Elliptic Curves, Bilinear Pairings & Multi-linear Maps

Ratna Dutta

Department of Mathematics

Indian Institute of Technology, Kharagpur

November 9-13, 2020

Outline

- Brief review of
  - Elliptic curves
  - Cryptographic bilinear pairings
  - Cryptographic multilinear Maps

Why Elliptic Curve Cryptosystems?

- The points on an elliptic curve E over a finite field K form an abelian group.
- The addition operation of this abelian group involves a few arithmetic operations in the underlying field K, and is easy to implement, both in hardware and in software.
- The DLP in this group is believed to be very difficult, in particular, harder than the DLP in finite fields of the same size as K.

- **The main motivation** in studying Elliptic Curve Cryptosystems (ECC) is there is no known sub-exponential algorithm (like Index Calculus Method) to solve the DLP on a general elliptic curve.
  - The standard cryptographic protocols all have analogues in the elliptic curve case
  - potentially providing equivalent security, but with smaller key sizes and hence smaller memory and processor requirements.
  - This makes them ideal for use in smart cards and other environments where resources such as storage, time, or power are at a premium.

- **Another potential advantage** of using elliptic curves is the great diversity of elliptic curves available to provide the groups.
  - Each user may select a different curve E, even though all users use the same underlying field K.
  - Consequently, all users require the same hardware for performing the field arithmetic, and the curve E can be changed periodically for extra security.

- Finally, **Pairing Based Cryptography** (PBC)
  - A new idea which facilitates novel and attractive cryptographic constructions
  - And good solutions to some old problems!
- Two things are needed to do PBC:
  - Efficient algorithms for pairing implementations
  - Suitable elliptic curves
- Both are available and the technology is viable.

Elliptic Curves

- K be a field and $\overline{K}$ its algebraic closure. (If $K = F_q$, then $\overline{K} = \cup_{m\geq 1} F_{q^m}$.)
- Weierstrass equation :

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

where $a_1, a_2, a_3, a_4, a_6 \in K$ with no singular point.

- The set of K–rational points

$$E(K) = \{(x, y) \in K \times K\} \bigcup \{\mathcal{O}\}$$

where $\mathcal{O}$ is called the identity (also point at infinity).

- Simplified Weierstrass equation :

  1. $\mathrm{char}(K) \neq 2, 3$:

     $$y^2 = x^3 + ax + b,\ a, b \in K, 4a^3 + 27b^2 \neq 0.$$

  2. $\mathrm{char}(K) = 2$:

     $$y^2 + xy = x^3 + ax^2 + b,\ a, b \in K, b \neq 0$$

     (non-supersingular)

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

     (supersingular)

  3. $\mathrm{char}(K) = 3$:

     $y^2 = x^3 + ax^2 + bx + c,\ a, b, c \in K$ (cubic on the right has no multiple roots)

Group Law

- $E = E(\overline{K})$ given by Weierstrass equation.
- For all $P, Q \in E$

  (i) $\mathcal{O} + P = P + \mathcal{O} = P$ (so $\mathcal{O}$ serves as the identity)

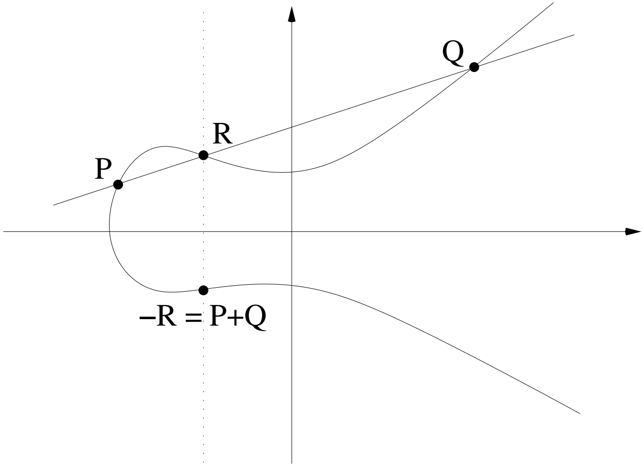
  (ii) $-\mathcal{O} = \mathcal{O}$

  (iii) if $P = (x_1, y_1) \neq \mathcal{O}$, then
  $-P = (x_1, -y_1 - a_1x_1 - a_3)$
  (P and $-P$ are the only points on E with x-co-ordinates equal to x_1)

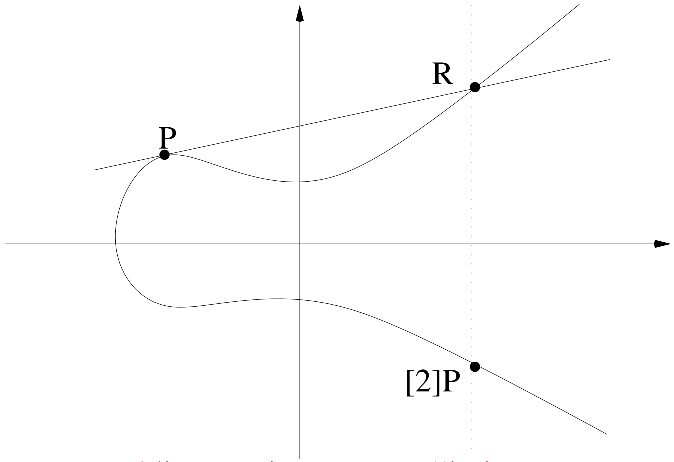
  (iv) if $Q = -P$, then $P + Q = \mathcal{O}$

(v) if $P \neq \mathcal{O}, Q \neq \mathcal{O}, Q \neq -P$, then $P + Q = -R$, where R is the third point of intersection of the line PQ (tangent PQ if $P = Q$) with the curve E.

- $\mathcal{O}$ is called point at infinity (if $Q = -P$, then $P + Q = \mathcal{O}$).



Adding two points P, Q on an elliptic curve



Doubling a point P on an elliptic curve

- **Theorem :**
  - $(E, +)$ *is an abelian group with identity element* $\mathcal{O}$.
  - *If* E *is defined over* K, *then* $E(K)$ *is a subgroup of* E.

Addition Formulae

- E/K : Weierstrass equation
  - if $P = (x_1, y_1) \neq \mathcal{O}$, then $-P = (x_1, -y_1 - a_1x_1 - a_3)$.
  - if $P = (x_1, y_1) \neq \mathcal{O}$, $Q = (x_2, y_2) \neq \mathcal{O}$, $P \neq -Q$, then $P + Q = (x_3, y_3)$ with

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

$$y_3 = -(\lambda + a_1)x_3 - \beta - a_3$$

where

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{if } P \neq Q \\ \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3} & \text{if } P = Q \end{cases}$$

and $\beta = y_1 - \lambda x_1$.

- $E/K : y^2 = x^3 + ax + b$
  - if $P = (x_1, y_1) \neq \mathcal{O}$, then $-P = (x_1, -y_1)$
  - if $P = (x_1, y_1) \neq \mathcal{O}$, $Q = (x_2, y_2) \neq \mathcal{O}$, $P \neq -Q$, then $P + Q = (x_3, y_3)$ with

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

- $E/K : y^2 + xy = x^3 + ax^2 + b$ (non-supersingular)
  - if $P = (x_1, y_1) \neq \mathcal{O}$, then $-P = (x_1, y_1 + x_1)$
  - if $P = (x_1, y_1) \neq \mathcal{O}$, $Q = (x_2, y_2) \neq \mathcal{O}$, $P \neq -Q$, then $P + Q = (x_3, y_3)$ with

$$x_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a & \text{if } P \neq Q \\ x_1^2 + \frac{b}{x_1^2} & \text{if } P = Q \end{cases}$$

and

$$y_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + x_3 + y_1 & \text{if } P \neq Q \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3 & \text{if } P = Q \end{cases}$$

- $E/K : y^2 + cy = x^3 + ax + b$ (supersingular)
  - if $P = (x_1, y_1) \neq \mathcal{O}$, then $-P = (x_1, y_1 + c)$
  - if $P = (x_1, y_1) \neq \mathcal{O}$, $Q = (x_2, y_2) \neq \mathcal{O}$, $P \neq -Q$, then $P + Q = (x_3, y_3)$ with

$$x_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2 & \text{if } P \neq Q \\ \frac{x_1^4+a^2}{c^2} & \text{if } P = Q \end{cases}$$

and

$$y_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + y_1 + a_3 & \text{if } P \neq Q \\ \left(\frac{x_1^2+a}{c}\right)(x_1 + x_3) + y_1 + c & \text{if } P = Q \end{cases}$$

Example: Point counting

- $E/Z_{11} : y^2 = x^3 + x + 6$
- **Quadratic residue modulo p:** Let p be an odd prime and x be an integer, $1 \leq x \leq p-1$. x is defined to be a *quadratic residue* or *square* modulo p if the congruence

$$y^2 \equiv x \pmod{p}$$

  has a solution $y \in Z_p$.
- *Example:* $\mathsf{QR}_{11} = \{1, 3, 4, 5, 9\}$.

x	$x^3 + x + 6 \bmod 11$	quadratic residue?	y
0	6	no	-
1	6	no	-
2	6	yes	$4, 7$
3	6	yes	$5, 6$
4	6	no	-
5	6	yes	$2, 9$
6	6	no	-
7	6	yes	$2, 9$
8	6	yes	$3, 8$
9	6	no	-
10	6	yes	$2, 9$

- E/Z_{11} has 13 points on it including $\mathcal{O}$
- We take a point $\alpha = (2, 7)$ and compute the power of α (which we will write as multiples of , since the group operation is additive).
- To compute $2\alpha = (2, 7) + (2, 7)$, we use the point doubling (Tangent law) and get $2\alpha = (5, 2)$.
- To compute $3\alpha = 2\alpha + \alpha = (5, 2) + (2, 7)$, we use the point addition (Chord law) and get $3\alpha = (8, 3)$.

$\alpha = (2,7)$	$2\alpha = (5,2)$	$3\alpha = (8,3)$
$4\alpha = (10,2)$	$5\alpha = (3,6)$	$6\alpha = (7,9)$
$7\alpha = (7,2)$	$8\alpha = (3,5)$	$9\alpha = (10,9)$
$10\alpha = (8,8)$	$11\alpha = (5,9)$	$12\alpha = (2,4)$

- $\alpha = (2,7)$ is a primitive element.
- We can implement ElGamal encryption scheme using elliptic curve group $G = \langle\alpha\rangle$ with operation $+$

Group Structure

- $E/F_q, q = p^m$, p is prime, char(F_q).
- $\#E(F_q)$: number of points on $E(F_q)$.
- $t = q + 1 - \#E(F_q)$
- **Theorem** (Hasse, conjectured by E. Artin):

  (i) $\phi \circ \phi - [t] \circ \phi + [q] = \mathcal{O}$ *and*

  (ii) $|t| \leq 2\sqrt{q}$

  where $[m] : P \rightarrow mP$ *and* $\phi : E \rightarrow E$ *is the Frobenius endomorphism on* E *defined by* $\phi(a, b) = (a^q, b^q)$, t *is the trace of the Frobenius endomorphism.*

- **Theorem** (Schoof's Algorithm):

  $\#E(F_q)$ can be computed in polynomial time.

- **Theorem** (Weil, proved by Hasse):

  Let $t = q + 1 - \#E(F_q)$. Then $\#E(F_{q^k}) = q^k + 1 - \alpha^k - \beta^k$, where α, β are complex numbers determined from the factorization of $1 - tT + qT^2 = (1 - \alpha T)(1 - \beta T)$.

- **Theorem** (Fundamental theorem of abelian groups):

  $E(F_q) \cong Z_{n_1} \oplus Z_{n_2},$ *where* $n_2 | n_1$ *and* $n_2 | q-1$.
  Moreover, $E(F_q)$ *is cyclic if and only if* $n_2 = 1$.

- **Theorem**:

  If $gcd(n, q) = 1$, *then* $E[n] \cong Z_n \oplus Z_n$ *where*
  $E[n] = \{P \in E | nP = \mathcal{O}\}$, *set of all* n*-torsion points.*

Supersingular Elliptic Curve

- E/F_q is supersingular if $p|t$ where $t = q + 1 - \#E(F_q), q = p^m$, p is the char(F_q), prime.
- **Theorem** (Waterhouse):

  E/F_q is supersingular if and only if $t^2 = 0, q, 2q, 3q$ or $4q$.

- Untill constructive applications of pairings were found, from 2000, supersingular curves were considered bad for cryptography (MOV attack)

- **Theorem** (Schoof):
  Let E/F_q be a supersingular elliptic curve with $t = q + 1 - \#E(F_q)$. Then

  1. *if $t^2 = q, 2q$ or $3q$, then $E(F_q)$ is cyclic.*
  2. *if $t^2 = 4q$ and $t = 2\sqrt{q}$, then* $E(F_q) \cong Z_{\sqrt{q}-1} \oplus Z_{\sqrt{q}-1}$
  3. *if $t^2 = 4q$ and $t = -2\sqrt{q}$, then* $E(F_q) \cong Z_{\sqrt{q}+1} \oplus Z_{\sqrt{q}+1}$
  4. *if $t = 0$ and $q \neq 3 \bmod 4$, then $E(F_q)$ is cyclic*
  5. *if $t = 0$ and $q = 3 \bmod 4$, then $E(F_q) \cong Z_{\frac{q+1}{2}} \oplus Z_2$.*

What's a Pairing?

- Pairings are functions which map a pair of elliptic curve points to an element of a multiplicative group of an underlying finite field.

  $\hat{e}(P, Q)$ where P and Q are points on an elliptic curve.

- It has the property of bilinieaity.

  $$\hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(P, Q)^{ab}$$

- Examples: **Weil pairing**, **Tate pairing**, **Ate pairing**, **Eta pairing** etc.

Cryptographic Bilinear Pairing

- G_1, G_2 two groups of same prime order n
- $G_1 = \langle P \rangle$, G_1 is additive group, identity $\mathcal{O}$
- G_2 is a multiplicative group with identity 1
- DLP is hard in both G_1, G_2

- <u>Cryptographic bilinear pairing</u> $\hat{e} : G_1 \times G_1 \rightarrow G_2$
  1. Bilinearity : for all $R, S, T \in G_1$

$$\hat{e}(S+R,T) = \hat{e}(S,T) \cdot \hat{e}(R,T)$$

$$\hat{e}(S,T+R) = \hat{e}(S,T) \cdot \hat{e}(S,R)$$

     In other words, $\hat{e}(aS, bT) = \hat{e}(S,T)^{ab}$ for all $a, b \in Z_n^*$
  2. Non-degeneracy : $\hat{e}(P,P) \neq 1$
  3. Computability : $\hat{e}$ can be efficiently computed.
  4. Symmetry : $\hat{e}(S,T) = \hat{e}(T,S)$.
- can be constructed from Weil, Tate pairing

Some Important Consequences

- **D**ecision **D**iffie-**H**ellman (DDH) Problem in $G_1 = \langle P \rangle$:–
  - Given $P, aP, bP, cP \in G_1$ for some $a, b, c \in Z_n^*$, decide whether $c = ab \bmod n$.

Theorem : *DDH Problem is easy in G_1.*
proof:

  - Pairings help us to solve DDH problem in G_1
  - Easy to check if $\hat{e}(aP, bP) = \hat{e}(P, cP)$

$$\hat{e}(aP, bP) = \hat{e}(P, P)^{ab} \text{ and } \hat{e}(P, cP) = \hat{e}(P, P)^{c}$$

$$\hat{e}(P, P)^{ab} = \hat{e}(P, P)^{c} \text{ iff } c = ab \bmod n$$

- **C**omputational **D**iffie-**H**ellman (CDH) Problem in $G_1 = \langle P \rangle$:–
  - Given $P, aP, bP \in G_1$ for some $a, b \in Z_n^*$, compute the value abP.
- Pairings do not help us to solve CDH problem (except by perhaps making the discrete log problem a bit simpler!)
- **B**ilinear **D**iffie-**H**elllman (BDH) Problem in $\langle G_1, G_2, \hat{e} \rangle$:–
  - Given $P, aP, bP, cP \in G_1$ for some $a, b, c \in Z_n^*$, compute the value $\hat{e}(P, P)^{abc}$.

- **Theorem :** *If CDH problem in* G_1 *is easy, then BDH problem in* $\langle G_1, G_2, \hat{e} \rangle$ *is easy.*
- **Theorem :** *If CDH problem in* G_2 *is easy, then BDH problem in* $\langle G_1, G_2, \hat{e} \rangle$ *is easy.*

Pairing computation

- Let P be a point of prime order r on a (supersingular) elliptic curve $E(F_q)$
- Let k be the smallest positive integer such that r divides $q^k - 1$ (k is called the embedding degree)
- Then the pairing $\hat{e}(P, Q)$ can be calculated, and evaluates as an element in F_{q^k} (via Miller's algorithm or Elliptic Nets)

Extension Fields

- An element in F_{q^k} can be represented as a polynomial with coefficients in F_q, modulo an irreducible polynomial of degree k.
- Simple example, $q = p, k = 2$
- Assume $p = 3 \bmod 4$
- Then $x^2 + 1$ is a suitable irreducible polynomial
- An element in F_{q^k} can be written as $a + xb$, where x is a root of the irreducible polynomial.
- In fact $x = \sqrt{-1} \bmod p$, so $a + b.\sqrt{-1}$ written as (a, b) – just like complex numbers!

Pairings for Cryptanalysis

- MOV Reduction :–
  (**M**enezes, **O**kamoto, **V**anstone, 1993)

  Theorem : *DLP in G_1 is no harder that DLP in G_2.*
  proof:

  – Consider the DLP on G_1 (an elliptic curve group):
  Given P and Q, where $Q = xP$, find x.

  – $\hat{e}(P, Q) = \hat{e}(P, P)^x$ by bilinearity.

  – Solve this DLP over finite field F_{q^k} using index calculus.

  – Relatively easy (if k is small)

Making it Secure

- If r is 160 bits, then Pohlig-Hellman attacks will take $\sim 2^{80}$ steps
- If $k \log(q) \sim 1024$ bits, Discrete Log attacks will also take $\sim 2^{80}$ steps
- So we can achieve appropriate levels of cryptographic security
- We have to deal with "RSA-sizes" values in the extension field F_{q^k}

Weil/Tate Pairing

How to construct Cryptographic Bilinear Pairing from Weil/Tate Pairing on Elliptic Curve

Divisors Theory

Divisors

- $E/F_q : C(x, y) = 0$.
- $E = E(F_{q^n})$.
- The group of divisor $Div(E)$ of E is the free abelian group generated by the points of E. For any $D \in Div(E)$,
$$D = \sum_{P \in E} n_P \langle P \rangle$$
where $n_P \in Z$ and $n_P = 0$ except for finitely many $P \in E$.

- $Supp(D) = \{P \in E | n_P \neq 0\}$
- $deg(D) = \Sigma_{P \in E} n_P \in Z$
- $Div^\circ(E)$: group of zero divisors : $\Sigma n_P = 0$.

Principal Divisor

- A rational function f on E is an element of the field of fractions of the ring $F_{q^n}[x, y]/(C(x, y))$
- $f(P) = f(x, y)$ if $P = (x, y)$
- The divisor of a rational function f

$$div(f) = \sum_{P \in E} ord_P(f) \langle P \rangle$$

where $ord_P(f)$ is the order of zero/pole f has at P.

- Principal divisor : $D = div(f)$ for some rational function f.
- $D_1 \sim D_2$ if $D_1 - D_2$ is principal.

Theorem: *Let* $D = \sum_{P \in E} n_P \langle P \rangle$ *be a divisor.* D *is principal if and only if* $\sum n_P = 0$ *and* $\sum n_P P = \mathcal{O}$.

- $Prin(E)$: set of all principal divisors

$$Prin(E) \subseteq Div^\circ(E)$$

- Picard group of E : the quotient group

$$Pic(E) = Div(E)/Prin(E)$$

- (degree zero part of the Picard group)

$$Pic^\circ(E) = Div^\circ(E)/Prin(E)$$

Theorem: *$Pic^\circ(E)$ is in $1-1$ correspondence with the points of E.*
Theorem: *For any $D \in Div^\circ(E)$, there exists a <u>unique point</u> $P \in E$ such that $D \sim \langle P \rangle - \langle \mathcal{O} \rangle$.*

- Given a rational function f and a divisor $D = \sum_{P \in E} n_P \langle P \rangle \in Div(E)$ with f and D having disjoint supports, we define

$$f(D) = \prod_{P \in Supp(D)} f(P)^{n_P}$$

Weil Pairing

- E/F_q
- n be an integer with $gcd(n, q) = 1$
- F_{q^k} : smallest extension of F_q such that $E[n] \subseteq E(F_{q^k})$.
  $(i.e\ n^2|\#E(F_{q^k})$ and $n|(q^k - 1))$
- μ_n : subgroup of order n in $F_{q^k}^*$.

- Weil Pairing $e_n : E[n] \times E[n] \rightarrow \mu_n$ is defined as follows:
  - Let $P, Q \in E[n]$
  - Let $D_P, D_Q \in Div(E)$ such that $D_P \sim \langle P \rangle - \langle \mathcal{O} \rangle$ and $D_Q \sim \langle Q \rangle - \langle \mathcal{O} \rangle$
  - Then $nD_P, nD_Q \in Prin(E)$.
  - So there exist rational functions f_P, f_Q such that $div(f_P) = nD_P$ and $div(f_Q) = nD_Q$.

$$e_n(P, Q) = \frac{f_P(D_Q)}{f_Q(D_P)}$$

Tate Pairing

$$e_n(P,Q) = f_P(D_Q)^{(q^k-1)/n}$$

Properties of Weil/Tate

1. Bilinearity : for all $R, S, T \in E[n]$,

$$e_n(S + R, T) = e_n(S, T) \cdot e_n(R, T)$$

$$e_n(S, T + R) = e_n(S, T) \cdot e_n(S, R)$$

2. Non-degeneracy : if $S \in E[n]$, then $e_n(S, \mathcal{O}) = 1$. Moreover, if $e_n(S, T) = 1$ for all $T \in E[n]$, then $S = \mathcal{O}$.

3. Computability : e_n can be computed in polynomial time (Miller's Algorithm, Elliptic Nets).

4. Identity : $e_n(S, S) = 1$ for all $S \in E[n]$.

5. Alternation : $e_n(S, T) = e_n(T, S)^{-1}$.

Note

- For cryptographic bilinear map $\hat{e}$, $\hat{e}(P, P) \neq 1$ for all $P \in G_1$
- For Weil/Tate pairing e_n,

  $e_n(P, P) = 1$ for all $P \in E[n]$.

  $e_n(P, Q) \neq 1$ if P, Q are linearly independent.
- Let $P \in E/F_q$ be of order n. Then a $Q \in E/F_{q^k}$ of order n can always be found such that P, Q are linearly independent.
- For supersingular elliptic curve, Q is found by means of a distorsion map ψ – an automorphism on E/F_{q^k}.

Example

- $E/F_p : y^2 = x^3 + 1, p > 3, p = 2 \bmod 3$
- $\#E(F_p) = p + 1$
- Let $P \in E/F_p$ be a point of order n where $n|p+1$
- E/F_{p^2} contains a point Q of order n which is linearly independent of points of E/F_p.
- E/F_{p^2} contains a subgroup $E[n]$ isomorphic to Z_{n^2}.

- $\zeta \in F_{p^2}$ be a non trivial root of $x^3 - 1 = 0 \bmod p$. Then $\psi(x, y) = (\zeta x, y)$ is an automorphism on E/F_{p^2}.
- ψ is called a distorsion map.
- For any elliptic curve, such a distorsion map can efficiently be found.
- $P, Q = \psi(P)$ are linearly independent.

Modified Weil Pairing

- $E[n]$ is a group generated by P and $\psi(P)$.
- $P, \psi(P)$ are linearly independent, each of order n.
- $G_1 = \langle P \rangle$
- G_2 be a subgroup of $F^*_{p^2}$ of order n.
- $e_n : E[n] \times E[n] \rightarrow G_2$ be the weil pairing.
  Then the modified weil pairing $\hat{e} : G_1 \times G_1 \rightarrow G_2$ is defined by
  $$\hat{e}(P, Q) = e_n(P, \psi(Q)).$$

Weil Pairing Computation

– Let $P, Q \in E[n]$

– To compute $e_n(P, Q) \in F^*_{p^2}$

– Let $P \neq Q$

– Let $R_1, R_2 \in E[n]$ be two random points

– Let $A_P = \langle P + R_1 \rangle - \langle R_1 \rangle \sim \langle P \rangle - \langle \mathcal{O} \rangle$

– Let $A_Q = \langle Q + R_2 \rangle - \langle R_2 \rangle \sim \langle Q \rangle - \langle \mathcal{O} \rangle$

– Then $nA_P, nA_Q \in Prin(E)$.

– So there exist rational functions f_P, f_Q such that $div(f_P) = nA_P$ and $div(f_Q) = nA_Q$.

$$e_n(P,Q) = \frac{f_P(A_Q)}{f_Q(A_P)} = \frac{f_P(Q+R_2)f_Q(R_1)}{f_P(R_2)f_Q(P+R_1)}$$

– Compute $f_P(A_Q)$ and $f_Q(A_P)$

Computing $f_P(A_Q)$

- $b \in Z_+$
- define $A_b = b\langle P + R_1\rangle - b\langle R_1\rangle - \langle bP\rangle + \langle \mathcal{O}\rangle$
- $A_b \in Prin(E)$
- So there exist rational functions f_b such that $div(f_b) = A_b$
- $div(f_P) = nA_P = n\langle P + R_1\rangle - n\langle R_1\rangle$
  $= n\langle P + R_1\rangle - n\langle R_1\rangle - \langle nP\rangle + \langle \mathcal{O}\rangle = A_n = div(f_n)$ as $P \in E[n]$
- So $f_P(A_Q) = f_n(A_Q)$

Computing $f_n(A_Q)$

– Given $f_b(A_Q), f_c(A_Q), bP, cP, (b+c)P$, $b, c \in Z_+$, we can compute $f_{b+c}(A_Q)$

– $g_1(x, y) = 0$ is the line through bP, cP

– $g_2(x, y) = 0$ be the vertical line through $(b+c)P$

– g_1, g_2 are rational functions

– $div(g_1) = \langle bP \rangle + \langle cP \rangle + \langle -(b+c)P \rangle - 3\langle \mathcal{O} \rangle$

– $div(g_2) = \langle (b+c)P \rangle + \langle -(b+c)P \rangle - 2\langle \mathcal{O} \rangle$

– then $A_{b+c} = A_b + A_c + div(g_1) - div(g_2)$

– so $f_{b+c}(A_Q) = f_b(A_Q)f_c(A_Q)\frac{g_1(A_Q)}{g_2(A_Q)}$ as $div(f_b) = A_b$

– Apply double and add to compute $f_n(A_Q) = f_P(A_Q)$ (Miller's algorithm)

– needs to evaluate $f_1(A_Q) = \frac{g_2(A_Q)}{g_1(A_Q)}$ as

$$div(f_1) = A_1 = \langle P + R_1 \rangle - \langle R_1 \rangle - \langle P \rangle + \langle \mathcal{O} \rangle = \frac{div(g_2)}{div(g_1)}$$

where g_1 is the line passing through P and R_1, g_2 is the verical line passing through $P + R_1$

Miller's Algorithm

- Let $\mathcal{D}$ be the algorithm that computes $f_{b+c}(A_Q)$ on input $f_b(A_Q), f_c(A_Q), bP, cP, (b+c)P$
- Let $n = b_m b_{m-1} \ldots b_1 b_0$ – binary representation of n
- Initially set $Z = \mathcal{O}$, $V = f_0(A_Q) = 1, k = 0$
- for $(i = m, m-1, \ldots, 1, 0)$ do
  - if $(b_i = 1)$ then set $V = \mathcal{D}(V, f_1(A_Q), Z, P, Z+P), Z = Z+P, k = k+1$
  - if $(i > 0)$ then set $V = \mathcal{D}(V, V, Z, Z, 2Z), Z = 2Z, k = 2k$

- Observe that at the end of each iteration, we have

$$Z = kP, V = f_k(A_Q)$$

- After the last iteration, we have $k = n, V = f_n(A_Q)$
- Time Complexity $O(\log p)$ arithmetic operations in F_{p^2}.

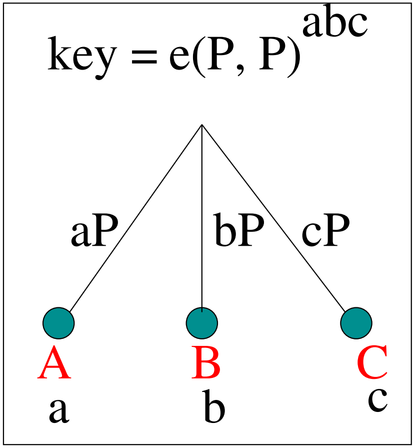
Why is pairing useful?

- Earlier bilinear pairings, namely Weil pairing and Tate pairing of algebraic curves were used in cryptography to reduce the DLP on some elliptic or hyperelliptic curves to the DLP in a finite field (MOV reduction).
- In recent years, bilinear pairings have found positive application in cryptography to construct new cryptographic primitives.

- The first introduction of pairings in the constructive sense were:
  - Joux's Key Agreement, 2000
  - Boneh-Franklin's Identity-Based Encryption (IBE), 2001
  - Boneh-Lynn-Shacham's Short Signature, 2001
- A multitude of pairing based protocols have been suggested.
- A handful of efficient pairing implementations have been developed.

Three-Party Key Agreement

(Joux, ANST IV 2000, LNCS, Springer)



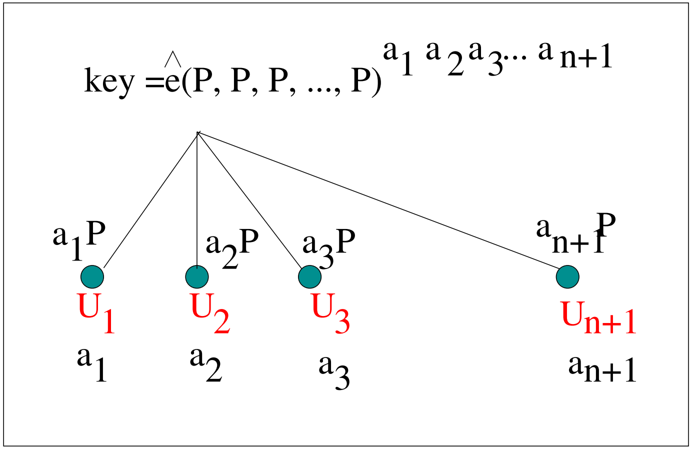
- $G_1 = \langle P \rangle$ additive, G_2 multiplicative group of a large prime order q, $\hat{e} : G_1 \times G_1 \to G_2$ the bilinear map

- security: hardness of BDH problem.
- BDH (Bilinear Diffie-Hellman) Problem in $\langle G_1, G_2, e\rangle$:

  given $\langle P, aP, bP, cP\rangle$ for some $a, b, c \in Z_q^*$, compute $e(P, P)^{abc}$.

$(n+1)$-party Key Agreement

(Boneh and Silverberg, 2003, Contemporary Mathematics, AMS)



- $G_1 = \langle P \rangle$ additive, G_2 multiplicative group of a large prime order q, $\hat{e} : G_1^n \to G_2$ the n-linear map

Multilinear Map

- extending bilinear elliptic curve pairings to multilinear maps is a long-standing open problem.
- amazingly powerful tool – so useful that a body of work examined their applications even before any candidate constructions is known to realize them

- two recent breakthrough constructions
  - GGH: (Garg, Gentry and Halevi, EUROCRYPT 2013, LNCS) - based on ideal lattices
  - CLT: (Coron, Lepoint and Tibouchi, CRYPTO 2013, LNCS) - over the integers
- Reliance on cryptographic tools built from multilinear maps may be perilous as existing multilinear maps are still heavy tools to use and suffering from many non-trivial attacks.