國立臺灣大學理學院數學系
碩士論文
Department of Mathematics
College of Science
National Taiwan University
Master Thesis

橢圓曲線密碼系統之曲線安全性研究
The Security of Curves for Elliptic Curve Cryptosystems

研究生: 江前佑
Student: Chien-Yeo Chiang

指導教授: 陳君明 博士
Advisor: Jiun-Ming Chen, Ph.D.

中華民國九十七年六月
June, 2008

國立臺灣大學（碩）博士學位論文
口試委員會審定書

橢圓曲線密碼系統之曲線安全性研究
The Security of Curves for Elliptic Curve Cryptosystems

本論文係江前佑君（學號 R94221032）在國立臺灣大學數學學系、所完成之碩（博）士學位論文，於民國九十七年七月二日承下列考試委員審查通過及口試及格，特此證明

口試委員：

陳君明 （簽名）

（指導教授）

鄭振牟　　黃柏嶧

系主任、所長 ______________ （簽名）

（是否須簽章依各院系所規定）

誌謝

首先要感謝我的指導教授陳君明老師。從開始請他指導以來, 每星期固定的討論, 使我從對橢圓曲線一無所知, 到現在有個大致上的了解, 眞是收穫匪淺。此外我也從老師身上, 學到許多做事的態度與方法, 表達能力方面也因此有所進步。在論文方面, 當我遇到問題時, 老師花了許多時間和我一起討論, 同時也指引我一些方向, 並在寫作上給了我許多寶貴的建議, 這篇論文才得以誕生。另外也要感謝在我寫論文的過程中, 和我一起討論的同學們以及在背後默默支持我的家人們。

摘要

現今許多密碼系統的安全性, 是以橢圓曲線離散對數問題 (ECDLP) 的困難度爲基礎。這些密碼系統的安全性, 通常取決於曲線的選擇。在這篇論文中, 我們對現在針對橢圓曲線離散對數問題的攻擊法做一個整理, 找出弱曲線的條件, 也提出一些安全曲線應該有的條件。另外, 我們也會討論一些其他的攻擊法, 這些攻擊法對 ECDLP 是失敗的。

關鍵字: 橢圓曲線密碼學; 橢圓曲線離散對數; 弱曲線; 索引演算; 離散對數。

Abstract

The elliptic curve discrete logarithm problem (ECDLP) forms the basis of numerous cryptosystems today. The security of these cryptosystems usually depends on the choice of curves. In this thesis, we give a summary of recent attacks on the ECDLP, find the criteria of weak curves, and suggest the conditions that a secure curve should have. We will also discuss some attacks which works on the DLP but may fail to the ECDLP.

Key words: elliptic curve cryptography; elliptic curve discrete logarithm; weak curve; index calculus; discrete logarithm.

Contents

口試委員會審定書 i

致謝 ii

Abstract in Chinese iii

Abstract in English iv

1 Introduction 1

2 General Attacks on the ECDLP 4

2.1 Baby Step, Giant Step 4

2.2 The Pollard Method 5

2.2.1 Pollard's ρ Method 5

2.2.2 Pollard's λ Method 9

2.3 Pohlig-Hellman Attack 11

3 Isomorphism Attacks on the ECDLP 15

3.1 Attacks on Anomalous Curves 15

3.1.1 Smart's Method 15

3.1.2 Semaev's Method 18

3.2 MOV Attack 22

3.3 Tate Pairing Attack 26

3.4 Weil Descent 29

4 Other Attacks 33

4.1 Index Calculus on the ECDLP 33

4.2 Xedni Calculus on the ECDLP 36

4.3 Semaev's Summation Polynomials 44

4.4 Further Results 47

5 Conclusions 50

References 52

A Computation of the Parings 57

1 Introduction

The discrete logarithm problem (DLP) in an abelian group G is that given two elements α and β in G, we want to find an integer k such that $\beta = \alpha^k$. Provided that such k exists, we denote $k = log_\alpha \beta$. In particular, a discrete logarithm problem on an elliptic curve group is called an elliptic curve discrete logarithm problem (ECDLP). The difficulty of the ECDLP depends on the choice of the curve and the base field. Therefore, it is important to use a good curve in an elliptic curve cryptosystem. In this thesis, we give a summary of recent attacks on the ECDLP to find the criteria of weak curves and weak base fields. Except for the brute force attack, recent cryptanalysis on the ECDLP can be roughly categorized into two classes: general attacks and isomorphism attacks.

The baby step, giant step method [31] can be used to solve the DLP in any finite abelian group, thus it solves the ECDLP as well. However, it has space and time complexity $O(\sqrt{n})$ where n is the order of the base point P. By using some random walks, Pollard [25] reduced the space to a constant amount and maintained the time complexity $O(\sqrt{n})$. Therefore, we can circumvent the Pollard method by a sufficiently large n. Pohlig and Hellman [24] also noticed that to solve the DLP in a finite abelian group G one needs only to solve the DLP in subgroups of a prime power order of G. The original DLP is then solved by using the Chinese Remainder Theorem (CRT). Our choice of curves can be reduced to a simple case: the curve has a base point P whose order n is a prime larger than 2^{163}.

If G is a group of prime order n, G and $\langle P \rangle$ are both cyclic, hence isomorphic. The main idea of the isomorphism attack is to find an efficiently computable isomorphism from $\langle P \rangle$ to G. If there exist subexponential-time (or faster) algorithms to the DLP in G, we can reduce the ECDLP to the DLP on G. The known isomorphism attacks are the following.

- The attack on anomalous curves (the elliptic curves with prime order p), due to Smart [35], Satoh and Araki [26], uses lifting and p-adic logarithm to reduce the ECDLP defined over prime field F_p to the DLP in F_p^+. The discrete logarithm can be solved efficiently by using the extended Euclidean algorithm. This method has been generalized by Semaev [29] to the case that an elliptic curve group which has a subgroup of prime order p.

- The Weil and Tate pairing attacks both establish an isomorphism from $\langle P \rangle$ to the subgroup μ_n of F_{q^l} for some integer l, where $q = p$ or $q = 2^m$. The former attack was developed by Menezes, Okamoto and Vanstone (MOV) [20] with an additional constraint $n \nmid (q-1)$, and the latter attack was developed by Frey and Rück [4] without this additional constraint. The ECDLP can be reduced to the DLP in $F_{q^l}^*$ where there exists subexponential-time algorithms.

- Gaudry, Hess and Smart (GHS) [9] proposed an efficient algorithm that reduces ECDLP instances in $E(F_{2^m})$, the elliptic curve defined over a binary field, to instances of the hyperelliptic curve discrete logarithm problem (HCDLP). Menezes and Qu [19] further showed that GHS attack fail to all cryptographically interesting elliptic curves over F_{2^m} for all prime $m \in [160, 600]$. Maurer, Menezes and Teske [17] completed the analysis of the GHS attack by identifying and enumerating the isomorphism classes of the elliptic curves over F_{2^m} for composite $m \in [160, 600]$.

To avoid the above attacks, one needs to compute the order of the elliptic curve group. There is a polynomial-time algorithm proposed by Schoof [27] to do this.

This method is improved by Atkins and Elkis [1].

The remainder of this thesis is organized as follows. In Section 2, we review the general attacks and set up some basic requirements of the curve. In section 3, we introduce the isomorphism attacks which is useful on some special curves. In section 4, we give an introduction to the index method, xedni method and their failure on ECDLP. We will also introduce a new idea which transforms the original ECDLP to a system of polynomial equations. In section 5, we give a summary of the weak curves and certain base fields which should not be used in an elliptic curve cryptosystem.

2 General Attacks on the ECDLP

The following notations will be used throughout this article.

F_p the finite field of p elements, where p is a prime.

F_{2^m} the finite field of 2^m elements, also called binary field.

F_q the finite field of q elements.

$E(K)$ the elliptic curve group defined over a field K, given by points on

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $a_i \in K$,

together with point at infinity ∞.

N the order of $E(K)$

n the order of the base point $P \in E(K)$

$E[n]$ the set of points of order dividing n with coordinates in the algebraic closure $\overline{K}$.

The elliptic curve discrete logarithm problem is that given $Q \in \langle P \rangle$, to find an integer k such that $Q = kP \in E(K)$. Note that we only concern about the cases that the base field K is F_p or F_{2^m}, since they are widely used in practice.

2.1 Baby Step, Giant Step

Shanks [31] developed a method which requires approximately $\sqrt{N}$ steps and $\sqrt{N}$ storage. Given a point P on an elliptic curve group, it is easy to compute its inverse. With this in mind, the algorithm is modified as follows.

1. Choose an integer $s \geq \sqrt{N}$ and compute sP
2. Calculate the x-coordinate of iP for $0 \leq i < s/2$ and store them as a list.
3. Compute the points $Q - jsP$ for $j = 0, 1, ..., s$ until the x-coordinate of one of them matches a point from the list. Set $i = i_0$ and $j = j_0$ for this match.

4. Using the y-coordinate to decide $Q - j_0 sP = i_0 P$ or $Q - j_0 sP = -i_0 P$.

5. If $Q - j_0 sP = i_0 P$, we have $k \equiv i_0 + j_0 s \pmod{N}$.

   If $Q - j_0 sP = -i_0 P$, we have $k \equiv -i_0 + j_0 s \pmod{N}$.

The above algorithm requires approximately $\sqrt{N}/2$ steps and $\sqrt{N}/2$ storage. Therefore we would like to choose the size N (usually with the same size as the key) of $E(K)$ is larger than 2^{224} bits in comparison with 2^{2048} which is the key size recommended for public-key schemes such as RSA. In practical implementation N is selected to be greater than 2^{160}.

To apply BSGS, although we have mentioned that the order of the elliptic curve group $N = |E(F_q)|$ can be computed by Schoof algorithm [27], we do not need to know the exact order N. The reason is that there is an upper bound of N by Hasse's theorem, so the number s can be chosen by satisfying $s^2 \geq q + 1 + 2\sqrt{q}$. Notice also that although our discussion here is on N, a similar discussion on the order n of the base point P gives the same result.

2.2 The Pollard Method

2.2.1 Pollard's ρ Method

The main idea behind the Pollard method is to find distinct pairs (a', b') and (a, b) modulo n such that $a'P + b'Q = aP + bQ$. Then $(a' - a)P = (b - b')Q = (b - b')kP$ implies

$$k = \log_P Q \equiv (a' - a)(b - b')^{-1} \pmod{n},$$

provided $(b - b')^{-1}$ exists.

At first glance, randomly selecting the pairs takes about $\sqrt{\pi n/2} \approx 1.2533\sqrt{n}$ as the expected number of iterations to find a collision according to the birthday paradox. It takes also $3\sqrt{\pi n/2} \approx 3.7599\sqrt{n}$ storage, Pollard's method gives roughly the same expected time, but needs very little storage.

The subgroup $\langle P \rangle$ of $E(K)$ is first partitioned into three subsets S_1, S_2, S_3 of roughly the same size by using the partition function H. We write $H(X) = j$ if $X \in S_j$. The idea of Pollard is to use an iterating function f to find a collision. The iterating function $f : \langle P \rangle \to \langle P \rangle$ is defined by

$$f(X) = \begin{cases} X + Q & \text{if } H(X) = 1 \\ 2X & \text{if } H(X) = 2 \\ X + P & \text{if } H(X) = 3 \end{cases}$$

If we start at a point $X_1 = a_1P + b_1Q$, we can generate a sequence of points recursively by $X_{i+1} = f(X_i)$. Then two integer sequences $\{a_i\}$ and $\{b_i\}$ satisfying $X_{i+1} = a_{i+1}P + b_{i+1}Q$ for $i \geq 0$ can be computed by

$$a_{i+1} = \begin{cases} a_i \pmod{n} & \text{if } H(X_i) = 1 \\ 2a_i \pmod{n} & \text{if } H(X_i) = 2 \\ a_i + 1 \pmod{n} & \text{if } H(X_i) = 3 \end{cases}$$

$$b_{i+1} = \begin{cases} b_i + 1 \pmod{n} & \text{if } H(X_i) = 1 \\ 2b_i \pmod{n} & \text{if } H(X_i) = 2 \\ b_i \pmod{n} & \text{if } H(X_i) = 3 \end{cases}$$

We store the pair (X_1, X_2) and iteratively compute pairs (X_i, X_{2i}) until $X_i = X_{2i}$ for some i. Since $\langle P \rangle$ is finite, this collision does happen. Hence we have a relation $a_iP + b_iQ = a_{2i}P + b_{2i}Q$, which means $(a_i - a_{2i})P = (b_{2i} - b_i)Q = (b_{2i} - b_i)kP$. Therefore

$$k = log_PQ \equiv (a_i - a_{2i})(b_{2i} - b_i)^{-1} (\text{mod } n)$$

when $b_{2i} - b_i$ is relative prime to n.

We summarize the Pollard's ρ method [25] to the ECDLP as follows.

1. Select a partition function $H : \langle P \rangle \rightarrow \{1, 2, 3\}$.

2. Select $a_1, b_1 \in [0, n-1]$ and compute the initial point $X_1 = a_1P + b_1Q$.

3. Repeat

   (a) Compute $X_{i+1} = f(X_i)$ and $X_{2i+2} = f(f(X_{2i}))$.

   (b) Compute a_i, b_i, a_{2i} and b_{2i}.

   until $X_i = X_{2i}$.

4. If $b_i = b_{2i}$ then go back to 2, else compute $k \equiv (a_i - a_{2i})(b_{2i} - b_i)^{-1} \pmod{n}$

Gallant, Lambert and Vanstone [6] and Wiener and Zuccherato [38] independently discovered the method to speed Pollard's method by using automorphisms. The main idea is to reduce the size of the set in the Pollard method, then the time required to find a collision is less.

Suppose $\psi : \langle P \rangle \rightarrow \langle P \rangle$ is an automorphism which can be computed efficiently. Since $\langle P \rangle$ is finite, ψ is finite of order t. That is, t is the smallest number such that $\psi^t(R) = R$ for all $R \in \langle P \rangle$. We then use this automorphism to define an equivalence relation $\sim$ on $\langle P \rangle$ by

$$R_1 \sim R_2 \text{ if and only if } R_1 = \psi^j(R_2) \text{ for some } j \in [0, t-1].$$

The only difficulty is to construct a random walk which is well defined among the equivalence classes. We may choose a representative which has the minimal x-coordinate in each equivalence class (with ties broken by selecting the point with a smaller y-coordinate), denoted by $\overline{R}$. Then an iterating function g defined by $g(R) = \overline{f(R)}$ is modified from f to be well-defined on these representatives.

Since ψ is an automorphism, we have $\psi(P) = \lambda P$ for some $\lambda \in [0, n-1]$. Suppose we know this integer λ, then $\psi(R) = \lambda R$ for all $R \in \langle P \rangle$. Thus, if we start at a point $X_1 = a_1 P + b_1 Q$, it will be easy to compute the representative $\overline{X_1}$ of equivalence class which contains X_1. Namely, if $\overline{X_1} = \psi^j(X_1) = aP + bQ$ for some integer j, then $a \equiv \lambda^j a_1 \pmod{n}$ and $b \equiv \lambda^j b_1 \pmod{n}$ [12].

Now g can be used as the iterating function on the representatives of equivalence classes with roughly n/t elements. Set the initial point $X_1' = \overline{X_1}$ and apply the Pollard method with $X_{i+1}' = g(X_i')$ for $i \geq 1$, then the expect number of iterations to find a collision is about $\sqrt{n\pi/2t}$.

We close this section by some examples which shows the security may be affected by this method.

Example 2.1. Suppose $p \equiv 1 \pmod{3}$ is a prime, then there exists an element $\beta \in F_p$ of order 3. For the elliptic curve $E : y^2 = x^3 + b$ defined over F_p, the map $\phi : E(F_p) \to E(F_p)$ defined by

$$\phi(x, y) = (\beta x, -y) \text{ and } \phi(\infty) = \infty$$

is an endomorphism of order 6. For a prime field of size 2^{160}, we require a work of

$$\sqrt{\frac{n\pi}{2t}} = \sqrt{\frac{\pi n}{2 \cdot 6}} \approx 2^{79}$$

to solve an ECDLP. The security reduced one bit in comparison with 2^{80} of the ordinary Pollard method.

Example 2.2. Consider the Koblitz curves (anomalous binary curve) defined over F_{2^m} of the form $y^2 + xy = x^3 + ax^2 + 1$ where $a \in \{0, 1\}$. The Frobenius map $\phi : E(F_{2^m}) \to E(F_{2^m})$ defined by

$$\phi(x, y) = (x^2, y^2) \text{ and } \phi(\infty) = \infty$$

is an endomorphism of order m. This method can reduce the security of the Koblitz curve over $F_{2^{163}}$ by an effort of approximately

$$\sqrt{\frac{n\pi}{2m}} = \sqrt{\frac{\pi n}{2 \cdot 163}} \approx 2^{77}$$

to break the ECDLP, rather than approximately 2^{81} of the ordinary Pollard method.

2.2.2 Pollard's λ Method

Pollard [25] also describes another λ-method which can be parallelized to solve an ECDLP. With a little more information than usual, he finds a collision by keeping track of two kangaroos. Each kangaroo is a random walk using the same iterating function but starting at different initial points [36]. One is called the tame kangaroo and another is the wild kangaroo. The main idea is to use the tame kangaroo to set up some traps to catch the wild kangaroo. Once the wild kangaroo falls into a trap set up by the tame kangaroo, it will then follow the footprints of the tame kangaroo. Eventually, the ECDLP is solved.

The following is a small variant of the Pollard method from [1]. As in the ρ-method, first we select a partition function H from $\langle P \rangle \to \{1, 2, \ldots, L\}$ where L is usually around 16. Let $S = \{M_1, M_2, \ldots, M_L\}$. Each jump of a kangaroo depends on the point from which the kangaroo jumps and in a distance that is randomly selected from the set S. A natural choice of M_j may be of the form

$$M_j = s_j P + t_j Q$$

where s_j, t_j are randomly selected from $[0, n-1]$.

Our iteration function $f : \langle P \rangle \to \langle P \rangle$ is then defined by

$$f(X) = X + M_j \text{ where } H(X) = j.$$

So, if $X_i = a_iP + b_iQ$, then it will be easy to compute $X_{i+1} = f(X_i) = a_{i+1}P + b_{i+1}Q$ where

$$X_{i+1} = X_i + M_j \text{ with } H(X_i) = j$$

$$a_{i+1} = a_i + s_j \pmod{n}$$

$$b_{i+1} = b_i + t_j \pmod{n}$$

The remaining problem is that if we start with the tame kangaroo at $T_1 = a_1P + b_1Q$ and the wild kangaroo at $W_1 = a'_1P + b'_1Q$, we must store all the computed points $T_{i+1} = f(T_i)$ and $W_{i+1} = f(W_i)$ until a collision is found. This requires $O(\sqrt{n})$ storage. How do we find a collision without using too much storage? An idea is to use the *distinguishing property.* A point is called *distinguished* if it satisfies some property which can be tested easily, such as the last digit of its x-coordinate being zero. We just look for the collision point which is distinguished. The algorithm is summarized as follows.

1. Select a partition function $H : \langle P \rangle \to \{1, 2, \ldots, L\}$.

2. Construct $S = \{M_1, M_2, \ldots, M_L\}$

3. Select $a_1, b_1 \in [0, n-1]$ and compute the initial point $T_1 = a_1P + b_1Q$.

4. Select $a'_1, b'_1 \in [0, n-1]$ and compute the initial point $W_1 = a'_1P + b'_1Q$.

5. Repeat

   (a) If T_i or W_i is distinguished then store (a_i, b_i, T_i) or (a'_i, b'_i, T'_i)

   (b) Compute $T_{i+1} = f(T_i)$ and $W_{i+1} = f(W_i))$.

   (c) Compute $a_{i+1}, b_{i+1}, a'_{i+1}$ and b'_{i+1}.

   until the processor stores some distinguished point Y for the second time. Let (c, d, Y) and (c', d', Y) be the two triples associated with Y.

6. If $d = d'$ then go back to 3, else compute $k \equiv (c - c')(d - d')^{-1} \pmod{n}$

Note that the above algorithm can be easily parallelized if we compute the tame and the wild kangaroo in different processors. Whenever a processor encounters a distinguished point, it transmits the point to a central server which stores it in a sorted list. In addition, starting with more than two initial points gives more kangaroos. Then it will be faster to find a collision. In fact, if we have u processors, this yields a speedup of factor u. Let θ be the proportion of points in $\langle P \rangle$ with this distinguishing property. One expects the random walk taking another $1/\theta$ steps in the worst case before a collision occurs. So the expect number of finding a collision of distinguished point is

$$\frac{1}{u}\sqrt{\frac{n\pi}{2}} + \frac{1}{\theta}.$$

Remark 2.3. The above algorithm is a generalization of the Pollard method. In the original Pollard method, he assumes that $k \in [a, b] \subset [0, n-1]$ such that $b - a$ is a fairly manageable quantity. The tame kangaroo is chosen to start at bP, wild kangaroo is chosen to start at Q, and $H = \lfloor \log_2(b - a) \rfloor$. Another choice of the iterating function is also available.

2.3 Pohlig-Hellman Attack

If the order of P can be factorized by

$$n = \prod_i p_i^{e_i}$$

where p_i are small primes such that the Pollard's method works in attacking the ECDLP of $E(F_{p_i})$. The idea of Pohlig and Hellman [24] attack is to find $k \pmod{p_i^{e_i}}$, then use the CRT to combine these results to obtain $k \pmod{n}$. We will write

k in expansion of base p_i as

$$k = k_0 + k_1 p_i + \ldots + k_{e_i-1} p_i^{e_i-1} (\text{mod } p_i^{e_i}),$$

then k (mod $p_i^{e_i}$) is evaluated by successively determining $k_0, k_1, \ldots, k_{e_i-1}$.

1. Compute $\frac{n}{p_i}P$.

2. Compute $Q_0 = \frac{n}{p_i}Q$

3. Solve the discrete logarithm k_0 of Q_0 to the base $\frac{n}{p_i}P$ by the Pollard method.

4. If $e_i = 1$, stop. Otherwise, continue.

5. From $j = 1$, let $Q_j = Q_{j-1} - k_{j-1} p_i^{j-1} P$.

6. Solve the discrete logarithm k_j of $\frac{n}{p_i^{j+1}} Q_j$ to the base $\frac{n}{p_i}P$ by the Pollard method.

7. Repeat until $j = e_i - 1$.

Then $k \equiv k_0 + k_1 p_i + \ldots + k_{e_i-1} p_i^{e_i-1}$ (mod p^{e_i}). We can check the above algorithm by

$$\begin{aligned} \frac{n}{p_i}Q = \frac{n}{p_i}kP &\equiv \frac{n}{p_i}(k_0 + k_1 p_i + \ldots + k_{e_i-1} p_i^{e_i-1})P \\ &\equiv k_0 \frac{n}{p_i} P + (k_1 + \ldots + k_{e_i-1} p_i^{e_i-2}) nP \\ &\equiv k_0 \frac{n}{p_i} P (\text{mod } p_i^{e_i}). \end{aligned}$$

Therefore we have indeed found k_0 in the algorithm. It is similar to k_i for $i = 1, \ldots, e_i - 1$.

It is obvious that the Pohlig-Hellman attack works well if the prime factors p_i of n are small. If there is a large prime number dividing $n \geq 2^{160}$, then the Pollard method can not work, which implies that the Pohlig-Hellman attack is of little use. For this reason, if a cryptosystem is based on the ECDLP, we would like to choose the order of the elliptic curve group contains a large ($\geq 2^{160}$) prime factor.

We close this section with an easy example which can be found in [1]. It solves the ECDLP by Pohlig-Hellam attack combined with the Pollard method.

Example 2.4. Consider the elliptic curve $E : y^2 = x^3 + 71x + 602$ defined over the finite field F_{1009}, then $N = 1060 = 2^2 \cdot 5 \cdot 53$. We want to find k such that $Q = kP$, where $P = (1, 237)$ and $Q = (190, 271)$, with the order of P is 530. First we use the reduction of Pohlig and Hellman to compute k modulo $2, 5$ and 53.

- k **(mod** 2**).** Compute the points

  $$(530/2)P = 265P = (50, 0) \text{ and } Q_0 = (530/2)Q = 265Q = (50, 0),$$

  then solve Q_0 to the base of $(530/2)P$. It is clearly $k \equiv 1 \pmod 2$.

- k **(mod** 3**).** Compute the points

  $$(530/5)P = 106P = (639, 160) \text{ and } Q_0 = (530/5)Q = 106Q = (639, 849),$$

  then solve Q_0 to the base of $(530/5)P$. We can see that $Q_0 = -(530/5)P$, which means $k \equiv -1 \equiv 4 \pmod 5$.

- k **(mod** 53**).** Compute the points

  $$P' = (530/53)P = 10P = (32, 737) \text{ and } Q_0 = (530/53)Q = 10Q = (592, 97),$$

  then solve Q_0 to the base of $(530/5)P$. First we select a partition function

  $$H : E(F_{1009}) \longrightarrow \{1, 2, 3\}.$$
  $$(x, y) \mapsto x(\text{mod } 3) + 1$$

Construct the set S as

$$M_1 = 2P' + 0Q_0 = (8, 623),$$

$$M_2 = 1P' + 1Q_0 = (654, 118),$$

$$M_3 = 3P' + 4Q_0 = (555, 82).$$

Now we set $T_1 = 1P' + 0Q_0$ and $W_1 = 0P' + 1Q_0$. Since $H(T_1) = 3$ and $H(W_1) = 2$, we obtain

$$T_2 = f(T_1) = T_1 + M_3 = 4P' + 4Q_0 = (200, 357),$$

$$W_2 = f(W_1) = W_1 + M_2 = 1P' + 2Q_0 = (817, 136).$$

All T_i and W_i can be computed in the same way. After collecting enough T_i and W_i, we have found that the tame kangaroo has crossed its own path $7P' + 8Q_0 = T_3 = T_6 = 12P' + 9Q_0$. We get $k \equiv -5 \equiv 48 \pmod{53}$.

After using the Chinese Reminder theorem with the above conclusion, we know that $k \equiv 368 \pmod{530}$.

3 Isomorphism Attacks on the ECDLP

3.1 Attacks on Anomalous Curves

An elliptic curve defined over a prime field $E(F_p)$ is called *anomalous* if $|E(F_p)| = p$, which implies that $E(F_p)$ is isomorphic to F_p^+, the additive group of F_p. The problem is how to define an isomorphism which can be computed efficiently. In 1997, Smart [35], Satoh, Araki [26] and Semaev [29] proposed three different attacks on anomalous curves independently. Each attack gives an isomorphism from $E(F_p)$ to F_p^+, which can be used to reduce an ECDLP on $E(F_p)$ to a DLP on F_p^+. Then a DLP on F_p^+ can be solved efficiently by using the extended Euclidean algorithm. In this section, we will introduce the methods presented by Smart and Semaev which gives a running time $O(\log p)$, and demonstrate an easy example.

3.1.1 Smart's Method

Smart's idea [35] is to use the standard logarithm map for the subgroup of the elliptic curve group defined over the field of p-adic number $\mathbb{Q}_p$. Suppose $E(F_p)$ is an anomalous elliptic curve defined over the field F_p. Given $P, Q \in E(F_p)$. We want to find k such that $Q = kP$. In order to apply the standard logarithm map, first we need to lift P and Q to the points $\tilde{P}$ and $\tilde{Q}$ on $\tilde{E}(\mathbb{Q})$.

Definition 3.1. Suppose R is a ring and $I \subseteq R$ is an ideal with $\bigcap_i I^i = \{0\}$. Let I^ν be given. A sequence $\{a_n\} \subseteq R$ is a *Cauchy sequence*, if there exists some $l \in \mathbb{N}$ such that

$$a_i - a_j \in I^\nu \text{ whenever } i, j \geq l.$$

The ring R is *complete with respect to* I, if every Cauchy sequence of I converges.

The lifting process can be done by the following lemma.

Lemma 3.2 (Hensel's Lemma)**.** *Let R be a ring which is complete with respect to some ideal $I \subset R$, and let $F(w) \in R[w]$ be a polynomial. Suppose that $a \in R$ satisfies* (*for some integer $i \geq 1$*)

$$F(a) \in I^i \text{ and } F'(a) \in R^*.$$

Then for any $\alpha \in R$ satisfying $\alpha \equiv F'(a) \pmod{I}$, the sequence $\{w_n\}$ with

$$w_0 =, w_{m+1} = w_m - F(w_m)/\alpha \text{ for } m \geq 1$$

converges to an element $b \in R$ satisfying

$$F(b) = 0 \text{ and } b \equiv a \pmod{I^i}$$

If R is an integral domain, then these conditions determine b uniquely.

Proof. ([32], IV.1) □

After lifting the points to the elliptic curve $\tilde{E}(\mathbb{Q}_p)$, the next step is to construct the isomorphism from $E(F_p)$ to F_p^+. Define the reduction map $\pi : \tilde{E}(\mathbb{Q}_p) \to E(F_p)$ by $\pi(x, y) = (x, y) \pmod{p}$. Assume the elliptic curve $\tilde{E}(\mathbb{Q}_p)$ has good reduction at p, that is, the reduction map reduces $\tilde{E}(\mathbb{Q}_p)$ to a nonsingular curve $E(F_p)$. The set of points in $\tilde{E}(\mathbb{Q}_p)$ which reduce modulo p to points of $E(F_p)$ is denoted by $\tilde{E}_0(\mathbb{Q}_p)$, and the set of points in $\tilde{E}(\mathbb{Q}_p)$ which reduce to zero is denoted by $\tilde{E}_1(\mathbb{Q}_p)$. We have the following theorem.

Theorem 3.3. *There are exact sequences of abelian groups*

$$0 \to \tilde{E}_1(\mathbb{Q}_p) \to \tilde{E}_0(\mathbb{Q}_p) \to E(F_p) \to 0$$

$$0 \to \tilde{E}_2(\mathbb{Q}_p) \to \tilde{E}_1(\mathbb{Q}_p) \to F_p^+ \to 0$$

where $\tilde{E}_2(\mathbb{Q}_p) = \{\tilde{P} \in \tilde{E}(\mathbb{Q}_p) | v(x_{\tilde{P}}) \leq -4\}$ and $v(x_{\tilde{P}})$ is the p-adic valuation of the x-coordinate of P.

Proof. The maps in the first exact sequence are the reduction modulo p. Their proof can be found in [32] VII.2. □

Since $E(F_p) \cong F_p^+$, the above theorem gives us the following isomorphism,

$$E(F_p) \cong \tilde{E}_0(\mathbb{Q}_p)/\tilde{E}_1(\mathbb{Q}_p) \cong \tilde{E}_1(\mathbb{Q}_p)/\tilde{E}_2(\mathbb{Q}_p) \cong F_p^+.$$

We start with the points $\tilde{P}, \tilde{Q} \in \tilde{E}_0(\mathbb{Q}_p)$, then compute $\tilde{P}_1 = p\tilde{P}$ and $\tilde{Q}_1 = p\tilde{Q}$. We will get $\tilde{P}_1, \tilde{Q}_1 \in \tilde{E}_1(\mathbb{Q}_p)$, since $\pi(p\tilde{P}) = p\pi(\tilde{P}) = \infty$. Now we can apply the logarithm

$$\vartheta_p(x, y) = p^{-1}\frac{-x}{y} \pmod{p}$$

to the points $\tilde{P}_1, \tilde{Q}_1$ when they are not in $\tilde{E}_2(\mathbb{Q}_p)$. The algorithm is as follows.

1. Lift the points $P, Q \in E(F_p)$ to the points $\tilde{P}, \tilde{Q} \in \tilde{E}(\mathbb{Q}_p)$ by Hensel's lemma.

2. Compute $\tilde{P}_1 = p\tilde{P}$ and $\tilde{Q}_1 = p\tilde{Q}$.

3. If $\tilde{P}_1 \in \tilde{E}_2(\mathbb{Q}_p)$, then choose new $\tilde{E}, \tilde{P}, \tilde{Q}$ and try again. Otherwise, compute $k \equiv \vartheta_p(\tilde{P}_1)/\vartheta_p(\tilde{Q}_1) \pmod{p}$.

Let's check why it works. Let $\tilde{R} = k\tilde{P} - \tilde{Q}$. We have

$$\infty = kP - Q = \pi(k\tilde{P} - \tilde{Q}) = \pi(\tilde{R})$$

This means $\tilde{R} \in \tilde{E}_1(\mathbb{Q}_p)$. Therefore $\vartheta_p(\tilde{R})$ is defined and $\vartheta_p(p\tilde{R}) = p\vartheta_p(\tilde{R}) \equiv 0 \pmod{p}$. Consequently,

$$\begin{aligned} k\vartheta_p(\tilde{P}_1) - \vartheta_p(\tilde{Q}_1) &= k\vartheta_p(p\tilde{P}) - \vartheta_p(p\tilde{Q}) \\ &= \vartheta_p(kp\tilde{P} - p\tilde{Q}) = \vartheta_p(p\tilde{R}) \equiv 0 \pmod{p} \\ &\Rightarrow\ k \equiv \frac{\vartheta_p(\tilde{Q}_1)}{\vartheta_p(\tilde{P}_1)} \pmod{p}. \end{aligned}$$

Notice that the non-trivial parts are the computations of $\tilde{P}_1$ and $\tilde{Q}_1$, which take $O(\log p)$ operations.

The above algorithm shows that we need only concern the numbers modulo p^2. We will write $O(p^i)$ to represent a rational number of the form $p^i z$ with $v_p(z) \geq 0$ when it doest not have any ambiguity.

Example 3.4. Consider an elliptic curve $E : y^2 = x^3 + 39x^2 + x + 41$ over F_{43}, we want to solve an ECDLP

$$Q = (10, 36) = kP = k(0, 16)$$

The group can be easily verified to have order 43, so it is an anomalous curve. Now P and Q are lifted by Hensel's lemma.

$$\tilde{P} = (0, 16 + 20 \cdot 43 + O(43^2))$$
$$\tilde{Q} = (10, 36 + 40 \cdot 43 + O(43^2))$$

We then need to compute $\tilde{P}_1$ and $\tilde{Q}_1$.

$$\tilde{P}_1 = (38 \cdot 43^{-2} + O(43^{-1}), 41 \cdot 43^{-3} + O(43^{-2}))$$
$$\tilde{Q}_1 = (24 \cdot 43^{-2} + O(43^{-1}), 35 \cdot 43^{-3} + O(43^{-2}))$$

Therefore,

$$\vartheta_p(\tilde{P}_1) = 19 \pmod{43} \text{ and } \vartheta_p(\tilde{Q}_1) = 3 \pmod{43}.$$

Consequently,

$$k \equiv \frac{\vartheta_p(\tilde{Q}_1)}{\vartheta_p(\tilde{P}_1)} \equiv \frac{19}{3} \equiv 16 \pmod{43}.$$

3.1.2 Semaev's Method

Semaev constructs an isomorphism different from Smart's. He uses the functions defined on an elliptic curve to derive an isomorphism. In order to proceed, we first briefly give an introduction to divisors which can be found in any standard textbook such as [32], [37] and [16] (for the case of hyperelliptic curve).

Definition 3.5. A *divisor* is a formal sum of points in $E(\overline{K})$, abbreviated as E,

$$D = \sum_{S \in E} n_S[S],$$

where $n_S = 0$ for all but finitely many points S. The degree of D is the integer

$$deg(D) = \sum n_S,$$

and the sum of D is the sum of all the points in D

$$sum(D) = \sum n_S S.$$

The collection of all divisors, denoted by $Div(E)$, forms a group with operation of formal sum. Its subgroup of elements of degree 0 is denoted by $Div^0(E)$.

Since $y^2 - x^3 - ax - b$ is irreducible over $\overline{K}$ for some $a, b \in \overline{K}$, the ideal $(y^2 - x^3 - ax - b)$ is a prime ideal. So the quotient ring $\overline{K}[x, y]/(y^2 - x^3 - ax - b)$ is an integral domain. We then consider its field of quotient, denoted by $\overline{K}(x, y)$. A function on E is a rational function $f(x, y) \in \overline{K}(x, y)$ defined for at least one point in $E(\overline{K})$. We denote these functions by $\overline{K}(E)$, a similar notation to $K(E)$. A function f is said to have a *zero* or a *pole* at a point P if it takes the value 0 or ∞ at P respectively. Suppose u_P is a function which takes the value 0 or ∞ at P. It can be shown that every f can be written in the form $f = u_P^s g$ with $s \in \mathbb{Z}$ and $g(P)$ is neither 0 nor ∞, so we have the following definition.

Definition 3.6. Suppose f is written in the form $f = u_P^s g$ with $s \in \mathbb{Z}$ and $g(P) \neq 0, \infty$. Define the order of f at P by

$$ord_P(f) = s.$$

The divisor of f is defined by

$$div(f) = \sum_{P \in E} ord_P(f)[P].$$

A divisor D is *principal* if there is some function f such that $div(f) = D$.

A useful property that we will frequently use is the following.

Proposition 3.7. *Let D be a divisor on E with $deg(D) = 0$, then D is principal if and only if $sum(D) = \infty$.*

Now we focus on the Semaev's method. Semaev's method can be used not only in an elliptic curve group of order p but also in a subgroup (the subgroup generated by P) of an elliptic curve group of order p. Since there is nothing to do in a subgroup of order 2, we assume $p > 2$. We only concern that the elliptic curve group defined over a prime field contains a subgroup of order p.

The main idea behind this method is to use the notation of a derivative. Suppose f is a rational function in $F_q(E)$, the definition of the derivative of f is the formal derivative of f just as the techniques we have learned in a calculus course. This gives the following definition.

Definition 3.8. Suppose $f \in F_q(E)$. The derivative of f respect to x is defined by

$$f' = \frac{df}{dx} + \frac{df}{dy}\frac{dy}{dx},$$

where $\frac{df}{dx}$ and $\frac{df}{dy}$ are ordinary derivative with respect to x and y, and

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}.$$

Suppose D_Q is a divisor with sum which equals Q, and f_Q is the function such that $div(f_Q) = pD_Q$. Assume $n = |\langle P \rangle| = p$, then the following theorem establishes the isomorphic embedding between $\langle P \rangle$ and F_q^+. This can be found in [29].

Theorem 3.9. *Suppose $R \in \langle P \rangle - \{\infty\}$ is a point which is not in the support of D_Q (points in D_Q with nonzero coefficient) for any point $Q \in \langle P \rangle$. Define*

$$\phi : \langle P \rangle \to F_q^+$$
$$Q \mapsto \frac{f'_Q}{f_Q}(R)$$

Then the value $\phi(Q)$ is well defined. The map ϕ is an isomorphic embedding of $\langle P \rangle$ into the additive of F_q.

Proof. Let D'_Q be another divisor representing Q. There is a function g such that $div(g) = D_Q - D'_Q$. If $div(f) = pD'_Q$, then $cg^p f = f_Q$ for some constant c. We have

$$\frac{f'_Q}{f_Q} = \frac{(cg^p f)'}{cg^p f} = p\frac{g^{p-1}g'f}{g^p f} + \frac{g^p f'}{g^p f} = \frac{f'}{f}.$$

So $\phi(Q)$ is well defined.

Now we show that ϕ is a homomorphism. Let $Q_1, Q_2 \in \langle P \rangle$ and $div(f_{Q_i}) = pD_{Q_i}$ for $i = 1, 2$. Notice that $D_{Q_1} + D_{Q_2}$ is a divisor with sum which is equal to $Q_1 + Q_2$, so we can take $D_{Q_1+Q_2} = D_{Q_1} + D_{Q_2}$. This implies

$$div(f_{Q_1+Q_2}) = pD_{Q_1+Q_2} = pD_{Q_1} + pD_{Q_2} = div(f_{Q_1} f_{Q_2}),$$

so the functions $f_{Q_1+Q_2}$ and f_{Q_1}, f_{Q_2} are equal up to a multiplicative constant. Consequently,

$$\frac{f'_{Q_1+Q_2}}{f_{Q_1+Q_2}} = \frac{(f_{Q_1} f_{Q_2})'}{(f_{Q_1} f_{Q_2})} = \frac{f'_{Q_1} f_{Q_2}}{f_{Q_1} f_{Q_2}} + \frac{f_{Q_1} f'_{Q_2}}{f_{Q_1} f_{Q_2}} = \frac{f'_{Q_1}}{f_{Q_1}} + \frac{f'_{Q_2}}{f_{Q_2}}$$

implies ϕ is a homomorphism. Besides, ϕ is injective which follows from the assumption that R is not in the support of D_Q for any $Q \in \langle P \rangle$. □

In order to find k such that $Q = kP$, we compute $\phi(Q)$ and $\phi(P)$. The discrete logarithm k can be computed by $k = \phi(Q)\phi(P)^{-1}$ in F_q.

3.2 MOV Attack

MOV attack, named after Menezes, Okamoto and Vanstone, solves the ECDLP by using the Weil pairing e_n to construct an isomorphism from $\langle P \rangle$ to μ_n, where μ_n is the set of n-th roots of unity. Notice that there exists a subexponential-time algorithm for DLP on a multiplicative group of a finite field. If we can choose some l such that μ_n is contained in F_{q^l}, then solving an ECDLP is equivalent to solving a DLP on $F_{q^l}^*$. In order to proceed, we introduce some important theorems. A complete discussion can be found in [20]. The following theorem that can be found in ([28], 4.2) determines whether or not an elliptic curve of a certain order exists.

Theorem 3.10. *There exists an elliptic curve of order $N = q + 1 - a$ over F_q if and only if the following conditions hold:*

- $a \not\equiv 0$ *(mod p) and* $a^2 \leq 4q$.
- m *is odd and one of the following holds.*

  1. $a = 0$.
  2. $a^2 = 2q$ *and* $p = 2$.
  3. $a^2 = 3q$ *and* $p = 3$.

- m *is even and one of the following holds:*

  1. $a^2 = 4q$.
  2. $a^2 = q$ *and* $p \not\equiv 1 \pmod 3$.
  3. $a = 0$ *and* $p \not\equiv 1 \pmod 4$.

An elliptic curve $E(F_q)$ is *supersingular* if p divides a. From the preceding result, we deduce that $E(F_q)$ is supersingular if and only if $a^2 = 0, q, 2q, 3q, 4q$. Our goal is to show that this attack works when the elliptic curve is supersingular or the trace $a = 2$. We will use the Weil pairing to derive the isomorphism between $\langle P \rangle$ and μ_n. The following theorem describes the existence of the Weil pairing and some related properties.

Theorem 3.11. *Suppose p is a prime. If n is relative prime to p, then there is a map*

$$e_n : E[n] \times E[n] \rightarrow \mu_n$$

called the Weil pairing, which satisfies the following properties:

1. *Identity: For all $P \in E[n]$, $e_n(P, P) = 1$.*

2. *Alternation: For all $P_1, P_2 \in E[n]$, $e_n(P_1, P_2) = e_n(P_2, P_1^{-1})$.*

3. *Bilinearity: For all P_1, P_2, and $P_3 \in E[n]$*

$$e_n(P_1 + P_2, P_3) = e_n(P_1, P_3)e_n(P_2, P_3)$$

$$e_n(P_1, P_2 + P_3) = e_n(P_1, P_2)e_n(P_1, P_3)$$

4. *Non-degeneracy: If $P_1 \in E[n]$ and $e_n(P_1, P_2) = 1$ for all $P_2 \in E[n]$, then $P_1 = \infty$. If $P_2 \in E[n]$ and $e_n(P_1, P_2) = 1$ for all $P_1 \in E[n]$, then $P_2 = \infty$*

5. *If $E[n] \subseteq E(F_{q^l})$, then $\mu_n \subseteq F^*_{q^l}$.*

Proof. ([32], III.8) □

The MOV attack can only applied under some constraints. The following proposition provides necessary and sufficient conditions.

Proposition 3.12. *Let E be an elliptic curve over F_q. Let n be a prime such that $n \mid N$, $E[n] \nsubseteq E(F_q)$, and $n \nmid q(q-1)$. Then*

$$E[n] \subseteq E(F_{q^l}) \textit{ if and only if } q^l \equiv 1 \pmod{n}$$

Proof. [37] P.155. □

The set $E[n]$ is partitioned into cosets of $\langle P \rangle$ by the following lemma.

Lemma 3.13. *Let $E(F_q)$ be an elliptic curve such that $E[n] \subseteq E(F_q)$, where n is relative prime to p. Let $P \in E[n]$ be a point of order n. Then for all $P_1, P_2 \in E[n]$, P_1 and P_2 are in the same coset of $\langle P \rangle$ within $E[n]$ if and only if $e_n(P, P_1) = e_n(P, P_2)$.*

We are ready to introduce the algorithm of the MOV attack. The following is from [20].

1. Choose smallest integer l such that $E[n] \subseteq E(F_{q^l})$.

2. Find $R \in E[n]$ such that $\alpha = e_n(P, R)$ has order n.

3. Compute $\beta = e_n(Q, R)$.

4. Compute k, the discrete logarithm of β to the base α in F_{q^l}, that is $k = log_\alpha \beta$.

It is not difficult to show that $E[n] \cong Z_n \oplus Z_n$ when $\gcd(n, p) = 1$. This implies $E[n]$ is finite. The existence of l follows from the fact that all points in $E[n]$ have coordinate in $\overline{F}_q = \bigcup_{i \geq 1} F_{p^i}$. Suppose $n \nmid q - 1$. We can use Proposition 3.12 to determine the integer l such that $n \mid q^l - 1$ in Step 1.

In Step 2, we need to check the existence of the point R.

Theorem 3.14. *There exists $R \in E[n]$ such that $e_n(P, R)$ is a primitive n-th root of unity for all $P \in E[n]$.*

The choice of R is modified as following. Choose a random point $R_1 \in E(F_{q^l})$, and compute the order M of R_1. Let $d = \gcd(M, n)$ and let $R = (M/d)R_1$. Then R has order d, which divides n, so $R \in E[n]$. This will give $k \pmod d$. We repeat this process until the least common multiple of the various d's is n, then we can use the Chinese Remainder Theorem to compute $k \pmod{n}$.

The above modification works well since $d \neq 1$ occurs very often. By the fundamental theorem of finite abelian groups, we know that $E(F_{q^l}) \cong Z_{n_1} \oplus Z_{n_2}$ for some integer n_1, n_2 where $n_1 | n_2$. Since n_2 is the largest possible order of an element in $E(F_{q^l})$, we get $n | n_2$. Let $\{T_1, T_2\}$ be a basis of $E(F_{q^l})$ where the order of T_1 is n_1 and the order of T_2 is n_2. We have $R_1 = a_1T_1 + a_2T_2$. Suppose s^e is a power of a prime dividing n, then s^f divides n_2 with some integer $f \geq e$. If $s \nmid a_2$, we have s^f divides M. We can show this by dividing M by s^f, which implies $M = s^f q_1 + r$ for some quotient q_1 and $0 \leq r < s^f$. Thus,

$$\begin{aligned} MR_1 = \infty \quad &\Rightarrow \quad M(a_1T_1 + a_2T_2) = \infty \Rightarrow Ma_2T_2 = \infty \\ &\Rightarrow \quad (s^f q_1 + r)a_2T_2 = \infty \\ &\Rightarrow \quad s^f | n_2 | (s^f q_1 + r)a_2 \end{aligned}$$

Since $s \nmid a_2$, we have $r = 0$ and $s^f | M$. As a result, s^e divides $\gcd(M, n)$. Since the probability that $s \nmid a_2$ is $1 - 1/s$, the probability of $d \neq 1$ is as high as that the full power s^e is in d.

The isomorphism between $\langle P \rangle$ and μ_n in Step 4 is from the following theorem.

Theorem 3.15. *Suppose $f : \langle P \rangle \to \mu_n$ is defined by $f(Q) = e_n(Q, R)$ for those $R \in E[n]$ in Step 2, then f is a group isomorphism.*

Proof. The reason why f is a homomorphism follows from the bilinearity of the Weil pairing. The existence of $R \in E[n]$ such that $e_n(Q, R)$ is a primitive n-th root of unity implies that f is surjective. Since $\langle P \rangle$ and μ_n are both of order n, we have f is injective. Therefore f is an isomorphism. □

Notice that the computation of the Weil pairing can be done in a probabilistic polynomial-time algorithm proposed by Miller [23]. The MOV attack then can be carried out in probabilistic subexponential-time. We will introduce the computation of the pairings in the appendix.

3.3 Tate Pairing Attack

Frey and Rück [4] showed that in some situations, the Tate pairing can be used to solve the ECDLP. This method is similar to the MOV attack which uses some kind of pairing to reduce the ECDLP to the DLP on F_{q^l}. The Tate pairing attack is generally faster than the MOV attack. The following theorem describes the existence of the Tate-Lichtenbaum Pairing. We can use it to construct an isomorphism from $\langle P \rangle$ to μ_n.

Theorem 3.16. *Let E be an elliptic curve over F_q. Suppose n is an integer such that $n | q-1$. Let $E(F_q)[n]$ denote the elements of $E(F_q)$ of order dividing n, and let $\mu_n = \{x \in F_q^* | x^n = 1\}$. Assume $E(F_q)$ contains an element of order n. Then there exist non-degenerate bilinear maps*

$$\langle \cdot, \cdot \rangle_n : E(F_q)[n] \times E(F_q)/nE(F_q) \to F_q^*/(F_q^*)^n$$

and

$$\tau_n : E(F_q)[n] \times E(F_q)/nE(F_q) \to \mu_n$$

Proof. The construction of the first pairing can be found in [37] 11.3. Since F_q^* is cyclic of order $q-1$, the $(q-1)/n$-th power map gives an isomorphism from $F_q^*/(F_q^*)^n$ to μ_n. Therefore, the second pairing is defined by

$$\tau_n(S, T) = \langle S, T \rangle_n^{(q-1)/n}.$$

□

The second pairing in this theorem is called the modified Tate-Lichtenbaum pairing. We will use this modified Tate-Lichtenbaum pairing τ_n since it gives a definite answer instead of a coset in F_q^* mod n-th powers. We will also write $\tau_n(S, T + nE(F_q))$ as $\tau_n(S, T)$. Now we are ready to construct an isomorphism from $\langle P \rangle$ to μ_n. First, we need the following lemma.

Lemma 3.17. *Let n be a prime with $n|q-1$, $n|N$, and $n^2 \nmid N$. Let P be a generator of $E(F_q)[n]$, then $\tau_n(P, P)$ is a primitive n-th root of unity.*

To compute k such that $Q = kP$, we have

$$\tau_n(P, Q) = \tau_n(P, kP) = \tau_n(P, P)^k.$$

This determines $k \pmod{n}$ by lemma 3.17. All computations can be done in F_q^*.

In comparison to the MOV attack, we can see that the Tate pairing attack does not need the constraint $n \nmid q - 1$, which is necessary in the MOV attack such that $E[n] \subseteq E(F_{q^l})$ for some l. In other words, the Tate pairing attack only needs one point of order n, rather than all of $E[n]$, to be in $E(F_{q^l})$. Therefore, if $n|q-1$, we can apply the Tate pairing attack. If $n \nmid q - 1$, choose l such that $n|q^l - 1$, we can apply both the MOV attack and the Tate pairing attack as long as l is not too large. Now we turn to the case of the supersingular curves. Recall that $E(F_q)$ is supersingular if and only if $a^2 = 0, q, 2q, 3q, 4q$. By Hasse's theorem and the Lagrange theorem, we have.

- If $a = 0$, then $n|q + 1$. We can take $l = 2$ such that

$$q^2 - 1 = (q + 1)(q - 1) \equiv 0 \pmod{n}.$$

- If $a^2 = q$, then $n|q + 1 \mp \sqrt{q}$. We can take $l = 3$ such that

$$q^3 - 1 = (q - 1)(q + 1 - \sqrt{q})(q + 1 + \sqrt{q}) \equiv 0 \pmod{n}.$$

- If $a^2 = 2q$, then $n|q+1 \mp \sqrt{2q}$. We can take $l = 4$ such that

$$q^4 - 1 = (q+1)(q-1)(q+1+\sqrt{2q})(q+1-\sqrt{2q}) \equiv 0 \pmod{n}.$$

- If $a^2 = 3q$, then $n|q+1 \mp \sqrt{3q}$. We can take $l = 6$ such that

$$q^6 - 1 = (q+1)(q-1)(q^2+q+1)(q+1+\sqrt{3q})(q+1-\sqrt{3q}) \equiv 0 \pmod{n}.$$

- If $a^2 = 4q$, then $n|q+1 \mp 2\sqrt{q}$. We can take $l = 1$, since

$$(q-1)^2 = (q+1+2\sqrt{q})(q+1-2\sqrt{q}) \equiv 0(\text{mod } n).$$

  This implies $q - 1 \equiv \pmod{n}$.

We can always take $l \leq 6$ in these cases, so the supersingular curves is not secure under the MOV and the Tate pairing attack.

We close this section with an easy example.

Example 3.18. Consider the elliptic curve $E : y^2 = x^3 + 16x + 27$ over the field F_{29}. An element of order 7 is given by $P = (21, 24)$. We want to solve the ECDLP.

$$Q = (9, 1) = kP = k(21, 24).$$

Let $D_P = [P] - [\infty]$ and let $D_Q = [Q + R] - [R]$, where $R = (13, 5)$. We apply Miller's algorithm to compute

$$\tau_7(P, Q) = \langle P, Q\rangle_7^{(29-1)/7} = (-2)^4 \equiv 16 \pmod{29}.$$

A similar calculation shows

$$\tau_7(P, P) = \langle P, P\rangle_7^{(29-1)/7} = 8^4 \equiv 7 \pmod{29}.$$

Consequently

$$\tau_7(P, P)^k = \tau_7(P, Q) \Rightarrow 7^k \equiv 16 \pmod{29}.$$

We get $k \equiv 5 \pmod{7}$. The detail of the computation can be found in the appendix.

3.4 Weil Descent

The Weil descent method applies to elliptic curves over the field extensions F_{q^s} over F_q for some $s > 1$, where q is a prime or prime power. Although it also works for the field of odd characteristic, we will only concern the case of characteristic two. This method was first proposed by Frey [5], then Galbraith and Smart [7] detailed that how this method might apply to the ECDLP. Finally, the GHS attack, named after Gaudry, Hess and Smart [9], gave a complete description of reducing the ECDLP to the discrete logarithm problem on a Jacobian of a hyperelliptic curve over F_q. Since there exist subexponential-time algorithms to solve the DLPs in high-genus curves, this gives a possible method against the ECDLP. First, we give some definitions.

Definition 3.19. A hyperelliptic curve C of genus g over F_q is defined by a non-singular equation

$$v^2 + h(u)v = f(u),$$

where $h, f \in F_q[u]$, $deg(f) = 2g + 1$, and $deg(h) \leq g$.

The definitions of divisors and rational functions on a hyperelliptic curve are similar to the definitions on an elliptic curve as we have mentioned in section 3.1.2.

Definition 3.20. Let $Div^0(C)$ be the set of all divisors of degree 0 of a hyperelliptic curve. The set of all principal divisors, denoted by $Pic(C)$, is a subgroup of $Div^0(C)$. The Jacobian J of C is defined by $J(C) = Div^0(C)/Pic(C)$.

Suppose F_{q^s} is a field extension of F_q, where $q = 2^l$ for some integers s and l. We assume the curve given by

$$E : y^2 + xy = x^3 + ax^2 + b \text{ where } a \in \{0, 1\}, b \in F_{q^s}^*.$$

This kind of curves is called the *Koblitz curves*, which is widely used in elliptic curve cryptosystems. We will focus on these curves, but remark that it can be extended to general cases.

The first step is to construct the Weil restriction of scalars of $E(F_{q^s})$. Choose a basis of F_{q^s} over F_q. Since x, y, and b belong to F_{q^s}, we can write them in expansions of this basis. After substituting into the original Weierstrass equation and equating the coefficient of each term of the basis, we obtain s equations with $2s$ variables over F_q. These s equations form an affine variety of dimension s over F_q, denoted by $W_{F_{q^s}/F_q}$. The variety $W_{F_{q^s}/F_q}$ is then intersected with $s-1$ chosen hyperplanes to get a hyperelliptic curve C with genus g over F_q.

In addition, the GHS attack constructs an explicit group homomorphism form $E(F_{q^s})$ to $J(C)$. Now we can translate the ECDLP to the DLP on $J(C)$. However, this method only works for a significant proportion of all elliptic curves over F_{q^s}. It depends on the resulting genus g of the curve C. If g is too small, the Jacobian $J(C)$ contains no subgroup of order n. If g is too large, the computations in $J(C)$ will be an infeasible work. The following theorem determines g. Define $\sigma : F_{q^s} \to F_{q^s}$ be the q-th power Frobenius automorphism.

Theorem 3.21. (Gaudry, Hess, and Smart [9]) *The genus of C is equal to either 2^{m-1} or $2^{m-1}-1$, where m is derived as follows. Let $b_i = \sigma^i(b)$, then m is given by*

$$m = m(b) = \dim_{F_2}(\mathrm{Span}_{F_2}\{(1, b_0^{1/2}), \ldots, (1, b_{s-1}^{1/2})\}$$

There are some algorithms which can be used to solve the DLP on $J(C)$ such as the Pollard method [25], the Gaudry's algorithm [11], and Enge and Gaudry's algorithm [3]. We remark that the GHS attack is *successful* if the genus g of C is small enough so that either Gaudry's algorithm, or Enge and Gaudry's algorithm is more efficient than the Pollard method. After comparing their expected running time, we say that the GHS attack fails if $q^g \geq 2^{1024}$ or $g = 1$. For the case $q = 2$, these conditions translate to $m \geq 11$ or $m = 1$.

Menezes and Qu [19] proved that the smallest value $m(b)$ in Theorem 3.21 is $M(s) = ord_s(2) + 1$ where $ord_s(2)$ is the multiplicative order of 2 modulo s. They found $M(s) \geq 17$ for all primes $s \in [160, 600]$ when $q = 2$. Consequently, the GHS attack is infeasible for all elliptic curves defined over F_{2^s}, where s is a prime in the range of $160 \leq s \leq 600$.

An *isogeny* is a rational map between curves E_1 and E_2 such that $|E_1| = |E_2|$. Galbraith, Hess, and Smart [10] extended the GHS attack by using isogenies. We call it the generalized GHS attack. If the resulting value $m(b)$ of a curve E over F_{2^s} is large, the idea is to find an isogenous curve E' which has small value m. Then the ECDLP on E can be mapped to the ECDLP on E', and the ECDLP on E' can be solved by GHS attack. The authors not only gave how these isogenies can be constructed but also showed that F_{q^7} is weak under the generalized GHS attack.

Further analysis of the GHS attack has been done by looking over the finite fields suggested in many standards. Jacobson, Menezes, and Stein [15] examined the field extension $F_{2^{155}}$ over F_5 and concluded that only 2^{33} of 2^{156} isomorphism classes of elliptic curves can be attacked by this strategy. The probability of finding one curve threaten by the GHS attack is rather small. However, the generalized GHS attack increases this probability from $1/2^{122}$ to $1/2^{52}$. We call a field F_{2^s} *partially weak* if the ECDLP can be solved faster than the Pollard method for only a non-negligible proportion of all elliptic curves. So, the field $F_{2^{155}}$ should be considered weak. Finally, Menezes and Teske [18] concluded that the fields $F_{2^{5l}}$ and $F_{2^{6l}}$ are weak.

The fields $F_{2^{3l}}$, $F_{2^{7l}}$, and $F_{2^{8l}}$ for some l are partially weak under the generalized GHS attack.

4 Other Attacks

In this section, we discuss the index calculus method and the xedni calculus method which both fail to solve the ECDLP. However, there are interesting ideas beyond them, so we give a brief introduction to them. In the third part of this section, we introduce the idea of summation polynomial. The author establishes a connection between the operations in the elliptic curve group and explicit modular multivariate polynomial equations. These ideas give us some new thoughts for further research.

4.1 Index Calculus on the ECDLP

It is well known that the discrete logarithm problem in the multiplicative group F_p^* of a finite field can be solved in subexponential time using the index calculus method, which has been discovered in 1920's. Miller [22] noticed that it is better to use the elliptic curve group instead of F_p^* in a cryptosystem, since the index calculus method is extremely unlikely able to solve the ECDLP. The main reasons are "rank/height obstruction" and "lifting obstruction". The first one is the problem of finding an elliptic curve with large number of small rational points. The second one is the problem of lifting a point in $E(F_p)$ to a point in $E(\mathbb{Q})$. We remark that the lifting here can be thought as a lifting into the p-adic integer $\mathbb{Z}_p$, then applying the reduction modulo map. We will introduce the index calculus attack on the ECDLP and discuss why it fails, which comes from Silverman's work [33].

1. Choose an elliptic curve $E(\mathbb{Q})$ which reduces to $E(F_p)$. It has a large number of independent rational points, say $\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_r \in E(\mathbb{Q})$.

2. Compute the multiples $P, 2P, 3P \ldots$ in $E(F_p)$. For each j, try to lift jP to a rational point $\tilde{jP}$ in $E(\mathbb{Q})$. That is, $jP \equiv \tilde{jP} \pmod{p}$. If this is successful,

then write $\tilde{jP}$ as a linear combination

$$\tilde{jP} = \sum_{i=1}^{r} n_i \tilde{P_i} \text{ in } E(\mathbb{Q}).$$

Reducing the coordinates of the points modulo p yields a desired relation

$$jP = \sum_{i=1}^{r} n_i P_i \text{ in } E(F_p).$$

3. After r of the jP's have been lifted, we have r linear equations

$$j = \sum_{i=1}^{r} n_i \log_P(P_i).$$

Each $\log_P(P_i)$ can be solved by these r linear equations.

4. Try to lift $Q, Q+P, Q+2P, Q+3P, \ldots,$ to $E(\mathbb{Q})$. We say that $Q+jP$ is lifted to $\tilde{T_j} \in E(\mathbb{Q})$. Write

$$\tilde{T_j} = \sum_{i=1}^{r} m_i \tilde{P_i} \text{ in } E(\mathbb{Q})$$

Then

$$\log_P Q + j = \sum_{i=1}^{r} m_i \log_P(P_i) \text{ in } E(F_p)$$

implies that we can recover the desired value of $\log_P Q$ by these $\log_P(P_i)$.

The above algorithm works well if we can find a lifting elliptic curve $E(\mathbb{Q})$ which has a lot of independent points with small number of bits need to write down for the coordinates. Unfortunately, Silverman and Suzuki in [33] gave an analysis which showed that this kind of curves is rare. This is the first rank/height obstruction we have mentioned above. Now we turn our discussion to the elliptic curve over $\mathbb{Q}$. Let the number r in the above algorithm be the rank of the elliptic curve $E(\mathbb{Q})$. Recall that the height of a rational number $t/s \in \mathbb{Q}$ is defined by $H(t/s) = \max(|t|, |s|)$. The canonical height of a point $P \in E(\mathbb{Q})$ is then defined by

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{n^2} \log H(x_{nP}),$$

with associated inner product for $P, Q \in E(\mathbb{Q})$

$$\langle P, Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Suppose $N(E,B)$ is the number of points with bounded height B in $E(\mathbb{Q})$. This value is estimated by counting the lattice points in $\mathbb{R}^r$ relative to the canonical height inner product. Under some reasonable assumption, based on the data from Mestre [21], the result follows [33].

Heuristic Bound. *Based on the numerical data contained in [21] and the above theoretical analysis, it appears to be possible to use Mestre's method to produce elliptic curves $E(\mathbb{Q})$ so that the number of rational points*

$$N(E,B) = \#\{P \in E(\mathbb{Q}) | H(x_P) \leq B\}$$

in $E(\mathbb{Q})$ grows like

$$N(E,B) \approx \frac{1}{\sqrt{\pi r}} \left(\frac{20\pi e \log B}{r \cdot \log |\Delta|} \right)^{r/2},$$

where Δ is the discriminant of the minimal Weierstrass equation. Further, it is probably not possible to find elliptic curves such that $N(E,B)$ grows significantly faster than this rate.

It is impossible to get $N(E,B)$ large unless one chooses

$$\log B \gg r \log |\Delta|$$

in this formula. If we make r large, then the value of B is also enormous. It does not help us solving an ECDLP, since we want B to be small and $N(E,B)$ to be large.

Silverman and Suzuki further estimated the quantity $\log|\Delta|$ by some experiments. They chose an elliptic curve over a fixed finite field and use Mestre's method [21] to look for lifts of this curve. Finally, they looked for independent integral points on the ones having small discriminant among all lifts. After observing the relevant data, they had an approximation on $\log|\Delta|$ which grows linearly in both $\log p$ and $r \log r$. Under the assumption of $N(E, B) \geq p/2^{10}$, they found that the value of r minimizes the lower bound. If $p \geq 2^{160}$, the rank r is 180 such that the lower bound $B \geq 2^{7830.74} \approx p^{48.94}$. Note that no curves of rank ≥ 24 are currently known [33]. Another explanation can be found in [13]. We will introduce it at the end of the next section.

Even if we have a curve with large number of independent points of bounded height, how do we lift a point in $E(F_p)$ to a point in $E(\mathbb{Q})$? A natural choice is to lift points p-adically. That is, lift mod p^2 first, then lift mod p^3, etc. However we have p possible lifts at each step but do not know which leads to an actual point in $E(\mathbb{Q})$. To check all the possibilities is clearly an infeasible task. This is the lifting obstruction we have mentioned. Even if there is another method for lifting, the numbers involved are so large that it seems unlikely that the lifting problem has a practical solution. These problems cause the failure of the index calculus method to the ECDLP.

4.2 Xedni Calculus on the ECDLP

The index calculus method fails to solve an ECDLP because of the height/rank obstruction and the lifting obstruction. Silverman presented a new attack in [34] which avoid these two obstructions. Instead of lifting the elliptic curve $E(F_p)$ and the related points jP, his idea is to lift the points first, then construct an elliptic curve $E(\mathbb{Q})$ which passes through these points. That is why it is called the "xedni calculus" method. Eventually, the lifting problem becomes a linear algebra problem. However, this attack later been proved not practical [14] in solving the ECDLP by a work group at the University of Waterloo. In this section, we will introduce it for a complete overview of all possible attacks, then explain the reason of its failure.

Suppose $P_1, P_2, \ldots, P_r \in E(F_p)$ are of the form $P_i = s_iP - t_iQ$, where s_i, t_i are randomly chosen in $[1, n-1]$ for $i = 1, \ldots, r$. We can also choose $Q_1, \ldots, Q_r$ with integer coordinates by using projective coordinates such that $P_1, P_2, \ldots, P_r$ are the reduction modulo p points of $Q_1, \ldots, Q_r$. Our main goal is to construct an elliptic curve $E(\mathbb{Q})$ passing through $Q_1, \ldots, Q_r$. If the points $Q_1, \ldots, Q_r$ are dependent, there is a nontrivial relation

$$n_1Q_1 + n_2Q_2 + \ldots + n_rQ_r = \infty$$

for some nonzero n_i. By taking modulo p, we get

$$(n_1(t_1P - s_1Q)) + (n_1(t_1P - s_1Q)) + \ldots + (n_r(t_rP - s_rQ)) = \infty.$$

That is, $\sum_{i=1}^{r} n_it_iP = \sum_{i=1}^{r} n_is_iQ = \sum_{i=1}^{r} n_is_i(kP)$. Consequently,

$$k \equiv \sum n_it_i / \sum n_is_i \pmod{n}.$$

The key point to this method is the dependence of the lifting points $Q_1, \ldots, Q_r$. Silverman introduces a method related to a conjecture called the Birch-Swinnerton-Dyer Conjecture. If we write $N_l = |E(F_l)| = l + 1 - a_l$ where l is a prime and a_l is the trace related to l, the conjecture comes from the idea of measuring the number of points N_l as l varies. One forms the product

$$\prod_l \frac{l}{N_l} = \prod_l \frac{l}{l+1-a_l} = \frac{1}{1 - a_l \cdot l^{-1} + l \cdot l^{-2}},$$

which is formally equal to the value of the Euler product $L(E,s)$ at $s=1$ (see [32], P.362). This conjecture states that $L(E,s)$ vanishes at $s=1$ if and only if the rank of the group $E(\mathbb{Q})$ is positive. In addition, the rank is equal to the order of the zero at $s=1$. Even some of important partial results have been proved in support of this fundamental conjecture; it remains a very difficult unsolved problem in its general form [14].

If we expect the rank of an elliptic curve $E(\mathbb{Q})$ being large, so is the order of zero at $s=1$. It would be reasonable to expect that the first few terms of this product are small. Thus, the first few numbers N_l are large. Mestre [21] applies this idea to generate curves with large rank, but Silverman uses it in an opposite way. He expects $|E(F_l)|$ being as small as possible such that $|E(F_l)| = l+1-\lfloor 2\sqrt{l}\rfloor$ for the first few primes l. The resulting rank of $E(\mathbb{Q})$ is smaller than the expected rank. We hope that this will increase the dependence of the lifting points. We call it the reverse Mestre conditions.

The problem of constructing this elliptic curve over $\mathbb{Q}$ will be a linear algebra problem. We consider a general cubic curve which can be determined by no more than 9 points in projective coordinates. For any set of r triples $P_i = [x_i, y_i, z_i]$, define an r-by-10 matrix $B = B(P_1, \ldots, P_r)$ of cubic monomials.

$$B = \begin{pmatrix} x_1^3 & x_1^2y_1 & x_1y_1^2 & y_1^3 & x_1^2z_1 & x_1y_1z_1 & y_1^2z_1 & x_1z_1^2 & y_1z_1^2 & z_1^3 \\ x_2^3 & x_2^2y_2 & x_2y_2^2 & y_2^3 & x_2^2z_2 & x_2y_2z_2 & y_2^2z_2 & x_2z_2^2 & y_2z_2^2 & z_2^3 \\ \vdots & & & \ddots & & & \ddots & & & \vdots \\ x_r^3 & x_r^2y_r & x_ry_r^2 & y_r^3 & x_r^2z_r & x_ry_rz_r & y_r^2z_r & x_rz_r^2 & y_rz_r^2 & z_r^3 \end{pmatrix}.$$

Therefore, the coefficient of the cubic curve can be found by computing the kernel of the matrix B. The associated cubic curve will be of the form

$$u_1x^3 + u_2x^2y + u_3xy^2 + u_4y^3 + u_5x^2z + u_6xyz + u_7y^2z + u_8xz^2 + u_9yz^2 + u_{10}z^3 = 0.$$

Now we give a summary of the xedni calculus algorithm [34]. The optional steps are omitted.

Step 1. Choose an integer r with $2 \leq r \leq 9$ and an integer M which is a product of small primes $l \in [7, 100]$. We shall assume $p \nmid M$. The integer r is the number of points to be lifted.

Step 2. Choose r points $P_{M,i} = [x_{M,i}, y_{M,i}, z_{M,i}]$ for $1 \leq i \leq r$, where the coordinates are integers. These points satisfy:

- The first four points are $[1, 0, 0], [0, 1, 0], [0, 0, 1], [1, 1, 1]$.
- For every prime $l|M$, the matrix $B = B(P_{M,1}, \ldots, P_{M,r})$ has the maximal rank modulo l.

These points $P_{M,i}$ can be found by choosing $P_{l,i}$ for each $l|M$, then we use the Chinese Remainder Theorem. Also choose a mod-M coefficient vector $(u_{M,1}, \ldots, u_{M,10})$ that is in the kernel of the matrix B such that the reducing modulo l curve $E(F_l)$ has fewest points for each $l|M$. We will get a cubic curve with coefficients $u_{M,i}$.

Step 3. Choose r random pairs of integers (s_i, t_i) satisfying $1 \leq s_i, t_i \leq n$ for $i = 1, \ldots, r$. Compute the points $P_{p,i}$ by $P_{p,i} = s_i P - t_i Q \in E(F_p)$.

Step 4. Make a change of variable so that the first four points of $P_{p,i}$ become $P_{p,1} = [1, 0, 0]$, $P_{p,2} = [0, 1, 0]$, $P_{p,3} = [0, 0, 1]$ and $P_{p,4} = [1, 1, 1]$. In this case $u_{p,i}$ for $i = 1, \ldots, r$ are the coefficients of the resulting equation for $E(F_p)$.

Step 5. Use the Chinese Remainder Theorem to find $u'_1, \ldots, u'_{10}$ satisfying

$$u'_i \equiv u_{p,i} \pmod{p} \text{ and } u'_i \equiv u_{M,i} \pmod{M}$$

for $i = 1, \ldots, r$.

Step 6. Lift the chosen points to $\mathbb{P}^2(\mathbb{Q})$. In other words, choose points $P_i = [x_i, y_i, z_i]$ for $i = 1, \ldots, r$ with integer coordinate satisfying

$$P_i \equiv P_{p,i} \pmod{p} \text{ and } P_i \equiv P_{M,i} \pmod{M}.$$

In particular, $P_1 = [1, 0, 0]$, $P_2 = [0, 1, 0]$, $P_3 = [0, 0, 1]$, and $P_4 = [1, 1, 1]$.

Step 7. Form the matrix $B(P_1, \ldots, P_r)$ by using the r points P_i in Step 6. Find a solution $u = (u_1, u_2, \ldots, u_n)$ such that $Bu = 0$ and $u_i \equiv u_i' \pmod{Mp}$. Let C_u denote the associated cubic curve.

Step 8. Make a change of coordinates to put C_u into standard minimal Weierstrass form with the point $P_1 = [1, 0, 0]$ the point at infinity. Write the resulting equation as

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

with $a_1, \ldots, a_6 \in \mathbb{Z}$, and let $Q_1, Q_2, \ldots, Q_r$ denote the image under this change of variable.

Step 9. Test the points $Q_1, \ldots, Q_r$ for the dependence. This process can be done by using the Descent Method or the Height Method (see [34]). If they are independent, return to Step 2 or 3.

Step 10. Compute

$$s = \sum_{i=1}^{r} n_i s_i \text{ and } t = \sum_{i=1}^{r} n_i t_i,$$

then $\log_P Q \equiv s^{-1}t \pmod{n}$, provided it exists. Otherwise, return to Step 2 or Step 3.

Jacobson, Koblitz, Silverman, Stein, and Teske [14] combined the theoretical and empirical points of view to show that the xedni calculus is impractical for p in the range used in elliptic curve cryptography today. On the theoretical side the main idea is the following:

Lemma 4.1. *Assume that* $\log|\Delta| \geq C_1 \max_{i=1,\ldots,r} \hat{h}(P_i)$ *for the lifted curves in the xedni algorithm, where* Δ *is the discriminant of the lifted curve,* P_i *are the lifted points,* $\hat{h}$ *is the canonical logarithmic height, and* C_1 *is a positive absolute constant. Then, under Lang's conjecture, if the lifted points are dependent, then they satisfy a nontrivial relation with coefficients bounded from above by an absolute constant* C_2*.*

This lemma is proved by directly counting the number of points of the subgroup which is spanned by the lifted points $P_1, \ldots, P_r$. The canonical logarithmic height of the points in this subgroup are bounded above by some constant B. Followed by a conjecture of Lang which states that there exists a positive absolute constant C_3 such that for all non-torsion points S, we have

$$m = \min \hat{h}(S) > C_3 \log|\Delta|.$$

Consequently, the constant C_2 can be found by the following inequality

$$C_2 \geq Tc(r-1)\left(\frac{r}{2}\right)^{r-1}(C_1)(C_3)^{-(r-1)/2}$$

where $T \leq 16$ and c is a function related to r. Since $1 \leq r \leq 9$, we can determine an absolute constant C_2.

If there is any relation among the lifted points $P_1, \ldots, P_r$, then these points can be reduced modulo p to get a relation of the original points $P_{p,1}, \ldots, P_{p,r}$ with the same coefficients. Hence, if the coefficients of the relation of the lifted points are bounded by some constant C_2, then so is true for the original points. Thus, if those original points $P_{p,i}$ do not satisfy any relation with coefficients less than the upper bound in the lemma, then the lifted points will be independent regardless how we use the reverse Mestre conditions. Therefore, the probability of success of the xedni calculus is less than the probability of the original points $P_{p,1}, \ldots, P_{p,r}$ satisfying a relation with coefficients bounded by C_2. Consider the map from r-tuples of integers less than the absolute value of C_2 to $E(F_p)$ given by $(n_1, \ldots, n_r) \mapsto n_1 P_{p,1} + \ldots + n_r P_{p,r}$. The image is a set of $\approx (2C_2)^r$ randomly distributed points. The probability that the image contains ∞ is approximately $(2C_2)^r/p$. This proves the following theorem with $C_0 = (2C_2)^r$.

Theorem 4.2. *Under certain plausible assumptions, there exists an absolute constant C_0 such that the probability of success of the xedni algorithm in finding a discrete logarithm on an elliptic curve over F_p is less than C_0/p.*

The quantity C_0 determines whether the xedni calculus is successful or failed, so we need to examine the constant C_0. Jacobson, Koblitz, Silverman, Stein, and Teske [14] estimated C_0 under some reasonable assumption which is related to the number r and the coefficients of the curve. They derived the following result.

r	rough value for C_0
2	10^4
3	10^{12}
4	10^{23}
5	10^{38}
6	10^{54}
7	10^{65}
8	10^{84}
9	10^{100}

Since $p \approx 10^{50}$ in practical elliptic curve cryptosystems, this result rules out the use of the algorithm with $r \leq 5$. For the case $r = 6, 7, 8, 9$, the authors took some experiments whose purpose is to see which parameter has an impact on the probability of dependence. They found that these theoretical bounds are far too generous. Furthermore, in the absence of other considerations, the reverse Mestre conditions do increase the likelihood of dependence. Unfortunately, they also cause the discriminant increase, and this makes the probability of a dependence decrease. This means the net effect of the reverse Mestre condition is doing more harm than help [14].

Another explanation is given by M. D. Huang, K. Kueh, and K. S. Tan [13] who made a easier description of Theorem 4.2. Suppose D is the minimal discriminant of the lifted curves $E(\mathbb{Q})$. The probability of success of the xedni calculus is bounded by

$$\frac{2^{O(r^3)}(h/\log|D|)^{O(r^2)}}{p}$$

where the lifted points are $P_0, \ldots, P_r$ in $\langle P \rangle$ with the canonical heights bounded by h. In order to achieve a subexponential running time $O(e^{c(\log p)^{1/2}(\log\log p)^{1/2}})$, it is necessary that $r^2 \log h > c' \log p$ for some constant c'. Even if we allow the lifted points with height about $e^{c(\log p)^{1/2}(\log\log p)^{1/2}}$, the number of $r+1$ lifted points still needs to be at least in the order of $(\log p)^{1/4}$ as p grows. This is true regardless how we use the reverse Mestre's conditions. In addition, we require the number of lifted points being at most 9. So the probability of success tends to zero asymptotically. Hence, the xedni calculus cannot work in subexponential time asymptotically.

For the index calculus, the fact that the rank of $E(\mathbb{Q})$ need to grow at least $(\log p)^{1/4}$ as p grows is already a difficulty which leads to failure.

4.3 Semaev's Summation Polynomials

The main idea behind the Semaev's summation polynomials [30] is to construct some explicit modular multivariate polynomial equations which are related to the summations of an elliptic curve group. Once these modular multivariate polynomial equations can be solved with bounded solutions in polynomial time or subexponential-time, we can collect some relations. The ECDLP can be solved by the reduction of these relations. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a field K of characteristic not equal to $2, 3$. We give the definition of the summation polynomial.

Definition 4.3. For any natural number $l \geq 2$, a polynomial $f_l = f_l(X_1, X_2, \ldots, X_l)$ in l variables is called a *summation polynomial* if it satisfies the following property. Let $x_1, x_2, \ldots, x_l \in \overline{K}$, then $f_l(x_1, x_2, \ldots, x_l) = 0$ if and only if there exist $y_1, y_2, \ldots, y_l \in \overline{K}$ such that $(x_i, y_i) \in E(\overline{K})$. Furthermore,

$$(x_1, y_1) + (x_2, y_2) + \ldots + (x_l, y_l) = \infty$$

is in the group $E(\overline{K})$.

The following theorem constructs the summation polynomials and lists some properties.

Theorem 4.4. *The polynomial f_l may be defined by $f_2(X_1, X_2) = X_1 - X_2$,*

$$f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2((X_1 + X_2)(X_1 X_2 + a) + 2b)X_3$$

$$+((X_1 X_2 - a)^2 - 4b(X_1 + X_2)),$$

and $f_l(X_1, X_2, \ldots, X_l) = Res_X(f_{l-j}(X_1, \ldots, X_{l-j-1}, X), f_{j+2}(X_{l-j}, \ldots, X_l, X))$ for any $l \geq 4$ and $l - 3 \geq j \geq 1$.

Furthermore, the polynomial f_l is symmetric of degree 2^{l-2} in each variable X_i for any $l \geq 3$.

The polynomial f_l is absolutely irreducible and

$$f_l(X_1, X_2, \ldots, X_l) = f_{l-1}^2(X_1, \ldots, X_{l-1}) X_l^{2^{l-2}} + \ldots$$

for any $l \geq 3$.

Proof. See [30] □

Now we turn to an ECDLP in $E(F_p)$, where E is given by $E : y^2 = x^3 + ax + b$ over F_p. We fix some natural number $l \geq 2$. Randomly choose u, v such that $R = (x, y) = uP + vQ$ in $E(F_p)$, then substitute x into the summation polynomial f_{l+1}. We get a modular equation

$$f_{l+1}(X_1, \ldots, X_l, x) \equiv 0 \pmod{p}$$

in variables $X_1, \ldots, X_l$. The author claimed that very likely this equation has a solution $x_1, x_2, \ldots, x_l$, where x_i are integers bounded by $p^{1/l+\delta}$ for some $\delta > 0$ or x_i are rational numbers with the numerator and the denominator bounded by $p^{1/(2l)+\delta}$. If there is an algorithm which solves this equation, it implies that we can find a relation

$$(x_1, y_1) + (x_2, y_2) + \ldots + (x_l, y_l) = uP + vQ$$

for some $y_1, y_2, \ldots, y_l$ in F_p or F_{p^2}. We then combine this relation with another relation

$$(x_1, y_1) + (x_2, y_2) + \ldots + (x_{l'}, y_{l'}) = \infty$$

which comes from another summation polynomial

$$f_{l'}(X_1, X_2, \ldots, X_{l'}) \equiv 0 \pmod{p}$$

for some $l' \geq l$, provided its solutions bounded by $p^{1/l+\delta}$. Collect these relations as many as we can, then apply the Gaussian elimination (or other possible reductions) to these relations until the left hand side of the points equal to ∞. We obtain the relation $\infty = u'P + v'Q$ for some $u', v' \in [1, n-1]$. This gives the discrete logarithm

$$k \equiv (-u')(v')^{-1} \pmod{n}.$$

It needs about $p^{1/l+\delta}$ nontrivial solutions to find the logarithm. If finding a bounded solution to the summation polynomial f_l requires $t_{p,l}$ operations, then the complexity of the discrete logarithm problem in $E(F_p)$ is roughly

$$t_{p,l}p^{1/l+\delta} + p^{2/l+2\delta}$$

operations [30].

This idea gives some possibility that solving an ECDLP is faster than the Pollard's method. The main problem is to solve the explicit modulo multivariate polynomial equations with bounded solutions. However, the author did not explain how to solve this kind of equations. Although we have some methods to solve systems of multivariate equations, such as the computation of Gröbner basis or the XL method for sparse equations, we cannot apply these methods since we have only one equation. Suppose the elliptic curve is defined over the finite field F_{p^l} for some $F_{p^l} \cong F[t]/(f(t))$ where f is an irreducible polynomial of degree l. The situation becomes easy since we can write the x-coordinate of $R = uP + vQ$ in the form of $x = x_0 + x_1 t + \ldots + x_{l-1}t^{l-1}$. Substituting it into the summation polynomial f_{l+1}, we have

$$f_{l+1}(X_1, X_2, \ldots, X_l, x) = 0.$$

We rewrite it as an equation of polynomials in t with reducing modulo $f(t)$, then the equation becomes

$$\sum_{i=0}^{l-1} \phi_i(X_1, X_2, \ldots, X_l)t^i = 0$$

for some polynomials ϕ_i. Each coefficient of t^i equals to 0, so we have l equations in l variables. This might gives solutions to $f_{l+1} \equiv 0 \pmod{p}$. The author expected that it is a polynomial time or a subexponential-time algorithm which yields a good time complexity in solving an ECDLP [30].

4.4 Further Results

P. Gaudry [8] proposed an index calculus algorithm to the discrete logarithm problem on general abelian varieties by using summation polynomials to simplify calculations. He applied his method to the Weil restriction of the elliptic curves and the hyperelliptic curves over small degree extension fields. He got a smaller complexity than Pollard's method.

Claus Diem [2] further showed that an ECDLP can be solved if one can decide whether certain systems of multivariate quadratic polynomial equations have a solution in the algebraic closure of the underlying field K. The main idea is the natural correspondence between the operations in $E(K)$ and the operations in other algebraic structure.

Let $P_1, P_2 \in E(K)$. If $P_1 + P_2 = R$, there exists a function $f \in K(E)$ such that $div(f) = [P_1] + [P_2] - [R] - [\infty] \in Div^0(E)$ by Property 3.7. It is equivalent that there exists a function f which satisfies

$$f \in \mathcal{L}([R] + [\infty] - [P_1] - [P_2]) \subset K(E)$$

and

$$f^{-1} \in \mathcal{L}([P_1] + [P_2] - [R] - [\infty]) \subset K(E)$$

where $\mathcal{L}(D)$ is the Riemann-Roch space corresponding to some $D \in Div(E)$. Let $t = (\log_2 n) + 1$ and let s be an integer with $3 \leq s \leq t - 2$. By the above property, we obtain a bijection between

$$\left\{ \underline{e} \in 0, 1^{\{0,\ldots,t-1\}} | \sum_{i=0}^{t-1} e_i 2^i P = Q \wedge |\underline{e}| = s \right\}$$

and

$$\left\{ \overline{f} \in K(E)^*/K^* \;\middle|\; \begin{array}{c} f \in \mathcal{L}([Q] + (s-1)[\infty]) \\ \wedge \\ f^{-1} \in \mathcal{L}(\sum_{i=0}^{t-1}[2^i P] - [Q] - (s-1)[\infty]) \end{array} \right\}.$$

where $|\underline{e}| = \sum_{i=0}^{t-1} e_i$. By the Riemann-Roch Theorem, the space $\mathcal{L}(D)$ is a K-vector space, so we can write the functions f and f^{-1} in the linear combination of the related basis respectively.

Finally, let $K(E) = K(X)[Y]$ where Y satisfies an equation of degree 2 over the rational function field, expand "everything" with respect to the basis $1, Y$, and compare the coefficients of the polynomials of the basis with respect to $\mathcal{L}(D)$. We will have a system of quadratic equations with $t - 1$ unknowns. The number of equations depends on the polynomials' degree of the basis of Riemann-Roch spaces.

Once one can find a solution to the system, one can construct the class $\overline{f} \in K(E)^*/K^*$ corresponding to the solution and check whether f has a zero at 2^iP for $i = 0, 1, \ldots, t-1$. Then the corresponding tuple $\underline{e} \in \{0,1\}^{\{0,\ldots,t-1\}}$ with $(\sum_{i=0}^{t-1} e_i 2^i) \cdot P = Q$ can be derived. Therefore, we can solve the ECDLP if we can solve the above quadratic systems.

We observe that the original ECDLP in the research has been transformed into a problem of solving multivariate polynomial equations. This means some thoughts behind the elliptic curve cryptography, a public key cryptography, is getting close to the multivariate polynomial equations which often appears in the symmetric key cryptography. Further research may lead to the construction of these systems of multivariate polynomials. It requires finding an algebraic structure which is related to the operations on an elliptic curve with a computable basis. Another way may lead to a deeper study of the algorithms of solving these systems, such as the computation of Gröbner basis, the implementation of the F_4, F_5 algorithms or the XL algorithm.

5 Conclusions

After looking back the possible methods to solve an ECDLP in modern elliptic curve cryptography, we conclude some criteria. In order to have a difficult ECDLP, the parameter of an elliptic curve should be chosen to satisfy the following properties. Assume

$$N = |E(F_q)| = n \cdot s$$

where n is the order of the base point P, then we have the following criteria.

- n should be a prime
- $n \geq 2^{160}$
- $n \neq p$
- n should not divide $q^l - 1$ for $l \leq 30$
- q should be a large prime or a prime power of two

Since there exist efficiently computable endomorphisms to decrease the security of an ECDLP by constructing an equivalence relation among $E(F_q)$, this reduction should be taken into account. For example, we have mentioned Koblitz curves and other special type of curves (Example 2.1). Therefore, we need to choose the parameters carefully in order to reach the desired security.

On the opposite side, we conclude the criteria of weak curves and weak fields.

- If n is not a prime, we can reduce to ECDLPs of subgroups of $\langle P \rangle$.
- If $n < 2^{160}$, the ECDLP can be solved by Pollard's method.
- The elliptic curve is prime-field-anomalous.

- If $n = p$, the ECDLP can be solved by Semaev's method.

- The elliptic curve is supersingular.

- If n divide $q^l - 1$ for some $l \leq 30$, we can apply the pairing attacks.

- The base field of the form $F_{2^{5l}}$ or $F_{2^{6l}}$ for some l is weak under generalized GHS attack.

- The base field of the form $F_{2^{3l}}$, $F_{2^{7l}}$, or $F_{2^{8l}}$ for some l is partially weak under the generalized GHS attack.

To choose a situation where the ECDLP is hard, we should avoid these weak curves and base fields.

References

[1] I.F. Blake, G. Seroussi and N.P. Smart. *Elliptic curve in cryptography. Chapter VII* volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2000.

[2] C. Diem. *Systems of polynomial equations associated to elliptic curve discrete logarithm problems.* Preprint, 2004.

[3] A. Enge and P. Gaudry. *A general framework for subexponential discrete logarithm algorithms.* Rapport de Recherche Lix/PR/00/04, June 2000.

[4] G. Frey and H. Rück. *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves.* Mathematics of Computation, 62:865-874, 1994.

[5] G. Frey. *Applications of Arithmetical Geometry to Cryptographic Constructions.* Finite Fields and Applications, 128-161, Springer, 1999.

[6] R. Gallant, R. Lambert and S. Vanstone. *Improving the parallelized Pollard lambda search on anomalous binary curves.* Mathematics of Computation, 69:1699-1705, 2000.

[7] S. Galbraith, and N. Smart. *A Cryptographic application of Weil descent* Cryptography and Coding, (LNCS 1176) 191-200. Springer-Verlag, 1999.

[8] P. Gaudry. *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem.* Preprint, 2004.

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

[10] S. Galbraith, F. Hess, and N. Smart. *Extending the GHS Weil descent attack.* Advances in Cryptology-EUROCRYPT 2002 (LNCS 2332)[248], 29-44, 2002.

[11] P. Gaudry. *An algorithm for solving the discrete log problem on hyperelliptic curves.* Advances in Cryptology-EUROCRYPT 2000 (LNCS 1807), 19-34, 2000.

[12] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography.* Springer, 2003.

[13] M.-D. Huang, K. Kueh, and K.-S. Tan. *Lifting elliptic curves and solving the elliptic curve discrete logarithm problem.* ANTS (LNCS 877), 377-384, Springer-Verlag, 2000.

[14] M. Jacobson, N. Koblitz, J. Silverman, A. Stein, and E. Teske. *Analysis of the xedni calculus attack.* Design, Codes, and Cryptography, 20:41-64, 2000.

[15] M. Jacobson, A. Menezes and A. Stein. *Solving elliptic curve discrete logarithm problems using Weil descent.* Preprint, 2001.

[16] N. Koblitz, A. Menezes, Y. H. Wu, and R. Zuccherato. *Algebraic aspects of Cryptography.* Springer. 1998.

[17] M. Maurer, A. Menezes, and E. Teske. *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree.* LMS Journal of Computation and Mathematics, 5:127-174, 2002.

[18] A. Menezes and E. Teske. *Cryptographic implications of Hess' generalized GHS attack.* http://www.cacr.math.uwaterloo.ca/ajmeneze/research/html December, 2004.

[19] A. Menezes and M. Qu. *Analysis of the Weil descent attack of Gaudry, Hess and Smart.* Topics in Cryptology CT-RSA 2001 (LNCS 2020)[338], 308-318, 2001.

[20] A. Meneze, S. Vanstone and T. Okamoto. *Reducing elliptic curve logarithms to logarithms in a finite field.* IEEE Transactions on Information Theory, 39:1639-1646, 1993

[21] J.F. Mestre. *Formules explicites et minoration de conducteurs de varietes algebriques.* Compositio Math. 58(1986), 209-232.

[22] V. Miller. *Use of elliptic curves in Cryptography.* Advances in Cryptology CRYPTO '85. (LNCS 218) 417-426, Springer, 1986.

[23] V. Miller. *Short programs for functions on curves.* Unpublished manuscript, 1986.

[24] S. Pohlig and M. Hellman. *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance.* IEEE Transactions on Information Theory, 24:106-110, 1978.

[25] J. M. Pollard. *Monte Carlo methods for index computation (mod p).* Mathematics of Computation, 32, 918-924, 1978.

[26] T. Satoh and K. Araki. *Fermat quotients and the polynomial time discrete log algorithm for anomalous curve.* Commentarii Mathematici Universitatis Sancti Pauli, 47:81-92, 1998.

[27] R. Schoof. *Elliptic curves over finite fields and the computation of square roots mod p.* Mathematics of Computation. 44(170):483-494, 1985.

[28] R. Schoof. *Nonsingular plane cubic curves over finite fields.* Journal of Combinatorial Theory, A 46(1987), 183-211.

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

[30] I. Semaev. *Summation polynomials and the discrete logarithm problem on elliptic curves.* Preprint, February 5 2004.

[31] D. Shanks. *Class number, a theory of factorization, and genera.* 1969 Number Theory Institute, page 415-440. American Mathematical Society, Providence, RI, 1971.

[32] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag. GTM 106.

[33] J. Silverman and J. Suzuki. *Elliptic curve discrete logarithms and the index calculus.* Advances in Cryptology-ASIACRYPT '98(LNCS 1514)[352], 110-125, 1998.

[34] J. Silverman. *The xedni calculus and the elliptic curve discrete logarithm problem.* Designs, Codes, and Cryptography, 20:5-40, 2000.

[35] N. Smart. *The discrete logarithm problem on elliptic curve of trace one.* Journal of Cryptology, 12:193-196, 1999.

[36] P. Van Oorschot and M. Wiener. *Parallel collision search with cryptanalytic applications.* Journal of Cryptology, 12:1-28, 1999.

[37] L. Washington. *Elliptic curves. Number theory and Cryptography.* Chapman and Hall, 2003.

[38] M. Wiener and R. Zuccherato. *Faster attacks on elliptic curve cryptosystems.* Selected Areas in Cryptography-SAC '98 (LNCS1556)[457], 190-200, 1999.

A Computation of the Parings

In this appendix, we briefly introduce a method used to compute the Weil pairing and the Tate-Lichtenbaum pairing. This algorithm is presented by Miller [23]. The following theorem gives us a way to compute the Weil pairing.

Theorem A.1. *Let $S, T \in E[n]$. Suppose that D_S and D_T are divisors of degree 0 with no points in common. Let f_S and f_T be functions such that*

$$div(f_S) = nD_S \text{ and } div(f_T) = nD_T.$$

Then the Weil pairing is given by

$$e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)}.$$

Choose $D_S = [S] - [\infty]$, $D_T = [T+R] - [R]$, for some $R \in (K)$. We have

$$e_n(S,T) = \frac{f_S(R)f_T(S)}{f_S(T+R)f_T(\infty)}.$$

Suppose g is a function such that $div(g) = nD_S$. We can calculate the Tate-Lichetenbaum pairing in section 3.3 as

$$\langle S,T\rangle_n = g(D_T) = \frac{g(T+R)}{g(R)} \in F_q^*$$

for any point $R \in E(F_q)$. Therefore, computing these pairings both involve evaluating $f(Q_1)/f(Q_2)$ for some Q_1, Q_2, where f is a function depending on P.

Now we are ready to introduce Miller's algorithm. Our goal is to find f such that $div(f) = nD_P$ and to compute $f(D_Q)$. Write $D_P = [P+R_1] - [R_1]$ and $D_Q = [Q+R_2] - [R_2] = [Q_1] - [Q_2]$, for some $R_1, R_2 \in E(K)$. We want to compute $f(D_Q) = f(Q_1)/f(Q_2)$. First, we introduce the divisors

$$D_j = j[P+R_1] - j[R_1] - [jP] + [\infty]$$

for all $j < n$. Since $sum(D_j) = \infty$ and $deg(D_j) = 0$, we can find a function f_j such that $div(f_j) = D_j$. Let $v_j = f_j(Q_1)/f_j(Q_2)$. The idea behind the algorithm is to compute all the v_j associated with D_j where j is a power of two. Accumulate these v_j until we find v_n. We will have

$$div(f_n) = n[P + R_1] - n[R_1] - [nP] + [\infty] = n[P + R_1] - n[R_1].$$

Consequently, the function f_n will be the function we want to find. This leads to

$$f(D_Q) = v_n = \frac{f_n(Q_1)}{f_n(Q_2)}.$$

The algorithm is as follows.

1. Write $n = (n_{t-1}, \ldots, n_2, n_0)_2$ in base 2.
2. Let $j = 0$, $s = 1$ and $f_0 = 1$. Compute f_1 by the divisor $D_1 = [P + R] - [P] - [R] + [\infty]$.
3. Compute v_0, v_1.
4. For i from 0 to $t - 1$ do
   - If $n_i = 1$, then compute $v_j \leftarrow v_{j+s}$ and change j to $j + s$.
   - compute $v_s \leftarrow v_{2s}$ and change s to $2s$.
5. Output $v_n = f_n(Q_1)/f_n(Q_2)$.

The only part we did not explain is the computation of v_{j+s} when we have already known v_j and v_s. This process can also be used to compute v_{2s}. Let $ax + by + c = 0$ be the line through jP and sP, and let $x + d = 0$ be the vertical line through $(j + s)P$. We obtain

$$div(ax + by + c) = [jP] + [sP] + [-(jP + sP)] - 3[\infty]$$

$$div(x + d) = [jP + sP] + [-(jP + sP)] - 2[\infty].$$

So,

$$div\left(\frac{ax+by+c}{x+d}\right) = [jP]+[sP]-[jP+sP]-[\infty].$$

Therefore,

$$\begin{aligned}
div(f_{j+s}) &= D_{j+s} = (j+s)[P+R_1]-(j+s)[R_1]-[(j+s)P]+[\infty] \\
&= D_j + D_s + div\left(\frac{ax+by+c}{x+d}\right) \\
&= div(f_j) + div(f_s) + div\left(f\frac{ax+by+c}{x+d}\right) \\
&= div\left(f_j f_s \frac{ax+by+c}{x+d}\right)
\end{aligned}$$

This means $f_{j+s} = f_j f_s(ax+by+c)/(x+d)$ up to some constant multiple. Finally,

$$v_{j+s} = \frac{f_{j+s}(Q_1)}{f_{j+s}(Q_2)} = v_j v_s \frac{(ax+by+c)/(x+d)|_{(x,y)=Q_1}}{(ax+by+c)/(x+d)|_{(x,y)=Q_2}}.$$

Example A.2. Consider the elliptic curve $E : y^2 = x^3 + 16x + 27$ over the finite field F_{29} in example 3.17. Let $P = (21, 24)$ and $Q = (9, 1)$. We want to compute $\langle P, Q\rangle_7$. Choose $R_1 = \infty$ and $R_2 = (13, 5)$, then $D_P = [(21, 24)] - [\infty]$ and $D_Q = [(8, 0)] - [13, 5]$.

1. $7 = (1, 1, 1)_2$.

2. Let $j = 0$, $s = 1$, and $f_0 = 1$. It is clearly $f_1 = 1$.

3. Compute $v_0 = 1$ and $v_1 = 1$.

4. Since $n_0 = 1$, compute $v_{j+s} = v_1 = 1$ and change j to 1. Compute $v_{2s} = v_2 = 1$ and change s to 2.

5. Since $n_1 = 1$, compute $v_{j+s} = v_3 = 27$ by v_1 and v_2. Change j to 3. Compute $v_{2s} = v_4 = 7$ and change s to 4.

6. Since $n_2 = 1$, compute $v_{j+s} = v_7 = (-2) \pmod{29}$.

7. Output v_7

So $\tau_n(P, Q) \equiv (-2)^4 \equiv 16 \pmod{29}$. A similar computation shows

$$\tau_n(P, P) \equiv 7 \pmod{29}$$