Safety Measures Using Probability Symmetric Curve Cryptography

W. R. Sam Emmanuel
Department of Computer Science
Nesamony Memorial Christian College
Marthandam, Tamil Nadu, India – 629165

C. Suyambulingom
Research Guide
Vinayaka Missions University,Salem
Tamil Nadu, India

ABSTRACT
This paper proposes Probability Symmetric Curve Cryptography (PSCC), which is a new milestone in the Symmetric Curve Cryptography. The PSCC proposes the new approach to do the point addition and point doubling. The finite field operations applied in the PSCC provides the new spirit of thinking more on the safety of the data. This paper also expresses the usage of domain parameters and key pair creation. The results of this approach express the security of data in terms of future technology. The overall objective is to generate valuable dynamic security measures using PSCC.

General Term
Cryptography

Keywords
Probability Symmetric Curve Cryptography, Point Addition, Point Doubling, Domain Parameters

1. INTRODUCTION
The data security[1] plays important role in the exchange of information through the developed media. The RSA and the Elliptic Curve Cryptography (ECC)[2][3][4] are the main leading algorithms to provide safety and security for the data. The main advantage of ECC over RSA is that the basic operation in ECC is point addition, which is known to be computationally very expensive. This is one of the reasons why it is very unlikely that a general sub-exponential attack on ECC will be discovered in the near future, though ECC has a few attacks on a few particular classes of curves. These curves can be readily distinguished and can be avoided. On the other hand, RSA already has a known sub-exponential attack which works in general. Thus, to maintain the same degree of security, in view of rising computing power, the number of bits required in the RSA generated key pair will rise much faster than in the ECC generated key pair. The ratio between RSA and ECC key size for the time to break in 1024 MIPS-years is 5:1[5][6]. The difference in the key-sizes between ECC and RSA will grow exponentially to maintain the same relative strength as compared to the average computing power available.

Due to increasing computation required for higher bit encryption, more transistors are required onboard for the smart card to perform the operation[7][8][9]. This leads to an increase in area used for processor. Using ECC, the number of transistors can be cut back on since the numbers involved are much smaller than an RSA system with as similar-level security.

Most attacks on ECC are based on attacks on similar discrete algorithm problems, but these work out to be much slower due to the added complexity of point addition[10][11]. The methods to avoid each of the attacks have already been designed. The author proposed a new approach in the symmetric curves, which is called Probability Symmetric Curve Cryptography (PSCC). The proposed method will provide high security for the data.

The rest of this paper is organized as follows. The second section expresses the origin and characteristics of the PSCC. The third section shows the procedure for the point addition. The fourth section explored the process of the point doubling. The finite field operations for harder security are presented in the section five. The domain parameters of the PSCC are explained in the section six. The key pair generation for the PSCC is presented in the section seven. The final results were discussed and analyzed in section eight. The paper ended with the concluding remarks and the future challenges.

2. PROBABILITY SYMMETRIC CURVE CRYPTOGRAPHY
The most widely used distribution in the theory of probability is the probability symmetric curve. Another symmetric curve is the t-distribution curve. However for large values of n, t tends to normal and hence we prefer to use the normal curve, for the probability symmetric curve cryptography.

2.1 Probability Symmetric Curves
The general form of the equation of the normal curve with mean m and standard deviation σ is

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

where m is the mean of the distribution σ, the standard deviation.

Shifting the origin to m is equivalent to assuming $m = 0$.

Thus the normal probability curve is

$$y = \frac{1}{\sigma\sqrt{2\pi}} e^{-x^2/2\sigma^2}$$

This curve is symmetric with respect to y axis, it is bell shaped with two points of inflexion at -σ and +σ. This helps for any two points in the curve to cut it again in the third point. Interchanging x and y, we can take the equation as

$$x = \frac{1}{\sqrt{2\pi}\sigma} e^{-y^2/2\sigma^2} \qquad \text{……..(1)}$$

Now the curve is symmetric with respect to x axis. This form is more handy for our cryptographic applications.

Expressing y as a function of x in (1)

$$\sqrt{2\pi}\sigma x e^{y^2/2\sigma^2} = 1$$

Take logarithm both sides and assign $b = 2\sigma^2$ then,

$$y^2 = -b\ln(x) + c, \qquad \text{…….(2)}$$

where $c = -\frac{b}{2}\ln(b\pi)$

The equation (2) will produce the standard form of the equation

$$6y^2 = b\{11 - 18x + 9x^2 - 2x^3\} + c \qquad \text{……..(3)}$$

For brevity we designate the probability symmetric curve (3) by $N(b,c)$.

2.2. Characteristics of Probability Symmetric Curves

Differentiating equation (2) with respect to x gives

$$\frac{dy}{dx} = -b\frac{1}{2xy} \qquad \text{..……(4)}$$

(i) A point on the curve is singular if $\frac{dy}{dx}$ is not well defined. This is a point at which both numerator and denominator are zero. Thus the curve will be singular only if it contains a point (x, y) such that $b = 0$ and $2xy = 0$, the point (x, y) satisfying these two equations lies on the curve.

(ii) Let us consider the case when the underlying field is of characteristic two. In this case the derivative becomes $\frac{dy}{dx} = \infty$, since 2 is same as zero in the field. Thus the curve is not singular.

(iii) If the characteristic is 3, then three is same as zero. In this case for singularity, a condition in b is involved and hence not admissible.

3. ALGEBRAIC EQUATION FOR ADDING TWO POINTS ON THIS CURVE

Given two points P and Q on the curve $N(b,c)$, we have to draw a line through P and Q. If R is the point which the line again intersects $N(b,c)$ then $P+Q$ is the mirror reflection of R about the x-axis.

ie. $P + Q = -R$

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

$$\alpha = \frac{y_Q - y_P}{x_Q - x_P}$$

For any point (x, y) to line at the intersection of the straight line and the curve $N(b,c)$, the following equation must be true

$$6\alpha^2 x^2 + 6\beta^2 + 12\alpha\beta x = 11b - 18bx + 9bx^2 - 2bx^3 + c \qquad \text{…….(5)}$$

Since it is a 3rd degree equation, there are three points of intersection. Already two points correspond to P and Q and 3rd root is the x_R, the x co-ordinate of R. Now equation (5) reduces to

$$2bx^3 + (6\alpha^2 - 9b)x^2 + (12\alpha\beta + 18b)x + (6\beta^2 - 11b - c) = 0 \qquad \text{……. (6)}$$

We have the sum of the roots

$$x_P + x_Q + x_R = \frac{(9b - 6\alpha^2)}{2b}$$

$$x_R = -x_P - x_Q + \frac{(9b - 6\alpha^2)}{2b} \quad \text{..... (7)}$$

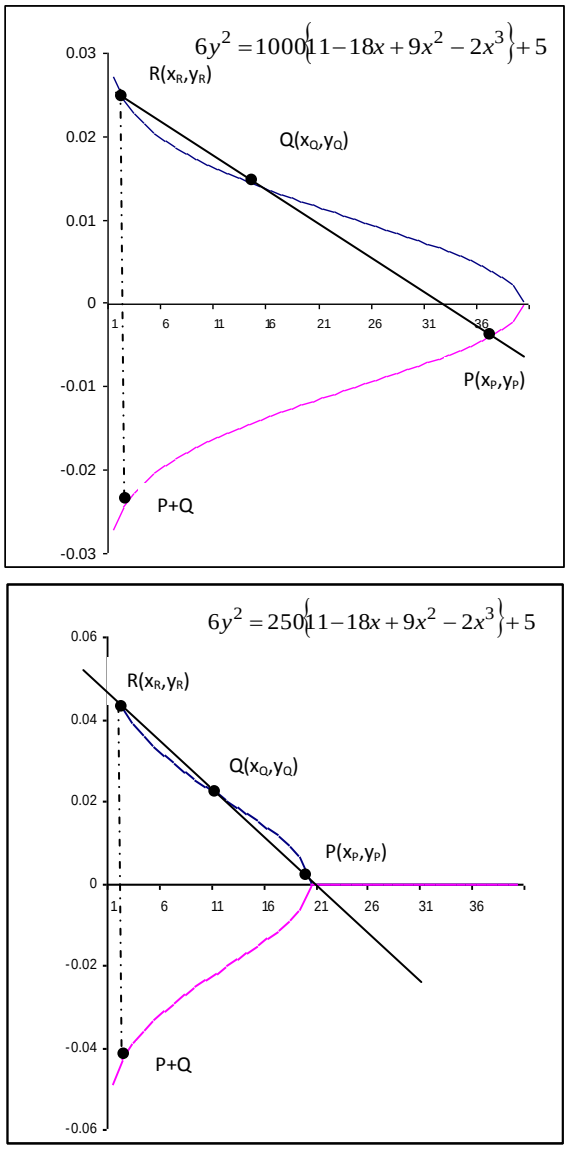


Fig-1 Point addition in Probability Symmetric Curve

Since (x_R , y_R) lie on $y = \alpha x + \beta$,

$$y_R = \alpha(x_R - x_P) + y_P \quad \text{..... (8)}$$

Since $P + Q = -R$

we have,

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

$$y_{P+Q} = \alpha(x_P - x_R) - y_P \quad \text{..... (10)}$$

Since y co-ordinate of the reflection $-R$ is negative of the y co-ordinate of the point R on the intersecting straight line. The illustrations for point additions are given in Figure 1.

4. AN ALGEBRAIC EXPRESSION FOR CALCULATING $2P$ FROM P

Computation of $2P$ by point multiplication [12] on $N(b,c)$, we draw a tangent at P and find the intersection of this tangent on the curve again leaving the point of intersection on the y -axis.

The slope of the tangent at (x, y) on $N(b,c)$ is

$$\alpha = -\frac{b}{2xy}$$

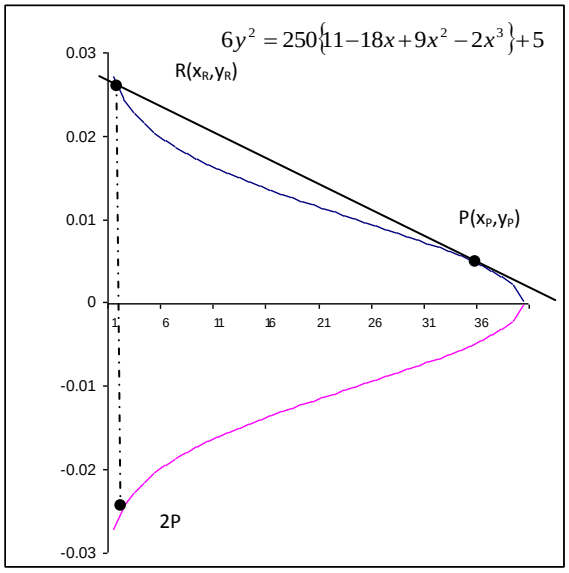
Hence the slope of the tangent at P is

$$\alpha = -\frac{b}{2x_P y_P} \quad \text{..... (11)}$$

Since drawing a tangent at P is the limiting case of drawing a line through P and Q as Q approaches P , two of the three roots of the equation

$$6(\alpha x + \beta)^2 = b\{11 - 18x + 9x^2 - 2x^3\} + c \quad \text{..... (12)}$$

must coalesce into the point x_P and the third root is x_R .



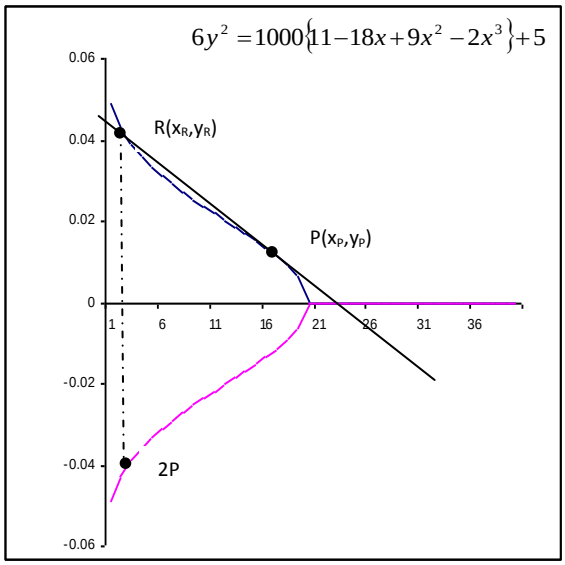


Fig-2 Point doubling in Probability Symmetric Curve

As before R is the point of intersection of the tangent with $N(b,c)$. Using (7)

$$x_R = -2x_P + \frac{(9b - 6\alpha^2)}{2b}$$

But,

$$\alpha = -\frac{b}{2x_P y_P} \quad \text{and} \quad \beta = \frac{2y_P^2 + b}{2y_P}$$

Thus if we draw a tangent at point P to the probability symmetric curve it will intersect the curve at R whose co-ordinates are given by

$$x_R = \frac{4bx_P^2 y_P^2 (9 - 4x_P) - 6b^2}{8bx_P^2 y_P^2}$$

$$y_R = \frac{b}{2x_P y_P}(x_P - x_R) + y_P$$

Since the value of $2P$ is the reflection of the point R about the x axis, the value of $2P$ is obtained by taking the negative of the y co-ordinate.

$$x_{2P} = \frac{4bx_P^2 y_P^2 (9 - 4x_P) - 6b^2}{8bx_P^2 y_P^2} \quad \ldots\ldots\ldots\ldots (13)$$

and

$$y_{2P} = \frac{b}{2x_P y_P}(x_R - x_P) - y_P \quad \ldots\ldots\ldots\ldots (14)$$

The illustrations for point doubling are given in Figure 2.

5. PROBABILITY SYMMETRIC CURVE ON FINITE FIELDS

The probability symmetric curve operations defined in the sections 3 and 4 are on real numbers. The operations over the real numbers are slower and inaccurate due to round-off error problems. The cryptographic operations required the faster and accurate results. To make the operations on probability symmetric curve accurate and more efficient, the curve cryptography is defined over Prime Field F_p [13][14][15]. The field is chosen with finitely large number of points suited for cryptographic operations.

5.1 Probability Symmetric Curve on Prime field F_p

The equation of the probability symmetric curve on a prime field F_p is given as

$6y^2 \bmod p = b\{11 - 18x + 9x^2 - 2x^3\} + c \bmod p$, where

$$\left(\frac{59b - 2c}{2b}\right) \bmod p \neq 0 \quad \ldots\ldots\ldots\ldots (15)$$

Here the elements of the finite field are integers between 0 and $p-1$. All the operations such as addition, subtraction, division and multiplication involve integers between 0 and $p-1$. The prime number p is chosen such that there is finitely large number of points on the $N(b,c)$ to make the cryptosystem secure. The graph for this Curve equation is not a smooth curve. Hence the geometrical explanation of point addition and doubling as in real numbers will not work here. However, the algebraic rules for point addition and point doubling can be adapted for $N(b,c)$ over F_p.

5.2 Point Addition

Consider two distinct points P and Q such that $P=(x_P,y_P)$ and $Q=(x_Q,y_Q)$.

Let $R=P+Q$ where $R=(x_R,y_R)$, then

$$x_R=-x_P-x_Q+\frac{(9b-6\alpha^2)}{2b}\bmod p$$ and

$$y_R=\alpha(x_P-x_R)-y_P \bmod p,\quad \alpha=\frac{y_Q-y_P}{x_Q-x_P}\bmod p,$$

α is the slope of the line through P and Q. If $Q=-P$ i.e. $Q=(x_P,-y_P)\bmod p$ then $P+Q=O$, where O is the point at infinity. If $Q=P$ then $P+Q=2P$ then point doubling equations are used.

5.3 Point Subtraction

Consider two distinct points P and Q such that $P=(x_P,y_P)$ and $Q=(x_Q,y_Q)$. Then $P-Q=P+(-Q)$ where $-Q=(x_Q,y_Q)\bmod p$. Point subtraction is used in certain implementation of point multiplication such as NAF (Non-Adjacent Form).

5.4 Point Doubling

Consider a point P such that $P=(x_P,y_P)$, where $y_P\neq 0$. Let $R=2P$ where $R=(x_R,y_R)$, then

$$x_R=-2x_P+\frac{(9b-6\alpha^2)}{2b}\bmod p$$ and

$$y_R=\frac{b}{2x_Py_P}(x_R-x_P)-y_P \bmod p,$$

$$\alpha=-\frac{b}{2x_Py_P}\bmod p \quad \text{and } \beta=\frac{2y_P^2+b}{2y_P}\bmod p,\ \alpha \text{ is}$$

the tangent at point P and b and c are the parameters chosen with the $N(b,c)$. If $y_P=0$ then $2P=O$, where O is the point at infinity.

6. PROBABILITY SYMMETRIC CURVE DOMAIN PARAMETERS

Apart from the curve parameters b and c, there are other parameters that must be agreed by both parties involved in secured and trusted communication using $N(b,c)$ are called domain parameters. Generally the protocols implementing the $N(b,c)$ specify the domain parameters to be used.

The operation of each of the public-key cryptographic schemes described in this document involves arithmetic operations on a $N(b,c)$ over a finite field determined by some of the domain parameters.

Two types of probability symmetric curve domain parameters may be used: Probability Symmetric curve domain parameters over F_p and Probability Symmetric curve domain parameters over F_{2^m}.

The domain parameters for $N(b,c)$ over F_p are a sextuple $T=(p,b,c,G,n,h)$, where p is the prime number defined for finite field F_p, b and c are the parameters defining the curve $6y^2 \bmod p=b\{11-18x+9x^2-2x^3\}+c \bmod p$, G is the generator point (x_G,y_G), a point on the probability symmetric curve chosen for cryptographic operations, n is the order of the $N(b,c)$. The scalar for point multiplication is chosen as a number between 0 and n – 1, h is the cofactor where h = #N(F_p)/n. #N(F_p) is the number of points on the $N(b,c)$.

7. PROBABILITY SYMMETRIC CURVE KEY PAIRS

All the public-key cryptographic schemes described in this document use key pairs known as Probability Symmetric curve key pairs. Given some probability symmetric curve domain parameters, $T=(p,b,c,G,n,h)$, a probability symmetric curve key pair (d,Q) associated with T consists of a probability symmetric curve secret key d which is an integer in the interval [1, n-1], and the curve public key $Q=(x_Q,y_Q)$ which is the point $Q=dG$.

8. RESULTS AND DISCUSSION

There are lot of symmetric curves in the literature[16]. Many of the curves are not suitable for the secure data transmission and digital signature applications. The Elliptic Curve Cryptography[5][7][9] was popularly used in lots of applications and research which helps in many secure transmission media. The Sextic Curve Cryptography[17] also proposed for the safety transmission. Instead of using the Elliptic Curve Cryptography and Sextic Curve Cryptography, it is possible to use the PSCC for secure transmission which is very easy to manipulate and

find out the points on the curve. Here the author shows the different methods of manipulating the points on the curve: using point addition, point doubling and in the finite field.

The PSCC will be applied in different situations for secure transmission as well as the digital signature standards. The constants of $N(b,c)$ may vary based on the condition. Different curves can be produced with the various parameters of b and c. Assume the values of b and c as 10 and 5, the probability symmetric curve for assumed values become $6y^2 = -20x^3 + 90x^2 - 180x + 115$. The Table-1 shows the list of points P and Q lies in the curve, which produced the corresponding point $P+Q$ which also lies on the same curve. The algebraic equation for point addition will produced the corresponding $P+Q$ points for the given points P and Q.

Table 1. Point Addition using the curve
$6y^2 = -20x^3 + 90x^2 - 180x + 115$

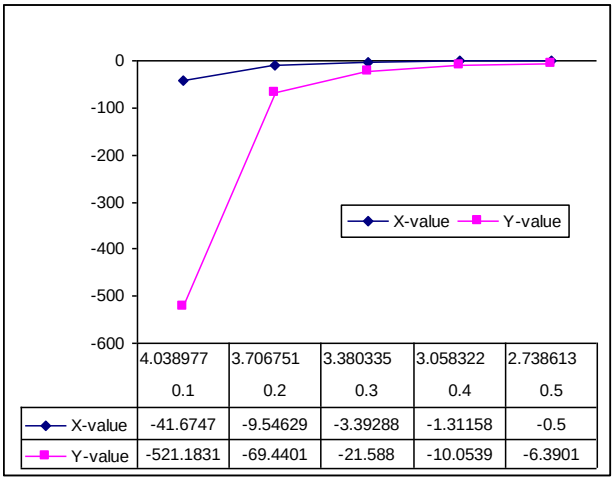
P	Q	P+Q
(0.1, 4.038977)	(0.5, 2.738613)	(0.729475, -1.99261)
(0.2, 3.706751)	(0.6, 2.417988)	(0.585796, -2.46375)
(0.3, 3.380335)	(0.7, 2.091252)	(0.384244, -3.10884)
(0.4, 3.058322)	(0.8, 1.749286)	(0.087044, -4.0825)
(0.5, 2.738613)	(0.9, 1.37356)	(-0.39380, -5.78888)

The algebraic equations for point doubling method applied in the PSCC produces $2P$, the point corresponding to the point P. The Table-2 shows $2P$, the list of points corresponding to the point P, which also lies on the same curve.

Table 2. Point doubling using the curve
$6y^2 = -20x^3 + 90x^2 - 180x + 115$

P	2P
(0.1, 4.038977)	(-41.6747, -521.1831)
(0.2, 3.706751)	(-9.54629, -69.4401)
(0.3, 3.380335)	(-3.39288, -21.588)
(0.4, 3.058322)	(-1.31158, -10.0539)
(0.5, 2.738613)	(-0.5, -6.3901)

The Figure-3 shows the x and y values of $2P$ corresponding to the point P of the curve $6y^2 = -20x^3 + 90x^2 - 180x + 115$, which says that when the x value increases the x and y values of the $2P$ also increases and which converges to zero. The points are calculated using the point doubling method.



	4.038977 0.1	3.706751 0.2	3.380335 0.3	3.058322 0.4	2.738613 0.5
X-value	-41.6747	-9.54629	-3.39288	-1.31158	-0.5
Y-value	-521.1831	-69.4401	-21.588	-10.0539	-6.3901

Fig-3 Point doubling plotting

For increasing the security, it is possible to use the prime field. Here the probability symmetric curve defined over F_{11} can get when the value of $p = 11$. The $\left(\frac{59b - 2c}{2b}\right) = 29 \equiv 7 \pmod{11} \neq 0$, so $N(10,5)$ is a probability symmetric curve. If (x, y) pass through the curve then the equation of $N(10,5)$ is of the form $6y^2 \pmod{11} = -20x^3 + 90x^2 - 180x + 115 \pmod{11}$

The Table-3 shows the different points on the curve $N(10,5)$ in the range [0.1, 1] when the interval is 0.1. There are thousands of points lie on the curve. For every x value it will produce two y values. The prime filed operations on the curve leads for more secure transmission.

Table 3. The points in
$6y^2 \pmod{11} = -20x^3 + 90x^2 - 180x + 115 \pmod{11}$

(0.1, 4.038977)	(0.1, 6.961023)	(0.2, 3.706751)	(0.2, 7.293249)
(0.3, 3.380335)	(0.3, 7.619665)	(0.4, 3.058322)	(0.4, 7.941678)
(0.5, 2.738613)	(0.5, 8.261387)	(0.6, 2.417988)	(0.6, 8.582012)
(0.7, 2.091252)	(0.7, 8.908748)	(0.8, 1.749286)	(0.8, 9.250714)
(0.9, 1.37356)	(0.9, 9.62644)	(1, 0.912871)	(1, 10.08713)

9. CONCLUSION

In this paper, the author proposed the new safety measures using the Probability Symmetric Curve. The point addition and point doubling presented here will create new chapter in the security issues. The techniques presented in the finite field will make better safety of data. We believe that the proposed method of PSCC is the blitzkrieg in the safety and security challenges in the communication technology.

The different values of b and c will produce the different curves; we can say that the harder security may get for a particular value of b and c. The PSCC over the binary field may boost the security features. The enhanced form of the PSC may produce better result in future.

10. REFERENCES

[1] William Stallings, "Cryptography and Network Security Principles and Practices", 3rd Ed., Pearson Education, 2004.

[2] Lee L. P. and Wong K. W., "A random number generator based elliptic curve operations", Computers and Mathematics with Applications, vol. 47, pp. 217-226, 2004.

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

[4] Menezes A., "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers, 1993.

[5] Atay S., Kottuksuz A, Hisil H. and Eren S., "Computational cost analysis of elliptic curve arithmetic", Proceedings of international conference on Hybrid Information Technology (ICHIT '06), vol.1, pp.578-582, 2006.

[6] Vivek Kapoor, Vivek Sonny Abraham and Ramesh Singh, "Elliptic Curve Cryptography", ACM Ubiquity, vol.9, pp.1-8, 2008.

[7] Alfred J Menezes and Scott A Vanstone, "Elliptic curve cryptosystems and their implementation", Journal of Cryptology, vol.6(4), pp.209-224, 2004.

[8] Gong G., Berson T. A. and Stinson D. R., "Elliptic curve pseudorandom sequence generators", Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography, LNCS 1758, pp 34-48, 1999.

[9] Shi Z. J. and Yan H., "Software implementations of elliptic curve cryptography", International Journal of Network Security, vol. 7(1), pp. 141-150, 2008.

[10] Berkhoff G. and Lane S. M., "A Survey of Modern Algebra", AKP Classics, USA, 2008.

[11] Koblitz N., "A Course in Number Theory and Cryptography", Springer Verlag, New York, 1984.

[12] Jarvinen K, Tommiska M. and Skytta J., "A scalable architecture for elliptic curve point multiplication", Proceedings of IEEE international conference on Field-Programmable Technology, pp.303-306, 2004.

[13] ElGamal T., "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information theory, vol. IT-31, pp.469-472, 1985.

[14] Hansen T. and Mullen G. L., "Primitive polynomials over finite fields", Mathematics of Computation, vol.59(200), pp. 639-643, 1992.

[15] Morain F., "Building cyclic elliptic curves modulo large primes", LNCS 547, pp. 328-336, 1990.

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

[17] Sam Emmanuel W.R. and Suyambulingom C., "Safety Measures Using Sextic Curve Cryptography", International Journal on Computer Science and Engineering, vol.3(2), pp.800-806,2011.