Safety Measures Using Sextic Curve Cryptography

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

Dr.C.Suyambulingom
Department of Mathematics,
Tamil Nadu Agricultural University,
Coimbatore, Tamil Nadu, India

Abstract - This paper proposes Sextic Curve Cryptography, which is used to increase the safety measures. The methods to find the critical points in the SCC based on Atriphtaloid symmetric curve using point addition and point doubling also explored here. The operations in finite fields makes the data more secure, which is expressed by several field operations. The experimental result shows the safety measures and harder security of data. The overall objective is to develop harder security measures using Sextic Curve Cryptography.

Keywords-Sextic Curve Cryptography; Domain Parameters; Point Addition; Point Doubling

I. INTRODUCTION

One of the fundamental tools used in information security is the signature. It is a building block for many other services such as non-repudiation, data origin authentication, identification, and witnessing. At contract age the signature evolves to take on a very integral part of the person's identity.

RSA and ECC[1][4] are very efficient algorithms used in signature. The code to implement ECC is no more complex than one that efficiently does modular arithmetic with big integers[5][9][12]. It is faster, at least for private key operations, since until someone comes up with a sub exponential algorithm for breaking ECC, the key can be smaller[7][8][10]. For public key operations, such as signature verification, RSA is likely to be faster, even with larger keys, because it can use a small public exponent[13]. The main advantage ECC has over RSA is that the basic operation in ECC is point addition, which is known to be computationally very expensive. To achieve reasonable security, a 1024-bit modulus would have to be used in a RSA system, while 160-bit modulus should be sufficient for ECC[14]. Most attacks on ECC are based on attacks on similar discrete algorithm problems[3][6], but these work out to be much slower due to the added complexity of point addition[2][11].

In order to rectify the problems faced in RSA and ECC, the author proposed the new approach in the symmetric curves, which is called Sextic Curve Cryptography (SCC). This proposed method will provide the harder safety measures.

The second section expresses the origin and characteristics of the SCC. The third and fourth sections produce the point calculation by point addition and point doubling. The methods to increase the harder security using finite fields, may available in the section five. The section six shows the key pair generation method. The experimental results and the discussion about the results are elaborated in the section seven. This paper concluded with the concluding remarks.

II. SEXTIC CURVE CRYPTOGRAPHY

The proposed SCC is defined from the Sextic Curves. As in the case of ECC the security of the derived curves grow exponentially in its parameters. In view of the smaller key sizes the new algorithms also can be implemented in smart cards without mathematical co-processors. It may also become important for wireless sensor networks.

A. Sextic Curves

Though there is a family of curves under this the most suitable one is Atriphtaloid, which is also called atriphtothlassic curve. The general form of the equation of the curve is

$x^4(x^2+y^2)-(ax^2-b)^2=0$, where a, b are the parameters.

The curve can be reduces to

$$x^2y^2 = a^2x^2 - 2abx + b^2 - x^3 \quad \text{.....(1)}$$

This equation is taken as the standard form throughout this paper. This equation involves additions and multiplications over objects that are represented by x, y, a and b with x always positive. The characteristic of this equation is zero. The forms of the curve for various parameters are presented in Figure 1.

The discriminant of the polynomial (1) is $b \neq 0$ and $2a^3 - b \neq 0$. Now for the curves to be non-degenerate, the above property should be satisfied. When the discriminant is zero, the curve will have cusps which should not be included in the analysis any further.

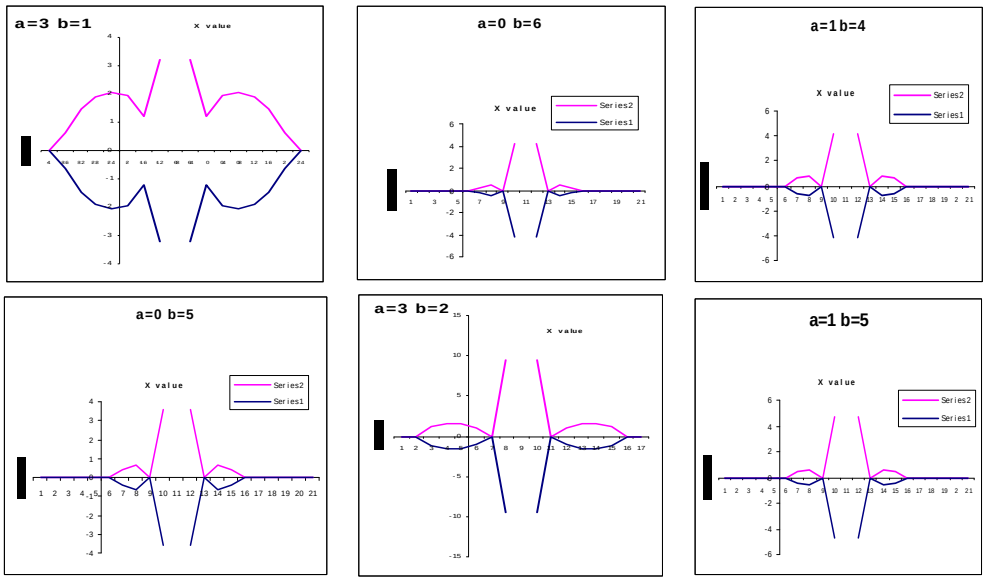


Figure 1. Forms of the curve for various parameters

Equation (1) shows that the SCC is symmetric with respect to x-axis. The non-zero value of the discriminant assures the existence of three distinct points on the curve which is used for addition and multiplication.

The points on SCC can be shown to constitute a group. Let P and Q be two points on the SCC. Now join P and Q by means of a straight line, the third point of intersection of the straight line with the curve, if such an intersection exist it is denoted by R. The mirror image of this point with respect to the x coordinate is the point P+Q. If the third point does not exist it is called a point at infinity. We denote this point at infinity by the symbol O, and this is used as the additive identity in the group operation.

We say that P+O = P for all P in the curve. The additive inverse of P is its mirror reflection with respect to the x axis. If Q denotes this point then Q = -P. We also say that, the mirror reflection of the point at infinity is same as the point at infinity. If we have a point at which the tangent is parallel to the y-axis, for this point the mirror image is itself. Here P + P = O.

We shall now define the addition of P with itself. If P and Q are distinct then there is no problem. The addition of P with itself is making the Q tends to P. In this case as Q tends to P, which implies that it will become

a tangent at P. Thus to find P+P, we draw a tangent at P find the cutting point of this tangent with the curve and take its mirror image. In case the tangent at P cuts the curve at infinity then P+P = O.

B. *Characteristics and Singularities of Sextic Curves*

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 S(a, b) will be singular only if it contains a point (x, y) such that $2abx - 2b^2 - x^3 = 0$ and $y = 0$ and the point (x, y) satisfying these two equations lies on the curve. Since $y = 0$, all the three points must be on the x-axis.

When the underlying field is of characteristic 2, thus the curve is not singular. When characteristics is two then it is not possible to crack. For the characteristic is 3, the curve becomes singular if

$$x^2 = \frac{2ab}{(2b^2 + 1)}$$

Thus when using the S(a, b) we avoid the field with characteristic 3 since it needs a constraint on the parameters in order for the curve to not become singular.

III. Point Addition In SCC

Let P and Q be two points on the curve S(a,b), we can draw a line through P and Q. Find the point at which this line again intersects S(a, b) if R denote this point then P+Q is the mirror reflection of R about the x-axis.

The equation of the straight line 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. For any point (x, y) to lie at the intersection of the straight line and the curve S(a, b), the equation $x^2(\alpha x + \beta)^2 = a^2x^2 - 2abx + b^2 - x^3$ must be true. Since it is a 4th degree equation, there are four points of intersection. The third point is the intersection on the y axis say S and the 4th root is the xR, the x co-ordinate of R. At S the x coordinate is zero, which implies that $b^2 = 0$.

We have, $x_{P+Q} = -x_P - x_Q - (1 + 2\alpha\beta)/\alpha^2$ and $y_{P+Q} = \alpha(x_P - x_R) - y_P$, where y coordinate of the reflection – R is negative of the y coordinate of the point R on the intersecting straight line. The illustrations for point addition are given in Figure 2.

IV. Point Doubling In SCC

To Compute 2P on S(a, b), 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. 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 $x(\alpha x + \beta)^2 = a^2x - 2ab - x^2$ must coalesce into the point xP and the third root is xR.

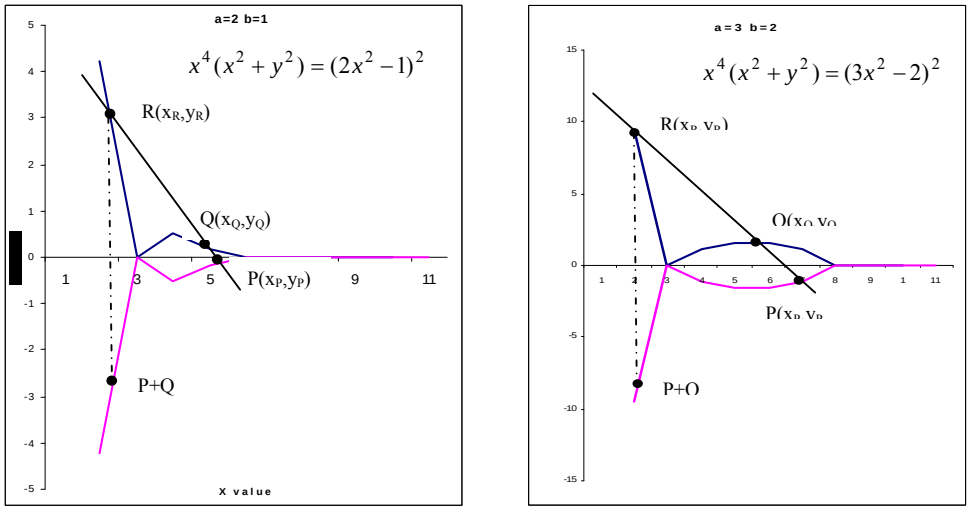


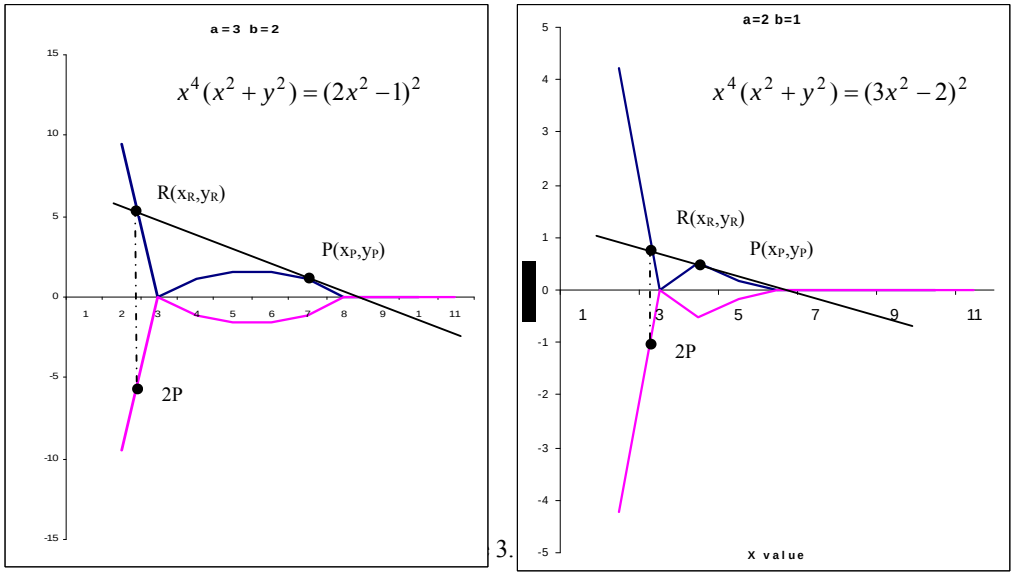
Figure 2. Point addition

The point R is the intersection of the tangent with the Atriphtaloid curve. Thus if we draw a tangent at point P to the Atriptaloid it will intersect the curve at R.

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-coordinate.

$$\therefore x_{2P} = -2x_P - \left[\frac{4x_P^4 y_P^2 + 2x_P\left(2ab - x_P^2\right)\left(2x_P y_P^2 - 2ab + x_P^2\right)}{\left(2ab - x_P^2\right)^2}\right] \text{ and } y_{2P} = \frac{2ab - x_P^2}{2x_P^2 y_P}(x_P - x_R) - y_P$$

The illustrations for point doubling are given in Figure 3.



3.

V. SEXTIC CURVES IN FINITE FIELDS

The Sextic Curve operations defined in the sections 3 and 4 are on real numbers. Operations over the real numbers are slow and inaccurate due to round-off error. Cryptographic operations need to be faster and accurate. To make operations on Sextic Curve accurate and more efficient, the curve cryptography is defined over Prime field F_p.

The field is chosen with finitely large number of points suited for cryptographic operations.

C. *SC on Prime Field* F_p

The equation of the Sextic Curve on a prime field F_p is

$$x^2y^2 \bmod p = b^2 - 2abx + a^2x^2 - x^3 \bmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

where $b \bmod p \neq 0$ and $2a^3 - b \bmod p \neq 0$. Here the elements of the finite field are integers between 0 and p–1. All the operations such as addition, substation, 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 Sextic Curve to make the cryptosystem secure. The graph for this Sextic 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 Sextic Curve over F_p.

D. *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 $x_R = -x_P - x_Q - (1+2\alpha\beta)/\alpha^2 \bmod p$ and $y_R = \alpha(x_P - x_R) - y_P \bmod p$, where $\alpha = \frac{y_Q - y_P}{x_Q - x_P} \bmod p$,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.

E. *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).

F. *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 $x_R = -2x_P - \left[\frac{1+2\alpha\beta}{\alpha^2}\right] \bmod p$ and $y_R = \alpha(x_P - x_R) - y_P \bmod p$, where $\alpha = \frac{2ab - x_P^2}{2x_P^2 y_P} \bmod p$, $\beta = y_P - \alpha x_P \bmod p$, a and b are the parameters chosen with the Sextic Curve. If $y_P = 0$ then $2P = O$, where O is the point at infinity.

VI. SEXTIC CURVE DOMAIN PARAMETERS

Apart from the curve parameters a and b, there are other parameters that must be agreed by both parties involved in secured and trusted communication using SCC. Generally the protocols implementing the SCC 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 Sextic curve over a finite field determined by some Sextic curve domain parameters.

A. *Domain Parameters For SC Over Field* F_p

The domain parameters for Sextic curve over F_p are a sextuple $T=(p, a, b, G, n, h)$, where p is the prime number defined for finite field F_p, a and b are the parameters defining the curve (2), G is the generator point (x_G, y_G), a point on the Sextic curve chosen for cryptographic operations, n is the order of the Sextic curve. The scalar for point multiplication is chosen as a number between 0 and n – 1, h is the cofactor where h = #S(F_p)/n. #S(F_p) is the number of points on a Sextic curve.

B. *SC Domain Parameters Over* F_p *Generation Primitive*

The approximate security level in bits required from the Sextic curve domain parameters must be an integer t. The output shows the Sextic curve domain parameters over F_p such that taking logarithms on the associated Sextic curve requires approximately 2t operations.

Select a prime p such that $\lceil \log_2 p \rceil = 2t$ if $t \neq 256$ and such that $\lceil \log_2 p \rceil = 521$ if $t = 256$ to determine the finite field F_p. Select elements $a, b \in F_p$ to determine the Sextic curve $S(F_p)$ defined by the equation (2), a base point $G=(x_G, y_G)$ on $S(F_p)$ a prime n which is the order of G, and an integer h which is the cofactor h=#S(F_p)/n, subject to the constraints: $b \bmod p \neq 0$ and $2a^3 - b \bmod p \neq 0$, #S(F_p) ≠ p, $p^B \neq 1 (\bmod n)$ for any $1 \leq B \leq 20$ and $h \leq 4$.

This primitive allows any of the known curve selection methods to be used. However to foster interoperability it is strongly recommended that implementers use one of the Sextic curve domain parameters over F_p.

C. SC Domain Parameters Over F_p Validation Primitive

Sextic curve domain parameters over F_p along with an integer t which is the approximate security level in bits required from the Sextic curve domain parameters. The output indicated that whether the Sextic curve domain parameters are valid or not. To validate the Sextic curve domain parameters over F_p we have to check that p is an odd prime such that $\lceil \log_2 p \rceil = 2t$ if $t \neq 256$. Also we have to check that a, b, xG and yG are integers in the interval [0, p-1], $b \bmod p \neq 0$ and $2a^3 - b \bmod p \neq 0$, $x_G^2 y_G^2 \equiv b^2 - 2abx_G + a^2 x_G^2 - x_G^3 \pmod p$, n is prime, h ≤ 4, and that $h = \left\lfloor \left(\sqrt{p}+1\right)^2 / n \right\rfloor$, nG = O, $q^B \neq 1 \pmod n$ for any 1 ≤B < 20, and that $nh \neq p$. If any of the checks fail, output 'invalid', otherwise output 'valid'.

VII. Sextic Curve Key Pairs

All the public-key cryptographic schemes described in this paper use key pairs known as Sextic curve key pairs. A Sextic curve key pair (d,Q) associated with T consists of a Sextic curve secret key d which is an integer in the interval [1, n-1], and a Sextic curve public key $Q = (x_Q, y_Q)$ which is the point $Q = dG$.

VIII. Results and Discussions

The proposed method analyzed and verified with different parameters of Sextic Curve. The Table-1 and Table-2 shows the list of points, while doing the point addition and point doubling. The Table-1 shows the list of points of P+Q of the Sextic Curve $x^2y^2 = -x^3 + 4x^2 - 4x + 1$ when the different set of coordinators of the points P and Q lies on the same curve. The point P+Q of the Table-I is produced by the method of point addition.

TABLE I. POINT ADDITION USING THE CURVE $x^2y^2 = -x^3 + 4x^2 - 4x + 1$

P	Q	P+Q
(1, 0)	(1.7, 0.541368)	(-2.3719, 2.607772)
(1.05, 0.217958)	(1.25, 0.43589)	(-1.44225, 2.49775)
(1.1, 0.300138)	(1.4, 0.503052)	(-3.37332, 2.725528)
(1.15, 0.357607)	(1.6, 0.539096)	(-8.3712, 3.482386)
(1.2, 0.401386)	(1.4, 0.503052)	(-5.64927, 3.080282)

The Table-II shows the list of points of 2P of the Sextic Curve $x^2y^2 = -x^3 + 4x^2 - 4x + 1$ when the corresponding list of point P lies on the same curve. The list of points, 2P shown in Table-2 is produced by the method of point doubling.

TABLE II. POINT DOUBLING USING THE CURVE $x^2y^2 = -x^3 + 4x^2 - 4x + 1$

P	2P
(1.05, 0.217958)	(-0.09982, 6.714228)
(1.1, 0.300138)	(-0.22405, 4.785805)
(1.15, 0.357607)	(-0.37746, 3.966208)
(1.2, 0.401386)	(-0.56641, 3.510402)
(1.25, 0.43589)	(-0.79947, 3.231526)

The Sextic Curve over the prime field defined over F_{11} is expressed by the curve $x^2y^2 = -x^3 + 225x^2 - 270x + 81$, by taking p = 11, a = 15 and b = 9. Here b ≠ 0 and 2a3-b = 6741 ≡ 9 (mod 11) ≠ 0, so S is indeed a Sextic Curve. The Table III shows the list of points in $S(F_{11})$.

TABLE III. THE POINTS IN $S(F_{11})$

(1, 5.91608)	(1, 5.08392)	(2, 10.40433)	(2, 0.595674)
(3, 0.874342)	(3, 10.12566)	(4, 1.59216)	(4, 9.40784)
(5, 2.009227)	(5, 8.990773)	(6, 2.275918)	(6, 8.724082)
(7, 2.456658)	(7, 8.543342)	(8, 2.583653)	(8, 8.416347)
(9, 2.674794)	(9, 8.325206)	(10, 2.740815)	(10, 8.259185)

IX. CONCLUSIONS

The existing models are not sufficient to maintain perfect security. The proposed SCC gives the valuable safety and security mechanisms in the communication field. The SCC indicates that any symmetric curve, with preferably a cubic in x can better be used in the place of elliptic curves. The curve arithmetic of SCC, expressed here will produce the new valuable security for different forms of data in the communication field.

REFERENCES

[1] Abi-Char P.E., Mhamed A., El-Hassan B., (2007), A secure authentication key agreement protocol based on elliptic curve cryptography; Proceedings of the international symposium on Information Assurance and Security (IAS 2007), pp.89-94.

[2] Abi-Char P.E., Mhamed A., and El-Hassan B., (2007), A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications, Proceedings of the international conference on Next generation mobile applications, services and technologies (NGMAST '07), pp.235-240.

[3] Al-Daoud E, Mahmod R., Rushdan M. and Kilicman A., (2002), A new addition formula for elliptic curves over GF(2^n), IEEE Transactions on Computers, Vol.51, No.8, pp.972-975.

[4] Alfred J Menezes and Scott A Vanstone, (2004), Elliptic curve cryptosystems and their implementation, Journal of Cryptology, Vol.6, No.4, pp.209-224.

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

[6] Brian King (2009), Mappind an Arbitary message to an Elliptic Curve when defined over GF(2^n), International Journal of Network Security, Vol.8, No.2, pp.169-176.

[7] Christopher Doche and Laurent Imbert, (2006), Extended double-base number system with applications to elliptic curve cryptography (INDOCRYPT 2006), Springer-Verlag Berlin Heidelberg, LNCS 4329, pp.335-348.

[8] Gueron S and Kounavis M, (2008), A Technique for accelerating characteristic 2 Elliptic curve cryptography, Proceedings of fifth international conference on Information Technology: New Generations, pp.265-272.

[9] Howon Kim, Thomas Wollinger, Doo-Ho Choi, Dong-Grrk Han and Hun-Kyu Lee, (2008), Hyper elliptic Crypto-coprocessor over affine and projective coordinates, ETRI Journal, Vol.30, No.3, pp.365-376.

[10] Hyun Min Choi, Chun Pyo Hong and Chang Hoon Kim, (2008), High performance elliptic curve cryptographic processor over GF(2^{163}), Proceedings of IEEE international symposium on Electronic Design, Test and Applications (DELTA 2008), pp.290-295.

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

[12] Morales-Sandoval M. and Feregrino-Uribe C. , (2006), GF(2^m) arithmetic modules for elliptic curve cryptography, Proceedings of the international conference on reconfigurable computing and FPGA's (ReConFig 2006), pp.1-8.

[13] Nel Koblitz, Algred Menezes and Scott Vanstone, (2000), The state of elliptic curve cryptography, Journal of Designs, Codes and Cryptography, Vol.19, pp.173-193.

[14] Vivek Kapoor, Vivek Sonny Abraham and Ramesh Singh, (2008), Elliptic Curve Cryptography; ACM Ubiquity, Vol.9, pp.1-8.

AUTHORS PROFILE

W.R. Sam Emmanuel, from INDIA, He received MPhil degrees in the fields of Computer Science and Library Science. He is currently pursuing the Ph.D. degree.

He is working as an Assistant Professor at the Computer Science Department of Nesamony Memorial Christian College, Marthandam, Tamil Nadu, India from the year 2000. He has more than 10 years teaching experience in the field of Computer Science. He has several publications in national and international journals. He had published the book "Data Encryption Algorithms" (India: Tony's Publications, 2007). His research interests include data encryption, image encryption, video encryption, compression, multimedia security, Cryptography, Security of e-resources.

Mr. Emmanuel is an associate member of "Computer Society of India", life member of "Indian Society for Technical Education", the member of "International Association of Computer Science and Information Technology", the member of "International Association of Engineers" and also the life member of SALIS