International Journal of Electrical and Computer Engineering (IJECE)
Vol.1, No.2, December 2011, pp. 195~201
ISSN: 2088-8708

A Survey Report on Elliptic Curve Cryptography

Samta Gajbhiye, Monisha Sharma, Samir Dashputre
Shri Shankaracharaya College of Engg. and Technology, Junwani ,Bhilai , Chhattisgarh, India
91-0788-2291605
e-mail: samta.gajbhiye@gmail.com, monisha.sharma10@gmail.com, samir231973@gmail.com

Abstract

The paper presents an extensive and careful study of elliptic curve cryptography (ECC) and its applications. This paper also discuss the arithmetic involved in elliptic curve and how these curve operations is crucial in determining the performance of cryptographic systems. It also presents different forms of elliptic curve in various coordinate system , specifying which is most widely used and why. It also explains how isogenenies between elliptic curve provides the secure ECC. Exentended form of elliptic curve i.e hyperelliptic curve has been presented here with its pros and cons. Performance of ECC and HEC is also discussed based on scalar multiplication and DLP.

Keywords*: Elliptic curve cryptography (ECC), isogenies, hyperelliptic curve (HEC) , Discrete Logarithm Problem (DLP), Integer Factorization , Binary Field, Prime Field*

1. Introduction

Public key cryptosystems are constructed by relying on the hardness of mathematical problem. RSA based on Integer Factorization Problem and DH based on the Discrete Logarithm Problem. The main problem of conventional Public key Cryptosystems is that the Key size has to be sufficiently large in order to meet the high level security requirement, resulting in lower speed and consumption of more bandwidth.

Elliptic curves have a rich and beautiful history, having been studied by mathematicians for over a hundred years. They have been deployed in diverse areas like :Number theory(proving Fermat`s Last Theorem) in 1995 [1], modern physics: String theory(The notion of a point-like particle is replaced by a curve-like string.), Elliptic Curve Cryptography(An efficient public key cryptographic system).

In 1985, Neal Koblitz [2] and Victor Miller [3] independently proposed using elliptic curves to design public key cryptographic systems. In the late 1990`s, ECC was standardized by a number of organizations such as ANSI [4, 5], IEEE[4,6], ISO[7, 8], NIST[9, 10] and it started receiving commercial acceptance. Nowadays, it is mainly used in the resource constrained environments, such as ad-hoc wireless networks and mobile networks. There is a trend that conventional public key cryptographic systems are gradually replaced with ECC systems.

In Sep'2000 Daniel V. Bailey and Christof Paar [11] showed efficient arithmetic in finite field extensions with application in *elliptic curve cryptography.*

In May 2002, M. Bednara, M. Daldrup, J. Shokrollahi, J. Teich, and J. von zur Gathen[12] , showed how an elliptic curve coprocessor based on the Montgomery algorithm for curve multiplication can be implemented using our generic coprocessor architecture.

In *February, 2005*, the NSA announced that it had decided on a strategy of adopting *elliptic curve cryptography* as part of a US government standard in securing sensitive-but-unclassified information. The NSA recommended group of algorithms called Suite B, including Elliptic-Curve Menezes-Qu-Vanstone and Elliptic-Curve Diffie-Hellman for key agreement, and the Elliptic Curve Digital Signature Algorithm for digital signatures. The suite also included AES.

In 2010 [13]Brian King provided a deterministic method that guarantees ,the map of a message to an elliptic curve point can be made without any modification.

In 1988 Koblitz suggested for the first time the generalization of EC to curves of higher genus namely hyper elliptic curves (HEC)[40]. Since then HEC has been analyzed and implemented in software [41-45] and hardware [46, 47]both.

2. Alternative representations of Elliptic curve

In this section, various forms of elliptic curve has been explored

2.1. Weierstrass curve

An elliptic curve E over a field K is defined by an equation (Weierstrass equation)

$$E : y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$,
where Δ is the discriminant of E and is defined as follows:

Received Oct 8th, 2011; Revised Nov 29th, 2011; Accepted Dec 8th, 2011

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

If both the coordinates of the point P ∈ E or P=∞(the point at infinity, or zero element. The set of points on E is:

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1\, xy+ a_3\, y-x^3 - a_2x^2 - a_4x - a_6 = 0\}\cup\{\infty\} \quad (2)$$

2.2. Hessian curve

This curve[14] was suggested for application in elliptic curve cryptography because arithmetic in this curve representation is faster and needs less memory than arithmetic in standard Weierstrass form

2.3. Edwards curve

This curve was introduced in 2007 by Edward[15] and in Bernstein and Lange [16] pointed out several advantages of the Edwards form in comparison to the more well known weierstrass form.

2.4. Twists of curve

In mathematics an elliptic curve E over a field K has its quadratic twist, that is another elliptic curve which is isomorphic to E over an algebric of K. In particular, an isomorphism between elliptic curves is an isogeny of degree 1, that is an invertible isogeny. Some curves have higher order twists such as cubic and quartic twists. The curve and its twists have the same j-invariant and is shown in [17]. Twisted Hessian curve [18] represents a generalization of Hessian curve. It was introduced in elliptic curvecryptography to speed up the addition and doubling formulas and to have strongly unified arithmetic. Twisted Edward curve [19] are plane models of elliptic curve, a generalisation of Edward curves introduced by Bernstein (2007).

2.5. Jacobian curve

It [20] is used in cryptography instead of the Weierstrass form because it can provide a defence against simple and differential power analysis style (SPA) attacks and also faster arithmetic compared to the Weierstrass curve.

2.6 . Montgomery curve

This curve was introduced by Peter L Montomery [21] , and it has been used since 1987 for certain computations,and in particular in different cryptography applications.

3. Arithemetic used in Elliptic curve

Let E be an elliptic curve defined over the field K(binary field , prime field or extension field). There is a chord-and-tangent rule for adding two points in E(K) to give a third point in E(K). Together with this addition operation, the set of points E(K) forms an abelian group with ∞ serving as its identity. It is this group that is used in the construction of elliptic curve cryptographic systems. This addition and doubling of points rule is best explained in [22]. This is known as group law.

The addition rule is best explained geometrically. Let *P = (x1, y1)* and *Q = (x2, y2)* be two distinct points on an elliptic curve *E*. Then the *sum R*, of *P* and *Q*, is defined as follows. First draw a line through *P* and *Q*; this line intersects the elliptic curve at a third point. Then *R* is the reflection of this point about the *x*-axis. This is depicted in Figure 1.

Similarly the double *R*, of *P*, is defined as follows. First draw the tangent line to the elliptic curve at *P*. This line intersects the elliptic curve at a second point. Then *R* is the reflection of this point about the *x*-axis. This is depicted in Figure 2.

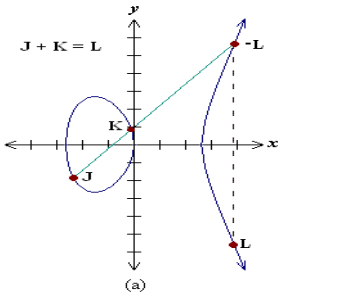

Figure 1. Geometric addition on elliptic curve points

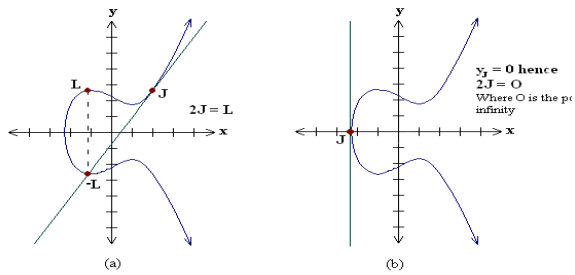

Figure 2. Geometric doubling on elliptic curve points

Hasse's theorem on elliptic curves [24] bounds the number of points on an elliptic curve over a finite field above and below. If $\#E(\mathbf{F_q})$ is the number of points on the elliptic curve E over a finite field with q elements, then Helmut Hasse's result states that

$$q+1-2\sqrt{q} \leq \#E(\mathbf{F_q}) \leq q+1+2\sqrt{q} \quad (3)$$

4. Field theory of Elliptic Curve

This section introduces the mathematical concepts necessary to understand and implement the arithmetic operations on an elliptic curve over a finite field(Galois field) [23]. Abstractly a finite field consists of a finite set of objects called field elements together with the description of two operations - addition and multiplication - that can be performed on pairs of field elements. These operations must possess certain properties. The finite field containing q elements is denoted by Fq. Generally two types of finite fields Fq are used — finite fields F_p with $q= p$, p an odd prime which are called prime finite fields, and finite fields F_2^m with $q=2^m$ for some $m>=1$ which are called characteristic two finite fields.

4.1. Finite field $\mathbf{F_p}$

The elements of F_p should be represented by the set of integers: {0, 1, 2… ,p-1} with operations as follows: If $a, b \in Fp$

Addition:, then $a+b = r$ in F p, where $r \in [0.. p-1]$ is the remainder.

Multiplication: then $a. b=s$ in F p, where $s \in [0.. p-1]$ is the remainder

Additive inverse: then the additive inverse $(-a)$ of a in F_p is the unique solution to the equation $a+x \equiv 0 \pmod p$.

Multiplicative inverse: $a\neq0$, then the multiplicative inverse a^{-1} of a in F_p is the unique solution to the equation $a. x \equiv 1 \pmod p$.

The prime finite fields F_p used should have:

$\log_2 p \in \{112,128;,,160;,192,;224;,256,;384,521\}$. This restriction is designed to facilitate interoperability in terms of computation and communication since p is aligned with word size.

4.2. The Finite Field F_2^m

The finite field F_2^m is the characteristic 2 finite field containing 2^m elements. Here the elements of F_2^m should be represented by the set of binary polynomials of degree m-1 or less:

$\{a_{m-1}x^{m-1}+ a_{m-2}x^{m-2}+. . . . . +a_1x+a_0 : a_i \in \{0;1\}\}$

with addition and multiplication defined in terms of an irreducible binary polynomial $f(x)$ of degree m,

known as the reduction polynomial, as follows:

If $a = a_{m-1}x^{m-1}+ a_{m-2}x^{m-2}+. . . . .+a_0$, $b = b_{m-1}x^{m-1}+ b_{m-2}x^{m-2}+. . . . .+b_0 \in F_2$,

Addition: then $a+b = r$ in F_2^m, where

$r = r_{m-1}x^{m-1}+ r_{m-2}x^{m-2}+. . . . .+a_0$ with $r_i \equiv a_i+b_i \pmod 2$.

Multiplication: then $a:b = s$ in F2m,

where $s = s_{m-1}x^{m-1}+sr_{m-2}x^{m-2}+. . . . .+s_0$ is the remainder when the polynomial $a.b$ is divided by $f(x)$ with all coefficient arithmetic performed modulo 2.

In this representation of F_2^m, the additive identity or zero element is the polynomial 0, and the multiplicative identity is the polynomial 1. Additive inverses and multiplicative inverses in F_2^m can be calculated efficiently using the extended Euclidean algorithm. Division and subtraction are defined in terms of additive and multiplicative inverses. Here the characteristic two finite fields F_2^m used should have:

$m \in \{113, 131, 163 ,193, 233, 239, 283, 409,571\}$

5. Elliptic curve domain parameters

Two types of elliptic curve domain parameters may be used: elliptic curve domain parameters over $\mathbf{F_p}$ and elliptic curve domain parameters over F_2^m . Domain parameters for Elliptic curve are specified in [25]. ECC uses modular arithmetic or polynomial arithmetic for its operations depending on the field chosen.

5.1. Parameters over $\mathbf{F_p}$

The domain parameters for Elliptic curve over F_p are p, a, b, G, n and h, where p is the prime number defined for finite field F_p , a *and* b are the parameters defining the curve $y^2 \bmod p = x^3 + ax + b \bmod p$, G is the generator point (x_G, y_G), n is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and $n – 1$, h is the cofactor where $h = \#E(F_p)/n$, $\#E(F_p)$ is the number of points on an elliptic curve.

5.2. Parameters over $\mathbf{F_2^m}$

The domain parameters for elliptic curve over F_2^m are $m, f(x), a, b, G, n$ *and* h , where m is an integer defined for finite field F_2^m. The elements of the finite field F_2^m are integers of length at most m bits , $f(x)$ is the

irreducible polynomial of degree m used for elliptic curve operations , *a* and *b* are the parameters defining the curve $y^2 + xy = x^3 + ax^2 + b$, *G* is the generator point (x_G, y_G), a point on the elliptic curve chosen for cryptographic operations , *n* is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between *0* and $n - 1$, *h* is the cofactor where $h = \#E(F_2^m)/n$, $\#E(F_2^m)$ is the number of points on an elliptic curve.

6. EC representation in different coordinate system

In order to add two points on elliptic curve E one needs, not only several additions and multiplications in F_q but also an inversion operation. The inversion is one to two orders of magnitude slower than multiplication. Fortunately, points on a curve can be represented in different coordinate systems which do not require an inversion operation to add two points. Various coordinate system are represented in Table 1 : An additional speed-up is possible if mixed coordinates are used for point addition and doubling[36].

Table 1 Representation of point and number of GF (p) elements

Coordinate system	Coordinates	Elements in GF (p)
Affine *A*	(x, y)	2
Projective *P*	(X, Y, Z)	3
Jacobian *J*	(X, Y, Z)	3
Chudnovsky Jacobian J^c	(X,Y,Z,Z^2, Z^3)	5
Modified Jacobian J^m	(X, Y, Z, aZ^4)	4

Table 2 Number of operations for adding and doubling points in different coordinate system.

Coordinate system	Addition	Doubling
Affine A	2M + S + I	2M + 2S + I
Projective P	12M + 2S	8M + 5S
Jacobian J	12M + 4S	4M + 6S
Chudnovsky Jacobian JC	11M + 3S	5M + 6S
Modified Jacobian J M	13M + 6S	4M + 4S

7. Integer factorization

Factoring is the act of splitting an integer into a set of smaller integers (factors) which, when multiplied together, form the original integer. For example, the factors of 15 are 3 and 5; the factoring problem is to find 3 and 5 when given 15. Prime factorization requires splitting an integer into factors that are prime numbers; every integer has a unique prime factorization. Multiplying two prime integers together is easy, but as far as we know, factoring the product of two (or more) prime numbers is much more difficult.

Factoring is the underlying, presumably hard problem upon which several public-key cryptosystems are based, including the RSA algorithm [33-35]. Factoring an RSA modulus would allow an attacker to figure out the private key; thus, anyone who can factor the modulus can decrypt messages and forge signatures. The security of the RSA algorithm depends on the factoring problem being difficult and the presence of no other types of attack. This is why the size of the modulus in the RSA algorithm determines how secure an actual use of the RSA cryptosystem is. Namely, an RSA modulus is the product of two large primes; with a larger modulus, the primes become larger and hence an attacker needs more time to factor it.

8. Discrete logarithm problem

If the elliptic curve groups is described using multiplicative notation, then the elliptic curve discrete logarithm problem is: given points P and Q in the group, find a number that Pk = Q; k is called the discrete logarithm of Q to the base P($k = \log_P Q$). When the elliptic curve group is described using additive notation, the elliptic curve discrete logarithm problem is: given points P and Q in the group, find a number k such that Pk = Q . n a real application, k would be large enough such that it would be infeasible to determine k.

Eg: What is the least integer *k* such that $5^k = 2$? [under multiplication modulo 7]

Answer: $((5 \times_7 5 = 4) \times_7 5 = 6) \times_7 5 = 2$.

So $5^4 = 2$. Or, $\log_5(2) = 4$.

The direct effect of this is that using elliptic curves over smaller finite field yields the same security as using discrete log or factoring based public key crypto systems of Diffie-Hellman and RSA with larger moduli.

9. Isogenies of elliptic curve

Isogenies are group homomorphisms [26 – 29]. They are used in algorithms for point counting on elliptic curves and for computing class polynomials for the complex multiplication (CM) method. They have applications to cryptanalysis of elliptic curve cryptosystems. They also have constructive applications: prevention of certain side

channel attacks; computing distortion maps for pairing-based cryptography; designing cryptographic hash functions; relating the discrete logarithm problem on elliptic curves with the same number of points.

The first application of isogenies to cryptography was as a tool in the Schoof- Elkies-Atkins (SEA) algorithm for counting the number of points on elliptic Curves over finitefields [30]. Originally Schoof had provided an algorithm that, when given a curve E defined over some finite field Fq , would return the number of points in the group of points on E defined over Fq . Earlier it has the complexity of $O(n^{5+e})$. Later the SEA improvement results in a complexity of $O(n^{4+e})$.This improvement fundamentally uses isogenies. More recently, isogenies have been used as a tool to analyze the computational difficulty of the elliptic curve discrete log problem (ECDLP) [31]. Specifically, the paper shows that isogenies can be used to create a randomized algorithm that will reduce the ECDLP from one set of curves to a significantly larger set of curves in polynomial time. Isogenies have also been proposed as a tool in constructing random number generators and hash functions [32].

10. .Hyper elliptic curve

A hyperelliptic curve (over the complex numbers) is an algebraic curve given by an equation of the form $y^2 = f(x)$, where $f(x)$ is a polynomial of degree $n > 4$ with n distinct roots. A hyperelliptic function is a function from the function field of such a curve; or possibly on the Jacobian variety on the curve, these being two concepts that are same for the elliptic function case, but different in this case.

The degree of the polynomial determines the genus of the curve: a polynomial of degree $2g + 1$ or $2g + 2$ gives a curve of genus g. When the degree is equal to $2g + 1$, the curve is called an imaginary hyperelliptic curve. Meanwhile, the curve that has degree $2g + 2$ is mentioned a real hyperelliptic curve. This statement about genus remains true for $g = 0$ or 1, but those curves are not called "hyperelliptic". Rather, the case $g = 1$ (if we choose a distinguished point) is an elliptic curve. All curves of genus 2 are hyperelliptic, but for genus ≥ 3 the generic curve is not hyperelliptic. Hyperelliptic curves can be used in cryptosystems based on the discerete logarithm problem [40]. The security of hyperelliptic cryptosystems is based upon the difficulty of solving the discrete logarithm problem in the Jacobian of the curve.

11. ECC implementation

ECC can be implemented in software and hardware [37]. Software ECC implementation provide moderate speed, higher power consumption and also have very limited physical security w.r.t key storage. Where as hardware implementation improves performance in terms of flexibility. Also hardware implementation provides greator security since they cannot be easily modified or read by an outside attacker. [38] specified an approach to combine the advantages of software and hardware in new paradigm of computation referred as *reconfigurable computing.*

12. Implementation issues in ecc

The most time consuming operation in ECC cryptographic schemes is the scalar multiplication (kP). Efficient hardware and software implementation of scalar multiplication have been the main research topic on ECC in recent years. [38] shows elliptic curve scalar multiplication according to three layers. Upper layer shows different algorithm to perform the multiplication. In middle layer there are several combinations for finite field representation and coordinate system. The lower level is about finite field operation and arithemetic. An efficient implementation of ECC over binary Galois field in normal and polynomial bases has been proposed by Ester and Henies [39].

13. Conclusion

Although ECC is a promising candidtate for public key cryptosystem, its security has not been completely evaluated. The ECC has been shown to have many advantages due to its ability to provide the same level of security as RSA yet using shorter keys. Implementing ECC with the combination of software and hardware is advantages as it provides flexibilty and good performance. Its disadvantage is its lack of maturity, as mathematicians believe that not enough research has been done in ECDLP. In particular, isogenies can be used as a one way function that can be used in these cryptographic primitives. However, this is now a deep and popular area of research. Also it hs been found that hyperelliptic curves of higher genus are potentially insecure from a cryptographic point of view[48], yet the researchers are trying to prove it better than ECC.

References

[1] G. Faltings, "The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles" . Notices of the AMS 42 (7): 743–746. ISSN 0002-9920. 1995
[2] Koblitz.:" Elliptic curve cryptosystems. Mathematics of Computation . 1987". vol.(48):2003–2009.
[3] V. Miller. "Use of elliptic curves in cryptography. Advances in Cryptology-CRYPTO '85. 1986", LNCS 218(483), pp. 417–426

[4] ANSI X9.62. "Public Key Cryptography for the financial Services Industry: The Elliptic curve Digital Signature Algorithm (ECDSA)" , 1999.
[5] ANSI X9.62, "Public Key Cryptography for the financial Services Industry: The Elliptic curve Key Agreement & Key Transport Protocols. 2000".
[6] IEEE 1363-2000, "Standard Specifications for Public Key Cryptography".
[7] ISO/IEC 14888, " Information Technology Security Techniques- Digital Signatures., with Appendix- part 3: Certificate based mechanism".
[8] ISO/IEC 15946," Information Security Technology - Cryptographic Techniques based on Elliptic curve." 1999.
[9] NIST, "Digital Signature standard. FIPS publication", 2000. 186-2
[10] NIST, "Advanced Encryption Standard".
[11] Daniel V. Bailey , Christof Paar. "Arithmetic in finite field extensions with application in elliptic curve cryptography", Journal of Cryptology. 2001: Vol.(14).
[12] M. Bednara, M. Daldrup, J. Shokrollahi, *et al,* "Tradeoff analysis o fpga based elliptic curve cryptography", Proc .of the IEEE International Symposium on Circuits and Systems (ISCAS-02), Scottsdale, Arizona, USA . *2002*
[13] Brian King, "Mapping an Arbitrary Message to an Elliptic Curve when Defined over GF (2n)", International Journal of Network Security. 2009: Vol.8(2). 169- 17
[14] N. P. Smart, "The Hessian form of an elliptic curve. Springer-Verlag Berlin Heidelberg", ISBN 978-3-540-42521-2, 2001.
[15] Edwards, Harold M, " A normal form for elliptic curves", Bulletin of the American Mathematical Society (Providence, R.I.: American Mathematical Society) Vol(44). 393– 422, ISSN 0002-9904
[16] Daniel Bernstein, T.Lange, "Faster Addition and Doubling on Elliptic curves", http://cr.yp. newelliptic/ new elliptic-20070906.pdf , 2007.
[17] F. Gouvea, B. Mazur, "The square free sieve and the rank of elliptic curve", Journal of American Mathematical Society, Vol 4(1), 1991.
[18] Twisted Hessian Curves Retrieved., http://hyperelliptic.org/EFD/g1p/auto-twisted hessian.html, 2010
[19] Daniel J. Bernstein, Marc Joye, Tanja Lange *et al* , "Twisted Edward curves" , http:// eprint.iacr.org/2008/013.pdf
[20] Olivier Billet, Marc Joye, "The Jacobi model of an Elliptic Curve and the Side-channel Analysis", Springer-Verlag Berlin Heidelberg, ISBN 978-3-540-40111-7, 2003.
[21] Peter L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", American Mathematical Society , http://www.jstor.org/stable/pdfplus/ 2007888.pdf, 1987.
[22] **H**. Lange and W. Ruppert**, "**Addition laws on elliptic curves in arbitrary characteristics", Journal of Algebra , Vol.107(1). 106-116, 1987.
[23] STANDARDS FOR EFFICIENT CRYPTOGRAPHY, "SEC 1: Elliptic Curve Cryptography" , Certicom Research September 20, Version 1.0 , 2000
[24] Silverman , Joseph H, "The arithmetic of elliptic curve"s, Gradute Texts in Mathematics", Springer Verlag, New York, Vol.106 ISBN 978-0-387-96203-8 . MR1329092, 1994.
[25] STANDARDS FOR EFFICIENT CRYPTOGRAPHY , "SEC 2. Recommended Elliptic Curve Domain parameters", www.secg.org/collateral/sec2_final.pdf
[26] B. Salvy, A. Bostan, F. Morain , *et al,* "Fast algorithms for computing isogenies between elliptic curves", http://arxiv.org/abs/cs/ 0609020, 1996
[27] Dewaghe L. Couveiges J.M, F. Morain, "Isogeny cycles and the schoof-elkies-atkin algorithm", http://citeseer.ist.psu.edu/couveignes96isogeny.html
[28] Steven Galbraith, "Constructing Isogenies between elliptic curves over finite field", Journal of Computational Mathematics, Vol. 2. 118–138, 1999.
[29] Alexander Rostovtsev ,Anton Stolbunov, "Public key cryptosystems based on isogenies", http://eprint.iacr.org /2006/145.ps , 2006 .
[30] I. Blake, G. Seroussi , N. Smart, "Elliptic Curves in Cryptography", Math. Soc. LNS, 265, Cambridge, London. 1999.
[31] D. Jao, S. Miller , R. Venkatesan, "Do all Elliptic Curves of the same order have the same difficulty of discrete logs", ASIACRYPT 2005. LNCS. Springer-Verlag ,Vol. 3788 21-40, 2005.
[32] D. Charles, K. Lauter, E. Goren, "Cryptographic hash functions from expander graphs", J. Cryptology, Vol. 22, pp. 93-113, 2009.
[33] Factorization of RSA-155, http://www. rsasecurity .com/rsalabs/ challenges/ factoring / rsa155.html
[34] Factorization of 512-bit RSA key using the general number field sieve, http://www.hamline. edu/~wnk/rsa/rsa.html
[35] Arjen K. Lenstra," Integer Factoring, *Designs, Codes and Cryptography*" ,Vol.19, pp. 101– 128, 2000.
[36] Michal Sramka , Otokar Grosek, "Efficiency of the Elliptic Curve Cryptosystem", SK–812 19 Bratislava, SLOVAKIA, 2000.
[37] Marisa W. Paryasto, Kuspriyante, Sarwan *et al*, "Issues in Elliptic Curve Crypyography implementation", Internetworking Indonesial Journal, Vol.1(1), 2009.
[38] Miguel Morales- Sandoval, "An interoperable and reconfigurable hardware architecture for elliptic curve cryptography", . Thesis, Mexico. National Institue for Astrophysics, optics and Electronics, 2006.
[39] Mathew Estes, Philip Hines, "Efficient implementation of an elliptic curve cryptosystems over binary galios field in normal and polynomial bases", George Massion university, Report number: GMU EE-746,2006.
[40] N. Koblitz, "A family of Jacobian suitable for Discrete Log Cryptosystem", Advances in Cryptology – Crypto'88, LNCS, Springer- Verlag. Berlin , Vol. 403. 94-99, 1988.
[41] Uwe Krieger Signature . C. Diplomaebeit, University Essen Faahbereich 6 (Mathematics and Informatics) , 1997
[42] Y.Sakai, K. Sakurai, "Design of hyperelliptic Cryptosystem in small characteristic and Software implantation over F_2^n", Advances in Cryptology – ASIACRYPT'98. LNCS, Berlin, springer Verlag. Vol.1514. 80-94.
[43] Y. Sakai, K. Sakurai, H. Ishizuka, "Secure hyperelliptic cryptosystems and their performance: Public Key Cryptography", LNCS. springer- Verlag. Vol.1431. 164-181,

[44] A.Enge, "The extended Euclidean algorithm on polynomial and the computational efficiency of hyperelliptic cryptosystems", 1999
[45] Sakai , K. Sakurai, "On the pratical performance of hyperelliptic curve cryptosystem in software implementation", IEICE transaction on Fundamental of Electronics, Communication and Computer Sciences, Vol. E83-A(4).692-703, 2000.
[46] T. Wollinger, "Computer Architecture for Cryptosystems based on hyperelliptic curves", Thesis. Worcester polytechnique Institute. 2001.
[47] N.Boston, T.Clancy, Y. Liow and J. Webster, "Genus Two Hyperelliptic curve coprocessor", Workshop on Cryptographic hardware and Embeded System –CHES, LNCS. springer Verlerg. New York . Vol. 2523, 2002.
[48] N. P smart, " On the performance of hyperelliptic Cryptosystem", Advances in cryptology- EUROCRYPT' 99, LNCS. springer- Verlag. Berlin, Vol. 592. 65-175, 1999.
[49] R.Harley,"Fast arithemetic on Genus Two curves", http://cristal.inria.fr/~harley/hyper . 2000
[50] Y. Miyamoto. H. Doi, K. Matrio, J. chao ,*et al*, "A Fast Addition algorithm of Genus Two hyperelliptic curve", SCIS. IEICE, Japan, pp. 497-502 , 2002.
[51] M. Tukahashi, "Improving Harley algorithm for Jacobians Genus2 Hyperelliptic Curve", SCIS, IEICE , Japan, 2002.
[52] T. Lange, "Efficient Arthemetic on Genus 2 Hyper elliptic curves over Finite Fields via Explicit Formulae", Cryptology eprint Archive, Report 2002/ 121, http://eprint.iacr.org/, 2002.
[53] J.M. Poll, Monte Carlo, "Methods for index computation mode", Mathematics of Computation, Vol.32(143), pp. 918-924, 1978.
[54] P. C. Van Oorschot and M.J Wiens, "Parallel collision search with cryptoanalytic application", Journal of Cryptology, Vol.12(1), pp. 1-28, 1999.
[55] P. Gaudry, "An algorithm for solving the discrete logarithm problem on hyper elliptic curves" , Advances in Cryptology-EUROCRYPT 2000, LNCS. Springer Verlag. Berlin Germany, Vol 1807.19-34, 2000.
[56] Michal Sramka , Otokar Grosek, " Efficiency of the Elliptic Curve Cryptosystems", Slovak University of Technology, Department of Mathematics, SK–812 19 Bratislava, SLOVAKIA.

Samta Gajbhiye is working as an Associate Professor in the Department of Computer Science and Engineering in Shri Shankaracharaya College of Engg. & Technology, Bhilai [Chattisgarh], India. She is presently in the process of enrolling in Ph.D Program. Her area of interest is computer network, Information Security and Cryptography. She is the life member of ISTE and IEI

Dr. Monisha Sharma is working as Professor in the Department of Electronics And Telecommunication Engg. in Shri Shankaracharaya College of Engg. & Technology, Bhilai [Chattisgarh], India. She has published more than 40 International/National journals. Her research area includes Image Processing, Information Security and Cryptography. She Received IE Young Engineers Award in Electronics and Telecommunication by Institution of Engineers(India) on 26th National Convention in Electronics and Telecommunication in West Bengal state center in Kolkatta on October 2010. She was awarded as "Young Engineer Award- 2010 in Electronics and Telecommunication" by Institution of Engineers (India) in West Bengal state center, Kolkatta. She is the Gold Medalist in M.Tech (ETC) 2008 from Pandit Ravi Shankar Shukla University ,Raipur. Also she was awarded as "Young Scientist award in Engineering science and Technology " in sixth Chhattisgarh Young Scientist Congress organized by Chhattigarh council of Science and Technology and Guru Ghasidas University, Bilaspur on 2008.

Dr. Samir Dashputre is working as Professor in Department of Mathematics. in Shri Shankaracharaya College of Engg. & Technology, Bhilai [Chattisgarh]. He has published more than 7 International/National journals. His area of Interest is Non Operator Theory , Number Theory and Cryptography