International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Secure e-Commerce Transactions using ElGamal Elliptic Curve Cryptosystem

Srishti Sharma

IIT ISM DHANBAD, Jharkhand, Computer Science Engineering with Spl. in Information Security (2016-18)

Abstract: ***Security of e-commerce transactions is a pre-requisite requirement nowadays as it is being used in almost every day to day lives. Large amounts of information are exchanged between users every time we do some online transaction. Active attacks like eavesdropping / replay attacks are threat to customer's money. Eavesdropping attack is the unauthorized interception of a private communication, such as phone call or message. Hence it is very much important that any good electronic commerce system should guarantee some basic securities such as authenticity, data protection, privacy and integrity. Elliptic curve cryptography (ECC) compared to RSA provides same cryptographic strength but with much shorter key size and also provides moderately fast encryption and decryption. Another issue with e-commerce transactions today is whether the two parties are authenticated. This becomes a weak link and leads to fraud and cyber thefts. To remove the above problem, we combine ECC with ElGamal encryption scheme. In this project, we suggest enhanced security model of cryptographic system using Elgamal encryption scheme with ECC. This mode can be used as a Secured electronic transaction set (SET) . It also gives better security with lesser key size.***

Keywords: e-commerce, secured electronic transaction(SET), Elliptic Curve Cryptography (ECC), ElGamal, Diffie Hellman Key Exchange.

1. Introduction

Nowadays, all e-commerce transactions are done through ATM or debit cards, credit card, online transfer or internet banking [1]. Electronic commerce or e-commerce is used for any type of transaction that involves the transfer of confidential information across the Internet. It is right now one of the most important aspects of the Internet. Computer networks provide platform to do e-commerce tasks, online banking and sharing of secret information and many more within a few seconds across the globe. It uses the world wide web to share all the information required to do all e-commerce tasks. While on one hand it is making our lives easier, it is also creating threats that could be disastrous. All the information shared should be confidential and secured from the attackers. While communicating with each other both the user and the merchant have issues regarding confidentiality, data authentication and non-repudiation. [3] The leakage or even the attack on these information may lead to frauds, thefts, spamming, etc. The personal information can be stolen including the person's name, social security number, birth date or credit card numbers. This stolen information can be then used to obtain new credit cards, debit cards, access anyone's merchant accounts or thefts. This model is used as a Secured electronic transaction set (SET). [4]

Hence, the security is required for two important purposes. They are,
(i) To preserve user's privacy
(ii) To preserve against fraud. [2]

A message is communicated between the two parties in an e-commerce transaction, to authenticate client and to avoid attacks like eavesdropping / replay attacks. The merchant and the buyer both are registered with the certificate authority. In order to transfer money from user's account to seller's account, a message is sent to the user by the merchant in order to authenticate him. This message is valid for only one transaction i.e. for every new transaction, a new message will be generated every time. As this message is also communicated through an insecure channel, it must also be protected. If the message itself gets attacked then there might be chance of attacking the current transaction and merchant account of the user. For this purpose, the message generated is encrypted by the sender and then sent through the channel. The client decrypts the cipher message and sends to the merchant for authentication. The merchant validates the message. If it is same then the transactions is executed otherwise , transaction is cancelled.. In this model, security of message is provided with shorter key length as compared to RSA (Rivest - Shamir - Adleman) using ECC (Elliptic curve cryptography). It offers higher security per bit with smaller key size.[5]

Also Elliptic Curve DiffieHellman(ECDH) is used to establish session key between the merchant and the user.[6] This session key is used while encryption of the message. This key is used for the parties having no prior knowledge of each other.

This research article has been organized as follows. Section - II describes related work. Section - III describes SET. Section - IV explains details of ECC. Section - V explains ElGamal encryption scheme. Section - VI explains proposed model. Section - VII gives results and Section - VIII describes conclusion.

2. Related Works

Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to do the attack on the channel. So the only secure way of exchanging keys would be exchanging them personally which is not very practical method. Therefore, better solution is to use asymmetric cryptosystems. Both the users have their own private keys and public keys

Many algorithms have been used for asymmetric encryption like diffie-hellman key exchange which establishes the key between two users and then establishes connection.[6] But the disadvantage with this algorithm is that it suffers from Man-in-the-middle attack. If once the attacker establishes connection between the two users he/she may receive every message passing through that transaction. Certificates and digital Signatures can be used to overcome this attack.

Many researchers have performed the implementation of cryptographic keys using biometric keys also for authentication of the users. The biometric keys are first generated and then used whenever the message is sent to that user. If the user is authenticated and uses his correct private key then he will be able to decrypt the cipher-message and send back to the merchant.[7] This system requires that the user is registered with the merchant first.

3. Secured Electronic Transaction (SET)

SET is a security protocol for an electronic payment system. It was invented by Visa and MasterCard in 1996.[8] A number of security experts predicted that SET would become a standard for e-commerce payment system.

Today electronic transactions have become a part of our daily life. The information shared over the network every time we do a transaction needs to be protected from the eavesdropper. It is necessary to prevent the privacy of the customer and prevent malicious activities which can lead to loss and theft of customer's money. It is major requirement that a good cryptographic system must guarantee authentication, confidentiality, integrity and data protection. For this the details of a transaction must be kept secret and valuable data should be protected.

The main requirements for SET are -

- To provide security, authentication, integrity and privacy with regard to confidential information.
- To provide authentication of both the merchant and the customer that they are authenticated bank account holders.
- To provide authentication that a merchant can accept the transactions.

1) ECC

ECC was proposed by two authors Neil Koblitz [9] and Victor S. Miller [10] in late 1985. ECC algorithms are public key algorithms that provide the same security as RSA algorithms but with shorter key size. Elliptic curve cryptography (ECC) is based on theorized discrete logarithm problem (DLP). The security of elliptic curve cryptography is based on hardness of elliptic curve discrete logarithm problem (ECDLP). ECC with 160 bit provides same security as RSA with 1024 bit and ECC with 224 bit provides security as equal as provided by RSA with 2048-bit. ECC needs lesser memory than other asymmetric cryptography. It provides greater level of security due to its complex mathematical operations. It is considered as essential techniques for cryptographic purposes because of the complexity and hardness of mathematical formulas used in ECC.

Table 1: RSA and ECC public key length (in bits)[11]

Security Bits Level	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

a) Mathematics behind ECC

There are two types of elliptic curves used for cryptographic purposes,

1. Elliptic curve over GF (2^m)
2. Elliptic curves over Z_p.

For cryptographic use, we need to consider the curve over the finite fields. For elliptic curves over Z_p, all arithmetic is performed modulo a prime p.

Definition: The elliptic curve over Z_p, $p>3$, is the set of all pairs $(u, v) \in Z_p$ which fulfill

$$v^2 = (u^3 + a \cdot u + b) \bmod p \quad \text{(i)}$$

with an imaginary point of infinity o, where $a, b \in Z_p$ and the condition

$$(4 \cdot a^3 + 27 \cdot b^2) \neq 0 \bmod p . \quad \text{(ii)}$$

The definition of elliptic curve requires that the curve is non - singular i.e. the plot has no self-intersections or vertices.

b) Elliptic curve Point addition and Point doubling

$$u_3 = s^2 - u_1 - u_2 \bmod p$$
$$v_3 = s(u_1 - u_3) - v_1 \bmod p$$

where,

$$s = \{(v_2 - v_1) / (u_2 - u_1)\} \bmod p$$
$$s = \{(3 (u_1)^2 + a)\} / 2 v_1) \bmod p$$

c) Mathematical Rules in ECC

1. Rules for addition over $E_p(a, b)$, for all points $A, B \in E_p(a, b)$, [9], [10].

Rule 1 : A + o (infinity) = A

Rule 2 : If point $A= (u_1, v_1)$, then $A + (u_1, -v_1) = o$.

Rule 3 : If $A = (u_1, v_1)$ and $B = (u_2, v_2)$, with $A \neq -B$, then $C = (u_3, v_3)$ is calculated as,

$u_3 = (t - u_1 - u_2) \bmod p$

$v_3 = \{t(u_1 - u_3) - v_1\} \bmod p$

where, $t = \{(v_2 - v_1) / (u_2 - u_1)\} \bmod p$, if $A \neq B$

and $t = \{(3 (u_1)^2 + a\} / 2 v_1) \bmod p$, if A = B.

2. Rules of multiplication is defined as repeated addition.

Let, $A = (u_1, v_1)$ be a point on elliptic curve.

Then , $8 * A = A + A + A + A + A + A + A + A$

$= 2 * A + 2 * A + 2 * A + 2 * A$

$= 4 * A + 4 * A.$

d) Points on ECC

The points on the elliptic curve together with o(infinity) have cyclic subgroups . Under certain conditions all points on an elliptic curve form a cyclic group. To do any calculation on the curve, all points on the curve must be calculated. [13]

- First find the left partvof the elliptic curve for all $(u, v) \in Z_p$.
- Then find the right part of the elliptic curve for all $(u, v) \in Z_p$.
- Choose the values of x and y as a pair for all $u, v \in Z_p$ for which left part is equal to the right part.

- All the selected pairs of values of (u , v) will be the points on elliptic curve.

e) Elliptic curve Diffie- Hellman Key exchange (ECDH)

A key exchange can be encountered using diffiehellman key exchange. This is alluded as Elliptic curve diffiehellman. [12], [5].

Let there be two users Alice and Bob. According to ECDH, the key generation and exchange of keys is done as follows:

- Alice has her private key, d_A.
- Alice calculates his public key, $P_A = d_A * G$.
- Bob has his private key, d_B.
- Alice calculates his public key, $P_B = d_B * G$.
- Alice sends her public key to Bob and Bob sends his public key to Alice.
- Session key is generated on Alice side, $Sk = d_A * P_B$.
- Bob creates the session key, $Sk = d_B * P_A$.

2) ElGamal Encryption Scheme

Elgamal is a probabilistic encryption scheme, i.e. encrypting two identical messages does not yield two identical ciphertexts. It is an extension of DHKE where derived session key is used as multiplicative masked to encrypt a message.[12], [15]

Elgamal encryption is performed in three parts. The set up part is executed one time by the side who issues the public key and will receive the message. The encryption and decryption parts are executed every time the message is sent. As compared to DHKE, no trusted third party is needed to choose a prime and a primitive element.

1) Receiver chooses a large prime p.
2) Receiver chooses primitive element $\alpha \in Z_p$.
3) Receiver chooses a private key $d_b \in \{2,... , p-2\}$
4) Receiver computes his public key , $P_b = \alpha^{db} \bmod p$ and sends to Sender.
5) Sender chooses its private key ,$i \in \{2, . . . , p-2\}$
6) Sender computes its ephemeral key , $K_e = \alpha^i \bmod p$
7) Computes the masking key , $K_m = P_b^i \bmod p$ and encrypts the message , $y \equiv x \cdot K_m \bmod p$ and sends it to Receiver.
8) Receiver computes the masking key, $K_m = K_e^{db} \bmod p$
9) Receiver decrypts the ciphertext , $x \equiv y \cdot K_m^{-1} \bmod p$.

Proposed Model

The architecture of proposed model is shown in figure 1. In this paper we are using DHKE to establish the session key between two users and then encrypt the message to be sent using this session key ElGamal encryption scheme with elliptic curve cryptography.

a) Architecture of proposed model

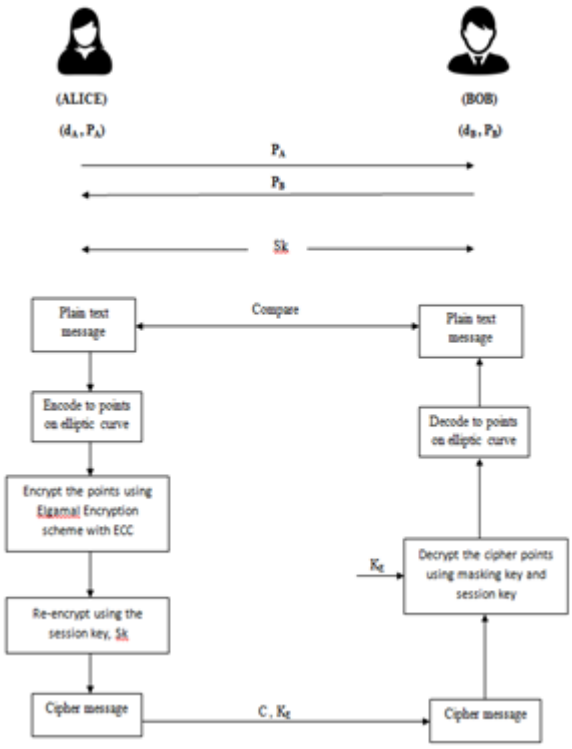

Figure 1: Architecture of proposed model

b) Steps of proposed methodology

The steps of proposed methodology are as follow:

- The user selects the item to be purchased and sends the details to the merchant.
- The merchant and the user then establishes a session key between them.
- The merchant then calculates the ephemeral key and the masking key.
- The encryption module on the merchant's side encrypts the plaintext message using the masking key and re-encrypts the message using the session key established.
- Cipher message along with the ephemeral key is sent to the user.
- The user calculates the masking key using his private key and the ephemeral key.
- The decryption module on the user side decrypts the cipher message and the plaintext message is generated.
- The plaintext message generated is entered as input for the transaction verification.
- If the entered message is same as original message generated for the transaction, then the transaction gets executed successfully, else transaction is cancelled.

c) Message Encryption

The message to be encrypted is in text form and to do encryption on elliptic curve the points are required on the elliptic curve. The plaintext message M, is first encoded as points P_m (x, y) on the elliptic curve. These points are then encrypted. The mapping algorithms are used for encoding. We use the basic scheme to map the plaintext to a point. [16] Given below are the steps for message encryption:

1. The plaintext message is encoded as points on elliptic curve, using the mapping scheme. The ASCII value of the characters of the plaintext is multiplied with the base point G of the elliptic curve.

$$P_m (x, y) = ASCII * G (x, y)$$

2. Ephemeral Key, K_E is calculated using some random number i and G,

$K_E = i * G (x, y)$

3. Masking Key is calculated using the public key of the user,

$K_M = i * P_B(x, y)$

4. The encoded point is then encrypted using the masking key and the session key already established.

$C_m = P_m + K_M$

$C = C_m + Sk.$

i. Message Decryption

1. The user calculates the making key K_M using the ephemeral key.

$K_M = d_B * K_E$

2. Using the masking key and the session key, user decrypts the cipher message,

$= C- K_M - Sk$

$= C_m + Sk - K_M - Sk$

$= P_m + K_M + Sk - K_M - Sk$

$= P_m .$

4. Results

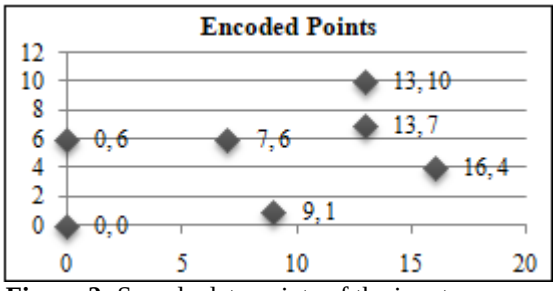

Figure 2: Sample data points of the input message

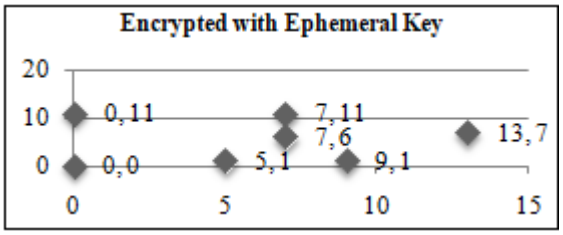

Figure 3: Encrypted data points

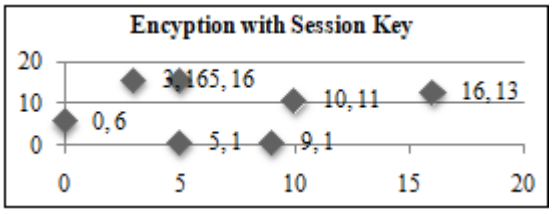

Figure 4: Encrypted points with session key

As we are using ECC, we are able to achieve high level of security with shorter key size. Thus it solves the key size problem. Also, ECDH suffers from Man-in-the-middle attack (MITM), which is solved using Elgamal encryption scheme. ECC requires very complex mathematical operations and ECDH which is more difficult to break than discrete logarithmic problem. Therefore, the strength of security of this model is very high.

5. Conclusion

In this paper, a very secured communication of message in network is given with the help of ECC with ElGamal encryption scheme. High level of security with shorter key length is the main advantage of ECC. Also Elgamal encryption scheme helps to avoid MITM attack. In today's world everything is on internet and hence e-commerce is growing very fast. Security of confidential information passing through the network needs to be protected. The proposed model strengthens the security of the e-commerce transaction systems. The proposed model can also be used in any other type of secure data communication system. It can also be used in secured electronic transaction system (SET).

References

[1] S.G.E. Garrett and P.J. Skevington. An introduction to electronic commerce. *BT Technology Journal*, 17(3):11–16, 1999.

[2] Ganesan R. and Vivekanandan K. A secured hybrid architecture model for internet banking (e-banking). *Journal of Internet Banking andCommerce*, 14(1):1–17, 2009.

[3] S. Mohammadi and S. Abedi. ECC-based biometric signature: A new approach in electronic banking security. In *Electronic Commerce andSecurity, 2008 International Symposium on*, pages 763–766, Aug 2008.

[4] Nikhil Khandareand Dr. B. B. Meshram. SECURITY OF ONLINE ELECTRONIC TRANSACTIONS *International Journal of Technical Research and Applications* ISSN: 2320-8163.

[5] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Recommendation for key management part 1: General (revision 3). *NIST SpecialPublication 800-57*, pages 1–147, July 2012.

[6] W. Diffie and M.E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, Nov 1976.

[7] DindayalMahto andDilip Kumar Yadav..Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Biometrics for E-Commerce Applications. 978-1-4799-4445-3/15/$31.00 c2015 IEEE.

[8] Pita Jarupunphol and WipawanBuathong. Secure Electronic Transactions (SET): A Case of Secure System Project Failures. *IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2, April 201*.

[9] Koblitz N. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[10] Victor S. Miller. Use of elliptic curves in cryptography. In HughC. Williams, editor, *Advances in Cryptology CRYPTO 85 Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer Berlin Heidelberg, 1986.

[11] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid, Recommendation for key management part 1: General (revision 3), NIST Special Publication 800-57 (2012) 1- 147.

[12] ChristofPaar and Jan Pelzl. Understanding Cryptography. *Springer*

[13] Ren Schoof and Par Ren E Schoof. Counting points on elliptic curves over finite fields. *Journal de Theorie des Nombres de Bordeaux 7*, pages 219–254, 1995.
[14] MEL H.X. and BAKER D. Cryptography decrypted. In *Oxford Handbook of Innovation*. Addison Wesley; 1 edition, Oxford, 2000.
[15] Andreas V. Meier. The ElGamal Cryptosystem. June 8, 2005.
[16] AritroSengupta* and Utpal Kumar R. Message mapping and reverse mapping in ellipticcurve cryptosystem. SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2016; **9**:5363–5375Published online 22 November 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1702