ECC in FLOSS

More curves to the set

Sergi Blanch Torné

Collaborora

February 3, 2023

FOSDEM

Presentation Outline

ECC overview

ECC standards

Implementations

Newer curves, more standards

Choose your curve

COLLABORATION

Elliptic curves

What's an elliptic curve?

COLLABORA

Elliptic curves

What's an elliptic curve?

Elliptic curve

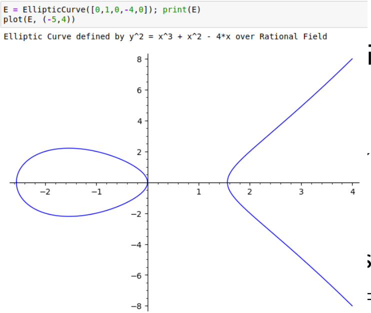
An elliptic curve over an odd field is a modular congruency with this odd number:

$$y^2 \equiv x^3 + ax + b \, (mod \, p)$$

where $a, b \in \mathbb{F}_p$
With the condition that it must **not** have singular points (aka non zero discriminant $\Delta = 4a^3 + 27b^2 \neq 0$)

Elliptic curves

What's an elliptic curve?



ield is a modular congruency

$+ b \, (mod \; p)$

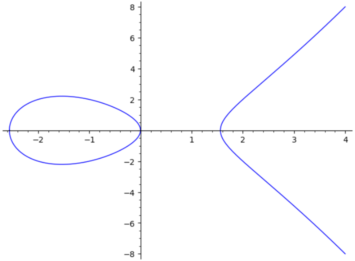
st **not** have singular points

$= 4a^3 + 27b^2 \neq 0)$

Elliptic curves

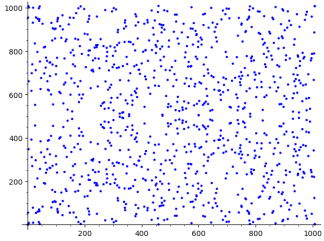
```
E = EllipticCurve([0,1,0,-4,0]); print(E)
plot(E, (-5,4))
```

```
Elliptic Curve defined by y^2 = x^3 + x^2 - 4*x over Rational Field
```




```
E_gf = E.change_ring(GF(1009)); print(E_gf)
plot(E_gf)
```

```
Elliptic Curve defined by y^2 = x^3 + x^2 + 1005*x over Finite Field of size 1009
```



What's an elliptic curve?

Elliptic curves

What's an elliptic curve?

Points on this elliptic curve

The set of points of the elliptic curve is $E/\mathbb{F}_p \cup \mathcal{O}_E$.

$$E(\mathbb{F}_p) =$$

$$\{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + ax + b\,(mod\; p) | \Delta \neq 0\}$$

$$\cup$$

$$\{\mathcal{O}_E\}$$

Elliptic curves

What's an elliptic curve?

Cyclic group for crypto

A cyclic subgroup of points over an elliptic curve:

$$\langle G \rangle = \{G, 2G, 3G, \ldots, \mathcal{O}_E = nG\}$$

where n is the order of the cyclic group. We need a big n, and $n \approx \#E(\mathbb{F}_p)$, because $|\langle G \rangle| \approx |E(\mathbb{F}_p)|$

$$h = \frac{\#E/\mathbb{F}_p}{n}$$

* On Discrete Logarithm Problem over finite fields you'll see notation like $y = g^x$ when in ec you see $Q = dP$

** Skip torsion points or Isogenies definitions

COLLABORA

Elliptic curves

- Neal Koblitz and Victor Miller independent co-discovered (for crypto purposes)

What's an elliptic curve?

Elliptic curves

- Neal Koblitz and Victor Miller independent co-discovered (for crypto purposes)
- Weiestraß Reduced Form (WRF)

$$y^2 = x^3 + ax + b \text{ over } \mathbb{F}_p$$
$$y^2 + xy = x^3 + ax^2 + b \text{ over } \mathbb{F}_{2^m}$$

What's an elliptic curve?

Elliptic curves

- Neal Koblitz and Victor Miller independent co-discovered (for crypto purposes)
- Weiestraß Reduced Form (WRF)

$$y^2 = x^3 + ax + b \text{ over } \mathbb{F}_p$$

$$y^2 + xy = x^3 + ax^2 + b \text{ over } \mathbb{F}_{2^m}$$

- Weiestraß Normal Form (WNF)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

What's an elliptic curve?

Elliptic curves

What's an elliptic curve?

- Neal Koblitz and Victor Miller independent co-discovered (for crypto purposes)
- Weiestraß Reduced Form (WRF)

$$y^2 = x^3 + ax + b \text{ over } \mathbb{F}_p$$

$$y^2 + xy = x^3 + ax^2 + b \text{ over } \mathbb{F}_{2^m}$$

- Weiestraß Normal Form (WNF)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Montgomery curves ($\mathcal{M}$)

$$By^2 = x(x^2 + Ax + 1)$$

Elliptic curves

What's an elliptic curve?

- Neal Koblitz and Victor Miller independent co-discovered (for crypto purposes)
- Weiestraß Reduced Form (WRF)
$$y^2 = x^3 + ax + b \text{ over } \mathbb{F}_p$$
$$y^2 + xy = x^3 + ax^2 + b \text{ over } \mathbb{F}_{2^m}$$
- Weiestraß Normal Form (WNF)
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
- Montgomery curves ($\mathcal{M}$)
$$By^2 = x(x^2 + Ax + 1)$$
- Edwards curves ($\mathcal{E}$) (untwisted $a = 1$, twisted $a = -1$)
$$ax^2 + y^2 = 1 + dx^2y^2$$

COLLABORA

Elliptic curves

What's an elliptic curve?

- Neal Koblitz and Victor Miller independent co-discovered (for crypto purposes)
- Weiestraß Reduced Form (WRF)
  $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$
  $y^2 + xy = x^3 + ax^2 + b$ over $\mathbb{F}_{2^m}$
- Weiestraß Normal Form (WNF)
  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- Montgomery curves ($\mathcal{M}$)
  $By^2 = x(x^2 + Ax + 1)$
- Edwards curves ($\mathcal{E}$) (untwisted $a = 1$, twisted $a = -1$)
  $ax^2 + y^2 = 1 + dx^2y^2$
- Double-odd Jacobi quartic curves ($\mathcal{J}$)
  $y^2 = (a^2 - 4b)x^4 - 2ax^2 + 1$

COLLABORA

Elliptic curves

What's an elliptic curve?

- Neal Koblitz and Victor Miller independent co-discovered (for crypto purposes)
- Weiestraß Reduced Form (WRF)
  $$y^2 = x^3 + ax + b \text{ over } \mathbb{F}_p$$
  $$y^2 + xy = x^3 + ax^2 + b \text{ over } \mathbb{F}_{2^m}$$
- Weiestraß Normal Form (WNF)
  $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
- Montgomery curves ($\mathcal{M}$)
  $$By^2 = x(x^2 + Ax + 1)$$
- Edwards curves ($\mathcal{E}$) (untwisted $a = 1$, twisted $a = -1$)
  $$ax^2 + y^2 = 1 + dx^2y^2$$
- Double-odd Jacobi quartic curves ($\mathcal{J}$)
  $$y^2 = (a^2 - 4b)x^4 - 2ax^2 + 1$$

Elliptic curves

Why $E(\mathbb{F}_q)$ better than $\mathbb{F}_p$?

COLLABORA

Elliptic curves

Why $E(\mathbb{F}_q)$ better than $\mathbb{F}_p$?

- The Discrete Logarithm Problem:
  DLP over $\mathbb{F}_p$
  requires a much larger p than
  ECDLP over $E(\mathbb{F}_p)$

Elliptic curves

Why $E(\mathbb{F}_q)$ better than $\mathbb{F}_p$?

- The Discrete Logarithm Problem:
  DLP over $\mathbb{F}_p$
  requires a much larger p than
  ECDLP over $E(\mathbb{F}_p)$
- **Yes**, smaller operations over the finite field,
  but ecc mean more operations over the finite field

Elliptic curves

Why $E(\mathbb{F}_q)$ better than $\mathbb{F}_p$?

- The Discrete Logarithm Problem:
  DLP over $\mathbb{F}_p$
  requires a much larger p than
  ECDLP over $E(\mathbb{F}_p)$
- **Yes**, smaller operations over the finite field,
  but ecc mean more operations over the finite field
- Other field can be used like $\mathbb{F}_{p^m}$
  but m prime in $\mathbb{F}_{2^m}$.

Elliptic curves

Why $E(\mathbb{F}_q)$ better than $\mathbb{F}_p$?

- The Discrete Logarithm Problem:
  DLP over $\mathbb{F}_p$
  requires a much larger p than
  ECDLP over $E(\mathbb{F}_p)$
- **Yes**, smaller operations over the finite field,
  but ecc mean more operations over the finite field
- Other field can be used like $\mathbb{F}_{p^m}$
  but m prime in $\mathbb{F}_{2^m}$.
- You can change the curve
  without changing underlying the field size.

Elliptic curves

Why $E(\mathbb{F}_q)$ better than $\mathbb{F}_p$?

- The Discrete Logarithm Problem:
  DLP over $\mathbb{F}_p$
  requires a much larger p than
  ECDLP over $E(\mathbb{F}_p)$
- **Yes**, smaller operations over the finite field,
  but ecc mean more operations over the finite field
- Other field can be used like $\mathbb{F}_{p^m}$
  but m prime in $\mathbb{F}_{2^m}$.
- You can change the curve
  without changing underlying the field size.

  This has a huge effect on cryptanalysis
  and the lifespan on embedded

Presentation Outline

ECC overview

ECC standards

Implementations

Newer curves, more standards

Choose your curve

ECC standards

- IEEE P1363-2000
- NIST 186-2
- ANSI X9.62-1998[a]
- Certicom Sec1v1 & Sec2v1

[a] Annex H.2: share curve means share cryptoanalysis

ECC standards

- IEEE P1363-2000
- NIST 186-2
- ANSI X9.62-1998[a]
- Certicom Sec1v1 & Sec2v1
- Brainpool
- GOST R 34.10

[a] Annex H.2: share curve means share cryptoanalysis

COLLABORA

ECC standards

- IEEE P1363-2000
- NIST 186-2
- ANSI X9.62-1998[a]
- Certicom Sec1v1 & Sec2v1
- Brainpool
- GOST R 34.10

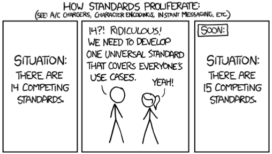
- rfc4492
- rfc5480
- rfc5639
- rfc6090
- rfc6637
- rfc7748
- rfc8734

[a] Annex H.2: share curve means share cryptoanalysis

ECC standards

- IEEE P1363-2000
- NIST 186-2
- ANSI X9.62-1998[a]
- Certicom Sec1v1 & Sec2v1
- Brainpool
- GOST R 34.10

- rfc4492
- rfc5480
- rfc5639
- rfc6090
- rfc6637
- rfc7748
- rfc8734



xkcd 927

[a] Annex H.2: share curve means share cryptoanalysis

COLLABORA

Presentation Outline

Implementations

	WRF	Edwards
OpenSSL	✓✓	✓
libgcrypt (GnuPG)	✓	✓
GnuTLS	✓	✓
Kernel	✓	✓
WolfSSL	✓	✓
crypto (rust)		✓
sequoia (rust)	✓	✓
cryptography (python)		
elliptic-py	✓	
elliptic (javascript)	✓	✓
crypto (go)	✓	✓

$*$ Not pretending to be exhaustive

✓✓ $E(\mathbb{F}_p)$ and $E(\mathbb{F}_{2^m})$

Implementations

- tor
  - torspec: rend-spec-v3[a]
    - `onion_address = base32(PUBKEY | CHECKSUM | VERSION) + ".onion`

[a] v2: was a 80-bit truncated SHA1 of a 1024 RSA key, onion addresses were 16 characters long

COLLABORA

Implementations

- tor
  - torspec: rend-spec-v3[a]
    - `onion_address = base32(PUBKEY | CHECKSUM | VERSION) + ".onion`
    - `PUBKEY`: is the 32 bytes ed25519 master pubkey of the hidden service
    - The result is a 56-characters onion address

[a] v2: was a 80-bit truncated SHA1 of a 1024 RSA key, onion addresses were 16 characters long

Implementations

- tor
  - torspec: rend-spec-v3[a]
    - `onion_address = base32(PUBKEY | CHECKSUM | VERSION) + ".onion`
    - `PUBKEY`: is the 32 bytes ed25519 master pubkey of the hidden service
    - The result is a 56-characters onion address
  - The key must not have torsion component
    (or multiple equivalent onion addresses could map to the same service).
    This is related with the `cofactor`.

[a] v2: was a 80-bit truncated SHA1 of a 1024 RSA key, onion addresses were 16 characters long

COLLABORA

Presentation Outline

COLLABORA

Edwards curves

They are Montgomery curves with a birationally equivalent [twisted] Edwards maps.

COLLABORA

Edwards curves

They are Montgomery curves with a birationally equivalent [twisted] Edwards maps.

- Curve25519 & Curve448
  - rfc7748: Few primes of the form $2^c - s$ with $<<$ s exist in $[2^{250}, 2^{521}]$

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

p	$2^{255} - 19$	$2^{448} - 2^{224} - 1$
A	486662	156326
h	8	4

NIST

  - ed25519 & ed448

$$x^2 + y^2 = a + dx^2y^2$$

Edwards curves

They are Montgomery curves with a birationally equivalent [twisted] Edwards maps.

- Curve25519 & Curve448
  - rfc7748: Few primes of the form $2^c - s$ with $<< s$ exist in $[2^{250}, 2^{521}]$

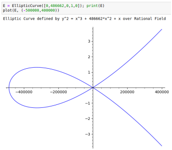
$$y^2 = x^3 + Ax^2 + x$$

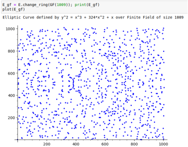
p	$2^{255} - 19$	$2^{448} - 2^{224} - 1$
A	486662	156326
h	8	4

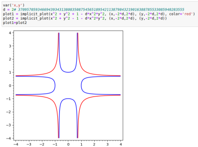
NIST

  - ed25519 & ed448

$$x^2 + y^2 = a + dx^2y^2$$







Edwards curves

They are Montgomery curves with a birationally equivalent [twisted] Edwards maps.

- Curve25519 & Curve448
  - rfc7748: Few primes of the form $2^c - s$ with $<< s$ exist in $[2^{250}, 2^{521}]$

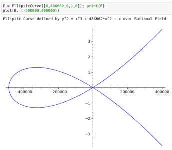
$$y^2 = x^3 + Ax^2 + x$$

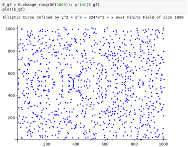
p	$2^{255} - 19$	$2^{448} - 2^{224} - 1$
A	486662	156326
h	8	4

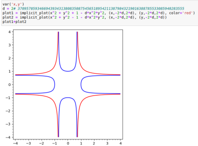
NIST

  - ed25519 & ed448

$$x^2 + y^2 = a + dx^2y^2$$







- Why they are good?
  - Build to avoid potential implementation pitfaills,
  - Immune to timing attacks,

Double-odd [Jacobi Quartic]

- `do255{e,s}`
  - curve $y^2 = x(x^2 + ax + b)$ order $2r \equiv 2 \ (mod\,4)$
  - Different base field and curves by operation:

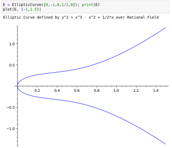
encryption	$p = 2^{255} - 18651$	$(a, b) = (0, -2)$
sign	$p = 2^{255} - 3957$	$(a, b) = (-1, \frac{1}{2})$
  - cofactor 2.
  - The mapping to a twisted Edwards curve can be used

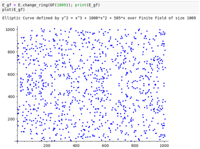
Double-odd [Jacobi Quartic]

- do255{e,s}
  - curve $y^2 = x(x^2 + ax + b)$ order $2r \equiv 2 \ (mod\, 4)$
  - Different base field and curves by operation:

    encryption $p = 2^{255} - 18651 \quad (a, b) = (0, -2)$

    sign $p = 2^{255} - 3957 \quad (a, b) = (-1, \frac{1}{2})$
  - cofactor 2.
  - The mapping to a twisted Edwards curve can be used





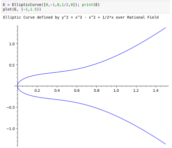
COLLABORA

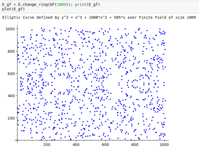
Double-odd [Jacobi Quartic]

- `do255{e,s}`
  - curve $y^2 = x(x^2 + ax + b)$ order $2r \equiv 2 \pmod 4$
  - Different base field and curves by operation:

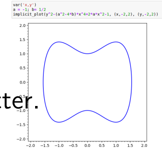
    encryption $p = 2^{255} - 18651$ $(a, b) = (0, -2)$

    sign $p = 2^{255} - 3957$ $(a, b) = (-1, \frac{1}{2})$
  - cofactor 2.
  - The mapping to a twisted Edwards curve can be used





- `jq255{e,s}`
  - Another mapping to a Jacobi Quartic: $y^2 = (a^2 - 4b)x^4 - 2ax^2 + 1$
  - Coordinates transformations and operations in the maps here they are better.
  - Even faster operations and shorter signatures



Presentation Outline

ECC overview

ECC standards

Implementations

Newer curves, more standards

Choose your curve

ristretto255, decaf448 and the zoo

- draft-irtf-cfrg-ristretto255-decaf448

ristretto255, decaf448 and the zoo

- draft-irtf-cfrg-ristretto255-decaf448
  - `Decaf` **is a technique** for constructing prime-order groups with non-malleable encodings from non-prime-order elliptic curves.
  - `Ristretto` **extends this technique** to support cofactor-8 curves such as Curve25519.

ristretto255, decaf448 and the zoo

- draft-irtf-cfrg-ristretto255-decaf448
  - `Decaf` **is a technique** for constructing prime-order groups with non-malleable encodings from non-prime-order elliptic curves.
  - `Ristretto` **extends this technique** to support cofactor-8 curves such as Curve25519.
  - Uses the **Twisted Edwards** mapping but also the **Jacobi Quartic** mapping

ristretto255, decaf448 and the zoo

- draft-irtf-cfrg-ristretto255-decaf448
  - `Decaf` **is a technique** for constructing prime-order groups with non-malleable encodings from non-prime-order elliptic curves.
  - `Ristretto` **extends this technique** to support cofactor-8 curves such as Curve25519.
  - Uses the **Twisted Edwards** mapping but also the **Jacobi Quartic** mapping
  - It is not for an specific curve, but for the maths behind a **family of curves**.

ristretto255, decaf448 and the zoo

- draft-irtf-cfrg-ristretto255-decaf448
  - `Decaf` **is a technique** for constructing prime-order groups with non-malleable encodings from non-prime-order elliptic curves.
  - `Ristretto` **extends this technique** to support cofactor-8 curves such as Curve25519.
  - Uses the **Twisted Edwards** mapping but also the **Jacobi Quartic** mapping
  - It is not for an specific curve, but for the maths behind a **family of curves**.

Perhaps there is some movement to make it easier,
so that we **don't have to share the curve!**

ristretto255, decaf448 and the zoo

- draft-irtf-cfrg-ristretto255-decaf448
  - `Decaf` **is a technique** for constructing prime-order groups with non-malleable encodings from non-prime-order elliptic curves.
  - `Ristretto` **extends this technique** to support cofactor-8 curves such as Curve25519.
  - Uses the **Twisted Edwards** mapping but also the **Jacobi Quartic** mapping
  - It is not for an specific curve, but for the maths behind a **family of curves**.

Perhaps there is some movement to make it easier,
so that we **don't have to share the curve!**

- Lenstra, A. K., & Wesolowski, B. (2015). A random zoo: sloth, unicorn, and trx. Cryptology ePrint Archive.

ristretto255, decaf448 and the zoo

- A random zoo: sloth, unicorn, and trx

ristretto255, decaf448 and the zoo

- A random zoo: sloth, unicorn, and trx
  - sloth: *slow*-time hash function

ristretto255, decaf448 and the zoo

- A random zoo: sloth, unicorn, and trx
  - sloth: *slow*-time hash function
  - unicorn: random number generator

ristretto255, decaf448 and the zoo

- A random zoo: sloth, unicorn, and trx
  - sloth: *slow*-time hash function
  - unicorn: random number generator
    - to who every one can contribute to **influence its results**
    - everyone can quickly **verify the correct inclusion** of their contribution
    - **Counter-contribution is hard**

ristretto255, decaf448 and the zoo

- A random zoo: sloth, unicorn, and trx
  - sloth: *slow*-time hash function
  - unicorn: random number generator
    - to who every one can contribute to **influence its results**
    - everyone can quickly **verify the correct inclusion** of their contribution
    - **Counter-contribution is hard**
  - trx: stream of trustworthy random ec parameters suitable for crypto

ristretto255, decaf448 and the zoo

- A random zoo: sloth, unicorn, and trx
  - sloth: *slow*-time hash function
  - unicorn: random number generator
    - to who every one can contribute to **influence its results**
    - everyone can quickly **verify the correct inclusion** of their contribution
    - **Counter-contribution is hard**
  - trx: stream of trustworthy random ec parameters suitable for crypto
    - Everyone can **influence and verify**
    - But no one can knowingly affect the choices
    - The results cannot be predicted or effectively manipulated
    - **Prevent prior cryptanalysis** or target malicious choices.

ristretto255, decaf448 and the zoo

Corollary

A random zoo: sloth, unicorn, and trx

"Is a way to **fix the small set of elliptic curves** *currently used, and it allows usage of parameters that are frequently refreshed and that cannot have been scrutinised before"*

FOSDEM

ECC in FLOSS

Thanks!

Q & A