International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 8; August 2017; Page No. 5338-5342
DOI: http://dx.doi.org/10.24327/ijcar.2017.5342.0701

Research Article

ENHANCING E-COMMERCE SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY

Javed R. Shaikh[1], Ravinder Kumar[2]*, Maria Nenova[1], Georgi Iliev[1] and Hitesh Singh[2]

[1]Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria
[2]Department of Computer Science and Engineering, HMR ITM, Affiliated with GGSIPU, Delhi, INDIA

A R T I C L E I N F O

Article History:

Received 19th May, 2017
Received in revised form 5th
June, 2017 Accepted 16th July, 2017
Published online 28th August, 2017

Key words:

E-commerce security; SSL; RSA; ECC; ECDLP.

A B S T R A C T

Over the past few years, the percentage of customers using electronic commerce (E-commerce) is increasing rapidly. E-commerce transaction security is a major concern for E-commerce websites along with its customers. The basic requirements for any E-commerce transaction are privacy, authentication, integrity and non-repudiation. To fulfil the E-commerce security requirement mentioned above, Rivest, Shamir, and Adelman (RSA) cryptography algorithm is widely used. In case of RSA with security requirement, key size is increasing proportionally. Large key size in RSA makes it inappropriate in environments where processing speed, storage, bandwidth, or power consumption is a major constraint. Due to these limitations of RSA algorithm, a new public key cryptography scheme known as the Elliptic Curve Cryptography (ECC) is emerging as a good option for RSA. In this paper ECC performance is analyzed in terms of computation time taken by elliptic curve when used for the ECC application. For the analysis of ECC different key sizes are considered. This paper explains by comparison how ECC is better than the traditional RSA. To improve the security in E-commerce business general security model is proposed by considering the ECC. The proposed E-commerce system is suitable in the constrained applications which have computation speed, bandwidth and storage as its major constraint. In proposed security model along with the payment information, customers purchase order information is also secured.

INTRODUCTION

The E-commerce market has grown exponentially over the last few years. As mentioned earlier the major requirements for any E-commerce transaction are privacy, authentication, integrity and non-repudiation [1]. According to most of the surveys, insecurity of financial transactions and loss of privacy are the major issues of concerns for electronic commerce users, but in fact, most users don't have much idea about the threats and risks in E-commerce. As a result, all kinds of misperceptions exist amongst the customers.

The protection of E-commerce data from unauthorised access, its alteration, or destruction is the primary task in providing E-commerce security. All these are achieved through various cryptographic techniques which helps to transmit secret information over insecure channel safely. Cryptographic techniques are broadly classified into two types as, the symmetric key (Private key) cryptographic techniques and asymmetric key (Public Key) cryptographic techniques (RSA, ECC). Most of the E-commerce applications use RSA algorithm to encrypt and decrypt the secret key. In Secure Socket Layer (SSL) / Transport Layer Security (TLS) protocols RSA is the most commonly used public key cryptosystem. As cryptanalysis is getting better day by day, it requires that both symmetric and public key size to increase proportionally to provide better security. As explained in [2] RSA is vulnerable to many attacks such as Integer Factoring Attacks, Wiener's Attack, Hastad Broadcasting Attack, etc. For RSA algorithm NIST has recommended to use key-size of 2048 bit till year 2030 and recommends increasing the key size to 3072 bit after that for better security [3]. The effectiveness of brute-force attacks has improved considerably on the RSA cryptosystem, with the noticeable impact on the choice of RSA modulus sizes [4].

The reason behind popularity of ECC is, with the minimum key length it provides more security than RSA. ECC requires 160-bit key length compared to 1024 bit key length of RSA and provide the same level of security [1]. Therefore, in this research work, ECC asymmetric key technique is analyzed as an alternative for RSA.

Overview of SSL/TLS Protocol

The SSL protocol which is just network data security protocol, designed and developed by the Netscape communication company. At present, the SSL protocol applies RSA public key cryptosystem to realise identity

Corresponding author:* **Ravinder Kumar
Department of Computer Science and Engineering, HMR ITM, Affiliated with GGSIPU, Delhi, India

authentication and key negotiation in most applications [5]. The main goal of SSL is to provide a reliable security service of a point to point based on Transmission Control Protocol (TCP), it also increase the security of data transmission between two application programs.

SSL and TLS are security protocols which are used to enable privacy between two applications. The public key technologies are used by the SSL to provide confidentiality and reliability of communications between the two applied processes. There are two sub-protocol layers in the architecture of the SSL, the one is the SSL Record Protocol Layer, and the second is the SSL Handshake protocol layer.

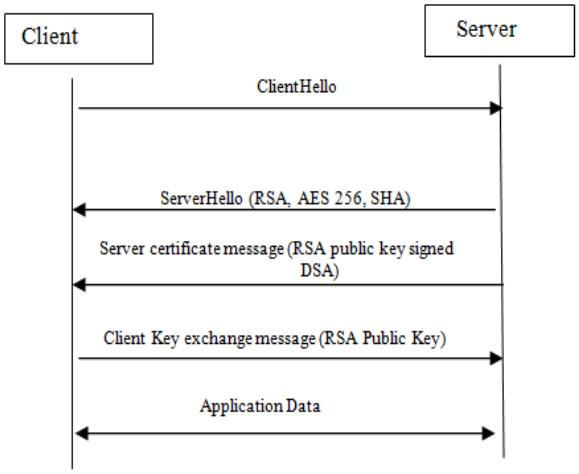

Fig 1 SSL handshake algorithm

SSL protocol is mainly used in HTTP but also utilised for other protocols like FTP and SMTP. ECC was first included in this protocol with the release of TLS 1.0 [3]. Fig.1 shows the SSL handshake algorithm during the information exchange which uses the RSA as a public key cryptographic system. The SSL handshake can be computationally expensive in cases where a mobile client is present. In SSL handshake algorithm RSA is used between a client and server to exchange the private key and to provide confidentiality, digital signatures and authentication [3].

Introduction to RSA

RSA is the public key cryptography system proposed in 1977. It is named after its inventors Rivest, Shamir, and Adleman. The pair of integers (n, e) forms the public key where the RSA modulus n is a product of two randomly generated prime numbers p and q of the same bit length (n=p*q). The e is encryption exponent which is integer, satisfys condition $1 < e < \varphi$ *and gcd* $(e,\varphi) = 1$,where $\varphi = (p-1)*(q-1)$.

The integer d is private key satisfying conditions $1 < d < \varphi$ *and* $e*d \equiv 1 \pmod{\varphi}$.The problem of finding the private key d from the public key (n, e) is equivalent to the problem of calculating the factors p and q of modulus n. RSA encryption and decryption is performed by using following schemes.

If m is the message which needs to be encrypted, then encryption is done by using equation,

$$c = m^e \bmod n \quad (1)$$

Where, m-Message to be encrypted.
c- Ciphertext.
e- Encryption key.

For the decryption of the message, the following formula is used in RSA.

$$m = c^d \bmod n \quad (2)$$

Where, d- Decryption key.

Computing $m^e \bmod n$ during encryption and $c^d \bmod n$ during decryption is computationally expensive step in RSA. To increase the efficiency of RSA encryption and signature verification, a small value of e is preferred, in practice, e = 3 or $e = 2^{16} + 1$ is commonly chosen [6].

Introduction to Elliptic Curve Cryptography

Neal Koblitz and Victor Miller discovered the Elliptic curve cryptography (ECC) in the year 1985. Elliptic curve cryptographic system is type of public-key cryptographic scheme which provides the same level of security as RSA schemes but with less key size. The security of ECC is dependent on the hardness of the elliptic curve discrete logarithm problem (ECDLP).

Elliptic Curve Systems **[6]**

Abelian Group

An abelian group is also known as the commutative group is the type of grupp where result of any operation on two group element does not depend on the order of elements. The abelian group satisfies the various group properties such as associativity, commutativity, existance of an identity and existance of inverse

The operations performed in the group are usually called addition (+) or multiplication (·). In the additive group, identity element is usually denoted by 0, and −a denotes the inverse of a. In the second group which is a multiplicative group, the identity element is usually denoted by 1, and a-1 denotes the inverse of a. The number of elements in G is called the order of G. The groups which are generally used for implementing discrete logarithm systems are the cyclic subgroups a finite field and cyclic subgroups of elliptic curve groups[6].

Elliptic Curve Groups

Consider an elliptic curve E over Fp, Where p is a prime number, and Fp denote the field of integers modulo p. Then elliptic curve E over Fp is defined by an equation of the form,

$$y^2 = x^3 + ax + b \quad (3)$$

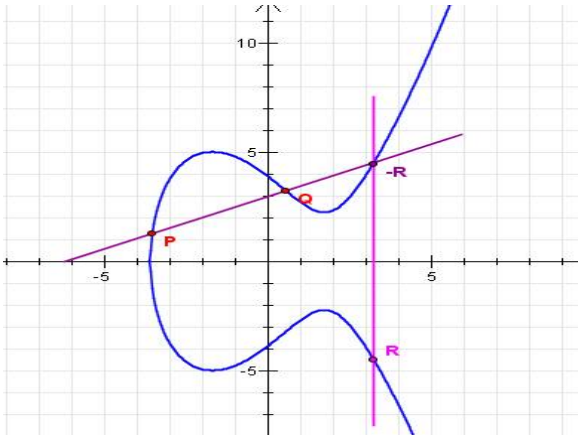

Fig 2 Elliptic Curve showing the addition of two points on the curve

where a, b ∈ Fp and satisfy the equation $4a^3 + 27b^2 \equiv 0 \pmod p$. Any point is said to be on the curve if its coordinates satisfies the equation 3.The standard formulas are there to add two elliptic curve points P = (x1, y1) and Q = (x2, y2) to produce a third point R which is on the elliptic curve. The addition rule requires a few arithmetic operations in finite field Fp. With this addition rule, the set of points E (Fp) forms an additive Abelian group with ∞ serving as the identity element. Cyclic subgroups of such elliptic curve groups can now be used to implement discrete logarithm systems [6]. Fig.2 demonstrates how the addition of two points takes place on an elliptic curve.

Elliptic Curve Discrete Logarithm Problem

Given an elliptic curve E defined over Fq. Consider two points P and Q are from the curve E. Find an integer x such that Q = xP, is the Elliptic curve discrete logarithm problem (ECDLP). ECDLP is considered as more difficult to solve than the various factorization problems and general discrete logarithm problem that are used in other cryptosystems. In fact, nobody knows exactly how difficult ECDLP problem is to solve because no effiecient algorrithm is available to solve it [7]. The required key sizes of RSA cryptographic systems rise exponentially with increase in difficulty, while in elliptic curve systems the increase in required key size is relatively less. If ECC cryptosystems is implemented then it can be cracked only by solving ECDLP, so using this system Bob and Alice's can exchange their messages securely.

To understand how ECC works let us consider The ElGamal elliptic curve cryptosystem. Consider one elliptic curve E defined over a finite field Fq where $q = p^n$ is large and p is a prime number. Suppose that E, q, and a point G which is on the curve E are publicly known. P is the point on which information message m is embedded (m→Pm).

When Alice wants to communicate secretly with Bob, they proceed as explained below [7].

- Bob chooses a random integer b which is secret and publishes the point bG .
- Alice chooses her own random integer a which is secret and sends the pair of points (aG, Pm+a(bG)) to Bob.
- To decrypt the message, Bob calculates the equation to get Pm and then reverses the embedding to get back the message m.
- $Pm + a(bG) - b(aG) = Pm + abG - abG = Pm,$
- Eve, who can only see bG, aG, and Pm + a(bG) must find a or b by making sense of Pm + a(bG), so her problem is reduced to the ECDLP.

Elliptic Curve Encryption and Decryption Scheme

Key generation in ECC

Consider elliptic curve E defined over a finite field Fp. Let P be a random point on the elliptic curve and P has prime order n. The cyclic subgroup of curve E (Fp) generated by point P is,

E (Fp) = {∞, P, 2P, 3P, . . . (n−1)P}

The public key parameters are prime number p, the elliptic curve E, the point P on the curve and its order n. A private key is d that is selected randomly from the interval [1, n−1] ($d \in_R [1, n-1]$) and the corresponding public key is Q = dP.The problem of determining d given the domain parameters and Q is the ECDLP [6].

Elliptic Curve Encryption and Decryption Scheme

The elliptic curve encryption and decryption procedures are similar to the basic ElGamal encryption scheme. The P is a random point on the elliptic curve. A plaintext m is embedded in the point on the curve that is M, and then encryption is performed by adding it to kQ, where k is a random integer, and Q is the Bob's public key. The Alice transmits the points C1 = kP and C2 = M +kQ to the Bob who then computes d*C1 = d*(kP) = k(dP) = kQ using her private key d, and thereafter recovers M = C2 − kQ. An eavesdropper who is unauthorised person wishes to recover M needs to compute kQ. This task of computing kQ from the domain parameters Q and C1 = kP is very difficult [6].

Performance Analysis of ECC

To analyze the performance of ECC, the Elliptic Curve Diffie-Hellman (ECDH) algorithm is performed for specific elliptic curve which is shown in the equation (4). ECDH is actually a key-agreement protocol, which defines how keys are generated and exchanged between two parties. For this purpose, the elliptic curve over a finite field having a large prime number is considered, and calculations are taken in terms of computation time it takes to perform point multiplication on the curve and computation time it takes for encryption and decryption of the secret message.

Consider the elliptic curve over a finite field Fp = F1009 where 1009 is the large prime number. The equation of the elliptic curve E which is used for the analysis is,

$$y^2 = x^3 + 3x + 5 \quad (4)$$

This curve has total 1023 points on it. Fig. 3 shows the position of various points in the given elliptic curve. To perform ECDH algorithm with this curve, one random point P is selected out of available points. The point P chosen has coordinates as P = (636:792:1). Two random integers a and b are selected to calculate the secret shared between two parties

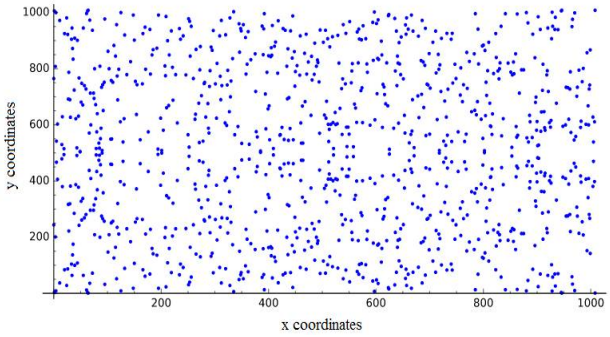

Fig 3 Position of x and y coordinates of points on an elliptic curve

i.e Alice and Bob. Here a and b are a = 688 and b = 438. The two parties will never share the values of their private keys. They will share the products a*P= (264:371:1) and b*P= (281:751:1). The values of a*P and b*P are shared over the insecure channel. At both sides, these shared secret is calculated by having multiplication with individual's private key. The calculated secret which is same on both sides is (350:534:1).

a*(b*P) = (350 :534 :1) and b*(a*P) = (350 :534 :1)

In this paper for the analysis purpose, ECDH algorithm as explained above is performed by considering various key sizes of the ECC such as 160 bit, 192 bit, 224 bit and 256 bit. To analyze ECC of 160 bit key size the elliptic curve over finite field is considered having prime field size of 160 bit (The prime number p is having the length of 160 bits). The same ECDH algorithm is repeated for different prime field sizes using the elliptic curve as given in the equation (4). During analysis the computation time required by elliptic curve with various field sizes is noted down. The system having Intel core i3 processor with 4 GB of RAM was used during analysis. Table I provides the details of computation time required by ECC for different key sizes during encryption process that is the point multiplication process on elliptic curve and Table II provides the details of computation time required by elliptic curve for decryption process of ECDH algorithm. With the increase in key size the time required for computation is also increased. Depending on the requirement of security level one can use the particular key size of the elliptic curve cryptographic algorithm. Today in practice 256 bit key size is preferred for strong security requirement.

Table I Computation Time Taken For Point Multiplication

Key Size (bits)	No of loops	Time per loop
160	25	8 ms
192	25	10.7 ms
224	25	12.4 ms
256	25	15 ms

Table II Computation Time Taken For Decryption

Key Size (bits)	No of loops	Time per Loop
160	25	7.95 ms
192	25	11.2 ms
224	25	8.97 ms
256	25	14.5 ms

Comparison of RSA and ECC

The efficiency of any algorithm is measured by the scarce resources it consumes. As in [8] authors performed the implementation of ECC and RSA on hardware and found that the performance of ECC over RSA increases as the word size of the processor decreases. If hardware acceleration is used for small devices then compared to RSA, Elliptic Curve Cryptography (ECC) has advantage of smaller key sizes, faster computation, as well as memory, energy, and bandwidth savings. According to [9] for 128-bit security levels, performance of RSA is generally 10-times slower than ECC for signature generation or key management operations. Typically for the comparison the measure used is time, but other measures such as space and number of processors are also considered. The efficiency of an algorithm is described as a function of the input size [6].

The comparison is based on parameter sizes providing comparable levels of security for RSA, Discrete Logarithm (DL), and ECC systems. If time is considered as only measure used for the efficiency of an algorithm, then the parameter sizes providing similar security levels for RSA, DL and ECC systems can be derived using the running times expressions explained by number field serve and Pollard rho algorithm. The key sizes that provide equivalent security levels for RSA, DL and ECC systems are listed in Table III [6].

Table III Key Sizes Rsa, Dl, and Ecc For Equivalent Security Levels

	Security levels in bits				
	80	**112**	**128**	**192**	**256**
DL parameter q ECC Parameter n (Key Size)	160	224	256	384	512
RSA modulus n DL modulus p (Key Size)	1024	2048	3072	8192	15300

Private-key operations for ECC are more efficient than RSA and DL private-key operations. Public-key operations for RSA are somewhat faster than for ECC if encryption exponent e is small. Only 160 bit secret key of ECC can reach the safety degree which RSA which needs 1024 bit. So using ECC in the E-commerce instead of RSA makes the improvement in E-commerce performance. The comparison of the efficiency of the pollard's rho which used for taking the logarithm and the way that using the general field to resolve a large number into 2 prime number is shown in Table IV.

Table IV Calculation Time Between Ecc and rsa [10]

Algorithm to break the large number.	Length of secret key	MIPS Year
Pollard's rho algorithm used for taking the	150	3.8×10^{10}
Logarithm for ECC	205	7.1×10^{18}
Using General number field	234	1.6×10^{28}
sieve decomposition of large	512	3×10^{4}
numbers in RSA	1024	3×10^{11}
	2048	3×10^{20}

Proposed Security Model for E-commerce using ECC

From comparison it is clear that the ECC is good alternative to RSA for the use in public key cryptosystem. Generally, in E-commerce the focus is on the security of payment information but customer's product information is not that secure. In proposed security model ECC technique is used to secure payment and purchase order information of the customer. The same elliptic curve cryptosystem is used to encrypt the customer's payment information and order information. The encrypted information can be decrypted by merchant only, who has the ECC decryption key (ECC private key). Using this model a high level of transaction security can be achieved in the E-commerce business. The proposed security model for electronic commerce business is shown in fig.4.

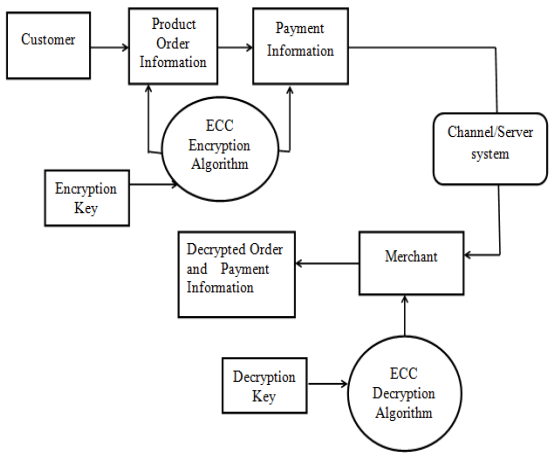

Fig 4 Proposed security model

CONCLUSION

In the field of E-commerce, the information security is a critical issue for customers as well as merchants. Customers fear the loss of their financial data and E-commerce websites fear the financial losses due to bad publicity. In RSA algorithm with the security requirement key size is increasing exponentially. Due to large key size, RSA is not suitable in environments where processing power, storage, bandwidth, or power consumption is a constraint. In this paper, the results of the analysis of ECC are considered which highlights the computation time taken by the encryption and decryption process by the ECDH algorithm with various key sizes. This paper proposes the general security model for E-commerce business using the elliptic curve cryptography which will be suitable for resource constrained environment and which provides the same level of security similar to RSA with less key size. In the proposed E-commerce security system ECC is used to encrypt the payment information along with the order information of the customer. Implementation of ECC in E-commerce will help to grow the online business rapidly.

References

1. Ganesan R, Dr. K. Vivekanandan, "A Novel Hybrid Security Model for E-commerce Channel," International Conference on Advances in Recent Technologies in Communication and Computing, 2009.
2. Salah I. K., Darwish A. and Oqeili S., "Mathematical attacks on RSA cryptosystem", *Journal of Computer Science*, August 2006.
3. Benjamin Clement Sebastian, Ugur Alpay, "Advantage of using Elliptic curve cryptography in SSL/TLS", Department of Computer Science University of California Santa Barbara, cs 290G fall term,2015.
4. Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, and Peter L. Montgomery, "On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography", Version 2.1, September 1, 2009.
5. Zhikao Ren, Minghua Liu, Chen Ye, Chuansheng Wang, "A Scheme of E-commerce Security based on ECC & SSL Protocol", IEEE, 2009.
6. Darrel Hankerson, Alfred Menezes,Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, Inc, 2004.
7. Elaine Brow, "Elliptic Curve Cryptography" Math 189A: Algebraic Geometry, 2010.
8. Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling
9. Chang Shantz, " Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs", CHES 2004, LNCS 3156, pp. 119-132, 2004.
10. Kerry Maletsky, "RSA vs. ECC Comparison for Embedded Systems" Atmel, White paper, 2015.
11. Xiuhua LIU, "The Study on E-commerce Security Based on ECC and SET" Third International Conference on Communications and Mobile Computing, IEEE, 2011.

How to cite this article:

Javed R. Shaikh *et al* (2017) 'Enhancing E-Commerce Security Using Elliptic Curve Cryptography', *International Journal of Current Advanced Research*, 06(08), pp. 5338-5342. DOI: http://dx.doi.org/10.24327/ijcar.2017.5342.0701

****