BLS12-381 elliptic curve

1. What is elliptic curve?

1.1 基础概念

- degree
- every conic can be affinely transformed into one of the following five curves:

1. $X^2 = 0$: a double line
2. $X^2 + Y^2 = 0$: a single point
3. $X^2 - Y^2 = 0$: two lines
4. $X^2 + Y^2 + Z^2 = 0$: the empty set
5. $X^2 + Y^2 - Z^2 = 0$: a unit circle

    - Affine transformation: 几何中，**对一个向量空间进行线性变换并接上一个平移，变换为另一个向量空间。**
    - Affine transformation几何的点集属性不变。
- an elliptic curve
    - 为如下曲线求解：

$$Y^2 = X^3 - 2X$$

在曲线（X_0，Y_0）通过隐微分求得在该点的切线方程为：

$$Y = \frac{3X_0^2 - 2}{2Y_0}(X - X_0) + Y_0$$

由于X_0是曲线解的二重平方根（因为（（X_0，Y_0）是椭圆曲线的切线）），根据二重根与一重根乘积的根求解，即可得另一个根为

$$X_1 = -\frac{(X_0^2 + 2)^2}{4(X_0^3 - 2X_0)}$$

    - 曲线族、包络、有限生成的阿贝尔群

Theorem [Mordell]: On a rational elliptic curve, the group of rational points is a finitely-generated abelian group.

Theorem [Mazur]: Write $E(\mathbb{Q}) = \mathbb{Z}^{(r)} \times \mathrm{Tor}(E(\mathbb{Q}))$. Then either

$$\mathrm{Tor}(E(\mathbb{Q})) \cong \mathbb{Z}/m\mathbb{Z}$$

where $m = 1, 2, \ldots, 10, 12$, or

$$\mathrm{Tor}(E(\mathbb{Q})) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

where $m = 2, 4, 6, 8$.

2. BLS12-381 (part of a family of curves)

2.1 name of BLS12-381

- BLS是提出算法的3位数学家名字首位
- 12: embedding degree
- 381: 48 bytes作为一个存储单元，其中有381 bit用于存储有限域的元素，另外3 bit用于存储运算符号

2.2 BLS12-381曲线的特性

- 基础的曲线方程：$y^2 = x^3 + 4$d
- 低Hamming weight （在最为常见的数据位符号串中，它是1的个数。）：为了提升计算pairings的效率
- field模除的p是素数且不超过383 bit：便于在32 bytes或64 bytes存储中运算
- 子群的阶数是r，且不超过255 bit，原因同上
- security target is 128 bits
- 需要获得域中单位根的大次幂，用于支持多项式乘法的快速傅里叶变换，用于实现zk-Snark方案

符合上述要求的值

x = -0xd201000000010000

3. Field Extensions

- 12 in name of the algo也是field extensions
- 什么是F E？

> The field F_q can be thought of as just the integers modulo q: $0, 1, \ldots, q-1$. But what kind of beast is $F_{q^{12}}$, the twelfth extension of F_q?

  - 通过FE解决乘法问题中出现的高阶计算问题
- The complex numbers are a quadratic extension of the real numbers.
- In practice, large extension fields like 12 field extensions are implemented as towers of smaller extensions.

4. Curves

- q的域上曲线

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

- 上述曲线的extension field

$$y^2 = x^3 + 4(1+i)$$

5. The Subgroups

- 由于bilinear map需要从两个群中取点作为输入，因此，采用extension数为12的扩展域作为另一个群，这也是embedding degree

6. Twists

- A twist is something like a coordinate transformation，便于高阶扩展域计算
- BLS12-381 uses a “sextic twist”， 即使用因子6进行降阶
- 降阶后，高低阶之间保持双射

So these are the two groups we will be using:

- $G_1 \subset E(F_q)$ where $E : y^2 = x^3 + 4$
- $G_2 \subset E'(F_{q^2})$ where $E' : y^2 = x^3 + 4(1 + i)$

- 由于G2的点为复数，因此占用2倍存储空间

7. Pairings

As far as BLS12-381 is concerned, a pairing simply takes a point $P \in G_1 \subset E(F_q)$, and a point $Q \in G_2 \subset E'(F_{q^2})$ and outputs a point from a group $G_T \subset F_{q^{12}}$. That is, for a paring e, $e : G_1 \times G_2 \to G_T$.

What we are interested in is that:

- $e(P, Q+R) = e(P, Q) \cdot e(P, R)$, and
- $e(P+S, R) = e(P, R) \cdot e(S, R)$

From this, we can deduce that all of the following identities hold:

- $e([a]P, [b]Q) = e(P, [b]Q)^a = e(P, Q)^{ab} = e(P, [a]Q)^b = e([b]P, [a]Q)$[11].

Reference

1. Stanford crypto课件：https://crypto.stanford.edu/pbc/notes/elliptic/
2. 多重根求解：https://www.youtube.com/watch?v=LHVkk2NcMaM
3. 有限域特征根：https://en.wikipedia.org/wiki/Characteristic_(algebra)
4. https://hackmd.io/@benjaminion/bls12-381#Embedding-degree