Performance Evaluation of Sextic Curve Cryptography and Probability Symmetric Curve Cryptography in Wireless Sensor Networks

W. R. Sam Emmanuel
Department of Computer Science
Nesamony Memorial Christian College Marthandam, Tamil Nadu, India – 629 165

ABSTRACT
This paper starts with a brief introduction of the different coordinate systems prevailing in cryptography, aims in developing security measures which could save atleast some amount of time in the execution processes. For this purpose the sextic curve and the probability symmetric curve are considered. Simulation exercises are carried out for both and it is proved that in both the cases the time taken for encryption and decryption is slightly lesser than that for RSA and ECC. On the whole this study brings out the new system for encryption and decryption with higher level of secrecy and lesser amount of time.

General Terms
Cryptography, Security.

Keywords
SCC, PSCC, Point Addition, Point Doubling.

1. INTRODUCTION

It is always necessary to transfer the data in secure form[1], because we are in the internet evolution age. There are different types of algorithm provide security[2] for the data to be transferred between the computers. The leading algorithms like RSA and Elliptic Curve Cryptography (ECC) are very expensive. Also RSA and ECC have general sub-exponential attack. It is essential to rise the number of bits required in the RSA generated key pairs than in the ECC generated key pairs[3][4], to maintain the same degree of security in view of rising computer power. The variations in the key sizes between ECC[5][6][7] and RSA will grow exponentially to maintain the same relative strength as compared to the average computing power available[8]. Due to the complexity in the point addition and point doubling[9][10] the encryption and decryption process in ECC are very slow[11][12].

The improvement in the computational time is very essential for the cryptographic schemes. To overcome the difficulties faced in the computation, the authors proposed the sextic curve cryptography and probability symmetric curve cryptography.

The rest of the paper is organized as follows. The second section shows the sextic curve cryptography (SCC) and different operations carried out by the SCC. The third section explores the operations and the origin of the probability symmetric curve cryptography (PSCC). The fourth section has the simulation results of SCC and PSCC, which is also compared with the RSA and ECC. The fifth section concluded the paper with different challenges of SCC and PSCC.

2. SEXTIC CURVE CRYPTOGRAPHY

There is a family of curve[13] under the sextic curves. The Atriphtaloid curve is the very suitable curve under this family which is also called atriphtothlassic curve. The Atriphtaloid cuve is used for defining the Sextic Curve Cryptography[14].

2.1 Sextic Curves

The general form of the Sextic curve is

$$x^4(x^2 + y^2) - (ax^2 - b)^2 = 0 \quad \text{..... (1)}$$

where a and b are the parameters.

The curve can be reduces to the standard form $S(a,b)$ as

$$x^2y^2 = a^2x^2 - 2abx + b^2 - x^3 \quad \text{..... (2)}$$

This equation (2) involves additions and multiplications over objects that are represented by x, y, a and b with x always positive. The characteristic of the equation is zero. The different forms of the curve with various parameters are presented in Figure-1. The $S(a,b)$ will be singular only if it contains a point (x, y) such that $2abx - 2b^2 - x^3 = 0$ and $y = 0$.

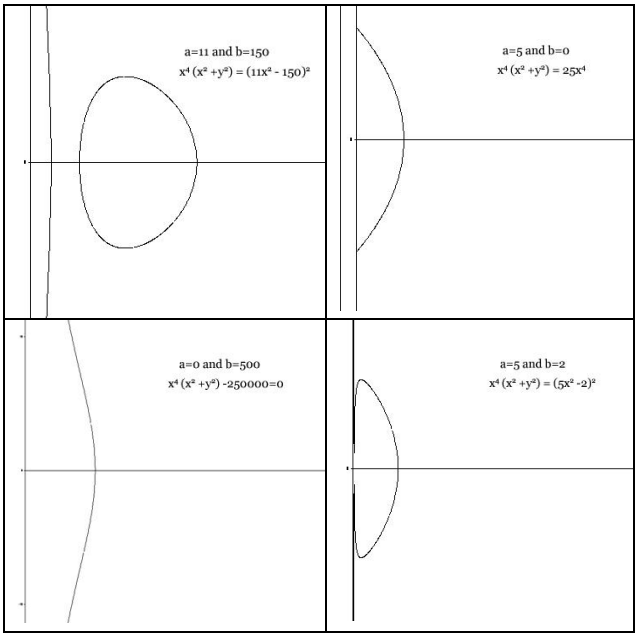

Figure-1. Forms of the Sextic curve for various parameters

2.2 Algebraic Equation for Adding Two Points on SCC

If we select any two points P and Q on the curve $S(a,b)$ and draw a straight line to join these points then the intersecting point R is the intersection of the straight line on the curve $S(a,b)$. The sum of the points[15][16] P and Q is the mirror reflection of R about the x axis.

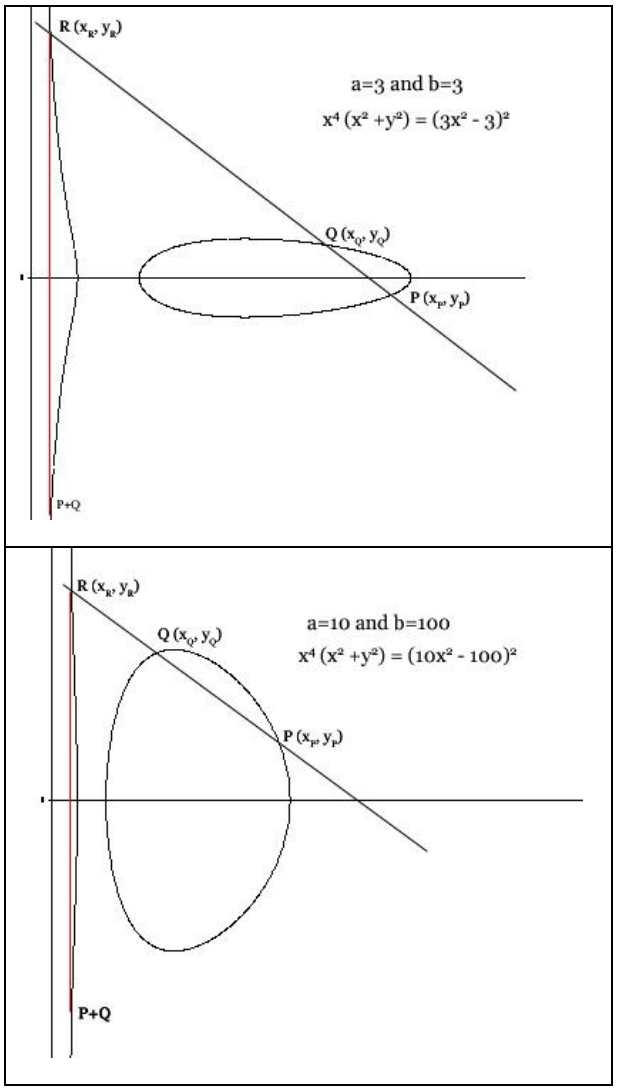

Fig-2. Point addition of Sextic Curve Cryptography

The equation of the straight line on the y axis runs through the points P and Q with the slope α and the intercept β is of the form $y = \alpha x + \beta$.

The equation $x^2(\alpha\alpha + \beta)^2 = a^2x^2 - 2abx + b^2 - x^3$ must be true for any point (x, y) which lies at the intersection of the straight line and the curve S(a, b). Therefore the sum of the points P and Q produced the coordinates[17] x_{P+Q} and y_{P+Q}, which can be expressed as

$$x_{P+Q} = -x_P - x_Q - (1 + 2\alpha\beta)/\alpha^2 \quad \text{..... (3)}$$

and $y_{P+Q} = \alpha(x_P - x_R) - y_P$, ... (4)

The y-coordinate of the reflection –R is negative of the y coordinate of the point R on the intersecting straight line. The Figure-2 shows the illustrations of the point addition operation carried out on the curves $x^4(x^2 + y^2) = (3x^2 - 3)^2$ and $x^4(x^2 + y^2) = (10x^2 - 100)^2$.

2.3 Algebraic Equation for Point Doubling on SCC

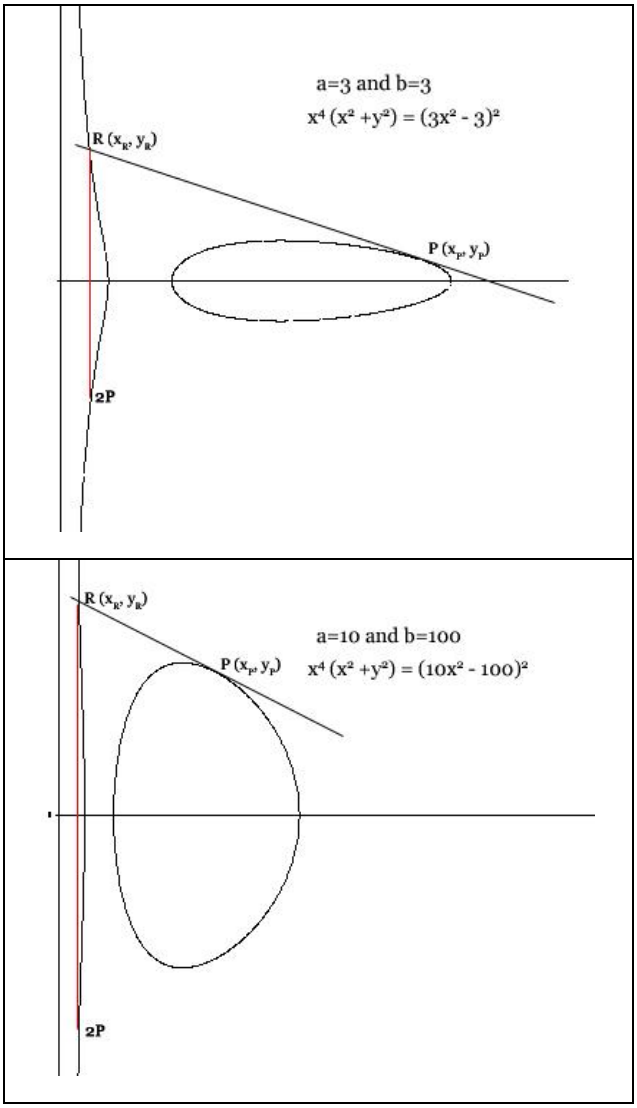

Figure-3. Point doubling of Sextic Curve Cryptography

When we draw a tangent at P and find the intersection R of this tangent on the curve $S(a,b)$, the point doubling[18] is the mirror reflection of the point R about the x axis.

The point R is the intersection of the tangent with the curve $S(a,b)$ and the point $2P$ is the reflection of the point R about the x axis, the value of $2P$ is obtained by taking the negative of the y-coordinate. The point doubling produced the coordinates x_{2P} and y_{2P}, which can be written as

$$x_{2P} = -2x_P - \left[\frac{4x_P^4 y_P^2 + 2x_P\left(2ab - x_P^2\right)\left(2x_P y_P^2 - 2ab + x_P^2\right)}{\left(2ab - x_P^2\right)^2}\right] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

and $y_{2P} = \frac{2ab - x_P^2}{2x_P^2 y_P}(x_P - x_R) - y_P$ …… (6)

The Figure-3 shows the illustrations of the point doubling operations carried out on the curves $x^4(x^2 + y^2) = (3x^2 - 3)^2$ and $x^4(x^2 + y^2) = (10x^2 - 100)^2$.

3. PROBABILITY SYMMETRIC CURVE CRYPTOGRAPHY

In the theory of probability the more widely used distribution is the probability symmetric curve. The t-distribution curve, the t value tends to the normal for the large values of n. It will be very suitable to use the normal curve for the probability symmetric curve cryptography[19].

3.1 Probability Symmetric Curves

The general form of the equation of the normal curve with mean m=0 and standard deviation σ after interchanging the x and y is

$$x = \frac{1}{\sqrt{2\pi}\sigma} e^{-y^2/2\sigma^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (7)$$

The equation (7) will produce the standard form $N(a,b)$ as

$$6y^2 = a\left\{11 - 18x + 9x^2 - 2x^3\right\} + b \quad \ldots\ldots\ldots (8)$$

where a and b are the parameters

3.2 Algebraic Equation for Adding Two Points on PSCC

If we select any two points P and Q on the curve $N(a,b)$ and draw a straight line to join these points then the intersecting point R is the intersection of the straight line on the curve $N(a,b)$. The sum of the points P and Q is the mirror reflection of R about the x axis.

The equation of the straight line on the y axis that runs through the points P and Q with the slope α and the intercept β is of the form $y = \alpha x + \beta$. Therefore the sum of the points P and Q produced the coordinates x_{P+Q} and y_{P+Q}, which can be expressed as

$$x_{P+Q} = -x_P - x_Q + \frac{(9a - 6\alpha^2)}{2a} \quad \ldots\ldots\ldots\ldots\ldots (9)$$

and $y_{P+Q} = \alpha(x_P - x_R) - y_P$ ……(10)

The Figure-4 shows the illustration of the point addition operation carried out on the curves $6y^2 = 5\left\{11 - 18x + 9x^2 - 2x^3\right\} + 10$ and $6y^2 = 3\left\{11 - 18x + 9x^2 - 2x^3\right\} + 15$.

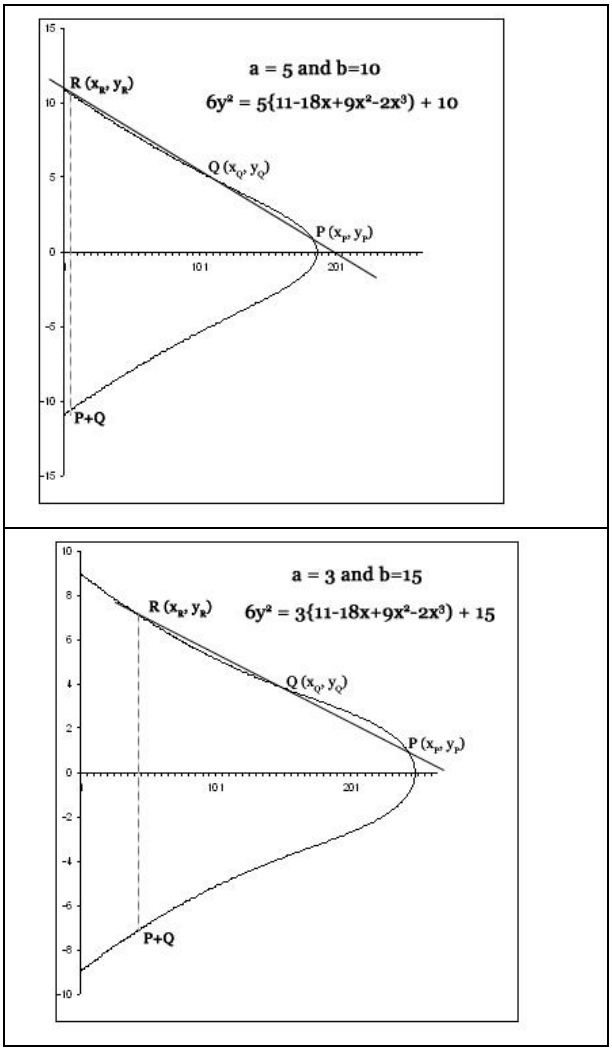

Figure-4 Point addition in Probability Symmetric Curve Cryptography

3.3 Algebraic Equation for Point Doubling on PSCC

When we draw a tangent at P and find the intersection R of this tangent on the curve $N(a,b)$, the point doubling is the mirror reflection of the point R about the x axis. The point doubling produced the coordinates x_{2P} and y_{2P}, which can be expressed as

$$x_{2P} = \frac{4ax_P^2 y_P^2(9 - 4x_P) - 6a^2}{8ax_P^2 y_P^2} \quad \ldots\ldots\ldots\ldots (11)$$

and $y_{2P} = \frac{a}{2x_P y_P}(x_R - x_P) - y_P$ …. …… (12)

The Figure-5 shows the illustrations of the point doubling operation carried out on the curves $6y^2 = 5\left\{11 - 18x + 9x^2 - 2x^3\right\} + 10$ and $6y^2 = 3\left\{11 - 18x + 9x^2 - 2x^3\right\} + 15$.

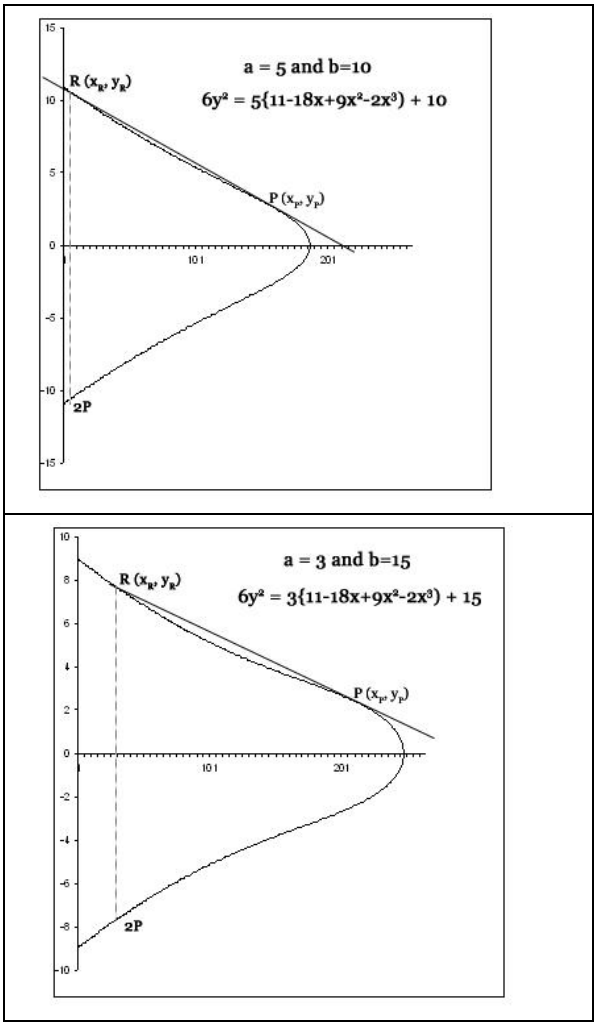

Figure-5 Point doubling of Probability Symmetric Curve Cryptography

4. RESULTS AND DISCUSSION

In order to show the superiority of the results got in this research, it is proposed to do simulation exercises on the communication through the new methods proposed in sensor network[20]. The existing range based localization techniques are (i) Received-Signal-Strength-Indicators(RSSI), (ii) Angle-of-Arrival(AoA), (iii) Time-of-Arrival(ToA) and (iv) Time-Difference-of-Arrival(TDoA). Among these techniques, majority of the researchers have used ToA. The requirements needed for ToA satisfies the Ultra-Wide Band(UWB) technique. Hence in this research, it is better to use the ToA for testing the time taken for communication. The MATLAB-9 is used for performing the simulation through ToA positioning scheme. The locations of 35 sensor nodes developed randomly in an area of size 50x50 are shown in Figure-6.

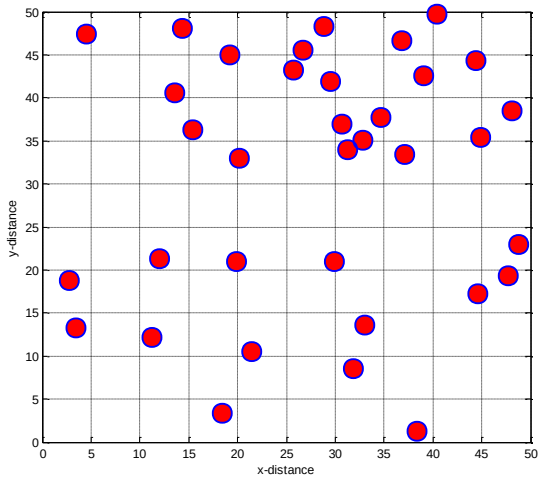

Figure-6 The position of sensor nodes

The sensor nodes in the network were selected by applying the ToA positioning scheme algorithm. A signal was send from the anchor node to the sensor node and the time of arrival was calculated by using a timer. The binary data[21] is used here. The transmission of data was done through QPSK transmitter, since it gives better performance and bit error rate, compared to other system.

Between node arrivals measurements were noted through the timer. In the receiving end a parallel to serial of data send by the anchor node is implemented, which is in the serial to parallel form. While measuring, the binary data was divided into odd bits and even bits and received through two different channels.

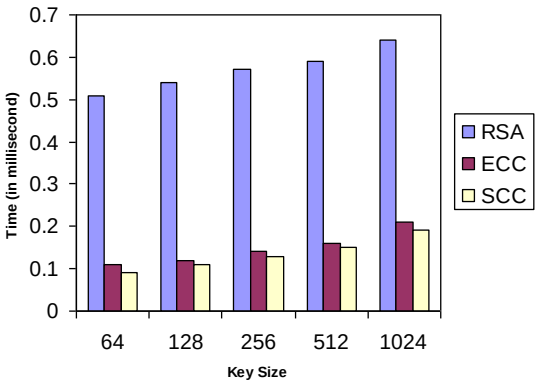

Figure-7 Comparison of Encryption schemes with SCC

From the time of arrival of signals, the distances between the nodes are calculated and these are used to find the position of nodes in the network. Every time when the last bit is received the timer is set off and the time is noted. After finding the time of arrival of signals between nodes, the positions of the nodes were located. The distance is computed from the product of speed and time. After computing the distance location verification was done for the validation of results.

After setting the locations of the sensors the exchanges between the sensors were done by SCC and PSCC techniques. The encryption time and the decryption time of the SCC and PSCC were observed for ten times, the average time is calculated. From the simulated results the encryption

and decryption time (in milliseconds) of the RSA, ECC, SCC and PSCC were analyzed. It is proved that the encryption time and decryption time of SCC and PSCC are improved from the RSA and ECC. The Figure-7 and Figure-8 show the performance of SCC and PSCC over RSA and ECC.

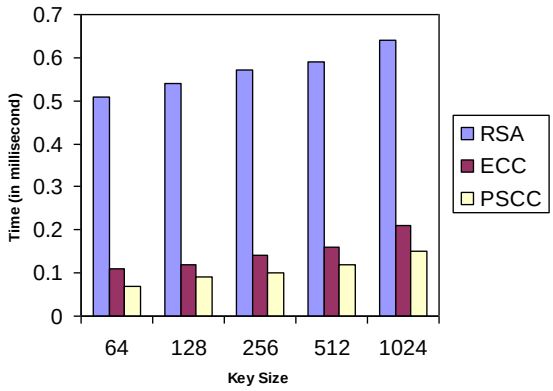

Figure-8 Comparison of Encryption schemes with PSCC

5. CONCLUSION

This paper presents the performance evaluation of the SCC and PSCC in the sensor networks. The comparative statements of the results shown in the section 4 say that the proposed approach comparatively takes better performance in time for communication between the sensor nodes than in the existing methods. Hence the proposed, SCC and PSCC are superior to the existing methods. Future work can identify all possible existing symmetric curves and curves which on transformation can be brought down to the symmetric form can be used for setting-up new coordinate systems and to reduce the time and space in the implementations.

6. REFERENCES

[1] Neal Koblitz. 2007. The uneasy relationship between Mathematics and Cryptography. Notes of the AMS, 54(8):972-979.

[2] William Stallings. 2004. Cryptography and Network Security Principles and Practices. 3rd ed. Pearson Education.

[3] Junfeng Fan, Kazuo Sakiyama, Ingrid Verbauwhede. 2008. Elliptic curve cryptography on embedded multi-core systems. Journal of Design Automation for Embedded Systems, 123-134.

[4] Kanniah, Samsudin. 2007. Multi-threading elliptic curve cryptosystems. Proceedings of Telecommunications and Malaysia International conference on communications, 134-139.

[5] Lee, Wong. 2004. A random number generator based elliptic curve operations. Computers and Mathematics with Applications, 47:217-226.

[6] Menezes. 1993. Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers.

[7] Nel Koblitz, Algred Menezes, Scott Vanstone. 2000. The state of elliptic curve cryptography. Journal of Designs Codes and Cryptography, 19:173-193.

[8] Atay et al. 2006. Computational cost analysis of elliptic curve arithmetic. Proceedings of international conference on Hybrid Information Technology, 1:578-582.

[9] Liu Wen-Yuan et al. 2007. A proxy blind signature scheme based on elliptic curve with proxy revocation. Proceedings of the international conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed computing, 1:99-104.

[10] Nassar, Watheq El-Kharashi, Mahmoud Shousha. 2007. An FPGA-based architecture of ECC point multiplication. Proceedings of the 2nd international design and test workshop, 237-238.

[11] Puttmann et al. 2008. Hardware Accelerators for Elliptic Curve Cryptography. Advances in Radio Science, 6:259-264.

[12] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh. 2008. Elliptic Curve Cryptography. ACM Ubiquity, 9:1-8.

[13] http://en.wikipedia.org/wiki/List_of_curves.

[14] Sam Emmanuel, C.Suyambulingom. 2011. Safety Measures Using Sextic Curve Cryptography. International Journal on Computer Science and Engineering, 3(2):800-806.

[15] Berkhoff, Lane. 2008. A Survey of Modern Algebra. USA:AKP Classics.

[16] Nel Koblitz. 1984. A Course in Number Theory and Cryptography. New York:Springer Verlag.

[17] Howon Kim et al. 2008. Hyper elliptic Crypto-coprocessor over affine and projective coordinates. ETRI Journal, 30(3):365-376.

[18] Jarvinen, Tommiska, Skytta. 2004. A scalable architecture for elliptic curve point multiplication. Proceedings of IEEE international conference on Field-Programmable Technology, 303-306.

[19] Sam Emmanuel, Suyambulingom. 2011. Safety Measures Using Probability Symmetric Curve Cryptography. International Journal of Computer Applications, 31(11): 42-48.

[20] Leonardo B. Oliveira et al. 2011. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 34:485–493.

[21] Jithra Adikari, Vassil S. Dimitrov, Laurent Imbert. 2011. Hybrid Binary-Ternary Number System for Elliptic Curve Cryptosystems. IEEE Transactions on computers, 60(2):254-265.