Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2011, Article ID 580749, 11 pages
doi:10.1155/2011/580749

Research Article

Analysis of the Fault Attack ECDLP over Prime Field

Mingqiang Wang and Tao Zhan

School of Mathematics, Shandong University, Jinan 250100, China

Correspondence should be addressed to Mingqiang Wang, mqwang71@hotmail.com

Received 17 May 2011; Revised 27 August 2011; Accepted 12 September 2011

Academic Editor: Tak-Wah Lam

In 2000, Biehl et al. proposed a fault-based attack on elliptic curve cryptography. In this paper, we refined the fault attack method. An elliptic curve E is defined over prime field $\mathbb{F}_p$ with base point $P \in E(\mathbb{F}_p)$. Applying the fault attack on these curves, the discrete logarithm on the curve can be computed in subexponential time of $L_p(1/2, 1 + o(1))$. The runtime bound relies on heuristics conjecture about smooth numbers similar to the ones used by Lenstra, 1987.

1. Introduction

In 1996, a fault analysis attack was introduced by Boneh et al. [1]. Biehl et al. [2] proposed the first fault-based attack on elliptic curve cryptography [3, 4]. Their 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 [2], it is claimed that the attacker can get the secret multiplier k with subexponential time, but the authors did not give the proof or even an outline of the proof. I find that this is not a trivial result. Since the distribution of the cardinality of elliptic curves over finite field $\mathbb{F}_q$ is not uniform in the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$.

In practice, in order to get a better function, the cryptosystem may be based on some special family of elliptic curve. Here, we assume that the fault attack is restricted on the following elliptic curve defined over prime field $\mathbb{F}_p$:

$$y^2 = x^3 + Ax^2 + B, \tag{1.1}$$

which is denoted by $E_{A,B}$. In this paper, we prove that the attacker can get the secret multiplier k with subexponential time when the fault attack is restricted to the elliptic curve family of $E_{A,B}$. It is noted that we can get a simpler proof when the fault attack is based on the general elliptic curves.

In Section 2, the fault attack method is described in detail and some improvements of the fault attack are introduced. Firstly, we can control the order of the fault point in $E_{A,\widehat{B}}$ by a suitable choice of the random key d. On the other hand, some points in $E_{A,B}$ can be chosen as fault point to increase the probability of success of the fault attack.

Our analysis depends on the number of $\sharp E_{A,\widehat{B}}(\mathbb{F}_p)$ with $\widehat{B} \in \mathbb{F}_p$. In Section 3, we research the isomorphism classes of the elliptic curves expressed by form (1.1). By Deuring [5], we find that the density of $\sharp E_{A,\widehat{B}}(\mathbb{F}_p)$ with $\widehat{B} \in \mathbb{F}_p$ in $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ is large enough to ensure our method success.

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 $p+1$ and the number of isomorphism classes of the elliptic curves which can be expressed by form (1.1). If a reasonable conjecture concerning the density of smooth integers is assumed, then the following can be proved.

Suppose that $0 \le \alpha \le 1$ and c is a positive constant; let $L_x(\alpha, c)$ denote

$$\exp\left(c(\log x)^{\alpha}(\log\log x)^{1-\alpha}\right). \tag{1.2}$$

There is a function $K : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ with $K(x) = L_x(1/2, 1+o(1))$ for $x \to \infty$. Then, with a suitable choice of parameters, ECDLP in the family of elliptic curves (1.1) can be determined by the attacker with probability at least $1 - e^{-h}$ within time $K(p)M(p)$, where $M(p) = O((\log p)^{11})$ and h is the number of times Algorithm 2 is applied.

The paper is organized as follows. In Section 2, we describe the scalar multiplication algorithm and elliptic curve discrete logarithm problem and refine the fault attack method. In Section 3, we discuss the isomorphism class of elliptic curves expressed by form (1.1). In Section 4, the efficiency of the attack algorithm is considered.

2. Preliminaries

2.1. Scalar Multiplication Algorithm

Let $E_{A,B}$ be an elliptic curve of form (1.1) defined over finite field $\mathbb{F}_p$ with $p \neq 2, 3$ and $P_i =: (x_i, y_i) \in E_{A,B}(\mathbb{F}_p)$, $i = 1, 2, 3$, such that $P_1 + P_2 = P_3$. The algorithm below is a description of the elliptic curve scalar multiplication (ECSM) on curves defined in its most common form:

$$\begin{aligned} x_3 &= \lambda^2 - A - x_1 - x_2, \\ y_3 &= -y_1 - (x_3 - x_1)\lambda \end{aligned} \tag{2.1}$$

with

$$\lambda = \begin{cases} \dfrac{3x_1^2 + 2Ax_1}{2y_1} & \text{if } x_1 = x_2, \text{ and } y_1 = y_2, \\ \dfrac{y_1 - y_2}{x_1 - x_2}, & \text{otherwise.} \end{cases} \tag{2.2}$$

The fault attack is based on the fact that the curve coefficient B is not used in any of the addition formulas given above.

2.2. Elliptic Curve Discrete Logarithm Problem

Let E be an elliptic curve and $P = (x_P, y_P) \in E$. Given $Q = (x_Q, y_Q) \in \langle P \rangle$, the discrete logarithm problem asks for the integer k such that $Q = kP$.

If the order of the base point P does not contain at least a large prime factor, then it is possible to use an extension for ECC of the Silver-Pohlig-Hellman algorithm [6] to solve the ECDLP 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 $p_i < p_{i+1}$, $i = 0, \ldots, j-2$.

Without losing generality, we assume that the order of the base point P is a prime number which is large enough for practical cryptosystems.

2.3. Fault Attack

In this section, we consider the following EC ElGamal cryptosystem. Let $E_{A,B}$ be an elliptic curve of form (1.1) defined over a prime field $\mathbb{F}_p$. Given a point $P = (x_P, y_P) \in E_A(\mathbb{F}_p)$, we assume that $Q = (x_Q, y_Q) = kP$ is the public key and $1 \leq k < \operatorname{ord}(P)$ the secret key of some user, where $\operatorname{ord}(P)$ denotes the order of the base point P.

> Encryption: Input message m, choose $1 < d < \operatorname{ord}(P)$ randomly, and return $(dP, x_{dQ} \bigoplus m)$.
>
> Decryption: Input (H, m'), compute kH, and return $(m' \bigoplus x_{kH})$.

The fault attack is that the attacker randomly chooses an elliptic curve $E_{A,\widehat{B}}$ defined over prime field $\mathbb{F}_p$, finds a point $\widehat{P} = (x_{\widehat{P}}, y_{\widehat{P}}) \in E_{A,\widehat{B}}(\mathbb{F}_p)$, and inputs $(d\widehat{P}, m')$ to the decryption oracle, then the attacker can get the x-coordinate of $kd\widehat{P}$. Having $x_{kd\widehat{P}}$, we compute $y_{kd\widehat{P}}$ by

$$y_{kd\widehat{P}} = \sqrt{x_{kd\widehat{P}}^3 + Ax_{kd\widehat{P}}^2 + \widehat{B}}. \tag{2.3}$$

In practice, we can compute $E_{A,\widehat{B}}$ and $\widehat{P} \in E_{A,\widehat{B}}(\mathbb{F}_p)$ as follows. Fix an element $x_{\widehat{P}} \in \mathbb{F}_p$, for any $y_{\widehat{P}} \in \mathbb{F}_p$, and define

$$\widehat{B} =: y_{\widehat{P}}^2 - x_{\widehat{P}}^3 - Ax_{\widehat{P}}^2. \tag{2.4}$$

Input: $P \in E(\mathbb{F}_p)$, $Q \in \langle P \rangle$, $n = \prod_{i=0}^{j-1} p_i^{e_i}$, where $p_i < p_{i+1}$, $i = 0, \ldots, j-2$.
Output: $k \mod n$.
(1) For $i = 0$ to $j - 1$ do
  (1.1) $Q' \leftarrow \mathcal{O}$, $k_i \leftarrow 0$.
  (1.2) $P_i \leftarrow (n/p_i)P$.
  (1.3) For $t = 0$ to $(e_i - 1)$ do
    (1.3.1) $Q_{t,i} \leftarrow (n/p_i^{t+1})(Q + Q')$.
    (1.3.2) $W_{t,i} \leftarrow \log_{P_i} Q_{t,i}$.{ECDLP in a subgroup of order ord(P_i).}
    (1.3.3) $Q' \leftarrow Q' - W_{t,i} p_i^t P$.
    (1.3.4) $k_i \leftarrow k_i + p_i^t W_{t,i}$.
(2) Use the CRT to solve the system of congruences $k \equiv k_i \mod p_i^{e_i}$.
  This gives us $k \mod n$
(3) Return (k)

Algorithm 1: Silver-Pohlig-Hellman algorithm for solving the ECDLP.

Input: E_A and $P = (x_P, y_P) \in E_A(\mathbb{F}_p)$, $Q = (x_Q, y_Q) = kP$,
w is a parameter to be chosen later and q is the order of point P.
Output: Scalar k partially with a probability.
(1) Randomly choose $x_{\widehat{P}}, y_{\widehat{P}} \in \mathbb{F}_p$.
  (1.1) $\widehat{B} \leftarrow y_{\widehat{P}}^2 - x_{\widehat{P}}^3 - A x_{\widehat{P}}^2$.
(2) $\widehat{P} \leftarrow (x_{\widehat{P}}, y_{\widehat{P}})$.
  (2.1) Obtain $n = \text{ord}(\widehat{P})$ in elliptic curve $E_{A,\widehat{B}}(\mathbb{F}_p)$.
  (2.2) Choose an integer $1 < d < \text{ord}(\widehat{P})$, compute $d\widehat{P}$.
(3) Apply decryption oracle to compute $x_{kd\widehat{P}}$.
  (3.1) $y_{kd\widehat{P}} \leftarrow \sqrt{x_{kd\widehat{P}}^3 + A x_{kd\widehat{P}}^2 + \widehat{B}}$.
(4) If all the prime factors of n are smaller than w, then
  (4.1) Utilize Algorithm 2 with $(d\widehat{P}, kd\widehat{P}, n)$ to obtain $k \mod n$.
(5) Return $(k \mod n)$

Algorithm 2: Basic fault attack on ECSM algorithm.

Let $E_{A,\widehat{B}}$ be an elliptic curve of form (1.1) as follows:

$$y^2 = x^3 + Ax^2 + \widehat{B}, \tag{2.5}$$

clearly $\widehat{P} =: (x_{\widehat{P}}, y_{\widehat{P}}) \in E_{A,\widehat{B}}(\mathbb{F}_p)$.

Having the points pair $d\widehat{P}, kd\widehat{P} \in E_{A,\widehat{B}}(\mathbb{F}_p)$, one can obtain $k \bmod n$, where $n = \text{ord}(d\widehat{P})$. This would be possible if all the prime factors of $\sharp E_{A,\widehat{B}}(\mathbb{F}_p)$ are smaller than order of P. The complete attack procedure is presented as Algorithm 2.

By repeating Algorithm 2, then applying CRT, we can get k from the congruences $k \mod n$. The following lemma is useful for us to increase the efficiency of Algorithm 2.

Lemma 2.1. *Let E be an elliptic curve defined over finite filed $\mathbb{F}_q$. Then,*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \tag{2.6}$$

with $n_1 \mid n_2$ and $n_1 \mid q - 1$.

For giving an elliptic curve $E_{A,\widehat{B}}$ defined over finite field $\mathbb{F}_p$, we assume that $E_{A,\widehat{B}}(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Then there exists a point $\widehat{P}$ such that $\mathrm{ord}(\widehat{P}) = n_2$. The number of such points is $n_1\phi(n_2)$, where $\phi(\cdot)$ is the Euler function. Let $n_2 = n_{2w}n_2'$, where n_{2w} is the product of all the prime factors of n_2 which are smaller than w. If, in Step (2.2), we choose d satisfying $n_2' \mid d$ and $(d, n_{2w}) = 1$, then the order of $d\widehat{P}$ is a w smooth integer.

Certainly, of course, we can choose a point $\widehat{P}$ in $E_{A,B}(\mathbb{F}_p)$. The procedure of choosing such a point is similar as above.

3. The Isomorphism Classes

In this section, we count the number of isomorphism classes over $\mathbb{F}_p$ of elliptic curves (1.1) defined over a prime field $\mathbb{F}_p$.

It is easy to see that the discriminant Δ and the j invariant of the formula (1.1) are equal to $-16((4/27)A^4(1-A^2) + 4A^2B + 27B^2)$ and $-(4^3A^6)/\Delta$, respectively. Hence, the number of elliptic curves over the prime field $\mathbb{F}_p$ with A fixed is the number of $B \in \mathbb{F}_p$ with

$$\frac{4}{27}A^4\left(1-A^2\right) + 4A^2B + 27B^2 \neq 0. \tag{3.1}$$

Let T be the number of the solutions of the following equation in $\mathbb{F}_p$:

$$27x^2 + 4A^2x + \frac{4}{27}A^4\left(1-A^2\right) = 0. \tag{3.2}$$

It is easy to see that $T \leq 2$. Hence, we conclude that the number of elliptic curves over $\mathbb{F}_p$ with B fixed is equal to $p - T$.

$E_{A,B}$ is isomorphic to $E_{A,\widehat{B}}$ if and only if there exists an admissible transform:

$$\begin{aligned} \overline{x} &= u^2x + r, \\ \overline{y} &= u^3y + u^2sx + t, \end{aligned} \tag{3.3}$$

where $r, s, t \in \mathbb{F}_p$ and $u \in \mathbb{F}_p^*$. Therefore, $E_{A,B} \cong E_{A,\widehat{B}}$ if and only if there exist $u \in \mathbb{F}_p^*, r \in \mathbb{F}_p$ such that the following conditions hold:

(i) $u^6 = 1$ and $A = Au^4 + 3u^4r$;

(ii) $3u^2r^2 + 2u^2rA = 0$ and $Ar^2 + r^3 + \widehat{B} = B$.

Given $A, B, \widehat{B}$, let T' denote the number of the solutions (u, r) of (i) and (ii); it is easy to see that $T' \leq 6$. For any $p \neq 2, 3$, the number of the automorphism of elliptic curve $E_{A,B}$ is at most 3. Hence, we have

$$\sum_{E_{A,\widehat{B}}}{}' \frac{1}{\sharp\mathrm{Aut}\left(E_{A,\widehat{B}}\right)} \geq \frac{p-T}{6}, \tag{3.4}$$

where $\sum'_{E_{A,\widehat{B}}}$ is over a set of representatives of the isomorphism classes. We express this by writing

$$\frac{\sharp'\left\{E_{A,\widehat{B}} : E_{A,\widehat{B}} \text{ elliptic curve of form (1.1) with } \widehat{B} \in \mathbb{F}_p\right\}}{\cong_{\mathbb{F}_p}}, \tag{3.5}$$

and in similar expression below, $\sharp'$ denotes the weighted cardinality, the isomorphism class of $E_{A,\widehat{B}}$ being counted with the weight $1/(\sharp\mathrm{Aut}(E_{A,\widehat{B}}))$.

For any elliptic curve E over $\mathbb{F}_p$, we have

$$\sharp E(\mathbb{F}_p) = p + 1 - t, \quad \text{with} \quad t \in \mathbb{Z},\ |t| \le 2\sqrt{p}, \tag{3.6}$$

which is obtained by a theorem of Hasse. Let, conversely, p be a prime > 3 and let t be an integer satisfying $|t| \le 2\sqrt{p}$. Then, the weighted number of elliptic curves E over $\mathbb{F}_p$ with $\sharp E(\mathbb{F}_p) = p + 1 - t$, up to isomorphism is given by a formula that is basically due to Deuring [5]; see also [7–9]:

$$\frac{\sharp'\{E : E \text{ elliptic curve over } \mathbb{F}_p,\ \sharp E(\mathbb{F}_p) = p + 1 - t\}}{\cong_{\mathbb{F}_p}} = H\left(t^2 - 4p\right), \tag{3.7}$$

where $H(t^2 - 4p)$ denotes the Kronecker class number of $t^2 - 4p$.

For the Kronecker class number, the following result is useful.

Lemma 3.1 (see [10]). *There exist effectively computable positive constants c_1, c_2 such that for each $z \in \mathbb{Z}_{>1}$ there is $\Delta^* = \Delta^*(z) < -4$ such that*

$$\frac{c_1\sqrt{-\Delta}}{\log z} \le H(\Delta) \le c_2\sqrt{-\Delta}\log|\Delta|\log\log|\Delta| \tag{3.8}$$

for all $\Delta \in \mathbb{Z}$ with $-z \le \Delta < 0$, $\Delta \equiv 0$, or $1 \mod 4$, except that the left inequality may be invalid if $\Delta_0 = \Delta^*$, where Δ_0 is the fundamental discriminant associated with Δ.

Let

$$\frac{\sharp'\left\{E_{A,\widehat{B}} : \widehat{B} \in \mathbb{F}_p, \sharp E_{A,\widehat{B}}(\mathbb{F}_p) = p + 1 - t\right\}}{\cong_{\mathbb{F}_p}} =: H_t. \tag{3.9}$$

In order to apply Algorithm 2, we divide $\mathbb{F}_p$ into two parts S^p_{QR} and S^p_{NQR} as follows:

$$\begin{aligned} S^p_{QR} &= \left\{\widehat{B} : \widehat{B} \in \mathbb{F}_p, \text{ and } x^3_{\widehat{P}} + Ax^2_{\widehat{P}} + \widehat{B} \text{ is a quadratic residue in } \mathbb{F}_p\right\}, \\ S^p_{QNR} &= \left\{\widehat{B} : \widehat{B} \in \mathbb{F}_p, \text{ and } x^3_{\widehat{P}} + Ax^2_{\widehat{P}} + \widehat{B} \text{ is a quadratic nonresidue in } \mathbb{F}_p\right\}. \end{aligned} \tag{3.10}$$

Since $H_t \le H(t^2 - 4p)$, Lemma 2.1 cannot be applied directly in the following estimation. In order to apply Lemma 2.1, S_{QR}^p should be partitioned into two parts S_{QR1}^p and S_{QR2}^p as follows:

$$S_{QR1}^p = \left\{ \widehat{B} : \widehat{B} \in S_{QR}^p, \sharp E_{A,\widehat{B}}(\mathbb{F}_p) = p + 1 - t, \text{with } H_t \ge \frac{\sqrt{p}}{\log p} \right\},$$
$$S_{QR2}^p = \left\{ \widehat{B} : \widehat{B} \in S_{QR}^p, \sharp E_{A,\widehat{B}}(\mathbb{F}_p) = p + 1 - t, \text{with } H_t < \frac{\sqrt{p}}{\log p} \right\}. \tag{3.11}$$

Let

$$T_{QR1}^p = \left\{ s : s \in \mathbb{Z}, \text{ and there exists } \widehat{B} \in S_{QR1}^p \text{ such that } s = \sharp E_{A,\widehat{B}}(\mathbb{F}_p) \right\}. \tag{3.12}$$

Theorem 3.2. *There exist an effectively computable positive constant c_3 such that, for each prime number $p > 3$, the following assertion is valid. If S is a set of integers $s \in T_{QR1}^p$ with*

$$\left| s - (p+1) \right| \le \sqrt{p}, \tag{3.13}$$

then

$$\sharp \left\{ E_{A,\widehat{B}} : \widehat{B} \in S_{QR1}^p, \sharp E_{A,\widehat{B}}(\mathbb{F}_p) \in S \right\} \cong_{\mathbb{F}_p} \ge c_3 (\sharp S - 2) \frac{\sqrt{p}}{\log p}. \tag{3.14}$$

Proof. The proof of Theorem 3.3 is similar to the proof of (1.9) in [10]; for self-containdeness, we give it here. The left-hand side of the inequality equals

$$\sum_{t \in \mathbb{Z}, p+1-t \in S} H_t. \tag{3.15}$$

Applying Lemma 3.1 with $z = 4p$, we note that $|t^2 - 4p| \ge 3p$ if $p + 1 - t \in S$. Since $S \subseteq T_{QR1}^p$, it suffices to prove that there are at most two integers t, $|t| \le \sqrt{p}$, for which the fundamental discriminant associated with $t^2 - 4p$ equals Δ^*. Let $L = \sqrt{\Delta^*}$, and let t be such an integer. Then, the zeros $\alpha, \overline{\alpha}$ of

$$X^2 - tX + p \tag{3.16}$$

belong to the ring of integers $\mathcal{O}_L$ of L. Also, $\alpha\overline{\alpha} = p$, and by the unique prime ideal factorization in $\mathcal{O}_L$ and the fact that $A^* = \{1, -1\}$ (because $\Delta^* < -4$) this determines α up to conjugation and sign. Hence, $t = \alpha + \overline{\alpha}$ is determined up to sign, as required. This completes the proof. □

Theorem 3.3. *There is a positive effectively computable constant c_4 such that, for each prime number $p > 3$, the following assertion is valid. Let S be a set of integers $s \in T_{QR1}^p$ with*

$$\left| s - (p+1) \right| \le \sqrt{p}, \tag{3.17}$$

and let $y_{\widehat{P}}$ be defined as above. Then, the number N of pair $(\widehat{B}, x_{\widehat{P}}) \in \mathbb{F}_p^2$ for which

$$4A^2 + 27\widehat{B} \neq 0, \qquad \sharp E_{A,\widehat{B}}(\mathbb{F}_p) \in S, \tag{3.18}$$

where $x_{\widehat{P}}^3 + Ax_{\widehat{P}}^2 + \widehat{B} = y_{\widehat{P}}^2$, is at least $c_4(\sharp S - 2)(\sqrt{p}^3/\log p)$.

Proof. The number to be estimated equals the number of pairs $(\widehat{B}, y_{\widehat{P}}) \in \mathbb{F}_p^2$ for which $E_{A,\widehat{B}}$ is an elliptic curve over $\mathbb{F}_p$ with $(x_{\widehat{P}}, y_{\widehat{P}}) \in E_{A,\widehat{B}}(\mathbb{F}_p)$ and $\sharp E_{A,\widehat{B}}(\mathbb{F}_p) \in S$. Each elliptic curve $E_{\overline{A}}$ over $\mathbb{F}_p$ is isomorphic to $E_{A,\widehat{B}}$ for exactly $T'/\sharp \mathrm{Aut}E$, value of $\overline{A} \in \mathbb{F}_p$. Each $E_{A,\widehat{B}}$ exactly gives rise to two points $(x_{\widehat{P}}, y_{\widehat{P}})$. Thus, the number to be estimated equals

$$\sum_{E_{A,\widehat{B}}}{}' \frac{2T'}{\sharp \mathrm{Aut}\left(E_{A,\widehat{B}}\right)}, \tag{3.19}$$

where the sum ranges over the elliptic curves $E_{A,\widehat{B}}$ over $\mathbb{F}_p$, up to isomorphism, for which $\sharp E_{A,\widehat{B}}(\mathbb{F}_p) \in S$. Applying Theorem 3.2, we obtain the result. □

Theorem 3.4. *There exists a positive effectively computable constant c_5 such that, for each prime number $p > 3$, the following assertion is valid. Let*

$$S_w = \left\{ s \in T_{QR1}^p : \left|s - (p+1)\right| < \sqrt{p}, \text{ and each prime dividing } s \text{ is} \leq w \right\}, \tag{3.20}$$

and let $y_{\widehat{P}}$ be defined as above. Then, the number N of triple $(\widehat{B}, x_{\widehat{P}}) \in \mathbb{F}_p^2$ for which

$$4A^2 + 27\widehat{B} \neq 0, \qquad \sharp E_{A,\widehat{B}}(\mathbb{F}_p) \in S_w, \tag{3.21}$$

where $x_{\widehat{P}}^3 + Ax_{\widehat{P}}^2 + \widehat{B} = y_{\widehat{P}}^2$, is at least $c_5(\sharp S_w - 2\sqrt{p}^3/\log p)$.

Proof. This can be deduced from Theorem 3.3 immediately. □

Theorem 3.5. *There exists a positive effectively computable constant c_6 such that the cardinality of T_{QR1}^p is at least $c_6\sqrt{p}/(\log p(\log\log p))$.*

Proof. The map

$$\phi : \mathbb{F}_p \longmapsto \mathbb{F}_p \qquad \widehat{B} \longmapsto x_{\widehat{P}}^3 + Ax_{\widehat{P}}^2 + \widehat{B} \tag{3.22}$$

is a bijective map. By the definition of S_{QR}^p and S_{QNR}^p, we have $\sharp S_{QR}^p = \sharp S_{QNR}^p = (p-1)/2$. By (3.6), the trace t of any elliptic curve E over $\mathbb{F}_p$ satisfies $|t| \leq 2\sqrt{p}$; hence, the cardinality of S_{QR2}^p is at most

$$2\sqrt{p}\frac{\sqrt{p}}{\log p} \leq 2\frac{p}{\log p}. \tag{3.23}$$

Therefore, the cardinality of S_{QR1}^{p} is

$$S_{QR}^{p} - S_{QR2}^{p} \geq p - 2\frac{p}{\log p}. \tag{3.24}$$

From the discussion about the isomorphism classes of elliptic curves and the fact that $H_t \leq H(t^2 - 4p)$, we have

$$\sharp T_{QR1}^{p} \geq \frac{\sharp S_{QR1}^{p} - T}{H(\Delta)}. \tag{3.25}$$

Applying Lemma 2.1, we get the proof of the result.

Let $T_1 = T_{QR1}^{p} \bigcap (p + 1 - \sqrt{p}, p + 1 + \sqrt{p})$. Our attack method depends on the following reasonable heuristic assumption.

Heuristic Assumption: *The set T_{QR1}^{p} is uniformly distributed in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$.*

By the assumption, one can deduce that $\sharp T_{QR1}^{p} \approx 2\sharp T_1$. □

Theorem 3.6. *There exists an effectively computable constant $c_7 > 1$ with the following property. Let $w \in \mathbb{Z}_{>1}$ and*

$$\sharp S_w = \left\{ s \in T_{QR1}^{p} : |s - (p+1)| < \sqrt{p}, \text{ and each prime dividing } s \text{ is} \leq w \right\}. \tag{3.26}$$

Let $f(w) = \sharp S_w / \sharp T_1$ denotes the probability that a random integer in the interval $(p+1-\sqrt{p}, p+1+\sqrt{p})$ has all its prime factors $< w$. The probability of success of Algorithm 2 on input $P, Q \in E_{A,B}, w$ is at least $1 - c_7^{-hf(w)/(\log p)^2(\log\log p)}$, where h is the number of times that Algorithm 2 is applied.

Proof. By Theorem 3.5, the failure probability of repeating Algorithm 2 h times equals $(1 - N/p^2)^h$, where

$$\frac{N}{p^2} \geq c_5 \frac{\sharp S_w - 2}{\sharp T_1} \frac{\sharp T_1}{\sqrt{p}\log p} \geq c_5 f(w) \frac{\sharp T_1}{\sqrt{p}\log p} \geq c_5 c_6 \frac{f(w)}{(\log p)^2(\log\log p)}. \tag{3.27}$$

It follows that

$$\left(1 - \frac{N}{p^2}\right)^h \leq e^{-c_5 c_6 h(f(w)/((\log p)^2(\log\log p)))}. \tag{3.28}$$

Consequently, the desired result follows. □

4. Efficiency

In the case of factoring, the best rigorously analyzed result is Corollary 1.2 of [11], which states that all prime factors of n that are less than w can be found in time $L_w(2/3, c)\log^2 n$.

Schoof [12] presents a deterministic algorithm to compute the number of $\mathbb{F}_p$-points of an elliptic curve that is defined over a finite field $\mathbb{F}_p$ and takes $O(\log^9 p)$ elementary operations.

Theorem 3.6 shows that, in order to have a reasonable chance of success, one should choose the number h of the same order of magnitude as $O((\log p)^2(\log\log p)/f(w))$. In Algorithm 2, for any $y_{\widehat{P}}$, we can obtain $\widehat{B} \in S^p_{QR}$. From the discussion in Theorem 3.6, the probability of $\widehat{B} \in S^p_{QR2}$ is approximately $1/\log p$. Hence, the cases of $\widehat{B} \in S^p_{QR2}$ are neglected, which does not affect the analysis result. Therefore, the time spent on Algorithm 2 is $O(hL_w(2/3,c)M(p))$, where $M(p) = O(\log^{11} p)$. The time required by Algorithm 2 is $\sqrt{w}$. Hence, to minimize the estimated running time, the number w should be chosen such that $L_w(2/3,c)/f(w) + \sqrt{w}$ is minimal.

A theorem of Canfield et al. [13] 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 $(x+1-\sqrt{x}, x+1+\sqrt{x})$. Putting $x = p$, we see that the conjecture implies that

$$f\left(L_p\left(\frac{1}{2},1\right)^{\alpha}\right) = L_p\left(\frac{1}{2},1\right)^{-1/2\alpha+o(1)} \quad \text{for } p \longrightarrow \infty, \tag{4.1}$$

for any fixed positive α, with $f(w) = \sharp S_w/\sharp T_1$.

The following identities are useful for our estimation:

$$\begin{aligned} L_p(\alpha,c_\alpha)L_p(\beta,c_\beta) &= L_p\left(\max\{\alpha,\beta\}, c_{\max\{\alpha,\beta\}}\right), \\ L_{L_p(\alpha,c_\alpha)}(\beta,c_\beta) &= L_p\left(\alpha\beta, c_\beta c_\alpha^\beta\right), \end{aligned} \tag{4.2}$$

where lower-order terms in the exponent are neglected.

With $w = L_p(1/2,1)^\alpha$, the conjecture would imply that

$$\frac{L_w(2/3,c)}{f(w)} + \sqrt{w} = L_p\left(\frac{1}{2},1\right)^{1/2\alpha+o(1)} + L_p\left(\frac{1}{2},1\right)^{\alpha/2}, \quad \text{for } p \longrightarrow \infty, \tag{4.3}$$

which suggests that for the optimal choice of w we have

$$w = L_p\left(\frac{1}{2},1\right), \qquad \frac{L_w(2/3,c)}{f(w)} = L_p\left(\frac{1}{2},1\right)^{1+o(1)}, \quad \text{for } p \longrightarrow \infty. \tag{4.4}$$

These arguments lead to the following conjectural running time estimation for solving the discrete logarithm problem on elliptic curve of form (1.1) over prime field.

Theorem 4.1. *There is a function $K : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ with*

$$K(x) = L_x\left(\frac{1}{2}, 1+o(1)\right) \quad \textit{for } x \longrightarrow \infty \tag{4.5}$$

such that the following assertion is true. Let p be a prime number that is not 2 or 3. Then, we can find the discrete logarithm of Montgomery elliptic curve over prime filed $\mathbb{F}_p$ within time $O(K(p)M(p))$.

Acknowledgments

One of the authors gratefully acknowledges the helpful comments and suggestions of the anonymous reviewers, which have improved the presentation. This work was supported by NSFC project under (Grant no. 60873041), Nature Science of Shandong Province (Grant no. Y2008G23), Doctoral Fund of Ministry of Education of China (Grant no. 20090131120012), and IIFSDU (Grant no. 2010ST075).

References

[1] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of eliminating errors in cryptographic computations," *Journal of Cryptology*, vol. 14, no. 2, pp. 101–119, 2001.

[2] I. Biehl, B. Meyer, and V. Müller, "Differential fault attacks on elliptic curve cryptosystems," in *Advances in Cryptology—CRYPTO 2000*, vol. 1880 of *Lecture Notes in Computer Science*, pp. 131–146, Springer, Berlin, Germany, 2000.

[3] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[4] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO '86*, vol. 263 of *Lecture Notes in Computer Science*, pp. 417–426, Springer, Berlin, Germany, 1987.

[5] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 14, no. 1, pp. 197–272, 1941.

[6] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 106–110, 1978.

[7] B. J. Birch, "How the number of points of an elliptic curve over a fixed prime field varies," *Journal of the London Mathematical Society, Second Series*, vol. 43, pp. 57–60, 1968.

[8] R. Schoof, "Nonsingular plane cubic curves over finite fields," *Journal of Combinatorial Theory, Series A*, vol. 46, no. 2, pp. 183–211, 1987.

[9] W. C. Waterhouse, "Abelian varieties over finite fields," *Annales Scientifiques de l'École Normale Supérieure, Quatrième Série*, vol. 2, pp. 521–560, 1969.

[10] H. W. Lenstra, Jr., "Factoring integers with elliptic curves," *Annals of Mathematics, Second Series*, vol. 126, no. 3, pp. 649–673, 1987.

[11] H. W. Lenstra, Jr., J. Pila, and C. Pomerance, "A hyperelliptic smoothness test. I," *Philosophical Transactions of the Royal Society of London A*, vol. 345, no. 1676, pp. 397–408, 1993.

[12] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Mathematics of Computation*, vol. 44, no. 170, pp. 483–494, 1985.

[13] E. R. Canfield, P. Erdős, and C. Pomerance, "On a problem of Oppenheim concerning "factorisatio numerorum"," *Journal of Number Theory*, vol. 17, no. 1, pp. 1–28, 1983.