International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 11, Number 2, pages 231–250, July 2021

Sophisticated analysis of a method to eliminate fruitless cycles for Pollard's rho method with skew Frobenius mapping over a Barreto-Naehrig curve

Hiromasa Miura, Syota Kanzawa, Rikuya Matsumura,
Yuta Kodera, Takuya Kusaka, Yasuyuki Nogami

Graduate School of Natural Science and Technology, Okayama University,
3-1-1 Tsushima-naka, Kita-ku, Okayama-city, 700-8530, Japan

Received: February 15, 2021
Revised: April 23, 2021
Accepted: June 2, 2021
Communicated by Toru Nakanishi

Abstract

In this paper, the authors focus on and propose an approach to attack a kind of pairing-friendly curves, the Barreto-Naehring (BN) curve, to accelerate the evaluation of the security level concerning the elliptic curve discrete logarithm problem (ECDLP). More precisely, this paper targets the BN curve, which is known to be a pairing-friendly curve, and Pollard's rho method based on the random-walk is adopted to attack the curve.

Though Pollard's rho method with skew Frobenius mapping is known to solve the ECDLP efficiently, this approach sometimes induces the unsolvable cycle, called the fruitless cycle, and such trials must restart with a different starting point. However, any effective method to eliminate such fruitless cycles has not been proposed. Therefore, the authors focus and give the sophisticated analysis to propose an effective approach to eliminate such cycles to optimize Pollard's rho method furthermore. In addition, we confirm the effectiveness of the method by applying it to a BN curve with 12, 17, and 33-bit parameters.

Keywords: ECDLP, Pollard's rho method, fruitless cycle, Barreto-Naehrig curve, skew Frobenius mapping

1 Introduction

The IoT era has arrived, and many IoT devices are connected to the Internet. IoT devices with few computing resources are required to have a safe, secure, and high-speed encryption system. Currently, though RSA encryption is widely used as a public-key cryptosystem, it requires more than 2000 bits length of a key. However, it is not always available for every IoT device due to the lack of computational resources. Therefore, elliptic curve cryptography (ECC) capable of ensuring security equivalent to that of the RSA cipher with a key length of 3072 bits at about 256 bits has attracted attention and studied. ECC is used as digital signatures and authentication technology in various things such as IC cards, server certificates, and Wi-Fi. The security of elliptic curve cryptography is guaranteed by the elliptic curve discrete logarithm problem (ECDLP).

Pairing-based cryptography enables many innovative and multi-function cryptographic applications such as ID-based encryption [1] and searchable encryption [2]. The authors focus on the BN curve used in pairing-based cryptography. One of the securities of pairing-based cryptography is guaranteed by ECDLP. If ECDLP is solved, the security of the pairing-based cryptography needs to be re-verified. Since the method of solving DLP has been improved[3], the length of the secret key is affected when the BN curve is used in pairing-based cryptography.

Pollard's rho method, simply, rho method, is one of the most efficient methods for solving ECDLP [4] and a variety of efficient rho methods are studied [5, 6, 7, 8, 9].

Skew Frobenius mapping can be applied to the rho method to decrease the solving time of ECDLP for the BN curve. In [8], Miura et al. showed that a rho method with the skew Frobenius mapping toward 9-bit ECDLP induces the increasing number of unsolvable cases called fruitless cycles rapidly. When a random-walk path results in a fruitless cycle, the random-walk path must restart with a different starting point. Though the cost to detect a fruitless cycle and restart the random-walk path is not large if the length of the fruitless cycle is short, the terminated random-walk path is a waste of resources of the attack. In addition, the results of [8] indicate that the probability of the restarted random-walk path results in yet another fruitless cycle can be a non-negligible problem for the rho method with skew Frobenius mapping. Therefore, combined with the restarting method, a method to reduce the occurrence of the fruitless cycles brings non-negligible benefits for the attackers, if the cost of the method is small enough. Note that, about 6 months were required to solve a 114-bit ECDLP even if 2000 cores were used[6]. Since the elimination of the fruitless cycles might result in a shorter attack time for the same setup, the fruitless cycles should be avoided.

In this paper, the authors show that the fruitless cycle increases rapidly in the rho method with skew Frobenius mapping over a BN curve with 12-bit parameters. In addition, a method to eliminate the fruitless cycles is proposed and applied to 12, 17, and 33-bit parameters. In this paper, the authors mainly employ rho methods consist of a single random-walk path to clarify the situation and structure of the fruitless cycles. Since the single path rho methods are not typical parallel rho methods with restarting methods, the major purpose of this paper is not the evaluation on the effectiveness of the proposed method with the parallel rho methods. Note that the authors assume that any practical implementations of parallel rho methods should employ the restarting methods for a random-walk path saturated with a fruitless cycle.

2 Mathematical fundamentals

The BN curve is one of the elliptic curves and is an elliptic curve defined on a finite field or an algebraic number field. In this chapter, we review the four arithmetic operations in these algebraic systems and describe the mathematical foundations of elliptic curves.

2.1 Group

A group $(\mathbb{G}, \circ)$ is a non-empty set together with a binary operation $\circ$ that satisfies the following group axioms:

G1: For $\forall a, b \in \mathbb{G}$, the result of $a \circ b$ is also in $\mathbb{G}$. (Closure)

G2: For $\forall a, b, c \in \mathbb{G}$, $(a \circ b) \circ c = a \circ (b \circ c)$. (Associativity)

G3: For $\forall a \in \mathbb{G}$, there exists an element $e \in \mathbb{G}$ such that $a \circ e = e \circ a = a$, where e is called unity. (Existence of unity)

G4: For $\forall a \in \mathbb{G}$, there exists an element $x \in \mathbb{G}$ such that $a \circ x = x \circ a = e$, where x is called inverse element. (Existence of inverse element)

In addition, $(\mathbb{G}, \circ)$ is said to be commutative group or abelian group when $(\mathbb{G}, \circ)$ satisfies the following property:

AG5: For $\forall a, b \in \mathbb{G}$, $a \circ b = b \circ a$. (Commutativity)

The order of a group $(\mathbb{G}, \circ)$ is defined as the number of elements in $\mathbb{G}$ and it is denoted by $|\mathbb{G}|$.

For a positive integer n, let $(Z_n, +)$ be a group with respect to an addition, where $Z_n = \{0, 1, 2, \ldots, n-1\}$. If addition $+$ is a normal integer addition, then **G1(Closure)** does not be fulfilled. Therefore, this paper adopts an addition with modular arithmetic defined below.

$$a + b \equiv c \pmod{n}, a, b \in Z_n,$$

where the notation "$c \pmod{n}$" means that c is assigned to a remainder on division by n when $a + b = c$ exceeds n. Then, c always belongs to Z_n and $(Z_n, +)$ forms a group. For simplicity, both addition and multiplication with modular arithmetic are represented as usual expressions such as $+$ and $\cdot$.

2.1.1 Field

A field $(\mathbb{F}, +, \cdot)$ has two operations denoted by $+$ and $\cdot$ such that:

F1: $\mathbb{F}$ is a commutative group with respect to $+$. (Additive Group)

F2: $\mathbb{F}^*$ is a group with respect to $\cdot$, where $\mathbb{F}^*$ is the set that consists of every element distinct from the unity (zero element) with respect to $+$. (Multiplicative Group)

F3: For all $a, b, c \in \mathbb{F}$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$. (Distributive law)

In general, the element 0 and 1 represent the unity concerning $+$ and $\cdot$, respectively. The order of $\mathbb{F}$ is the number of elements in $\mathbb{F}$. If the order of $\mathbb{F}$ is finite, $\mathbb{F}$ is called finite field.

2.1.2 Prime field

Let $(\mathbb{F}, +, \cdot)$ be a field and $(\mathbb{K}, +, \cdot)$ be a subfield of $(\mathbb{F}, +, \cdot)$. If $\mathbb{K} \neq \mathbb{F}$, then $(\mathbb{K}, +, \cdot)$ is a proper subfield of $(\mathbb{F}, +, \cdot)$. Prime field is defined as a field with no proper subfields. In other words, if $(\mathbb{K}, +, \cdot)$ does not have any subfields except itself, then $(\mathbb{K}, +, \cdot)$ is called prime field.

For example, $(Z_p, +, \cdot)$ is a prime field and in what follows, it is denoted by $\mathbb{F}_p$. This paper especially focuses on a prime field with an odd prime number p where the field is called an odd characteristic field.

2.2 Extension field

A field $\mathbb{F}$ is said to be an extension field of a field $\mathbb{F}'$, if $\mathbb{F}'$ be a subfield of $\mathbb{F}$. In addition, the unity exists in $\mathbb{F}'$. Let p be a large prime number and m a relatively small positive integer called extension degree. An extension field $\mathbb{F}_{p^m}$ is a vector space over prime field $\mathbb{F}_p$ in which arithmetic operations such as multiplication for $a, b \in \mathbb{F}_p$ are carried out with modulo p such as $a \times b \pmod{p}$. In order to deal with the extension field $\mathbb{F}_{p^m}$ as a vector space over $\mathbb{F}_p$, a certain basis of dimension m be denoted as $(e_1, e_2, \ldots, e_m)$ is needed. Then, arbitrary element $A \in \mathbb{F}_{p^m}$ is represented as a vector as follows,

$$A = (a_1e_1, a_2e_2, \ldots, a_me_m) \quad a_1, a_2, \ldots, a_m \in \mathbb{F}_p. \tag{1}$$

2.3 l-th power residue

For $a \neq 0 \in \mathbb{F}_p$, when there exists an element $x \in \mathbb{F}_p$ such that $x^l = a \pmod{p}$, a is called a l-th power residue. On the other hand, when there does not exist an element $x \in \mathbb{F}_p$ such that $x^l = a \pmod{p}$, a is called a l-th power non-residue. More Formally, we say that a is l-th power residue when $a^{\frac{p-1}{l}} \pmod{p} = 1$. Otherwise, a is l-th power non-residue.

In this paper, the case of $l = 2$ and $l = 3$ are described.

- $l = 2$
  In this case, an element a is called a quadratic residue(QR) element if a has a square root in $\mathbb{F}_p$, a quadratic non-residue(QNR) element in $\mathbb{F}_p$ otherwise.

$$a^{\frac{p-1}{2}} \pmod{p} = \begin{cases} 1, & \text{if } a \text{ is QR,} \\ -1, & \text{if } a \text{ is QNR,} \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

  This discriminant is widely known as the Legendre symbol$(a/p) = a^{\frac{p-1}{2}}$.

- $l = 3$
  In this case, an element a is called a cubic residue(CR) element if a has a cubic root in $\mathbb{F}_p$, a cubic non-residue(CNR) element in $\mathbb{F}_p$ otherwise.

$$a^{\frac{p-1}{3}} \pmod{p} = \begin{cases} 1, & \text{if } a \text{ is CR,} \\ \epsilon, \epsilon^2, & \text{if } a \text{ is CNR,} \\ 0, & \text{otherwise,} \end{cases} \tag{3}$$

  where ϵ is a primitive cubic root of unity.

3 Elliptic curve and ECDLP

In this section, we review the definition of an elliptic curve over a prime field and the fundamental property of rational points on the curve. In addition, a brief review of the rho method with the skew Frobenius mapping is given.

3.1 BN curve

BN curve [10] is a class of non-supersingular pairing friendly elliptic curve whose embedding degree is 12. For a prime p, a BN curve is defined over $\mathbb{F}_q$ where $q = p^{12}$. For simplicity, a BN curve E can be defined over $\mathbb{F}_p$ where

$$E : y^2 = x^3 + b \quad (b \neq 0 \in \mathbb{F}_p \text{ and } x, y \in \mathbb{F}_p). \tag{4}$$

$\mathbb{F}_p$ is a field of prime order p. It is noted that for a certain integer χ, integers p and r is given by

$$p = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1, \tag{5}$$

$$r = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1.$$

Let $E(\mathbb{F}_p)$ be the set of rational points including the point at infinity which is denoted by $\mathcal{O}$. Then, we have $r = |E(\mathbb{F}_p)|$ and $E(\mathbb{F}_p)$ forms an additive cyclic group.

For two rational points $Q_1(x_1, y_1)$ and $Q_2(x_2, y_2) \in E(\mathbb{F}_p)$, an addition between the rational points $Q_1(x_1, y_1) + Q_2(x_2, y_2) = Q_3(x_3, y_3) \in E(\mathbb{F}_p)$ is called an Elliptic Curve Addition (ECA). For Q_1 and Q_2, we have an auxiliary parameter λ defined by

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } Q_1 \neq Q_2 \text{ and } x_1 \neq x_2, \\ \frac{3x_1^2}{2y_1}, & \text{else if} Q_1 = Q_2 \text{ and } y_1 \neq 0, \\ 0, & \text{otherwise.} \end{cases}$$

Then, ECA gives x_3 and y_3 with $\lambda \neq 0$ as follows:

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = (x_1 - x_3)\lambda - y_1.$$

On the other hand, if $\lambda = 0$, then we have

$$Q_3 = \mathcal{O}.$$

For two rational points P and Q, and an integer $s \in Z_r$, let $[s]P$ denote $s - 1$ times ECA on P where

$$Q = [s]P = \underbrace{P + P + \cdots + P}_{s}.$$

Note that for the case $s = 0$, we have $[s]P = \mathcal{O}$.

The basic idea of the elliptic curve discrete logarithm problem (ECDLP) is to find a scalar s such that $Q = [s]P$ from given rational points P and Q.

Generally, computing Q from s and P is relatively easy owing to the ECA, however, the inverse is considered to be hard for an adequate bit size in most cases. In this sense, the robustness and hardness against computational attack for an ECDLP are essential aspects of ECC security.

3.2 Skew Frobenius mapping

As a kind of endomorphisms, skew Frobenius endomorphism is known [11]. For a rational point $R(x, y)$, the skew Frobenius mapping ϕ is defined as follows:

$$\phi(R) = \left(v^{\frac{p^2-1}{3}} x, v^{\frac{p^2-1}{2}} y \right),$$

where v is a quadratic and cubic non-residue in $\mathbb{F}_{p^2}$. In this case, we have $\phi(R)^6 = \phi$, and $v^{\frac{p^2-1}{3}}$ becomes a primitive cubic root ϵ of unity in $\mathbb{F}_p$, and $v^{\frac{p^2-1}{2}}$ becomes $p - 1$. Thus, in what follows, the skew Frobenius map ϕ in this case is denoted by ϕ_6. Then, ϕ_6 enables an efficient grouping in the rho method as shown in the next section.

3.3 Grouping of six points on BN curve

Let us consider a rational point T_i as generated in the random-walk process. Then, the rational points obtained in the random-walk are found to be corresponding to the following six rational points via skew Frobenius mapping ϕ.

$$\phi_6^0(T_i) = (x_i, y_i), \tag{6a}$$
$$\phi_6^1(T_i) = (\epsilon x_i, -y_i), \tag{6b}$$
$$\phi_6^2(T_i) = (\epsilon^2 x_i, y_i), \tag{6c}$$
$$\phi_6^3(T_i) = (x_i, -y_i), \tag{6d}$$
$$\phi_6^4(T_i) = (\epsilon x_i, y_i), \tag{6e}$$
$$\phi_6^5(T_i) = (\epsilon^2 x_i, -y_i). \tag{6f}$$

A set of the six points forms an equivalent class. Then, a certain representative point among the six points is systematically and efficiently determined, which enables the following efficient grouping attack. When $T_j = [\alpha_j]P + [\beta_j]Q$ is $\phi_6^t(T_i)$ where $0 \leq t < 6$, α_j and β_j are given as follows:

$$\alpha_j = p^{2t} \cdot \alpha_i, \ \beta_j = p^{2t} \cdot \beta_i \pmod{r}.$$

For a rational point T_i, let $Rep(T_i)$ be a function that determines the representative element from Eq.(6). The rational point obtained by the function $Rep(T_i)$ is called the representative point. For example, the representative point $Rep(T_i)$ is a rational point with the maximum x coordinate and even y coordinate in the group of the six points.

Figure 1: Illustration of a random-walk in Pollard's rho method

4 Pollard's rho method

In this chapter, Pollard's rho method and Pollard's rho method with the skew Frobenius mapping are described. A typical rho method is used for parallel attacks using one server and many clients. Generally, though one of the simplest methods requires the server to save numerous points sent from the clients, here we also review a typical distinguished point method to reduce the burden of the server.

4.1 Normal Pollard's rho method

Pollard's rho method is one of the most efficient methods for solving ECDLP [4]. The seed points are a set of rational points that are used to generate new rational points in a random-walk path.

The algorithm of the rho method is illustrated in Algorithm 1. Let n denote the number of seed points. For an integer i where $0 \leq i < n$ and two random scalars α_i and $\beta_i \in Z_r$, let $T_i \triangleq [\alpha_i]P+[\beta_i]Q$ denote the seed points. Note that Z_r is a set of integers greater than or equal to 0 and less than r. For a rational point $P(x', y')$, let $\eta(P(x', y')) = x' \mod n$. The procedure of iterations from steps 6 to 11 form a random-walk, and step 10 is for collision detection. When β_i is equal to β_j in step 12, the random-walk cannot be solved. This case is called a fruitless cycle. In most cases, a client does not save rational points for a solvable collision detection. Thus, the fruitless cycle cannot be detected on the client-side and a random-walk on the client side must restart from selecting starting point after detecting the fruitless cycle by the server with parameters concerning rational points. Note that for short length fruitless cycles, local collision detection methods can be employed on the client for practical parallel rho methods.

The fruitless cycles are obviously redundant for attacking and evaluating the robustness of the ECDLP using parallel rho methods. In this context, the authors propose a method to eliminate those fruitless cycles through a sophisticated analysis to conducting the parallel rho methods more efficiently.

In addition, the number of repeats in steps 6-11 in Algorithm 1 is called the random-walk length. By using a random-walk length, comparisons can be made regardless of the performance of a device. On the other hand, it is known from the birthday paradox[12] that the rho method has a collision probability of 50% when $\sqrt{\pi r/2}$ points are generated. Therefore, the authors compare the random-walk length and the estimation based on the birthday paradox. The performance of a rho method would be evaluated by average length of the random-walk path when the rho method stops with a solvable collision over enough number of trials, and the average length is a probable value.

Figure 1 illustrates the random-walk in a typical single rho method, and the shape of the random-walk resembles the symbol ρ as the name stand for. That is because the random-walk generates points randomly, and the rational points form a cyclic set, which is called a cycle. In Figure 1, $j - i$ is called the cycle length, and $i - n$ is called the foot length.

The random-walk shown in Figure 1 consists of a single staring point, a single foot and a single

Algorithm 1: Pollard's rho method

```
Input  : $P, Q(=[s]P) \in \mathrm{E}(\mathbb{F}_p)$ $(s \in Z_r)$.
Output: $s$.
for $i = 0$ to $n - 1$ do
    $\alpha_i, \beta_i$ are assigned two random elements in $Z_r$.
    $T_i \leftarrow [\alpha_i]P+[\beta_i]Q$.
$\alpha_n, \beta_n$ are assigned two random elements in $Z_r$.
$T_n \leftarrow [\alpha_n]P+[\beta_n]Q$.
for $i = n + 1$ to $r - 1$ do
    $l \leftarrow \eta(T_i)$.
    $\alpha_i \leftarrow \alpha_{i-1} + \alpha_l, \beta_i \leftarrow \beta_{i-1} + \beta_l$.
    $T_i \leftarrow T_{i-1} + T_l$.
    if $T_i = T_j (n \leq j < i)$ then
        go out this loop.
$s \leftarrow -(\alpha_i - \alpha_j)/(\beta_i - \beta_j)$.
```

cycle. In the case, the lengths of the foot and cycle are more than zero, respectively, the random-walk is translated as a single rho method. Note that a special case is a random-walk path consists of single cycle without a foot, which draws a shape of 'o' character. A typical parallel rho method consists of massive clients which consist of massive random-walk paths with different starting points and a collision detection server. In addition, a typical termination state of the parallel rho method is a solvable collision which is a joining point of two different feet from two starting points. Then, the two different random-walk paths draw a λ shape, which is not a ρ shape. Note that a special case is two random-walk paths share a single foot without a cycle.

There is a possibility that the parallel rho method includes several disconnected random-walk paths which draw standalone ρ shapes with unsolvable collisions, which are the fruitless cycles. In addition, there is a possibility that the two different random-walk paths, which include a solvable collision point, result in a fruitless cycle where the cycle can be confirmed by intentionally continuing the random-walks.

Therefore, in this paper, the authors mainly focus on the rho method which consists of single starting point to clarify the result of the cycle of the random-walk path. Note that since the length of the single rho method becomes longer than that of the parallel rho methods, the efficiency of the ECDLP could not be evaluated by the average length of the random-walk path of the single rho method.

4.2 Pollard's rho method with the skew Frobenius mapping

In this section, Pollard's rho method with the skew Frobenius mapping is explained. In this paper, this method is also referred to as the previous method [6].

Except the fruitless cycle cases, the normal rho method can solve ECDLP when the same rational point is generated from the rational points on the curve. The search range is equal to the order r of the curve. By applying the skew Frobenius mapping, the rational points on the BN curve can be divided into groups of 6 points each. In this case, each client decides a representative point among the 6 points, and map to the representative point each time with much smaller computational cost than that of ECA. Therefore, a client sends only the representative points to the server, and the server makes collision detection using only the representative points. It immediately enables us to shrink the search range into $r/6$, and the average length of the random-walk path with a solvable collision become shorter than that of the normal rho method on the average.

The algorithm of the previous method is illustrated in Algorithm 2. Same as the normal rho method, let n denote the number of seed points. For an integer i where $0 \leq i < n$ and two random scalars α_i and $\beta_i \in Z_r$, let $T_i \triangleq [\alpha_i]P + [\beta_i]Q$ denote the seed points. For a rational point $P(x', y')$,

Figure 2: Illustration of a random-walk in the previous method

Algorithm 2: Pollard's rho method with the skew Frobenius mapping

```
   Input  : $P, Q(=[s]P) \in \mathrm{E}(\mathbb{F}_p)$ $(s \in Z_r)$.
   Output: $s$.
1  for $i = 0$ to $n - 1$ do
2      $\alpha_i, \beta_i$ are assigned two random elements in $Z_r$.
3      $T_i \leftarrow [\alpha_i]P+[\beta_i]Q$.
4  $\alpha_n, \beta_n$ are assigned two random elements in $Z_r$.
5  $T_n \leftarrow [\alpha_n]P+[\beta_n]Q$.
6  $\overline{T}_n \leftarrow Rep(T_n)$.
7  $l \leftarrow \eta(\overline{T}_n)$.
8  for $i = n + 1$ to $r - 1$ do
9      $\alpha_i \leftarrow \alpha_{i-1} + \alpha_l, \beta_i \leftarrow \beta_{i-1} + \beta_l$.
10     $T_i \leftarrow \overline{T}_{i-1} + T_l$.
11     $\overline{T}_i \leftarrow Rep(T_i)$.
12     $l \leftarrow \eta(\overline{T}_i)$.
13     if $\overline{T}_i = \overline{T}_j (n \leq j < i)$ then
14         go out this loop.
15 $s \leftarrow -(p^{2t} \cdot \alpha_i - p^{2t'} \cdot \alpha_j)/(p^{2t} \cdot \beta_i - p^{2t'} \cdot \beta_j) \pmod r$, where $0 \leq t < 6$ and $0 \leq t' < 6$.
```

let $\eta(P(x', y')) = x' \mod n$. The procedure of iterations from steps 8 to 14 forms a random-walk, and step 13 is collision detection. Note that t and t' are integers between 0 and 5. Note that the major difference from the normal rho method is to employ representative points of rational points based on skew Frobenius mapping shown in steps 6 and 11 in Algorithm 2.

In addition, the number of repeats in steps 8-14 in Algorithm 2 is called the random-walk length. By using a random-walk length, comparisons can be made regardless of the performance of a device. On the other hand, it is known from the birthday paradox that the rho method with skew Frobenius mapping has a collision probability of 50% when $\sqrt{\pi r/12}$ points are generated. Therefore, the authors compare the random-walk length and the estimation based on the birthday paradox.

Figure 2 illustrates the random-walk of the previous method. In Figure 2, $j - i$ is called the cycle length, and $i - n$ is called the foot length. For a rational point T_{i-1} where $T_{i-1} \neq \mathcal{O}$, a cycle length zero is a case where $T_i = \mathcal{O}$. A cycle length one is a case where $T_{i-1} \neq \mathcal{O}$ and $T_{\eta(\overline{T}_{i-1})} = \mathcal{O}$.

For two rational points T_i and T_j where $Rep(T_i) = Rep(T_j)$ and $n \leq i < j \leq r$, we call the situation as a collision of the rho method applied the skew Frobenius mapping. For a collision where $p^{2t} \cdot \alpha_i \neq p^{2t'} \cdot \alpha_j$ and $p^{2t} \cdot \beta_i \neq p^{2t'} \cdot \beta_j$, the scalar s can be solved by the following:

$$s = -\frac{p^{2t} \cdot \alpha_i - p^{2t'} \cdot \alpha_j}{p^{2t} \cdot \beta_i - p^{2t'} \cdot \beta_j} \pmod r, \tag{7}$$

Figure 3: Illustration of a fruitless cycle by the distinguished point method

Figure 4: Illustration of a cycle of length two in the previous method

where $0 \leq t < 6$ and $0 \leq t' < 6$.

When the denominator is zero in Eq.(7), the scalar s cannot be obtained, and this cycle is also called a fruitless cycle.

4.3 Distinguished point

In practical rho methods, a distinguished point method might be employed to reduce the number of rational points to check a collision. For $\overline{T}_i(x_i, y_i)$, a typical distinguished point method checks whether lower bits of x_i equals zero or not. For a positive integer τ, let the lower τ bits of the distinguished point method be called thinned bits. In this research, since this is a preliminary study to solve larger bit ECDLP, the results where the distinguished point method is applied or not is verified.

In addition, a new fruitless cycle may occur by applying the distinguished point method. An example is shown in Figure 3. A red cross mark is drawn on rational points that do not meet the conditions of the distinguished point method. If all the rational points, which draw the cycle, do not satisfying the distinguished point method, then it results in a fruitless cycle. Detecting this fruitless cycle is synonymous with solving ECDLP. If the cycle length of the fruitless cycle is short, it can be detected by saving the rational points on the client, locally. However, most of the long fruitless cycles cannot be detected by the local collision detection. Therefore, the number of bits to be thinned out in the distinguished point method and the parameters of the BN curve or a rho method must be carefully selected.

Note that for the parallel rho methods, the new fruitless cycle can be a solvable cycle if the local collision detection on the client-side properly handles the collision. The experiments in Chapter 6 do not employ the local collision detection.

Table 1: The parameters of a BN curve and the value of χ

χ	The parameters of a BN curve		
	prime(p)	Order(r)	b in Eq.(4)
3	2143	2089	5
7	75223	74929	7
107	4675038223	4674969529	10

5 Reduction of fruitless cycles

In this chapter, the case of the fruitless cycle in the rho method with the skew Frobenius mapping[8] is reviewed. The authors propose a method to eliminate the fruitless cycles based on this review.

5.1 Review of the cause of the fruitless cycle

The authors review the cause of fruitless cycles, taking cycle length two which is the most frequent as an example.

Figure 4 shows the cycle of length two in the previous method. If rational points are calculated according to the previous method, $p^{2t_0} \cdot \alpha_i$ and $p^{2t_0} \cdot \beta_i$ can be expressed as follows:

$$\overline{T}_i = Rep(T_i) = \phi_6^{t_0}(T_i), \tag{8a}$$

$$T_{i+1} = \overline{T}_i + T_{\eta(\overline{T}_i)} = \phi_6^{t_0}(T_i) + T_{\eta(\overline{T}_i)}, \tag{8b}$$

$$\overline{T}_{i+1} = Rep(T_{i+1}) = \phi_6^{t_1}(T_{i+1}) = \phi_6^{t_1}(\overline{T}_i) + \phi_6^{t_1}(T_{\eta(\overline{T}_i)}), \tag{8c}$$

$$T_{i+2} = \overline{T}_{i+1} + T_{\eta(\overline{T}_{i+1})} = \phi_6^{t_1}(T_{i+1}) + T_{\eta(\overline{T}_{i+1})}, \tag{8d}$$

$$\begin{aligned}\overline{T}_{i+2} &= Rep(T_{i+2}) = \phi_6^{t_2}(T_{i+2}) = \phi_6^{t_2}(\overline{T}_{i+1}) + \phi_6^{t_2}(T_{\eta(\overline{T}_{i+1})}) \\ &= \phi_6^{t_2+t_1}(\overline{T}_i) + \phi_6^{t_2}(\phi_6^{t_1}(T_{\eta(\overline{T}_i)}) + T_{\eta(\overline{T}_{i+1})}),\end{aligned} \tag{8e}$$

where $0 \leq t_0, t_1, t_2, t_3 < 6$. When $\phi_6^{t_1}(T_{\eta(\overline{T}_i)}) + T_{\eta(\overline{T}_{i+1})} = \mathcal{O}$ where $\mathcal{O}= [0]P + [0]Q$ in Eq.(8e), the cycle becomes the fruitless cycle of length two. For example, the conditions of the fruitless cycle of length two are $t_1 = t_2 = 3$ and $T_{\eta(\overline{T}_{i+1})} = T_{\eta(\overline{T}_i)}$ because of $\phi_6^3(T_{\eta(\overline{T}_i)}) = -T_{\eta(\overline{T}_i)}$.

That is, it is possible to eliminate fruitless cycles by preventing to refer the same rational point in succession.

5.2 Method to eliminate the fruitless cycles

In the previous section, the authors showed that the fruitless cycles can be eliminated by not to refer to the same rational point in succession. Therefore, in this study, the authors propose a method that avoids continuous reference of seed points by dividing the set of seed points into two sets, and referencing the sets alternately.

The proposed method for ruling out fruitless cycles is illustrated in Algorithm 3. Let n be the number of seed points. For an integer i where $0 \leq i < n$ and two random scalars α_i and $\beta_i \in Z_r$, let $T_i \triangleq [\alpha_i]P + [\beta_i]Q$ denote the seed points.

The proposed method does not refer to the same rational points continuously. The condition to result in a fruitless cycle of length two is to refer to the same rational points continuously in each of the two seed point tables. In the previous method with one table, it takes at least two steps to result in a fruitless cycle on the random-walk. On the other hand, since the proposed method has two tables, it requires at least four steps to result in a fruitless cycle on the random-walk. The conditions to result in the fruitless cycle become severe and the fruitless cycle can be eliminated.

Algorithm 3: Proposed method for ruling out fruitless cycles

```
Input  : $P, Q(=[s]P) \in E(\mathbb{F}_p) \quad (s \in Z_r)$.
Output: $s$.
$n' = n/2$.
for $i = 0$ to $n - 1$ do
    $\alpha_i, \beta_i$ are assigned two random elements in $Z_r$.
    $T_i \leftarrow [\alpha_i]P + [\beta_i]Q$.
$\alpha_n, \beta_n$ are assigned two random elements in $Z_r$.
$T_n \leftarrow [\alpha_n]P + [\beta_n]Q$.
$\overline{T}_n \leftarrow Rep(T_n)$.
$l \leftarrow x \pmod{n'}$ where $\overline{T}_n(x, y)$.
for $i = n + 1$ to $r - 1$ do
    $\alpha_i \leftarrow \alpha_{i-1} + \alpha_l, \beta_i \leftarrow \beta_{i-1} + \beta_l$.
    $T_i \leftarrow \overline{T}_{i-1} + T_l$.
    $\overline{T}_i \leftarrow Rep(T_i)$.
    if $i \pmod 2 = 0$ then
        $l \leftarrow x' \pmod{n'}$ where $\overline{T}_i(x', y')$
    else
        $l \leftarrow x' \pmod{n'} + n'$ where $\overline{T}_i(x', y')$
    if $\overline{T}_i = \overline{T}_j (n \leq j < i)$ then
        go out this loop.
$s \leftarrow -(p^{2t} \cdot \alpha_i - p^{2t'} \cdot \alpha_j)/(p^{2t} \cdot \beta_i - p^{2t'} \cdot \beta_j) \pmod r$, where $0 \leq t < 6$ and $0 \leq t' < 6$.
```

6 Experimental result

In this chapter, the authors apply the normal rho method and the previous method to the BN curve and confirm that the fruitless cycle increases. The authors also apply the previous method and the proposed method to the BN curve and verify the effect. The relationship between the parameters of the BN curve used in the experiment and the value of χ is shown in Table 1.

6.1 Confirmation of increase in the number of fruitless cycles

The authors compare the normal rho method with the previous rho method. The previous method is Pollard's rho method with the skew Frobenius mapping, and the number of seed point tables is one. The authors consider a BN curve with $\chi = 3$ in Eq.(5) and parameters which include a set of seed points ($n = 16$ and 32), and a starting point. The case is a 12-bit ECDLP. The representative point $Rep(T_i)$ is a rational point with the maximum x coordinate and even y coordinate in the group of six points. Since the number of combinations is huge, two rational points P and Q, which are the seed points and the starting point, are randomly selected for each trial, and 100 thousand trials are executed.

Table 2 shows the relationship between the number of rational points and the cycle length that can be solved when a collision occurs in the normal rho method where $\chi = 3$, the number of seed points is 16. The distinguished point method is not applied in the confirmation of the increase in the number of fruitless cycles. The second column of Table 2 represents the number of combinations for which the scalar s can be solved. The third column represents the number of combinations that result in a fruitless cycle in which the scalar s cannot be solved. If the cycle length is 401 or more, it is indicated as "else". The fourth column shows the sum of the second and third columns.

It can be confirmed that the number of fruitless cycles is 56, which is very small. The average length of a random-walk path of the solvable cases was 59.7. Since the fruitless cycle keeps drawing the same cycle forever without the detection of the fruitless cycle, the random-walk length cannot

Table 2: Frequency distribution of cycle length when ECDLP is solvable or unsolvable in the normal rho method with $\chi = 3$, the number of seed points $n = 16$, and without thinned bits

cycle length	(1) solvable	(2) unsolvable	(1)+(2)
0	2931	1	2932
1	685	0	685
2	1882	1	1883
3	2476	1	2477
4	2442	3	2445
5	2431	2	2433
6-200	87097	48	87145
201-400	0	0	0
else	0	0	0
all	99944	56	100000

Table 3: Frequency distribution of cycle length when ECDLP is solvable or unsolvable in the previous method with $\chi = 3$, the number of seed points $n = 16$, and without thinned bits

cycle length	(1) solvable	(2) unsolvable	(1)+(2)
0	1046	0	1046
1	5325	1	5326
2	5201	19623	24824
3	5229	360	5589
4	4901	173	5074
5	4523	18	4541
6-200	53572	28	53600
201-400	0	0	0
else	0	0	0
all	79797	20203	100000

be defined in this context. On the other hand, with the detection of the fruitless cycle, the length of the fruitless cycled random-walk path should be defined as the total length of a foot and a cycle.

Table 3 shows the relationship between the number of rational points and the cycle length that can be solved when a collision occurs in the previous method where $\chi = 3$, the number n of seed points is 16. The number of fruitless cycles when ECDLP could not be solved was 20203 in the previous method. The number of fruitless cycles was 360 times that of the normal rho method. In particular, the increase in fruitless cycles of length two is remarkable. On the other hand, the average length of the solvable random-walk path is 22.7, and the application of skew Frobenius mapping achieves a reduction in the time required to solve ECDLP.

Table 4 shows the relationship between the number of rational points and the cycle length that can be solved when a collision occurs in the normal rho method where $\chi = 3$, the number n of seed points is 32. Since the number of seed points affects the occurrence of the fruitless cycle, it can be confirmed that the number of fruitless cycles decreases as the number of seed points increases. The average length of the solvable random-walk path was 58.3. The random-walk length was not significantly affected by the number of seed points.

Table 5 shows the relationship between the number of rational points and the cycle length that can be solved when a collision occurs in the previous method where $\chi = 3$, the number n of seed points is 32. By increasing the number of seed points, the number of solvable cases of ECDLP increased. However, the number of fruitless cycles is large. Increasing the number of seed points is a measure to eliminate the fruitless cycle, but it is equivalent to increasing the conserved quantity of rational points. Therefore, the authors consider a method that can eliminate the fruitless cycle without increasing the number of rational points. The average length of the solvable random-walk

Table 4: Frequency distribution of cycle length when ECDLP is solvable or unsolvable in the normal rho method with $\chi = 3$, the number of seed points $n = 32$, and without thinned bits

cycle length	(1) solvable	(2) unsolvable	(1)+(2)
0	2841	2	2843
1	1152	0	1152
2	2364	1	2365
3	2565	2	2567
4	2508	1	2509
5	2375	1	2376
6-200	86146	42	86188
201-400	0	0	0
else	0	0	0
all	99951	49	100000

Table 5: Frequency distribution of cycle length when ECDLP is solvable or unsolvable in the previous method with $\chi = 3$, the number of seed points $n = 32$, and without thinned bits

cycle length	(1) solvable	(2) unsolvable	(1)+(2)
0	1062	0	1062
1	5796	2	5798
2	5693	10457	16150
3	5523	47	5570
4	5239	55	5294
5	4866	2	4868
6-200	61229	29	61258
201-400	0	0	0
else	0	0	0
all	89408	10592	100000

path was 23.3.

From the above results, it was confirmed that the number of fruitless cycles increased by applying the skew Frobenius mapping. In addition, the ratio between the unsolvable cases and the solvable cases of the previous method, which include the skew Frobenius mapping, becomes much larger than that of the normal method. The results confirms that the probability of the case where a restarted random-walk path after a fruitless cycle is non-negligible for the previous method, and a method to eliminate the fruitless cycle will be a counter measure for the problem.

6.2 Verification of the effect of the proposed method

The authors show the experimental results of applying the previous method and the proposed method to a BN curve. The previous method is Pollard's rho method with the skew Frobenius mapping, and the number of seed point tables is one. On the other hand, the proposed method is also Pollard's rho method with the skew Frobenius mapping where the number of seed point tables is two. The authors consider a BN curve with $\chi = 3$, 7 and 107 in Eq.(5) and parameters which include a set of seed points ($n = 16$, 32, and 64), and a starting point. If the number of seed points is 64, the experiment is performed for $\chi = 7$ and 107. The cases of $\chi = 7$ and 107 are a 17-bit ECDLP and a 33-bit ECDLP, respectively. The representative point $Rep(T_i)$ is a rational point with the maximum x coordinate and even y coordinate in the group of six points. In addition, the authors consider a number of bits to be thinned out ($\tau = 0$, 1, and 2) in the distinguished point method. Since the number of combinations is huge, two rational points P and Q, which are the seed points and the starting point, are randomly selected for each trial, and 100 thousand trials are executed.

A rho method is usually used in parallel attacks using a server and massive clients. The clients

Table 6: The number of solvable or unsolvable cases and average random-walk length with $\chi = 3$, the number of seed points $n = 16$ and 32, and thinned bits $\tau = 0$, 1, and 2 in the previous method

n	τ	solvable	unsolvable		average random-walk length		
			$\langle 1 \rangle$	$\langle 2 \rangle$	solvable	$\langle 1 \rangle$	solvable+$\langle 1 \rangle$
16	0	79797	20203	0	22.7	15.8	21.3
	1	60141	20765	19094	23.1	15.8	21.2
	2	38356	21037	40607	23.1	15.6	20.4
32	0	89408	10592	0	23.3	16.4	22.6
	1	67228	10998	21774	23.7	16.3	22.7
	2	43325	11381	45294	23.7	16.3	22.2

Table 7: The number of solvable or unsolvable cases and average random-walk length with $\chi = 3$, the number of seed points $n = 16$ and 32, and thinned bits $\tau = 0$, 1, and 2 in the proposed method

n	τ	solvable	unsolvable		average random-walk length		
			$\langle 1 \rangle$	$\langle 2 \rangle$	solvable	$\langle 1 \rangle$	solvable+$\langle 1 \rangle$
16	0	99131 (47304)	869	0	24.1	18.6	24.1
	1	83397 (47977)	1111	15492	27.9	23.1	27.8
	2	59398 (35960)	1203	39399	30.0	22.9	29.9
32	0	99725 (47718)	275	0	24.0	18.8	24.0
	1	84107 (48464)	306	15587	27.7	36.5	27.7
	2	59595 (36166)	373	40030	30.0	25.2	30.0

send only the rational points that satisfy the distinguished point method and the server detects a collision. Only the server saves the received rational points. In order to analyze the structure of the rho method, the authors focus on one server and one client, and the rational points generated on the client are also saved separately in this experiment. If the server detects a collision, ECDLP can be solved. If the generated rational points colliding over the client and continue to draw the same cycle, ECDLP cannot be solved.

Table 6 shows the frequency distribution among the solving ratio, the number of seed points ($n = 16$ and 32), the number of thinned bits, and the random-walk length in the previous method with $\chi = 3$. The first column of Table 6 represents the number of seed points n. The second column of Table 6 represents the condition of the distinguished point method and represents the number of bits that is 0 from the least significant bit of the x coordinate of the rational point that the client sends to the server. The third column of Table 6 represents the number of combinations for which the scalar s can be solved. The fourth and fifth column represents the number of combinations that result in a fruitless cycle in which the scalar s cannot be solved. The fourth column $\langle 1 \rangle$ is the number of fruitless cycles described in Section 5.1. The fifth column $\langle 2 \rangle$ shows the number of solvable cycles that include rational points that do not satisfy the condition of the distinguished point method among the unsolvable cases. That is, it is a cycle that can be solved when the distinguished point method is not applied and cannot be solved on the server when the distinguished point method is applied, and we call the new fruitless cycle case. From the sixth to the eighth columns are the average lengths of the random-walk path. The sixth column is the average length of solvable random-walk paths. The seventh column is the average length of the unsolvable random-walk paths, since the cases are the old fruitless cycle cases, the average length of the cases is shorter than of the solvable cases. The eighth column is the average length of the stoppable random-walk paths, which include both the solvable cases and the old fruitless cycle cases.

As the number of thinned bits increases, the solvable cases decrease. The result of adding the number in the third column and the number in the fifth column is almost the same regardless of the thinned bit. Therefore, it can be confirmed that the solvable cycles when the distinguished point method is not applied became unsolvable cycles because the condition of the distinguished point method was not satisfied. The average random-walk length was slightly increased by applying the

Table 8: The number of solvable or unsolvable cases and average random-walk length with $\chi = 7$, the number of seed points $n = 16$, 32 and 64, and thinned bits $\tau = 0$, 1, and 2 in the previous method

n	τ	solvable	unsolvable		average random-walk length		
			⟨1⟩	⟨2⟩	solvable	⟨1⟩	solvable+⟨1⟩
16	0	28711	71289	0	96.7	57.1	68.5
	1	21552	71354	7094	97.7	56.7	66.2
	2	12641	71229	16130	97.8	56.5	62.7
32	0	51007	48993	0	116.4	70.9	94.1
	1	38872	48426	12702	116.5	71.7	91.6
	2	22218	48772	29010	116.3	71.4	85.5
64	0	70980	29020	0	127.3	80.8	113.8
	1	52910	29527	17563	128.7	80.6	111.5
	2	30718	29410	39872	127.8	80.8	104.8

Table 9: The number of solvable or unsolvable cases and average random-walk length with $\chi = 7$, the number of seed points $n = 16$, 32, and 64, and thinned bits $\tau = 0$, 1, and 2 in the proposed method

n	τ	solvable	unsolvable		average random-walk length		
			⟨1⟩	⟨2⟩	solvable	⟨1⟩	solvable+⟨1⟩
16	0	94020 (46890)	5980	0	130.1	91.7	127.8
	1	77971 (46463)	6910	15119	160.9	105.4	156.4
	2	50483 (32035)	7588	41929	175.8	115.0	167.9
32	0	98512 (48749)	1488	0	140.9	94.3	140.2
	1	81990 (48756)	1732	16278	162.4	105.6	161.2
	2	53544 (33942)	1889	44567	177.9	116.1	175.8
64	0	99652 (49505)	348	0	140.9	85.2	140.7
	1	83284 (49522)	450	16266	162.9	105.5	162.6
	2	54438 (34271)	530	45032	177.4	113.8	176.8

distinguished point method.

Table 7 shows the distribution among the solving ratio, the number of seed points ($n = 16$ and 32), the number of thinned bits, and the random-walk length in the proposed method with $\chi = 3$. Since the proposed method has two seed point tables, it does not always continue to collide even if it results in the collision once. Therefore, the numbers in parentheses in the third column represent the numbers that continue to collide on a cycle. Note that the case of the first collision point is not a distinguished point, the random-walk continues until the first collision occurs with a distinguished point. The fourth column in Table 7 shows the number of fruitless cycles, and it can be confirmed that the number of fruitless cycles has been reduced by 94.2% or more compared to Table 6. The authors compare the case where the number of seed points is 16 and the distinguished point method is not applied. The number that can be solved ECDLP on the server is 79797 in the previous method and 99131 in the proposed method. When the number of bits to be thinned out in the distinguished point method was two, the number of solvable cases of the proposed method is 1.55 times of the previous method. In addition, the larger the number of the seed points, the smaller the occurrence rate of the fruitless cycle. The average length of the random-walk paths of the proposed method is slightly longer than that of the previous method. The authors consider the cause is that the eliminated fruitless cycle appeared as a random-walk of other lengths. From the values estimated by the birthday paradox, the average random-walk length is $\sqrt{\pi r/12}$. Therefore, it is considered that the average length of the random-walk paths of the proposed method has become longer, and the result is theoretically acceptable. In addition, since a practical rho method is usually used in parallel attacks, which stops with a λ shaped collision before drawing a cycle, the effect of increased

Table 10: The number of solvable or unsolvable cases and average random-walk length with $\chi = 107$, the number of seed points $n = 16$, 32, and 64, and thinned bits $\tau = 0$ and 1 in the previous method

n	τ	solvable	unsolvable		average random-walk length		
			⟨1⟩	⟨2⟩	solvable	⟨1⟩	solvable+⟨1⟩
16	0	0	1000	0	N/A	92.7	92.7
	1	0	518	482	N/A	96.2	96.2
32	0	0	1000	0	N/A	189.4	189.4
	1	0	507	493	N/A	197.7	197.7
64	0	0	1000	0	N/A	387.7	387.7
	1	0	481	519	N/A	352.1	352.1

Table 11: The number of solvable or unsolvable cases and average random-walk length with $\chi = 107$, the number of seed points $n = 16$, 32, and 64, and thinned bits $\tau = 0$ and 1 in the proposed method

n	τ	solvable	unsolvable		average random-walk length		
			⟨1⟩	⟨2⟩	solvable	⟨1⟩	solvable+⟨1⟩
16	0	6(4)	994	0	2879.2	2076.0	2080.8
	1	4(1)	505	491	5171.0	2157.8	2181.5
32	0	83(40)	917	0	13163.8	7488.4	7959.5
	1	61(41)	497	460	14353.1	8416.6	9087.29
64	0	435(227)	565	0	27718.3	16361.9	21301.9
	1	357(235)	329	314	30915.2	17164.4	24320.4

average random-walk length is considered to be small.

Then, the authors show the experimental results when $\chi = 7$. Table 8 shows the distribution among the solving ratio, the number of seed points ($n = 16$, 32, and 64), the number of thinned bits, and the random-walk length in the previous method with $\chi = 7$. As the parameters of the BN curve become larger, the search range of ECDLP becomes larger. Therefore, the random-walk length becomes longer and the number of solvable cases becomes smaller. The estimated value by the birthday paradox is $\sqrt{\pi r/12} \fallingdotseq 140.1$, but the experimental results show that the random-walk length is smaller than the estimated value. The longer the random-walk length, the higher the frequency of fruitless cycles described in Section 5.1. Therefore, the number of long random-walks that can solve ECDLP is reduced, and the random-walk length is shortened. In addition, the more seed points, the longer the random-walk length. The authors consider that the more seed points, the less likely it is to have a fruitless cycle, making it possible to decipher long random-walks.

Table 9 shows the distribution among the solving ratio, the number of seed points ($n = 16$, 32, and 64), the number of thinned bits, and the random-walk length in the proposed method with $\chi = 7$. Compared with the previous method, the proposed method succeeded in reducing the fruitless cycle by 89.3% or more. On the other hand, the random-walk length became longer. It is considered that the eliminated fruitless cycle resulted in a long random-walk that can solve ECDLP.

Tables 10 and 11 are the distribution among the solving ratio, the number of seed points ($n = 16$, 32, and 64), the number of thinned bits, and the random-walk length in the previous method and proposed method, respectively, with $\chi = 107$ over 1000 trials. Though the number of trials is small, we can observe that the solvable cases are successfully increased by the proposed method, especially for the 64 seed points. The results indicate that the effectiveness to increase the ratio of the solvable cases is large for the large χ with the large number of seed points. Roughly speaking, effectiveness of the proposed method could be equivalent to increase the number of parallel random-walk paths at the starting time of the attack.

In order to further compare the previous method and the proposed method, the authors focus on cycle lengths in Pollard's rho method with $\chi = 7$, the number n of seed points is 64 and the number τ of thinned bits is zero.

Table 12 shows the relationship between the number of rational points and the cycle length that

Table 12: Frequency distribution of cycle length when ECDLP is solvable or unsolvable in the previous method with $\chi = 7$, the number of seed points $n = 64$, and without thinned bits

cycle length	(1) solvable	(2) unsolvable	(1)+(2)
0	154	0	154
1	815	0	815
2	868	28824	29692
3	833	134	967
4	896	59	928
5	910	1	911
6-200	64819	2	64821
201-400	1710	0	1710
else	2	0	2
all	70980	29020	100000

Table 13: Frequency distribution of cycle length when ECDLP is solvable or unsolvable in the proposed method with $\chi = 7$, the number of seed points $n = 64$, and without thinned bits

cycle length	(1) solvable	(2) unsolvable	(1)+(2)
0	192	0	192
1	1002	0	1002
2	1035	0	1035
3	1117	0	1117
4	1052	345	1397
5	1076	3	1079
6-200	90609	0	90609
201-400	3557	0	3557
else	12	0	12
all	99652	348	100000

can be solved when a collision occurs in previous method where $\chi = 7$ and the number of seed points is 64. The second column of Table 12 represents the number of combinations for which the scalar s can be solved. The third column represents the number of combinations that result in a fruitless cycle in which the scalar s cannot be solved. If the cycle length is 401 or more, it is indicated as "else". The fourth column shows the sum of the second and third columns.

Table 13 shows the relationship between the number of rational points and the cycle length that can be solved when a collision occurs in the proposed method where $\chi = 7$ and the number of seed points is 64. In the proposed method, the number of the fruitless cycles of length two and three were reduced, and the number of the fruitless cycles of length four were increased. In the next section, the authors consider why the fruitless cycle of length four has increased.

From the above, the proposed method succeeded in significantly eliminating the fruitless cycle. Since the major cost of the proposed method is to switch the two seed tables, the benefit of the proposed method can be estimated by the number of the increased solvable random-walk paths which increase the probability of the solvable collision for the parallel rho method. However, there are still problems such as the long random-walk length of the proposed method. The effectiveness of the long random-walks would be confirm by the experiments for the parallel rho method as a future work.

6.3 Consideration of the proposed method

The proposed method eliminated the fruitless cycles of lengths two and three and increased the number of fruitless cycles of length four. The authors consider the cause of the increased fruitless cycle of length four. From T_{i+1} to T_{i+4} are expressed as follows, as in (8):

$$\overline{T}_i = Rep(T_i) = \phi_6^{t_0}(T_i), \tag{9}$$

$$T_{i+1} = \overline{T}_i + T_{\eta_1(\overline{T}_i)} = \phi_6^{t_0}(T_i) + T_{\eta_1(\overline{T}_i)}, \tag{10}$$

$$\overline{T}_{i+1} = Rep(T_{i+1}) = \phi_6^{t_1}(T_{i+1}) = \phi_6^{t_1}(\overline{T}_i) + \phi_6^{t_1}(T_{\eta_1(\overline{T}_i)}), \tag{11}$$

$$T_{i+2} = \overline{T}_{i+1} + T_{\eta_2(\overline{T}_{i+1})} = \phi_6^{t_1}(T_{i+1}) + T_{\eta_2(\overline{T}_{i+1})}, \tag{12}$$

$$\overline{T}_{i+2} = Rep(T_{i+2}) = \phi_6^{t_2}(T_{i+2}) = \phi_6^{t_2}(\overline{T}_{i+1}) + \phi_6^{t_2}(T_{\eta_2(\overline{T}_{i+1})}), \tag{13}$$

$$T_{i+3} = \overline{T}_{i+2} + T_{\eta_1(\overline{T}_{i+2})} = \phi_6^{t_2}(T_{i+2}) + T_{\eta_1(\overline{T}_{i+2})}, \tag{14}$$

$$\overline{T}_{i+3} = Rep(T_{i+3}) = \phi_6^{t_3}(T_{i+3}) = \phi_6^{t_3}(\overline{T}_{i+2}) + \phi_6^{t_3}(T_{\eta_1(\overline{T}_{i+2})}), \tag{15}$$

$$T_{i+4} = \overline{T}_{i+3} + T_{\eta_2(\overline{T}_{i+3})} = \phi_6^{t_3}(T_{i+3}) + T_{\eta_2(\overline{T}_{i+3})}, \tag{16}$$

$$\begin{aligned} \overline{T}_{i+4} &= Rep(T_{i+4}) = \phi_6^{t_4}(T_{i+4}) = \phi_6^{t_4}(\overline{T}_{i+3}) + \phi_6^{t_4}(T_{\eta_2(\overline{T}_{i+3})}), \\ &= \phi_6^{t_4+t_3+t_2+t_1+t_0}(T_i) + \phi_6^{t_4+t_3}\{\phi_6^{t_2+t_1}(T_{\eta_1(\overline{T}_i)}) + T_{\eta_1(\overline{T}_{i+2})}\} \\ &+ \phi_6^{t_4}\{\phi_6^{t_3+t_2}(T_{\eta_2(\overline{T}_{i+1})}) + T_{\eta_2(\overline{T}_{i+3})}\}, \end{aligned} \tag{17}$$

where $0 \leq t_0, t_1, t_2, t_3, t_4 < 6$. In order to distinguish the table of seed points to be added, the η function is distinguished as the η_1 function and the η_2 function. Let the η_1 and η_2 functions be the same functions as the η function.

From Eq.(17), the condition to achieve a fruitless cycle is that the added tables of seed points cancel each other out. Therefore, the condition to achieve the fruitless cycle is that the following equations hold:

$$t_1 + t_2 + t_3 + t_4 = 0 \pmod 6, \tag{18a}$$

$$t_1 + t_2 = 3 \pmod 6, \tag{18b}$$

$$t_2 + t_3 = 3 \pmod 6, \tag{18c}$$

$$\eta_1(\overline{T}_i) = \eta_1(\overline{T}_{i+2}), \tag{18d}$$

$$\eta_2(\overline{T}_{i+1}) = \eta_2(\overline{T}_{i+3}), \tag{18e}$$

where $0 \leq t_1, t_2, t_3, t_4 < 6$. If even one of these conditions is not met, the fruitless cycle of length two will not occur. The number of conditions to achieve the fruitless cycles of the proposed method is greater than those of the previous method, and it is difficult to satisfy all conditions of the proposed method. Therefore, the authors succeeded in greatly eliminating the fruitless cycles. Although most of the eliminated fruitless cycles become solvable cycles only on the client, it is difficult to avoid or detect these cycles when the distinguished point method is applied.

Note that there may be cases where a fruitless cycle occurs due to the combination of seed points added and the skew Frobenius mapping even when the conditions of Eq.(18) is not satisfied. A part of this fruitless cycle will be eliminated by the method proposed in [8], but the occurrence rate depends on the order r of the curve. Even with the 17-bit parameter, since this fruitless cycle hardly occurs, it is not necessary to consider the occurrence of this fruitless cycle of curves with larger parameters.

7 Conclusion

The authors applied Pollard's rho method with the skew Frobenius mapping to a BN curve with $\chi = 3, 7$, and 107, and proposed and theoretically considered a method for eliminating fruitless cycles. The increase of the probability of the fruitless cycles for the single rho method with the skew Frobenius mapping is confirmed by the experiments. The effectiveness of the proposed method was confirmed by the experiments with the single rho methods for the small prime orders 12, 17, and 33-bits of BN curves. However, most of the eliminated fruitless cycles became the cycles that could be solved ECDLP only on the client-side when the distinguished point method was applied for the small order BN curves, and the cases are defined as the new fruitless cycles.

One of future works is to confirm the effectiveness of the proposed method by experiments of the parallel rho method for a large prime order BN curve. To consider a method to eliminate the new fruitless cycles in a practical parallel rho method is also a future work. In contrast, the length of a typical random-walk path with an old style fruitless cycle becomes shorter than that with a solvable cycle, to confirm the possibility of a collision of two different random-walk paths with the old style fruitless cycle is also a future work. In addition, since the behavior of Pollard's rho method changes depending on the parameters, it is also a future work to consider the optimum parameters such as the seed points or thinning out bits.

8 Acknowledgment

The authors thank the anonymous reviewers to improve this work. This work was supported by the JSPS KAKENHI Challenging Research (Pioneering) 19H05579.

References

[1] D.Boneh, B.Lynn, and H.Shacham, "Short Signatures from the Weil Pairing," ASIACRYPT2001, LNCS, vol.2248, pp.514–532, Springer, Berlin, Heidelbelg, 2001.

[2] D.Boneh, G.D.Crescenzo, R.Ostrovsky, and G.Persiano, "Public Key Encryption with Keyword Search," EUROCRYPT2004, LNCS, vol.2248, pp.506–522, Springer, Berlin, Heidelbelg, 2004.

[3] T.Kim and R.Barbulescu, "Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case," Advances in Cryptology - CRYPTO 2016., LNCS, vol.9814, pp.543–571, Springer, Berlin, Heidelbelg, 2016.

[4] J.M.Pollard, "Monte Carlo Methods for Index Computation (mod p)," Mathematics of computation, 32(143):918–924, 1978.

[5] E.Teske, "On Random Walks for Pollard's Rho Method," Mathematics of computation, 70(234):809–825, 2000.

[6] T.Kusaka, S.Joichi, K.Ikuta, M.A.-A.Khandaker, Y.Nogami, S.Uehara, and N.Yamai, "Solving 114-bit ECDLP for a Barreto-Naehrig Curve," Information Security and Cryptology(ICISC2017), pp.231–244, 2017.

[7] E.Teske, "speeding up pollard's rho method for computing discrete logarithms," ANTS 1998, LNCS, vol.1423, pp.541–554, Springer, Berlin, Heidelbelg, 1998.

[8] H.Miura, R.Matsumura, K.Ikuta, S.Joichi, T.Kusaka, and Y.Nogami, "A Preliminary Study on Methods to Eliminate Short Fruitless Cycles for Pollard's Rho Method for ECDLP over BN Curves," 2019 7th International Symposium on Computing and Networking Workshops (CANDARW), pp.353–359, IEEE, 2019.

[9] H.Miura, K.Ikuta, S.Joichi, T.Kusaka, and Y.Nogami, "Analysis of the fruitless cycle of Pollard's rho method based attack for solving ECDLP over Barreto-Naehrig curves," 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), pp.162–165, IEEE, 2019.

[10] P.S.Barreto and M.Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order," SAC 2005, LNCS, vol.3897, pp.319–331, Springer, Berlin, Heidelbelg, 2005.

[11] Y.Sakemi, Y.Nogami, K.Okeya, H.Kato, and Y.Morikawa, "Skew Frobenius Map and Efficient Scalar Multiplication for Pairing-Based Cryptography," CANS 2008, LNCS, vol.5339, pp.226–239, Springer, Berlin, Heidelbelg, 2008.

[12] J.Patarin and A.Montreuil, “Benes and Butterfly Schemes Revisited,” ICISC 2005, LNCS, vol.3935, pp.92–116, Springer, Berlin, Heidelbelg, 2005.