Attack Cryptosystems Based on HCDLP *

Mingqiang Wang, Xiaoyun Wang[1,2], and Tao Zhan[3]
1. School of Mathematics, Shandong University,
Jinan 250100, China
2. Institute for Advanced Study, Tsinghua University,
Beijing 100084, China
3. School of Mathematics, Jilin University,
Changchun 130012, China
Email: *wangmingqiang@sdu.edu.cn*

Abstract

We present an algorithm for solving the discrete logarithm problem on hyperelliptic curves defined over finite field when the cyclic group can be represented by special form. On the general case, we design a method to attack on hyperelliptic curve cryptosystems. As an example, we illustrate an attack on the Twin Diffie-Hellman key agreement scheme[5]. As a byproduct, we enumerate the isomorphism classes of genus 2 hyperelliptic curves which satisfy some special conditions over a finite field.

Keywords: Hyperelliptic curve; Discrete logarithm; Subexponentiality; Smooth integer.

Mathematics Subject Classification 2000: 11G20

1 Introduction

In 1996 a fault analysis attack was introduced by Boneh et al. [4]. Biehl et al.[2] proposed the first fault-based attack on elliptic curve cryptography [11, 16]. Karabina and Ustaoglu[10] demonstrated that invalid-curve attacks can be successfully mounted on protocols based on genus 2 hyperelliptic curves if the appropriate public-key validation is not performed. They illustrated their attacks on two recently-proposed discrete logarithm protocols the Twin Diffie-Hellman key agreement scheme[5] and the XCR signature scheme [12]. Their

*This work was supported by national 973(Grant No.2007CB807902); and Doctoral Fund of Ministry of Education of China (Grant No 20090131120012); and IIFSDU(Grant No 2010ST075).

basic idea is to change the input points, elliptic curve parameters, or the base field in order to perform the operations in a weaker group where solving the elliptic curve discrete logarithm problem (ECDLP) is feasible. A basic assumption for this attack is that one of the two parameters of the governing elliptic curve equation is not involved for point operations formulas. In this way, the computation could be performed in a cryptographically less secure elliptic curve.

In this paper, we consider the hyperelliptic curves of genus 2 which is given by the following Weierstrass equation

$$\mathcal{H} : y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0. \tag{1}$$

The divisor classes $\overline{D} \in J_{\mathcal{H}}(\mathbb{F}_q)$ are in one-to-one correspondence with the pairs of polynomials (u, v) with $u, v \in \mathbb{F}_q[x]$, $\deg(v) < \deg(u) \leq g$, u monic, and $u|(v^2 + hv - f)$.

Our work are based on the facts that the two parameters f_1, f_0 of the hyperelliptic curve equation does not involved for point operations formulas. If $\deg(u) = 1$, we can convert the HCDLP in $J_{\mathcal{H}}(\mathbb{F}_q)$ into the HCDLP in $J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$, where $\widehat{\mathcal{H}}$ is another hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$. This is the key ingredient of our attack method. If all prime factors of $\sharp J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$ are small, one can solve the HCDLP in group $J_{\mathcal{H}}(\mathbb{F}_q)$.

If $\deg(u) = 2$, we design a method to attack cryptosystems based on HCDLP. As an example, we illustrate the attacks on the Twin Diffie-Hellman key agreement scheme[5].

The efficiency our attack method is depend on the number of $\widehat{\mathcal{H}}$ over $\mathbb{F}_q$. In Section 3, we research the isomorphism classes of the elliptic curves expressed by form (1). The analysis of our method in this paper shows that the performance of the algorithm is largely determined by the density of numbers built up from small primes in the neighborhood of $q^2 + 1$ and the number of isomorphism classes of the hyperelliptic curves which can be expressed by form (1).

The paper is organized as follows. In Section 2, some basic knowledge are described. In Section 3, we discuss the isomorphism class of hyperelliptic curves expressed by form (1). Then in Section 4, we give the main idea of the algorithm. In section 5, the efficiency of the attack algorithm is considered.

2 Preliminaries

2.1 Hyperelliptic curve

A hyperelliptic curve $\mathcal{H}$ of genus g over a finite field $\mathbb{F}_q$ is defined by a non-singular Weierstrass equation

$$\mathcal{H} : Y^2 + h(x)y = f(x),$$

where $f, h \in \mathbb{F}_q[x]$, f is monic, $\deg(f) = 2g+1$, and $\deg(h) \leq g$. If $Char(\mathbb{F}_q) \neq 2$, the transformation $y \mapsto y - h(x)/2$ leads to an isomorphic curve given by

$$\mathcal{H} : Y^2 = f(x).$$

If additionally $Char(\mathbb{F}_q)$ is coprime to $2g$, a transformation allows to give

$$\mathcal{H} : y^2 = f(x),$$

where

$$f(x) = x^{2g+1} + \sum_{i=0}^{2g-1} f_i x^i.$$

Let $\mathcal{H}$ be an affine hyperelliptic curve of genus g with function field $\mathbb{F}_q(\mathcal{H})$ and coordinate ring $\mathcal{O} = \mathbb{F}_q[\mathcal{H}]$. The group of $\mathcal{O}$-ideal classes is denoted by $\mathrm{Cl}(\mathcal{O})$. The Jacobian $J_{\mathcal{H}}(\mathbb{F}_q)$ of $\mathcal{H}$ over $\mathbb{F}_q$ is the quotient group of the degree zero divisors defined over $\mathbb{F}_q$ by the group of principal divisors defined over $\mathbb{F}_q$.

Lemma 1 *We use the notation from above. There exists a surjective homomorphism from $J_{\mathcal{H}}(\mathbb{F}_q)$ to $\mathrm{Cl}(\mathcal{O})$.*

Assume that there is a cover

$$\varphi : \mathcal{H} \to \mathbb{P}^1,$$

in which one point P_∞ is totally ramified and induces the place v_∞ in the function field $\mathbb{F}_q(x_1)$ of $\mathbb{P}^1$. Then ϕ is an isomorphism. In this paper, we consider this type of hyperelliptic curves $\mathcal{H}$.

Lemma 2 *Let $\mathcal{H}$ be a hyperelliptic curve over finite field $\mathbb{F}_q$ of genus g and let ω denote the nontrivial automorphism of $\mathbb{F}_q(\mathcal{H})$ over $\mathbb{F}_q(x)$ with a $\mathbb{F}_q$-rational Weierstrass point P_∞ lying over the place x_∞ of $\mathbb{F}_q[x]$. Let $\mathcal{O} = \mathbb{F}_q[x,y]/(y^2 + h(x) - f(x))$.*

1. *In every nontrivial ideal class c of $\mathrm{Cl}(\mathcal{O})$ there is exactly one ideal $I \subseteq \mathcal{O}$ of degree $t \leq g$ with the property: the only prime ideals that could divide both I and $\omega(I)$ are those resulting from Weierstrass points.*

2. *Let I be as above. Then $I = \mathbb{F}_q[x]u(x) + \mathbb{F}_q[x](v(x) - y)$ with $u(x), v(x) \in \mathbb{F}_q[x]$, u monic of degree t, $\deg(v) < t$ and u divides $v^2 + h(x)v - f(x)$.*

3. *The polynomial $u(x)$ and $v(x)$ are uniquely determined by I and hence by c. So $[u, v]$ can be used as coordinates for c.*

The divisor classes $\overline{D} \in J_{\mathcal{H}}(\mathbb{F}_q)$ are in one-to-one correspondence with the pairs of polynomials (u, v) with $u, v \in \mathbb{F}_q[x]$, $\deg(v) < \deg(u) \leq g$, u monic, and $u|(v^2 + hv - f)$.

In this paper, we consider the hyperelliptic curves of genus 2 which is given by the following Weierstrass equation of form (1). In genus 2 setting, we will use the affine formulae for the group law as described in [1], and refer to these formulae as F_{2a} throughout the paper. The formulae F_{2a} depends only on f_2 and f_3.

3 The attack algorithm

3.1 attack algorithm if $\deg(u) = 1$

Let $\mathcal{H}$ be a hyperelliptic curve of genus 2 defined over a finite field $\mathbb{F}_q$, and $g \in J_{\mathcal{H}}(\mathbb{F}_q)$. The discrete logarithm problem asks, given $h \in \langle g \rangle$, for the integer k such that $h = kg$. Let $[u_g, v_g]$ and $[u_h, v_h]$ be the Mumford representation of the divisors g, h respectively.

If the order of the divisor g contain only small prime factor, then it is possible to use the Silver-Pohlig-Hellman algorithm [18] to solve the DLP as presented in Algorithm 1. Let n be the order of the base point P with a prime factor $n = \prod_{i=0}^{j-1} p_i^{e_i}$, where $p_i < p_{i+1}$.

Algorithm 1 Silver-Pohlig-Hellmans algorithm for solving the DLP

Input: $g \in J_{\mathcal{H}}(\mathbb{F}_q)$, $h \in \langle g \rangle$, $n = \prod_{i=0}^{j-1} p_i^{e_i}$, where $p_i < p_{i+1}$.
Output: An integer k with $h = kg$

1. For $i = 0$ to $j - 1$ do
   1.1 $h' \leftarrow \mathcal{O}$, $k_i \leftarrow 0$.
   1.2 $g_i \leftarrow (n/p_i)g$.
   1.3 For $t = 0$ to $(e_i - 1)$ do
      1.3.1 $h_{t,i} \leftarrow (n/p_i^{t+1})(h + h')$.
      1.3.2 $W_{t,i} \leftarrow \log_{g_i} h_{t,i}$. {DLP in a subgroup of order $ord(g_i)$.}
      1.3.3 $h' \leftarrow h' - W_{t,i} p_i^t g$.
      1.3.4 $k_i \leftarrow k_i + p_i^t W_{t,i}$.
2. Use the CRT to solve the system of congruences $k \equiv k_i \bmod p_i^{e_i}$.
This gives us $k \bmod n$
3. Return (k)

Without losing generalization, we assume that the order of the base point P is a large prime number.

The following result is the key ingredient of our attack method.

Theorem 1 *Let $\mathcal{H}$ be a hyperelliptic curve of genus 2 defined over a finite field $\mathbb{F}_q$, and $g, h \in J_{\mathcal{H}}(\mathbb{F}_q)$ such that $h = kg$. Let $[u_g, v_g]$ and $[u_h, v_h]$ be the Mumford representation of the divisors g, h respectively. If $\deg(u_g) = 1$, then there exist a hyperelliptic curve $\widehat{\mathcal{H}}$ defined over $\mathbb{F}_q$ and divisors $\widehat{g}, \widehat{h} \in J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$ whose Mumford representations are $[u_g, v_g]$ and $[u_h, v_h]$ respectively, such that $\widehat{h} = k\widehat{g}$.*

Proof. Without losing generalization, we assume that the divisor g is a reduced divisor in $J_{\mathcal{H}}(\mathbb{F}_q)$. If $\deg(u_g) = 1$, then there is a point $P \in \mathcal{H}(\mathbb{F}_q)$ such that the divisor g can be uniquely represented by $g =< P > - < P_\infty >$. Put $P = (x_P, y_P)$, then

$$y_P^2 = x_P^5 + f_3 x_P^3 + f_2 x_P^2 + f_1 x_P + f_0,$$

and $[u_g, v_g] = [x - x_P, y_P]$. For any fixed $\widehat{f_1} \in \mathbb{F}_q$, let

$$\widehat{f_0} = y_P^2 - (x_P^5 + f_3 x_P^3 + f_2 x_P^2 + \widehat{f_1} x_P).$$

Define

$$\widehat{\mathcal{H}} : y^2 = x^5 + f_3 x^3 + f_2 x^2 + \widehat{f_1} x + \widehat{f_0},$$

obviously $P = (x_P, y_P) \in \widehat{\mathcal{H}}(\mathbb{F}_q)$ and

$$\widehat{g} =:< P > - < P_\infty > \in J_{\widehat{\mathcal{H}}}(\mathbb{F}_q).$$

It is easy to see the Mumford representation of $\widehat{g}$ equals to $[u_g, v_g]$. Since the formulae F_{2a} depends only on f_2 and f_3, we have $kg = k\widehat{g}$. Therefore, by the Mumford representation of divisor h, we can find a divisor $\widehat{h} \in J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$ such that $\widehat{h} = k\widehat{g}$. This complete the proof of the theorem.

Having the points pair $\widehat{g}, \widehat{h} \in J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$, one can obtain $k \bmod n$, where $n = ord(\widehat{g})$. This would be possible if all the prime factors of n are smaller than order of g. The complete attack procedure is presented as Algorithm 2.

Algorithm 2 Basic attack on F_{2a} algorithm

Input: Hyperelliptic curve $\mathcal{H}$ defined over $\mathbb{F}_q$,
$g \in J_{\mathcal{H}}(\mathbb{F}_q)$, $h \in \langle g \rangle$, $h = kg$, w a parameter to be chosen later.
the Mumford representations $[u_g, v_g]$, $[u_h, v_h]$ of g, h with $\deg(u_g) = 1$.
Output: Scalar k partially with a probability.

1. By $[u_g, v_g]$, find $P = (x_P, y_P)$.
2. Randomly choose $\widehat{f_1} \in \mathbb{F}_q$.
   2.1 Compute $\widehat{f_0} = y_P^2 - (x_P^5 + f_3 x_P^3 + f_2 x_P^2 + \widehat{f_1} x_P)$.
3. Define $\widehat{\mathcal{H}} : y^2 = x^5 + f_3 x^3 + f_2 x^2 + \widehat{f_1} x + \widehat{f_0}$.
   3.1 Obtain $n = ord(< P > - < P_\infty >)$ in $J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$.
4. If all the prime factors of n are smaller than w, then
   4.1 Utilize Algorithm 1 on $J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$
   with $([u_g, v_g], [u_h, v_h], n)$ to obtain $k \bmod n$.
5. Return ($k \bmod n$)

By repeating Algorithm 2, then applying CRT, we can get k from the congruences $k \bmod n$.

Remark. In theorem 1, the divisors of g, h and $\widehat{g}, \widehat{h}$ have the same representations $[u_g, v_g]$ and $[u_h, v_h]$ respectively. Since the same polynomials can

generate different ideals in the rings $K[\mathcal{H}]$ and $K[\widehat{\mathcal{H}}]$. Therefore the ideal pair corresponding to the pair (g, h) in $J_{\mathcal{H}}(\mathbb{F}_q) \bigotimes J_{\mathcal{H}}(\mathbb{F}_q)$ is different from the ideal pair corresponding to the pair $(\widehat{g}, \widehat{h})$ in $J_{\widehat{\mathcal{H}}}(\mathbb{F}_q) \bigotimes J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$.

3.2 Attack algorithm when $\deg(u_g) = 2$

Cash, Kiltz and Shoup [5] proposed and analyzed a simple Diffie-Hellman type protocol depicted in the following. The security of TDH relies on the twin Diffie-Hellman assumption which is equivalent to the computational Diffie-Hellman assumption. This is in contrast with many other key agreement protocols, where security has only been proven with respect to the gap Diffie-Hellman assumption.

We design a small subgroup attacks on the static Diffie-Hellman protocol to the TDH protocol in the genus 2 setting. We show how an adversary can successfully break the protocol should honest parties fail to obtain assurances that the static public keys of their peers were validated.

The twin Diffie-Hellman protocol: A cyclic group $< g >$ which the discrete logarithm is infeasible.

1. Party $\widehat{A}$ compute $X = xg$, and $A = ag$, send X, A to party $\widehat{B}$.
2. Party $\widehat{B}$ compute $Y = yg$, and $B = bg$, send Y, B to party $\widehat{A}$.
3. $\widehat{A}$ and $\widehat{B}$ compute

$$k = H(\widehat{A}, \widehat{B}, \mathrm{CDH}(A, B), \mathrm{CDH}(A, Y), \mathrm{CDH}(X, B), \mathrm{CDH}(X, Y)).$$

We now describe an attack that allows $\mathcal{M}$ to recover the static private key of an honest party. Suppose that the underlying group is a prime-order subgroup of $J_{\mathcal{H}}$, where $\mathcal{H}$ is the hyperelliptic curve over finite field $\mathbb{F}_q$ defined by the polynomial

$$\mathcal{H} : y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

Suppose also that honest parties use group addition formula F_{2a}, Recall that F_{2a} does not explicitly use the coefficients f_1 and f_0. in this case $\mathcal{M}$ chooses curves $\widehat{\mathcal{H}}$ over finite field $\mathbb{F}_q$ represented by the equation

$$\widehat{\mathcal{H}} : y^2 = x^5 + f_3x^3 + f_2x^2 + \widehat{f_1}x + \widehat{f_0},$$

according to $\mathcal{H}$ and a random point $P \in \mathcal{H}(\mathbb{F}_q)$, such that $\widehat{\mathcal{H}}(P) = 0$ and $\mathcal{H}(P) = 0$. $\mathcal{M}$ choose x, a according the order of the divisor $h =: < P > - < P_\infty >$. Then $\mathcal{M}$ compute $X = xh$, $A = ah$ such that the order of X, A are small number u, v respectively, with $\gcd(u, v) = 1$. Then $\mathcal{M}$ initiates a session with $\widehat{B}$ and obtains the session key

$$k = H(\widehat{A}, \widehat{B}, bA, yA, bX, yX).$$

Now $\mathcal{M}$ computes

$$k' = H(\widehat{A}, \widehat{B}, i_1A, i_2A, i_3X, i_4X),$$

where i_1, i_2 range over $\mathbb{Z}_v$ and i_3, i_4 over $\mathbb{Z}_u$, until $k' = k$ in which case $\mathcal{M}$ obtain the following congruence equations

$$\begin{cases} b & \equiv & i_1 (\mathrm{mod} v), \\ b & \equiv & i_3 (\mathrm{mod} u), \end{cases}$$

$$\begin{cases} y & \equiv & i_2 (\mathrm{mod} v), \\ y & \equiv & i_4 (\mathrm{mod} u). \end{cases}$$

After repeating the procedure, $\mathcal{M}$ can recover $\widehat{B}$'s static private key (b, y).

4 Analysis of the attack

4.1 Isomorphism classes of hyperelliptic curves over $\mathbb{F}_q$

Let

$$\mathcal{P}_{f_2,f_3} = \{P_{\widehat{f}_1,\widehat{f}_0} = x^5 + f_3 x^3 + f_2 x^2 + \widehat{f}_1 x + \widehat{f}_0 : \widehat{f}_1, \widehat{f}_0 \in \mathbb{F}_q\}.$$

In this section, we count the number polynomial satisfying some conditions in $\mathcal{P}_{f_2,f_3}$ over $\mathbb{F}_q$. To analysis the attacks, the following results are needed.

Theorem 2 *Let $\mathcal{H}$ be a hyperelliptic curve defined over finite field $\mathbb{F}_q$ which is represented as (1) and $P = (x_P, y_P) \in \mathcal{H}(\mathbb{F}_q)$. There exist subset S_P of $\mathcal{P}_{f_2,f_3}$, for any $P_{\widehat{f}_1,\widehat{f}_0} \in S_P$ satisfying*

$$y_P^2 = P_{\widehat{f}_1,\widehat{f}_0}(x_P).$$

The cardinality of the set S_P is q.

Proof. Since $P = (x_P, y_P) \in \mathcal{H}(\mathbb{F}_q)$, we have

$$y_P^2 = x_P^5 + f_3 x_P^3 + f_2 x_P^2 + f_1 x_P + f_0.$$

For any fixed $\widehat{f}_1 \in \mathbb{F}_q$,we can compute $\widehat{f}_0$ by

$$\widehat{f}_0 = y_P^2 - (x_P^5 + f_3 x_P^3 + f_2 x_P^2 + \widehat{f}_1 x_P).$$

Obviously $y_P^2 = P_{\widehat{f}_1,\widehat{f}_0}(x_P)$, this gives the desired result.

Theorem 3 *Let $\mathcal{H}$ be a hyperelliptic curve defined over finite field $\mathbb{F}_q$ which is represented as (1) and $P \in \mathcal{H}(\mathbb{F}_q)$. There exist subset S of $\mathcal{P}_{f_2,f_3}$, such that for any $P_{\widehat{f}_1,\widehat{f}_0} \in S$, we can find a point $P \in \mathcal{H}(\mathbb{F}_q)$ satisfying*

$$y_P^2 = P_{\widehat{f}_1,\widehat{f}_0}(x_P),$$

where $P = (x_P, y_P)$. The cardinality of the set S is $\frac{\sharp\mathcal{H}(\mathbb{F}_q)+T_2-1}{2}(q-1)+1$, where T_2 is the number of points $P \in \mathcal{H}(\mathbb{F}_q)$ satisfying $P = -P$.

Proof. By Theorem 2, we have $S = \bigcup_{P\in\mathcal{H}(\mathbb{F}_q)} S_P$. We claim that for any $P_1, P_2 \in \mathcal{H}(\mathbb{F}_q)$, if $P_1 = \pm P_2$ then $S_{P_1} = S_{P_2}$, and if $P_1 \neq \pm P_2$ then $S_{P_1} \bigcap S_{P_2} = \{P_{f_1,f_0}\}$.

Since $\mathcal{H}$ is a hyperelliptic curve represented by equation (1), if $P_1 = -P_2$, then we have $x_{P_1} = x_{P_2}$ and $y_{P_1} = -y_{P_2}$. This gives $y_{P_1}^2 = (-y_{P_2})^2$, by the argument of Theorem 2, we have $S_{P_1} = S_{P_2}$. If $P_1 \neq \pm P_2$, then we have $x_{P_1} \neq x_{P_2}$ and $y_{P_1} \neq \pm y_{P_2}$. Let

$$A_i = y_{P_i}^2 - (x_{P_i}^5 + f_3 x_{P_i}^3 + f_2 x_{P_i}^2), \quad i = 1, 2.$$

$P_1, P_2 \in \mathcal{H}(\mathbb{F}_q)$ implies that

$$\begin{cases} f_1 x_{P_1} + f_0 &= A_1, \\ f_1 x_{P_2} + f_0 &= A_2. \end{cases}$$

Since the rank of the coefficient matrix $\begin{pmatrix} x_{P_1} & 1 \\ x_{P_2} & 1 \end{pmatrix}$ is 2. Hence there is an unique solution the following equations set

$$\begin{cases} f_1 x_{P_1} + f_0 &= A_1, \\ f_1 x_{P_2} + f_0 &= A_2. \end{cases}$$

So we have $S_{P_1} \bigcap S_{P_2} = \{P_{f_1,f_0}\}$. It is noticed that $S_{P_\infty} = \emptyset$. This shows that the cardinality of the set S is $\frac{\sharp\mathcal{H}(\mathbb{F}_q)-T_2-1}{2}(q-1) + T_2(q-1) + 1$ which can complete the theorem.

4.2 Efficiency of the attack method

A hyperelliptic curve $\mathcal{H}'$ of form (1) isomorphic to $\mathcal{H}$ if and only if there exists an admissible transform

$$\begin{cases} x' &= u^2 x, \\ y' &= u^{2g+1} y, \end{cases}$$

where $u \in \mathbb{F}_q^*$. Let

$$\mathcal{H}' : y^2 = x^5 + f_3 x^3 + f_2 x^2 + \widehat{f_1} x + \widehat{f_0}.$$

Therefore, $\mathcal{H} \cong \mathcal{H}'$ if and only if there exists $u \in \mathbb{F}_q^*$ such that $u^4 = 1, u^6 = 1$.

By the Hasse-Weil Theorem, $|\sharp\mathcal{H}(\mathbb{F}_q) - q - 1| \leq 4\sqrt{q}$. Let T_2 be defined as in Theorem 2, then T_2 is the number of the solutions in $\mathbb{F}_q$ of $P_{f_1,f_0}(x) = 0$, and $T_2 \leq 5$. Let

$$S_P^{\mathcal{H}} = \{y^2 = f(x) : f(x) \in S_P\}, \quad S^{\mathcal{H}} = \{y^2 = f(x) : f(x) \in S\}.$$

where S_P and S is defined as in Theorem 2 and Theorem 3 respectively. Then we have $\sharp S_P^{\mathcal{H}} \geq q/6$ and $\sharp S^{\mathcal{H}} \geq q^2/12$.

For $0 \leq \alpha \leq 1$, let $L_x(\alpha, c)$ denote

$$\exp(c(\log x)^{\alpha}(\log\log x)^{1-\alpha}),$$

where c is a constant. A theorem of Canfield, Erdös and Pomerance [6] implies the following result. Let α be a positive real number. Then the probability that a random positive integer $s < x$ has all its prime factors less than $L_x(1/2,1)^{\alpha}$ is $L_x(1/2,1)^{-1/2\alpha+o(1)}$ for $x \to \infty$. The conjecture we need is that the same result is valid if s is a random integer in the interval $(x+1-x^{\frac{3}{2}}, x+1+x^{\frac{3}{2}})$.

It follows that we have to consider subexponentially many random hyperelliptic curves until one of them has subexponentially smooth order. Thus the expected number of trials of the attack with random hyperelliptic curves $\widehat{\mathcal{H}}(\mathbb{F}_q)$ until we find that $\sharp J_{\widehat{\mathcal{H}}}(\mathbb{F}_q)$ is a subexponentially smooth integer and can determine the secret multiplier k is subexponential again.

References

[1] R. Avanzi, H. Cohen, C. Docke, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman and Hall/CRC, Boca Raton, FL, USA, (2005).

[2] I. Biehl, B. Meyer and V. Müller, Differential fault attacks on elliptic curve cryptosystems, In CRYPTO 2000, LNCS 1880, (2000), 131-146.

[3] B. J. Birch, How the number of points of an elliptic curve over a fixed prime field varies, J. London Math. Soc. 43 (1968), 57-60.

[4] D. Boneh, R.A. DeMillo and R.J. Lipton, On the importance of eliminating errors in cryptographic computations, J. Crypto. 14(2), (2001), 101-119.

[5] D. Cash, E. Kiltz and V. Shoup, The twin Diffie-Hellman problem and applications, in Advances in Cryptology-EUROCRYPT 2008, (2008), 127-145.

[6] E. R. Canfield, P. Erdös and C. Pomerance, On a problem of Oppenheim concerning " Factorisatio Numerorum", J. Number Theory 17 (1983), 1-28.

[7] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkbrper, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197-272.

[8] G. Frey and H. Ruck, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Mathematics of Computation, 62 (1994), 865-874.

[9] P. Gaudry, F. Hess and N. Smart, Constructive and destructive facets of Weil descent on elliptic curves, Journal of Cryptology, 15 (2002), 19-46.

[10] K. Karabina, B. Ustaoglu, INVALID-CURVE ATTACKS ON (HYPER)ELLIPTIC CURVE CRYPTOSYSTEMS, Advances in Mathematics of Communications, Vol 4, No.3, (2010), 307-321.

[11] N. Koblitz. Elliptic curve cryptosystems. Math. Comp., 48(177)(1987), 203-209.

[12] H. Krawczyk, HMQV: A high-performance secure Diffie-Hellman protocol, in Advances in Cryptology-CRYPTO 2005, (2005), 546-566.

[13] H. W. Lenstra, Mathematics Factoring Integers with Elliptic Curves, Annals of Mathematics, Second Series, Vol.126, No. 3 (1987), pp. 649-673.

[14] H. W. Lenstra, Jr., J. Pila, and C. Pomerance, A hyperelliptic smoothness test. I, Phil. Trans. R. Soc. Lond. (A) 345 (1993), pp. 397-408.

[15] A. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory, 39 (1993), 1639-1646.

[16] V. Miller. Use of elliptic curves in cryptography. In CRYPTO 86, LNCS 263(1987), 417-426..

[17] P.L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization. Math. Comput. 48 (1987), 243-264.

[18] S. Pohlig, M. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. IEEE Trans. Inf. Theory 24, (1978), pp. 106-110.

[19] J.M. Pollard, Monte Carlo methods for index computation (mod p). Math. Comput. 32,(1978), 918-924.

[20] T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, Commentarii Mathematici Uni- versitatis Sancti Pauli, 47 (1998), 81-92.

[21] R. J. Schoof, Nonsingular plane cubic curves over finite fields, Journal of Combinatorial Theory, Series A, Vol 46, No. 2, (1987), 183-211.

[22] R. J. Schoof, Elliptic curves over finite fields and the computation of square roots mod$p$, Math. Comp. Vol 44(1985), 483-494.

[23] D. Shanks, Class number, a theory of factorization, and genera, in Proceedings of the Symposium in Pure Mathematics, vol. 20 (1971), pp. 415-440.

[24] I. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, Mathematics of Computation, 67 (1998), 353-356.

[25] N. Smart, The discrete logarithm problem on elliptic curves of trace one, Journal of Cryptology, 12 (1999), 193-196.

[26] W. C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Ecole Norm. Sup. (4) 2 (1969), 521-560.