Journal of Advances in Science and Technology
Vol. 17, Issue No. 1, March-2020, ISSN 2230-9659

A Study of Security Protocols using Elliptic Curve Encryption for Data Transport and Encryption

Deepak Kumar Sharma[1]*, Dr. Birendra Singh Chauhan[2]

[1] Research Scholar, Shri Krishna University, Chhatarpur M.P.

[2] Associate Professor, Shri Krishna University, Chhatarpur M.P.

Abstract - Invention of public-key cryptography is the greatest revolution in the history of cryptography. Two factors influence the security of the public key cryptography 1) length of the key and 2) computational overhead to break the cipher. Public-key cryptography suffers with two types of problems symmetric encryption and key distribution. Whitefield Diffie and Martin Hellman published an interesting solution to the problem of key agreement or key exchange in 1976 called Diffie-Hellman key exchange protocol. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Neil Koblitz and Victor Miller. Elliptic Curve Cryptographic (ECC) schemes are public-key cryptosystems. They not only provide the same functionality but also preserve the same level of security as RSA schemes with shorter key length and relatively computational overhead. They are attractive because they offer the same security level as a finite field based cryptosystem, shorter key length and fast encryption/decryption process. The proposed work in this study is basically divided into two parts (i). Secure and Authentic Key Transport (ii). Data Encryption/ Decryption using elliptic curves over finite fields. The principal focus of inventors of ECC was the study the advantages of elliptic curve cryptography in the wireless communications in place of well-known traditional RSA cryptosystem.

Keywords - Security Protocols, Elliptic Curve Encryption, Data Transport, Encryption, Elliptic Curve Cryptography

----------X----------

INTRODUCTION

Elliptic curve cryptography is protected by elliptic curve discrete logarithmic problem. Alfred J. Menezes and Scott A. Vanstone in their research paper explained the implementation of elliptic curve cryptography. They have also analyzed the elliptic curve analogue of the ElGamal cryptosystem. Miyaji A. in his research paper discussed the types of elliptic curves that are suitable for encryption purposes. Asrjen K. Lenstra and Eric R. Verheul in their research paper explained the selection of key for cryptosystems using elliptic curves over finite fields. Andreas Enge [8] explained elliptic curves and their applications. Antoines Joux [10] in his research paper and Anna M. Johnston, Peter S. Gemmell [9] explained how the Diffie-Hellman key exchange protocol is vulnerable to man-in-middle attack in their papers. MarisaW.Paryasto et.al. explained in detail the issues in elliptic curve cryptography implementation.

ELLIPTIC CURVE ARITHMETIC:

Affine Plane:

An Affine Plane over the field K is the set KxK which is denoted by A2 (K). Affine Plane Curve: An Affine Plane curve over the finite field K is the set of all zeros of an irreducible polynomial C belongs to K [x,y] in the affine plane. i.e., {(x,y) ∈ to A2 (K)}. Example: - For K = R, the curves D = y2 – (x3 +x2) and E = y2 – (x3 -x) are affine curves.

1 Affine Elliptic Curves:

An equation of the form E: y2 + a1xy + a3y = x 3 + a2x 2 + a4x + a6…….. (1) is called an affine Weierstrass equation [40,108] over the set of real numbers.

Here a1, a2, a3 , a4, a6 are real numbers ∈ R, x and y take on values in the real numbers. The quantities that relate to E are

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

Here Δ is said to be the discriminant of the elliptic curve E. If Δ≠0 then the elliptic curve is known as a smooth curve. That is the Weierstrass equation is non-singular and only one tangent line can be drawn at every point on the curve. ∞ is the only point on

the line at infinity satisfying the projective form of the Weierstrass equation [4, 8]. If L is the field of extension of real numbers, then the set of L-rational points on the elliptic curve E is $E(L)=\{(x,y)\in LXL: y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6=0\}\cup\{\infty\}$ ∞ the point at infinity.

2 Projective Plane:

To construct the group laws on the elliptic curves the line that intersects the curve at three points is needed. The sum of two points is more or less the third point of intersection of the line through these points on the curve. The famous Bezouts's theorem states that two elliptic curves having degrees m and n respectively intersect in mn points, on counting multiplicities in proper way. Two parallel lines never intersect. So Bezout's theorem holds good if one point is added for each parallel class of lines. This is called the projective plane.

3 Group laws on elliptic curve over finite field E(K):

Consider an elliptic curve defined over the field of integers K. There is a chord-and-tangent rule for adding two points in E (K), to give the third point. The set of all points of E (K) forms an abelian group with addition operation. Here ∞, the point at infinity is the identity elements.

Geometric rules of Addition:

If P(x1,y1) and Q(x2,y2) be two points on the elliptic curve E. If a line is drawn through P and Q it intersects the elliptic curve at the third point. The reflection of this point about x-axis is the point R which is the sum of the points P and Q. The same rule is also applied to two points P and –P, with the same x-coordinate. The points are joined by a vertical line, which is assumed to be intersecting the curve at the point infinity. We therefore have P + (-P) = ∞, the identity element which is the point at infinity.

Doubling the point on the elliptic curve:

If a tangent line is drawn to the elliptic curve at the point P which intersects the curve at a point. Then the reflection of this point about x-axis is R. As an example the addition of two points and doubling of a point are shown in the following figures 1 and figure 2 for the elliptic curve y 2 = x3 -x.

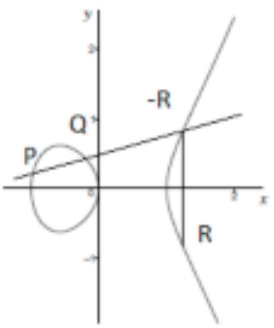

Figure 1. Geometric addition

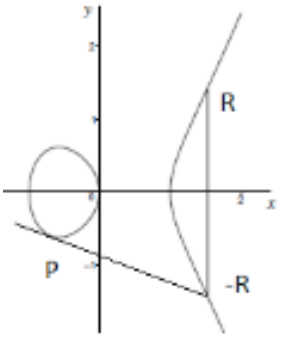

Figure 2. Geometric doubling

Existence of Identity: P + ∞ = ∞ +P = P for all P∈ E(K) where ∞ is the point at infinity.

Existence of Negatives: - Let P(x,y) ∈E(K) then(x,y) + (x,-y) = ∞ where (,) x y − is the negative of P denoted by –P, and ∞ the point at infinity.

Point addition: Let P(x1,y1), Q(x2,y2) ∈ E(K) where P ≠ Q. Then P + Q = (x3,y3) where

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2 \text{ and } y_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1$$

Point Doubling: Let $P(x_1,y_1)\in$ E(K) where $P\neq -P$ then

$$2P=(x_3,y_3) \text{ where } x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1 \text{ and } y_3=\left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3)-y_1$$

Point Multiplication:-

If E is an elliptic curve over the field K of integers and let P be any point on the elliptic curve. Then for an integer k in K the point multiplication is defined as repeated addition. kP = P+P+……..k times.

4 Elliptic Curves over Finite Fields:

For designing cryptographic protocols using elliptic curves it is sufficient to consider the elliptic curve of third degree equation y2 = x 3 + ax + b over the finite field Fp (p ≠ 2,3) where p is a large prime number. Here a,b are coefficients and the variables x and y take the values in the set of integers from 0 through p-1. All the elliptic curve arithmetic is done in this field with respect to modulo p.

5 Group Order:

The order of the elliptic curve E defined over the finite field Fp is the number of points of E(Fp) and is denoted by # E(Fp) Since the Weierstrass equation 1 has almost two solutions for each x ∈ Fp, then # E (Fp) ∈ [1, 2p+1].

6 Hasse Theorem: If E is an elliptic curve defined over the Fp.

Then $p+1-2\sqrt{p} \le \#E(F_p) \le p+1+2\sqrt{p}$

Proof:- The interval$[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ is called Hasse interval [86,97]. An alternate formulation of Hasse's theorem is: If E is defined over the field F_p, then $\#E(F_p) = p+1-t$, where $|t| \le 2\sqrt{p}$; t is called the trace of E over the field F_p. Since $2\sqrt{p}$ is small relative to p we have $\#E(F_p) \approx p$

7 Admissible orders of Elliptic curves:

Consider an elliptic curve E defined over the field F_p. Let $p = q^m$, where q is the characteristic of Fp. Then the order of the elliptic curve $\#E(F_p) = p+1-t$ provided one of the following conditions holds

(i) $t \not\equiv 0 \pmod q$ and $t^2 \le 4p$

(ii) m is odd and either (a) t = 0; or (b) $t^2 = 2p$ and q = 2 or (c) $t^2 = 3p$ and q = 3

(iii) m is even and either (a) $t^2 = 4p$ or (b) $t^2 = p$ and $q \not\equiv 1 \pmod 3$ or (c) t = 0 and $q \not\equiv 1 \pmod 4$

8 Super singular Curves:

Let E be an elliptic curve defined over the field Fp and let q be the characteristic of Fp then the elliptic curve E is said to a super singular curve if q divides t where t is the trace. If q does not divide t then the elliptic curve E is said to be non-super singular curve. Menezes and Vanstone have observed the advantages of super singular elliptic curves in cryptosystems over the field Fp

Group Structures:

If E be an elliptic curve defined over Fp. Then E(Fp) is said to be isomorphic to 1 2 Z Z n n + . Heren1 and n2 are unique positive integers such that n2 divides both n1 and p – 1

9 Diffie-Hellman Key Exchange Protocol:

In Diffie-Hellman Key exchange protocol the communicating parties exchange secret keys before they start communication. DiffieHellman key exchange algorithm is a public-key mechanism having publicly known values: a prime number p and a number α which is a primitive root of p. If two communicating parties A and B want to exchange the secret key then A chooses a number X1 and computes the

secret key $K_1 = \alpha^{X_1} \bmod p$. A communicates K_1 to B. Similarly B selects a number X_2 and computes $K_2 = \alpha^{X_2} \bmod p$ and communicates K_2 to the A. Then A computes the shared secret key K as $K = (K_2)^{X_1} \bmod p = (\alpha^{X_2})^{X_1} \bmod p = \alpha^{X_2 X_1} \bmod p$ and B computes the secret key K as $K = (K_1)^{X_1} \bmod p = (\alpha^{X_1})^{X_2} \bmod p = \alpha^{X_1 X_2} \bmod p$

10 ElGamal Method of Encryption:

The ElGamal method is a public-key algorithm, which is used for digital signatures and encryption. The security of ElGamal method depends on the complexity of computing discrete logarithms in a finite field. Here a key pair is generated by the sender. The sender selects a prime number p, two random numbers g and x less than p. The sender computes y = gx mod p. He keeps x as his secret key and publishes y, g, p. If the sender wants to communicate the message M, first he selects a random number k such that k is relatively prime to p-1 and computes a = g k mod p, b = yk M mod p. Then M = (ax+kb) mod (p-1). Then the pair of (a, b) becomes the cipher text. Here the cipher text is double the size of the plain text. To decrypt (a, b) to the plain text M the receiver calculates M = b/ax mod p.

11 Elliptic Curve Discrete logarithmic Problem (ECDLP):

Consider an equation Q =kS where Q,S∈Ep(a,b) and k<p. It is relatively easy to calculate Q given k and S. But it is relatively hard to determine k given Q and S.

12 Analogue of Diffie-Hellman Key Exchange Method:

The exchange of secret key between two communicating parties can also be done using elliptic curve Ep(a,b) similar to Diffie-Hellman key exchange method [97, 129]. In this method the communicating parties agree upon to use and elliptic curve Ep(a,b) and a generator G on Ep(a,b) of order n. The sender selects an integer SA, computes PA = SA G and communicates PA to the receiver. Similarly the receiver selects an integer SB, computes PB = SB G and communicates PB to the sender. Then both the sender and the receiver compute the shared secret key as K = SAx PB = SBx PA.

13 Analogue of ElGamal:

If two communicating parties A and B want to communicate the messages they agree upon to use an elliptic curve Ep(a,b) and a generator G of order n. A selects a random number nA and computes PA = nAxG. He keeps nA as the secret key and publishes PA. Similarly B selects a random number nB, computes PB = nB x G. B keeps nB as his secret key and publishes PB. If A wants to communicate the message Pm to B then he selects a random number k. Pm it is encrypted as Cm = {kG, Pm+k PB}. This encrypted message Cm is communicated to B. Here A used B's public key for encryption. B decrypts the message as Pm + k PB – nB(kG) = Pm + k(nBG) - nB(kG) = Pm

14 Insecure curves for ECC:

The following types of curves are not suitable for ECC

(i). Curves whose group order # E(Fp) factorizes into small primes. These curves are susceptible to Pohlig-Hellman attacks.

(ii). Super singular curves

(iii). Anomalous curves. i.e., # E(Fp) = p.

PROPOSED WORK:

PART (I) SECURE AND AUTHENTIC KEY TRANSPORT USING ELLIPTIC CURVES OVER FINITE FIELDS

Two algorithms have been proposed as section A and section B of Part (i) in this study for secure and authentic key transport using elliptic curves over finite fields

1 Key Transport Protocol:

In key exchange protocols such as Diffie-Hellman key exchange protocol all the members of a group of communicating parties contribute the information in deriving the secret key. In key transport protocol any member of the group creates the secret key and communicates it to the others. If two parties want to communicate the messages through public channel with absolute security, one of the means of achieving the security is using a one-time key that is for each communication different key is used and the key used is discarded.

2 Advantages of Key Transport Protocols:

The Diffie-Hellman key exchange algorithm is insecure against the man-in-middle attack An adversary C in between A and B interrupts the message. C selects XC1 and XC2 and computes KC1 and KC2 similar to K1 and K2 and the adversary communicates KC1 rather K1 to B and KC2 rather K2 to A. In the method proposed here work secure and authentic key transport between two communicating parties is demonstrated. The Diffie-Hellman key exchange protocol is vulnerable to man-in-middle attack since the communicating parties exchange the shared secret key. Here both the communicating parties do not have any control over what will be the secret key for their communication. But, in both the algorithms proposed in section A and section B of part (i) the communicating parties can transport their own secret keys for the communication of the messages in an insecure channel rather than sharing the part of the secret key. The secure and authentic key transport protocols proposed in sections A and B have overcome the difficulties with which the Diffie-Hellman key exchange protocol is suffering from.

3 Section

A The communicating parties Alice and Bob agree upon to use the elliptic curve Ep (a,b), and a point C on the elliptic curve Ep (a,b). Alice selects a large random number α which is less than the order of the generator of the elliptic curve Ep (a,b) and a point A on the elliptic curve. She computes A1 = α (C+A) and A2 = α A. She keeps the random number α and the point A as her secret/private keys and publishes A1 and A2 as her general public keys. Similarly Bob selects a large number β and a point B on the elliptic curve. He computes B1 = β (C+B) and B2 = β B. He keeps the random number β and the point B as his secret/private keys and publishes B1 and B2 as his general public keys. After publishing the general public keys, the communicating parties again calculate the following quantities and publish those quantities as their specific public keys.

Alice calculates AB = α B2 and publishes it as her specific public key for Bob

Bob calculates BA = β A2 and publishes it as his specific public key for Alice

Alice's private/secret key 1 = α, a large random number less than the order of Ep (a,b)

Alice's private/secret key 2 = a point A on the elliptic curve Ep (a,b)

Alice's general public key 1 = a point A1on the elliptic curve Ep (a,b)

Alice's general public key 2 = a point A2 on the elliptic curve Ep (a,b)

Alice's specific public key for Bob = a point AB on the elliptic curve Ep (a,b)

Bob's private/secret key 1 = β, a large random number less than the order Ep (a,b)

Bob's private/secret key 2 = B, a point on the elliptic curve Ep (a,b)

Bob's general public key 1 = B1, a point on the elliptic curve Ep(a,b)

Bob's general public key 2 = B2, a point on the elliptic curve Ep (a,b)

Bob's specific public key fr Alice = BA, a point on the elliptic curve Ep(a,b)

Encryption of the secret key:

Bob selects a point S on the elliptic curve that can be used as the secret key in the process of communication with Alice. The secret key S is a pair of numbers. For conventional encryption a single number should be generated from S. The x or y coordinate of the point S are some function of x and y, say f(x, y) can be used to generate a single number. Bob encrypts the secret key S as follows.

$$S^E = \beta A_1 + A_B + S$$

Decryption:- Alice decrypts S^E and retrieves S as $S = S^E - \alpha B_1 - B_A$

The Decryption works out properly:

$$S^E - \alpha B_1 - B_3 = \beta A_1 + A_B + S - \alpha B_1 - B_A$$

$$= \beta\alpha (C + A) + \alpha\beta B + S - \alpha\beta (C+B) - \beta\alpha A$$

$$= \beta\alpha C + \beta\alpha A + \beta\alpha B + S - \alpha\beta C - \alpha\beta B - \alpha\beta A$$

Example:-

Consider an elliptic curve whose equation is $y^2 = x^3 + 2x + 9$. The graph of the function is shown in figure 3.

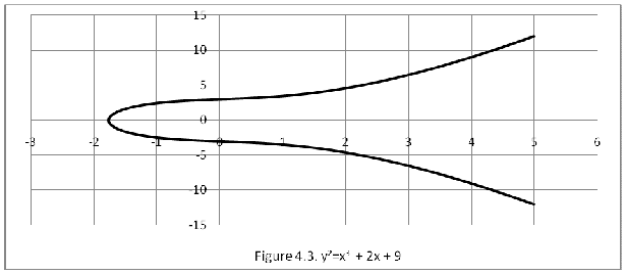

Figure 3 $y^2 = x^3 + 2x + 9$

In the above graph the right lines can be drawn in xy-plane such that 1) there is no intersection between the right line and elliptic curve 2) the line intersects the elliptic curve at one point or two points or three points.

CONCLUSION

ECC protocols provide solution for both the key distribution and secure information exchange. The security of the Elliptic Curve Cryptography depends on the difficulty of finding the value of k, given kP and P where k is a large number less than the order of the generator of Ep (a,b) and P is a random point on the elliptic curve. The elliptic curve parameters for cryptographic schemes should be carefully chosen in order to resist all known types of attacks of Elliptic Curve Discrete Logarithmic Problem (ECDLP). The exhaustive search attack can be restricted by selecting elliptic curve parameters with p sufficiently large to present an infeasible amount of computation. The conventional public key encryption provides confidentiality but not the authentication. In the key transport protocol described in section A of part(i) of this study each communicating party separately selects a random number and a point on the elliptic curve as their private keys. The communicating parties publish two public keys instead of one. The secret key is encrypted using communicator's private key and receiver's public keys. At the other end the receiver decrypts it using her private key and the public key of the communicator. Such protocol ensures confidentiality, authentication and non-repudiation. This process ensures high level of security .In the data encryption /decryption method using elliptic curves proposed in part (ii) of this study each communicating party uses a large random number and a point on Ep (a,b) as secret keys and two points on Ep (a,b) as general public keys. Each communicating party publishes a specific public key for each intended recipient basing on the recipient's general public key. The communicator of the message encrypts the message using his private key and the specific public key published by the receiver. This ensures that the message is almost digitally signed. The receiver alone can decrypt the cipher because he has to use his private/secret key. In addition to this each character of the message is coded to the point on the elliptic curve using the code table which is agreed upon by the communicating parties and each message point is encrypted to a pair of points on the elliptic curve.

REFERENCES

[1] Acricmez O., Koc C.K., Seifert J.P. "Predicting secret keys via branch prediction" in Proc. RSA (CT-RSA)2007, Lecture Notes in Computer Sciences, Vol.4377 (Springer Berlin, 2007) pp.225-242.

[2] Adams C. "Simple and effective key scheduling for symmetric ciphers" workshop in selected areas of cryptography SAC'94, 1994.

[3] Advanced Encryption Standards [AES] website http://csrc.nist.gov/encryption/aes/

[4] Alfred J. Menezes and Scott A. Vanstone, "Elliptic curve cryptosystems and their implementations", Journal of Cryptology, 1993, Volume-6, Number-4, pp. 209-224.

[5] Alter R., "Some remarks and results on Catalan numbers", proceedings of Louisiana Conference on Conbinatorics, Graph Theory and computing (1971).

[6] Alter R., and Kubota K.K. "Prime power divisibility of Catalan numbers", Journal of Combinatorial Theory, series A, 15 (1973), 243-256.

[7] Amos Beimel., Tal Malkin., Kobbi Nissim, and Enav Weinreb, "How should we solve search problems privately", Journal of Cryptology, Springer 2010, Volume-23, Number-2, pages 344-371.

[8] Andreas Enge. "Elliptic curves and their applications to cryptography," Kluwer Academic Publishers, Boston, 1999.

[9] Anna M. Johnston, Peter S. Gemmell, "Authenticated key exchange provably secure against the man-in-middle attack", Journal of Cryptology (2002) Vol. 15 Number 2 pages 139-148.

[10] Antoines Joux "A one round protocol for Tripartite Diffie-Hellman", Journal of Cryptology, 2004, Volume 17, Number 4, pages 263-276.

[11] Apostol T. M. "Introduction to analytic number theory". New York: Springer-Verlag, 1976.

[12] Asrjen K., Lenstra and Eric R. Verheul "Selecting cryptographic key size", Journal of Cryptology, 2001, Volume-14, Number 4, pages 255-293.

[13] Atul Kahate, "A text book of Cryptography and network security", II Edition, Tata Mc Graw Hill Education Private Limited, New Delhi, 2009.

[14] Ayoub R. G. "An Introduction to the analytic theory of numbers", Providence, RI: Amer. Math. Soc., 1963.

[15] Balasubramanian R. "Elliptic curves and cryptography", in Bhandari A.K., Nagraj D.S., Ramakrishnan B., Venkataraman T.N. (editors), Elliptic Curves, Modular Forms, and Cryptograph, Hindustan Book Agency, New Delhi, 2003. ISBN 81-85931-42-9,pp 325-345.

[16] Barreto P.S.L.M., Lynn B., Scott M. "Constructing elliptic curves with prescribed embedding degrees", in security and communication networks – SCN 2002 Lecture Notes in Computer Science, Vol. 2576 (Springer, Berline, 2002), pp. 354-368.

Corresponding Author

Deepak Kumar Sharma*

Research Scholar, Shri Krishna University, Chhatarpur M.P.