A review on Elliptic Curve Cryptography and Variant

Sneha Patil[1], Vidyullata Devmane[2]

[1] *P.G. Student, Department of Computer Engineering, Shah and Anchor College of engineering, Chembur, Mumbai, India*
[2] *Asst. Professor, Department of Computer Engineering Shah and Anchor College of engineering, Chembur, Mumbai, India*

Abstract - *Cryptography is a now a days a need for everywhere data needs to be transferred for securing data over the network. Elliptic curve cryptography along with its own properties like homomorphism for encryption and decryption implementation will give us less computational complexity with same level of security. The security of ECC schemes dependent of resolution of an underlying mathematical problem called the Elliptic Curve Discrete Logarithm Problem (ECDLP) [4]].It has features like point doubling as well as point, multiplication, Homomorphic property of an algorithm gives an advantage of operating a data even after encryption over the networks*.

***Key Words*: Elliptic curve cryptography; point doubling; encryption; homomorphic property; finite fields.**

1. INTRODUCTION

Cryptography in today's world ensures the data integrity, security and confidentiality. Elliptic curve cryptography along with its own properties like homomorphism for encryption and decryption implementation will give us less computational complexity with same level of security like other algorithms. Elliptic curves if simulated with ElGamal, Paillier and RSA gives better security with smaller key generation so that even small devices like mobile phones, pager etc. also can be protected in terms of data transfer. Most efficient algorithm with ECC can be known through comparison of all with respect to distinguishable parameters. The effort will be useful in many areas where streaming data is used also in the areas where data is centrally located. As air is the medium for communication used now a days, this study will help to understand the basics and essential entities required to build a cryptographic system in future. This kind of system will be helpful in future for deployment of various real time applications like online voting, secure data transfer, transferring money through end to end encryption where data is essential entity is to handle and need to protect from different network attacks. Efforts are taken for sharing an information that Combine effect of Elliptic curve cryptography and some good existing cryptosystems gives better results.

2. LITERATURE REVIEW

[1] In This paper, an attempt has been made to prove that the Weierstrass equation is the root of elliptic curve. Also described the group operation on elliptic curve that is point addition and point doubling used for encryption application based on prime field Fp. Finally the proposed work is based on elliptic curve group operations solved in extension field Fp.The objective of this paper is to explain importance of extension field in the arithmetic of ECC so that it will enhance the security of the communication system with computations of ECC over extension fields and proposed algorithm.

This paper introduced the Elliptic curve cryptography which is used to develop a variety of scheme for security purpose in 2016. It also briefs about Point addition and point doubling arithmetic used in elliptic curve is applicable for prime field. When same arithmetic performs over extension field it increases the complexity of the application but enhances the security in the field of communication technology.

[2] In this, Author compares the performance of an ECC with other cryptosystems also the homomorphism of different algorithms like RSA, Paillier etc. In this ECC is followed by an additively homomorphism one and ends with fully homomorphism system.

[3] In this paper, authors have empirically analyze various ECC based homomorphism encryption schemes based on performance metrics such as computational cost and communication cost. They recommend an efficient algorithm amongst several selected ones that offers security with lesser overheads and can be applied in any application demanding privacy. It focuses on Elliptic Curve Cryptography based approach for Secure Multiparty Computation (SMC) problem.

For preserving privacy of data owned by parties, a best approach to SMC is to perform computation using Trusted Third Party (TTP). They proposes Elliptic Curve Cryptography (ECC) based approach for SMC that is scalable in terms of computational and communication cost and avoids TTP.

[4] in this paper, Author states that an ECC is more efficient than the ubiquitous RSA based schemes because ECC utilizes smaller key sizes for equivalent security. A comparative study of ECC with RSA is made in terms of key size, computational power, size of data files and encrypted files. Also, the author defines another aim of presenting this approach is to design on APl to implement ECC encryption /decryption algorithm.

It represents this research to develop a basis for utilizing efficient encryption schemes in wireless communications and in devices with low computing power and resources. Elliptic Curve Cryptography (ECC) fits well for an efficient and secure encryption scheme. Compared to currently prevalent cryptosystems such as RSA, ECC offers equivalent security with smaller key sizes. With the help of table which gives approximate comparable key sizes for symmetric- and asymmetric-key cryptosystems based on the best-known algorithms for attacking them.

Symmetric	ECC	DH/DSA/RSA
80	163	1024
112	233	2048
128	283	3072
192	409	7680
256	571	15360

Table 1: Comparable Key Sizes (in bits)[2]

Author [5] in 2016, investigated how to ensure the data security and the privacy preserving. The traditional way to solve Secure Multiparty Computation (SMC) problem is using Trusted Third Party (TTP), however, TTPs are particularly hard to achieve and compute complexity. To protect user's privacy data, the encrypted outsourcing data are generally stored and processed in cloud computing by applying homomorphism encryption.

According to above situation, we propose Elliptic Curve Cryptography (ECC) based homomorphic encryption scheme for SMC problem that is dramatically reduced computation and communication cost. It shows that the scheme has advantages in energy consumption, communication consumption and privacy protection through the comparison experiment between ECC based homomorphic encryption and RSA & Paillier encryption algorithm. Specifically states working of ECC with different dataset.

Also in this paper homomorphism can be compatible with variants of ECC has been cross checked. In this paper author have addressed implementation of ECC in cloud computing for providing better security which is one of the required aspect of cryptography.

3. SYSTEM WORK

- Elliptic Curve Cryptography:

Public key cryptography systems are constructed by relying on the hardness of mathematical problems

- RSA: based on the integer factorization problem
- DH: based on the discrete logarithm problem

It is theoretically possible to break such a system but practically it is not possible without known scheme which can be public key cryptosystems. The main problem of conventional public key cryptography systems is that the key size has to be sufficient large in order to meet the high-level security requirement.

This results in lower speed and consumption of more bandwidth and hence we need an approach which will result into better level of security with less computations, ultimately which will give us less bandwidth and power consumption hence solution is Elliptic Curve Cryptography system.

Elliptic curve can be utilized in cryptography as it is more secure to the best of recent knowledge. Their popularity has led to various implementations in terms of algorithms, curves, coordinate systems, platforms, faster calculations, shortest processing time, lower power and memory consumption. etc. [1] Level of security obtained by Elliptic Curve Cryptography (ECC) is same as RSA with smaller key size.

The advantages offered by ECC that it works in less storage area and smaller bandwidth. It also provides a solution to better performance of encryption and decryption with short keys size with a high security level. Encryption and decryption of data, digital signature algorithm (DSA) and key distribution implemented using elliptic curve cryptography [3][4].

NIST have recommended ECC for encryption as well as decryption based on the generation of keys:

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

3.1.1 Elliptic Curves over Real Fields[3]

An elliptic curve E over R (real numbers) is defined by a Weierstrass equation as $Y2=x3+ax+b$

3.1.2 Elliptic Curve over Finite Fields

- Elliptic curves needs fast and accurate arithmetic.
- Elliptic curve cryptography most commonly deals with functioning with two finite fields.

Over Prime Field Fp Where p is prime field

Over Binary Field $F2^m$ Where m is any positive no.

3.1 Point Addition on EC[3]

Over prime field = 5

E will be given by y2 (mod p) = x3 + ax + b(mod P)

Hence the value of E will be y2 = x3 + 4x + 4(mod 5)

Solving y as a prime field and calculating roots for x we will get points on the curve as (0,2),(0,3),(1,2),(1,3),(2,0),(4,2),(4,3) where x=0,1,2,3,4

If we consider any two points to add on the curve the slope can be given by previous equation [5]

Let's take P= (1, 2) & Q = (4,2)

So the m =0(mod5) & (x_3, - y_3)= (0, 3)

3.2 Point doubling on EC

When 2P=P+P,

Third point on the curve can be given as calculating slope which comes = 3 & (x_3,- y_3)=(2,0).Hence we can have basic formation of ECC w.r.t Weierstrass equation as,

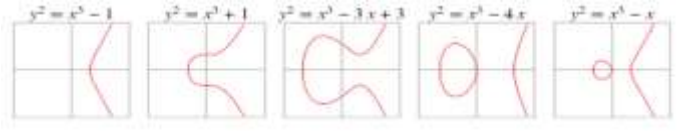

Fig 3.2

Elliptic curve cryptosystem (ECC) has the same security level with about 7-fold smaller length key as compared to RSA cryptosystem, it is said that ECC is more practical as compared to RSA. [1][3].

Comparison of performance of ECC with existing public key cryptography in key generation is discussed in table 1[2].

If we consider various ECC based encryption schemes, variation in time and cost will be shown as:

Table 2: Time variation

ENCRYPTION		EC-NS	EC-P	EC-EG
KEY SIZE(bits)				
112	TIME (ms)	303	247	254
160	TIME (ms)	349	285	286
256	TIME (ms)	402	351	322

Table 3: Cost variation

ENCRYPTION		EC-NS	EC-P	EC-EG
KEY SIZE(bits)				
112	COST(kb)	4224	2437	1740
160	COST(kb)	4906	3741	2766
256	COST(kb)	7487	7125	4865

4. CONCLUSION

Cryptography have become necessary due to increased usage of internet. With increased usage of networks, the vulnerabilities have also increased into the network system. Hence using only encryption techniques are not enough. To provide better security we need even more secure and less power consuming encryption scheme. It helps to provide better security when data is centrally located. Here we focused on the Elliptic Curve Cryptography study, which may be a mainly used in various tools. Finally, we say, Variant of ECC will be helpful to maintain data integrity.

5. FUTURE SCOPE

Here, WE referred previous study of the existing cryptography schemes: RSA, Elgamal, and Paillier. Since they have been designed to serve better security. WE have focused on the features, advantages, disadvantages and performance. We have also tried elaborate the comparison study of Elliptic Curve NaccacheStern (EC-NS) Encryption, Elliptic Curve Paillier (EC-P) Encryption, Elliptic Curve Elgamal (EC-EG) Encryption with respect to their features, key sizes and encryption-decryption standards, etc. RSA, Paillier and NaccacheStern have different features and they behave distinct with different inputs [4]. It helps to develop new ways of looking towards data security. On the other hand Elgamal performs better compared to both. If Elgamal is simulated with ECC it will provide even more security with lesser computational loss [5]. Considering these few significant differences it is quite clear that, Elliptic Curve Elgamal (EC-EG) Encryption scheme can provide better security with its distinct features. Future work can comprise the same.

REFERENCES

[1] Santoshi Poteet al, "Elliptic Curve Arithmetic over Extension Field to Intensify Security and Privacy" in IEEE Wisp NET 2016 conf. 978-1-4673-9338-6/16.

[2] Sigrun Goluch "The development of holomorphic cryptography" thesis presented to the Institute of Discrete Mathematics and Geometry Vienna University of Technology.

[3] Sankita J. Patel et al "Comparative Evaluation of Elliptic Curve Cryptography Based Homomorphic Encryption

Schemes for a Novel Secure Multiparty Computation" Published in Journal of Information Security, January 2014, 5, 12-18.

[4] G.V.S. Raju and Rehan & bani" Elliptic Curve Cryptosystem and its Applications" published in 0-7803-7952-7/03/@ 2003 IEEE.

[5]Ming-quan Hong, Wen-bo Zhao et al "Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing" published in 2016 IEEE 2nd International Conference on Big Data Security on Cloud, High Performance and Smart Computing, Intelligent Data and Security.

[6] https://bitcoin.org/en/

[7]http://security.stackexchange.com/questions/78621/which-elliptic-curve-should-i-use