Fundamentals of Cryptography: Project Report

Jiang Jiaxuan & Chen Junjie YaoClass 70 2017012515 & 2017012510

January 10, 2020

1 Abstract

In this report, we will first explain why there exists a prerequisite for elliptic curve and what would happen if removing it by theoretical analysis and examples. Then we will introduce a method of calculation of points on elliptic curve by using projective coordinates that can defend side-channel attack.

2 Background

2.1 Elliptic Curve

For cryptography application, we usually only consider elliptic curves over finite fields F_p. And for convenience, we assume $p > 3$. Let $p > 3$ be a prime and let $a, b \in \mathcal{F}_p$ satisfy $4a^3 + 27b^2 \neq 0$. An elliptic curve E defined over $\mathcal{F}_p$ is given by equation

$$y^2 = x^3 + ax + b.$$

And We write $E/\mathcal{F}_p$ to denote the fact that E is defined over $\mathcal{F}_p$. Here we stress the condition $4a^3+27b^2 \neq 0$, which can ensure the equation $x^3 + ax + b = 0$ has no double root. The reason for it will be given in the following sections.

We say that a point (x, y) where $x, y \in \mathcal{F}_p$, is a point on the curve E if (x, y) satisfies the curve equation $y^2 = x^3 + ax + b$. In addition, we introduce a special point $\mathcal{O}$ as the point of infinity on the curve. Then we can use $E(\mathcal{F}_p)$ to denote the set of all points on the curve E that are defined over $\mathcal{F}_p$, including the point $\mathcal{O}$.

Now we can come to consider the addition operation in the group. We define the point $\mathcal{O}$ as the identity element of addition, i.e. $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P(\mathcal{F}_p)$. And suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points in $E(\mathcal{F}_p)$, let $R = (x_3, y_3) = P + Q$. Then there are the following 3 cases:

- If $x_1 \neq x_2$ we use the chord method. Let $s_c = \frac{y_1-y_2}{x_1-x_2}$ be the slope of the cord through the points P and Q. Then $x_3 = s_c^2 - x_1 - x_2$ and $y_3 = s_c(x_1 - x_3) - y_1$.
- If $x_1 = x_2$ and $y_1 = y_2 \neq 0$ (i.e.$P = Q$) we use the tangent method. Let $s_t = \frac{3x_1^2+a}{2y_1}$ be the slope of the tangent at P. Then $x_3 = s_t^2 - 2x_1$ and $y_3 = s_t(x_1 - x_3) - y_1$.
- If $x_1 = x_2$ and $y_1 = -y_2$ then we let $P + Q = \mathcal{O}$.

Then we can see the addition law makes the set $E(\mathcal{F}_p)$ into a group with identity $\mathcal{O}$.

2.2 Cubic Equation

For a cubic equation denoted by $a_3x^3 + a_2x^2 + a_1x_m + a_0 = 0$, where $a_3 \neq 0$, transfer $x' = kx + t$ where k and t can be determined later, then it can be equally solved by another cubic equation $x^3 + ax + b = 0$. Now we will show how to solve $x^3 + ax + b = 0$.

First, assume $x = x_m + x_n$ so that we will have one more free dimension. Then equation should be $(x_m + x_n)^3 + a(x_m + x_n) + b = 0$, which can be rewritten as $x_m^3 + x_n^3 + b + (x_m + x_n)(3x_m x_n + a) = 0$. As we have one free dimension, we can assume $3x_m x_n + a = 0$. Then we have the following equation set:

$$x = x_m + x_n, \tag{1}$$

$$3x_m x_n + a = 0, \tag{2}$$

$$x_m^3 + x_n^3 = -b. \tag{3}$$

By equation (2), we have $x_m^3 x_n^3 = -\frac{a^3}{27}$. Coupled with equation (3), we can know that x_m^3 and x_{n3} are two roots of quadratic equation

$$x^2 + bx - \frac{a^3}{27} = 0. \tag{4}$$

Without loss of generality, we assume $x_m^3 = \frac{-b+\sqrt{b^2+\frac{4a^3}{27}}}{2}$ and $x_n^3 = \frac{-b-\sqrt{b^2+\frac{4a^3}{27}}}{2}$. Since $x_m x_n = -\frac{a}{3}$, we can know that the three root of cubic equation $x^3 + ax + b = 0$ are:

$$x_1 = \sqrt[3]{\frac{-b+\sqrt{b^2+\frac{4a^3}{27}}}{2}} + \sqrt[3]{\frac{-b-\sqrt{b^2+\frac{4a^3}{27}}}{2}}, \tag{5}$$

$$x_2 = \omega\sqrt[3]{\frac{-b+\sqrt{b^2+\frac{4a^3}{27}}}{2}} + \omega^2\sqrt[3]{\frac{-b-\sqrt{b^2+\frac{4a^3}{27}}}{2}}, \tag{6}$$

$$x_3 = \omega^2\sqrt[3]{\frac{-b+\sqrt{b^2+\frac{4a^3}{27}}}{2}} + \omega\sqrt[3]{\frac{-b-\sqrt{b^2+\frac{4a^3}{27}}}{2}}, \tag{7}$$

where $\omega = \frac{-1+\sqrt{3}i}{2}$, i.e., cubic root of 1.

2.3 Side-channel Attack

The side-channel attack is a class of possible attacks to elliptic curve cryptosystems. Based on some given side-channel information such as the working time of each machine or the power consumption, it may be possible to get the information of the working state of the algorithm, and moreover, the secret key. There are different kinds of side-channel attack based on different side-channel information. Here we only consider simple side-channel analysis i.e. side-channel analysis from a single execution of the crypto-algorithm.

Here we will give a kind of simple side-channel attack as an example. In implementation of elliptic curve cryptosystems, we usually use the following double-and-add algorithm to compute $Q = kP$ on an elliptic curve.

Input: $\mathbf{P}$, $k = (k_{l-1}, \ldots, k_0)_2$
Output: $\mathbf{Q} = k\mathbf{P}$

1. $\mathbf{R}_0 = \mathbf{P}$
2. for $i = l - 2$ downto 0 do
3. $\quad \mathbf{R}_0 \leftarrow 2\mathbf{R}_0$
4. $\quad$ if $(k_i \neq 0)$ then $\mathbf{R}_0 \leftarrow \mathbf{R}_0 + \mathbf{P}$

return $(\mathbf{Q} = \mathbf{R}_0)$

Figure 1: Double-and-add algorithm for computing $Q = kP$

Suppose the addition operation and the doubling operation are implemented with different formula. Then the implementation of these two operations can be distinguished easily by simple power analysis (SPA). If we find a doubling operation is followed by an addition operation, the current bit is 1, otherwise it is 0.

2.4 Projective Coordinates

Projective plane is the union set of the plane and a line called line at infinity. In order to denote this new space, we now introduce projective coordinates.

Projective coordinates is a ternary array (a, b, c) where (a, b, c) and (a', b', c') are equivalent if and only if $\frac{a}{c} = \frac{a'}{c'}$ and $\frac{b}{c} = \frac{b'}{c'}$. For any point that is not infinity point, which means it has Euclidean coordinates (x, y), its projective coordinates are denoted equivalently as (xt, yt, t) where t is a non-zero real number. However, for infinity point, its projective coordinates are denoted equivalently as $(x, y, 0)$ where $x^2 + y^2 \neq 0$ where x and y denote its direction.

So for any curve that can be denoted by an equation of Euclidean coordinates can be denoted by a homogeneous equation of projective equation. For example, a homogeneous linear equation can denote a line either a Euclidean line or an infinity line in projective plane; a homogeneous quadratic equation can denote a quadratic curve either an ellipse or a hyperbola or a parabola.

3 Why Is There Such a Prerequisite

As we show in section 2.2, assume a regular form elliptic curve is denoted by $y^2 = x^3 + ax + b$, the interaction of the curve and x-axis can be determined by solving a cubic equation. Note that the discriminant of equation (4), $\Delta = b^2 + \frac{4a^3}{27}$, we know that only when $\Delta \neq 0$, that is $4a^3 + 27b^2 \neq 0$, the three roots of the cubic equation are different in complex domain. In this case, we know that the curve is smooth on any point of the curve.

Here is an example of elliptic curve when $4a^3 + 27b^2 \neq 0$: the elliptic curve $y^2 = x^3 - 4x^2 + 16$ is drawn as figure 2. It's shown the the curve is always smooth.

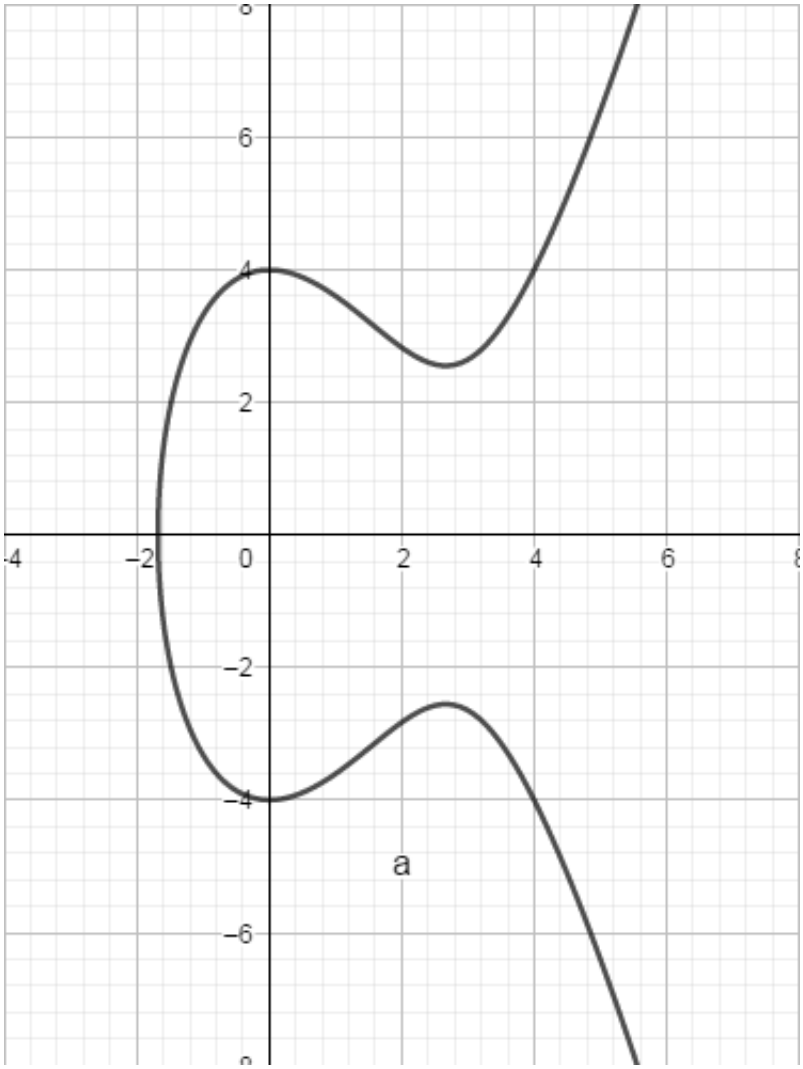

Figure 2: $y^2 = x^3 - 4x^2 + 16$

However, when $\Delta = 0$, which means $x_m = x_n$, we have $x_2 = x_3 = -\sqrt[3]{x_m}$, $x_1 = 2\sqrt[3]{x_m}$. Then we have 2 cases, one is that $x_m = 0$, leading to $x_1 = x_2 = x_3 = 0$; the other is that $x_m \neq 0$, leading to $x_1 \neq x_2 = x_3$. Here we draw the figure of $y^2 = x^3$ as figure 3 and that of $y^2 = x^3 + x^2$ as figure 4. It's shown that they are both non-smooth on points $(0, 0)$.

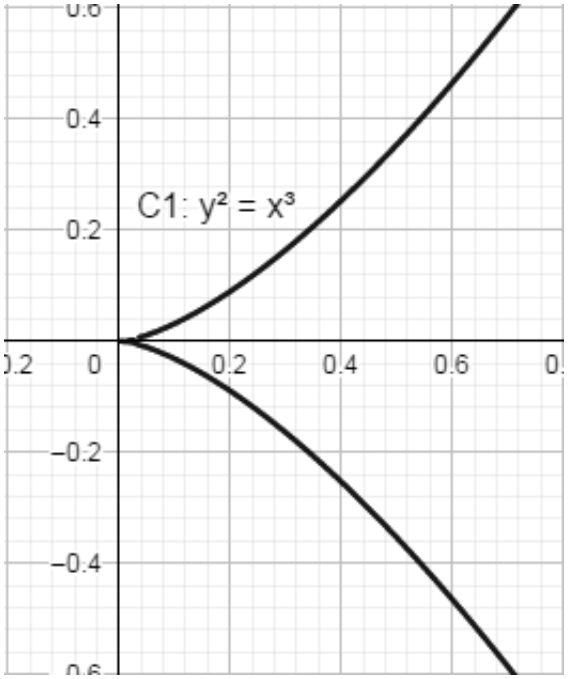

Figure 3: $y^2 = x^3$

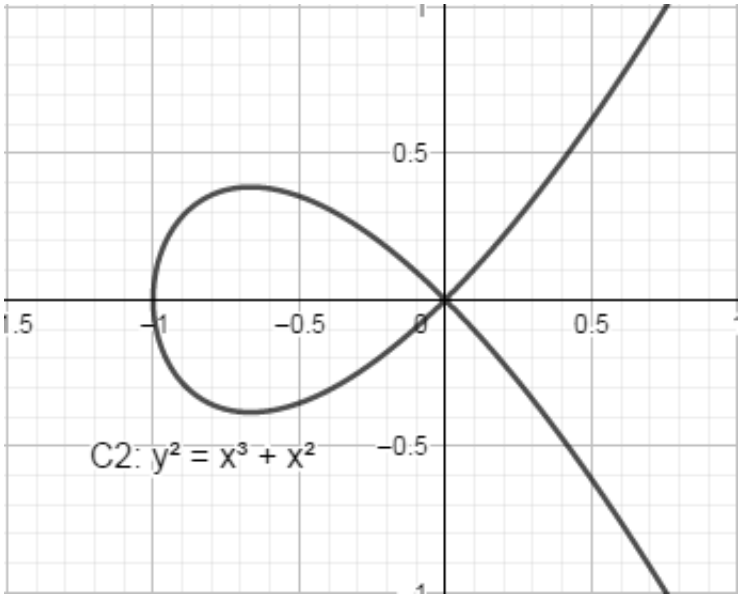

Figure 4: $y^2 = x^3 + x^2$

In section 4, we will show that we can still define a cycle group on these two kinds of group when excluding the non-smooth point and will talk about their unique characters.

4 What Would Happen If the Prerequisite Is Removed

If the prerequisite $4a^3+27b^2 \neq 0$ doesn't holds, in some cases we can also find a proper cyclic group. Here we take the elliptic curve $y^2 = x^3 \mod p$ as an example where p is a prime number and $p \neq 2$, i.e. $a = b = 0$. First we can prove the group over this elliptic curve is a cyclic group of order p. In fact, if we consider all possible x^3 where $x \in [p-1]$, only half of them can be written as a square of numbers in $[p-1]$. And for all such x^3, we can find two difference $y \in [p-1]$ s.t. $y^2 = x^3$. So after adding the point of infinity, there are totally $\frac{p-1}{2} \cdot 2 + 1 = p$ elements in the group $E(\mathcal{F}_p)$. Then by the knowledge of group theory we can see $E(\mathcal{F}_p)$ is a a cyclic group of order p. Then we can also build elliptic curve cryptosystem with this elliptic curve. For example, when $p = 7$, the cyclic group is

$$\{(1,1),(2,1),(4,6),(4,1),(2,6),(1,6),(\infty,\infty)\}.$$

There is also another kind of elliptic curves satisfying $4a^3+27b^2 = 0$, for example, $y^2 = x^3 - 3x + 2 \mod 7$. By enumeration, we can find the elements of it are

$$\{(6,2),(2,5),(0,4),(5,0),(0,3),(2,2),(6,5),(\infty,\infty)\}.$$

And they form a cyclic group of order 8, which may also be used in elliptic curve cryptosystems. As a comparison of it, we can consider the cyclic group over the elliptic curve $y^2 = x^3 + x + 1 \mod 23$ whose $4a^3 + 27b^2 \neq 0$. We can verify that it is also a cyclic group of order 28, whose order is also even:

$$\{(3,10),(7,12),(19,5),(17,7),(9,16),(12,4),(11,3),(13,16),(0,1),(6,4),(18,20),(5,4),(1,7),(4,0),(1,10),$$
$$(5,19),(18,3),(6,19),(0,22),(13,7),(11,20),(12,19),(9,7),(17,20),(19,18),(7,11),(3,13),(\infty,\infty)\}$$

So by abandon the non-smooth point we can also construct proper cyclic groups which can be used in elliptic curve cryptosystem.

5 Avoiding Side-channel Attack Using Projective Coordinates

As we show in section 2.4, for $(x_3, y_3) = (x_2, y_2) + (x_1, y_1)$, we set $x_i = \frac{X_i}{Z_i}$, $y_i = \frac{Y_i}{Z_i}$, then we have

$$X_3 = 2FW, \tag{8}$$
$$Y_3 = R(G - 2W) - L^2, \tag{9}$$
$$Z_3 = 2F^3, \tag{10}$$

where $U_1 = X_1Z_2, U_2 = X_2Z_1, S_1 = Y_1Z_2, S_2 = Y_2Z_1, Z = Z_1Z_2, T = U_1 + U_2, M = S_1 + S_2, R = T^2 - U_1U_2 + aZ^2, F = ZM, L = MF, G = TL$, and $W = R^2 - G$. Therefore, adding two points with our unified formula require 17 multiplications plus 1 multiplication by constant. When $a = -1$ then we may write $R = (T-Z)(T+Z) - U_1U_2$ and the number of multiplications decreases to 16. Then we can implement the addition of two points in this way.

After that, we can implement the algorithm of computing kP given an integer k and a point P on elliptic curve as follow:

Input: $\mathbf{P}$, $k = (k_{l-1}, \ldots, k_0)_2$
Output: $\mathrm{x}(k\mathbf{P})$

1. $\mathbf{R}_0 = \mathbf{P}$; $\mathbf{R}_1 = 2\mathbf{P}$
2. for $i = l - 2$ downto 0 do
3. if $(k_i = 0)$ then
4. $\mathrm{x}(\mathbf{R}_1) \leftarrow \mathrm{x}(\mathbf{R}_0 + \mathbf{R}_1)$; $\mathrm{x}(\mathbf{R}_0) \leftarrow \mathrm{x}(2\mathbf{R}_0)$
5. else [if $(k_i = 1)$]
6. $\mathrm{x}(\mathbf{R}_0) \leftarrow \mathrm{x}(\mathbf{R}_0 + \mathbf{R}_1)$; $\mathrm{x}(\mathbf{R}_1) \leftarrow \mathrm{x}(2\mathbf{R}_1)$

return $(\mathrm{x}(\mathbf{R}_0))$

Figure 5: Computing $\mathrm{x}(k\mathbf{P})$

In the algorithm, x can be any function including the 3 elements of its projective coordinates. Observe that the difference $\mathbf{R}_1 - \mathbf{R}_0$ remains invariant throughout the algorithm: $\mathbf{R}_1 - \mathbf{R}_0 = \mathbf{P}$.

In this way, we can defend side-channel attack but do not need to do dummy operation or require an elliptic curve of specific form.

References

[1] Brier, E., Joye, M.: Weierstraß Elliptic Curves and Side-Channel Attacks. In: Naccache, D and Paillier, P., editors, Public Key Cryptography 2002, Volume 2274 of Lecture Notes in Computer Science, pages 335-345. Springer-Verlag, 2002.

[2] Boneh, D., Shoup, V.: A Graduate Course in Applied Cryptography, 400 pp. (2015).

[3] Wenfei Wu and Students in IIIS: Fundamentals of Cryptography Lecture Notes.