IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN:2319-765X. Volume 10, Issue 2 Ver. V (Mar-Apr. 2014), PP 61-63
www.iosrjournals.org

Comparative Study of Elliptic and Hyper elliptic Curve Cryptography in Discrete Logarithmic Problem

[1]Mrs. M.T.Wankhede-Barsgade, [2]Dr. S. A. Meshram
[1]Department of Mathematics, B.N.Bandodkar College of Science, Thane.
[2]Associate Proffessor, Department of Mathematics, R.T.M. Nagpur University, Nagpur University.

Abstract: *Binary and prime fields are being considered for practical implementation on both Elliptic and Hyperelliptic curves for software curve implementation. The main operations like scalar multiplication and group operations are compared in both hyperelliptic and elliptic cryptography.*

ECC and HECC are implemented on different binary fields and also compare the encryption and decryption system in discrete logarithmic problem.

Keywords: *Elliptic/ Hyperelliptic curves, Encryption/decryption, Discrete logarithm.*

I. Introduction:

Elliptic and hyperelliptic curves are the basis for a relative new class of public-key schemes. It is predicted that elliptic and hyperelliptic curves will replace many existing schemes in near future. It is thus of great interest to develop algorithms which allow efficient implementations of elliptic and hyperelliptic curve cryptosystem.

Properties and functions of elliptic curves have been studied in Mathematics for 150 years. Use of Elliptic curves in cryptography was virtually unheard before 1985. Elliptic curve cryptography (ECC) was introduced by Victor Miller and Neal Koblitz in 1985.ECC is used extensively and there has been much work in the recent years on their implementation. Subsequently HECC was proposed by Koblitz in 1989 based on discrete logarithm problem on the Jacobian of hyperelliptic curves over finite fields.

Almost all of the standard discrete logarithm based protocols such as DSA and El Gamal have Elliptic and Hyperelliptic varients. This is because such protocols only require the presence of a finite abelian group, with the large prime order subgroup, within which the basic group operation is easy whilst the associated discrete logarithm problem is hard.

The Jacobian of a genus g HECC will have have q^g points on it, where q denotes the number of elements in the field of definition of the Jacobian. By chosing HECC we can achieve the same order of magnitude of the group order with a smaller value of q when compared with ECC. On the other hand, the group operation is much more cumbersome in HEC than in EC and it turns out that the DLP is much easier on the Jacobian of a high genus curve than on a comparably sized group of points of an elliptic curve.

In this paper we have explored in details the main operations like scalar multiplication, group operations on Jacobian, finite field operations which are prime steps for efficient implementation of ECC and HECC.

II. Elliptic Curve

Definition: Let K be a field of characteristic $\neq 2, 3$, and let $x^3 + ax + b$ (where $a, b \in K$) be a cubic polynomial with no multiple roots. An elliptic curve over K is the set of points (x, y) which satisfy the equation

$$y^2 = x^3 + ax + b,$$

together with single element denoted by O and called the “point at infinity”.

If K is a field of characteristic 2, then an elliptic curve over K is the set of points satisfying an equation of the type either

$$y^2 + cy = x^3 + ax + b$$

or else

$$y^2 + xy = x^3 + ax^2 + b$$

together with a “ point at infinity” O.

If K is a field of characteristic 3, then an elliptic curve over K is the set of points satisfying an equation

$$y^2 = x^3 + ax^2 + bx + c$$

together with a “ point at infinity” O.

III. Hyper elliptic curve

Definition: A hyperelliptic curve C of genus g defined over a field F_q of characteristic p is given by an equation of form

$Y^2 + h(x)y = f(x)$

Where h(x) and f(x) are polynomials with coefficients in F_q with degree of h(x) ≤ g and degree of f(x) = 2g + 1.

An additional requirement is that the curve should not be a singular curve. The condition that there are no x any y in the algebraic closure of F_q that satisfy the equation of the curve and the two partial derivatives $2y + h(x) = 0$, $h'(x)y - f'(x) = 0$.

As opposed to the case of elliptic curves, there is no natural way to provide C(K) with a group structure. Instead one can introduce different object related to C, which to each field extension K of F_q associates a group. This object is called the Jacobian of C.

A divisor D of the curve is a formal sum $\sum_{P \in C(L)} C_P[P]$ with C_P as an integer having finitely many C_P nonzero. The set of all divisors is denoted by $\mathrm{Div}_c(L)$.

Given two divisors $D = \Sigma_P C_P[P]$ and $D = \Sigma_P C_{P'}[P]$ the sum D + D' is defined as

$D + D' = \Sigma_P(C_P + C_{P'})[P]$.

This gives $\mathrm{Div}_c(L)$ a group structure.

The degree of a divisor $D = \sum_{P \in C(L)} C_P[P]$ is $\deg(D) = \Sigma_P C_P$.

The group of degree zero divisor is $\mathrm{Div}_C^{O}(L) = \{ D \: \varepsilon \: \mathrm{Div}_C(L) \mid \deg(D) = 0\}$.

For any extension K of F_q, consider the set $C(K) = \{(x ,y) \: \varepsilon \: K \times K \mid y^2 + h(x)y = f(x)\} \cup \{\infty\}$. It is called set of K – rational points on C.

The definition of the group $J_C(K)$ can be considered as a natural generalisation of the group of points on elliptic curves.

IV. Performance analysis

HECC scalar multiplication takes less time than ECC scalar multiplication as shown in the table below.

Curves	Field	Group order	Scalar multiplication
Elliptic curve	F_2^{81}	2^{162}	2.12
Hyperelliptic curve	F_2^{163}	2^{163}	4.24

It is also observed that addition and doubling operation in Hyperelliptic curves is more cumbersome than in elliptic curves as shown below.

Curves	Addition	Doubling
Elliptic curve	I + 2M + S	I + 2M + 2S
Hyperelliptic curve in odd characterstic	I + 22M + 3S	I + 22M + 5S
Hyperelliptic curve in even characteristic	I + 22M + 3S	I + 20M + 6S

Comparison of encryption and decryption time of ECC and HECC shows that HECC decryption time is relatively less compared to ECC decryption time for same level of security as shown in the table below.

Curves	Encryption	Decryption
ECC	797	281
HECC	668	191

It is observed that genus 2 HECC is faster than ECC in the experiment to study the relative performance of ECC and HECC. Genus 2 HECC has the advantage over ECC in constrained environment due to its short operant size.

Furthermore it has been shown that in order to achieve cryptographic security equivalent to the one provided by an elliptic curve defined over a field size log q it is necessary to use a hyperelliptic curve of genus 3 defined over a field size smaller than log q.

V. Discrete logarithm problem

The elliptic curve discrete logarithm problem (ECDLP) is: given an elliptic curve E defined over a finite field F_q, a point P ε $E(F_q)$ of order n, a point Q ε < P >, find an integer l ε [0, n-1] such that Q = lP. The integer l is called the discrete logarithm of Q to the base P, denoted by

$l = \log_Q P$.

The hyperelliptic curve discrete logarithm problem (HECDLP) is: given hyperelliptic curve of genus g over a finite field F_q, a point P ε J $_C$(K) of order n, a point Q ε < P >, find an integer l ε [0, n-1] such that Q = lP. The integer l is called the discrete logarithm of Q to the base P, denoted by
l = log $_Q$ P.

Elliptic curves have become popular choice in many protocols. Recent attack shows that hyperelliptic curves of genus 2 and genus 3 have comparable properties. Weil descent allows one to reduce ECDLP on some elliptic curves defined over a finite field of composite degree to an instance of the HECDLP of high genus defined over a smaller field.

Four instances of the ECDLP were considered for which the curves were defined over F_2^{62}, F_2^{93}, F_2^{124}, F_2^{155}. Weil descent reduces this to instances of HEDLP where the curves have genus 31 and are defined over F_2^{2}, F_2^{3}, F_2^{4}, F_2^{5}.

VI. Conclusion:

Elliptic and hyperelliptic curves were proposed for use in public key cryptographic protocols based on discrete logarithm problem in the Jacobian of these curves.

Hyperelliptic curve cryptography (HECC) has some advantages over Elliptic curve cryptography (ECC). IF HECC of genus 2 curves can be worked in the field $F_2{}^n$, the same security level is obtained in ECC over fields of bit-lengths that are twice as large.

The field of embedded system is growing at a rapid rate, as devices such as mobile phones, smart cards, sensor nodes has become most in our everyday life. The most challenging task for embedded security is implementations of public key cryptography. HECC has some advantages over ECC because of the possibility to work in a smaller field.

Further experiments are needed in order to judge the true merits of HECC over competing scheme such as ECC.

[1]. Darrel Hankerson, Alfred Menezes, Scott Vanstone, 2004. “Guide to elliptic curve cryptography” Springer publication, ISBN 0-387-95273-X.

[2]. Henry Cohen and Gerhard Frey, 2006. “Handbook of Elliptic and Hyperelliptic Curve Cryptography”, Chapman and Hall/CRC press.

[3]. Kakali Chatterjee, Daya Gupta, 2009. “Secure access of smart cards using elliptic curve cryptosystem”, Wicom, IEEE catlog No. CFPO9WNM-CDR.

[4]. Tanja Lange, 2005. “Formula for Arithmetic on Genus 2 hyperelliptic curves” Applicable Algebra in Engineering and Computing, Volume 15.

[5]. P. Longa, Catherine Gebotys, 2009. “Novel precomputation Schemes for elliptic Curve Cryptosystems”, ACNS, LNCS vol-5536, pp:71-88.

[6]. Kakali Chatterjee, Asok De, Daya Gupta, 2011. “Software implementation of Curve based Cryptography for constrained Devices. Volume 24 – No.5, June 2011.