I J C T A, 9(34) 2016, pp. 503-514

Design of an Optimized Novel Cryptographic Algorithm and Comparative Analysis with the Existing Cryptographic Algorithms

Shailendra Singh Gaur[1], A. K. Mohapatra[2] and Sarfaraz Masood[3]

ABSTRACT

In this paper, threshold cryptographic techniques has been analyzed and studied. Threshold based ECC algorithm has been implemented using GMP tool and their performance have been evaluated. The result shows that it is an effective technique to encrypt the data required in networking, when the given shares of each shareholder are up to 1024 input bits. In threshold cryptography we not only rely on one person but on several people for the decryption of our message.

Keywords: RSA, ECC, Threshold cryptography, GMP tool.

1. INTRODUCTION

Threshold cryptography is used to protect the information by using the distributed key among the several servers and not by giving it to a single server [1]. It is proved to be an effective technique for key distribution and decryption.

The cipher text is provided by the key value entered for encryption along with the text . Then the given cipher text is to be transmitted. When the recipient received the cipher text, it is decrypted to recover the plain text which cannot be decoded by the eavesdropper, as the key is not known to him. [2]. In this paper, we discuss various techniques to implement threshold cryptography effectively in real life scenarios.

2. METHOD

Shamir [11] discussed about the secret key, for signing the documents digitally for a single entity and explained threshold scheme problem as:

The data (D) is divided into (Di), so that the number of Di helps to compute D easily and k-1 helps to determine D easily.

The concept given by Shamir is used in Threshold Cryptography and act as a building blocks. Different problems occurred during the signature generation are:

1. The issue of leaked master key and
2. Modified data after being signed and

2.1. Introduction to Elliptic Curve Cryptography

Neal Koblitz and Victor Miller proposed an Elliptic Curve Systems, which was first implemented in 1985.

[1] Assistant Professor, BPIT, G. G. S. I. P. U., Delhi
[2] Associate Professor, Dr. A. K. Mohapatra, IGDTU, Delhi
[3] Assistant Professor, Jamia Millia Islamia, Delhi

- ECC is totally based on N.P. hard Problems that defines the complexity of discrete algorithm.
- It is used in embedded devices where processing and space capacity is less with power consumption.
- Elliptic Curve Cryptography is widely in new trends of E-Commerce and Network Security.
- In a given curve, Elliptic Curve Cryptography takes two points and combined them to get the final curve [3]

Using an equation with two variables , we can define an elliptic curve cryptography known as “finite field” where set is defined by the variables and coefficients [3] defined as:

$$y2 + (a)xy + by = x3 + (c)x2 + (d)x + e \quad (1)$$

where the real number values are given by a,b,c,d and e along with the x and y values, that are dependent on real numbers. The equation of ECC is also defined as:

$$y2 – x8 + (d)x + e \quad (2)$$

In ECC, the EC defines the number of the set where the group is calculated that means when we perform. an operation of two elements in a given set will provide the same set and operations of two elements.

High level of security is provided by ECC in terms of bit or key value. It is explained in terms of public key, performance, high efficiency, minimum consumption of power and hardware requirements [4]. It uses mathematical and algebraic calculation of curves using finite fields [5]. Here, a finite field is defined in terms of variables and functions.

One of the application of ECC is that , it is used in Wireless Sensor Networks using various Public Key Cryptographic algorithm that helps in execution using minimum number of key size and its signatures or signing document is comparable to RSA. As we know that an ECC needs 160 bit keys as compared to 1024 bit keys of RSA for same level of security. [9]

2.2. Introduction to Threshold Cryptography

Sharing of a key in a Threshold Cryptography by the number of users engaged in encryption or decryption of a message or to share the message either before or after encryption[13]. It avoids trusting and engaging only one node for transmitting of message. Hence, the primary objective is to share this authority in a way such that each individual node performs a calculation on the message without knowing the secret key.

Threshold cryptography provides distributed architecture in a cryptographic environment For encryption or decryption of a message, nodes called threshold t is used. Suppose, there will be the n number of partie then it is known as threshold cryptography based system defined by (t,n), if the value of ‘t’ of the given share can perform the decryption of the cipher text and the signature is created using least t number of shares. Therefore, the threshold schemes includes the generation of key, to encrypt the data, generation of shares and verification, and finally combining all these parameters to get the data secured. Hence, Threshold Cryptography till compromising nodes are less than t since it is difficult to decode partial messages if the number is less than the threshold.

Threshold cryptography provides confidentiality, integrity of data against malicious nodes that also provides verified data sharing. In Threshold cryptography, all these can be achieved without revealing the concerned secret key. [10]

2.3. Shamir’s Scheme based on Secret Sharing

In this method, n parties are messages, or involved to carry shares, say s(i) of the given we can say secret messages, so that the set s1, s2 to sn, the number of parts can easily determine the concerned message.[15]

It is an efficient secret sharing method if no relevant information is given by subset or parts of given shares that provides the secret key.

2.3.1 Using two party secret sharing scheme: Suppose the given secret s, encoding in the integer form of Z/mZ. Also assuming that s1and s2 of the form Z/mZ generated randomly by a party. Then, the two namely s1 and s-s1 shares are defined, separately. Finally, the secret share is recovered i.e. s = s1 + s2.

2.3.2 Using multiple party secret sharing scheme: Suppose secret *s* is using *n* number of parties then generate *n* – 1 shares i.e. *s*1, *s2* upto *sn* – 1 randomly and set

$$s_n = s - \Sigma_{i-1}^{n-1}. \tag{3}$$

Finally, the secret is obtained as

$$s = \Sigma_{i=1}^{n} s_i \tag{4}$$

In this method using n members to carry shares i.e. s(i) of the given message *s*, using any value of *t* to reconstruct the message again, but t – 1 cannot be done easily. It is secured and accurate method if, the value of secret *s* cannot be revealed.

2.3.3 Introduction to Shamir's threshold scheme: Shamir provide a (t, n) threshold method called Lagrange interpolation also known as classical algorithm. Here, Lagrange interpolation theorem is discussed. Lagrange Interpolation defines t distinct points say (xi, yi) of the given form in terms of (xi, f(xi)), where f(x) is defined by a degree of polynomial less than the value of t, then function f(x) is explained by:

$$f(x) = \Sigma_{i=1}^{t} \Pi_{I \le j \le t} \frac{x - x_j}{x_i - x_j} \tag{5}$$

In Shamir Secret Sharing scheme, we put the value a0 = M (message) and a1……..at-1 and coefficients are assigned randomly for this polynomial. We get

$$f(x) = \Sigma_{k=0}^{t-1} a_k x^k \tag{6}$$

But to generate the shares we put numbers of different values of x. As a resultant, we get n number of f(x) values and that are our shares by computing f(i) , where 1< i <n . The given shares i and f(i)) are shared among different members of the group. Now to recover the message ,explained by equation (7), our constant term a(0) holds our message .We can easily get our message back from t number of shares (i, f(i)) by putting i = 0, that is

$$f(0) = a0 = M$$

$$\Sigma_{i \in I} c_i f(i), \; where\, each\, c_i = \Pi_{\substack{j \in I \\ j \neq i}} \frac{i}{j - i} \tag{7}$$

3. ALGORITHMS USED

3.1. ECC algorithm

The elliptic curve equation is defined as:

$$y^2 = x^3 + (a)x + b \tag{8}$$

The different values of (a and b) defines the equation of elliptic curve. Using the (x and y) points that satisfied the equation for the (a and b) value at infinity point. The point is defined by public key on the curve and the random number is generated by private key. The multiplication of 'P' generator point with private key generates the public key. [6]

3.1.1. At the Sender End

1. Point P is taken from the elliptic curve equation .
2. The private key ‘d’ or a number is selected randomly .
3. With the given value of private key and P, The sender will generate the public key (Q = d*P).
4. Curve ‘E’ has the point ‘M’ to send the message.
5. Select ‘k’ randomly from the value [1 to (n-1)].
6. The strings (C1 and C2) are generated known as cipher text.
7. Finally, C1 and C2 are generates the encrypted message.

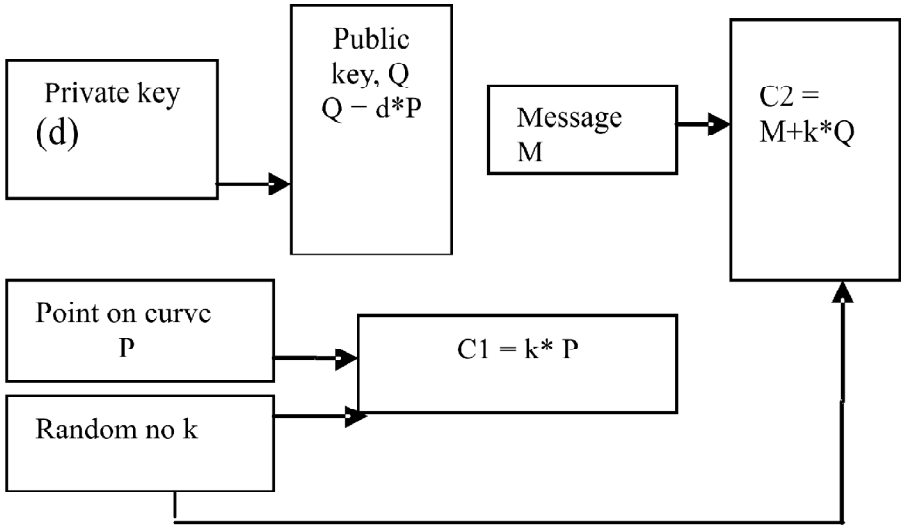

Figure 1: Encryption at sender end

3.1.2. At the Receiver End

1. Cipher texts C1 and C2 used by the receiver for decryption of M .
2. For decryption of message M, private key is used decrypt M.
3. The private key ‘d’ is used by the receiver where M = [C2 –(d*C1)].
4. Hence, original message ‘M’ is received.

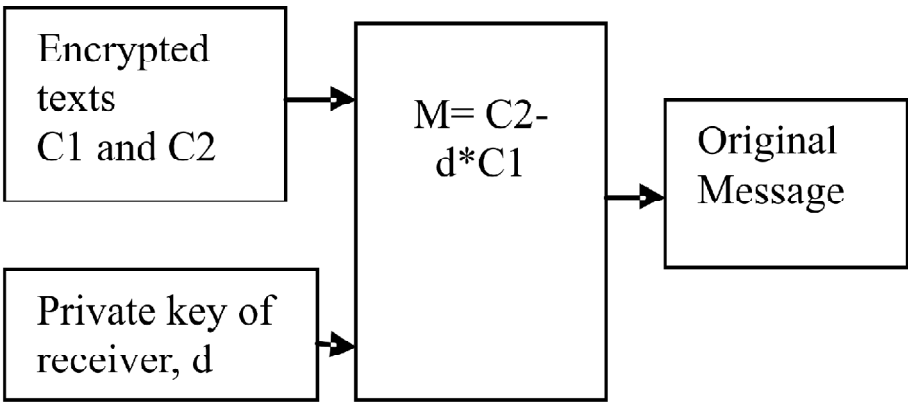

Figure 2: Decryption at the receiver site

3.2. Threshold Cryptography Algorithm

3.2.1 For Generating Shares

1. Sender enters the message M.
2. Sender also enters the number of shares (say n) he wants to generate and the minimum number (threshold number say t) of shares he want to use to recover the message back.
3. Using Lagrange interpolation algorithm, we compute a lagrange polynomial (that is f(x)) whose constant term is our message M that is a_0 = M. Other constant terms (a_1, a_2 , ….. , a_{t-1}) are randomly set. The degree of this polynomial is one less than the threshold number that is t-1.
4. Now we generate shares by substituting x with the values 1 to n.
5. Now we have our n number of shares in the form (i , f(i)) where $1 \leq i \leq n$
6. We send these shares to n different number of people.

3.2.2. For Recovering the Message

1. In order to recover the message M , we at least need threshold number of shares.
2. We combine these shares using a formula and as the constant term of our lagrange polynomial was our message M, we substitute x with 0 as f(0) = M.
3. Finally, we get our message back.

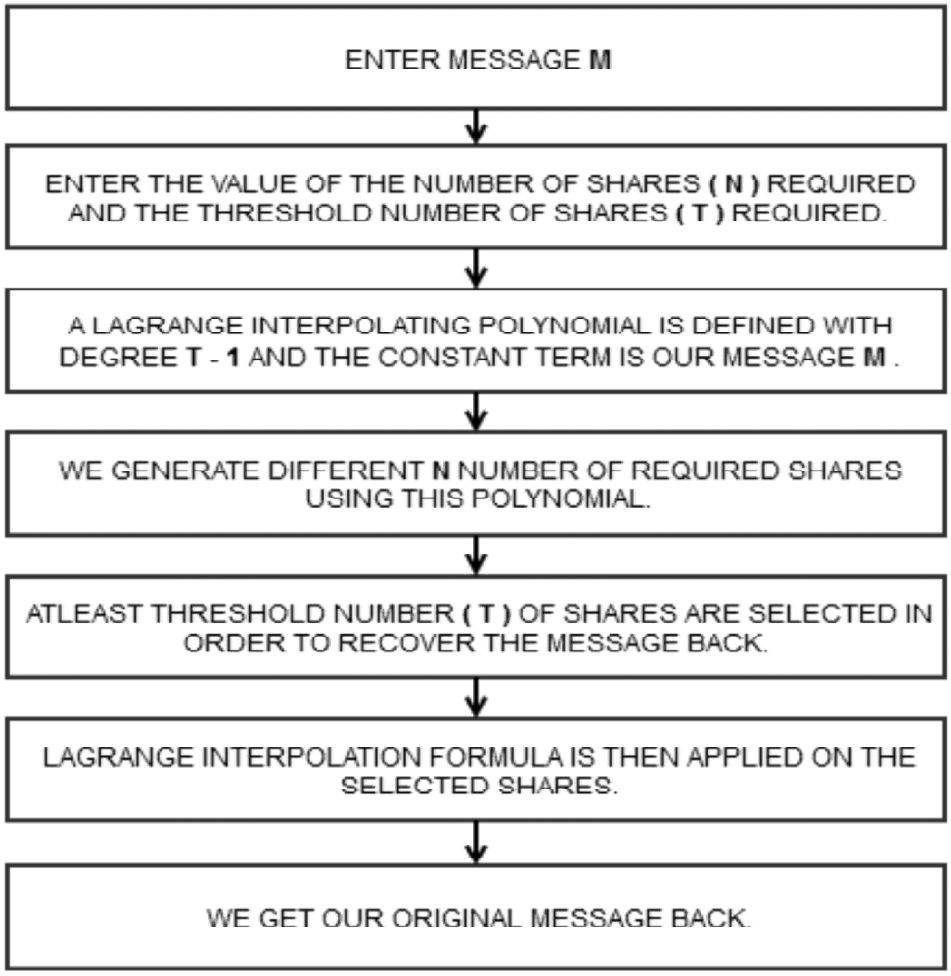

Figure 3: Threshold cryptography algorithm

3.3. Proposed Cryptographic Algorithm (Threshold Cryptography Based ECC Algorithm):

3.3.1. At the Sender's End

1. Point P is taken from the elliptic curve equation
2. The private key 'd' is generated by the sender randomly.
3. Now the sender enters the message M.
4. This message is then processed by the threshold cryptographic algorithm in order to generate the shares, as explained by equation number (7).
5. Now sender enters the number of shares (say n) he wants to generate and the minimum number (threshold number say t) of shares he want to use to recover the message back.
6. Using Lagrange interpolation algorithm, we compute a lagrange polynomial (that is f(x)) whose constant term is our message M that is a_0 = M. Other constant terms (a_1, a_2 , ….. , a_{t-1}) are randomly set. The degree of this polynomial is one less than the threshold number that is t-1, as explained by equation number (6).
7. Now we generate shares by substituting x with the values 1 to n.
8. Now we have our n number of shares in the form (i, f(i)) where $1 \leq i \leq n$.
9. Now we encrypt theses individual shares using the Elliptic curve cryptography algorithm.
10. For each share we generate two cipher texts C1 and C2 with the help of another random number (that is K).
11. C1 is generated as : C1 = K.P

    C2 is generated as : C2 = M + K.Q
12. As we can see in the above steps , we are multiplying a scalar K with co-ordinate points (X,Y). This is not a normal multiplication. This process involves point multiplication and point addition algorithms. An algorithm called point doubling is also used.
13. Now these cipher texts are transmitted to n number of people.
14.

3.3.2. For recovering message back

1. Now n people receive encrypted shares.
2. These encrypted shares are then decrypted using ECC decryption algorithm.
3. For each share we have two cipher texts C1 and C2.
4. Each person decrypts the share using the private key that is *d* by a Share = C2 – d.C1
5. In this way all the shares can be decrypted.
6. Now in order to recover the original message M , we at least need threshold number of shares.
7. We combine these shares using a formula and as the constant term of our lagrange polynomial was our message M, we substitute x with 0 as f(0) = M, as explained by equation number (7).
8. Finally, we get our message back.

4. RESULT

4.1. Elliptic Curve Cryptography

This algorithm has been implemented by using these codes. Different length of 1 bit, 2 bit and upto 10 bit of messages are given as an input to ECC. Then, a random number is generated. Sender has a The private

Figure 4: Threshold cryptography based ECC algorithm

key used by the sender is only issued to the concerned person at the receiving side. The carrier will receive the two cipher text and issued public key, that means we are getting a encrypted message. After receiving the cipher text, message is decrypted using private key to get the original message.

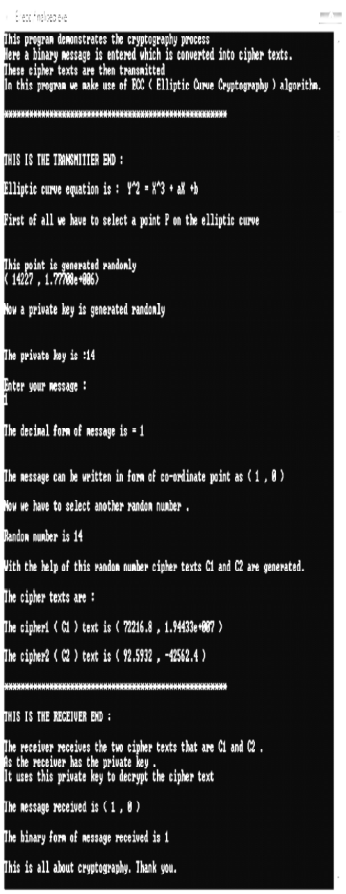

Figure 5 : Output of 1bit number

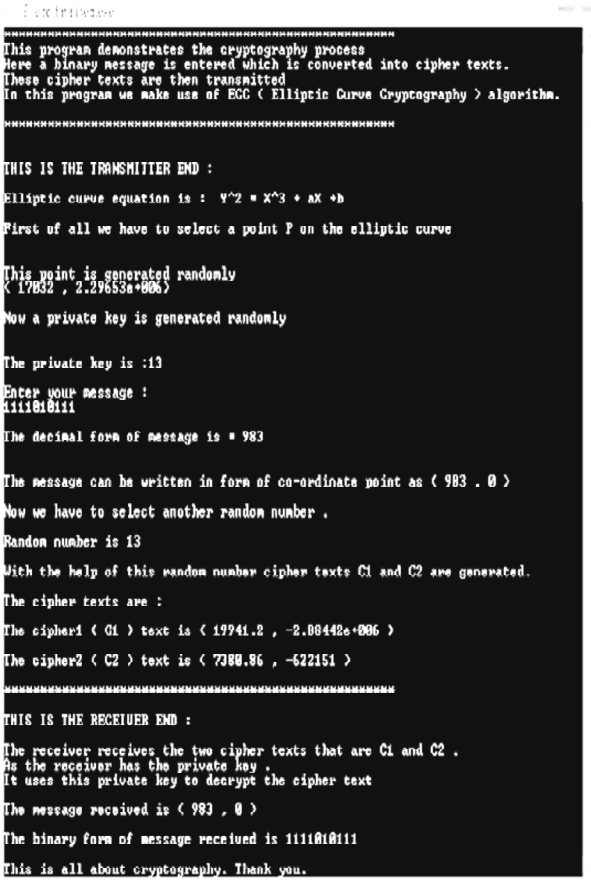

Figure 6 : Output of 10 bit number

4.1.1. Analysed Output

Output at the sender's side

POINT ON CURVE (P)	PRIVATE KEY (d)	ORIGINAL MESSGAE (M)	RANDOM NO (k)	CIPHER TEXT (C1)	CIPHER TEXT (C2)
(14368,1.80201e+006)	17	0	23	(5380.57,-510939)	(98.5765,-44140.4)
(14227,1.77708e+006)	14	1	14	(72216.8,1.944e+007)	(92.5932,-42562.4)
(14505,1.82636e+006)	16	10	6	(9469.52,1.017e+006)	(5259.61,498212)
(14622,1.84725e+006)	18	11	2	(2763.97,274246)	(63.851,-34778.6)
(14276,1.87487e+006)	11	101	21	(48105.6,-1.06e+007)	(2477.67,252020)
(14959,1.9079e+006)	10	111	13	(147.409,53907.5)	(398.062,87918.4)
(15089,1.93149e+006)	2	1011	9	(89.7893,42145.3)	(53840.4, -1.25311e+007)
(15194,1.95062e+006)	15	1111	10	(23138.5, -3.58342e+006)	(13243.4, -1.60426e+006)
(15605,2.02618e+006)	12	11011	22	(3720.01,-352533)	(117076, -4.00739e+007)
(15716,2.04676e+006)	8	11101	21	(3.17266,-8992.35)	(18309.4, 2.54292e+0006)
(15850,2.07171e+006)	4	101010	1	(15850,2.07171e+006)	(302.217,-71606.6)
(16017,2.10296e+006)	10	110011	23	(6854.3,675386)	(2195.48,-227677)
(16147,2.12741e+006)	2	1101011	9	(854.854,131790)	(5210.94,-482529)
(16432,2.18136e+006)	11	11001100	10	(179.994,59549.7)	(2810.77,-261485)
(16670,2.22679e+006)	19	111100001	16	(2154.07,228380)	(350456, 2.07057e+008)
(16918,2.27448e+006)	14	1010101011	14	(59.1795,-34305)	(531019, 3.86226e+008)

Figure 7 : Output at sender's side

Output at the receiver's side

CIPHER TEXT (C1)	CIPHER TEXT (C2)	PRIVATE KEY (d)	MESSAGE RECEIVED
(5380.57,-510939)	(98.5765,-44140.4)	17	0
(72216.8,1.944e+007)	(92.5932,-42562.4)	14	1
(9469.52,1.017e+006)	(5259.61,498212)	16	10
(2763.97,274246)	(63.851,-34778.6)	18	11
(48105.6,-1.06e+007)	(2477.67,252020)	11	101
(147.409,53907.5)	(398.062,87918.4)	10	111
(89.7893,42145.3)	(53840.4,-1.25311e+007)	2	1011
(23138.5,-3.58342e+006)	(13243.4,-1.60426e+006)	15	1111
(3720.01,-352533)	(117076,-4.00739e+007)	12	11011
(3.17266,-8992.35)	(18309.4,2.54292e+0006)	8	11101
(15850,2.07171e+006)	(302.217,-71606.6)	4	101010
(6854.3,675386)	(2195.48,-227677)	10	110011
(854.854,131790)	(5210.94,-482529)	2	1101011
(179.994,59549.7)	(2810.77,-261485)	11	11001100
(2154.07,228380)	(350456,2.07057e+008)	19	111100001
(59.1795,-34305)	(531019,3.86226e+008)	14	1010101011

Figure 8: Output at receiver's side

Here, the results shows that the Encrypted and Decrypted messages are same.

4.2. Threshold Cryptography

For[12] threshold cryptography algorithm we have used SHAMIR SECRET SHARING SCHEME. We have implemented it in C language using GMP library.

4.3. Threshold Cryptography Based ECC Algorithm

We have combined threshold cryptography and elliptic curve cryptography concepts and designed an algorithm using GMP library.

Figure 9: Threshold cryptography

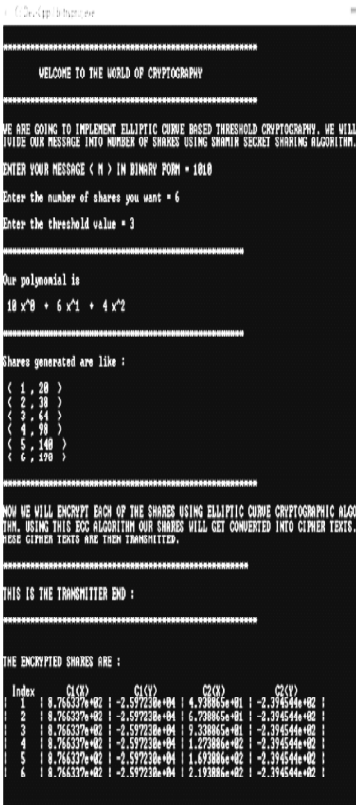

Figure 10: Threshold based ECC

Figure 11: Threshold based ECC

5. ANALYSIS

5.1. Comparison of Threshold cryptographic algorithm and proposed algorithm

1) Threshold Cryptography based ECC algorithm provides double level of authentication as compared to Threshold Cryptographic based ECC algorithm.
2) Encryption in Threshold Cryptography based ECC algorithm is done by number of shares and cipher texts.
3) In Decryption , shares are decrypted using Lagrange interpolation of ECC as compared to private key of ECC algorithm.

Table 1
Comparison of various cryptographic algorithm

Parameters	*ECC Algorithm*	*Threshold Cryptography Algorithm*	*Proposed Novel Algorithm*
Level of Authentication	Single	Single	Double
Encryption method	Cipher texts C1 & C2 are generated	Generated N number of required shares.	Generated N number of required shares and encrypted using ECC.
Decryption method	Private key of receiver used	Threshold (T) of shares are selected	Shares are decrypted using ECC i.e. Lagrange Interpolation

5.2. Comparison of Threshold cryptographic algorithm and proposed algorithm:

Table 2
Comparison of algorithms on various parameters

Parameters	*Threshold Cryptography Algorithm*	*Proposed Novel Algorithm*
Splitting of Shares	Lagrange Interpolation	Shamir Secret Sharing Algorithm
Message Encryption	Shares Generated	Shares and Cipher texts Generated
Message Decryption	Lagrange Interpolation	Lagrange Interpolation

5.3. Comparison on the basis of shares generated and index of shares

Input Parameters

1) Secret Message : 1010
2) Number of shares: 6
3) Threshold value : 3

Table 3
Comparison of algorithms based on number of shares and threshold values

Number of Shares	*Threshold Cryptography Algorithm*		*Proposed Novel Algorithm*	
	Shares Generated	*Index of Share (4)*	*Shares Generated*	*Index of Share (4)*
1	1027	1027	20	20
2	1064	1064	38	38
3	1121	Nil	64	Nil
4	1198	1198	98	98
5	1295	1295	140	140
6	1412	Nil	190	Nil

1) Proposed algorithm provides double level of encryption as compared to threshold cryptography algorithm.
2) Reduced length of shares generated in the proposed algorithm as compared to shares generated in Threshold cryptography algorithm.
3) Minimum execution time is required to generate the output in the proposed algorithm .

It took 9 seconds for the algorithm to generate this output. We have plot two graphs. One for the shares generated for the input 1010 and one graph illustrating the encrypted shares which are encrypted using ECC algorithm.

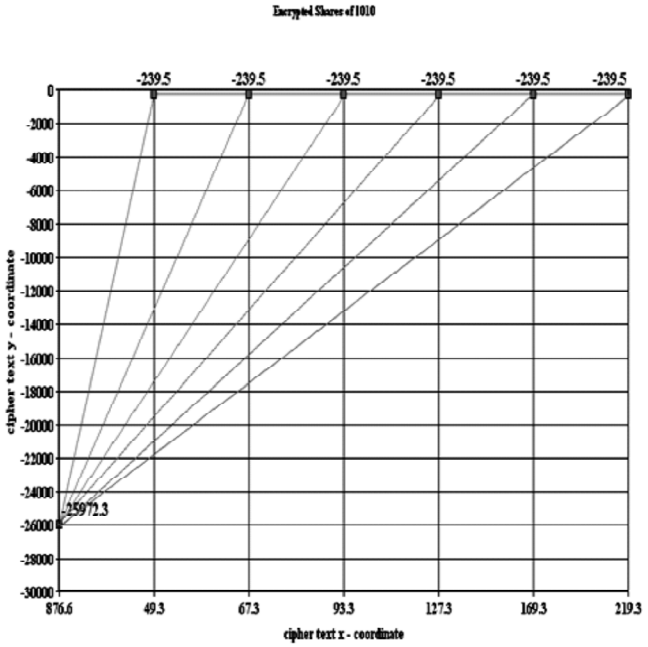

Figure 12: Encrypted shares for 1010

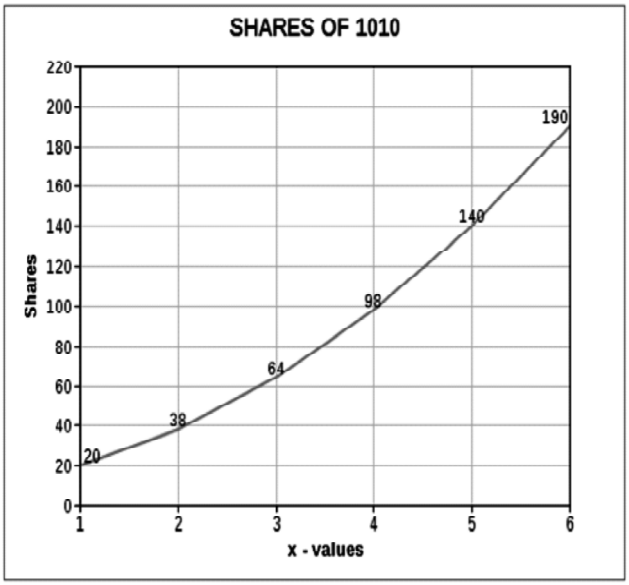

Figure 13: Generated shares for 1010

For each share we have two cipher texts. Therefore for each point in the graph Fig. 15 we have two points in the graph Fig. 16.

Here, same key is used for encrypting all the generated shares, so the cipher texts generated will vary very little from each other but still nobody can get the original message back without using the key. If different keys would have used for encrypting each individual share then the cipher text generated must have varied too much from each other.

6. CONCLUSIONS

Elliptic Curve Cryptography along with digital signature covers various security aspects -like Message Integrity, Authentication and non-repudiation of a message and provide confidentiality .

Elliptic Curve Cryptography provides secured transmission and services like mobile communication, wireless sensor networks using cryptographic techniques and encryption techniques etc. A lot of research is required in the field of communication and its security. [16]

Threshold cryptography enhances security by dividing the secret key into several bits. It is a very effective technique for encrypting data, in which the shares of each shareholder are refreshed periodically. It maintains the security by interchanging the shares among its shareholders to prevent unauthorized access.

7. FUTURE WORK

As a part of future work, we can interface the Threshold Cryptographic techniques with the Clustering techniques to make the Wireless Sensor Networks, more secured. Secondly, the concept of Cloud Computing with ECC can be introduced. The biometric values can be introduced and then encrypt them using our Elliptic Curve Cryptography based Threshold Cryptography. With the growth of Wireless Sensor Networks in coming years, it is required to consider the security aspects of services like mobile communication and its secured transmission. Using data aggregation in secured WSN, the proposed algorithm can reduce the power consumption and key size.

REFERENCES

[1] M. Bellare, S. Meiklejohn and S. Thomson, (2014), Advances in Cryptology - Eurocrypt 2014 Proceedings, Lecture Notes in Computer Science Vol., P. Nguyen and E. Oswald eds, Springer.

[2] K. Tamil Selvi and Prof. S.Kuppuswami, (2014), Enhancing Security in Optimized Link State Routing Protocol for MANET using Threshold Cryptography Technique, IEEE: Kongu Engineering College, Erode, India.

[3] Haimabati Dey and Raja Datta, (2012), Monitoring Threshold Cryptography based Wireless Sensor Networks with Projective Plane, IEEE: Indian Institute of Technology , Kharagpur, India.

[4] Wang Wei-hong , Lin Yu-bing and Chen Tie-ming. (2008), The Study and Application of Elliptic Curve Cryptography Library on Wireless Sensor Network, 11th IEEE International Conference on Communication Technology Proceedings.

[5] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, (2004), Guide to Elliptic Curve Cryptography: Springer.

[6] A. Athavale, K. Singh, and S. Sood., (2009), "Design of a Private Credentials Scheme Based on Elliptic Curve Cryptography", First International Conference on Computational Intelligence, Communication Systems and Networks, page 332-33.

[7] G. Agnew, R. Mullin, and S. Vanstone, (1991) , On the development of a fast elliptic curve processor chip, Advances in Cryptology CRYPTO'91, pp. 482-487, New York, Springer-Verlag.

[8] D. V. Chudnovsky and G. V. Chudnovsky, (1986) , Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Advances in Applied Mathematics vol. 7, no. 4, pp. 385-434.

[9] Amr I. Hamed and Said E. El-Khamy , (2009), "New Low Complexity Key Exchange and Encryption protocols for Wireless Sensor Networks Clusters based on Elliptic Curve Cryptography". Alexandria University, Egypt.

[10] Levent and Weimin lu, (2005), ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET, Springer-Verleg, Pages 102-113.

[11] A. Shamir.(1979) How to share a secret. Commun. ACM, 22, pp. 612-613.

[12] R. A. Croft and S. P. Harris. (1986) Public-key cryptography and reusable shared secrets. Cryptography and coding, pp. 189-201.Royal Agricultural College, Cirencester.

[13] Y. Desmedt. (1988), Society and group oriented cryptography : a new concept. pp. 120-127. Springer-Verlag,. Santa Barbara, California, U.S.A.

[14] P. Feldman. (1987) , A practical scheme for non-interactive variable secret sharing. In 28th Annual Symposium on Foundations of Computer Science, pages 427{437. IEEE Computer Society.

[15] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, (1985), Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults, FOCS85, pp. 383-395.

[16] M. Durairaj and A. Persia (2014), An Efficacious Algorithm to Thwart MAC Spoof DoS Attack in Wireless Local Area Infrastructure Network, Indian Journal of Science and Technology, Volume 7, Issue 5.

[17] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma and Sundaram Vats, (2015), Threshold Cryptography Based Data Security in Cloud Computing, IEEE International Conference on Computational Intelligence & Communication Technology, India.