

Pairings and pairing-friendly elliptic curves for Cryptography

An introduction for Youssef El Housni's talk of May 11

Aurore Guillevic

Aarhus University and Inria Nancy

May 4, 2022

<https://members.loria.fr/AGuillevic/files/talks/22-Aarhus-pairings.pdf>

Outline


Elliptic Curves

Pairings

Pairing-friendly curves

Materials


Steven Galbraith's Chapter IX in

 Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors.
Advances in Elliptic Curve Cryptography.
London Mathematical Society Lecture Note Series. Cambridge University Press,
2005.

Chapter 26 in

 Steven D. Galbraith.
Mathematics of Public Key Cryptography.
Cambridge University Press, 2018.
<https://www.math.auckland.ac.nz/%7Esgal018/crypto-book/main.pdf>.

Chapter 11 Section 3 in

 Lawrence C. Washington.
Elliptic Curves: Number Theory and Cryptography.
Chapman and Hall/CRC, New York, 2nd edition, 2008.

Outline

Elliptic Curves

Pairings

Pairing-friendly curves

Elliptic curves in cryptography

- 1985 (published in 1987) Hendrik Lenstra Jr., Elliptic Curve Method (ECM) for integer factoring
- 1985, Koblitz, Miller: Elliptic Curves over a finite field form a group suitable for Diffie–Hellman key exchange
- 1985, Certicom: company owning patents on ECC
- 2000 Elliptic curves in IEEE P1363 standard
- 2000 Bilinear pairings over elliptic curves
- NSA cipher suite B, elliptic curves for public-key crypto
- 2014: Quasi-polynomial-time algorithm for discrete log computation in $GF(2^n)$, $GF(3^m)$
No more pairings on elliptic curves over these fields
- 2015: Tower Number Field Sieve in $GF(p^n)$
Pairing-friendly curves should have larger key sizes
- 2016: NIST Post-Quantum competition
Isogenies on elliptic curves

Widely deployed elliptic curves in cryptosystems

- elliptic curve over the prime field $2^{255} - 19$ of order $8r$ where r is prime
 - Curve25519 in Montgomery form $E: y^2 = x^3 + 48662x^2 + x$
 - Ed25519 in twisted Edwards form $E: -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$
- NIST P-xxx curves
- ...

Usage:

- Digital signatures (ECDSA): Play Station, EU Covid Certificate...
- Diffie–Hellman key exchange: open-ssl, TLS...
- Encryption: PGP, ...

Why elliptic curves?

Diophantine equations

From Diophantus of Alexandria, mathematician

Finding integer or rational solutions to polynomial equations

Bachet equation $y^2 - x^3 = c$

given an integer c , find a cube x^3 and a square y^2 whose difference is c

Claude-Gaspard Bachet de Méziriac (1581–1638)

Translated Diophantus' *Arithmetica* from Greek to latin.

Fermat's conjecture, a.k.a. Fermat's Last Theorem

Pierre de Fermat (1601–1665)

For $n \geq 3$, the equation $X^n + Y^n = Z^n$ has no solutions in non-zero integers X, Y, Z .

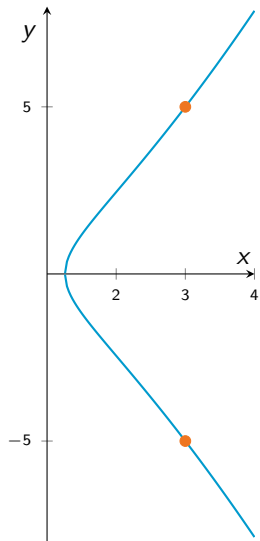
Actually not proven by Fermat



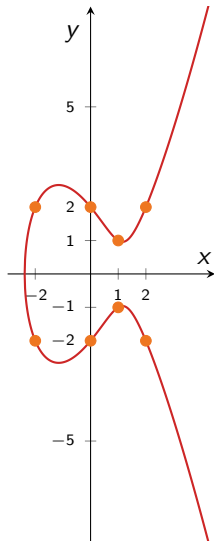
<https://www.wikitimbres.fr/>

Examples of elliptic curves

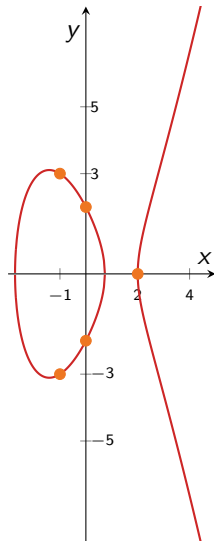
$$y^2 = x^3 - 2$$



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

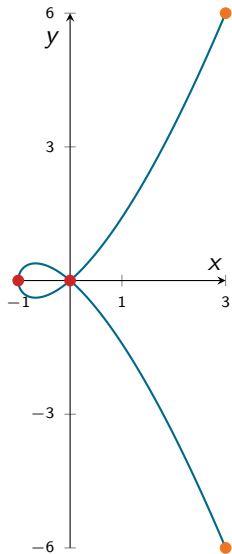


$$y^2 = x^3 - 6x + 4$$

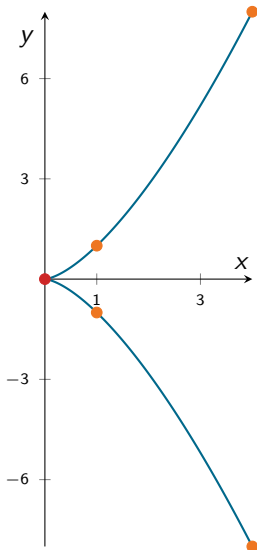


Curves with singularities are not elliptic curves

$$y^2 = x^2(x + 1)$$



$$y^2 = x^3$$



$$E: y^2 = x^3 + ax + b$$

singularities \iff

multiple roots of
 $x^3 + ax + b$

no singularities \iff

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

smooth curve

Weierstrass model

- An elliptic curve over a field \mathbb{F}_q of characteristic $\neq 2, 3$ is given by an equation of the form

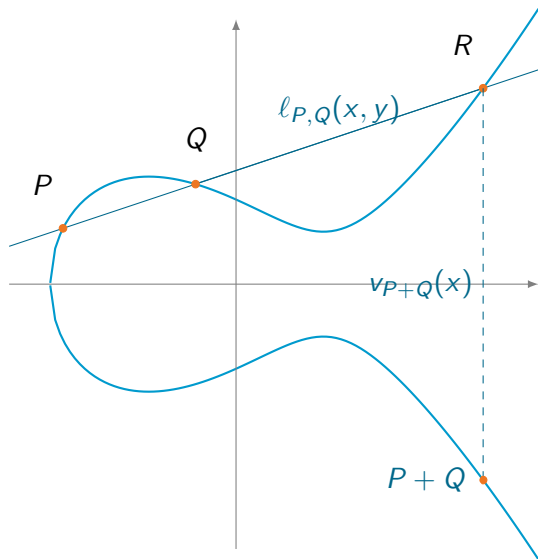
$$E: y^2 = x^3 + ax + b, \text{ with } a, b \in \mathbb{F}_q$$

and $\Delta = -16(4a^3 + 27b^2) \neq 0$ so that E is smooth

- The set of \mathbb{F}_q -rational points of an elliptic curve is

$$E(\mathbb{F}_q) = \left\{ (x, y) \in \mathbb{F}_q \times \mathbb{F}_q; y^2 = x^3 + ax + b \right\} \cup \{\mathcal{O}\}$$

Chord and tangent rule



$P(x_1, y_1), Q(x_2, y_2), x_1 \neq x_2$

$$\text{slope } \lambda = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1}$$

line L through P and Q has equation

$$L: y = \lambda(x - x_1) + y_1$$

$$P, Q, R \in L \cap E$$

Algebraic description of the addition operation

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on

$$E: y^2 = x^3 + ax + b .$$

The slope of the line (P_1, P_2) is given by

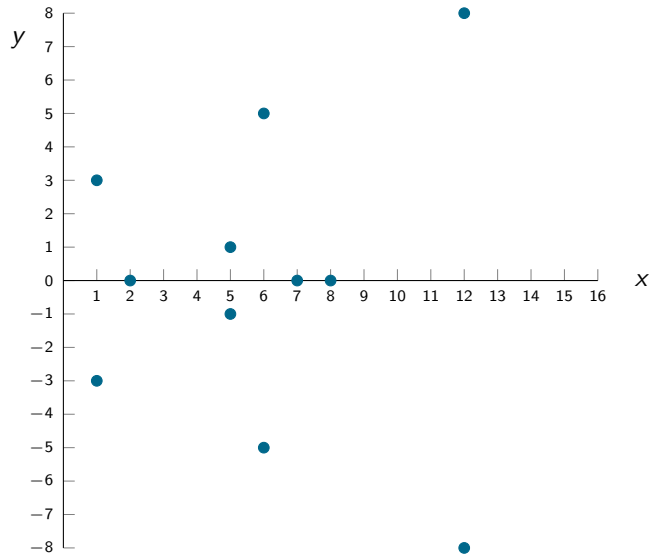
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2 \\ \frac{3x_1 + a}{2y_1} & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0 \end{cases}$$

The sum of P and Q is the point

$$P + Q = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1) .$$

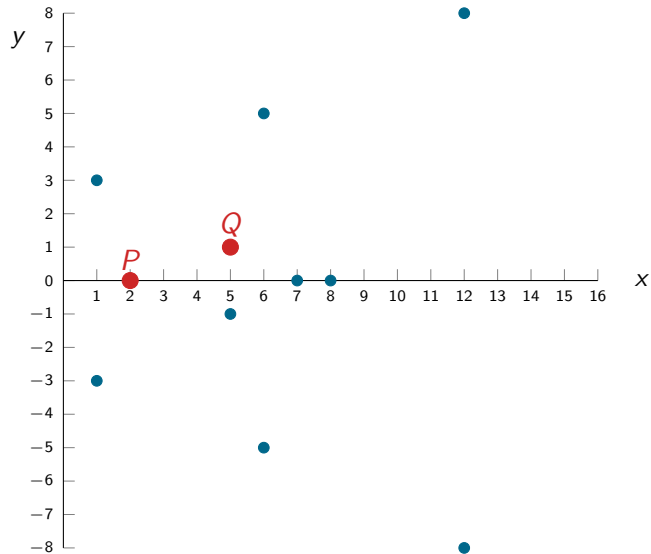
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}: y^2 = x^3 + x + 7$$



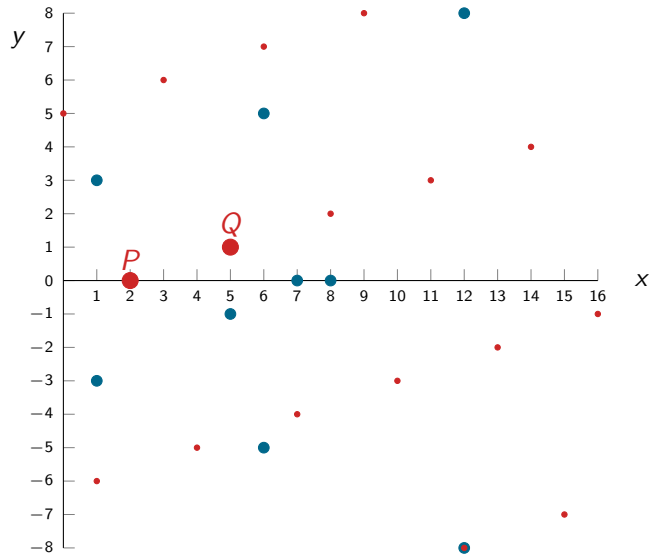
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}: y^2 = x^3 + x + 7$$



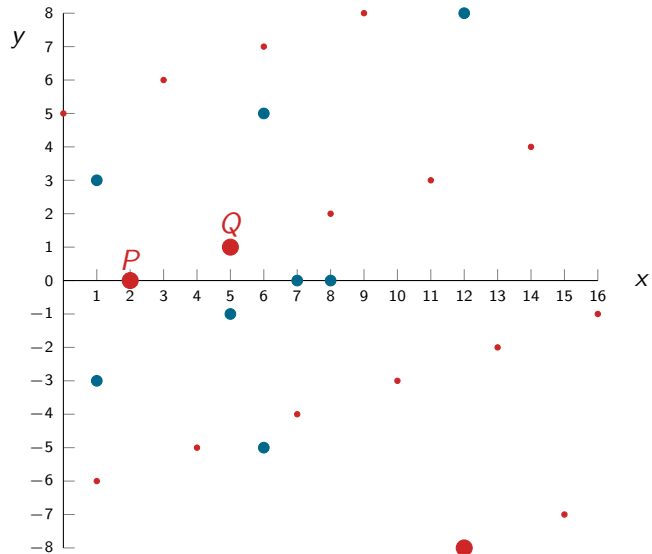
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}: y^2 = x^3 + x + 7$$



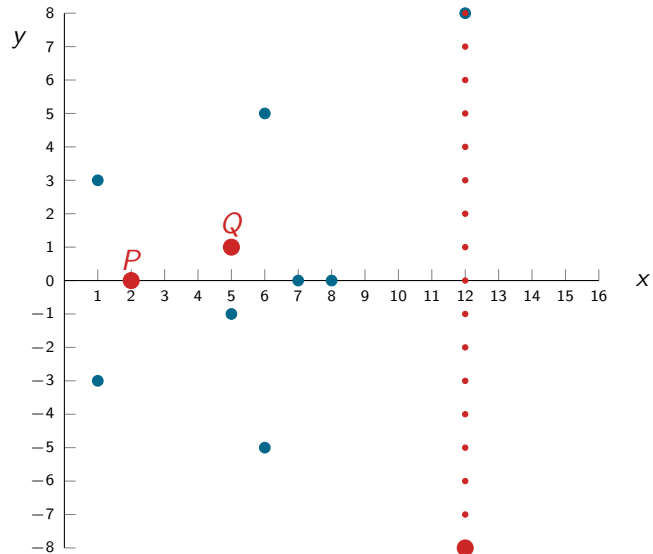
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}: y^2 = x^3 + x + 7$$



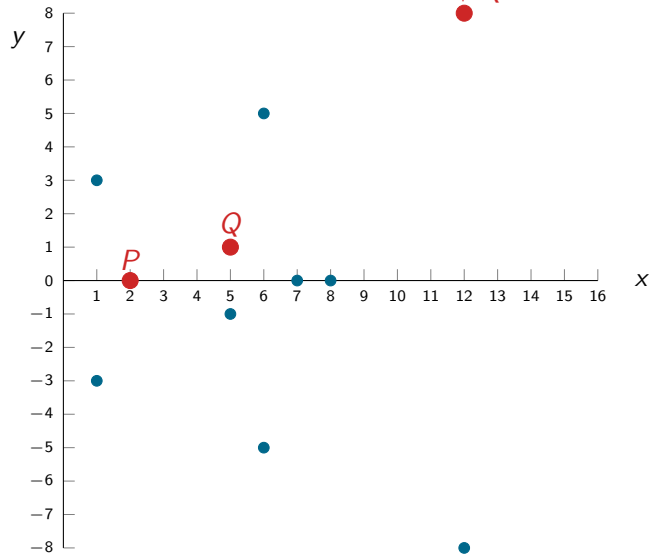
Elliptic curves over finite fields

$$E/\mathbb{F}_{17}: y^2 = x^3 + x + 7$$



Elliptic curves over finite fields

$$E/\mathbb{F}_{17}: y^2 = x^3 + x + 7$$



Scalar multiplication

With an addition law on \mathcal{E} , the points on the curve form a group $\mathcal{E}(K)$.

Scalar multiplication (exponentiation)

The **multiplication-by- m** map, or **scalar multiplication** is

$$\begin{aligned} [m]: \mathcal{E} &\rightarrow \mathcal{E} \\ P &\mapsto \underbrace{P + \dots + P}_{m \text{ copies of } P} \end{aligned}$$

for any $m \in \mathbb{Z}$, with $[-m]P = [m](-P)$ and $[0]P = \mathcal{O}$.

- a key-ingredient operation in public-key cryptography
- given $m > 0$, computing $[m]P$ as $P + P + \dots + P$ with $m - 1$ additions is **exponential** in the size of m : $m = e^{\ln m}$
- we can compute $[m]P$ in $O(\log m)$ operations on \mathcal{E} .

Naive Scalar multiplication: Double-and-Add

Input: \mathcal{E} defined over a field K , $m > 0$, $P \in \mathcal{E}(K)$

Output: $[m]P \in \mathcal{E}$

1 **if** $m = 0$ **then return** \mathcal{O}

2 Write m in binary expansion $m = \sum_{i=0}^{n-1} b_i 2^i$ where $b_i \in \{0, 1\}$

3 $R \leftarrow P$

4 **for** $i = n - 2$ **downto** 0 **do**

loop invariant: $R = [\lfloor m/2^i \rfloor]P$

5 $R \leftarrow [2]R$

6 **if** $b_i = 1$ **then**

7 $R \leftarrow R + P$

8 **return** R

Question: What are the best- and worst-case costs of the algorithm?

Question: Why is this algorithm dangerous if m is secret?

Outline

Elliptic Curves

Pairings

Pairing-friendly curves

What is a pairing?

$(\mathbf{G}_1, +)$, $(\mathbf{G}_2, +)$, (\mathbf{G}_T, \cdot) three cyclic groups of large prime order ℓ

Pairing: map $e : \mathbf{G}_1 \times \mathbf{G}_2 \rightarrow \mathbf{G}_T$

1. bilinear: $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$, $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. non-degenerate: $e(G_1, G_2) \neq 1$ for $\langle G_1 \rangle = \mathbf{G}_1$, $\langle G_2 \rangle = \mathbf{G}_2$
3. efficiently computable.

Most often used in practice:

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

\leadsto Many applications in asymmetric cryptography.

Pairings in cryptography: 1993 and 2001

1993

Menezes–Okamoto–Vanstone attack on supersingular curves

2001

- Joux' tri-partite key exchange
- Boneh Franklin Identity based encryption
- Boneh Lynn Shacham short signature

Example of application: identity-based encryption

- 1984: idea of identity-based encryption formalized by Shamir
- 1999: first practical identity-based cryptosystem of Sakai-Ohgishi-Kasahara
- 2000: constructive pairings, Joux's tri-partite key-exchange
- 2001: IBE of Boneh-Franklin

Example of application: identity-based encryption

- 1984: idea of identity-based encryption formalized by Shamir
- 1999: first practical identity-based cryptosystem of Sakai-Ohgishi-Kasahara
- 2000: constructive pairings, Joux's tri-partite key-exchange
- 2001: IBE of Boneh-Franklin

Rely on one of

- Discrete Log Problem (DLP): given $g, y \in \mathbf{G}$, compute x s.t. $g^x = y$
- Diffie-Hellman Problem (DHP): given $g, x, y \in \mathbf{G}$, compute $z \in \mathbf{G}$ s.t. $z = g^{ab}$ where a, b satisfy $x = g^a, y = g^b$
- bilinear DLP : Given $\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_T, g_1, g_2, g_T$ and $y \in G_T$, compute $P \in \mathbf{G}_1$ s.t. $e(P, g_2) = y$, or $Q \in \mathbf{G}_2$ s.t. $e(g_1, Q) = y$ if $g_T^x = y$ then $e(g_1^x, g_2) = e(g_1, g_2^x) = g_T^x = y$
- bilinear DHP: 3-dimensional DHP
- pairing inversion problem

Pairing setting: elliptic curves

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p, \quad p \geq 5$$

- proposed in 1985 by Koblitz, Miller
- $E(\mathbb{F}_p)$ has an efficient group law (chord and tangent rule) $\rightarrow \mathbf{G}_1$
- $\#E(\mathbb{F}_p) = p + 1 - t$, trace t : $|t| \leq 2\sqrt{p}$
- efficient group order computation (*point counting*)

Pairing setting: elliptic curves

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p, \quad p \geq 5$$

- proposed in 1985 by Koblitz, Miller
- $E(\mathbb{F}_p)$ has an efficient group law (chord and tangent rule) $\rightarrow \mathbf{G}_1$
- $\#E(\mathbb{F}_p) = p + 1 - t$, trace t : $|t| \leq 2\sqrt{p}$
- efficient group order computation (*point counting*)
- large subgroup of prime order ℓ s.t. $\ell \mid p + 1 - t$ and ℓ coprime to p
- $E(\mathbb{F}_p)[\ell] = \{P \in E(\mathbb{F}_p) : [\ell]P = \mathcal{O}\}$ has order ℓ
- $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ (for crypto)
- only generic attacks against DLP on well-chosen genus 1 and genus 2 curves
- optimal parameter sizes

Tate Pairing and modified Tate pairing

$$\ell \mid p^n - 1, E[\ell] \subset E(\mathbb{F}_{p^n})$$

Tate Pairing: $e : E(\mathbb{F}_{p^n})[\ell] \times E(\mathbb{F}_{p^n})/\ell E(\mathbb{F}_{p^n}) \rightarrow \mathbb{F}_{p^n}^*/(\mathbb{F}_{p^n}^*)^\ell$ (equivalence classes)

For cryptography,

- $\mathbf{G}_1 = E(\mathbb{F}_p)[\ell] = \{P \in E(\mathbb{F}_p), [\ell]P = \mathcal{O}\}$
- embedding degree $n > 1$ w.r.t. ℓ : smallest¹ integer n s.t. $\ell \mid p^n - 1$
 $\Leftrightarrow E[\ell] \subset E(\mathbb{F}_{p^n})$
- $\mathbf{G}_2 \subset E(\mathbb{F}_{p^n})[\ell]$
- $\mathbf{G}_1 \cap \mathbf{G}_2 = \mathcal{O}$ by construction for practical applications
- $\mathbf{G}_T = \mu_\ell = \{u \in \mathbb{F}_{p^n}^*, u^\ell = 1\} \subset \mathbb{F}_{p^n}^*$

When n is small i.e. $1 \leq n \leq \sim 50$, the curve is *pairing-friendly*.

This is very rare: For a given curve, $\log n \sim \log \ell$ (Balasubramanian–Koblitz).

¹ $n = 1$ is possible too in rare circumstances

Divisors

Let E be an elliptic curve defined over a field K .

Definitions

A **divisor** is a *finite* formal sum of points $P_i \in E(K)$, $D = \sum_{i=1}^n a_i(P_i)$, $a_i \neq 0 \in \mathbb{Z}^\times$

Degree: $\deg(D) = \sum_{i=1}^n a_i \in \mathbb{Z}$: sum of the weights a_i , can be 0

Sum: $\text{sum}(D) = a_1 P_1 + \dots + a_n P_n$ the sum on E of the weighted points $a_i P_i$.

Support: $\text{supp}(D) = \{P_i\}_{1 \leq i \leq n}$ the set of points of D of weight $a_i \neq 0$.

Evaluating a function at a divisor

Let $D = \sum_{i=1}^n a_i(P_i) - (\sum_{j=1}^m a_j(P_j))$ where $a_i, a_j > 0$.

$$f(D) = \frac{\prod_{i=1}^n (f(P_i))^{a_i}}{\prod_{j=1}^m (f(P_j))^{a_j}}$$

Tate Pairing

$$\ell \mid p^n - 1, E[\ell] \subset E(\mathbb{F}_{p^n})$$

$$P \in \mathbf{G}_1 \subset E(\mathbb{F}_{p^n})[\ell], Q \in \mathbf{G}_2 \subset E(\mathbb{F}_{p^n})[\ell].$$

Definition: Tate pairing

Let D_Q be a divisor such that $\text{sum}(D_Q) = Q$, $\text{deg}(D_Q) = 0$, and $P, \mathcal{O} \notin \text{supp}(D_Q)$.

Let f_P be a function whose divisor is $\text{Div}(f_P) = [\ell]P - [\ell]\mathcal{O}$.

One has $\text{supp}(f_P) \cap \text{supp}(D_Q) = \emptyset$.

$$e_{\text{Tate}}(P, Q) = f_P(D_Q) \in \mathbb{F}_{p^n}^* / (\mathbb{F}_{p^n}^*)^\ell$$

Example: choose some point $R \neq \mathcal{O}, P$ s.t. $R + Q \neq \mathcal{O}, P$ and set $D_Q = (Q + R) - (R)$, then

$$e_{\text{Tate}}(P, Q) = \frac{f_P(Q + R)}{f_P(R)}.$$

Tate pairing

From its definition to its efficient implementation

- John Tate, 1958
- Stephen Lichtenbaum, 1969
- Victor Miller, 1986, Miller algorithm for f_P
- Frey–Rück, 1994: the MOV attack with the Tate pairing instead of the Weil pairing
- Harasawa, Shikata, Suzuki, Imai, 1999, 161467 s (112 days)
163-bit supersingular curve, $\mathbf{G}_T \subset \mathbb{F}_{p^2}$ of 326 bits.
- Antoine Joux, 2000: how to compute Miller algorithm more efficiently
1 s on a supersingular 528-bit curve, $\mathbf{G}_T \subset \mathbb{F}_{p^2}$ of 1055 bits)

Modified Tate pairing

Avoid equivalence classes:

need one representative of the equivalence class instead.

Ensure the pairing is non-degenerate: $\mathbf{G}_1 \cap \mathbf{G}_2 = \mathcal{O}$

$$E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}\ell\mathbb{Z} = \mathbf{G}_1 \times \mathbf{G}_2$$

Let $P \in \mathbf{G}_1 = E(\mathbb{F}_p)[\ell]$, $Q \in \mathbf{G}_2 \subset E(\mathbb{F}_{p^n})[\ell]$.

Let $f_{\ell,P}$ the function s. t. $\text{Div}(f_{\ell,P}) = \ell(P) - \ell(\mathcal{O})$.

Modified Tate pairing (in cryptography):

$$\begin{array}{ccc} E(\mathbb{F}_p)[\ell] & & E(\mathbb{F}_{p^n})[\ell] \\ \wr & & \cup \\ \mathbf{G}_1 & \times & \mathbf{G}_2 \\ & (P, Q) & \end{array} \begin{array}{l} \rightarrow \mu_\ell \subset \mathbb{F}_{p^n}^* \\ \mapsto (f_{\ell,P}(Q))^{\frac{p^n-1}{\ell}} \end{array}$$

Modified Tate pairing

Final exponentiation to avoid equivalence classes in $\mathbb{F}_{p^n}^*$

$x \mapsto x^{(p^n-1)/\ell}$ clears the cofactors in $(\mathbb{F}_{p^n}^*)^\ell$.

Consider the ℓ -powering $x \mapsto x^\ell$ as an endomorphism of $\mathbb{F}_{p^n}^*$

- $(\cdot)^\ell$ has image $(\mathbb{F}_{p^n}^*)^\ell$ and kernel $\mu_\ell = \{x \in \mathbb{F}_{p^n}^* : x^\ell = 1\}$
- $x_1 \equiv x_2 \in \mathbb{F}_{p^n}^*/(\mathbb{F}_{p^n}^*)^\ell \iff x_1 \cdot x_2^{-1} \in (\mathbb{F}_{p^n}^*)^\ell \iff (x_1/x_2)^{(p^n-1)/\ell} = 1$

Replace Divisor D_Q by point Q in the evaluation

Replace $f_{\ell,P}(Q + R)/f_{\ell,P}(R)$ by $(f_{\ell,P}(Q))^{\frac{p^n-1}{\ell}}$

Lemma 26.3.11 in Galbraith's book

Miller algorithm

Principal divisor

A divisor D is **principal** $\iff \deg(D) = 0$ and $\text{sum}(D) = \mathcal{O}$.

In that case there exists a function f_D whose divisor is D .

Miller function

The Tate pairing requires a function f_P of divisor $\ell(P) - \ell(\mathcal{O})$.

$D = \ell(P) - \ell(\mathcal{O})$ is principal $\implies f_P$ exists.

Define the Miller function $f_{i,P}$ to have divisor

$$D_{i,P} = \text{Div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O})$$

- $\deg(D_{i,P}) = 0$
- $\text{sum}(D_{i,P}) = \mathcal{O}$
- $D_{i,P}$ is principal
- $D_{\ell,P} = \ell(P) - \ell(\mathcal{O}) = \text{Div}(f_P)$

Miller Loop

Input: integer s , points P, Q of order s

Output: $m = f_{s,P}(Q)$, where $\text{Div}(f) = s(P) - s(\mathcal{O})$

```
1  $m \leftarrow 1; S \leftarrow P;$ 
2 for  $b$  from the second most significant bit of  $s$  to the least do
3    $\ell \leftarrow \ell_{S,S}(Q); S \leftarrow [2]S;$  // Double Line
4    $v \leftarrow v_{[2]S}(Q);$  // Vertical Line
5    $m \leftarrow m^2 \cdot \ell/v;$  // Update 1
6   if  $b = 1$  then
7      $\ell \leftarrow \ell_{S,P}(Q); S \leftarrow S + P;$  // Add Line
8      $v \leftarrow v_{S+Q}(Q);$  // Vertical Line
9      $m \leftarrow m \cdot \ell/v;$  // Update 2
10 return  $m;$ 
```

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e : E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e : E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Attacks

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e : E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$



Attacks

- inversion of e : hard problem (exponential)

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e : E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$


Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{\ell})$)

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e : E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^n})[\ell] \longrightarrow \mathbb{F}_{p^n}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$


Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{\ell})$)
- discrete logarithm computation in $\mathbb{F}_{p^n}^*$: **easier, subexponential** \rightarrow take a large enough field

Outline

Elliptic Curves

Pairings

Pairing-friendly curves

First ordinary pairing-friendly curves: MNT

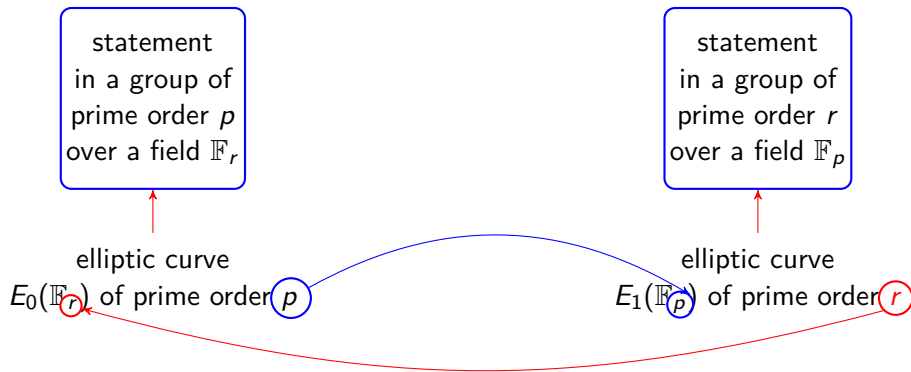
Miyaji, Nakabayashi, Takano, $\#E(\mathbb{F}_p) = p(u) + 1 - t(u)$, $r(u) \mid \#E(\mathbb{F}_p)$

| k | param | MNT |
|-----|--------|-------------------------|
| 3 | $t(u)$ | $-1 \pm 6u$ |
| | $r(u)$ | $12u^2 \mp 6u + 1$ |
| | $p(u)$ | $12u^2 - 1$ |
| | Dy^2 | $12u^2 \pm 12u - 5$ |
| 4 | $t(u)$ | $-u, u + 1$ |
| | $r(u)$ | $u^2 + 2u + 2, u^2 + 1$ |
| | $p(u)$ | $u^2 + u + 1$ |
| | Dy^2 | $3u^2 + 4u + 4$ |
| 6 | $t(u)$ | $1 \pm 2u$ |
| | $r(u)$ | $4u^2 \mp 2u + 1$ |
| | $p(u)$ | $4u^2 + 1$ |
| | Dy^2 | $12u^2 - 4u + 3$ |

CODA: $k = 6$, 753 bits, ≈ 137 bits of security, $D = -241873351932854907$, seed $u =$

0xaa3a58eb20d1fec36e5e772ee6d3ff28c296465f137300399db8a5521e18d33581a262716214583d3b89820dd0c000

Cycle of curves



MNT-4 and MNT-6 curves form a cycle

$$\begin{array}{llll} k = 4, \text{ MNT-4 parameters} & t_4 = -v, & r_4 = v^2 + 1, & p_4 = v^2 + v + 1 \\ k = 6, \text{ MNT-6 parameters} & t_6 = 1 - 2u, & r_6 = 4u^2 + 2u + 1, & p_6 = 4u^2 + 1 \end{array}$$

$$\begin{array}{ll} r_4 = p_6 & v = 2u \\ \text{and} & \iff \text{and} \\ p_4 = r_6 & r_4, r_6 \text{ are primes} \end{array}$$

Unique known cycle of pairing-friendly curves.

Impossibility results:



Alessandro Chiesa, Lynn Chua, and Matthew Weidner.

On cycles of pairing-friendly elliptic curves.

SIAM Journal on Applied Algebra and Geometry, 3(2):175–192, 2019.

Very popular pairing-friendly curves: Barreto-Naehrig (BN)

$$E_{BN} : y^2 = x^3 + b, \quad p \equiv 1 \pmod{3}, \quad D = -3 \text{ (ordinary)}$$

$$p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$

$$t = 6x^2 + 1$$

$$\ell = p + 1 - t = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

$$t^2 - 4p = -3(6x^2 + 4x + 1)^2 \rightarrow \text{no CM method needed}$$

Comes from the Aurifeuillean factorization of Φ_{12} :

$$\Phi_{12}(6x^2) = \ell(x)\ell(-x)$$

| Security level | $\log_2 \ell$ | finite field | n | $\log_2 p$ | $\deg P, p = P(u)$ | ρ |
|----------------|---------------|--------------|-----|------------|--------------------|--------|
| 102 | 256 | 3072 | 12 | 256 | 4 | 1 |
| 123 | 384 | 4608 | 12 | 384 | 4 | 1 |
| 132 | 448 | 5376 | 12 | 448 | 4 | 1 |

BLS12

Barreto, Lynn, Scott method.

Becomes more and more popular, replacing BN curves

$$E_{BLS} : y^2 = x^3 + b, \quad p \equiv 1 \pmod{3}, \quad D = -3 \text{ (ordinary)}$$

$$p = (u - 1)^2 / 3(u^4 - u^2 + 1) + u$$

$$t = u + 1$$

$$r = (u^4 - u^2 + 1) = \Phi_{12}(u)$$

$$p + 1 - t = (u - 1)^2 / 3(u^4 - u^2 + 1)$$

$$t^2 - 4p = -3y(u)^2 \rightarrow \text{no CM method needed}$$

BLS12-381 with seed `-0xd201000000010000`

The Cocks–Pinch method

Three equations:

$$\ell \mid p + 1 - t \quad (1)$$

$$\ell \mid \Phi_n(p) \quad (2)$$

$$t^2 - 4p = -Dy^2 \quad (3)$$

From (1), $p \equiv t - 1 \pmod{\ell}$

From (2) and (1), $\ell \mid \Phi_n(t - 1) \iff t - 1 = \zeta_n \pmod{\ell}$

where ζ_n is a primitive n -th root of unity modulo ℓ , ζ_n exists $\iff \ell \equiv 1 \pmod{n}$.

$$\mathbf{t = \zeta_n + 1 \pmod{\ell}}$$

From (3) and (1), with $p = (t^2 + Dy^2)/4$,

$$p + 1 - t = \frac{1}{4} (t^2 - 4t + 4 + Dy^2) = \frac{1}{4} ((t - 2)^2 + Dy^2)$$

Because $\ell \mid p + 1 - t$, assuming ℓ odd,

$$(t - 2)^2 + Dy^2 = 0 \pmod{\ell} \implies \mathbf{y = \frac{t - 2}{\sqrt{-D}} \pmod{\ell}}$$

The Cocks–Pinch method

Input: A positive integer n and a positive square-free integer D

Output: E/\mathbb{F}_q with an order- ℓ subgroup and embedding degree n

- 1 Choose a prime ℓ such that n divides $\ell - 1$ and $-D$ is a square modulo ℓ
 - 2 Compute $t = 1 + x^{(\ell-1)/n}$ for x a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$, $t - 1 \equiv \zeta_n \pmod{\ell}$
 - 3 Compute $y = (t - 2)/\sqrt{-D} \pmod{\ell}$
 - 4 Lift t and y in \mathbb{Z}
 - 5 Compute $q = (t^2 + Dy^2)/4$ in \mathbb{Q}
 - 6 **if** q is a prime integer **then**
 - 7 | Use CM method ($D < 10^{20}$) to get the coefficients of E/\mathbb{F}_q with order- ℓ subgroup
 - 8 **else**
 - 9 | Go back to 1
 - 10 **return** E/\mathbb{F}_q with an order- ℓ subgroup and embedding degree n
-

The Cocks–Pinch method

Drawback: $\log |t|, \log |y| \approx \log \ell \implies \log p \approx 2 \log \ell$

rho-value:

$$\rho = \frac{\log p}{\log \ell} \approx 2$$

The optimal would be $\rho = 1$ for a prime-order curve, $\ell = p + 1 - t$.

How to compute primitive n -th roots of unity:

Input: prime ℓ , integer $n > 0$, $\ell \equiv 1 \pmod n$

Output: $\zeta_n \pmod \ell$

- 1 $z \leftarrow \text{random}(\ell)$
 - 2 $z \leftarrow z^{(\ell-1)/n}$
 - 3 **while** $\Phi_n(z) \not\equiv 0 \pmod \ell$ (or: $z^d = 1 \pmod \ell$ for some $d \mid n$, $1 \leq d < n$) **do**
 - 4 $z \leftarrow \text{random}(\ell)$
 - 5 $z \leftarrow z^{(\ell-1)/n}$
 - 6 **return** z
-

The CM method (Complex Multiplication)

Hard problem to compute the curve coefficients (a, b) given a prime p and a trace t .
The other way: given p and (a, b) in E/\mathbb{F}_p : $y^2 = x^3 + ax + b$ and computing the order $\#E(\mathbb{F}_p)$ is done with the SEA algorithm (Schroof–Elkies–Atkin).

The CM method computes a j -invariant, given p, t .

1. Compute the discriminant $-D$ as the square-free part in $t^2 - 4p = -Dy^2$
2. If $D \equiv 1, 2 \pmod{4}$, $D \leftarrow 4D$
3. Compute a Hilbert Class Polynomial $H_{-D}(X) \pmod{p}$ with Sutherland's software classpoly at <https://math.mit.edu/~drew/>
4. Compute a root j_0 of $H_{-D}(X) \pmod{p}$
5. Set $E: y^2 = x^3 + \frac{3j_0}{1728-j_0}x + \frac{2j_0}{1728-j_0}$

The CM method

For specific (small) values of $-D$, the j -invariants are known:

- $-D = -3, j = 0$
- $-D = -4, j = 1728$
- $-D = -8, j = 8000$
- $-D = -7, j = -3375$
- $-D = -11, j = -32768$
- $-D = -19, j = -884736$
- $-D = -43, j = -884736000$
- $-D = -67, j = -147197952000$
- $-D = -163, j = -262537412640768000$

The Brezing–Weng method: The Cocks–Pinch method with polynomials

Start with $r(x)$ an irreducible polynomial s.t. the number field $K = \mathbb{Q}[x]/(r(x))$ contains ζ_n and $\sqrt{-D}$

Algorithm 1: Idea of Barreto–Lynn–Scott and Brezing–Weng methods

Input: A positive integer n and a positive square-free integer D

Output: Polynomials $p(x), r(x), t(x)$ s.t. $t^2(x) - 4p(x) = -Dy^2(x)$,
 $r(x) \mid p(x) + 1 - t(x)$, $r(x) \mid \Phi_n(p(x))$

- 1 Choose an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ with positive leading coefficient such that $\sqrt{-D}$ and $\zeta_n \in K = \mathbb{Q}[x]/(r(x))$
 - 2 Choose $t(x) \in \mathbb{Q}[x]$ a polynomial representing $\zeta_n + 1$ in K
 - 3 Set $y(x) \in \mathbb{Q}[x]$ a polynomial mapping to $(\zeta_n - 1)/\sqrt{-D}$ in K
 - 4 Compute $p(x) = (t^2(x) + Dy^2(x))/4$ in $\mathbb{Q}[x]$
 - 5 If $p(x)$ does not represent primes go back to 1 or 2
 - 6 **return** $p(x), r(x), t(x)$
-

The BLS family

If $3 \mid n$, then $\sqrt{-3} \in K = \mathbb{Q}[x]/(\Phi_n(x))$

- $n = 3$: $\zeta_3 = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$, $\Phi_3 = x^2 + x + 1$

For $n \equiv 3 \pmod{6}$, $\zeta_3 = x^{n/3} \pmod{\Phi_n(x)}$

$$\sqrt{-3} = 2x^{n/3} + 1 \text{ and } 1/\sqrt{-3} = \sqrt{-3}/3 = (2x^{n/3} + 1)/3$$

- $n = 6$: $\zeta_6 = \frac{11+\sqrt{-3}}{2} \in \mathbb{C}$, $\Phi_6 = x^2 - x + 1$

For $n \equiv 0 \pmod{6}$, $\zeta_6 = x^{n/6} \pmod{\Phi_n(x)}$

$$\sqrt{-3} = 2x^{n/6} - 1 \text{ and } 1/\sqrt{-3} = \sqrt{-3}/3 = (2x^{n/6} - 1)/3$$

Given n multiple of 3,

1. $r(x) \leftarrow \Phi_n(x)$
2. $t(x) \leftarrow x + 1$
3. $y(x) \leftarrow (x - 1)/\sqrt{-3}$
 - $y(x) = (x - 1)(2x^{n/3} + 1)/3$ if $n \equiv 3 \pmod{6}$
 - $y(x) = (x - 1)(2x^{n/6} - 1)/3$ if $n \equiv 0 \pmod{6}$
4. $p(x) = (t^2(x) + 3y^2(x))/4$

Tate pairing

Let E be an elliptic curve over a finite field \mathbb{F}_q , let $\ell \mid \#E(\mathbb{F}_q)$, $\gcd(\ell, q) = 1$

pre- \mathbf{G}_1 , \mathbf{G}_2 and \mathbf{G}_T

With $\ell E(\mathbb{F}_q) = \{[\ell]Q : Q \in E(\mathbb{F}_q)\}$

- $E(\mathbb{F}_q)[\ell] = \{P \in E(\mathbb{F}_q) : [\ell]P = \mathcal{O}\}$ has order ℓ
- $E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) = \{P + \ell E(\mathbb{F}_q) : P \in E(\mathbb{F}_q)\}$ has order ℓ
- $\mathbb{F}_q^*/(\mathbb{F}_q^*)^\ell$ has order ℓ

The multiplication-by- ℓ map $[\ell]$ on $E(\mathbb{F}_q)$ has image $\ell E(\mathbb{F}_q)$ and kernel $E(\mathbb{F}_q)[\ell]$.

$E(\mathbb{F}_q)/\ell E(\mathbb{F}_q)$ is a notation for an *equivalence relation* $P, Q \in G/H \iff P - Q \in H$

$P, Q \in E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) \iff P - Q \in \ell E(\mathbb{F}_q)$

$E(\mathbb{F}_q)/\ell E(\mathbb{F}_q)$ is the quotient of $E(\mathbb{F}_q)$ by the image of $[\ell]$, and has order ℓ .