ISSN: 2229 – 6948 (ONLINE)
DOI: 10.21917/ijct.2011.0034

COMPARATIVE ANALYSIS OF HIGHER GENUS HYPERELLIPTIC CURVE CRYPTOSYSTEMS OVER FINITE FIELD F_P

R. Ganesan[1] and K. Vivekanandan[2]
[1]*Department of Computer Science and Applications, PSG College of Arts & Science, Tamil Nadu, India*
E-mail: rganrao@gmail.com
[2]*Bharathiar School of Management and Entrepreneur Development, Bharathiar University, Tamil Nadu, India*
E-mail: vivekbsmed@gmail.com

Abstract
The performance analysis of Hyperelliptic Curve Cryptosystems (HECC) over prime fields (Fp) of genus 5 and 6 are discussed in this paper. We have implemented a HECC system of genus 5 & 6 in a Intel Pentium III Celeron Processor @ 933 MHz speed with 256 MB RAM in Java 1.5. We have also compared their efficiency on the parameters of time taken for divisor generation, key generation, encryption and decryption. Our results demonstrate that the performance of higher genus HECC system gets degraded in terms of divisor generation, key generation, encryption and decryption process.

Keywords:
HECC, Finite Field, Genus, Divisor Generation, Key Generation, Encryption, Decryption

1. INTRODUCTION

In recent times, hyperelliptic curve based cryptographic systems are considered as an alternative to finite-field based Public Key Cryptosystems, such as RSA, ECC and El-Gamal which are susceptible to attacks [9] [1]. In this paper, we mainly deal with Hyperelliptic Curve Cryptosystems (HECC) over prime fields (Fp) of genus 5 and 6. We have implemented HECC for genus 5 and 6 and provide details of the performance analysis between genus 5 and 6. The implementation of HECC system of genus 2 and 4 and their performance analysis are discussed in [7]. The organization of the paper is as follows. In section 2, an overview of hyperelliptic curves is presented. In section 3, the algorithm for key generation, encryption and decryption are discussed. In section 4, the implementation details are provided. Section 5 highlights the various results. In section 6, we provide the analysis details of various hyperelliptic curve cryptosystems. The paper finally ends with conclusions.

2. BASICS OF HYPERELLIPTIC CURVES

The general equation of a non-singular hyperelliptic curve C of genus g over a field F_k is defined by the following equation:

$C : v^{2} + h(u)v = f(u),$

where h, f ε k[u], f is monic, and the degree of f = 2g + 1, degree of h ≤ g.

Elliptic Curves are hyperelliptic curves of genus 1 and there exists hyperelliptic Curves whose range is from 2 to infinity. For hyperelliptic curves there is no natural group law on C, by which one can "add" points like that is done in an elliptic curve. The reason is that the points on a hyperelliptic curve do not form a group. Hence, for hyperelliptic curves, a group law is defined via the Jacobian Variety of C over a field, which is a finite abelian group. The Jacobian of the hyperelliptic curve C is the quotient group $J = D^0/P$, where D^0 is the set of divisors of degree zero, and P is the set of divisors of rational functions. The equivalence classes of the Jacobian are each represented by a unique reduced divisor upon which one performs the group law.

2.1 MUMFORD REPRESENTATION

Let g be the genus of a hyperelliptic curve

$C: y^2 + h(x)y = f(x)$

Each nontrivial divisor class over the field K can be represented via Mumford representation (u(x), v(x)), where u(x) and v(x), u, v ε K[x], are a unique pair of polynomials satisfying the constraints of

- u is monic
- deg v < deg u ≤ g
- $u \mid v^2 + vh - f$

Various mathematical operations can be carried out on these hyperelliptic curves which are discussed in [2] [5] [6] [7] [11] [12] [13] [15].

2.2 DISCRETE LOGARITHM PROBLEM (DLP) BASED ON HYPERELLIPTIC CURVES

The Hyperelliptic Curve DLP is defined as:

"Let C be the hyperelliptic curve and let F*q* be a finite field within C with q elements. Given two divisors D_1 and D_2 in the Jacobian, determine the integer *m* ε Z, such that $D_2 = mD_1$ "

2.3 HYPERELLIPTIC CURVE EQUATIONS FOR GENUS 5 AND 6 OVER PRIME FIELD FP

The general equation format of a hyperelliptic curve defined over Fp is given in Table 1.

The following are the hyperelliptic curves over prime fields we have considered for genus 5 & 6.

For genus 5:

$y^2 = x^{11} + x^5 + a_0$

For genus 6:

$y^2 = x^{13} + x^{11} + x^3 + x$

Table.1. Hyperelliptic curves over Fp of various genus g

Genus	HC over Fp ,where p is prime
5	$y^2 = x^{11} + f_{10}x^{10} + f_9x^9 + f_8x^8 + f_7x^7 + f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x^1 + f_0$
6	$y^2 = x^{13} + f_{12}x^{12} + f_{11}x^{11} + f_{10}x^{10} + f_9x^9 + f_8x^8 + f_7x^7 + f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x^1 + f_0$

3. ALGORITHM FOR A HYPERELLIPTIC CURVE CRYPTOSYSTEM (HECC)

The basis for a Hyperelliptic curve cryptosystem is the Discrete Logarithm problem. The following section describes the algorithm for Key generation process, Encryption and Decryption process [7] [8].

3.1 KEY GENERATION ALGORITHM

Input: The public parameters are Hyperelliptic curve C, Prime p and Divisor D.

Output: The Public key P_A and Private key a_A

1. $a_A \varepsilon_R$ N [choose ‘a’ at random in N]
2. $P_A \longleftarrow [a_A]$ D [The form of P_A is (u(x), v(x)) representation]
3. Return P_A and a_A

For the random prime number generation in step 1, one can apply the Rabin-Miller Primality Test [14] or AKS algorithm [10].

3.2 ENCRYPTION/DECRYPTION ALGORITHM

In this section, we describe the methodology for encryption and decryption. The message ‘m’ that is to be sent will be encoded as a series of points represented as (u(x), v(x)). The encoded message is referred as E_m. For the encryption and decryption process using HECC, we have adopted El-Gamal method [9] to design HEC-ElG Algorithm (HEC-ElGA). Details on HEC-ElGA method can be had from [8].

4. IMPLEMENTATION

The Hyperelliptic curve cryptosystem for genus 5 & 6 was implemented in Java 1.5 and executed in Intel Pentium III Celeron Processor @ 933 MHz speed with 256 MB RAM. The system was tested for the time taken for a) Divisor generation b) key generation c) encryption and d) decryption processes.

5. RESULTS

The followings are the results of the HECC system.

5.1 HYPERELLIPTIC CURVE CRYPTOSYSTEM FOR GENUS 5 OVER PRIME FIELD Fp

HECC for Genus 5 over Prime Field Fp	
HECC Equation	C:v^2=u^11+u^5+1 Prime: 15500223400233542322271631 Time taken for curve generation : 10ms
Divisor Gen.	div (u^5+ 5308937822212580211940952952221399u ^4+134612719003949219042159941895941 1u^3+799737948655647935100432884455 2830u^2+196973135363761559312632158 8922057u+8611409421799544821211754 218774437, 3221454815665988134562034534382230u ^4+9464011480333322079006149163499622u^3+717655703382936786375966752395 5107u^2+614588620454584404772969254 1508387u+4971733125487588920481463 09121910) Time (in ms)taken for divisor generation: 1221
Key Generation	Time taken for key generation: 8505 Milliseconds
Encryption (Size of the txt file : 301 bytes)	Time (Milliseconds): 8622
Decryption	Time (Milliseconds): 10700

5.2 HYPERELLIPTIC CURVE CRYPTOSYSTEM FOR GENUS 6 OVER PRIME FIELD Fp

HECC for Genus 6 over Prime Field Fp	
HECC Equation	C: v^2 = u^13 + u^11 + u^3 + u Prime: 98335577979347609283016230317 Time taken for curve generation : 11.4 Milliseconds
Divisor Generation	D: div (u^6+ 134078333831452908529223880916399960u^5+ 32606593858398885736828000042071221u^4+ 55636650634750917666246285479868839u^3+ 14597528736458876964425366997387822u^2+ 12101270981360112608136091617090170u+ 11785678507511323903930661188035422, 89879075615611947251300300747416664u^5+ 12950415090557298829604230510121215u^4+ 11815991969843890827581574345701176u^3+ 73625759767624791112662762357215527u^2+ 56727769455172781090535103405840133u+ 75115003997565479452123500041299909) Time taken for divisor generation: 1871 Milliseconds
Key Generation	Time taken for key generation : 9021 Milliseconds
Encryption	(Size of the txt file : 301) bytes) Time : 9322 Milliseconds
Decryption	Time : 11595 Milliseconds

6. PERFORMANCE ANALYSIS OF THE HECC

The performance of the HECC for genus 5 and genus 6 was analyzed based on the length of the prime generated and the time taken for the various processes. The size of the input text file used for the encryption process is 500 bytes. Table.2 shows the time (in Milliseconds) taken for the various processes.

Table.2. Performance Analysis of the HECC for Genus 5 and 6 (Time in milliseconds)

	Length of prime = 35		Length of prime = 55	
	G5	G6	G5	G6
Divisor Generation	1221	1871	1771	2313
Key Generation	8505	9021	8860	11743
Encryption	8622	9322	8997	12109
Decryption	10700	11595	11100	15012

The following graph displays the performance analysis of HECC for both genus 5 and genus 6.

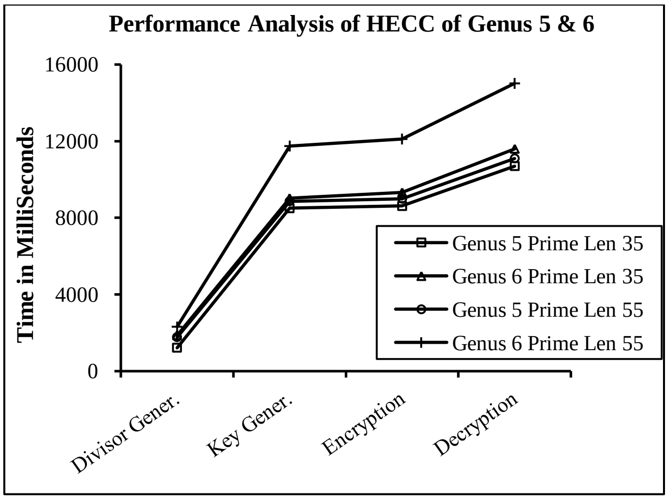

Fig.1. Performance analysis of HECC of Genus 5 & 6

7. CONCLUSION

In this work, we have implemented a hyperelliptic curve cryptosystem of genus 5 & genus 6 and compared their performance in terms of divisor generation, key generation, and encryption and decryption process. The entire work was coded and implemented in Java 1.5 and executed in Intel Pentium III Celeron Processor @ 933 MHz speed with 256 MB RAM. Analysing the results, we found that the performance of higher genus HECC gets degraded in terms of divisor generation, key generation, and encryption and decryption process. Moreover, there exists sub exponential discrete log algorithm on higher genus ($g > 2$) hyperelliptic curves which reduces the security level of the cryptosystem [4] and also the HECC system of higher genus are slower than HECC system of genus 2 [3] [7]. Thus, the hyperelliptic curves of genus 2 are the best suitable curves for the cryptographic purpose.

ACKNOWLEDGEMENT

The author wishes to thank the Management and Principal of PSG College of arts & science, Coimbatore for their constant encouragement and support given to do this research work.

REFERENCES

[1] Adleman, L., 1979, “A subexponential algorithm for the discrete logarithm problem with applications to cryptography”, Proc. 20th IEEE Found. Comp. Sci. Symp., pp. 55-60.

[2] Avanzi R M and Tanja Lange, 2006, “Introduction to Public key cryptography” from “Handbook of Elliptic and Hyper elliptic curve cryptography” eds. Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, Taylor and Francis, Florida, pp. 1-15.

[3] Avanzi R M, 2004, “Aspects of hyper elliptic curves over large prime fields in software implementations”, Cryptographic Hardware and Embedded Systems – CHES 2004, Lecture Notes in Computer. Sci., Vol. 3156, Springer-Verlag, pp. 148-162.

[4] Blake I.F, Seroussi G, Smart N.P, 2000, “Elliptic Curves in Cryptography”, London Math. Soc. Lecture Note Series, 265, Cambridge Univ. Press.

[5] Duquesne S and Tanja Lange, 2006, “Arithmetic of Hyper elliptic curves” from “Handbook of Elliptic and Hyper elliptic curve cryptography” by Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, Taylor and Francis Group, Florida, pp. 303-353.

[6] Eigeartaigh C O, “A comparison of point counting methods for Hyper elliptic curve over prime fields and field of characteristics of 2”, Technical report, School of Computing, Dublin City University, Dublin, Ireland

[7] Ganesan R, Dr. Vivekanandan K, 2008, “Performance Analysis of Hyper-Elliptic Curve Cryptosystems over Finite Field F_p for Genus 2 and 4”, International Journal of Computer Science and Network Security (IJCSNS), Vol. 8 No. 12 pp. 415-418.

[8] Ganesan R, Gobi M, and Dr. Vivekanandan K, Sep 2010, “A Novel digital envelope approach for secure e-commerce channal”, International Journal of Network security, Vol.11, Issue 2, pp. 88-94.

[9] http://www.deutsche-telekom laboratories.de/~kuehnulr/paper/k_scatr_pkc2003.pdf

[10] Jin T, May 2005, “Researching and Implementing on AKS Algorithm”, University of Bath.

[11] Lange T, 2002, “Efficient arithmetic on genus 2 hyper-elliptic curves over finite fields via explicit formulae", Cryptology ePrint Archive: Report 2002/121.

[12] Menezes A J, Yi Hong Wu, Robert J Zuccherato , November 1996, ”An elementary introduction to hyper elliptic curves”, Technical Report CORR 96-19, University of Waterloo, Ontario, Canada.

[13] Sakai Y, Kouichi Sakurai, April – 2000, “On the practical performance of hyper-elliptic curve cryptosystems in software implementation”, IEICE Transaction fundamentals, Vol. E83-A, No. 4, pp. 692-703.

[14] Stallings W, 2002, “Cryptography and Network Security: Principles and Practice”, 2nd Edition, Pearson Education, pp. 221-222

[15] Weng A, 2003, “Constructing hyperelliptic curves of genus 2 suitable for cryptography", Mathematics of Computation, Vol. 72, pp. 435-458.