TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 12593 - 12599

Implementation of Two level Key Exchange Mechanism based on Elliptic Curve Cryptography

Poomagal C T[1]*, Sathish kumar G A[2], Deval Mehta[3]

[1,2]Department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Sriperumbudur,Kanchipuram, INDIA.

[3]SAC, ISRO, Ahmedabad

Article Info
Volume 82
Page Number: 12593 - 12599
Publication Issue:
January-February 2020

Article History

Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 24 February 2020*

Abstract:
The enhancement of communications over the networks for various purposes like IoT, space, military, telecommunication, commercial and consumer electronics encounters numerous challenges concerning the privacy and security paves an ideal and demanding way to design effective public key mechanism, which is to use Elliptic Curve Cryptography(ECC) with indulging more intricate mathematics in the calculation of public-key to formulate the key exchange, digital signature and encryption schemes. This paper proposes an unhackneyed public key cryptosystem that gives all the security imperatives such as privacy, integrity, validity and non-repudiation of the information utilizing the Elliptic Curves. Consequently, the investigations on the proposed work were depicted in terms of security, communication and computational overhead.

Keywords: *ECC, Elliptic curve Discrete Logarithm Problem, Elliptic Curve Diffie-Hellman key exchange, Public key exchange.*

1. INTRODUCTION

At recent times, Elliptic Curve Cryptography (ECC) has evoked more interests towards cryptographers, mathematicians and digital makers around the globe. The essential purpose here is its higher level of security than that of the current cryptographic structures of the public key [1]. The security strength of ECC relies upon the hardness of Discrete Logarithmic Problem. There are three stages associated with exchanging data safely from one node to another over a public system. They are encryption of plaintext to encrypted data, exchange of encrypted data and deciphering it back to the plaintext. The objective of public key cryptography is to model the difficult deciphering operation of the encrypted message to do in a reasonable time by any intruder, except if certain key values are known by them. Ideally, the proposed sender and recipient of a message should know these specific key certainties.

Public key cryptography depends on two keys, a secret key and a public key. The public key is distributed over the communication in which anybody has access to it. Anyhow, every distinct individual node picks a private key that must be known only to that person. The significance of the key to the encryption algorithm is very high, that if the key is lost, it ought to be computationally infeasible to recuperate the plaintext data from the encoded data.

The Diffie-Hellman key exchange mechanism was elaborated in 1976 by the two specialists White Diffie and Martin Hellman in the article [2]. For the basic model of security, it is an efficient panacea for making a common secret key between two nodes of the communications through an unprotected channel. In this algorithm, for the two communicating nodes say Sender(Alice) and Receiver(Bob), a prime number P and a generator of a cyclic group Z_P is chosen. Two secret numbers were chosen for Alice and Bob respectively. Alice computes $K_1 =$

January-February 2020
ISSN: 0193-4120 Page No. 12593 - 12599

$g^a mod\ P$and sends it to Bob, whereas Bob calculates $K_2 = g^b mod\ P$and sends it to Alice. Then, Alice and Bob has to compute the secret key individually that is shared between the corresponding authorities, which is unknown to the intruder using the below given equations (1) and (2).

$$K = {K_2}^a mod P = g^{b\,a} = g^{ab} mod P (1)$$

$$K = {K_1}^b mod P = g^{a\,b} = g^{ab} mod P (2)$$

The effectiveness of this framework depends on the inflexibility of discrete logarithm problem (DLP) understanding which includes in estimation of the common secret key $K = g^{ab} mod\ P$, from $K_1 = g^a mod\ P$ and $K_2 = g^b mod\ P$ without realizing the secret keys a and b. However, the Diffie-Hellman key exchange algorithm is exposed against the man - in- middle attacks [3].

In this work, a new protocol for secured and authenticating key exchange in unsecured channel using the Elliptic Curve (EC) is proposed. This work is based on the idea of the Elliptic curve diffie-hellman protocol with some more enhancements in the computations described in the paper [2]. And the remaining part of this article is portrayed as below: II. Elliptic Curve Cryptography (ECC), III. Background: Elliptic Curve Diffie-Hellman key exchange (ECDH), IV. Proposed Protocol, V. Verification of the proposed protocol, VI. Analysis of the formulated protocol, VII. Conclusion and References

2. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is devised independently by the mathematicians Neal Kobiltz [4] and Victor Miller [5]. It is one of the public key security methods depending on the field arithmetic computations on elliptic curves and Elliptic Curve Hardness Protection Discrete Logarithm Problem. This method is used for encryption of original data and key exchange operations [6]. The primary factor of importance to the ECC contrasting to RSA is that it offers parallel security for a minimum key-size as appeared in TABLE.1.

Table 1. Minimum Key Size for ECC and RSA

Key Size	ECC	RSA/DLP
64 bit	128 bit	700 bit
80 bit	160 bit	1024 bit
128 bit	256 bit	2048-3072 bit

A. *Elliptic* Curve *(EC)*

An algebraic, non-singular curve that can be represented by the generalized Weierstrass equation is the elliptic curve E formed in a finite field is

$$E : \{(x,y)|y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6 = 0\} \cup \{O\} (3)$$

Where $\alpha_1, \alpha_2, \alpha_3, \alpha_4$and $\alpha_6 \in$ E and $'O'$ the point at infinity. In this paper, the analysis is limited to a third-degree elliptic curve over a finite fieldFp as in Fig.1, having the form: $y^2 = x^3 + a.x + b$, where a, b and $4a^3 + 27b^2 \neq 0$, with an additional point O, called the point at infinity.

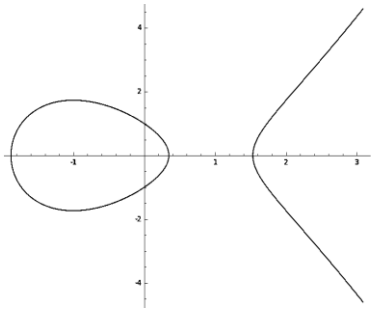

Fig. 1. An elliptic curve of $y^2 = x^3 - 3x + 1$

B. *Field Arithmetic*

Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ be two points on the elliptic curve $Ep(a, b)$ and if $P \neq Q$, then the point addition can be calculated as a third point $P + Q = R(x_3, y_3) \in Ep(a, b)$ is shown in Fig. 2.a.

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad (4)$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \quad (5)$$

January-February 2020
ISSN: 0193-4120 Page No. 12593 - 12599

And if $P = Q$, then the point doubling operator will allow us to calculate a third point $P + P = 2P = R(x_3, y_3) \in Ep(a, b)$ shown in Fig. 2.b.

$$x_3 = \left(3{x_1}^2 - \frac{a}{2y_1}\right)^2 - 2\,x_1 \qquad (6)$$

$$y_3 = \left(3{x_1}^2 - \frac{a}{2y_1}\right)^2 - (\,x_1 - x_3\,) - y_1 (7)$$

Similarly, the vertical points will be added as if $P = -P$, then group operator is $P + (-P) = O$,the point at infinity.

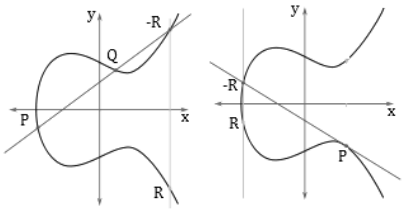

Fig. 2. a.Point addition b. Point doubling

C. *Pointmultiplication* (*scalarmultiplication*)

Let $P(x, y)$ be any point on the elliptic curve $Ep(a, b)$ and k is a large integer. A series of point doublings and additions operation results in the computation of the value k*P gives scalar multiplication value.

$$kP = P + P + P \ldots\ldots \text{ k times} \qquad (8)$$

D. *Elliptic Curve Discrete Logarithmic Problem (ECDLP)*

ECC is based on the problem of ECDLP to predict the estimation of k in the expression $Q = k{*}P$ for the existing points (P, Q) on the given curve$E_P(a, b)$, such that the range of k is less than$p$.

3. BACKGROUND: ELLIPTIC CURVE DIFFIE-HELLMAN KEY EXCHANGE (ECDH)

One of the fundamendal publickey cryptosystems f or secret key sharing is the Diffie-Hellman protocol.

When the sender Alice and the receiver Bob describe a curve $E_P(a, b)$, they also need to decide on the values of the parameters, along with thegenerator point G of the elliptic curve $E_P(a, b)$. At this point they share the private key as in ECDH convention. Sender then chooses a random private key a and estimates the point $a * G$ to send to receiver. Likewise, before sending it to sender, receiver chooses a random secret integer$b$, then estimates the point $b * G$. Now both the party can measure a mutual secret key value $K = abG$. Sender finds K by increasing the given point with its private key a and receiver also finds K by increasing the given point with its private key private key b[7]. If someone who spies on both the parties, as they know $G, aG,$ and bG, and tries to estimate the key value K. The Discrete Logarithm problem on the elliptic curve will eventually be encountered.

4. PROPOSED WORK

In this section, an improved convention of secure and authentic key transport in the open channel is proposed. A key exchange protocol establishes the key to the communicating nodes where one conveying party makes the secret key and moves to other in a secure way. LetE_P (a,b), be the elliptic curve in a field of F_P, where p is the field prime number to be considered for communicating between two parties Alice and Bob. The proposed work is shown in Fig.3.

Step 1: Alice selects two random values α and x in a given field and agreed upon a point G on the given curve. Now it calculates and publishes A as her first level public key or her round 1 Public key as below

$$A = \alpha.G + x.G \qquad (9)$$

Step 2: Bob selects two random values β and y in a given field with an agreed point G on the given curve. Here Bob calculates and publishes B as his first level public key or his round 1 Public key as below

$$B = \beta.G + y.G \qquad (10)$$

Step 3: Alice calculates K_1 and publishes as next level public key specifically for Bob or her round 2 public key as below.

$$K\_1 = (\alpha + x).B + \alpha x G \qquad (11)$$

January-February 2020
ISSN: 0193-4120 Page No. 12593 - 12599

Step 4: Similarly, Bob calculates K_2 and publishes as next level public key specifically for Alice or his round 2 public key as below.

$$K\_2=(\beta+y).A+\beta yG \quad (12)$$

Step 5: Alice's shared secret key is calculated by adding the values of specific public key derived from other nodes with their own private key, which implies that for Alice, she needs to calculate the shared secret key as S as below

$$S=K\_2+\alpha xG \quad (13)$$

Step 6: And for Bob, he calculated as S as below and this value of 'S' will be same for both Alice and Bob, without expelling to the third party intruders.

$$S=K\_1+\beta yG \quad (14)$$

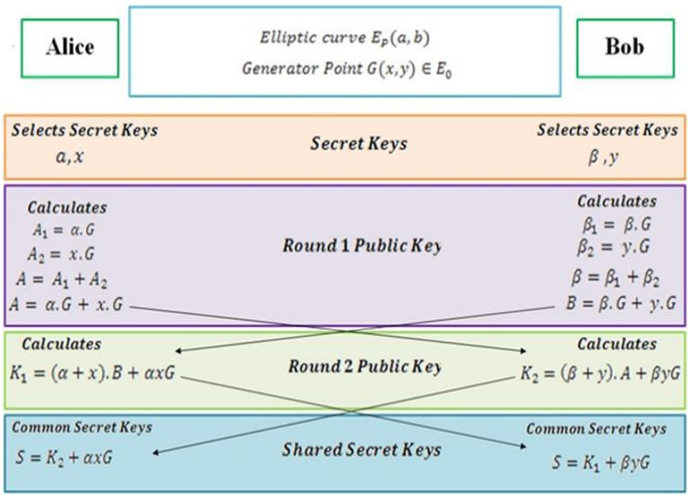

Fig. 3. The proposed key exchange protocol.

5. VERIFICATION OF THE PROPOSED WORK

In the present protocol, every node can communicate with each other in a safe and authentic manner using a secret key; this protection is provided with the support of the complexity of an elliptic curve (ECDLP) discrete logarithm problem. In addition, the particular public key for each group is actualized. The calculation of the specific public key is determined by multiplying each private key by the opponent's public key, which enables us to derive a new convention for exchanging the key that is less harmful to man-in-middle attacks.

The recipient encrypts the key safely with the public key of the receiver, thereby maintaining the security of the secret key. The sender-specific public key of the receiver is used to ensure the secret key's credibility, while its private key is designed to sign the secret key transfer to the receiver digitally.

The below derivation illustrates our proposed protocol and helps to analyse it deeply. An elliptic curve E can be defined over Fp. In the Initial phase, Alice and Bob selects the two secret keys α,x and β,y respectively. Now they calculates and exchange the Round 1 Public key as A= α.G+ x.G and B=β.G+ y.G respectively.

At next level, Alice and Bob calculate and exchange the Round 2 Public key as K_1=(α+x).B+αxG and K_2=(β+y).A+βyG respectively.

Correctness at Round 2 key:

At Alice Side: K_1=(α+x).B+αxG

$$K\_1=(\alpha\beta.G+ \alpha y.G+x\beta.G+ xy.G)+\alpha xG \quad (14)$$

At Bob Side: K_2=(β+y).A+βyG

$$K\_2=(\beta A+yA)+\beta yG$$

$$K\_2=(\beta\alpha.G+\beta\, x.G+y\alpha.G+yx.G)+\beta yG \quad (15)$$

Finally Alice and Bob calculates secret shared key separately as 'S'.Hence the correctness for Shared Secret key is given by

At Alice side: S=K_2+αxG

$$S=(\beta\alpha.G+\beta\, x.G+y\alpha.G+yx.G)+\beta yG+\alpha xG \quad (16)$$

At Bob Side: S=K_1+βyG

$$S=(\alpha\beta.G+ \alpha y.G+x\beta.G+ xy.G)+\alpha xG +\beta yG \quad (17)$$

The equation (16) and (17) clearly shows that the shared secret key calculated by Alice and Bob are same. So this key value can be utilized as a secret key for next level of key exchange or encryption of data through a public channel. Hence, the verification for the proposed key exchange protocol was done and the secret key is shared without revealing to the third party intruder.

The proposed work is implemented and simulated to verify the correctness of the algorithm and the same is evaluated with the standard NIST curve on sample text data. For the curve NIST P-256 having the parameters of prime P=257; a=-3; b=41058363725152142129326129780047 2

January-February 2020
ISSN: 0193-4120 Page No. 12593 - 12599

6840911444101599372555483525631403946740129 1 forms the Elliptic curve equation

$$y^2 = x^3 - 3x$$

+4105836372515214212932612978004726840911444101599372555483525631403946740129 1(mod257) …..... (18)

And the generator point and random secret key values chosen are E= [255, 36]; x=9; y=8 with results of the proposed algorithm is explicated in Fig. 4 as public key and shared secret key calculations.

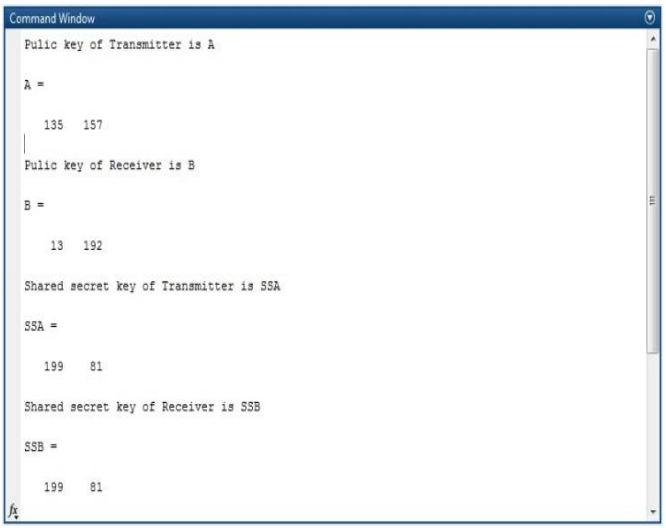

Fig. 3. Simulation output for the proposed work

6. ANALYSIS OF THE PROPOSED WORK

The implementation of the proposed work can be used to analyse the optimality of the algorithm re-garding time complexity, computational delay and overhead requirements; Key exchange protocols are shown to allow at least two authorized parties to communicate through an open communication channel with a common and asymmetrically secret key which may successively utilized to achieve certain crypto-graphic goals such as confidentiality or data integrity. Secure and validated key exchange conventions are important as a reliable substitute for traditional key exchange methods to resolve the certain important se-curity attributes [10] and the comparison of the security parameters concerning with different protocols are shown in the table 1.

The computational attributes of the proposed algorithm can be drafted with the calculation of counting the usage of number of point additions and scalar multiplication operation for the given protocol and it is clearly shown in table 2 with the comparison of existing protocols.

The computation time of the presented algorithm and other related algorithm is calculated based on the finite field operations viz point addition, scalar multiplication, field inversion and hash operation. An ECC scalar multiplication requires 0.063075 seconds [12-14], field inversion takes 0.007565 seconds and point addition takes 0.021seconds [15]. And the hash function requires 0.00032 seconds. In this paper, the computation time for normal multiplication operation can be neglected, which involves negligible time du-ration than the other operations. In table 3, the gross computation time for all the operations of related pro-tocols and the proposed protocol are depicted with the notations as TPA TSM TFI TH which denotes the computation time requires for Point Addition, Scalar Multiplication operation, Field Inversion, Hash func-tion respectively. The protocol in [17] and [18] takes more time than the proposed algorithm and the tech-niques used in [16] takes lesser time than the proposed one but lags more in security. So the proposed key exchange protocol works well with two rounds of key exchange using field arithmetic operations only.

Table 1. Comparison of Security Attributes

Parameters/Protocols	*Proposed Work*	*Wang et al Protocol[16]*	*Strangio Protocol[17]*	*Song et al Protocol[18]*
Implicit Key authentication	Yes	Yes	Yes	No
Known-key security	Yes	Yes	Yes	Yes

January-February 2020
ISSN: 0193-4120 Page No. 12593 - 12599

Forward secrecy	Yes	Yes	Yes	Yes
Unknown key-share	Yes	Yes	Yes	Yes
Key-compromise impersonation	Yes	Yes	No	No
Update Shared Secret Key	Yes	No	Yes	Yes

Table 2. Comparison of Computational Attributes

Operations/Protocol	*Proposed Work*	*Wang et al Protocol[16]*	*Strangio Protocol[17]*	*Song et al Protocol[18]*
Point Addition	3	0	0	0
Scalar Multiplication	3	3.5	5	4
Field Inversion	0	1	0	0
Hash Function	0	2	2	0

Table 3. Computational Cost Analysis

Parameters/Protocol	*Proposed Work*	*Wang et al Protocol[16]*	*Strangio Protocol[17]*	*Song et al Protocol[18]*
Total Computation cost for all the operations of the protocols.	$3T_{PA}+3T_{SM}$	$3.5\ T_{SM}+1T_{FI}+2T_H$	$5\ T_{SM}+2\ T_H$	$4\ T_{SM}$
Computation cost (in Secs)	0.2522	0.2289675	0.316015	0.2523

From this analysis, the future optimization can be done for the better performance of the proposed protocol. Also, The aim of scientists is to find a practical and secure approach for public key cryptosystems even in the most complex environments, while maintaining the speed and lesser size of these cryptosystems.

7. CONCLUSION

This paper proposes a novel protocol of secure key transport of two rounds in public channel using the Elliptic Curve. Public-key cryptography gives a resolution for both the secure key administration and secure information interchanging. ECC's security is based on the problem of Elliptic Curve Discrete Logarithm Problem (ECDLP) using ECC key exchange, i.e. the device can guarantee confidentiality, secrecy, validation and non-repudiation. Additionally, we can infer that the proposed protocol is robust. In future works, The exchange of public keys and specific public keys suggested in this paper can be used to encrypt and decrypt messages by ensuring the validity of the message in order to ensure that the Elliptic Curve Discrete Logarithm problem (ECDLP) is protected by an asymmetric cryptosystem.

REFERENCES

1. O. Reyad, Z and Kotulskil, “On Pseudo-Random Number Generators Using Elliptic Curves and Chaotic Systems”, International Journal Appl. Math. Inf. Sci. 9, No. 1, 31-38 (2015).
2. W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, IT-22 :644-654, Nov 1976.
3. M. Johnston, P. S. Gemmell, “Authenticated key exchange Provably Secure Against the Man-in-Middle Attack”, Journal of Cryptology, Springer , 2002, Vol. 15 Number 2 pages 139-148.
4. N. Koblitz,“Elliptic curve cryptosystems,” Mathematics of Compution, Vol. 48, No.177, pp.203-209, Jan 1987.
5. V.S. Miller, “uses of elliptic curves in cryptography,” in Advances in Cryptology,

January-February 2020
ISSN: 0193-4120 Page No. 12593 - 12599

CRYPTO'85, Lecture Notes in Computer Science, vol. 218, Springer, 1986. pp. 417-428. 5. N.

6. J. Menezes and S.A. Vanstone, "Elliptic Curve Cryptosystems and their implementations", Journal of Cryptology, Springer, 1993, Volume-6, Number-4, pages 209-224.
7. Diffie–Hellman key exchange (2019) Available from: https : //en.wikipedia.org/wiki/Diffie
8. W. Stalling, Cryptography and Network Security, Principles and Practice, 5th edition New Jersey: Prentice Hall, 2011.
9. E.-J. Yoon and K.-Y. Yoo, "Cryptanalysis of a simple three party password-based key exchange protocol," International Journal of Communication Systems, vol. 24(4), pp. 532–542, 2011.
10. C. Paar, and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, 1st ed. Springer Publishing Company, 2009.
11. S. Tavares and H. Meijer, "Authenticated Diffie Hellman Key Agreement Protocols", SAC'98, Springer-Verlag Berlin Heidelberg, LNCS 1556, pp. 339-361, 1999.
12. Li C.-T, Hwang M.-S, and. Chu Y.-P, 2008, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Computer Communications. 31(12): 2803–2814.
13. Lee J.-S and Chang C.-C, 2007, "Secure communications for cluster based ad hoc networks using node identities," Journal of Network and Computer Applications. 30(4): 1377– 1396.
14. Li W.-M, Wen Q.-Y, Su Q and Jin Z.-P, 2012, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," Computer Communications. 35(2): 188–195.
15. Zhi Li, John Higgins, M Clement, "Performance of Finite Field Arithmetic in an Elliptic Curve Cryptosystem", MASCOTS 2001, IEEE Xplore, August 2002.
16. S Wang, Z Cao, M A Strangio, L Wang, "Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol," IEEE Communications Letters, Vol. 12(2), February 2008.
17. M. A. Strangio, "Efficient Diffie–Hellmann two-party key agreement protocols based on elliptic curves," in Proc. 20th ACM Symposium on Applied Computing (SAC), pp. 324-331, 2005.
18. B. Song and K. Kim, "Two-pass authenticated key agreement protocol with key confirmation," in Proc. Indocrypt'00, LNCS 1977, pp. 237-249, 2000.