Research into Singular Elliptic Curve Groups

2019012325 Benyu Wang

January 15, 2021

In this project, we will think about removing the prerequisite $4a^3+27b^2 \neq 0$ for the Elliptic curve system in cryptography. Here we discuss about the group generated by the curve $y^2 = x^3+ax+b, 4a^3+27b^2 = 0$. We will give a proof of the group structure and reasons why using singular curves is not secure.

1 The "singular curve" and its group

1.1 The singular curve and its singularity

The curve we get here is not an elliptic curve by the definition in [1]. Here we call it a "singular curve" since it has a singularity. By the cubic equation discriminant we know $x^3+ax+b = 0$ has a double or triple root if and only if $-\Delta = 4a^3+27b^2 = 0$. Then we will have a singularity on the double or triple root. In fact, as the picture shows, if there's a triple root, the singularity will be a cusp; if there's a double root, it will be a node.

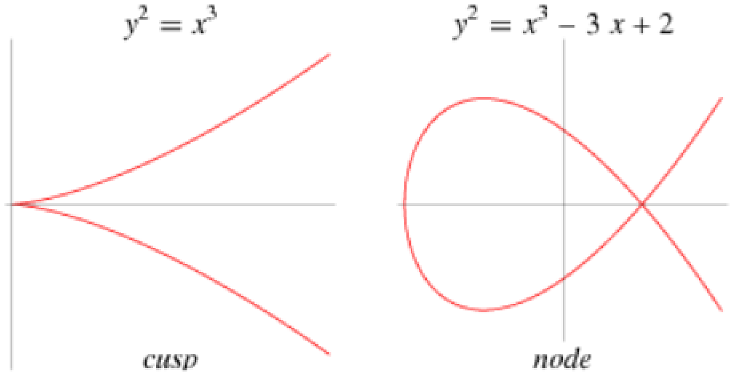

Figure 1: Two types of singular curves, from [2].

At the singularity $S(s,0)$, if we draw a line $y = k(x-s)$ intersect the curve, we will get $k^2(x-s)^2 = x^3+ax+b$, so $(x-s)^2$ divides both sides and we know $x = s$ is always a double root or triple root for the cubic equation. Thus, there are at most two intersections and the line can't be tangent to the other intersection (it can't be a double root as well).

1.2 The singular curve group

The singular curve group can be constructed similarly to the elliptic curve group. We use the same binary operation as what we have used in the elliptic curve group, but the set will have a difference: we must remove the singularity.

If we don't remove the singularity, the group operation will not be well defined. When we add the singularity to another point, since we don't have a third intersection of the line to the curve, and the line is not tangent to both points, we can't define the adding result by the addition law. Even if we want to define the sum as the singularity point or the infinity point, we find this disobeys the group law.

However, after removing the singularity, we will find the set given by other points, together with the addition we defined in the elliptic curve group, will give us a group structure. We will prove it here.

1.3 Proof for the group structure

To prove it is really a group, we check closure, associativity, identity and inverse.

Identity. The identity 0 is defined as the infinity point.

Inverse. The inverse of (x, y) is defined as $(x, -y)$, and by the addition law we know $(x, y) + (x, -y) = 0$.

Closure. We verify the group is closed under addition. By the property of cubic functions, we know if a line has two intersection points with different x coordinate on the curve, then the cubic eqation defined by intersection the line and the curve has all three roots in the field. Moreover, the third root can't be the singularity since it can't be a double or triple root. Therefore, we know the closure holds when we add two points $(x_1, y_1), (x_2, y_2), x_1 \neq x_2$. And if we add 0 to a point, or add a point to its inverse, the result will also in the group. So the group is closed under addition.

Associativity. By definition we know the addition is commutative, however, proving associativity is more involved. For special cases, such that we have a 0 in the sum (then the result is certainly the sum of the other two points), or we have a pair of $\pm A$ in the sum ($A, B, -(A+B)$ are colinear, so $-A, (A+B), -B$ are colinear, then $-A + (A+B) = B = (-A+A) + B$ and if we place them in different orders by commutativity it can also be transformed to this case), the associativity can be proved easily.

But for generic cases, the associativity law is hard to prove. However, if we can prove the addition is associative in the elliptic curve group, we can believe the addition is associative in this group as well. Lemma 2.1 in [3] gave an elementary proof only using the first equation and the algebraic representation of the addition law. Since the proof doesn't require the second condition $4a^3 + 27b^2 \neq 0$, it can be a valid proof for the singular curve group as well. Therefore, we can get the associativity.

Therefore, we know it is a group, and moreover, the group is an Abelian group.

2 The security problem using singular curves

2.1 Why we use ECC

Recall the reason why we use the elliptic curve groups but not the number theoretic additive or multiplicative groups. We want a group "safe" enough, so the discrete logarithm problem is hard to solve in it. For *mod p* additive groups Z_p^+, the problem is easily solved by extended GCD; for multiplicative groups Z_p^*, we also have sub-exponential algorithms, but for general elliptic curve groups, there's no sub-exponential algorithm now.

Therefore, if we at last get some groups on which the discrete logarithm problem is not hard enough, we will think the group is not secure. And in fact, the singular curve group turns out to be too easy.

So below we consider the two types of singular curves: one with a triple root, and the other with a double root. With a cyclic shift of x we can assume the singularity is $(0, 0)$, and then the two types of curves can be represented as $y^2 = x^3$ and $y^2 = x^2(x + a)$.

We will analyze them below. And the contents below are from the theorems in [4], chapter 2.10.

2.2 $y^2 = x^3$

Theorem. Let $f(x, y) = y/x$, for infinity, $f(\infty) = 0$. Then f is an isomorphism from the singular curve group G to Z_p^+.

We prove the theorem. Let $t = y/x$, then since $y^2 = x^3$, we know $x = 1/t^2$, $y = 1/t^3$. Consider adding (x_1, y_1) and (x_2, y_2), we know:

$$\begin{aligned} t_3^{-2} = x_3 &= (y_2 - y_1)^2/(x_2 - x_1)^2 - x_1 - x_2 \\ &= (t_2^{-3} - t_1^{-3})^2/(t_2^{-2} - t_1^{-2})^2 - t_2^{-2} - t_1^{-2} \\ &= (t_1 + t_2)^{-2} \end{aligned}$$

Similarly, we can calculate:

$$\begin{aligned} -t_3^{-3} = -y_3 &= (y_2 - y_1)(x_3 - x_1)/(x_2 - x_1) + y_1 \\ &= -(t_1 + t_2)^{-3} \end{aligned}$$

Therefore, we know $t_3 = t_1 + t_2$, and thus this is a homomorphism, whose kernel is not the whole group, so it is surjective. Since $y^2 = x^3$ has two solutions when x is square and no solution when x is not, we know there are exactly $((p - 1)/2) * 2 = p - 1$ points, so with the infinity, there are p points in the group in total. Therefore, we know we get an isomorphism.

Therefore, we can first use the isomorphism to get the corresponding number in Z_p and then use extended GCD to solve the discrete logarithm problem. Thus, the system is insecure.

2.3 $y^2 = x^2(x + a)$

Theorem. Let $\alpha^2 = a$, $f(x, y) = (y + \alpha x)/(y - \alpha x)$, for infinity, $f(\infty) = 0$. Let H be the multiplicative group generated by field F_p extending α (if α is in F_p, it is F_p^*, otherwise it is $F_{p^2}^*$). Then f is a homomorphism from the singular curve group G to H.

We prove the theorem. Let $t = (y + \alpha x)/(y - \alpha x)$, then we also know $x + a = y^2/x^2 = \alpha^2(t + 1)^2/(t - 1)^2$, so $x = 4at/(t - 1)^2$, $y = 4\alpha^3 t(t + 1)/(t - 1)^3$.

We also substitute x, y into the equations

$$x_3 = (y_2 - y_1)^2/(x_2 - x_1)^2 - a - x_1 - x_2$$
$$-y_3 = (y_2 - y_1)(x_3 - x_1)/(x_2 - x_1) + y_1$$

By calculation and simplification we get:

$$4t_3/(t_3 - 1)^2 = 4t_1t_2/(t_1t_2 - 1)^2$$
$$4\alpha^3 t_3(t_3 + 1)/(t_3 - 1)^3 = 4\alpha^3 t_1t_2(t_1t_2 + 1)/(t_1t_2 - 1)^3$$

Therefore:

$$(t_3 + 1)/(t_3 - 1) = (t_1t_2 + 1)/(t_1t_2 - 1)$$

So we know $t_3 = t_1t_2$ and thus f is a homomorphism.

Moreover, f is injective since the kernel $\{\infty\} \cup \{(x, y) \neq (0, 0)|(y + \alpha x) = (y - \alpha x), y^2 = x^2(x + a)\}$ has only one element ∞.

Therefore, we use the homomorphism and we only need to solve the same discrete logarithm problem in the group H. Since H is F_p^* or $F_{p^2}^*$, by [5], appendix E, we learn that Pohlig-Hellman Algorithm can be used to solve the problem in H, which is the multiplicative group. Therefore, we still have sub-exponential algorithm to solve the discrete logarithm problem in these singular curve groups, so we think it is insecure.

References

[1] C. Paar and J. Pelzl. Understanding cryptography: A textbook for students and practitioners.

[2] Rowland, Todd. ”Elliptic Discriminant.” https://mathworld.wolfram.com/EllipticDiscriminant.html

[3] Friedl, S. An elementary proof of the group law for elliptic curves. https://arxiv.org/pdf/1710.00214.pdf

[4] L. C. Washington, Elliptic curves: Number theory and cryptography, 2nd ed.

[5] Wenfei Wu and students in IIIS: Crypto lecture notes 2018.