International Journal of Mathematical Archive-3(1), 2012, Page: 137-142
Available online through www.ijma.info ISSN 2229 – 5046

AUTHENTIC KEY TRANSPORT IN SYMMETRIC CRYPTOGRAPHIC PROTOCOLS USING SOME ELLIPTIC CURVES OVER FINITE FIELDS

D. Sravan Kumar[1], CH. Suneetha[2*] and A. Chandrasekhar[3]

[1]Reader in Physics, SVLNS Government College, Bheemunipatnam, India
E-mail: skdharanikota@gmail.com

[2]Assistant Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India
E-mail: gurukripachs@gmail.com

[3]Professor in Engineering Mathematics, GITAM University, Visakhapatnam, India
E-mail: acs@gitam.edu

(Received on: 20-12-11; Accepted on: 09-01-12)

ABSTRACT

Cryptology is the study of techniques for ensuring the secrecy and authentication of the information. Public –key encryption schemes are secure only if the authenticity of the public-key is assured. Elliptic curve arithmetic can be used to develop a variety of elliptic curve cryptography (ECC) schemes including key exchange, encryption and digital signature. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size, thereby reducing the processing overhead. In the present paper a new technique of autheitic key transport using elliptic curve cryptography is proposed.

***Key Words**:- Elliptic Curve Cryptography, public-key, secret key, encryption, decryption.*

INTRODUCTION:

The study of elliptic curves by algebraists, algebraic geometers and number theorists dates back to the middle of the nineteenth century. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Neil Koblitz and Victor Miller [9, 11]. Elliptic Curve Cryptography (ECC) schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, their security is based on the hardness of a different problem, namely the Elliptic Curve Discrete Logarithmic Problem (ECDLP). Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA schemes. The competing system to RSA is elliptic curve cryptography and the principal attraction of elliptic curve cryptography; is that it offers same level of security for smaller key size [8]. An elliptic curve E over a field R of real numbers is defined by an equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

Here a_1, a_2, a_3 , a_4, a_6 are real numbers belong to R, x and y take on values in the real numbers. If L is an extension field of real numbers, then the set of L-rational points on the elliptic curve E is

$E(L) = \{(x, y) \in LXL : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$ where ∞ the point is at infinity. Equation (1) is called Weierstrass equation. Sometimes E can also be defined over the field of real numbers. If E is defined over the field of integers K, then E is also defined over any extension field of K. The condition $\Delta \neq 0$ ensures that the elliptic curve is "smooth". i.e., there are no points at which the curve has two or more distinct tangent lines. The point ∞ is the only point on the line at infinity that satisfies the projective form of the Weierstrass equation [1, 7, 11]. In the present paper for the purpose of the encryption and decryption using elliptic curves it is sufficient to consider the equation of the form $y^2 = x^3 + ax + b$. For the given values of a and b the plot consists of positive and negative values of y for each value of x. Thus this curve is symmetric about the x-axis.

Corresponding author: CH. Suneetha[2], *E-mail: gurukripachs@gmail.com

GROUP LAWS OF E (K):

Let $E_p(a, b)$ be an elliptic curve defined over the field of integers K. There is a chord-and-tangent rule for adding two points in $E_p(a, b)$, to give the third point. Together with this addition operation, the set of points of $E_p(a, b)$ forms an abelian group with ∞ , the point at infinity serves as identity elements.

GEOMETRIC RULES OF ADDITION:

Let $P(x_1, x_2)$ and $Q(x_2, y_2)$ be two points on the elliptic curve E. The sum R is defined as: First draw a line through P and Q, this line intersects the elliptic curve at a third point. Then the reflection of this point of intersection about x-axis is R which is the sum of the points P and Q.

The same geometric interpretation also applies to two points P and –P, with the same x-coordinate. The points are joined by a vertical line, which can be viewed as also intersecting the curve at the infinity point. We therefore have P + (-P) =O, the identity element which is the point at infinity.

DOUBLING THE POINT ON THE ELLIPTIC CURVE:

First draw the tangent line to the elliptic curve at P which intersects the curve at a point. Then the reflection of this point about x-axis is R.

The addition of two points and doubling of a point are shown in the following figures 1 and 2 for the elliptic curve **$y^2 = x^3 - x$**.

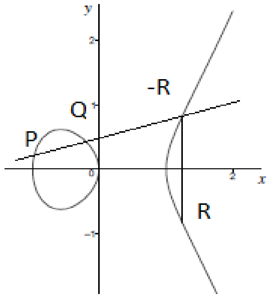

Figure: 1 Geometric addition

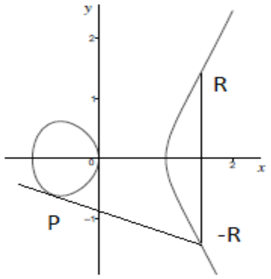

Figure: 2 Geometric doubling

Identity: P + ∞ = ∞ + P = P for all $E_K(a,b)$, where O is the point at infinity.

Negatives: Let $P(x, y) \in E_p(a, b)$ then$(x, y) + (x,-y) = 0$. Where $(x,-y)$ is the negative of P denoted by –P.

Point addition: Let $P(x_1, x_2), Q(x_2, y_2) \in E_p(a, b)$ where $P \neq Q$. Then $P + Q = (x_3, y_3)$ where

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

Points Doubling: Let $P(x_1, y_1) \in E_K(a,b)$ 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:- Let P be any point on the elliptic curve $E_K(a,b)$ where K is the field of integers. Then the operation multiplication of P is defined as repeated addition. $kP = P + P + P.........ktimes$

ELLIPTIC CURVE CRYPTOGRAPHY:

Elliptic Curve Cryptography (ECC) [5, 7, 8, 12] makes use of the elliptic curve in which the variables and coefficients are all restricted to elements of the finites fields [10]. Two families of elliptic curves are used in cryptographic applications: Prime curves over Z_p and binary curves GF(2^m). For a prime curve over Z_p, we use a cubic equation in which the variables and the coefficients all take on values in the set of integers from 0 through p-1 and the calculations are performed with respect to modulo p.

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 [13]. i.e., for each communication different key is used and the key used is discarded. For authentic key exchange for each communication here we propose a method using algebra of elliptic curves. The present work demonstrates a technique of key transports protocol using elliptic curve [6, 4]. Though the key exchange using Elliptic Curve is analogous to Diffie-Hellman key exchange protocol, it is less prone to man-in-middle attacks because in this method both the users can securely transport their own secret keys for encryption/decryption of the messages in their communication through the public channel rather than partial sharing of the keys. Moreover, the encrypted key size is same as that of the unencrypted key.

ELLIPTIC CURVE DISCRETE LOGARITHMIC PROBLEM (ECDLP):

To form a cryptographic system using elliptic curve a hard problem is required. It is very hard to determine the value of k from the equation

Q = kP for known points P,Q on the elliptic curve E_p a,b) where k is a large random number less than p.

DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL:

In Diffie-Hellman Key exchange algorithm both the sender and the receive exchange secret keys that can be used for subsequent encryption of the messages. In Diffie-Hellman key exchange algorithm, there are publicly known numbers: a prime number P and a number α which is a primitive root of P. Suppose two users A and B want to exchange the secret key then user A selects a number X_1 and computes the secret key $K_1 = \alpha^{X_1} \bmod P$. User A communicates this K_1 to user B. Similarly user B selects a number X_2 and computes $K_2 = \alpha^{X_2} \bmod P$ and communicates this K_2 to the user A. Then the user A computes the shared secret key K as

$$K = \left(K_2\right)^{X_1} \bmod P = \left(\alpha^{X_2}\right)^{X_1} \bmod P = \alpha^{X_2 X_1} \bmod P$$

Similarly the use B computes the secret key K as $K = \left(K_1\right)^{X_1} \bmod P = \left(\alpha^{X_1}\right)^{X_2} \bmod P = \alpha^{X_1 X_2} \bmod P$

But Diffie-Hellman key exchange algorithm is insecure against the man-in-middle attack [2,3]. An adversary C in between A and B intercepts the message. C selects X_{C1} and X_{C2} and computes K_{C1} and K_{C2} similar to K_1 and K_2. Then he interrupts the key K_1 which is being communicated to the user B by the user A , rather communicates K_{C1} to B. Similarly he also interrupts the key K_2 which is being communicated by the user B to the user A, rather communicates K_{C2} to A.

ANALOGUE OF DIFFIE-HELLMAN KEY EXCHANGE METHOD:

The addition operation in Elliptic Curve Cryptography (ECC) is the counterpart of modular multiplication in RSA and multiple addition is the counterpart of modular exponentiation.

The exchange of key between two communicating parties Alice and Bob can also be done using elliptic curve E_p (a, b) similar to Diffie-Hellman key exchange method. In this method Alice selects an integer s_A and computes $P_A = s_A G$, where G is the generator on the elliptic curve E_p (a, b). She communicates P_A to Bob. Similarly Bob selects an integer s_B and computes $P_B = s_B G$, where G is the generator on the elliptic curve E_p (a, b). He communicates P_B to Alice. Then both Alice and Bob compute the shared secret key as $K = s_A x\ P_B = s_B x\ P_A$. In this method of exchange of key using elliptic curve neither Alice nor Bob has any control over what will be the shared secret key used for encryption/decryption in their communication. Moreover, it is vulnerable to man-in-middle attack which is the basic weakness of the Diffie-Hellman key exchange protocol.

Here in the present paper we propose a new technique of secure key and authentic transport in public channel. In this method the secret key will be transported by one of the communicating parties to the other rather than sharing the part of the secret key.

KEY TRANSPORT PROTOCOL:

A key transport protocol [1] is a key establishment protocol where one entity creates the secret key and securely transfers it to the others. A key agreement protocol is a key establishment protocol where all participating entities contribute information which is used to derive the shared secret key. There are various methods of distribution and exchange of secret keys: For example Diffie-Hellman key exchange protocol, a key agreement protocol using Elliptic Curve Cryptography etc.

PROPOSED METHOD:

Two communicating parties Alice and Bob agree upon to use the elliptic curve E_p (a, b), where p is a large prime number or almost prime number, p should not be written as the product of small prime numbers, and the elliptic curve E_p (a, b) should not be a super singular curve or anomalous curve. They also agree upon to use a point C on the elliptic curve E_p (a, b). Alice selects a large random number α which is less than the order of E_p (a, b) and a point A on the elliptic curve. She computes

$A_1 = \alpha (C + A)$ and $A_2 = \alpha A$. She keeps the random number α and the point A as her private keys and publishes A_1 and A_2 as her general public keys. Similarly Bob selects a large random number β and a point B on the elliptic curve. He computes $B_1 = \beta (C+B)$ and $B_2 = \beta B$. He keeps the random number β and the point B as his private keys and publishes B_1 and B_2 as his general public keys. After publishing the public keys, the communicating parties again calculate the following quantities and publish them as their specific public keys for each other.

Alice calculates $A_B = \alpha B_2$ and publishes it as her specific public key for Bob calculates $B_A = \beta A_2$ and publishes it as his specific public key for Alice

Alice's private key 1	= α, a large random number less than the order of the generator
Alice's private key 2	= a point A on the elliptic curve E_p (a, b)
Alice's general public key 1	= a point A_1on the elliptic curve E_p (a, b)
Alice's general public key 2	= a point A_2 on the elliptic curve E_p (a, b)
Alice's specific public key for Bob	= a point A_B on the elliptic curve E_p (a, b)
Bob's private key 1	= β, a large random number less than the order of the generator G
Bob's private key 2	= B, a point on the elliptic curve E_p (a, b)
Bob's general public key 1	= B_1, a point on the elliptic curve Ep(a, b)
Bob's general public key 2	= B_2, a point on the elliptic curve E_p (a, b)
Bob's specific public key for Alice	= B_A, a point on the elliptic curve Ep(a, b)

Encryption: 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 or some function of x and y, say f(x, y) can be used to generate a single number.

Bob encrypts the shared 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:

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

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

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

$$= S$$

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

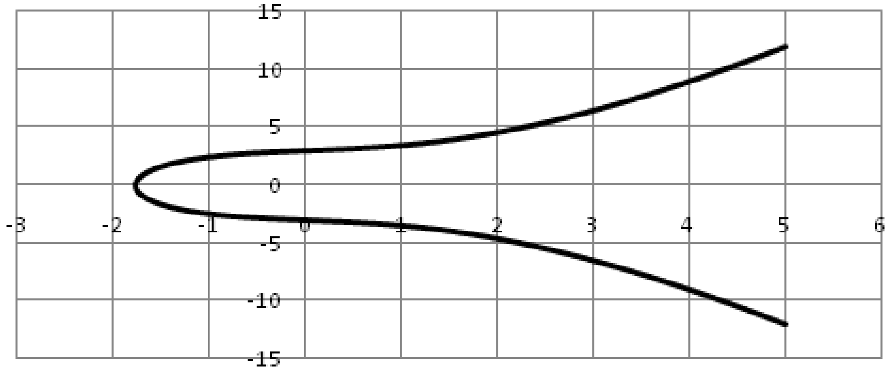

Figure: 3 $y^2=x^3 + 2x + 9$

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.

Now consider an elliptic curve $(y^2 = x^3 + 2x + 9)_{\text{mod37}}$, E_{37} (2,9). The points on the elliptic curve E_{37} (2, 9) are { ∞,(5,25), (1,30), (21,32), (7,25), (25,12), (4,28), (0,34), (16,17), (15,26), (27,32), (9,4),(2,24), (26,5), (33,14), (11,17), (31,22), (13,30), (35,21), (23,7), (10,17), (29,6), (29,31), (10,20), (23,30), (35,16),(13,7), (31,15), (11,20), (33,23), (26,32),(2,13), (9,33), (27,5), (15,11), (16,20), (0,3), (4,9), (25,25), (7,12), (21,5), (1,7), (5,12),}

The graph of the function is shown in Figure 4.

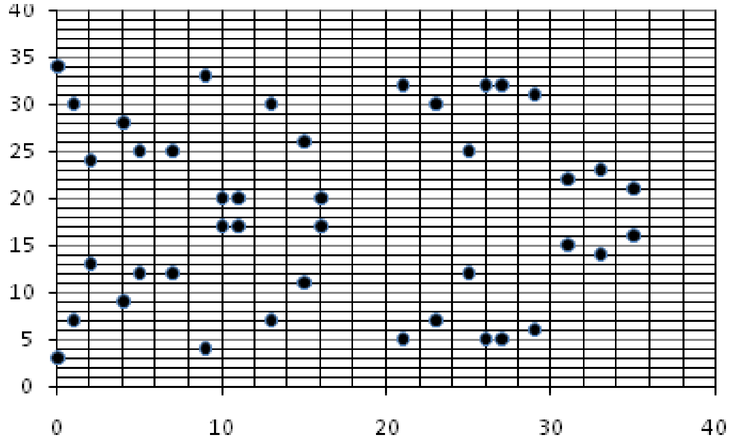

Figure: 4. Elliptic Curve Group (Cyclic) $E_{37}(2,9)$

Let C = (9,4). Alice selects a random number α = 5, any point A = (10, 20) on the elliptic curve. She computes

$A_1 = \alpha (C+A) = 5[(9,4) + (10,20)] = (1,7)$
$A_2 = \alpha A = (33,23)$.

She keeps the random number α and the point A on the elliptic curve as her secret keys and publishes A_1 and A_2 as her general public keys.

Bob selects β = 7, B = (11,20) on the elliptic curve. He computes
$B_1 = \beta (C+B) = (11, 17)$
$B_2 = \beta B = (23, 30)$.

He keeps the random number β and the point B on the elliptic curve as his secret keys and publishes B_1 and B_2 as his general public keys.

Alice calculates $A_B = \alpha B_2 = (15,11)$ and Bob calculates $B_A = \beta A_2 = (2,13)$. Alice publishes A_B as specific public key for Bob and Bob publishes B_A as specific public key for Alice.

Encryption of the secret key by Bob: If Bob wants to send the secret key S = (26, 32) on the elliptic curve E37 (2, 9) for encryption/decryption of a particular message then he encrypts this secret key S as $S^E = S + \beta\, A_1 + A_B = (0, 34)$. He sends the encrypted key to Alice.

Decryption by Alice: Alice decrypts the shared secret key as

$S = S^E - \alpha\, B_1 - B_A = (26, 32)$

CONCLUSIONS:

Public key cryptography provides 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 where k is a large number less than the order of the generator and P is a point on the elliptic curve. This is known as Elliptic Curve Discrete Logarithmic Problem (ECDLP). 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 communicator. Such protocol ensures confidentiality, authentication and non-repudiation. The elliptic curve parameter for cryptographic scheme should be chosen carefully to resist all known types of attacks on Elliptic Curve Discrete Logarithmic Problem ECDLP. The attack of exhaustive search can be circumvented by choosing elliptic curve parameters such that infeasible amount of computational overload is presented to the adversary, who can mount various types of attacks.

REFERENCES:

[1] Alfred J. Menezes and Scott A. Vanstone, "Elliptic Curve Cryptosystems and their implementations", Journal of Cryptology, 1993, Volume-6, Number-4, pages 209-224.

[2] 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.

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

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

[5] A. Chandrasekhar *et.al.* "Some Algebraic Curves in public Key crypto systems", International Journal of Ultra Scientist of Physical Sciences, 2007.

[6] Darrel Hankerson, Alfered Menezes, Scott Vanstone, "A Gide to elliptic curve Cryptography", Springer, 2004.

[7] Enge A. "Elliptic curves and their applications to cryptography", Norwell, MA: Kulwer Academic publishers 1999.

[8] Gura N., Shantz S., Eberle H., et al "An End-to End Systems Approach to Elliptic Curve Cryptography", Sun Microsystems Laboratories; 2002; Retrieved May, 10, 2006, http://research.sun.com/projects/crypto

[9] V. Miller, "Uses of Elliptic curves in Cryptography". In advances in Cryptography (CRYPTO 1985), Springer LNCS 218,417-4 26, 1985

[10] A. Miyaji. Elliptic Curves over F_p Suitable for Cryptosystems. Advances in Cryptology - AUSCRYPT '92, pp. 479{491, 1993 (Projective plane) J. Edge, "An introduction to elliptic curve cryptography", http://lwn.net/Articles/174127/, 2006.

[11] Neil Koblitz, " An Elliptic Curve implementation of the finite field digital signature algorithm", in Advances in cryptology, (CRYPTO 1998), Springer Lecture Notes in computer science, 1462, 327-337,1998.

[12] Rosing M. "Implementing elliptic curve cryptography", Greenwich, CT: Manning publications, 1999.

[13] William Stallings, "A text book of Cryptography and Network security", Principles and practices, Pearson education, fourth edition, 2007.

****