Cyclic Groups in Cryptography

Palash Sarkar

Indian Statistical Institute

Structure of Presentation

- Exponentiation in General Cyclic Groups.
- Cyclic Groups from Finite Fields.
- Cyclic Groups from Elliptic Curves.
- Bilinear Pairings in Cryptography.

Exponentiation in General Cyclic Groups

Exponentiation

Let $G = \langle g \rangle$ be a cyclic group of order $|G| = q$.

Basic Problem:

Input: $a \in \mathbb{Z}_q$.

Task: Compute $h = g^a$.

Let $a = a_{n-1} \dots a_0$,

- $n = \lceil \log_2 q \rceil$;
- each a_i is a bit.

Two simple methods.

- Right-to-left.
- Left-to-right.

Right-to-Left

- $n = 1$: $h = g^{a_0}$.
- $n = 2$: $h = g^{2a_1+a_0} = (g^2)^{a_1} \times g^{a_0}$.
  $t = g; r = g^{a_0};$
  $t = t^2; r = t^{a_1} \times r; h = r.$
- $n = 3$: $h = g^{2^2 a_2+2a_1+a_0} = (g^{2^2})^{a_2} \times (g^2)^{a_1} \times g^{a_0}$.
  $t = g; r = g^{a_0};$
  $t = t^2; r = t^{a_1} \times r;$
  $t = t^2; r = t^{a_2} \times r; h = r.$
- At ith step: square t; multiply t to r if $a_i = 1$.

Left-to-Right

- $n = 1$: $h = g^{a_0}$.
- $n = 2$: $h = g^{2a_1+a_0} = (g^{a_1})^2 \times g^{a_0}$.
  $r = g^{a_1}$;
  $r = r^2 \times g^{a_0}$; $h = r$.
- $n = 3$: $h = g^{2^2 a_2+2a_1+a_0} = ((g^{a_2})^2 \times g^{a_1})^2 \times g^{a_0}$.
  $r = g^{a_2}$;
  $r = r^2 \times g^{a_1}$;
  $r = r^2 \times g^{a_0}$; $h = r$.
- At ith step: square r; multiply r by g if $a_{n-i} = 1$.
- Important: always multiply by g.

Also called square-and-multiply algorithm.

Addition Chains

An addition chain of length ℓ is a sequence of $\ell + 1$ integers such that

- the first integer is 1;
- each subsequent integer is a sum of two previous integers.

Example: 1,2,3,5,7,14,28,56,63.

Addition chains can be used to compute powers.

Consider the set of $(n_1, \ldots, n_p, \ell)$ such that there is an addition chain of length ℓ containing $n_1, \ldots, n_p$.

- Downey, Leong and Sethi (1981) proved this set to be NP-complete.

Exponentiation Algorithms

A survey by Bernstein with the title

Pippenger's Exponentiation Algorithm

- Brauer (1939): "the left-to-right 2^k-ary method".
- Straus (1964): computes a product of p powers with possibly different bases.
- Yao (1976): computes a sequence of p powers of a single base.
- Pippenger (1976): improves on both Straus's and Yao's algorithm.

Cyclic Groups from Finite Fields

Structure of Finite Fields

Let $(\mathbb{F}, +, *)$ be a finite field with $q = |\mathbb{F}|$.

- $q = p^m$, where p is a prime and $m \geq 1$;
  p is called the characteristic of the field.
- $(\mathbb{F}, +)$ is a commutative group.
- $(\mathbb{F}^* = \mathbb{F} \setminus \{0\}, *)$ is a cyclic group.

Basic Operations:

- addition and subtraction;
- multiplication;
- inversion (and division).

Useful Fields

We are interested in “large” fields: $p^m \approx 2^{256}$.

Commonly used fields.

- Large characteristics: $m = 1$ and p is “large”.
- Characteristics 2: $p = 2$.
- Characteristics 3: $p = 3$, relevant for pairing based cryptography.
- Other composite fields: Optimal extension fields.

Criteria for choosing a field:
security/efficiency trade-off.

Large Characteristics

Use of multi-precision arithmetic;

- p is stored as several 32-bit words;
- each field element is stored as several 32-bit words;
- all computations done modulo p;
- combination of Karatsuba-Ofman and table look-up used for multiplication;
- Inversion using Itoh-Tsuji algorithm;
- [I]$\approx$ 30 to 50 [M].

Characteristics Two

Polynomial Basis Representation.

- Let $\tau(x)$ be an irreducible polynomial of degree n over $GF(2)$.
- $\mathbb{F}$ consists of all polynomials of degree at most $n-1$ over $GF(2)$.
- Addition and multiplication done modulo $\tau(x)$.
- Multiplication: Karatsuba-Ofman, table look-up.
- Inversion: extended Euclidean algorithm.
  [I] $\approx$ 8 to 10 [M] (or lesser).

Normal Basis Representation: squaring is "free" but multiplication is costlier.

Choice of Cyclic Group

The whole of $\mathbb{F}^*$ is not used.

- Let r be a prime dividing $q = p^m$.
- Then $\mathbb{F}_q^*$ has a subgroup G of order r.
- Being of prime order, this subgroup is cyclic, i.e., $G = \langle g \rangle$.
- Cryptography is done over G.

Necessary Criteria:

The discrete log problem should be hard over G.

Discrete Log Algorithms

Generic algorithms: $O(\sqrt{|G|})$.

- Pollard's rho algorithm.
- Pohlig-Hellman algorithm.

Index calculus algorithm: $O\left(e^{(1+o(1))\sqrt{\ln p \ln \ln p}}\right)$.

Works over $\mathbb{Z}_p^*$.

Number field sieve: $O\left(e^{(1.92+o(1))(\ln q)^{1/3}(\ln \ln q)^{2/3})}\right)$;

sub-exponential algorithm.

Security Versus Efficiency

- Size of G and $\mathbb{F}$ has to be chosen so that all known discrete log algorithms have a minimum run time.
- Size of $\mathbb{F}$ determines the efficiency of multiplication and inversion.
- For 80-bit security:
  $|G|$ is at least 2^{160}; $|\mathbb{F}|$ is at least 2^{512};
- Existence of sub-exponential algorithms necessitates larger size fields.
- Detailed study of feasible parameters by Lenstra and Verheul.

Cyclic Groups from Elliptic Curves

Weierstraß Form

Weierstraß equation: elliptic curve over a field K.

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

$a_i \in K$; there are no “singular points”.
L-rational points on E: ($L \supseteq K$),

$$E(L) = \{(x, y) \in L \times L : C(x, y) = 0\} \cup \{\mathcal{O}\}.$$

$C(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$.
If $L \supseteq K$, then $E(L) \supseteq E(K)$.
$\overline{K}$: algebraic closure of E; denote $E(\overline{K})$ by E.

Simplifying Weierstraß Form

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

replacing y by $\frac{1}{2}(y - a_1x - a_3)$ gives

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6.$$

If characteristics $\neq 2, 3$, then replacing (x, y) by $((x - 3b_2)/36, y/108)$ gives

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Simplifying Weierstraß Form

Define

$$
\begin{aligned}
b_8 &= a_1^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
&\quad \text{(discriminant)} \\
j &= c_4^3/\Delta (j\text{-invariant}) \\
\omega &= dx/(2y + a_1x + a_3) \\
&= dy/(3x^2 + 2a_2x + a_4 - a_1y) \\
&\quad \text{(invariant differential)}
\end{aligned}
$$

Relations: $4b_8 = b_2b_6 - b_4^2, 1728\Delta = c_4^3 - c_6^2.$

Simplified Weierstraß Form

$\mathrm{char}(K) \neq 2, 3$: the equation simplifies to

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

$a, b \in K$ and $4a^3 + 27b^2 \neq 0$.

- ensures $x^3 + ax + b$ does not have repeated roots;
- $x^3 + ax + b$ has repeated roots iff $x^3 + ax + b$ and $\frac{d}{dx}(x^3 + ax + b) = 3x^2 + a$ have a common root;
- eliminating x from these two relations gives the condition $4a^3 + 27b^2 = 0$;
- this corresponds to $\Delta = 0$.

Simplified Weierstraß Form

$\mathrm{char}(K) = 2$: the equation simplifies to

- $y^2 + xy = x^3 + ax^2 + b$,
  $a, b \in K$, $b \neq 0$, non-supersingular, or
- $y^2 + cy = x^3 + ax + b$,
  $a, b, c \in K$, $c \neq 0$, supersingular.

Group Law

- $E(L)$: L-rational points on E is an abelian group;
- addition is done using the "chord-and-tangent law";
- $\mathcal{O}$ acts as the identity element.

Consider $E/K : y^2 = x^3 + ax + b$.
Addition formulae are as follows:

- $P + \mathcal{O} = \mathcal{O} + P = P$, for all $P \in E(L)$.
- $-\mathcal{O} = \mathcal{O}$.
- If $P = (x, y) \in E(L)$, then $-P = (x, -y)$.
- If $Q = -P$, then $P + Q = \mathcal{O}$.

Group Law (contd.)

- If $P = (x_1, y_1)$, $Q = (x_2, y_2)$, with $P \neq -Q$, then $P + Q = (x_3, y_3)$, where

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$

and

$$\begin{aligned} \lambda &= \tfrac{y_2 - y_1}{x_2 - x_1} \quad \text{if } P \neq Q; \\ &= \tfrac{3x_1^2 + a}{2y_1} \quad \text{if } P = Q. \end{aligned}$$

Deriving Addition Law

Let $P = (x_1, y_1), Q = (x_2, y_2)$ and $P \neq -Q$.

- If $P \neq Q$, then the line $\ell(x, y) : y = \lambda x + \nu$ through P and Q intersects the curve $E(x, y)$ at a third point R; the reflection of R on the x-axis is defined to be the point $P + Q$ given by (x_3, y_3);
- If $P = Q$, then the tangent $\ell(x, y) : y = \lambda x + \nu$ intersects the curve at a point R; the reflection of R on the x-axis is defined to be the point $2P$ given by (x_3, y_3);

Deriving Addition Law

Let $P = (x_1, y_1), Q = (x_2, y_2)$ and $P \neq Q, -Q$. So
$\lambda = (y_2 - y_1)/(x_2 - x_1), \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.
Putting $\ell(x, y)$ into $E(x, y)$ we get
$(\lambda x + \nu)^2 = x^3 + ax + b$
which is the same as
$x^3 - \lambda^2 x^2 + (a - 2\nu\lambda)x + b - \nu^2 = 0$.
This equation has three roots and x_1, x_2 are two of the roots.
So the third root is $x_3 = \lambda^2 - x_1 - x_2$.
Also, $-y_3 = \lambda x_3 + \nu$ and $y_1 = \lambda x_1 + \nu$ gives
$y_3 = \lambda(x_1 - x_3) - y_1$.
(Note: the line through (x_1, y_1) and (x_2, y_2) passes through $(x_3, -y_3)$.)

Deriving Addition Law

Let $P = (x_1, y_1), Q = (x_2, y_2)$ and $P = Q$.

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

$2y\frac{dy}{dx} = 3x^2 + a.$

Slope λ at (x_1, y_1) is $\frac{3x_1^2+a}{2y_1}$.

Rest of the analysis same as the previous case.

Obtained formula for (x_3, y_3) same except for the changed value of λ.

Elliptic Curve Group

- $\mathcal{O}$ is the additive identity;
- for any point P, $P + (-P) = \mathcal{O}$;
- for any points P, Q and R,

$$P + (Q + R) = (P + Q) + R.$$

associative property;
this is difficult to verify directly;
follows easily from the notion of divisors.

Frobenius Map

$$\tau_p : E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p), \qquad \tau_p(x, y) = (x^p, y^p).$$

τ_p is a group homomorphism.
Trace of Frobenius: $t_p = p + 1 - \#E(\mathbb{F}_p)$.

Theorem (Hasse): $\#E(\mathbb{F}_p) = p + 1 - t_p$, where $|t_p| \leq 2\sqrt{p}$. Consequently, $\#E(\mathbb{F}_p) \approx p$.

Theorem (Birch):
$\#\{E/\mathbb{F}_p : \alpha \leq t_p \leq \beta\} \approx \frac{1}{\pi} \int_\alpha^\beta \sqrt{4p - x^2}\, dx.$

Number of Points

Let $K = \mathbb{F}_q$ and $\overline{K} = \cup_{m \geq 1} \mathbb{F}_{q^m}$.

- **Schoof's Algorithm.**
  - Compute t modulo small primes and then use CRT.
  - Improvement by Elkies and Atkin. $\#E(\mathbb{F}_p)$ can be computed in time $O((\log p)^6)$ by **SEA** algorithm.
  - Subsequent work for computing points on EC on different fields.
- **Weil's Theorem:** Let $t = q + 1 - \#E(\mathbb{F}_q)$. Let α, β be complex roots of $T^2 - tT + q$. Then $\#E(\mathbb{F}_q) = q^k + 1 - \alpha^k - \beta^k$ for all $k \geq 1$.

Koblitz Curves

Characteristics 2, $q = 2^k$.

$$E : y^2 + xy = x^3 + ax^2 + 1, \qquad a \in \{0, 1\}.$$

- Chosen for reasons of efficiency.
- For security reasons k is taken to be a prime.

$$\#E(\mathbb{F}_q) = 2^k - \left(\frac{-1+\sqrt{-7}}{2}\right)^k - \left(\frac{-1-\sqrt{-7}}{2}\right)^k + 1.$$

Structure Theorem

Let E be an elliptic curve defined over $\mathbb{F}_q$.

- $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$,
  where $n_2 | n_1$ and $n_2 | (q-1)$.
- $E(\mathbb{F}_q)$ is cyclic if and only if $n_2 = 1$.

$P \in E$ is an n-torsion point if $nP = \mathcal{O}$;
$E[n]$ is the set of all n-torsion points.

Theorem : If $\gcd(n, q) = 1$, then $E[n] \cong Z_n \oplus Z_n$.

Supersingular Elliptic Curves

An elliptic curve $E/\mathbb{F}_q$ is supersingular if $p|t$ where $t = q + 1 - \#E(\mathbb{F}_q)$.

Theorem (Waterhouse): $E/\mathbb{F}_q$ is supersingular if and only if $t^2 = 0, q, 2q, 3q$ or $4q$.

Supersingular Elliptic Curves

Theorem (Schoof): Let $E/\mathbb{F}_q$ be supersingular with $t = q + 1 - \#E(\mathbb{F}_q)$. Then

- If $t^2 = q, 2q$ or $3q$, then $E(\mathbb{F}_q)$ is cyclic.
- If $t^2 = 4q$ and $t = 2\sqrt{q}$, then $E(\mathbb{F}_q) \cong Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$.
- If $t^2 = 4q$ and $t = -2\sqrt{q}$, then $E(\mathbb{F}_q) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$.
- If $t = 0$ and $q \neq 3 \bmod 4$, then $E(\mathbb{F}_q)$ is cyclic.
- If $t = 0$ and $q \equiv 3 \bmod 4$, then $E(\mathbb{F}_q)$ is cyclic or $E(\mathbb{F}_q) \cong Z_{\frac{q+1}{2}} \oplus Z_2$.

Summary

- Elliptic curves over finite fields provide rich examples of abelian groups.
- Let r be a prime such that $r | \#E(L)$ where $L \supseteq \mathbb{F}_q$. Then there is a cyclic subgroup $G = \langle P \rangle$ of $E(L)$.
- It is possible to do cryptography over G.
- **Advantage:** no sub-exponential algorithm for solving discrete log is known for G. (We will qualify this statement later.)
- Consequently, one can work over relatively small fields.

Jacobian Coordinates

- Affine coordinates: $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.
- Slope computation: $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ or $\frac{3x_1^2 + a}{2y_1}$.
- One inversion required.
- Jacobian coordinates: (X, Y, Z) represents $(X/Z^2, Y/Z^3)$.
- Addition using Jacobian coordinates avoids inversions.

Doubling in Jacobian

Curve: $y^2 = x^3 + ax + b$.
(X_1, Y_1, Z_1) is doubled to obtain (X_3, Y_3, Z_3).

$$x_3 = \frac{(3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2}{4Y_1^2Z_1^2}$$

$$y_3 = \frac{3X_1^2 + aZ_1^4}{2Y_1Z_1}\left(\frac{X_1}{Z_1^2} - X_3'\right) - \frac{Y_1}{Z_1^3}$$

$$X_3 = (3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2$$

$$Y_3 = (3X_1^2 + aZ_1^4)(4X_1Y_1^2 - X_3) - 8Y_1^4$$

$$Z_3 = 2Y_1Z_1.$$

Mixed Addition

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

(X_1, Y_1, Z_1) and $P = (X, Y, 1)$ are added to obtain (X_3, Y_3, Z_3) as follows.

$$x_3 = \left(\frac{Y - \frac{Y_1}{Z_1^3}}{X - \frac{X_1}{Z_1^2}} \right)^2 - \frac{X_1}{Z_1^2} - X$$

$$y_3 = \left(\frac{YZ_1^3 - Y_1}{(XZ_1^2 - X_1)Z_1} \right) \left(\frac{X_1}{Z_1^2} - X_3' \right) - \frac{Y_1}{Z_1^3}$$

Mixed Addition (contd.)

$$\begin{aligned}
X_3 &= x_3 Z_3 \\
&= (YZ_1^3 - Y_1)^2 - X_1(XZ_1^2 - X_1)^2 \\
&\quad -X(XZ_1^2 - X_1)^2 Z_1^2 \\
&= (YZ_1^3 - Y_1)^2 - (XZ_1^2 - X_1)^2(X_1 + XZ_1^2) \\
Y_3 &= y_3 Z_3 \\
&= (YZ_1^3 - Y_1)((XZ_1^2 - X_1)^2 X_1 - X_3) \\
&\quad -Y_1(XZ_1^2 - X_1)^3 \\
Z_3 &= (XZ_1^2 - X_1)Z_1
\end{aligned}$$

Scalar Multiplication

Let $G = \langle P \rangle$ be a subgroup of $E(L)$ of prime order r.

Instance: P and $a \in \mathbb{Z}_r$.
Task: Compute aP.

- a is usually a secret.
- Basic algorithm:
  left-to-right "double and add" algorithm;
  addition is always by P;
  underlines the importance of mixed addition.

Side Channel Information

Let $a = a_{n-1}a_{n-2}\ldots a_0$.

- At the ith step:
  - a doubling takes place;
  - if $a_{n-i} = 1$, then an addition takes place.

Suppose it is possible to measure the time required for the ith step.

- Then a_{n-i} can be uniquely determined.
- Instead of time, it may be possible to measure the power consumption at each step.
- The attack actually works and has been demonstrated.

Countermeasures: several are known; ongoing research.

Scalar Multiplication Issues

Representation of scalars.

- Expansion using $\{0, \pm 1\}$ instead of $\{0, 1\}$;
  negation of a point is "free";
  not good for finite fields.
- Non-adjacent form: "no two non-zero adjacent digits"; example: $100\bar{1}01$;
  known results on length of representation and density of non-zero digits;
  left-to-right "online" algorithm to obtain NAF.

Scalar Multiplication Issues

- Window method.
- Base-ϕ representation of the scalar; ϕ is the Frobenius map.
- Double base chain expansion;
  use bases $\{2, 3\}$ or $\{2, 3, 5\}$ instead of base 2;
  optimal length and density of non-zero digits not yet known.
- Parallelism, memory requirement.

Other Curve Forms

- Montgomery form: x-coordinate only scalar multiplication.
  $ay^2 = x^3 + bx + x$, $a \neq 0$;
- (Twisted) Edwards form: complete (and hence unified) formulae for addition and doubling.
  $ax^2 + y^2 = 1 + dx^2y^2$; $a, d \neq 0$, $a \neq d$.
- Jacobi-Quartic form.

Bilinear Pairings in Cryptography.

Divisors

Let $E/\mathbb{F}_q$ be given by $C(x,y)=0$.
The group of divisors of $E(\mathbb{F}_{q^n})$ is the free abelian group generated by the points of $E(\mathbb{F}_{q^n})$.
Thus any divisor D is of the form

$$D = \sum_{P \in E(\mathbb{F}_{q^n})} n_P \langle P \rangle.$$

- $n_P \in Z$,
- $n_P = 0$ except for finitely many P's.
- **Zero divisors:** $\sum n_P = 0$.

Rational Functions

A rational function f on E is an element of the field of fractions of the ring $\mathbb{F}_{q^n}[x, y]/(C(x, y))$.

The divisor of a rational function f is defined by

$$\mathrm{div}(f) = \sum_{P \in E(\mathbb{F}_{q^n})} \mathrm{ord}_P(f)\langle P \rangle$$

where $\mathrm{ord}_P(f)$ is the order of the zero/pole that f has at P.

A divisor D is said to be *principal* if $D = \mathrm{div}(f)$, for a rational function f.

Rational Functions (contd.)

Theorem: A divisor $D = \sum_{P \in E(\mathbb{F}_{q^n})} n_P \langle P \rangle$ is principal if and only if

- $\sum n_P = 0$ and
- $\sum n_P P = \mathcal{O}$.

Definition. Two divisors D_1 and D_2 are said to be *equivalent* $(D_1 \sim D_2)$ if $D_1 - D_2$ is principal.

Rational Functions (contd.)

Theorem : Any zero divisor $D = \sum n_P \langle P \rangle$ is equivalent to a (unique) divisor of the form $\langle Q \rangle - \langle \mathcal{O} \rangle$ for some $Q \in E(\mathbb{F}_{q^n})$.

If $P = (x, y)$, then by $f(P)$ we mean $f(x, y)$.

Definition. Given a rational function f and a zero divisor $D = \sum n_P \langle P \rangle$, define

$$f(D) = \prod_{P \in E(\mathbb{F}_{q^n})} f(P)^{n_P}.$$

Tate Pairing (Preliminaries)

- Embedding Degree: Let r be co-prime to q and $r|\#E(\mathbb{F}_q)$. The least positive integer k such that $r|(q^k - 1)$ is called the embedding degree.
- n-Torsion Points: Let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$E(\mathbb{F}_{q^k})[n] = \{P \in E(\mathbb{F}_{q^k}) : nP = \mathcal{O}\}.$$

- $\mu_r(\mathbb{F}_{q^k})$: cyclic subgroup of $\mathbb{F}_{q^k}$ of order r. Here r is prime and $r|(q^k - 1)$.

Tate Pairing (Preliminaries)

- $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$: collection of all cosets of $rE(\mathbb{F}_{q^k})$.
- $f_{s,P}$: an $\mathbb{F}_{q^k}$-rational function $f_{s,P}$ with divisor

$$\langle f_{s,P} \rangle = s\langle P \rangle - \langle [s]P \rangle - (s-1)\langle \mathcal{O} \rangle.$$

Tate Pairing Definition

Tate pairing $e(\cdot,\cdot)$**:**
(modified: reduced and normalised)

$$E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mu_r(\mathbb{F}_{q^k})$$

is given by

$$e(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}.$$

- P is an r-torsion point from $E(\mathbb{F}_{q^k})$;
- Q is any point in a coset of $rE(\mathbb{F}_{q^k})$;
- the result is an element of $\mathbb{F}_{q^k}$ of order r.

Computing Tate Pairing

Note: P is from $E(\mathbb{F}_q)$ while Q is from $E(\mathbb{F}_{q^k})$.

$$\begin{aligned} \langle f_{r,P} \rangle &= r\langle P \rangle - \langle [r]P \rangle - (r-1)\langle \mathcal{O} \rangle \\ &= r\langle P \rangle - r\langle \mathcal{O} \rangle. \end{aligned}$$

The computation of $f_{s,P}$ is using a double-and-add algorithm similar to that of scalar multiplication.

Some Simple Facts

Assume that E is given in Weierstraß form.
Let P and R be points on E.

- $\ell_{P,R}$, $R \neq P$: line passing through P, R and $-(P+R)$.
- $\ell_{R,R}$: line passing through R and $-2R$.
- $\ell_{R,-R}$: line passing through R and $-R$.

$$\begin{aligned}
\langle \ell_{P,R} \rangle &= \langle P \rangle + \langle R \rangle + \langle -(P+R) \rangle - 3\langle \mathcal{O} \rangle \\
\langle \ell_{R,R} \rangle &= 2\langle R \rangle + \langle -2R \rangle - 3\langle \mathcal{O} \rangle \\
\langle \ell_{R,-R} \rangle &= \langle R \rangle + \langle -R \rangle - 2\langle \mathcal{O} \rangle
\end{aligned}$$

Some Simple Facts

$h_{P,R}$, $R \neq P$:

$h_{P,R} = \ell_{P,R} / \ell_{T,-T}$; $T = P + R$.

$h_{R,R}$:

$h_{R,R} = \ell_{R,R} / \ell_{T,-T}$; $T = 2R$.

$$\begin{aligned} \langle h_{P,R} \rangle &= \langle \ell_{P,R} \rangle - \langle \ell_{T,-T} \rangle \\ \langle h_{P,R} \rangle &= \langle \ell_{R,R} \rangle - \langle \ell_{T,-T} \rangle \end{aligned}$$

$\langle f_{1,P} \rangle = \langle P \rangle - \langle P \rangle = 0$: So, $f_{1,P} = 1$.

Recurrence for $f_{s,P}$

$$
\begin{aligned}
\langle f_{2m,P}\rangle &= 2m\langle P\rangle - \langle 2mP\rangle - (2m-1)\langle \mathcal{O}\rangle \\
&= 2(m\langle P\rangle - \langle mP\rangle - (m-1)\langle \mathcal{O}\rangle) \\
&\quad +2\langle mP\rangle - \langle 2mP\rangle - \langle \mathcal{O}\rangle \\
&= 2\langle f_{m,P}\rangle + 2\langle mP\rangle + \langle -2mP\rangle - 3\langle \mathcal{O}\rangle \\
&\quad -(\langle 2mP\rangle + \langle -2mP\rangle - 2\langle \mathcal{O}\rangle) \\
&= 2\langle f_{m,P}\rangle + \langle \ell_{mP,mP}\rangle - \langle \ell_{2mP,-2mP}\rangle \\
&= 2\langle f_{m,P}\rangle + \langle h_{mP,mP}\rangle .
\end{aligned}
$$

Recurrence for $f_{s,P}$

$$
\begin{aligned}
\langle f_{2m+1,P} \rangle &= (2m+1)\langle P \rangle - \langle (2m+1)P \rangle \\
&\quad -2m\langle \mathcal{O} \rangle \\
&= 2m\langle P \rangle - \langle 2mP \rangle - (2m-1)\langle \mathcal{O} \rangle \\
&\quad +\langle P \rangle + \langle 2mP \rangle - \langle (2m+1)P \rangle - \langle \mathcal{O} \rangle \\
&= \langle f_{2m,P} \rangle + \langle P \rangle + \langle 2mP \rangle \\
&\quad +\langle -(2m+1)P \rangle - 3\langle \mathcal{O} \rangle \\
&\quad -(\langle (2m+1)P \rangle + \langle -(2m+1)P \rangle \\
&\quad -2\langle \mathcal{O} \rangle) \\
&= \langle f_{2m,P} \rangle + \langle \ell_{2mP,P} \rangle \\
&\quad -\langle \ell_{(2m+1)P,-(2m+1)P} \rangle \\
&= \langle f_{2m,P} \rangle + \langle h_{P,2mP} \rangle .
\end{aligned}
$$

Recurrence for $f_{s,P}$

$$\langle f_{2m,P} \rangle = 2\langle f_{m,P} \rangle + \langle h_{mP,mP} \rangle.$$

So,

$$f_{2m,P} = f_{m,P}^2 \times h_{mP,mP}.$$

$$\langle f_{2m+1,P} \rangle = 2\langle f_{m,P} \rangle + \langle h_{P,2mP} \rangle.$$

So,

$$f_{2m+1,P} = f_{2m,P} \times h_{P,2mP}.$$

Miller's Algorithm

Given $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$
to compute $f_{r,P}(Q)$.
Let $r_{t-1}r_{t-2}\ldots r_0$ be the binary expansion of r.

- Set $f \leftarrow 1$.
- Compute rP from left-to-right using "double and add".
- Let R be the input before the ith iteration.
  - $f \leftarrow f^2 \times h_{R,R}(Q)$; $R \leftarrow 2R$;
  - if $r_{n-i} = 1$
    $f \leftarrow f \times h_{R,P}(Q)$;
    $R \leftarrow R + P$.

Effect of Bilinear Map

Recall

$$e : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r(\mathbb{F}_{q^k})$$

$$e(aP, Q) = e(P, Q)^a$$

- reduces discrete log over $E(\mathbb{F}_q)$ to that over $\mu_r(\mathbb{F}_{q^k})$;
- security depends on k;
- for supersingular curves $k \leq 6$;
- for general elliptic curves k is large.

Effect of Bilinear Map

- Symmetric bilinear map: The second argument Q of $e(P, Q)$ is an element $E(\mathbb{F}_{q^k})$.
  Using a distortion map, one can consider Q to be an element of $E(\mathbb{F}_q)$.
- Solution to DDH:
  given (P, aP, bP, Q) determine if $Q = abP$;
  verify $e(aP, bP) = e(P, Q)$.
- Gap DH-groups: groups where CDH is hard but DDH is easy.

Joux's Key Agreement Protocol

3-party, single-round.

- Three users U_1, U_2 and U_3;
- U_i chooses a uniform random r_i and broadcasts $X_i = r_i P$;
- U_i computes $K = e(X_j, X_k)^{r_i}$, where $\{j, k\} = \{1, 2, 3\} \setminus \{i\}$;

$$K = e(P, P)^{r_1 r_2 r_3}.$$

Efficiency Improvements

- Irrelevant denominators: the denominator of $h_{P,R}$ need not be evaluated.
- Point tripling: the line through P and $2P$ passes through $-3P$;
  instead of doubling, use tripling;
  applicable for characteristics three curves.
- Variants: Ate and Eta pairings;
  the aim is to reduce the number of Miller iterations.
- Pairings on other forms of elliptic curves.
- Other implementation issues.

Pairing Friendly Curves

- Supersingular curves have embedding degree at most 6.
- Obtain non-supersingular curves with low embedding degree k;
  typically $k \leq 12$;
  involves a lot of computation with computer algebra packages;
  only a few examples are known.
- Embedding degree and group size determines the security level of the target protocol.

Thank you for your kind attention!