KOBLITZ CURVES

JANE AHN

1. Elliptic Curves in Characteristic 2

Definition 1.1. An ellitpic curve is *singular* if it has cusps or self intersections.

In characteristic 2, the elliptic curve $y^2 = x^3 + Ax + B$ is always singular. Thus, mathematicians often use the form $y^2 + Axy + By = x^3 + Cx^2 + Dx + E$ instead. The group law still holds.

2. Koblitz Curves

Definition 2.1. A *Koblitz curve* $E(\mathbb{F}_q), q = 2^k$ is the set of points $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ that satisfy $E : y^2 + xy = x^3 + ax + 1, a \in \{0, 1\}$ with O, the point at infinity.

It is clear that the curve has coefficients in $\mathbb{F}_2$. It is known that the points on this curve form an abelian group under point addition, similar to a regular elliptic curve.

The points on $E(\mathbb{F}_q)$ with $q = 2^k$ for a large k are often used for cryptography. They are used because it is quite easy to calculate the number of points on a Koblitz curve.

$$\#E(\mathbb{F}_{2^k}) = 2^k - \left(\frac{-1 + \sqrt{-7}}{2}\right)^k - \left(\frac{-1 - \sqrt{-7}}{2}\right)^k + 1$$

3. Properties of a Koblitz Curve

(1) They are ordinary (nonsupersingular)
(2) The order of the group has a large prime factor $\rightarrow$ prevents solving of the Discrete Log problem by using Baby-Step-Giant-Step algorithm or the Pollard Rho algorithm
(3) Doubling of points on the curve is very efficient
(4) The curves are easy to find

4. Group Homomorphism of a Koblitz Curve

There exists a group homomorphism $\tau : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_q), \tau(x, y) = (x^2, y^2)$, which makes computations with Koblitz curves simple. The map τ also satisfies $\tau^2(P) + \tau(P) + 2P = O$, the point at infinity. Using this relation, we see that every integer m has a $\tau-adic$ expansion, similar to a binary expansion or a ternary expansion.

$$m = m_0 + m_1\tau + m_2\tau^2 + \cdots + m_r\tau^r$$

with $m_0, \ldots, m_r \in \{0, \pm 1\}$. Then, mP can be computed as

$$mP = m_0P + m_1\tau(P) + m_2\tau^2(P) + \cdots + m_r\tau^r(P)$$

Date: May 4, 2016.