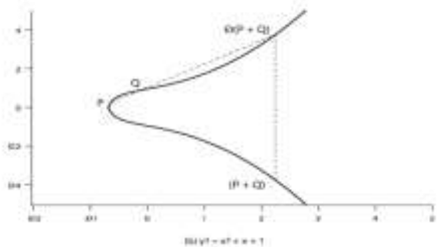
In public key cryptography , each user or the device taking part in the communication have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the Algorithms, it can be easily exchanged online.

ECC systems are also well suited for applications that need long-term security requirements. Elliptic Curve Cryptography (ECC) is a public key technology that offers performance advantages at higher security levels. Every user taking part in public key cryptography will take a pair of keys, a public key and a private key. Only the particular user knows the private key whereas the public keys are 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. In ECC we call these predefined constants as 'Domain Parameters'

BASICS OF ELLIPTIC CURVE

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

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



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, 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 ANALYSIS ATTACKS**
- **SIMPLE POWER ANALYSIS (SPA) ATTACKS**
- **DIFFERENTIAL POWER ANALYSIS (DPA) ATTACKS**

2. Literature Survey

An Elliptical curve architecture has worked by many peoples . In that architecture thereare certain theory has been applied for the technique.

Mr. S. Kumar, T. Wollinger and C.Paar has performed in"Optimum digit serialmultipliers for curve based cryptography "it has been defined various digital appliances used for building networks where various faults has been provided with various optimum
solutions for different curves in 2006.

Similarly M. Mozaffari Kermani and A. Reyhani-Masoleh, "A Low lower high Performance concurrent fault detection approach for the composite field S-box and inverse S-box ,", various theory has been applied for des algorithm in which various tools has been implemented for various other features for various location s and they had been worked for various individuals for different ways for detection of faults in them and there should be various tools for the corrrction of faults handling in them.

In the Implementation of binary Edwards curves for very constrained devices there should be an implementation of many devices which should have been worked for
different regions in them and they had been introduced by

U.Kocabas, J.Fan, and I.Verbauwhede who mentions the architectures of various tools for the processors.

R. Azarderakhsh and A. Reyhani-Masoleh , "A modified low complexity digit-level Gaussian normal basis multiplier in 2010 defines the low level of complexities in them ,it involves the normal guassian techniques on them which multiplies many differential analysis on them for their complexities on them for their normal form occurences on them for their rather verifications on them.

J. adikari, V. Dimitrov, and K. Jarvinen includes an architecture by the use of integer to NAF coversion for Koblitz curve cryptosystems for the framing structure by the use of their conversions of the number fractions into them.

3. METHODOLOGY

3.1 User authentication

In user authentication ,no repetitive registration is needed for the multiserver environments. No verification table is stored in the server. Mutual authentication and session key agreement can be achieved between the users and the service servers to carry on subsequent communications. Various possible attacks can be resisted.

3.2 ECPM Encryption

Elliptic curve cryptography is being used popularly over years due to the fact that it has fundamental and very efficient technological alternatives for building up secure public key cryptosystems. They provide distinct advantages such as smaller key sizes and higher security strength for each bit of the data. The major issue of key storage for networks can also be solved using ECC. As these cryptosystems require fewer amounts of storage and low bandwidth requirements, they are feasible to implement over wireless networks. The security depends on the difficulty of solving discrete logarithmic problem for large prime numbers. The more the problem difficulty is, the better the security is to be calculated

3.3 Key exchange module

ECMQV (Elliptic curve Menezes Qu Vanstone) is an authenticated key agreement protocol, which is based on Diffie-Hellman scheme. Considering the worst case of active attacks, this algorithm is best

3.4 RNS based Multiplication methods

3.4.1 Elliptic Curve Point Multiplication[ECPM]

The dominant operation in ECC cryptographic schemes is point multiplication. This is the operation which is the key to the use of elliptic curves for asymmetric cryptography---the critical operation which is itself fairly simple, but whose inverse (the elliptic curve discrete logarithm problem defined below) is very difficult . ECC arranges itself so that when you wish to performance operation the cryptosystem should
make easy encrypting a message with the public key, decrypting it with the private key the operation you
are performing is point multiplication .

Point multiplication is simply calculating the value of *kP*, where *k* is an integer and *P* is a point on the elliptic curve defined in the prime field. In point multiplication, a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point Q on the same elliptic curve, i.e. kP=Q.

Point multiplication is achieved by two basic elliptic curve operations.

- Point addition, adding two points J and K to obtain another point L i.e., L = J + K.
- Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J.

3.4.2 Elliptic Curve Point Addition

Point addition is the addition of two points J and K on an elliptic curve to obtain another point L on the
same elliptic curve.

Consider two points J and K on an elliptic curve as shown in figure (a). If K ≠ -J then a line drawn through
he points J and K will intersect the elliptic curve at exactly one more point –L. The reflection of the point –
L with respect to x-axis gives the point L, which is the result of addition of points J and K. Thus on an
elliptic curve L = J + K. If K = -J the line through this point intersect at a point at infinity O. Hence J + (-J)
= O. This is shown in figure 2(b). O is the additive identity of the elliptic curve group. A negative of a point

is the reflection of that point with respect to x-axis.

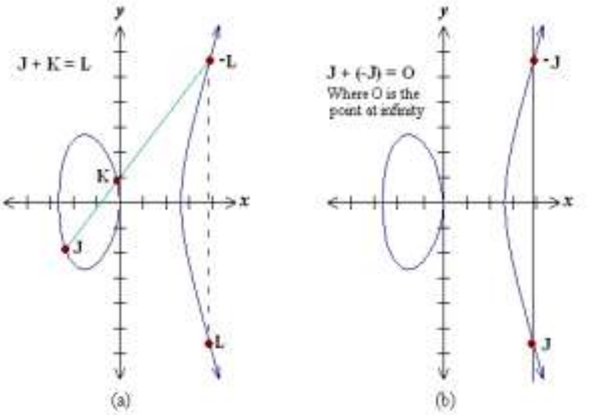


Fig2(a) & 2(b). Addition of two points

3.4.3 Elliptic curve Point doubling

Point doubling is the addition of a point J on the elliptic curve to itself to obtain another point L on the same elliptic curve. To double a point J to get L, i.e. to find L = 2J, consider a point J on an elliptic curve as shown in figure 3(a). If y coordinate of the point J is not zero then the tangent line at J will intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respect to x-axis gives the point L, which is the result of doubling the point J.

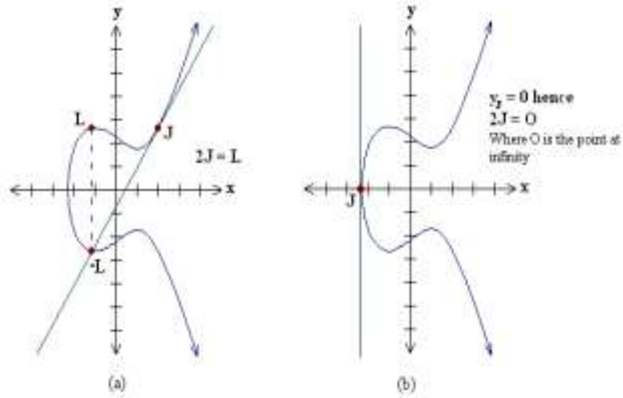
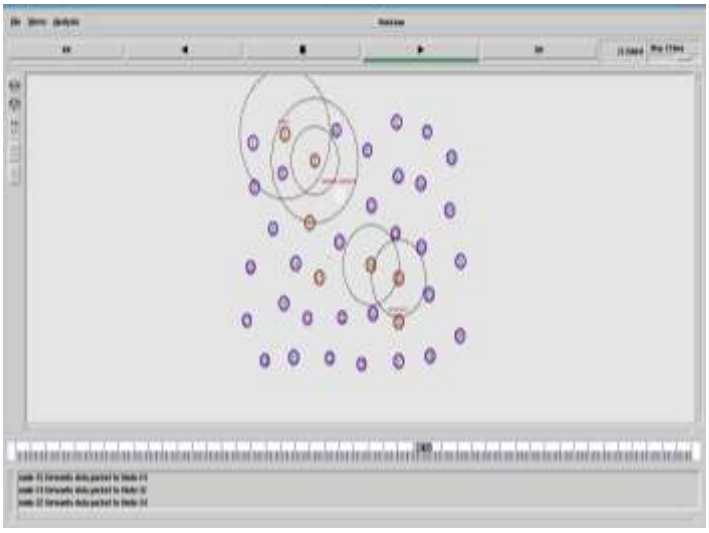


Fig 3(a) & 3(b) doubling

Thus L = 2J. If y coordinate of the point J is zero then the tangent at this point intersects at a point at infinity O. Hence 2J = O when yJ = 0.This is shown in fig 3(b).

3.5 ECPM Decryption

Elliptic curves uses this technology for the reverse process of ECC encryption and they provide different algorithms for obtaining the vice versa of Encryption.



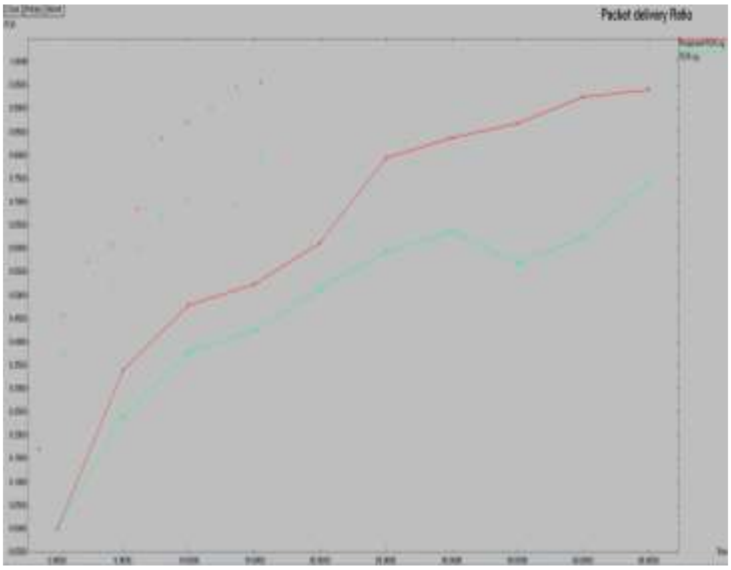
4. Experimental Results and Analysis

Performance parameter such as packet delivery ratio(PDR) analysis, end to end delay analysis, Packet drop , Average trust percentage are taken into consideration while comparing the previous proposed system.

4.1 PDR analysis

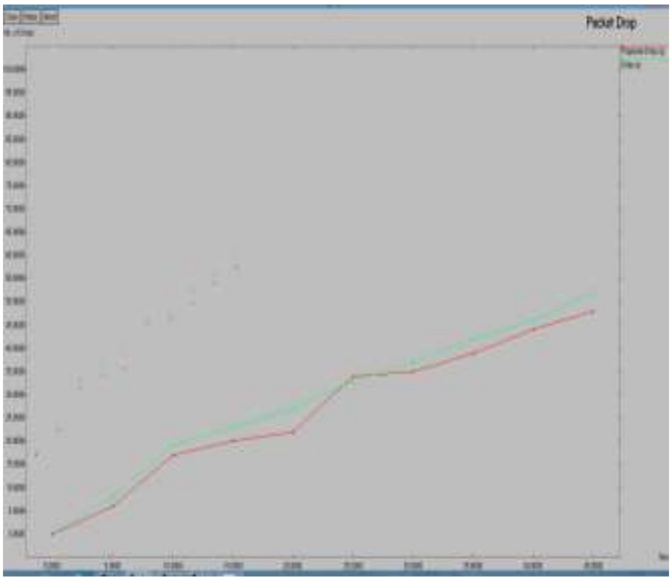
PDR analysis is nothing but the ratio of the number of data packet delivered to the destination. If the value of PDR is greater it means it has greater performance level.

In our result analysis we have shown that the PDR ratio i.e ratio of number of packet received upon number of packet send is greater than existing system.Fig below shows the PDR of our system.



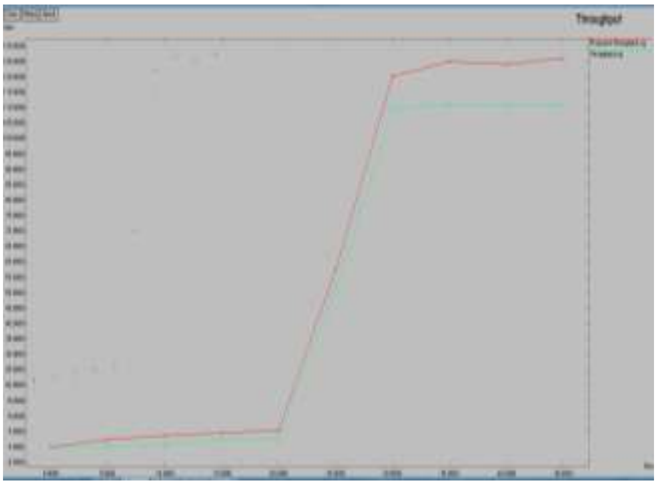
4.2 Packet Loss

Packet loss is total number of packet dropped during simulation which is given as number of packet send minus number of packets received. Fig. below depicts the packet loss in system which is less than the existing systems packet loss.



4.3 Throughput Analysis

The average trust percentage is calculated depending upon the performance of the overall sytem.Fig below shows the throughput analysis of the project.



5. Conclusion

IN this I concluded that ECC are stronger options for providing more security in future. They are small in size and faster in its access in multiplication of finite factors for future use. The technologies used for encryption and decryption of data in this paper provides more security and more faster to access by using the above methodologies in the system with more perfection of data. In previous technologies there should be delayed of data if size is high it also cannot be defeated sometimes with outside attacker so by using these small size ECC with advance methodology we removes the defect for encryption and decryption of data. The dynamic nature of such a system helps to improve performance of a network with respect to various network parameters like packet loss, PDR delays and throughput percentage.

6. References

[1] 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. Comput., vol.60, no. 9, pp. 1327–1340, 2011.

[2] 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. Elec-tron., vol. 60, no. 12, pp. 5925–5932, Dec. 2013.

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

[4] 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,

[5] 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.

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

[7] L. Gao and G. E. Sobelman, "Improved VLSI designs for multiplication an inversion inover normal bases," inProc. 13th Ann.IEEE Int. ASIC/SOC Conf. , 2000, pp. 97–101.

[8] A. Reyhani-Masoleh and M. A. Hasan, "A new construction of Massey-Omura parallel multiplier over,"IEEE Trans.Comput., vol. 51, no. 5, pp. 511–520, 2002.

[9] 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.

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

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

[12] D. Hankerson, S. Vanstone, and A. Menezes , Guide to Elliptic Curve Cryptography New York, NY, USA: Springer-Verlag, 2004.

[13] K. Järvinen, J. Forsten, and J. Skyttä, "Efficient circuitry for computing -adic non- adjacent form," in oc.13thIEEE Int. Conf. Electron.,Circuits Syst., (ICECS- 2006), 2006.

[14] B. B. Brumley and K. U. Järvinen, "Conversion algorithms and im-plementations for Koblitz curve

cryptography,"IEEE Trans. Comput.vol. 59, no. 1, pp. 81–92, 2010.

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

[16] M. A. Hasan, "Power analysis a ttacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems,"IEEE Trans. Comput., vol. 50, no. 10, pp. 1071–1083,2001.

[17] D. Bernstein, T. Lange, and R. Farashahi, "Binary Edwards curves," in Proc. Workshop onCryptographic Hardware and Embedded Systems (CHES 2008) , 2008, vol. 5154, pp. 244–265.

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

[19] 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.

[20] K. Järvinen, "On repeated squarings in binary fields," in Proc. The 16th International Workshop on Selected Areas in Cryptography (SAC 2009). New York, NY, USA: Springer-Verlag, 2009, vol. 5867, ser. Lecture Notes in Computer Science, pp. 331–349.

[21] R. Azarderakhsh and A. Reyhani-Masoleh, "High-Performance imple-mentation of point multiplication on Koblitz curves," IEEE Trans. Cir-cuits Syst. II, Exp. Briefs , vol. 60, no. 1, pp. 41–45, 2013.

[22] S. S. Roy, C. Rebeiro, and D. Mukhopadhyay, "A parallel Architecture for Koblitz curve scalar multiplications on FPGA platforms," in Proc.15th Euromicro Conf. Digital Syst. Des. 2012, 2012, pp. 553–559.

Author Profile

Mrs. Sweta Nigam Completed MCA and tried all efforts for the completion of M.tech in computer science from Nagpur University. During my educational qualification I did many live projects works for the completion of my aspects. And now I am doing research project on Side channel Attacks using Elliptic Curve Cryptography.