BLS12-381 Curve

Presentation Project 2

by

Miguel Angel Schweizer

Berner
Fachhochschule

History

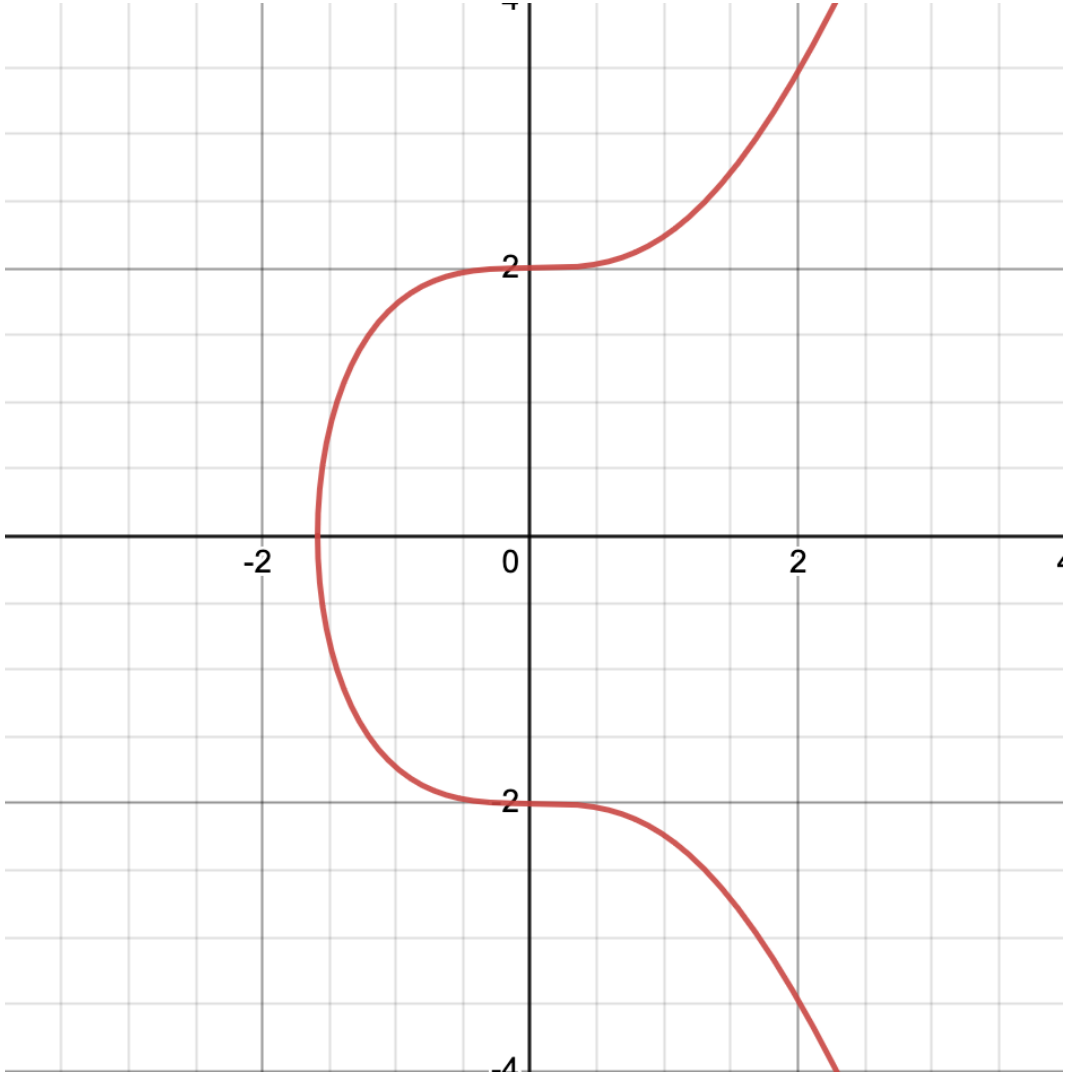
- Pairing-fiendly elliptic curve
- Designed by Sean Bowe in 2017
- Zcash protocol update

Naming

- Family of curves from Baretto, Lynn and Scott (BLS)
- 12 = embedding degree
- 381 = size in bits of base field modulus q

Curve Equation

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



Berner
Fachhochschule

Groups – G_1

- Cyclic group
- Group order r
- Generated with base point BP=(x,y)
- Field F_p
- G_1 defined over E: $y^2=x^3+4$

Groups – G_2

- Cyclic group
- Subgroup order r
- Generated with base point BP'=(x',y')
- Field F_p^2
- G2 defined over E': y2=x3+4(1+i)

Berner
Fachhochschule

Groups – G_T

- Subgroup of multiplicative group F_p^{12}
- Group order r

Parameters

- IETF draft suggestions
  - Security level
  - Subgroup size r
  - Field modulus q^k
  - Embedding degree k
  - Cofactor h

Embedding degree

- k = 12
- Smallest positive integer so that r devides $(q^k - 1)$
- Impact on security and efficiency

Cofactor

- Relevant for mapping the hashed messages
- Used for finding generators of G_1 and G_2

Secret and public keys

- sk = secret key
- pk = public key
- sk selected randomly between 1 ... (r-1)
- pk = $[sk]g_1$

Signing

- m = message
- G_2 is now used
- 'Hash-and-check' → not very good
- Simplified SWU map
  - Guarantees to translate field point to point on the curve
  - Optimized for BLS12-381
- Sign → $\sigma = [sk]H(m)$

Verification

- Pairing is used
- Signature valid if $e(g_1, \sigma) = e(pk, H(m))$

$$e\big(pk, H(m)\big) = e\big([sk]g_1, H(m)\big) = e(g_1, H(m))^{(sk)}$$
$$e(g_1, H(m))^{(sk)} = e\big(g_1, [sk]H(m)\big) = e(g_1, \sigma)$$

Berner
Fachhochschule