Solving 94-bit ECDLP with 70 Computers in Parallel

Shunsuke Miyoshi, Yasuyuki Nogami, Takuya Kusaka, Nariyoshi Yamai

Abstract—Elliptic curve discrete logarithm problem (ECDLP) is one of problems on which the security of pairing-based cryptography is based. This paper considers Pollard’s rho method to evaluate the security of ECDLP on Barreto-Naehrig (BN) curve that is an efficient pairing-friendly curve. Some techniques are proposed to make the rho method efficient. Especially, the group structure on BN curve, distinguished point method, and Montgomery trick are well-known techniques. This paper applies these techniques and shows its optimization. According to the experimental results for which a large-scale parallel system with MySQL is applied, 94-bit ECDLP was solved about 28 hours by parallelizing 71 computers.

Keywords—Pollard’s rho method, BN curve, Montgomery multiplication.

I. INTRODUCTION

RECENT Ate-based pairings such as Optimal ate[1] and Xate[2] on Barreto-Naehrig (BN) curve[3] have received much attention since they realize quite efficient pairing calculations. However, few researchers have tried to evaluate the security of pairings. Elliptic curve discrete logarithm problem (ECDLP)[4] is one of problems on which the security of pairing-based cryptography is based. Pollard’s rho method[5] is known as an efficient algorithm to solve a large-scale ECDLP. This paper optimizes Pollard’s rho method to solve ECDLP on $G_1$ over Barreto-Naehrig (BN) curve. $G_1$ is a rational point group on BN curve defined over prime field from which an input for pairing is chosen. The rho method basically consists of two steps: randomly generating points on the curve and detecting a collision from the generated points.

Some techniques such as Montgomery multiplication, Montgomery trick, distinguished point method, and the group structure on BN curve have been proposed to make generating random points step more efficient. Montgomery trick reduces the number of inversions required in the calculation procedure. Distinguished point method reduces the load of a collision detection at server. The group structure on BN curve reduces the size of ECDLP itself. This paper optimizes Montgomery multiplication to make the arithmetic operations on BN curve more efficient.

When attacking large size ECDLPs, the system for detecting collisions is important. When solving 110-bit ECDLP, the rho method requires about 1600[GB] storage area and it needs to detect a collision from about $1.8 \times 10^{16}$ points even if using the distinguished point method. Thus, this paper considers about a client-server model, and then the server detects a collision using MySQL.

Then, this paper attacks 94-bit ECDLP for evaluating the security. This experiment uses 69 clients, and 2 servers in our university. We used these computers during about 2 days and the system solved a 94-bit ECDLP.

II. PRELIMINARIES

This section introduces elliptic curve over finite field and some properties of rational point on elliptic curve. In addition, this section introduces Pollard’s rho method.

A. Elliptic Curve

In what follows, $F_p$ denotes a prime field. An elliptic curve $E$ is generally defined as follows.

$$E : y^2 = x^3 + ax + b, \quad a, b \in F_p, \quad x, y \in F_p. \quad (1)$$

$E(F_p)$ that is a set of rational points on $E$ over $F_p$, including the infinity point $O$, forms an additive Abelian group. $r$ denotes the group order of $E(F_p)$.

1) Elliptic Curve Addition: Elliptic curve addition is the addition between rational points. $Q_1(x_1, y_1) + Q_2(x_2, y_2) = Q_3(x_3, y_3)$ is defined as follows, where $Q_1, Q_2$ and $Q_3$ are rational points of elliptic curve $E(F_p)$.

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

$$(x_3, y_3) = \begin{cases} \left( \frac{\lambda^2 - x_1 - x_2}{(x_1 - x_3)\lambda - y_1} \right) & \text{if } \lambda \neq \phi, \\ O & \text{otherwise.} \end{cases}$$

2) Barreto-Naehrig Curve: Barreto-Naehrig (BN) curve[3] that is well known to realize an efficient pairing is defined in the form of

$$E : y^2 = x^3 + b, \quad b \in F_p, \quad (4)$$

together with the following parameter settings,

$$p = 36\ell^4 - 36\ell^3 + 24\ell^2 - 6\ell + 1, \quad (5)$$
$$r = 36\ell^4 - 36\ell^3 + 18\ell^2 - 6\ell + 1, \quad (6)$$

where $\ell$ is a certain integer and $p$ is the characteristic of $F_p$.

The embedding degree $k$ of BN curve is 12.
B. Ate Pairing

Ate pairing $e$ is defined as follows, where $E(\mathbb{F}_{p^2})[r]$, Ker, and $r$ denote the set of rational points of order $r$, kernel of homomorphism, and Frobenius element, respectively.

$$G_1 = E(\mathbb{F}_{p^2})[r] \cap \text{Ker}(\pi - [1]),$$ (7)

$$G_2 = E(\mathbb{F}_{p^2})[r] \cap \text{Ker}(\pi - [p]),$$ (8)

$$e(\cdot, \cdot) : G_1 \times G_2 \rightarrow G_3 = \mathbb{F}_{p^2}^{*}/(\mathbb{F}_{p^2}^{*})^r.$$ (9)

In the case of BN curve, the above $G_1$ is equal to $E(\mathbb{F}_p)$.

C. Twist and Skew-Frobenius Mapping

In order to improve Ate pairing with BN curve, the sextic-twist technique is available. Since the embedding degree of BN curve is 12 and BN curve is written as Eq.(4), sextic-twist technique is available. Since the embedding degree of BN curve is 12 and BN curve is written as Eq.(4), sextic-twist technique is available.

$$E = \mathbb{F}_{p^2}[x, y]/(y^6 - \pi),$$. (10)

where $\pi$ is a cubic and quadratic non residue in $\mathbb{F}_{p^2}$. In this case, we have the following isomorphism.

$$G'_1 = E'(\mathbb{F}_{p^2})[r] \cap \text{Ker}(\pi^2 - [p^2]).$$ (11)

$$\psi_0 : (x, y) \in G_1 \mapsto (v^{1/3} x, v^{1/2} y) \in G'_1.$$. (12)

$G'_1$ has the following isomorphism $\tilde{\pi}$, where $Q$ is a rational point on $G'_1$. It is called skew-Frobenius mapping.

$$\tilde{\pi}(Q) = \psi_0^{-1}(\pi^2(\psi_0(Q)))$$

$\equiv (v^{2/3} x, v^{1/2} y).$. (13)

In this case, $\tilde{\pi}^6(Q) = \tilde{\pi}$. Thus, in what follows, it is denoted by $\tilde{\pi}_0$. $\tilde{\pi}_0$ is used for the grouping in the rho method.

D. Security of Pairing-based Cryptography

The security of pairing-based cryptography based on discrete logarithm problem on $G_1$, $G_2$, and $G_3$, and pairing inversion problem. Thus, pairing-based cryptography requires all of these difficulties. This paper evaluates the security of all of these difficulties. This paper evaluates the security of elliptic curve discrete logarithm problem on $G_1$ for which this section introduces Pollard’s rho method.

1) ECDLP: ECDLP is the problem that calculates the scalar $s$ only by using rational points $P$ and $Q$ on $E$ such that $Q = [s]P$, where $[s]P$ means $[s]P = P + P + \cdots$ $\times$ s points. (14)

2) Pollard’s Rho Method: Pollard’s rho method is known as an efficient technique for solving an ECDLP. The rho method consists of two steps. The first step randomly generates a lot of rational points as follows, where $a_i, b_i$ are random numbers from 0 to $r - 1$.

$$T_i = \{a_i\}P + \{b_i\}Q.$$ (15)

The next step detects a collision among the generated points. When a collision is found such as $T_i = T_j (i \neq j)$, the ECDLP is solved by a simultaneous equation.

The original algorithm of rho method is given as Alg. 1. In this paper, we precompute a table which consists of $n$ rational points such as Eq.(15) and generate random points by using the table. In what follows, $\gamma(T_i)$ is a function that decides the index of a rational point in the table corresponding to the input $T_i$. It is said that a collision occurs when $\sqrt{\pi r/2}$ points are generated according to the birthday paradox.

**Algorithm 1: Pollard’s Rho Method**

Input: $P, Q = [s]P \in E(\mathbb{F}_p)$ $(0 \leq s < r)$

Output: $s$

1. for $i = 0$ to $n - 1$ do

   2. $a_i, b_i$ are random elements $(0 \leq a_i, b_i < r)$,

   3. $T_i \leftarrow \{a_i\}P + \{b_i\}Q$.

   4. $a_n, b_n$ are random elements $(0 \leq a_n, b_n < r)$,

   5. $T_n \leftarrow \{a_n\}P + \{b_n\}Q$.

6. for $i = n + 1$ to $r - 1$ do

   7. $l \leftarrow \gamma(T_{i-1})$.

   8. $a_i \leftarrow a_{i-1} + a_{i}, b_i \leftarrow b_{i-1} + b_i, T_i \leftarrow T_{i-1} + T_l$.

   9. if $T_i = T_j (0 \leq j \leq i)$ then go out this loop.

10. $s \leftarrow \{a_{i-1} - a_i\}/\{b_{i-1} - b_i\}$ (mod r).

III. IMPROVEMENT OF RHO METHOD

This section denotes some techniques for making the attack more efficient.

A. Using The Group Structure on BN Curve

The skew-Frobenius mapping $\tilde{\pi}_0$ is available for the grouping technique. In $G_1$ of BN curve, suppose that the rho method detected a collision by $T_i$ and $T_j$ as $T_i = \tilde{\pi}_0^{a_j}(T_j)$ $(0 \leq n < 6)$. Because, from the Eq.(8), $\tilde{\pi}_0^{a_j}(T_j) = [p^{2n}]T_j$. Thus, this technique enables to reduce the average number for a collision from $\sqrt{\pi r/2}$ to $\sqrt{\pi r/12}$. In detail,

$$T_i = \tilde{\pi}_0^{a_j}(T_j),$$

$$T_i = [p^{2n}]T_j, a_i + b_i \cdot s \equiv [p^{2n}]a_j + [p^{2n}]b_j \cdot s \pmod{r},$$

$$s \equiv \frac{(a_i - a_j - b_j)}{(b_i - p^{2n}b_j)} \pmod{r}.$$ (16)

$\tilde{\pi}_0^{a_j}(T_j)(0 \leq n < 6)$ are thus conjugates to each other that helps efficiently solving ECDLPs since they are connected by not only efficient mapping $\tilde{\pi}_0^{a_j}$ but also scalar multiplications $[p^{2n}]$. In detail, they are given as follows, where $e = \sqrt{\pi r/2}$,

$$T_i = (x_j, y_j),$$

$$\tilde{\pi}_0^{a_j}(T_j) = (e^{a_j}, y_j),$$

$$\tilde{\pi}_0^{2a_j}(T_j) = (e^{2a_j}, y_j),$$

$$\tilde{\pi}_0^{a_j}(T_j) = (x_j, -y_j),$$

$$\tilde{\pi}_0^{2a_j}(T_j) = (e^{2a_j}, -y_j).$$ (19)

In order to apply this grouping technique to the rho method, a function $L(\cdot)$ that determines a representative of the
D. Parallelization

Suppose that a collision \( T_i = U_j \) was detected. Then, their following points similarly collide as follows,

\[
T_{\eta(T_i)} = U_{\eta(U_j)}, \quad T_{\eta(T_{\eta(T_i)})} = U_{\eta(U_{\eta(U_j)})}, \quad \ldots
\]  \hspace{1cm} (23)

where \( \eta \) is used for uniquely determining a certain point in the random walk table. Thus, it is found that a parallelization is effective for the rho method.

IV. OPTIMIZATION

This section shows an optimization for the rho method. The target of this paper is about 100-bit ECDLP and this paper uses 64-bit word length computer. The compiler is gcc version 4.5.4, this version supports 128-bit integer. Thus, an addition in \( \mathbb{F}_p \) is easily implemented when using 128-bit integer, however a multiplication and inversion in \( \mathbb{F}_p \) require additional ideas.

A. Montgomery Multiplication

This paper applies Montgomery multiplication for a multiplication in \( \mathbb{F}_p \). Montgomery multiplication calculates a multiplication in \( \mathbb{F}_p \) using only additions and bit shift operations. The algorithm is shown as Alg. 2.

Algorithm 2: Montgomery Multiplication

**Input:** \( X = (x_{m-1} \cdot 2^w (m-1), \ldots, x_1 \cdot 2^w 1, x_0 \cdot 2^w 0), \)

\( Y = (y_{m-1} \cdot 2^w (m-1), \ldots, y_1 \cdot 2^w 1, y_0 \cdot 2^w 0), \)

\( N = (n_{m-1} \cdot 2^w (m-1), \ldots, n_1 \cdot 2^w 1, n_0 \cdot 2^w 0), \)

\( W = -N^{-1} \mod 2^w \)

**Output:** \( Z = XY^2 \cdot m^{-w} \mod N \)

1. \( Z = 0 \)
2. for \( i = 0 \) to \( m - 1 \) do
3. \( t_i = (z_0 + x_i y_0) W \mod 2^w \)
4. for \( j = 0 \) to \( m - 1 \) do
5. \( Q = z_j + x_j y_j + t_i n_j + C \)
6. if \( j \neq 0 \) then
7. \( z_{j+1} = Q \mod 2^w \)
8. \( C = Q/2^w \)
9. \( z_{m-1} = C \)
10. if \( Z \geq N \) then
11. \( Z = Z - N \)

This paper considers the optimization of Alg. 2. \( j \) at line 5 equals to 0 or 1. When \( j = 0 \), it is same value of \( 2^w z_0 + x_i y_0 + t_i n_j + C \) at line 4 and \( z_j + x_j y_j + t_i n_j + C \) at line 6. However, \( Q \) at line 6 maybe 128-bit. This paper deals with this carry by comparison. In line 6, store \( x_i y_j \) first. Next, calculate \( Q \) and compare with the stored \( x_i y_j \). If \( Q < x_i y_j \), a carry occurs. The optimized Montgomery multiplication algorithm is shown in Alg. 3.

Algorithm 3: Optimized Montgomery Multiplication

**Input:** \( X = (x_1 \cdot 2^{64}, x_0), \quad Y = (y_1 \cdot 2^{64}, y_0), \)

\( N = (n_1 \cdot 2^{64}, n_0), \quad W = -N^{-1} \mod 2^{64} \)

**Output:** \( Z = XY^2 \cdot 2^{-128} \mod N \)

1. \( xy = x_0 \times y_0 \)
2. \( t = xy \times W \mod 2^{64} \)
3. \( Q = xy + (t \times n_0) \)
4. if \( carry \) then
5. \( Q = Q + 2^{64} \)
6. if \( Q < Q/2^{64} \) then
7. \( Z = Q/2^{64} \)
8. \( xy = x_1 \times y_0 + Q \mod 2^{64} \)
9. \( t = xy \times W \mod 2^{64} \)
10. if \( carry \) then
11. \( Z = Z + 2^{64} \)
12. \( xy = x_1 \times y_1 + t \times n_1 + Q/2^{64} \)
13. if \( carry \) then
14. \( Z = Z + 2^{64} \)
15. if \( Z \geq N \) then
16. \( Z = Z - N \)

B. Collision Detection at Server

This paper considers about a model such that many clients generate random rational points by the optimized rho method in parallel and then send the generated and distinguished points to the server, and the server detects a collision.

There are a few rational points on the server when using the technique described in Sec. III-C, however it is difficult that
all points are stored on memory. For example, when solving 110-bit ECDLP and setting the parameter $\theta$ by $2^{20}$, about $\sqrt{\pi \times 2^{110}/12}/2^{20} \approx 1.8 \times 10^{16}$ points need to be stored. If the size of 1 data is 100[Byte], it requires 1600[GB] storage area.

Therefore this paper stores rational points on the storage such as HDD (Hard Disk Drive). When rational points are stored in HDD, the number of storing points are increased, however, the performance degradation is caused by disk IO. This paper avoids the performance degradation by controlling the size of $\theta$ in Sec.III-C.

V. EXPERIMENT

This paper implemented the optimized rho method described in Chap.III and Chap.IV and evaluated the security of ECDLP. In this experiment, the target is 94-bit ECDLP, where $r = 9401882149685691336171017(94\text{-bit})$. Then average number for detecting a collision is $\sqrt{\pi r}/12 \approx 49599992270415$ according to the birthday paradox on the technique described in Sec.III-A. This paper tried to find the scalar $s$ for the following $P$ and $Q$ ($= [s]P$).

$$P = (7262408195386367430506168279, 5909492387210969059012426224)$$
$$Q = (8830658031211912159902020265, 7909569409614716533720230088)$$

Table I shows the computational environment. Table II shows the result. The scalar value $s$ was 4960155460405181786913975321 from solving result. The number of generated points in Table II is given by multiplying the number of stored points and $\theta$ for the distinguished points. According to the result, 94-bit ECDLP was solved in 100779[sec] by generating about 42069934473216 points. Since, the average number for a collision is $\sqrt{\pi r}/12 \approx 49599992270415$, it is estimated that 94-bit ECDLP is averagely solved by $100779 \times 49599992270415 \approx 118818[sec]$. 

Table I shows the computational environment. Table II shows the result. The scalar value $s$ was 4960155460405181786913975321 from solving result. The number of generated points in Table II is given by multiplying the number of stored points and $\theta$ for the distinguished points. According to the result, 94-bit ECDLP was solved in 100779[sec] by generating about 42069934473216 points. Since, the average number for a collision is $\sqrt{\pi r}/12 \approx 49599992270415$, it is estimated that 94-bit ECDLP is averagely solved by $100779 \times 49599992270415 \approx 118818[sec]$. 

VI. CONCLUSION

This paper has evaluated the security of $G_1$ in pairing-based cryptography on BN 94-bit curve by optimized the rho method. The results of the experiment of a 94-bit ECDLP show that the problem was solved in 28 hours with 71 computers. Since the number of the generated points in the experiment is 42069934473216, the number is much smaller than the estimated average number of the rho method.

REFERENCES