International Journal of Engineering & Technology, 7 (3.27) (2018) 421-423

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Implementation Methodology of ECC to Overcome Side Channel Attacks

M. Maheswari[1], R.A. Karthika[2*], Anuska Chatterjee[3]

[1]Department of Software Engineering, SRM Institute of Science & Technology.
[2]Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies.
[3]Department of Software Engineering, SRM Institute of Science & Technology
**Corresponding author E-mail:karthika.se@velsuniv.ac.in*

Abstract

Elliptic Curve Cryptography (ECC) is a form of public-key cryptography. This implies that there is the involvement of a private key and a public key for the purpose of cryptography. ECC can be used for a wide range of applications. The keys used are much smaller than the non-ECC cryptographic algorithms. 256 bit and 384 bit ECC are used by NSA for storage of classified intel as ECC is considered to be a part of suit B cryptography by the NSA. When it comes to normal usage, other versions of ECC are used. So, many of the applications protected by ECC are vulnerable to side channel attacks. So, the objective is to modify the existing method of implementation of ECC is some regular domains like media, smart grid, etc., such that the side-channel attacks [7], [3] vulnerabilities are fixed.

Keywords: *elliptic curve cyptography, side channel attacks.*

1. Introduction

There are various kinds of side channel attacks that can be performed on ECC [6].

- Power Analysis Attack: Happens in hardware implementations
- Fault attack
- EM attack (Electromagnetic analysis)
- The fault disrupts the operation of the cryptographic process. Due to this, a faulty output is generated. Security systems are affected due to fault attacks. There are two kinds of side channel fault attacks.
- The fault that occurs during the operation of the system or computation of the cryptographic module.
- Attack module is sent incorrect input data which results in the attack.

Several techniques have been implemented for prevention of fault attacks. However, many of them are quite difficult to implement when it comes to real world scenarios due to several constraints. Whitfield Diffie and Martin Hellman had introduced a method in 1976. In this, they found the discrete logarithms that are present in a fault key which can be used to find the secret key. Johannes Bloomer introduced a method of fault attack on sign change attacks.

2. Related Work

Elliptic Curve Cryptography

Elliptic-curve cryptography (ECC) is considered as the most secure public key cryptography algorithm based on the algebraic arrangement of the elliptic curve over a defined finite fields. ECC needs smaller keys against non-ECC cryptography (based on plain Galois fields) to provide relative security.[1]

[2] Elliptic curves has a wide variety of application such as key harmony and a vital role in digital signatures, and are applied to generate pseudo-random generators and many other tasks. Also encryption is possible in a numerous ways by using a combination of key agreement with a symmetric encryption. It is evaluated by using many integer factorization algorithms[2] that is relying d on elliptic curves that have applications in network cryptography.

Since cryptography involves the methodology of encrypting and decrypting the messages so as to prevent the messages from tampered from unwanted resources, many algorithms have been proposed on the field of cryptography. Symmetric and Asymmetric encryption algorithm have proven to provide the best security to the messages. Also cryptographic algorithm involving mathematical analysis is also proven to be more effective. One such algorithm is ECC(Elliptic Curve Cryptography), which finding the coordinates on the finite field of the Elliptic curve, plotting the point. The difficulty and complexity of the point is determined by the size of the elliptic curve

The major advantage given by ECC is the use of minor size of keys and have a less storage and transmission requirements. It is considered that the level of security given by an RSA based system with 3072 keys is analogous to the security provided by the 256 bit elliptic curve public key.

Requirement Gathering

Elliptic curve functions act as set tuples. The parameters needed are as follows:

T = (p,a,b,G,n,h)

Here, integer p specifies the finite field Fp, two elements a,b ∈Fp specifies an elliptic curve E(Fp) defined by the equation:

E : y2 ≡ x3 + a.x + b (mod p), a base point G = (xG,yG) on E(Fp), a prime n which is the order of G, and an integer h which is the cofactor h = #E(Fp)/n.
Now, there are a few properties of the parameters of Fp which have been given below:

Parameters	Strength	Size	RSA/DSA	Koblitz or Random
secp192kl	96	192	1536	k
secp192rl	96	192	1536	r
secp224kl	112	224	2048	k
secp224rl	112	224	2048	r
secp256kl	128	256	3072	k
secp256rl	128	256	3072	r
secp384rl	192	384	7680	r
secp521rl	256	521	15360	r

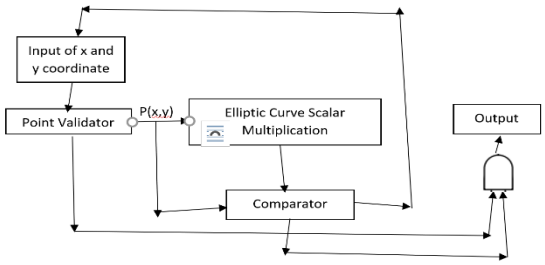
Risk Factors

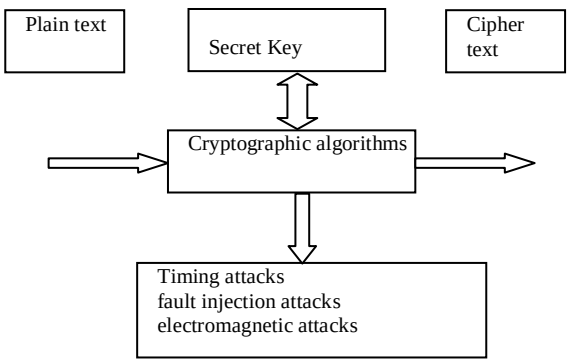
- Add CRC
  - checks for private and public parameters
  - takes more time for execution
- Randomize the computation
  - e.g., d ← d + r n with n = ordE (P)
- Compute the operations twice
  - the running time is twice
- Verify the signatures
  - ECDSA verification is generally slower than signing
- More the steps involved in the encryption/decryption process, more is the processing power that is consumed research

Strengths	Weaknesses
• It is able to prevent some forms of side chain attacks in ECC	• Takes up more computational power • Takes some more time to encrypt than traditional ECC
Opportunities	**Threats**
• Can be made better if more parameters are taken care of	• If somehow the entire system was compromised beforehand then this algorithm can be manipulated by the hacker and can be used as he pleases

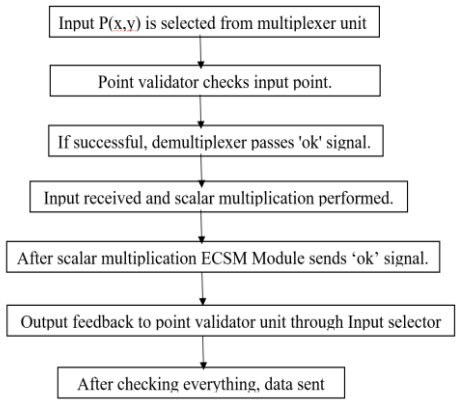
Fig. 1: SWOT analysis

3. Proposed System

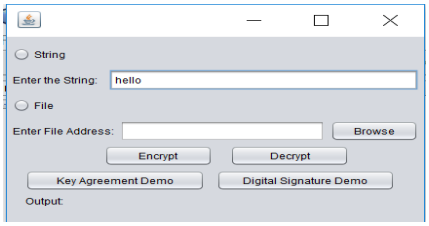


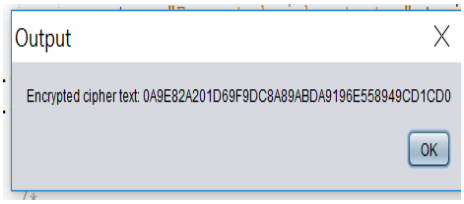


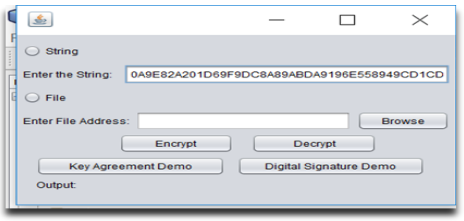
Data Flow Diagram

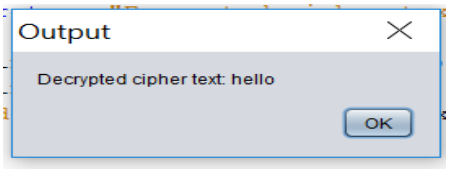


4. Implementation and Result









Furthermore, a multiplexer is used to check for side channel attacks. Only if the multiplexer confirms that no data tampering has occurred, the text will get encrypted. Else, it will only show the plaintext.
The sample output of the image is shown above and this describes about the process of raw image converted as a machine understandable image for the healthcare process.

5. Conclusion

In this paper, the safety measures that can be implemented to counter fault attacks and how it the security can be provided through ECC is discussed. Also ECC being a Public key Cryptosystem proves that it is Secure to protect the system from any vulnerabilities. and also we have tried to implement a countermeasure for side channel fault attack in this paper.[10]

Many mathematical fault models presented in several publications are found to be difficult to implement in real life[4] High precision measuring and fault injection tools are required by bit fault models. The cost involved in implementing that algorithm is very higher and also the system that is proposed in this paper is perfect when it is compared with the protocols that are used in the existing system as countermeasures.[11]

6. Performance Analysis and Future Enhancement

In this paper, the implementation of ECC over side channel attacks is done. Also the same security measure can be applied to the world of smart cities and in to the concept of IOT is largely employed. Since ECC can be implemented in the means of Lightweight, Heavy weight and middle weight methodology, the implementation of ECC using heavy weight methodology for smartcities in IOT could be less vulnerable to attacks that are most preferable happen during data transfer between sensor networks.

Quality of Service and Energy Optimisation is a very important aspect in terms of network security and data transfer aspect. And hence when the level of efficiency for QOS should be high with a very less amount of energy utilisation. And hence considering this factor for further enhancement could give the researchers a fruitful result.

References

[1] Schmidt JM & Medwed M, "A fault attack on ECDSA", *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, (2009), pp.93-99.

[2] Zode PP & Deshmukh RB, "Novel fault attack resistant Elliptic Curve processor architecture", *Annual IEEE India Conference (INDICON)*, (2014), pp.1-6.

[3] Reddy EK, "Overview of the side channel attacks", *International Journal of Advanced Networking and Applications*, Vol.4, No.6, (2013).

[4] Will MA, Ko RK & Schlickmann SJ, "Anonymous Data Sharing Between Organisations with Elliptic Curve Cryptography", *IEEE Trustcom/BigDataSE/ICESS*, (2017), pp.1024-1031.

[5] Harkanson R & Kim Y, "Applications of EllipticCurve Cryptography", *CISRC*, (2017).

[6] Agrawal D, Archambeault B, Rao JR & Rohatgi P, "The EM Side-Channel(s) Attacks and Assessment Methodologies", *Internet Security Group, IBM Watsonsearch Center*.

[7] Pourazarm S & Cassandras CG, "Energy-Based Lifetime Maximization and Security of Wireless-Sensor Networks With General Nonideal Battery Models", *IEEE Transactions on Control of Network Systems*, Vol.4, No.2,(2017), pp.323-335.

[8] Panda M, "Data security in wireless sensor networks via AES algorithm", *IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, (2015), pp.1-5.

[9] Wu J, Ota K, Dong M & Li C, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities", *IEEE Access*, Vol.4, (2016), pp.416-424.

[10] D, Ibrayeva, Z Salkhanova, B Joldasbekova, Zh Bayanbayeva (2018). The specifics of the art autobiography genre. Opción, Año 33. 126-151.

[11] Z Yesembayeva (2018). Determination of the pedagogical conditions for forming the readiness of future primary school teachers, Opción, Año 33. 475-499