Print ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

# Comparative analysis of Elliptic Curve Cryptosystem and its survey

**Vijayakumar Perumal[1*], Xiao-Zhi Gao[2]**
[1]School of Electronics Engineering, VIT University, Chennai Campus, Chennai 600 127, Tamil Nadu, India.
[2]Dept. of Electrical Engineering and Automation, Aalto University, School of Electrical Engineering, Finland
***Corresponding author: E-Mail: vijayrgcet@gmail.com**

**ABSTRACT**

Over the past 30 years, Public Key Cryptography (PKC) has become a mainstay for secure communications over the Internet and throughout many forms of communications. Many algorithms have been implemented to improve the performance communication system and networks. Existing cryptographic algorithms such as RSA, DSA, and DES are providing high level of security with lager key size. It tends to high computational and communication overhead. In order to improve the performance of algorithm, new public key technique is built on the arithmetic of elliptic curves known as Elliptic Curve Cryptography (ECC). This paper will provide the mathematical background, types of curve, encryption and decryption algorithm, and various implementations. Finally, it shows the comparison tables which will prove the security level of ECC compared with other cryptography algorithm. This paper also examines the use of ECC in many constrained environments.

**KEY WORDS:** Public key cryptography, Elliptic Curve Cryptography, Rivert Shamir Adelman, Elliptic Curve, Elliptic Curve Discrete Logarithm Problem, Cryptosystem.

## 1. INTRODUCTION

Cryptography algorithms suggested best solution for many communication network systems by providing by offering security feature such as confidentiality, data integrity, authenticity and non-repudiation. Elliptic curve cryptography (ECC) is one of the best public key cryptography technique which offers optimal solution to many constrained environment such as power, bandwidth, speed, small device etc., Public Key Cryptography consists of pair of keys, named a public key and a private key which would be used to operate encryption and decryption of data. Each end user generates these key pairs where private key knows only by particular user and whereas the public key is distributed to all users taking part in the communication (William Stallings, 2009). ECC based cryptographic algorithm requires many predefined constant parameter to be known by the entire user in the communication system. These parameters are used to perform encryption and decryption operation during transmission of data. ECC require lesser key size than other cryptosystem. Unlike symmetric key cryptosystem, it does not share secret key between the end users which will tends to insecure communication. But symmetric key cryptosystem is much faster than public key cryptosystem due to generation of key pairs. Many researchers put their effort to increase the speed of process for key generation, encryption and decryption of message. As a result, a new algorithm was developed to fulfil the requirement of public key cryptosystem known as Elliptic Curve Cryptosystem. ECC is one of the famous public key cryptosystem alternatives to RSA based cryptosystem. The main advantage of Elliptic Curve Cryptography (ECC) is that it will secure the sensitive data using very short bit length compared to other asymmetric systems. For example, RSA require 1024 bit key length to each a security level, which is equivalent to an ECC key with a length of 160 bits are sufficient with elliptic curves (Avanzi, 2010). This would be proved in simulation result section. This paper was organized as follows: This section described about requirement of security service, introduction to Elliptic Curve Cryptosystem and existing cryptosystem; Section II deals with mathematical background of ECC, different types of curves, ECC encryption and decryption algorithm; Section III implements Elliptic Curve Cryptosystem with example; Section IV shows the simulated comparative result and its discussion. Finally, it gives conclusion and future scope of this work.

**Elliptic Curve Cryptography:** Elliptic Curve Cryptography is one of the famous public key cryptographic technique was independently proposed by Miller and Koblitz in 1985. It uses elliptic curve where variables and coefficient are bounded to elements of finite field. These researchers puts enormous amount of work to offer same level of security with lesser key size compared with existing methods which are based on difficulties of solving discrete logarithm problem over integers or integer factorization (Koblitz, 1987; Miller, 1986).

**Elliptic curves:** Elliptic curves are represented in many forms as shown below:

**Weierstrass curve:** An elliptic curve Cover a finite field K is defined by an Weierstrass equation shown in Eq.(1)

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

Where $a^1$, $a^2$, $a^3$, $a^4$, $a^6 \in K$ and $\Delta \neq 0$, where $\Delta$ is the discriminant of E and is defined as follows:

$$\Delta = d_2^2 + d_8 - 8\,d_4^3 - 27d_6^2 + 9d_2d_4d_6$$
$$d_2 = a_1^2 + 4a_2$$
$$d_4 = 2a_2 + a_1a_3$$
$$d_6 = a_3^2 + 4a_6$$
$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

If both the coordinates of points are P are belongs to Curve C or the point at infinity or zero elements (5). Then the set of points on E is given by Eq.(2)

$$E(L) = \{ (x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\} \quad (2)$$

**Hessian Curve:** A hessian curve of equation is given by Eq.(3)

$$x^3 + y^3 + 1 = 0.3xy \quad (3)$$

This curve is a plane curve where arithmetic operation such as point addition and doubling require less memory, faster operation than standard Weierstrass form. This leads to suggest this curve for application in elliptic curve cryptography (Leinweber, 2011).

**Edwards Curve:** The equation of an Edwards curve over a field K is given by Eq.(4)

$$x^2 + y^2 = 1 + dx^2y^2 \quad (4)$$

This curves enable the arithmetic operation such as point addition, doubling and in addition tripling can also possible which would provide faster operation (Edwards) (Daniel Bernstein, 2007). Twisted Edward curve and Hessian curve in Elliptic curve cryptography helps to speed up the addition and doubling operation by applying higher order twist such as cubic and quadric twists (Gouvea,1991) (Daniel).

**Jacobian Curve:** A Jacobi quartic of equation is given by Eq.(5)

$$y^2 = x^4 - 1.9x^2 + 1 \quad (5)$$

Jacobian curve is a representation of an elliptic curve which will defense the simple and differential power analysis style attack combined with cryptography. It also offers faster point addition and doubling operation than standard Weierstrass equation (Olivier Billet, 2003).

**Montgomery Curve:** Montgomery curve is a form of elliptic curve over finite field K is defined by an Eq.(6)

$$By^2 = x^3 + Ax^2 + x \quad (6)$$

Where A, B $\epsilon$ K and B $(A^2 - 4) \neq 0$

These elliptic curve forms are used to perform point addition, doubling and tripling operation in fast manner. These operations play a vital role for key generation, encryption and decryption process in Elliptic Curve Cryptosystem (Peter, 1987). The best curve chosen for Elliptic Curve Cryptosystem is Jacobian curve.

**Mathematical Background:** An elliptic curve E over finite integer field K is defined by an Eq.(7)

$$E: y^2 = x^3 + ax + b \quad (7)$$

Where $4a^3 + 27b^2 \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All the points on the elliptic curve E which satisfies the above equation plus a point at infinity lies on the elliptic curve. The elliptic curve operations defined over a real number are slow and inaccurate due to round-off error. In order to increase the speed of operation and accurate, the curve based cryptography is defined over prime field and binary field (Lange, 1987).

**Elliptic curve over Prime field**: The equation of the elliptic curve over a prime field Fp is given by Eq.(8)

$$E: y^2 \bmod p = (x^3 + ax + b) \bmod p \quad (8)$$

$$(4a^3 + 27b^2) mod\ p \neq 0$$

All the elements of the finite field and all the operations such as addition, subtraction, division, multiplication involves integers between 0 and p – 1.The prime number p is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure (Certicom Research).

**Point addition**: Consider two distinct points J and K such that J = $(x_J, y_J)$ and K = $(x_K, y_K)$. Let L = J + K where L = $(x_L, yL)$, then

$$X_L = S^2 - X_J - X_K \bmod p \quad (9)$$

$$Y_L = -Y_J + S(X_J - X_L) \bmod p \quad (10)$$

$$S = (Y_J - Y_K)/(X_J - X_K) \bmod p \quad (11)$$

Where S is the slope of the line through J and K. If K = -J i.e. K = $(x_J, -y_J \bmod p)$ then J + K = O. where O is the point at infinity. If K = J then J + K = 2J, then point doubling equations are used. Also J + K = K + J

**Elliptic curve over GF (2m):** Polynomials are defined over finite field GF (2m) which consists of 2m elements, to perform addition and multiplication operations. The cubic equation of Elliptic curves over GF(2m) took all variables and coefficients from GF(2m) in which all the arithmetic operation are performed. This cubic equation is used appropriately for cryptographic applications than Zp (Silverman, 1994).

$$y^2 + xy = x^3 + ax^2 + b \quad (12)$$

Where x and y are variables; a and b are coefficients of GF (2m).

**Generation of Elliptic Curve Points:** The equation of Elliptic curve prime field is used to generate the elliptic curve points which help to generate private and public key pairs. If x=0, y=1……..p. To Substitute x=1, y=0; a=1;b=1; p=23 in the Eq.(8).

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

$0 \bmod 23 = (13+1(1)+(1)) \bmod 23$

$0 = 3 \bmod 23$

$0 = 3$

Like wise to find the points when both sides will be equal then it should be a point. Like x=1; y=7; a=1; b=1;p=23 in the equation.

$7^2 \bmod 23 = 3 \bmod 23$

$3 = 3$

Then (1, 7) is one of the elliptic curve points in the table. This process continued until to generate p points by varying x and y values in Eq.(8) as shown in Table.1. These points are used to draw the elliptic curve as shown in Fig.1. In the above mentioned curve, elliptic curve over prime field equations are chosen, to perform point scalar point multiplication which require both point addition and doubling operation.

**Table.1. points on the elliptic curve $E_{23}$ (1, 1)**

| | | |
|---|---|---|
| (0, 1)<br>(0, 22) | (6, 4)<br>(6, 19) | (12, 9)<br>(13, 7) |
| (1, 7)<br>(1, 16)<br>(3, 10) | (7, 11)<br>(7, 12)<br>(9, 7) | (13, 16)<br>(17, 3)<br>(17, 20) |
| (3, 13)<br>(4, 0)<br>(5, 4) | (9, 16)<br>(11, 3)<br>(11, 20) | (18, 3)<br>(18, 20)<br>(19, 5) |
| (5, 19) | (12, 4) | (19, 18) |

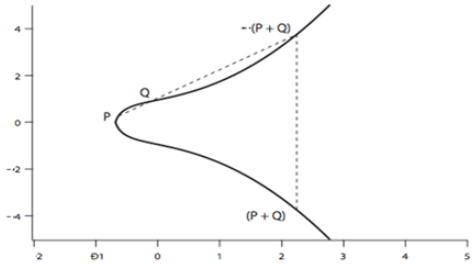



**Figure.1. Elliptic Curve Equation $y^2 = x^3+x+1$**

**Elliptic Curve Discrete Logarithm Problem (ECDLP):** Let P and Q are the two points chosen from table.1 to perform scalar multiplication operation such that Q = k x P where k is scalar. It is very difficult to find k, if P and Q values are known by intruder provided k is sufficiently large known as Elliptic Curve Discrete Logarithm Problem. So this discrete logarithmic problem provides high security to elliptic curve cryptosystem. Hence the main operation involved in ECC is point multiplication. i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve.

**Scalar point multiplication:** Scalar point multiplication is achieved by two basic elliptic curve operations such as point addition (adding two points J and K to obtain another point L i.e., L = J + K) and point doubling (adding a point J to itself to obtain another point L. i.e. ( L =2J)).

## 2. METHODS & MATERIALS

**Implementation of elliptic curve cryptosystem:** Elliptic curve cryptosystem mainly preferred to provide security to power, bandwidth constrained devices due to shorter key length and less computational overhead than RSA and Diffie-Hellman algorithm. RSA based cryptosystem have to perform prime integer factorization and modular exponentiation require more time to process and larger key size to provide the same level of security offered by elliptic curve cryptosystem. Counterpart of ECC is modular addition and requires shorter key length to perform encryption and decryption operation. Elliptic curve cryptosystem consist of three main processes such as key generation, encryption and decryption. Consider user A and B in the cryptosystem are agree upon domain parameters such as a, b, p, G and n. a and b are coefficient of Eq.(8); p is large prime number; G is generator point; n is the order of curve.

**Key generation process:**

- User A generates a random private key $n_A < n$.
- User A also computes public key $P_A = n_A \times G$; $P_A = G+G+G\ldots+nA$ times. (Point Addition)
- User B generates a random private key $n_B < n$.
- User B also compute his public key, $P_B = n_B \times G$; $P_B = G+G+G\ldots+nB$ times. (Point Addition)

**Elliptic curve encryption process:** The process of converting plaintext $P_m$ into cipher text $C_m$ known as encryption process. Since elliptic curve cryptography deals with elliptic curve point for key generation process. Each character

of plaintext should be converted into points using Koblitz method. Then converted plaintext points are encrypted with the help of its generated keys to generate cipher text points ($C_m$).

$$C_m = \{k \,.\, G \,, P_m + \, k.P_B\} \qquad (13)$$

Where; G - Generator Point; $P_m$ - Plaintext point on the curve; k - Random number chosen by A; $P_B$ - Public key of user B.

**Elliptic curve decryption process:** The cipher text points $C_m$ are converted into plaintext point $P_m$ using Koblitz method.

$$P_m + k.\, P_B - n_B\,(k \,.\, G) = P_m + k\,(n_B)G - n_B\,(k \,.\, G) = P_m \qquad (14)$$

**Elliptic curve cryptographic algorithm:** ECC algorithm involves to perform key generation, generation of elliptic curve points, mapping of plaintext into numbers, conversion of number into points, encrypt the plaintext points using private key and finally decrypt the cipher text points. These operations are performed by following sequence of steps as shown below:

- Public domain parameter An elliptic curve $E_p(a,b)$ over finite prime field p has been chosen.
  - $E_{751}$ (-1,188); N = 727;
- Elliptic curve E has N points on it.
- Message having digits 0,1,2,3,4,5,6,7,8,9 are coded as 0 to 9 and letters A, B, C,. . . , X,Y,Z are coded as 10,11,. . . , 35.
  - B = 11
- Plaintext $P_m$ converted into a series of numbers between 0 and 35.
- Auxiliary base parameter k should be agreed upon both parties.
  - *k* = 20
- Compute x = mk + 1 using converted plaintext number *mk.*
- *Compute x = mk* +2 and then *x = mk* +3 until y coordinate value could be solved. (as shown in table.1)
  - x=mk+4; x=224 and y= 248;
- Above steps are repeated until all the messages are converted into sequence of points (x,y).
- Plaintext points are encrypted using Eq.(13) to obtain cipher text points.
- These cipher text points are decrypted using Eq.(14) to obtain plaintext points.
- Each point (*x,y*) should choose *m* integer value less than (*x*-1)/*k* to decode the point (*x,y*) as the symbol *m*.
  - (224-1)/20 = 223/20 i.e 11.15 = 11 = B

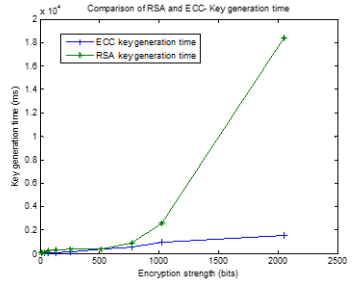
## 3. SIMULATION RESULT

RSA and Elliptic Curve Cryptosystem mainly involve three different process namely key generation, encryption and decryption process. These processes are implemented using MATLAB simulation tool and notice the parameters such as processing time and key size. Processing time is the time taken by processor (Intel 5) to execute the operations. Key size is the size of the key used to encrypt and decrypt the data. National Institute of Standard and Technology recommended key bit size for RSA as well as ECC to achieve better security level using different algorithm. Fig.3 compares the time taken to generate the key with respect to encryption strength for both RSA and ECC algorithm. RSA takes more processing time for 1024 bit key size than ECC-160 bit key size for key generation process.

**Table.2. NIST- Recommended field sizes for U.S federal government use**

| Symmetric Cipher key length | RSA (n Bits) | ECC | |
|---|---|---|---|
| | | $F_P$ (p bits) | $F_{2^m}$ (m Bits) |
| 80 | 1024 | 160 | 163 |
| 96 | 1536 | 192 | 193 |
| 112 | 2048 | 224 | 233 |
| 128 | 3072 | 256 | 283 |
| 192 | 7680 | 384 | 409 |
| 256 | 15360 | 521 | 571 |

Memory required for RSA is very high compare with ECC algorithm, since it require less key size for encryption and decryption operation as shown in Fig.5. RSA algorithm took more time to encrypt or decrypt the data than ECC algorithm as shown in Fig.6. Since RSA require more memory space due to larger key size, it would increase the encryption and decryption time. But ECC require less memory space due to shorter key size decreases encrypt /decrypt time.




**Fiure.4. Key generation time**

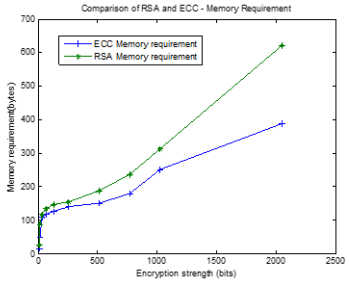



**Figure.5. Memory requirement**

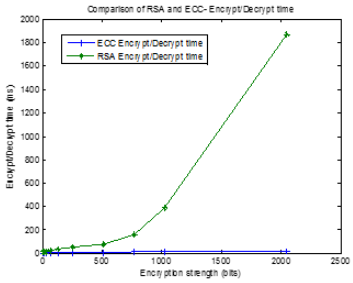



**Figure.6. Comparison of RSA and ECC- Encrypt / Decrypt time**

**ECC Survey and Its Application:**

**ECC Survey:** Many companies have incorporated ECC in their products due to its advantage over other algorithms. This is due to ECC has begin to establish itself as both secure and efficient. These advantages of ECC makes ECDSA used in several government and major research institution security standards, including IEEE P1363, ANSI X9.62, ISO 11770-3 and ANSI X9.63. Certicom is a software company which provides solution and service to information security based software to its client. Certicom has published numerous papers in support of ECC and has also implemented ECC in all of its commercial products. Its success prompted many other companies to look more closely at the benefits and security of ECC. Now, ECC is becoming the mainstream cryptographic scheme in all mobile and wireless devices. There are many researchers are trying to establish the benefits of ECC and its security on various environment. Few surveys have been done as follows: Liu Yongliang (2007) proposed an ECC-based wireless authentication protocol. This protocol avoid the man in the middle attack and forging certificate attack by employing user authentication protocol resultant in lower computational and communication overhead. Vivek Katiyar (2010) did the survey on ECC for pervasive computing environment where systems are constrained with battery power, computational power and memory. Pritam Gajkumar Shah (2010) provided the implementation issues on wireless sensor network using Elliptic Curve Cryptography. Kaleel (2010), constructed reconfigurable architecture for Elliptic Curve Cryptography where Lopez-Dahab elliptic curve point multiplication algorithm are used to achieve high throughput rate resulting 4.8 time faster operation speed for key generation, encryption and decryption process using Xilinx software (2010). Maria (2012), proposed a text based elliptic curve cryptosystem where plaintexts are converted into ASCII and then change into an affine point on EC. These affine points are encrypted using ECC encryption algorithm and did the reverse process to obtain plaintext (2009). ECC Encryption and Decryption methods can only encrypt and decrypt a point on the curve not messages. But padma (2010) provided a encoding (message to a point) and decoding (point to a message) methods for encryption and decryption process using Koblitz equation. Sahoo (2011) compare the RSA and Elliptic curve cryptographic algorithm in terms of key size and suggested these algorithm for power constrained devices. Maria (2012) suggested a new Comparative Linear Congruential Generator method rather than random generator to encrypt and decrypt the text as well as image file. This random number generation proved that it avoids the brute force attack.

**ECC Application:**

- Secure on-line transactions and web security
- Personal computers
- Cell phones, PDAs, Pagers
- Smart Cards, RFIDs
- Route discovery in MANETs
- Wireless Sensor Networks
- Wireless Mobile Networks
- Base Station Authentication in mobile networks
- E-Banking Security

## 4. CONCLUSION

Finally, conclude that ECC is the suitable public key cryptosystem for limited power, limited bandwidth, limited storage requirement devices such as RFID, smart cards, sensor devices, mobile devices due to less communication and computational overhead. These feature makes ECC is an alternative cryptosystem such as RSA, DSA etc., ECC also used to make powerful crypto processor for powerful computers and networks.

**Scope for Future Work:** The best alternative for ECC is Hyper elliptic Curve cryptography which will provide same level of security using only 80 bit key size.

**REFERENCES**

Amara M and Siad A, Elliptic Curve Cryptography and Its Applications, IEEE proceeding of International workshop on Systems, Signal Processing and their Applications, 2011, 247-250.

Avanzi R.M and Tanja L, Introduction to Public key cryptography from Handbook of Elliptic and Hyper elliptic curve cryptography eds. Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, Taylor and Francis, Florida, 2010.

Daniel B and Lange T, Faster Addition and Doubling on Elliptic curves, International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology, 2007, 29-50.

Daniel B, Peter B, Marc J, Tanja L and Christiane P, Twisted Edward Curves, A normal form for elliptic curves, Bulletin of the American Mathematical Society Providence, 44, R.I, 2007, 393– 422.

Gouvea F and Mazur B, The Square free sieve and the rank of elliptic curve, Journal of American Mathematical Society, 4 (1), 1991.

Jao D, Miller S and Venkatesan R, Do all Elliptic Curves of the same order have the same difficulty of discrete logs, ASIACRYPT, LNCS. Springer-Verlag, 3788, 2005, 21-40.

Kaleel A and Athisha G, Reconfigurable Architecture for Elliptic Curve Cryptography, IEEE proceedings of the International Conference on Communication and Computational Intelligence, 2010, 461-466.

Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48, 1987, 2003–2009.

Lange H and Ruppert W, Addition laws on elliptic curves in arbitrary characteristics, Journal of Algebra, 107 (1), 1987, 106-116.

Leinweber L, Papachristou C and Wolff F.G, An analysis of efficient formulas for elliptic curve point addition over binary extension fields, IEEE proceeding of 45th Annual conference on Information Sciences and Systems (CISS), 2011, 1-5.

Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu, Elliptic Curve Cryptography Based Wireless Authentication Protocol, International Journal of Network Security, 5 (3), 2007, 327–337.

Maria Celestin Vigila S and Muneeswaran K, Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications, International Journal of Network Security, 14 (4), 2012, 236-242.

Maria S, Vigila C, Muneeswaran K, Implementation of Text based Cryptosystem using ECC, IEEE proceeding of ICAC'09, 2009, 82-85.

Miller V, Use of elliptic curves in cryptography, Advances in Cryptology-CRYPTO '85. 1986, LNCS, 218 (483), 1986, 417–426.

Olivier Billet and Marc Joye, The Jacobi model of an Elliptic Curve and the Side-channel Analysis, Springer-Verlag Berlin Heidelberg, 2003.

Padma Bh, Chandravathi D and Prapoorna Roja P, Encoding and Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method, International Journal on Computer Science and Engineering, 02 (5), 2010, 1904-1907.

Peter L, Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization, American Mathematical Society, 1987.

Pritam Gajkumar Shah, Xu Huang and Dharmendra Sharma, Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks, IEEE proceeding of 24th International Conference on Advanced Information Networking and Applications Workshops, 2010, 589-592.

Silverman and Joseph H, The arithmetic of elliptic curves, Gradute Texts in Mathematics, Second Edition, Springer Publication, 2009.

Smart N.P, The Hessian form of an elliptic curve, Springer-Verlag Berlin Heidelberg, 2001.

Vivek Katiyar, Kamlesh Dutta and Syona Gupta, A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment, International journal of computer application, 11 (10), 2010, 41-46.

William Stallings, Cryptography and Network Security, 4th ed, Principles and Practices, Dorling Kindersley (India) Pvt, ltd, 2009.