Reference

Friday, April 26, 2024 1:21 PM

1. https://hackmd.io/@benjaminion/bls12-381
2. https://hackmd.io/@jpw/bn254

BLS12-381

Thursday, May 30, 2024 11:37 AM

Pairing friendly:

- A random EC is not pairing friendly with high probability
- BLS12-381 was constructed to be pairing friendly

Why pairing friendly?

Verifier step:

Pairing1 = Pairing2 + Pairing3 + Pairing4

Naming:

- 12 -> embedding degree
- 381 -> # bits of field modulus q

Curve equation and parameters:

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

X = -0xd201000000010000 (not x in equation)

Field modulus $q = \frac{1}{3}(x-1)^2(x^4 - x^2 + 1) + x$

Subgroup size $r = x^4 - x^2 + 1$

Field extension

"12" in BLS12-381 also represents degree of field extension.

$\mathbb{F}_{q^{12}}$: 12th extension of $\mathbb{F}_q$ ...... wait what ???

Look at a simpler example: Constructing $\mathbb{F}_{q^2}$ from $\mathbb{F}_q$.

$$\mathbb{F}_q = \{0, 1, \cdots, q-1\}$$

$$\mathbb{F}_{q^2} = \{a_0 + a_1 x \mid a_0, a_1 \in \mathbb{F}_q\}$$
$$= \{(a_0, a_1) \mid a_0, a_1 \in \mathbb{F}_q\}$$

$+$: $(a, b) + (c, d) = a + bx + c + dx$
$$= (a+c) + (b+d)x$$
$$= (a+c, b+d)$$

$\cdot$: $(a, b) \cdot (c, d) = (a+bx)(c+dx)$
$$= ac + adx + bcx + bdx^2 \quad ???$$

How to handle x^2 term? Rule: $x^2 + 1 = 0$
$$x^2 = -1$$

$\Rightarrow$ $(a, b) \cdot (c, d) = ac + (ad+bc)x - bd$
$$= (ac - bd) + (ad+bc)x$$
$$= (ac - bd, ad + bc)$$

Looks familiar? This is $\mathbb{C}$

General criteria for the "rule":

1. Extension degree is k, then "rule" is degree k polynomial.
2. "rule" must be irreducible (can't be further factored)

kind of like prime number

Note that we can't further extend C, since there isn't any irreducible polynomial in C.
(Fundamental theorem of algebra)

In contrast, we often can find irreducible poly in finite field.
If we find degree k irreducible poly:

$$\mathbb{F}_q \to \mathbb{F}_q$$

$$\mathbb{F}_{q^k} = \{a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \mid a_0, \cdots a_{k-1} \in \mathbb{F}_q\}$$

$$= \{(a_0, a_1, \cdots, a_{k-1}) \mid a_0, \cdots, a_{k-1} \in \mathbb{F}_q\}$$

The curves

There are TWO curves in BLS12-381:

1. $E(\mathbb{F}_q)$: $y^2 = x^3 + 4$ over $\mathbb{F}_q$
2. $E'(\mathbb{F}_{q^2})$: $y^2 = x^3 + 4(1+i)$ over $\mathbb{F}_{q^2}$

About curve_order: Use Hasse's theorem

N: # points on curve E over $\mathbb{F}_q$, then:

N: # points on curve E over F_q, then:

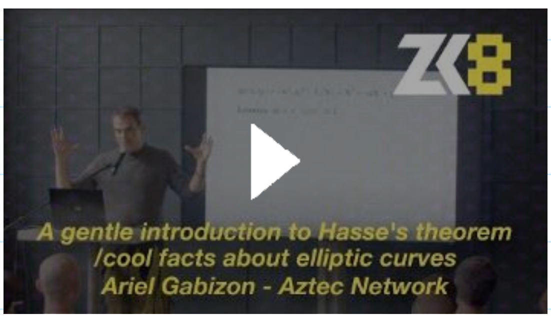
$$|N-(q+1)| \le 2\sqrt{q}$$

$$-2\sqrt{q} \le N-q-1 \le 2\sqrt{q}$$

$$\underbrace{q+1-2\sqrt{q}}_{\approx q} \le N \le \underbrace{q+1+2\sqrt{q}}_{\approx q}$$

Further study:

[ZK8: An introduction to Hasse's theorem/cool facts about elliptic curves – Ariel Gabizon - Aztec]()



Conclusion:

→ curve_order of $E(F_q)$: $\sim q$

→ curve_order of $E(F_{q^2})$: $\sim q^2$

The subgroups

Bilinear pairing : $G_1 \times G_2 \to G_T$

should have same order r

a pre-defined prime with ≤ 255 bit in size

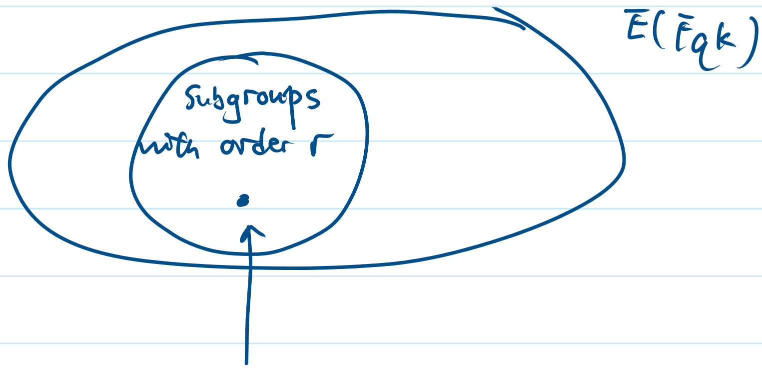
But :

But:

a pre-defined prime with ≤ 255 bit in size

$E(\mathbb{F}_q)$ only has 1 large subgroup of order r, can define G_1 here but need something larger to define G_2.

We can keep extending $E(\mathbb{F}_q)$ to $E(\mathbb{F}_{q^k})$, so that $E(\mathbb{F}_{q^k})$ contains other subgroups of order r.



One subgroup will contain only points with trace = 0, this subgroup is G_2.

involved math, can think of it as "a special property".

That k in $E(\mathbb{F}_{q^k})$ is "embedding degree". In BLS12-381, it is 12 → $E(\mathbb{F}_{q^{12}})$ is good enough to define G_2.

→ G_1 and G_2 share the same O

Now we have:

1. G_1 of order r from $E(\mathbb{F}_q)$

2. G_2 of order r from $E(\mathbb{F}_{q^{12}})$

$G_1 \times G_2 \rightarrow$ we can do pairing

Twists

Motivation: Computation in $\mathbb{F}_{q^{12}}$ is hard.

Introducing twist:

Transform $E(\mathbb{F}_{q^{12}})$ into a curve defined over lower degree field.

BLS12-381 uses "sextic twist": reduce the degree of field extension by a factor of 6.

$\mathbb{F}_{q^{12}} \rightarrow \mathbb{F}_{q^2}$, new subgroup is isomorphic to G_2

How sextic twist works?

Work in progress

Find u s.t. $u^6 = (1+i)^{-1}$

Define $(x, y) \rightarrow (\frac{x}{u^2}, \frac{y}{u^3})$

Then cure transformation:

$$E: y^2 = x^3 + 4 \rightarrow E': (\frac{y}{u^3})^2 = (\frac{x}{u^2})^3 + 4$$

$$\frac{y^2}{\cdot 6} = \frac{x^3}{\prime} + 4$$

$$\frac{y^2}{u^6} = \frac{x^3}{u^6} + 4$$

$$y^2 = x^3 + \underline{4 \cdot u^6} \quad ?$$

I haven't seen this written down anywhere--but attempting to decode section 3 of this--if we find a u such that $u^6 = (1+i)^{-1}$, then we can define our twisting transformation as $(x, y) \to (x/u^2, y/u^3)$. This transforms our original curve $E: y^2 = x^3 + 4$ into the curve E' : $\underline{y^2 = x^3 + 4/u^6 = x^3 + 4(1+i)}$. E and E' look different, but are actually the same object presented with respect to coefficients in different base fields[10].

$$y^2 = x^3 + 4 \cdot (1+i)^{-1}$$

Anyway, the idea of sextic twist is to simplify the computation of G2, so we only work in E(Fq2) instead of E(Fq12).

Now we have:

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

In G_1, points are pair of integers : (a, b)

In G_2, points are pair of complex numbers : $((a, b), (c, d))$

Pairings

$$e: \underset{P}{G_1} \times \underset{Q}{G_2} \to G_T \qquad e(P, Q)$$

$$e: G_1 \times G_2 \to G_T \qquad e(P, Q)$$

G_1 ↑ $E(\mathbb{F}_q)$, G_2 ↑ $E'(\mathbb{F}_{q^2})$, G_T ↑ $E(\mathbb{F}_{q^{12}})$

Properties:

1. $e(P, Q+R) = e(P, Q) \cdot e(P, R)$

2. $e(P+S, R) = e(P, R) \cdot e(S, R)$

Combine 1 and 2:

$$e([a]P, [b]Q) = e(P, [b]Q)^a$$

↑ scalar multiplication

$$= e(P, Q)^{ab}$$

$$= e(P, [a]Q)^b$$

$$= e([b]P, [a]Q)$$

Insight: (still black box lol)

Pairing ≈ mutiply G_1-point and G_2-point

Embedding degree

field modulus

Embedding degree k = smallest integer s.t. $r \mid q^k - 1$

predefined prime, order of G_1 and G_2

$r \mid q^{12} - 1$

BLS signature

(The L is the same L as in BLS12-381; the B and the S are different.)

<u>keygen:</u>

$\mathbb{Z}/r\mathbb{Z}$, or $\mathbb{F}_r$

private key : sk, random number between 1 and r-1

public key : pk = [sk] g_1 → G_1 point

chosen generator of G_1

protected by ECDLP

<u>Signing:</u>

Map message m onto a point in G_2

1. hash m to integer mod q
2. check if point with that x-coordinate is on curve. If not, m += 1 and try again.
3. Multiply resulting point by G_2 ⇒ H(m) as G_2 point

Sign message: $\sigma = [sk] H(m) \rightarrow G_2$ point

Sign message: $\sigma = [sk]H(m) \rightarrow G_2$ point

$\uparrow$

protected by ECDLP

Verification:

Given (m, σ, pk), verify if sk corresponds to pk

$$e(g_1, \sigma) == e(pk, H(m))$$

$\uparrow$

pairing in py_ecc.bls12_381

correctness: $pk \rightarrow G_1$ point

$$e(pk, H(m)) = e(\underbrace{[sk]g_1}, \underbrace{H(m)}_{G_2 \text{ point}})$$

$$= e(g_1, H(m))^{sk}$$

$$= e(g_1, \underbrace{[sk]H(m)}_{\rightarrow \sigma})$$

$$= e(g_1, \sigma)$$

Aggregation:

- Verifying a single m signed by n parties requires 2 pairings
- Verifying n messages signed by n parties requires n+1 pairings

Example:

$\sigma_{agg} = \sigma_1 + \sigma_2 + \cdots + \sigma_n \rightarrow G_2$ point

$pk_{agg} = pk_1 + pk_2 + \cdots + pk_n \rightarrow G_1$ point

$\Rightarrow$ just verify $e(g_1, \sigma_{agg}) = e(pk_{agg}, H(m))$

BN254/BN128 - WIP

Monday, May 20, 2024 5:27 PM

BN254 is used in Ethereum precompiled, so it is widely used for on-chain verification for schemes such as Groth16 and PlonK.

BN254 == BN128. 254 means 254-bit prime modulus associated to the base field. 128 means it provides 2**128 bit of security.

$y^2 = x^3 + 3$

BN curve

$Y^2 = X^3 + b$ over $\mathbb{F}_p$, $p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$

parameter X, not x in curve equation

X also determines:

$t = 6x^2 + 1$, "trace of Frobenius"

Embedding degree $= 12$

How to find b from parameter X

1. Iterate through b s.t. $b+1$ is a quadratic residue mod p
2. For such b, the point $G = (1, \sqrt{b+1})$ lies on $E(\mathbb{F}_p)$
3. Check whether $rG = 0$, i.e. the point G has order r
4. If $rG \neq 0$, iterate to next b.

$G = (1, 2)$ when $b = 3$

```
ret2basic@PwnieIsland: ~ 80x24
ret2basic@PwnieIsland:~$ python3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from py_ecc.bn128 import G1
>>> G1
(1, 2)
>>>
```

Field extension towers

Represent $\mathbb{F}_{p^{12}}$ as a specific tower of field extensions of $\mathbb{F}_p$:

$$\mathbb{F}_{p^2} = \mathbb{F}_p[u] / (u^2 - \beta) \rightarrow u^2 - \beta = 0$$

$$\mathbb{F}_{p^6} = \mathbb{F}_{p^2}[v] / v^3 - \xi \rightarrow v^3 - \xi = 0$$

$$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}(w) / w^2 - v \rightarrow w^2 - v = 0$$

- β is a quadratic non-residue in $\mathbb{F}_p$
  $\Rightarrow$ $X^2 - \beta$ is irreducible over $\mathbb{F}_p[x]$
- ξ is quadratic non-residue and cubic non-residue in $\mathbb{F}_{p^2}$
  $\Rightarrow$ $X^6 - \xi$ is irreducible over $\mathbb{F}_{p^2}[x]$

Further reading

Thursday, May 30, 2024 3:34 PM

1. Pairing for beginners: https://static1.squarespace.com/static/5fdbb09f31d71c1227082339/t/5ff394720493bd28278889c6/1609798774687/PairingsForBeginners.pdf
2. BN254 For The Rest Of Us https://hackmd.io/@jpw/bn254