# The Fault Attack ECDLP Revisited *

Mingqiang Wang[1] 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**

Biehl et al.[2] 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 in [9].

**Keywords:** Discrete logarithm; Subexponential; Smooth integer; Kroneck class number.

**Mathematics Subject Classification 2000:** 11G20

## 1 Introduction

In 1996 a fault analysis attack was introduced by Boneh et al. [3]. Biehl et al.[2] proposed the first fault-based attack on elliptic curve cryptography [8, 12]. 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,

*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).

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 maybe 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 $\mathbb{F}_p$

$$y^2 = x^3 + Ax^2 + B, \tag{1}$$

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). 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). If a reasonable conjecture concerning the density of smooth integers is assumed, then the following can be proved.

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. 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) 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 repeating Algorithm 2.

The paper is organized as follows. In Section 2, we describe the scalar multiplication algorithm, 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). In section 4, the efficiency of the attack algorithm is considered.

# 2 Preliminaries

## 2.1 Scalar Multiplication Algorithm

An elliptic curve $E$ can be defined as following equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and $P_i =: (x_i, y_i) \in E(\mathbb{F}_p)$, $i = 1, 2, 3$, 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.

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - A - x_1 - x_2 \\ y_3 &= -y_1 - (x_3 - x_1)\lambda - a_1x_3 - a_3 \end{aligned}$$

with

$$\lambda = \begin{cases} \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3} & \text{if } x_1 = x_2 \text{ and } y_1 = y_2, \\ \frac{y_1-y_2}{x_1-x_2} & \text{otherwise.} \end{cases}$$

The fault attack is based on the fact that the curve coefficient $a_6$ 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 [15] 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 $p_i < p_{i+1}$.

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

## 2.3 Fault attack

In this section, we consider the following EC EIGamal cryptosystem. Let $E_{A,B}$ be an elliptic curve of form (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 $1 \leq k < ord(P)$ the secret key of some user.

**Algorithm 1** Silver-Pohlig-Hellmans algorithm for solving the ECDLP

**Input:** $P \in E(\mathbb{F}_p)$, $Q \in \langle P \rangle$, $n = \prod_{i=0}^{j-1} p_i^{e_i}$, where $p_i < p_{i+1}$.
**Output:** $k \bmod n$.

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 $k \equiv k_i \bmod p_i^{e_i}$.
   This gives us $k \bmod n$
3. Return $(k)$

**Encryption:** Input message $m$, choose $1 < d < ord(P)$ randomly, return $(dP, x_{dQ} \bigoplus m)$.

**Decryption:** Input $(H, m')$, compute $kH$ , return $(m' \bigoplus x_{kH})$.

The fault attack is that the attacker randomly choose an elliptic curve $E_{A,\widehat{B}}$ defined over prime field $\mathbb{F}_p$, find a point $\widehat{P} = (x_{\widehat{P}}, y_{\widehat{P}}) \in E_{A,\widehat{B}}(\mathbb{F}_p)$ and input $(d\widehat{P}, m')$ 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

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

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

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

Let $E_{A,\widehat{B}}$ be an elliptic curve of form (1) as follows:

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

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 $n = ord(d\widehat{P})$. 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 $k \bmod n$. The following Lemma is useful for us to increase the efficiency of Algorithm 2.

**Algorithm 2** Basic fault attack on ECSM algorithm

**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 $\widehat{B} \leftarrow y_{\widehat{P}}^2 - x_{\widehat{P}}^3 - Ax_{\widehat{P}}^2$.
2. $\widehat{P} \leftarrow (x_{\widehat{P}}, y_{\widehat{P}})$.
   2.1 Obtain $n = ord(\widehat{P})$ in elliptic curve $E_{A,\widehat{B}}(\mathbb{F}_p)$.
   2.2 choose an integer $1 < d < ord(\widehat{P})$, compute $d\widehat{P}$.
3. Apply decryption oracle to compute $x_{kd\widehat{P}}$.
   3.1 $y_{kd\widehat{P}} \leftarrow \sqrt{x_{kd\widehat{P}}^3 + Ax_{kd\widehat{P}}^2 + \widehat{B}}$.
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 $k \bmod n$.
5. Return $(k \bmod n)$

**Lemma 1** *Let $E$ be an elliptic curve defined over finite filed $\mathbb{F}_q$. Then*

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

*with $n_1 | n_2$ and $n_1 | q - 1$.*

For given 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 $ord(\widehat{P}) = n_2$. 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 $w$. In step 2.2, we can choose $d$ satisfying $n_2' | d$ 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 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) defined over a prime field $\mathbb{F}_p$.

It is easy to see that the discriminant $\triangle$ and the $j$ invariant of the formula (1) equal to $4A^3 + 27B$ and $-\frac{16^2A^6}{4A^3B+27B^2}$ respectively. Hence the number of elliptic curve over prime field $\mathbb{F}_p$ with $B$ fixed is the number of $A \in \mathbb{F}_p$ with $4A^3 + 27B \neq 0$. Let $T$ be the number of the solutions of the following equation in $\mathbb{F}_p$

$$x^3 + \frac{27}{4}B = 0.$$

It is easy to see that

$$T = \begin{cases} 0 \text{ or } 3, & \text{if } p \equiv 1(\text{mod}3), \\ 1, & \text{if } p \equiv -1(\text{mod}3). \end{cases}$$

Hence we conclude that the number of elliptic curves over $\mathbb{F}_p$ with $B$ fixed equals to $p - T$.

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

$$\begin{cases} \overline{x} &= u^2 x + r, \\ \overline{y} &= u^3 y + u^2 s x + t, \end{cases}$$

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 exists $u \in \mathbb{F}_p^*, r \in \mathbb{F}_p$ such that the following conditions hold:
(i) $u^6 = 1$ and $A = Au^4 + 3u^4 r$;
(ii) $3u^2 r^2 + 2u^2 rA = 0$, and $Ar^2 + r^3 + \widehat{B} = B$.
Let $T'$ denote the solutions of (i) and (ii), it is easy to see that $T' \leq 12$. For any $p \neq 2, 3$, the automorphism of these elliptic curves is at most 3. Hence we have

$$\sum\nolimits'_{E_{A,\widehat{B}}} \frac{1}{\sharp Aut(E_{A,\widehat{B}})} \geq \frac{p - T}{12},$$

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

$$\sharp'\{E_{A,\widehat{B}} : E_{A,\widehat{B}} \text{ elliptic curve of form (1) with } \widehat{B} \in \mathbb{F}_p\}/\cong_{\mathbb{F}_p}$$

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

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

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

which is obtained by a theorem of Hasse. Let, conversely, $p$ be a prime $> 3$ and $t$ be an integer satisfying $|t| \leq 2\sqrt{p}$. 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[1, 17, 22]:

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

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

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

**Lemma 2** *[9] 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*

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

*for all* $\Delta \in \mathbb{Z}$ *with* $-z \leq \Delta < 0$, $\Delta \equiv 0, \text{or } 1 \bmod 4$,*except that the left inequality may be invalid if* $\Delta_0 = \Delta^*$, *where* $\Delta_0$ *is the unique number related to* $\Delta$.

Let

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

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

$$S^p_{QR} = \{\widehat{B} : \widehat{B} \in \mathbb{F}_p, \text{ and } x^3_{\widehat{P}} + Ax^2_{\widehat{P}} + \widehat{B} \text{ is a quadratic residue in } \mathbb{F}_p\},$$

$$S^p_{QNR} = \{\widehat{B} : \widehat{B} \in \mathbb{F}_p, \text{ and } x^3_{\widehat{P}} + Ax^2_{\widehat{P}} + \widehat{B} \text{ is a quadratic nonresidue in } \mathbb{F}_p\}.$$

Since $H_t \leq H(t^2 - 4p)$, Lemma 1 can not be applied directly in the following estimation. In order to apply Lemma 1, $S^p_{QR}$ should be partitioned into two parts $S^p_{QR1}$ and $S^p_{QR2}$ as follows

$$S^p_{QR1} = \{\widehat{B} : \widehat{B} \in S^p_{QR}, \sharp E_{A,\widehat{B}}(\mathbb{F}_p) = p + 1 - t, \text{ with } H_t \geq \frac{\sqrt{p}}{\log p}\},$$

$$S^p_{QR2} = \{\widehat{B} : \widehat{B} \in S^p_{QR}, \sharp E_{A,\widehat{B}}(\mathbb{F}_p) = p + 1 - t, \text{ with } H_t < \frac{\sqrt{p}}{\log p}\}.$$

Let

$$T^p_{QR1} = \{s : s \in \mathbb{Z}, \text{and there exists } \widehat{B} \in S^p_{QR1} \text{ such that } s = \sharp E_{A,\widehat{B}}(\mathbb{F}_p)\}.$$

**Theorem 1** *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* $s \in T^p_{QR1}$ *with*

$$|s - (p + 1)| \leq \sqrt{p},$$

*then*

$$\{E_{A,\widehat{B}} : \widehat{B} \in S^p_{QR1}, \sharp E_{A,\widehat{B}}(\mathbb{F}_p) \in S\} \cong_{\mathbb{F}_p} \geq c_3(\sharp S - 2)\frac{\sqrt{p}}{\log p}.$$

**Proof**. The proof of Theorem 2 is similar to the proof of (1.9) in [9], for self-contained, we give it here. The left hand side of the inequality equals

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

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

$$X^2 - tX + p$$

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 $\alpha$ up to conjugation and sign. Hence $t = \alpha + \overline{\alpha}$ is determined up to sign, as required. This completes the proof.

**Theorem 2** *There is a positive effectively computable constant $c_4$ such that for each prime number $p > 3$, the following assertion is valid. If $S$ is a set of integers $s \in T^p_{QR1}$ with*

$$|s - (p+1)| \leq \sqrt{p},$$

*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*

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

*where $x^3_{\widehat{P}} + Ax^2_{\widehat{P}} + \widehat{B} = y^2_{\widehat{P}}$, is at least $c_4(\sharp S - 2)\frac{\sqrt{p}^3}{\log p}$.*

**Proof.** The number to be estimated equals the number of double-tuples $(\widehat{B}, y_{\widehat{P}}) \in \mathbb{F}_p^2$ 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 $T'/\sharp AutE$, where $\overline{A} \in \mathbb{F}_p$. Each $E_{A,\widehat{B}}$ exactly gives rise to two points $(x_{\widehat{P}}, y_{\widehat{P}})$. Thus the number to be estimated equals

$$\sum\nolimits'_{E_{A,\widehat{B}}} \frac{2T'}{\sharp Aut(E_{A,\widehat{B}})},$$

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 2, we obtain the result.

**Theorem 3** *There exists a positive effectively computable constant $c_5$. Let*

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

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

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

*where $x^3_{\widehat{P}} + Ax^2_{\widehat{P}} + \widehat{B} = y^2_{\widehat{P}}$, is at least $c_5(\sharp S_w - 2)\frac{\sqrt{p}^3}{\log p}$.*

**Proof.** This can be deduced form Theorem 2 immediately.

**Theorem 4** *There exists a positive effectively computable constant $c_6$. The cardinality of $T^p_{QR1}$ is at least $c_6 \frac{\sqrt{p}}{\log p(\log\log p)}$.*

**Proof.** Since the map

$$\phi : \mathbb{F}_p \mapsto \mathbb{F}_p, \widehat{B} \mapsto x^3_{\widehat{P}} + Ax^2_{\widehat{P}} + \widehat{B}$$

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

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

Therefore, the cardinality of $S^p_{QR1}$ is

$$S^p_{QR} - S^p_{QR2} \geq p - 2\frac{p}{\log p}.$$

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

$$\sharp T^p_{QR1} \geq \frac{\sharp S^p_{QR1} - T}{H(\Delta)}.$$

Applying Lemma 1, we get the proof of the result.

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

**Heuristic assumption:** *The set $T^p_{QR1}$ is uniform distribution in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$.*

By the assumption, one can deduce that $\sharp T^p_{QR1} \approx 2\sharp T_1$.

**Theorem 5** *There exists an effectively computable constant $c_7 > 1$ with the following property. Let $w \in \mathbb{Z}_{>1}$ and*

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

*Let $f(w) = \frac{\sharp S_w}{\sharp T_1}$ 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 repeating Algorithm 2.*

**Proof.** By Theorem 4, the failure probability of repeating Algorithm 2 $h$ times equals $(1 - N/p^2)^h$, where

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

It follows that

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

Consequently, the desired result can be obtained here.

# 4 Efficiency

In the case of factoring, the best rigorously analyzed result is Corollary 1.2 of [10], 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 [18] presents a deterministic algorithm to compute the number of $\mathbb{F}_p$-points of an elliptic curve that is defined over a finite field $\mathbb{F}_p$ takes $O(\log^9 p)$ elementary operations.

Theorem 5 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 5, 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, Erdös and Pomerance [4] implies the following result. Let $\alpha$ 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

$$f(L_p(1/2, 1)^\alpha) = L_p(1/2, 1)^{-1/2\alpha+o(1)} \quad \text{for } p \to \infty,$$

for any fixed positive $\alpha$, with $f(w) = \frac{\sharp S_w}{\sharp T_1}$.

The following identities are useful for our estimation.

$$L_p(\alpha, c_\alpha)L_p(\beta, c_\beta) = L_p(\max\{\alpha, \beta\}, c_{\max\{\alpha,\beta\}}),$$

$$L_{L_p(\alpha,c_\alpha)}(\beta, c_\beta) = L_p(\alpha\beta, c_\beta c_\alpha^\beta),$$

where lower order terms in the exponent are neglected.

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

$$L_w(2/3, c)/f(w) + \sqrt{w} = L_p(1/2, 1)^{1/2\alpha+o(1)} + L_p(1/2, 1)^{\alpha/2}, \quad \text{for } \ p \to \infty,$$

which suggests that for the optimal choice of $w$ we have

$$w = L_p(1/2, 1), \quad L_w(2/3, c)/f(w) = L_p(1/2, 1)^{1+o(1)}, \quad \text{for } \ p \to \infty.$$

These arguments lead to the following conjectural running time estimation for solving the discrete logarithm problem on elliptic curve of form (1) over prime field.

**Theorem 6** *There is a function* $K : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ *with*

$$K(x) = L_x(1/2, 1 + o(1)) \quad \text{for } x \to \infty$$

*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* $O(K(p)M(p))$*.*

# References


[1] 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.

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

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

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

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

[6] 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.

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

[8] N.Koblitz, Elliptic curve cryptosystems. Math. Comp., Vol. 48, No.177(1987), 203-209.

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

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

[11] 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.

[12] V. Miller, Use of elliptic curves in cryptography. In CRYPTO 86, Lecture Notes in Comput. Sci. 263, (1987), 417-426.

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

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

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

[16] 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.

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

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

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

[20] 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.

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

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