IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735. Volume 7, Issue 3 (Sep. - Oct. 2013), PP 56-60
www.iosrjournals.org

"Proposed Model for Network Security Issues Using Elliptical Curve Cryptography"

[1]Garima Kaushik, [2]Mr. Shailendra Gaur
[1]Btech (CSE 4th year), Bhagwan Parshuram Institute of Technology, GGSIPU, India
[2]Assisstant Professor, Bhagwan Parshuram Institute of Technology, GGSIPU, India

***Abstract**: Elliptic Curve Cryptography (ECC) plays an important role in today's public key based security systems. . ECC is a faster and more secure method of encryption as compared to other Public Key Cryptographic algorithms. This paper focuses on the performance advantages of using ECC in the wireless network. So in this paper its algorithm has been implemented and analyzed for various bit length inputs. The Private key is known only to sender and receiver and hence data transmission is secure.*

I. Introduction

The electronic revolution in our daily life has created an environment where information is available to the masses; let it be our address, phone number, our social security number or personal conversation on a website. In this age of information overload there are some elements that can use this information against you. So, we need to convert our data in a form that cannot be read or understood by anyone. This is the idea of encryption.

Every alphabet or character that we type is represented by a binary number. The Encryption process focuses on mixing up these binary numbers after performing mathematical operations which converts the binary number in a newer arrangement which is not understandable. This is done by a key.

Every encryption process uses a "key" for encryption. The key we use to encrypt a text is used again to decrypt it. Such encryption process is called symmetric encryption. There is one more process that uses two distinct keys, one to encrypt and a different one to decrypt. The mathematics of this was first purposed by Elliptical Curve Cryptography. [1]

The key is a parameter that is passed in the encryption function along with the text needed to be encrypted, which generates a cipher text. This cipher text can be transmitted over an unsecure net-work. When received by the intended recipient, it will decrypt the cipher text using a key, which is again passed into a decryption function to recover the plain text back. If any other eavesdropper intercepts the message over the network, he will not be able to decode it, as the key is not known to him. [2]

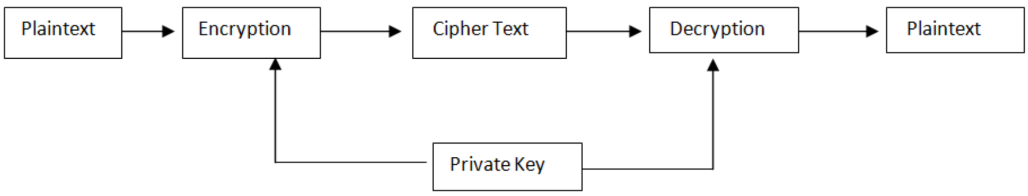

Figure 1.1 – Encryption/ Decryption Process

II. Elliptic Curve Cryptography (ECC)

A: Basics Of Elliptic Curve

- Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.
- Elliptic Curve Cryptography is based on the complexity of elliptic curve discrete algorithm which is also known as N.P hard Problem.
- ECC was basically designed to run on small, constrained devices especially embedded devices which has less storage space capacity, less processing capabilities , less power consumption.
- ECC can be widely used in information security and Ecommerce.
- ECC uses points on the elliptic curve to derive a 162 bits public key that is equivalent in strength to 1024 bits RSA key. Hence, main benefit of ECC is that by using smaller key it provide equivalent level of security as the conventional crypto systems.
- RSA has exponentiation which is raising the message or ciphertext to the public or private values whereas

ECC has point multiplication which has repeated addition of two points.

- The idea of Elliptic Curve has unique property which makes it suitable for use in cryptography. This uniqueness forms the ability to take any two points on a specific curve, add them together, and get a third point on the same curve. The confusion in cryptography is that which two points were added together to obtain the third point.

Basic Concepts -

The Elliptic Curve [3] has a very unique property which makes it suitable for use in cryptography. This uniqueness forms the ability to take any two points on a specific curve, add them together, and get a third point on the same curve.An elliptic curve is defined by an equation is two variables, with coefficient. For the purpose of cryptography, the variable and coefficient are limited to a special kind of set called a FINITE FIELD. The general equation for an elliptic curve is:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where a,b,c,d and e are real numbers and x and y also take their values from real number .A simplified version of the equation will be:

$$y^2 – x^8 + dx + e$$

In Elliptical Curve Cryptography, the Elliptic Curve is used to define the members of the set over which the group is calculated i.e. an operation on any two elements of the set will give a result that is the member of the same set as well as operations between them.

ECC is considered as the one which has the highest security quality in per bit key among current public key cryptosystems. It's characterized by small key, small system parameter, small public key, saving bandwidth, fast implementation, low power, and low hardware requirements. [4]

ECC is "an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields" [5].For the purpose of cryptography the variables and coefficients are limited to a special kind of set called a FINITE FIELD.

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP). Let P and Q be the two points on the curve such that kP = Q, where k is a scalar and is called elliptic curve discrete logarithm of Q to the base P. Given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large. [6]

The implementation of ECC mainly relies on the operations at three levels: the scalar multiplication, the pointaddition / doubling, and the finite field modulo arithmetic. The ECC system based on $GF(2n)$ is widely utilized for its simple field arithmetic and efficient scalar multiplication algorithms.

Two different coordinates: the affine coordinate and the projective coordinate can be used for the ECC where the curve is defined over $GF(2n)$. It was shown in [3][7][8] that the projective coordinate is more desirable for hardwareimplementation because it avoids the costly field inversion operation

In Wireless sensor Networks, Elliptic Curve Cryptography (ECC) was the natural choice between Various Public Key Cryptographic options due to its efficient execution and computation, small key size and signatures comparable to other PKC schemes such as RSA.

For example, an ECC protocol only needs 160 bit keys to provide equivalent security to 1024-bit RSA. In addition, the benefits of having small key size results significant advantages such as smaller ROM, smaller RAM, faster execution and more efficient storage. [9]

III. Algorithm / Methodology Used

The mathematical operations of ECC are defined over the elliptic curve equation

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

where 4a3 + 27b2 ≠ 0. Each value of 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfy the above equation for given (a, b) plus a point atinfinity. The public key is a point on the curve and the private key is a random number. The public key is obtained by multiplying the private key with a generator point P on the curve. [6]

<u>At the Sender End</u> –

Step 1 - The sender will take a point P on the elliptic curve equation given above.

Step 2 – A random number'd' is selected within the range of 1- (n-1). 'd' is the private key.

Step 3 – The sender will generate a public key Q by private key and point P.

$$Q = d*P$$

Step 4 – The message to be sent has point ‘M’ on curve E.
Step 5 – Randomly select ‘k’ from 1 to (n-1).
Step 6 – Generate two cipher text strings C1 and C2.

$$C1 = k * P$$
$$C2 = M + K * Q$$

Step 7 – Send C1 and C2. C1 and C2 are encrypted texts.

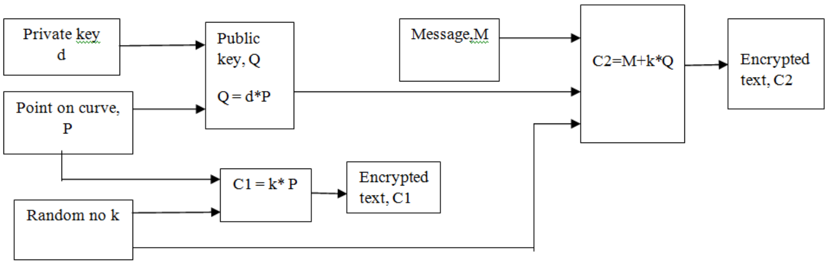

Figure 1.2 – Encryption at sender site

<u>At the Receiver End –</u>
Step 1 – The receiver uses the cipher texts C1 and C2 to decrypt the message M.
Step 2 – The receiver uses the private key to decrypt the message M.
Step 3 – The receiver has private key ‘d’.

$$M = C2 - d*C1$$

Step 4 – ‘M’ is the original message.

So, we get the original message back which we sent.

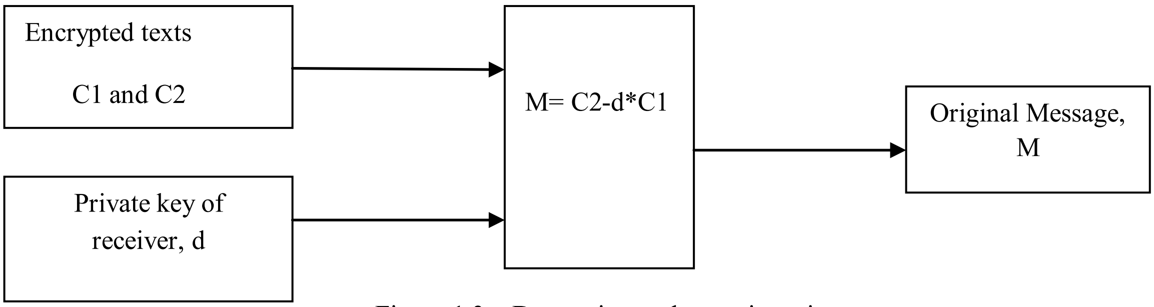

Figure 1.3 – Decryption at the receiver site

V. Output

The given Algorithm has been implemented by use of the above mentioned codes. It has been given inputs of various length bit words i.e. it can take messages of 1-bit, 2-bit,3-bit….10bits. It generates a random number which is taken as a point on curve. Sender has a private key which is known to only him and the receiver. The public keys as two cipher texts are generated and sent over the carrier. These are the encrypted texts. At the receiver end, the two cipher texts are received which along with the private key help to decrypt the text.

Figure 1.4 – Output of 1bit number

Figure 1.5 – Output of 1bit number

VI. Analysis Of The Output

At the sender end :

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)

At the receiver end :

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

The Encrypted message sent at the receiver side is same as the Decrypted message at the Receiver site.

VI. Conclusion

The digital signature based Elliptic Curve Cryptography covers all four aspects of security - Integrity, Authentication , Non-repudiation and Confidentiality.

The promise of ECC for the better and secure data transmission is opening new dimensions of its application in every field of communication. Mobile computing, wireless sensor net-works, server based encryption, image encryption, government and financial communication protocols and many other. But there is still a lot of research required for its practical implementation.

1. It is used in the growing wireless industry.
2. It depends on the case of use and level of security it provides.

Future Work-

This is a completely new domain and has tremendous scope of research.
ECC can be used to provide authentication and enhanced security.
USE OF ECC - Mobile computing, wireless sensor net-works, server based encryption, image encryption, government and financial communication protocols and many other areas.

References -

[1]. An Elliptic Curve Cryptography Primer, Certicom "Catch the curve" White paper series, June 2004

[2]. Elliptic Curve Cryptography A new way for Encryption, Rahim Ali , Department of Computer Science and Engineering, Bahria University, 13 National Stadium Road Karachi

[3]. IEEE Standard P 1363-2000, IEEE standard specification for public key cryptography', Aug2000.

[4]. The Study and Application of Elliptic Curve Cryptography Library on Wireless Sensor Network, 2008 11th IEEE International Conference on Communication Technology Proceedings.

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

[6]. "Design of a Private Credentials Scheme Based on Elliptic Curve Cryptography" , 2009 First International Conference on Computational Intelligence, Communication Systems and Networks.

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

[8]. D. V. Chudnovsky and G. V. Chudnovsky, "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, May 1986.

[9]. "New Low Complexity Key Exchange and Encryption protocols for Wireless Sensor Networks Clusters based on Elliptic Curve Cryptography", NRSC2009.