J. KSIAM **Vol.4**, No.1, 23-28, 2000

ON THE SECURITY OF CERTAIN HYPERELLIPTIC CURVES

Insuk Kim, Sungtae Jun

Abstract. We compute the order of jacobian groups of hyperelliptic curves on a finite field of characteristic 3 and we determine which curves are secure against known attacks.

1. Introduction

As a source of finite abelian groups suitable for cryptographic discrete logarithm problems, elliptic curves have been studied. A practical advantage of elliptic curve cryptosystems is that they can be constructed over a smaller definition field compared to the conventional discrete-log based cryptosystems and to RSA cryptosystems. Another source of finite abelian groups is the jacobians of hyperelliptic curves defined over finite fields [4]. Since there is no known practical advantage of hyperelliptic cryptosystems compared to elliptic cryptosystems or RSA, it is worthwhile to study hyperelliptic cryptosystems compared to other cryptosystems and to design hyperelliptic cryptosystems secure against known attack including Frey-Rück-method [2].

In [3], Koblitz has studied the jacobians of hyperelliptic curves $v^2 + v = u^{2g+1}$ over a field of characteristic 2 and found the induced hyperelliptic cryptosystems secure against three known attacks. First, Shank's baby step and giant step method and Pohlig-Hellman method [5]. Second, Frey's generalization of MOV attack [2]. Third, Adelman-DeMarrais- Hwang method of subexponential time algorithm for discrete logarithm over a rational subgroup of the jacobian of large genus of hyperelliptic curve over a finite field [1]. In [4], Koblitz has computed the number of elements in the jacobian groups of hyperelliptic curves $v^2 + v = u^{2g+1}$ over a field of characteristic 2 and found that several curves were good for a secure cryptosystem. Recently, Sakai, Sakurai and Ishizuka studied hyperelliptic curves of the form $v^2 = f(u)$ where the coefficients of $f(u)$ were 1 or 0 over a field of characteristic 2, 3, 5 and 7 [7] and they design a hyperelliptic curve cryptosystem.

In this paper, we will compute the order of jacobians of several hyperelliptic curves of genus 2 over a finite field of characteristic 3, which are not treated in [7], and we

Key words and phrases. jacobian, hyperelliptic curve, genus, cryptosystem.
AMS Subject Classification 11F11
This work is partially supported by Wonkwang University in 1999

check out which curves are good for a secure cryptosystem. Hence this paper does not contain any theoretical new facts, however hyperelliptic curves we study here give a good source for designing a cryptosystem.

2. Hyperelliptic Curve

2.1. Throughout this chapter, let $\mathbb{F}$ be a field and $\bar{\mathbb{F}}$ its algebraic closure.

Definition 2.1. *A hyperelliptic curve of genus g over $\mathbb{F}(g \geq 1)$ is an equation of the form*

$$C : v^2 + h(u)v = f(u) \qquad in \quad \mathbb{F}[u, v],$$

where $h(u) \in \mathbb{F}[u]$ is a polynomial of degree at most g and $f(u) \in \mathbb{F}[u]$ is a monic polynomial of degree $2g + 1$. This curve must be smooth at all points $(x, y) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$ that satisfy the equation $y^2 + h(x)y = f(x)$.

2.2 Jacobian groups.

Let C be a hyperelliptic curve over a field $\mathbb{F}$. A divisor D is a finite formal sum of $\bar{\mathbb{F}}$-points $D = \sum_i m_i P_i$ where $m_i \in \mathbb{Z}, P_i \in C$. We define the degree of D to be $\deg(D) = \sum m_i$. The divisors form an additive group D, in which the divisors of degree 0 form a subgroup D^0. Let P be the principal divisors. Then the jacobian group is defined as $\mathbb{J}(C; \mathbb{F}) = D^0/P$.

The zeta function of a hyperelliptic curve is a basic tool in counting the order of a jacobian. Let $\mathbb{J}$ be the jacobian of a hyperelliptic curve C defined over $\mathbb{F}_q$ and given by the equation $v^2 + h(u)v = f(u)$. Let $\mathbb{F}_{q^r}$ denote an extension field of $\mathbb{F}_q$, and let N_r denote the order of the finite abelian group $\mathbb{J}(\mathbb{F}_{q^r})$.

Definition 2.2. *Let C be a hyperelliptic curve defined over $\mathbb{F}_q$, and let $M_r = \#C(\mathbb{F}_{q^r})$, the number of $\mathbb{F}_{q^r}$-points on C including the point at infinity for $r \geq 1$. The zeta function of C is the power series*

$$Z(C/\mathbb{F}_q; T) = exp(\sum_{r \geq 1} M_r T^r / r),$$

where $exp(x) = e^x$.

Theorem 2.1 (Weil). *Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$, and let $Z(C/\mathbb{F}_q; T)$ be the zeta function of C. Then*

(1)

$$Z(C/\mathbb{F}_q; T) = \frac{P(T)}{(1 - T)(1 - qT)},$$

where $P(T)$ is a polynomial of degree $2g$ with integer coefficients of the form

$$P(T) = 1 + a_1 T + \cdots + a_{g-1} T^{g-1} + a_g T^g + q a_{g-1} T^{g+1} + q^2 a_{g-2} T^{g+2} + \cdots + q^{g-1} a_1 T^{2g-1} + q^g T^{2g}$$

(2) $P(T)$ *factors as*

$$P(T) = \prod_{i=1}^{g}(1-\alpha_i T)(1-\bar{\alpha}_i T)$$

where each α_i *is a complex number of absolute value* $\sqrt{q}$ *and* $\bar{\alpha}_i$ *denote the complex conjugate of* α_i.

(3) $N_r = \#\mathbb{J}(\mathbb{F}_{q^r})$ *is given by*

$$N_r = \prod_{i=1}^{g}|1-\alpha_i^r|^2,$$

where $|\quad|$ *denote the usual complex absolute value. In particular,* $N_1 = P(1)$.

Proof. See [3] and [8] .

2.3 Jacobians of the Hyperelliptic curves.

By Weil's theorem, we have the following procedures to compute the order of jacobian of curves of genus 2 over a finite field of characteristic 3. Similar procedure is explained in [3], [4] for the field of characteristic 2.

(1) Compute M_1, M_2 and let $a_1 = M_1 - 1 - 3$ and $a_2 = (M_2 - 1 - 9 + a_1^2)/2$.
(2) Let $X^2 + a_1X + (a_2 - 6) = 0$ and find the roots, γ_1 and γ_2 .
(3) We have two equations,

$$X^2 - \gamma_1 X + 3 = 0, \quad X^2 - \gamma_2 X + 3 = 0.$$

(4) Let α_1 be a root of $X^2 - \gamma_1 X + 3 = 0$ and let α_2 be a root of $X^2 - \gamma_2 X + 3 = 0$.
(5) $N_r = |1 + 3^r - \alpha_1^r - \bar{\alpha}_1^r| \cdot |1 + 3^r - \alpha_2^r - \bar{\alpha}_2^r|$.

3. Security

To construct a secure hyperelliptic curve cryptosystem, it must resist all known attacks. That is, we have to choose jacobian groups to satisfy the following three conditions. First, the order of $\mathbb{J}(C, \mathbb{F}_{q^n})$ has a sufficiently large prime factor (at least 40 decimal digits), which resists Pohlig-Hellman method [6]. Second, $\mathbb{J}(C, \mathbb{F}_{q^n})$ cannot be embedded into a small finite field $\mathbb{F}_{(q^n)^k}$ for some integer k, which is against Frey's generalization of MOV-attack using Tate pairing [2]. Finally, $2g + 1 \leq \log q^n$. The last condition is against Adleman-DeMarrais-Hwang method [1]. The second can be replaced with the sufficient condition that the largest prime factor of the order of $\mathbb{J}(C, \mathbb{F}_{q^n})$ does not divide $(q^n)^k - 1$ for every integer $k < (\log q^n)^2$.

One of the most efficient algorithm of integer factoring is the number field sieve method. This algorithm takes $exp(O((\ln m)^{1/3}(\ln \ln m)^{2/3}))$ running CPU time for an integer m. On the other hand, Pohlig-Hellman method, an efficient algorithm for discrete logarithm problem has running time of the form $exp(O(\ln m))$ where $m = \#\mathbb{J}(C, \mathbb{F}_{q^n})$ (See p133 [3]). Therefore, if the size of $\#\mathbb{J}(C, \mathbb{F}_{q^n})$ is greater than 160 bits and $\mathbb{J}(C, \mathbb{F}_{q^n})$ is secure, then the security level is approximately same as RSA with 1024-bit key or with a larger key.

Let $f(u)$ be a monic polynomial of degree 5 over $\mathbb{F}_3$ such that $v^2 = f(u)$ is a hyperelliptic curve. In [7], several hyperelliptic curves on a field of characteristic 3 were studied. Here, we restrict ourselves to the hyperelliptic curves of genus 2 over characteristic 3.

Now, we like to choose some examples which were not treated in [7]. The following examples are selected because they contains a large prime and running times are less than 2 hours. Since the order of jacobian group of the following examples is less than 20 decimal digits for $n \leq 20$, we will consider $\mathbb{J}(C, \mathbb{F}_{q^n})$ for $n \geq 21$. Then each case satisfies $2g + 1 = 5 \leq \log 3^n$ for $n \geq 21$, the security against Adleman-DeMarrais-Hwang method is checked trivially. The largest prime of the jacobian of example of $n = 59$ cases does not divide $3^{59k} - 1$ for $k < (59log3)^2 \approx 4202$. The running time of checking Frey's generalization of MOV attack is approximately 3 hours and 17 ± 5 minutes for each example by Pentium II 400MHz. For example of $n = 53$ cases, the largest prime of the jacobian does not divide $3^{53k} - 1$ for $k < (53log3)^2 \approx 3391$. The running time of checking Frey's generalization of MOV attack is approximately 1 hour 20 minutes. Namely, the second condition is checked. For the first condition, we compute and factorize $\#\mathbb{J}(C, \mathbb{F}_{q^n})$. If $\#\mathbb{J}(C, \mathbb{F}_{q^n})$ has a prime factor with more than 40 decimal digits, we tabulate them as follows. Here, P_m denote the decimal digits of the largest prime factor of $\#\mathbb{J}(C; \mathbb{F}_{3^n})$ and $\#\mathbb{J}$ denotes the number of bits of $\#\mathbb{J}(C, \mathbb{F}_{q^n})$. Timing means the running CPU time (seconds) of the program to compute and factorize $\#\mathbb{J}(C, \mathbb{F}_{q^n})$ for $1 \leq n \leq 59$.

Table 1. The Jacobians of $v^2 = f(u)$ on $\mathbb{F}_{q^n}$.

$f(u)$	M_1	M_2	γ_1	γ_2	n	$\#\mathbb{J}$	P_m	Timing
$u^5 + u^2 + 2u$	6	14	$-1 + \sqrt{3}$	$-1 - \sqrt{3}$	59	187	55	1908
$u^5 + u^2 + 2u + 2$	3	11	$\frac{1+\sqrt{21}}{2}$	$\frac{1-\sqrt{21}}{2}$	53	167	43	7120
$u^5 + u^2 + u$	3	13	$\frac{-1+\sqrt{17}}{2}$	$\frac{-1-\sqrt{17}}{2}$	53	167	50	6993
$u^5 + 2u^2 + u + 2$	2	10	$1 + \sqrt{5}$	$1 - \sqrt{5}$	59	187	56	480
$u^5 + 2u^2 + u + 1$	5	7	$\frac{-1+\sqrt{29}}{2}$	$\frac{-1-\sqrt{29}}{2}$	59	187	56	1623
$u^5 + 2u + 1$	7	15	$\frac{-3+\sqrt{5}}{2}$	$\frac{-3+\sqrt{5}}{2}$	53	167	50	4716
$u^5 + 2u + 1$	7	15	$\frac{-3+\sqrt{5}}{2}$	$\frac{-3-\sqrt{5}}{2}$	59	187	49	4716
$u^5 + u^3 + u + 2$	3	11	$\frac{3+\sqrt{13}}{2}$	$\frac{3-\sqrt{13}}{2}$	53	167	42	6531
$u^5 + u^3 + u + 2$	3	11	$\frac{3+\sqrt{13}}{2}$	$\frac{3-\sqrt{13}}{2}$	59	187	56	6531

The curves shown in the table 1 secure against Pohlig-Hellman method. Finally, we conculde that the curves in the table 1 are secure and have the same or higher level of security as RSA-1024.

Now, the jacobian of the curves are as follows.

3.1 $v^2 = u^5 + u^2 + 2u$.

$$\#\mathbb{J}(C; \mathbb{F}_{3^{59}}) = 2 \cdot 11 \cdot 907580959552746065956638365488890264818739931340524734 1$$

3.2 $v^2 = u^5 + u^2 + 2u + 2$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{53}}) = 7 \cdot 14676443 \cdot 365707736651416972511226676001858773160953 7$$

3.3 $v^2 = u^5 + u^2 + u$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{53}}) = 2^4 \cdot 2348188828835725964353217648765817261100963697 4803$$

3.4 $v^2 = u^5 + 2u^2 + u + 2$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{59}}) = 2^2 \cdot 499169527754012419446726113474724719461062517603828667 89$$

3.5 $v^2 = u^5 + 2u^2 + u + 1$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{59}}) = 5 \cdot 399335622203204601331203684185775813963398495578687049 77$$

3.6 $v^2 = u^5 + 2u + 1$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{53}}) = 29 \cdot 1295552457288739633398676135829506136869406852859 1$$

3.7 $v^2 = u^5 + 2u + 1$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{59}}) = 29 \cdot 1233101 \cdot 55835628505191308859942767225992208682276667215 89$$

3.8 $v^2 = u^5 + u^3 + u + 2$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{53}}) = 3 \cdot 107 \cdot 955425074400944254369398594943412406176699$$

3.9 $v^2 = u^5 + u^3 + u + 2$.

$$\#\mathbb{J}(C;\mathbb{F}_{3^{59}}) = 3 \cdot 665559370338680285883649379349846511557917907242356326 89$$

For the above computations, we use mathematica 3.0 to factorize the order of jacobian group using Pentium II 400MHz. This software contains factorizing algorithm, elliptic curve method.

References

1. L.M.Adleman, J.DeMarrais, M. Hwang, *A subexponential algorithm over a rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields.*, In Proc. of ANTS1 **877 of LNCS** (1994), Springer, 28-40.
2. G. Frey, H.G. Ruck, *A remark on m-divisibility and the Discrete Logarithm in the divisor class group of Curves*, Math. Comp, **62** (1994), 865-874.
3. N, Koblitz, *Algebraic aspects of cryptography* (1996), Springer.
4. N, Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139-150.
5. A.M. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, Advances in Cryptology-Euro Crypt 89, Springer Verlag, 224-314.

6. S.C.Pohlig, M.E. Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Tansactions on Information Theory **24** (1978), 106-110.
7. Y.Sakai, K.Sakurai, H.Ishizuka, *Secure hyperelliptic cryptosystems and their performance*, In "public key cryptosystem", **1 of LNCS** (1998), Springer, 164-181.
8. A. Weil, *Numbers of solutions of equations in finite fields*, Bull.Amer.Math.Soc. **55** (1949), 497-508.

Division of Mathematical Science
Wonkwang University
Iksan, Cheonbuk 570-749
iki@wonnms.wonkwang.ac.kr

Department of Applied Mathematics
Konkuk University
Chungju, Chungbuk 380-701
sungtae.jun@kku.ac.kr