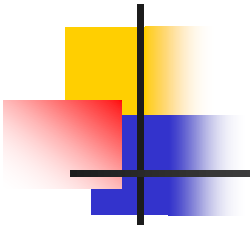
ECC 2008

Efficient and Generalized Pairing Computation on Abelian Varieties

Hyang-Sook Lee
Ewha Womans University
Korea

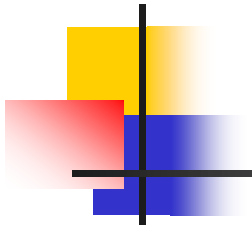
Joint Work with
Eunjeong Lee (North Carolina State University)
Cheol-Min Park (EWHA)

2008. 9. 22

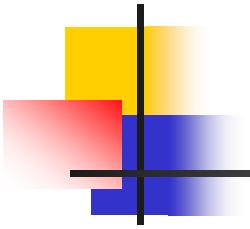


Contents

- Background of pairings
- Efficient pairing computations – “review”
  - Motivation for efficient pairing computation
  - Eta and Eta_T pairings on supersingular curves
  - Ate and Ate_i pairings on ordinary curves
- R-ate pairing
- Optimal pairing



- Background of Pairings



Pairings

$(G_1,+)$, $(G_2,+)$ and $(G_3,*)$: cyclic groups of a prime order r

e be a map $e : G_1 \times G_2 \rightarrow G_3$ satisfying

- ► Non-degeneracy : If $e(P, Q) = 1$ for all $Q \in G_2$, then $P \in G_1$ is the identity (vice versa)
- ► Bilinearity : $e(aP, bP) = e(P, P)^{ab}$ for $a, b \in Z$
- ► e is computable in polynomial time

⇒ e : bilinear map or pairing

(ex) Weil and Tate pairings on supersingular curves using distortion map.

Tate pairing/Ate pairing

F_q : finite field with q elements

C : nonsingular curve of genus g over F_q

J_C : a group of degree zero divisor classes of C

g = 1 $\Rightarrow$ J_C elliptic curve

r : a positive divisor of $|J_C(F_q)|$ with gcd(r, q) = 1

k is the smallest integer s.t. if $r | q^k - 1$, $r \nmid q^s - 1$, $0 < s < k$

$\Rightarrow$ k: embedding degree

$J_C[r]$: divisor classes of order dividing r

Tate pairing

Define the Tate pairing

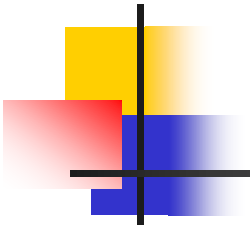
$$< , > : J_C[r] \times J_C(F_{q^k})/rJ_C(F_{q^k}) \rightarrow F_{q^k}^*/ (F_{q^k}^*)^r \quad \text{by}$$

$$<D, E> = f_{r,D}(E')$$

where $\mathrm{div}(f_{r,D}) = rD$, $E' \sim E$ with $\mathrm{supp}(E') \cap \mathrm{supp}(\mathrm{div}(f_{r,D})) = \Phi$.

For the uniqueness in F_{q^k}, define the reduced Tate pairing

$$e(D, E) = f_{r,D}(E')^{(q^k - 1)/r}$$



Ate pairing

Let φ be the q-power Frobenius endomorphism on J_C.
$G_1 = J_c[r] \cap \ker(\varphi - 1)$, $G_2 = J_c[r] \cap \ker(\varphi - [q])$.

For $D \in G_1$, $E \in G_2$,

Ate pairing (g=1)[HSV] : $a(E, D) = f_{t-1,E}(D)^{(q^k-1)/r}$

Ate pairing (g≥2)[GHOTV] : $a(E, D) = f_{q,E}(D)^{(q^k-1)/r}$

Ate$_i$ pairing (g=1)[ZZH] : $a_i(E, D) = f_{q^i \bmod r,E}(D)^{(q^k-1)/r}$, $0<i<k$

Miller's Algorithm

Input : $r=\sum^{n-1}_{i=0} r_i 2^i \in Z$, $D \in J_C[r]$, $E \in J_C(F_{q^k})/rJ_C(F_{q^k})$

Output : $e(D,E)$

Number of iterations

Def.
Miller length

$n = \log_2 r$

$V=D$, $f=1$

For $i=n-1$ down to 0

$f \leftarrow f^2 \cdot g_{V,V}(E)/g_{2V}(E)$ $\quad V \leftarrow 2V$

If $r_i=1$ then

$f \leftarrow f^2 \cdot g_{V,D}(E)/g_{V+D}(E)$ $\quad V \leftarrow V+D$

Return $f^{(q^k-1)/r}$

Miller's Algorithm

- $div(f_n) = n(P) - n(O)$
- $div(f_2) = 2(P) - (2P) - (O)$ ⇄ $(f_4 = f_2^2 * g_{2P,2P} / g_{4P,-4P})$
- $div(f_4) = 4(P) - (4P) - 3(O)$ ⇄ $(f_8 = f_4^2 * g_{4P,4P} / g_{8P,-8P})$
- $div(f_8) = 8(P) - (8P) - 7(O)$ ⇄ $(f_9 = f_8 * g_{8P,P} / g_{9P,-9P})$
- $div(f_9) = 9(P) - (9P) - 8(O)$

  : : :

  $Log_2 n$ – step
- $div(f_n) = n(P) - n(O)$

Supersingular curves

An elliptic curve E/F_q is called supersingular if it has $E[p^s](F_q) = \{O\}$ or $p \mid t$, where $p=\text{char } F_q$.

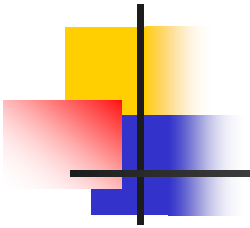
- $\exists$ distortion map $\Rightarrow$ Eta pairing approach
- small embedding degree

  $p=2 \Rightarrow k \leq 4$

  $p=3 \Rightarrow k \leq 6$,

  over prime fields F_p with $p \geq 5 \Rightarrow k \leq 2$.
- small number of curves

Ordinary curves



Otherwise, is called ordinary curve,

and $E[p^s](F_q) = Z/p^sZ$

- no distortion map ⇒ Ate pairing approach
- can be used over prime fields p for large prime
- more and larger embedding degree
- more choice of curves

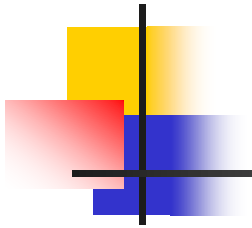
Hyperelliptic cuves

- A hyperelliptic curve is called *supersingular* if its Jacobian is isogenous to the product of supersingular elliptic curves

- A hyperelliptic curve is called *superspecial* if its Jacobian is isomorphic to the product of supersingular elliptic curves

➔ Ate pairing applicable (GHOTV07)

➔ e.g. DL-curves



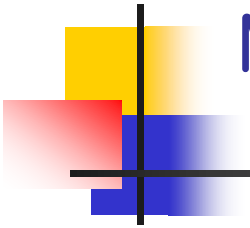
- Efficient Pairing Computation

Pairing application in crypto

Pairings in cryptanalysis

$$\text{ECDLP} \Rightarrow \text{DLP} / F_q$$

- MOV reduction, using Weil pairing
  (Menezes, Okamoto, Vanston 1993)
- FR reduction, using Tate pairing
  (Frey Rück 1994)



Motivation for efficient pairing computation

Cryptosystem using pairings

- one round tree party key agreement (A. Joux, 2000)
- ID based encryption (Boneh & Franklin, 2001)
- Short signatures/ID based signatures
- ID based key agreement protocols
- Certificateless PKC . . . Signcryption, Broadcast encryption, Traitor tracing . . . . . .

Recent progress in pairing computation

⇒ BKLS/GHS algorithm (2002)

⇒ Duursma-Lee technique (2003)

⇒ Eta_T pairing on supersingular curves (BGES 2004)

⇒ Ate pairing on ordinary curves (HSV 2006/GHOTV 2007)

⇒ optimized Ate pairing (MKHO 2007)

⇒ Ate_i pairing (ZZH 2007)

⇒ R-Ate pairing (LLP 2008)

⇒ Optimal pairing (V 2008)

⇒ Pairing Lattice (H 2008)

goal of this process is **simplifying Miller's algorithm** and **reducing the loop length of Miller's algorithm**.

Improvements on Tate pairing

BKLS/GHS algorithm, 2002 on $y^2 = x^3 - x + d$, $d=\pm 1$

1. Evaluate at divisor ⇒ evaluate at point
2. Removing the denominator in Miller algorithm
   after final exponentiation.
3. Using multiplication by 3 rather than 2 : multiplication
   $V \rightarrow 3V$ is particularly simple, $V = (\alpha,\beta)$, $3V = ((\alpha^3)^3-d,-(\beta^3)^3)$.

Duursma-Lee Algorithm, 2003

1. generalized to a hyperelliptic curve,
2. providing the loop shortening idea ⇒ "eta pairing approach"

Eta, Eta_T, Ate pairing

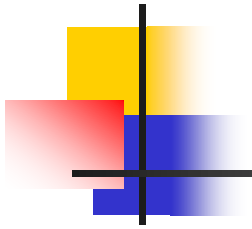
- $\#E(F_q) = q+1-t = q-T = N$ $(|t| \le 2\sqrt{q})$

  $\#J(F_q) = q^2+aq+b = N$

  $(f_{A,P}) = A(P) - ([A]P) - (A-1)(O)$

- $f_{N,P}$: Tate pairing
- $f_{q,P}$: Eta pairing (Ate pairing)
  - Supersingular curve with $y^2=x^p-x+b$, $(b=\pm 1,\ p\equiv 3 \bmod 4)$ (DL 03)
  - Hyperelliptic curve (Ate pairing) (GHOTV 07)
- $f_{T,P}$: Eta_T pairing (Ate pairing)
  - Supersingular elliptic/ Hyperelliptic curve (BGES 04)
  - Ordinary elliptic curve (Ate pairing) (HSV 06)

Optimized Ate and Ate_i pairing



- $\#E(F_q) = q+1-t = q-T = N$
- $t \geq r^{1/\varphi(k)}$ ($r \mid N$)
- $S \equiv q \bmod r$, $f_{S,D}$ (Optimized Ate) (MKHO 07)
- $T_i \equiv q^i \bmod r$, $f_{T_i,D}$ (Ate_i) (ZZH 07)

Pairings on Elliptic curve

- $\#E(F_q) = q+1-t = q-T = N$ ($|t| \le 2\sqrt{q}$), $r \mid N$, $r \sim q$(size)

	Supersingular	Ordinary	Miller length	
Tate pairing	$f_{r,P}(Q)$	$f_{r,P}(Q)$	$\log_2 r$	r:prime
Eta pairing	$f_{q,P}(\psi(Q))$		$\log_2 q$	ψ:distortion map
Eta_T pairing	$f_{T,P}(\psi(Q))$		$\log_2 q^{1/2}$	
Ate pairing	$f_{T,P}(Q)$	$f_{T,Q}(P)$	$\log_2 q^{1/2}$	$P \in G_1$ $Q \in G_2$
Op Ate, Atei	$f_{T_i,P}(Q)$	$f_{T_i,Q}(P)$	$\ge \log_2 r^{1/\varphi(k)}$	$T_j = q^j \bmod r$

Example – BN curve

- $k=12,\ \varphi(k)=4$
- $p=36z^4+36z^3+24z^2+6z+1$
- $r= 36z^4+36z^3+18z^2+6z+1$
- $T := \min\{T_i=p^i \bmod r,\ 1\le i \le k\}$

  $= T_1 = 6z^2$
- Miller length for Ate_i pairing: $\log_2 r^{1/2}$
- There are many elliptic curves which cannot reach the low bound, $\log_2 r^{1/\varphi(k)}$

Pairings on Hyperelliptic curve with genus 2

- $\#J(F_q) = q^2+aq+b = N,\ \ r \mid N,\ \ r \sim q^2$

	Supersingular	Ordinary	Miller length	
Tate pairing	$f_{r,P}(Q)$	$f_{r,P}(Q)$	$\log_2 r$	
Eta pairing	$f_{q,P}(\psi(Q))$		$\log_2 q$	ψ:distortion map DL-curve
Eta$_T$ pairing	$f_{T,P}(\psi(Q))$		$\log_2 q^{3/2}$	$y^2+y=x^5+x^3+d$ /F_{2^m}
Ate pairing	$f_{q,P}(Q)$*	$f_{q,Q}(P)$	$\log_2 q$	$P \in G_1$ $Q \in G_2$ * Superspecial

[Pairing 2007, Galbraith, Hess, Vercauteren]

- Can further loop shortening be performed for the hyperelliptic Ate pairing such that Miller length $\leq \log_2 q^a$ with $a < 1$?

R-ate pairing [08, Lee, Lee & Park]

- Recall the Ate pairing and the Tate pairing
  - $\#E(Fq) = q - T = N$
  - $f_{q,Q}(P) = f_{N+T,Q}(P) = f_{N,Q}(P) f_{T,Q}(P) G_{NQ,TQ}(P)$
  - Use two parameters q and N for a new pairing
- Use other parameters for a new pairing
  - Improve the efficiency of the pairing computation
    - for some pairing friendly curves
    - for supersingular hyperelliptic curves with genus 2
  - Generalize previous pairings

Definition: R-ate pairing

Let $\omega = a\tau + b$ for $\omega, a, \tau, b \in Z$

$f_{\omega,D} = f_{a\tau+b,D} = (f_{\tau,D})^a \cdot f_{a,\tau D} \cdot f_{b,D} \cdot G_{a\tau D,bD}$ $(G_{a\tau D,bD} = l_{a\tau D,\ bD} / v_{(a\tau+b)D})$

If $f_{\omega,D}$, $(f_{\tau,D})^a$ are bilinear, then

$\Rightarrow$ $f_{a,\tau D} \cdot f_{b,D} \cdot G_{a\tau D,\ bD}$ is bilinear.

Ratio of two pairings

R

$R_{\omega,\tau}(D,E) = f_{a,\tau D}(E) \cdot f_{b,D}(E) \cdot G_{a\tau D,bD}(E)$ $\Leftrightarrow$ R-ate pairing

Theorem

Let

- $N = \#J(F_q)$
- $\omega = a\tau + b$
  - $f_{\omega,D}$, and $f_{\tau,D}$ provides non-degenerate pairings with

    $e(D,E)^{L_1} = f_{\omega,D}(E)^{M_1}$, $e(D,E)^{L_2} = f_{\tau,D}(E)^{M_2}$

  Let $M=\mathrm{lcm}(M_1,M_2)$, $L=M(L_1/M_1 - aL_2/M_2)$
- If $r \nmid L$, $R_{\omega,\tau}(D, E)$ is a non-degenerate bilinear pairing with the relation, $e(D,E)^L = R_{\omega,\tau}(D, E)^M$

Corollary

- $(\omega, \tau) = (q, r)$: R-ate pairing = Ate pairing
  - $q = ar+T$
  - $f_{q,D} = f_{ar+T,D} = f_{ar,D} \cdot f_{T,D}$
  - R-ate pairing = $f_{T,D}$
- $(\omega, \tau) = (q^i, r)$: R-ate pairing = Ate_i pairing
  - $q^i = ar+T_i$
  - $f_{q^i,D} = f_{ar+T_i,D} = f_{ar,D} \cdot f_{T_i,D}$
  - R-ate pairing = $f_{Ti,D}$

Corollary

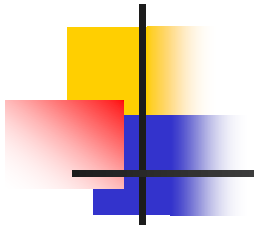
- $(\omega, \tau) = (T_i, T_j)$ or (r, T_j)
  - $T_i = aT_j + b$ or $r = aT_j + b$
  - $f_{T_i,D}$ (or $f_{r,D}$) $= f_{aT_j+b,D} = (f_{T_j,D})^a \cdot f_{aD,T_j} \cdot f_{b,D} \cdot G_{aT_jD,bD}$

    $= (f_{T_j,D})^a \cdot (f_{a,D})^{q^j} \cdot f_{b,D} \cdot G_{aT_jD,bD}$
  - R-ate pairing $= (f_{a,D})^{q^j} \cdot f_{b,D} \cdot G_{aT_jD,bD}$

R-ate pairings

$1 \le i, j \le k$, $\omega = a\tau + b$, $T_i = q^i \mod r$

(ω, τ)	R-ate pairing	
(q,r)	$f_{T,D}$	Ate
(q^i,r)	$f_{Ti,D}$	Ate_i
(T_i, T_j)	$(f_{a,D})^{q^j} \cdot f_{b,D} \cdot G_{aTDj,bD}$	New type
(r, T_j)	$(f_{a,D})^{q^j} \cdot f_{b,D} \cdot G_{aTDj,bD}$	



- How can we compute the R-ate pairing with better efficiency than Ate or Ate_i even if it looks complicated?

- goal : Miller length ~> $r^{1/\varphi(k)}$

Algorithm

- Input: D,E, (T_i, T_j)
- Output: $R(D,E)=(f_{a,D})^{qj} \cdot f_{b,D} \cdot G_{aT_jD,bD}$
  with $T_i=aT_j+b$

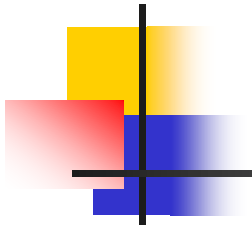
Let $a=cb+d$

1. $(f_{b,D}, bD) \leftarrow$ Miller alg.(D,E,b)
2. $(f_{c,bD}, cbD) \leftarrow$ Miller alg.(bD,E,c)
3. $(f_{d,D}, dQ) \leftarrow$ Miller alg.(D,E,d)
4. $f_1 \leftarrow f_{b,D}^{c} f_{c,bD} f_{d,D}$
5. $f_{a,D} \leftarrow f_1 G_{cbD,dD}$
6. $aD \leftarrow cbD+dD$
7. $f_2 \leftarrow f_{a,D}^{qj} f_{b,D}$
8. $f_3 \leftarrow f_2 G_{\phi j(aD),bD}$

Return f_3

A Criterion for efficient R-ate pairing on elliptic curves

- Assumption
  - k : even embedding degree
  - $\mathbf{t}_{MO}$: time for computing one loop in Miller's algorithm
- Note
  - $\mathbf{t}$(Miller)~Miller length · $\mathbf{t}_{MO}$
  - $\mathbf{t}(g^c \text{ in } F_{q^k}) \leq 2(\log_2 c) \cdot \mathbf{t}_{MO}$ /17



- Then
  - $t(Ate_i) = \log_2 T \cdot t_{MO}$, $T = \min_{1 \le i \le k}(T_i)$
  - $t(R_{\omega,\tau}) \le \Lambda \cdot t_{MO}$
    - $\omega = a\tau + b$, $\max\{a,b\} = c \cdot \min\{a,b\} + d$
    - $\Lambda = \log_2(\min\{a,b\}) + 19\log_2 c/17 + \log_2 d + 2$
  - $\gamma(\omega,\tau) := \Lambda / \log_2 T$
- Thus
  - $\exists(\omega,\tau)$ such that $\gamma(\omega,\tau) < 1$

    $\Rightarrow \exists$ efficient R-ate pairing

Supersingular elliptic curves with char 2,3

- $E : y^2=x^3-x+b$ / F_q $(b=\pm 1,\ q=3^m,\ (m,6)=1)$
- $\#E(F_q)=3^m+1\pm b3^{(m+1)/2}=3^m-T$
- $3^m=\pm b3^{(m-1)/2}(T+1)$
- $f_{3^m} = f_{3^{(m-1)/2}(T+1)} = (f_{T+1})^{3^{(m-1)/2}} \cdot f_{3^{(m-1)/2},T+1}$
  $= (f_T)^{3^{(m-1)/2}} \cdot \underbrace{f_{3^{(m-1)/2},(T+1)} \cdot (G_{T,1})^{3^{(m-1)/2}}}$
- R-ate pairing $= f_{3^{(m-1)/2},(T+1)} \cdot (G_{T,1})^{3^{(m-1)/2}}$
- Eta_T pairing $= f_{3^{(m+1)/2}} \cdot G_{3^{(m+1)/2},1}$

Ordinary elliptic curves(1)

- E1 curve (MF05) : k=7
  - T_2 : 54bits (Ate_i pairing = f_{T_2})
  - $r = T_1 + b$ (b: 27bits, r: 160 bits)
  - R-ate pairing = $f_{b,D} \cdot G_{T_1D,bD}$
- E2 curve (MF05) : k=10
  - T_6 : 60bits (Ate_i pairing = f_{T_6})
  - $T_9 = aT_2 + a^2$ (a: 20bits, r: 160 bits)
  - R-ate pairing = $(f_{a,D})^{q^2} \cdot f_{a^2,D} \cdot G_{aT_2D,\ a^2D}$
  - $\gamma(T_9, T_2) = 2/3$

Ordinary elliptic curves(2)

- E3 curve (FST06) : k=8
  - $r = 9z^4+12z^3+8z^2+4z+1$
  - $T_1 = -9z^3-3z^2-2z-1$ (Ate_i pairing = f_{T_1})
  - $T_3 = T_2 + b$ (b=3z+1)
  - R-ate pairing = $f_{b,D} \cdot G_{T_1D,bD}$
  - $\gamma(T_3, T_2) = 1/3$

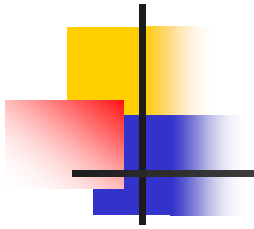
- E4 curve (F06) : k=10
  - $T_2 = 5z^2$ (Ate_i pairing = f_{T_2})
  - $T_9 = (a+2)T_2 + a$ (a=5z+1)
  - R-ate pairing = $(f_{a+2,D})^{q^2} \cdot f_{a,D} \cdot G_{(a+2)T_2D,aD}$
  - $\gamma(T_9, T_2) = 1/2$

Ordinary elliptic curves(3)

- E5 curve (BN05)
- $k=12$, $\varphi(k)=4$
- $r= 36z^4+36z^3+18z^2+6z+1$
- $T = T_1 = 6z^2$ (Ate_i pairing $= f_{T_1}$)
- $T_{10} = (a+1)T_1 + a$ $(a=6z+2)$
- R-ate pairing $= (f_{a+1})^q \cdot f_a \cdot G_{(a+1)T_1,\, a}$
- $\gamma(T_{10}, T_1) = 1/2$

curve	Parameters	Ate_i	R-ate	γ
E1 [MF05]	$k=7,\ \varphi(k)=6,\ \log_2 r=160$ $p=152683916815195328299425822768509148050335333587091954124192528892961908503610 31$ $r=1040722131042824291503998495039735508885676564761$	$T_2=1013\cdots6225$ (54bits)	$r=T_1+100667465$ (27bits)	N/A
E2 [MF05]	$k=10,\ \varphi(k)=4,\ \log_2 r=160$ $p=396120610547891063909698040682890664156040501831963430185626838652064692433391635091$ $r=1253732242268690674049383020671966019699064954321$	$T_6=1088\cdots2309$ (60bits)	$T_9=1028669\,T_2+1028669^2$ (40bits)	2/3
E3 [FST06]	$k=8,\ \varphi(k)=4$ $p=(81z^6+54z^5+45z^4+12z^3+13z^2+6z+1)/4$ $r=9z^4+12z^3+8z^2+4z+1$	$T_1=-9z^3-3z^2-2z-1$	$T_3=T_2+3z+1$	1/3
E4 [F06]	$k=10,\ \varphi(k)=4$ $p=25z^4+25z^3+25z^2+10z+3$ $r=25z^4+25z^3+15z^2+5z+1$	$T_2=5z^2$	$T_9=(5z+3)T_2+(5z+1)$	1/2
E5 [BN05]	$k=12,\ \varphi(k)=4$ $p=36z^4+36z^3+24z^2+6z+1$ $r=36z^4+36z^3+18z^2+6z+1$	$T_1=6z^2$	$T_{10}=(6z+3)T_1+6z+2$	1/2

Supersingular hyperelliptic curve with genus 2



- $q = p^n$, n odd
- *H : supersingular hyperelliptic curve of genus 2 defined over* F_q
- $\#J(F_q) = q^2+aq+b$, r : large prime factor of $\#J(F_q)$
- $G_1 = \mathbf{J}_c[r] \cap \ker(\varphi - 1)$, $G_2 = \mathbf{J}_c[r] \cap \ker(\varphi - [q])$ as before

Supersingular hyperelliptic curve with genus 2

[Theorem] $\#J(F_q) = q^2+aq+b$

(1) $|a| \le 4\sqrt{q} + 10$, $|b| \le 4\sqrt{q} +1$, $|a-b| \le 9$

(2) R-ate pairing :

$$\begin{cases} (f_{a,Q}(P))^q \cdot f_{b,Q}(P) \cdot G_{aT_1,b} & \text{if supersingular} \\ (f_{a,P}(Q))^q \cdot f_{b,P}(Q) \cdot G_{aT_1,b} & \text{if superspecial} \end{cases}$$

Remark on Miller length

$R_{T_2,T_1}(Q,P)=(f_{a,Q}^{q} \cdot f_{b,Q} \cdot G_{qaQ,bQ})(P)$

- $a = b + d$
- $|d| \leq 9$
- $\log_2 \min\{a,b\} \sim (\log_2 q) / 2$
- $\mathbf{t}(\text{R-ate}) \leq \mathbf{t}_{MO}(\log_2 \min\{a,b\}+\log_2 9) + \mathbf{t}_{MA} + 3M_k + \mathbf{t}_{G,A}$
  - $\mathbf{t}_{MA} + 3M_k + \mathbf{t}_{G,A} \leq 2\,\mathbf{t}_{MO}$
- : time for addition, an mult in F_{q^k}, and computing $G_{qaQ,bQ}$

However, *not quite half in practical.*

The next case is example.

$\mathbf{t}(\text{R-ate}) \leq \mathbf{t}_{MO} \cdot (\log_2 \min\{a,b\}+5)$

Miller length ~ half of $\log_2 q$

Supersingular hyperelliptic curve with genus 2

- $H_2 : y^2=x^5-x+b$ / F_q $(b=0,1,\ q=5^m)$
- $\#J(F_q) = 5^{2m} + (a+2)5^m + a$ $\left(a = \pm 5^{(m+1)/2} + 1 \right)$
  - $T_2 = (a+2)T_1 + a$
  - R-ate pairing = $(f_{a+2})^q \cdot f_a \cdot G_{(a+2)T_1,\ a}$
  - Ate pairing = f_{5^m}

Comparison of the Miller length

Curve	E1	E2	E3	E4	E5*	H5
Miller length for Ate_i	54	60	123	117	128	89
Miller length for R-ate	28	44	43	62	68	70

<80 bit security level, *128 bit>

Optimal pairing[08, Vercateran]

- Using q-expansion of a multiple $\lambda = m \cdot r$
- Using LLL-Alg, find small coeff of q-expansion
- Let e: $G_1 \times G_2 \rightarrow G_T$ be a non-degenerate, bilinear with order r, called **optimal pairing** if **e** can be computed in $\log_2 r/\varphi(k) + \varepsilon(k)$ basic Miller iterations, with $\varepsilon(k) \leq \log_2 k$

- $\lambda = m \cdot r = \Sigma\, c_i\, q^i$

$$\underbrace{t(Q,P)^m} = f_{r,Q}(P)^m = f_{mr,Q}(P) = f_{\lambda,Q}(P) = f_{\Sigma\, c_i\, q^i,Q}(P)$$

Tate pairing

$$= \prod f_{c_i\, q^i,Q}(P) \cdot \prod G_{i,Q}(P)$$

$$= \prod \left(f_{c_i}{}^{q^i}{}_{,Q}(P) \cdot f_{q^i,\, c_iQ}(P) \right) \cdot \prod G_{i,Q}(P)$$

$$= \prod \underbrace{\left(f_{c_i}{}^{q^i}{}_{,Q}(P) \cdot G_{i,Q}(P) \right)} \cdot \underbrace{\prod f_{q^i\, ,\, c_iQ}(P)}$$

Candidate of Optimal pairing

Product of Eta pairing

- $L := \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -q & 1 & 0 & \cdots & 0 \\ -q^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ -q^{\varphi(k)-1} & 0 & 0 & \cdots & 1 \end{pmatrix}$

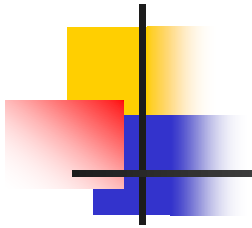
- $\exists$ short vector $V \in L$ with $\| V \| \leq r^{1/\varphi(k)}$

- Using LLL-Algorithm, we can find V.

$$
\begin{array}{l}
m\ x \\
c_1\ x \\
c_2\ x \\
\vdots \\
c_\ell\ x
\end{array}
\begin{pmatrix}
r & 0\ 0 \cdots 0 \\
-q & 1\ 0 \cdots 0 \\
-q^2 & 0\ 1 \cdots 0 \\
\vdots & \vdots \quad \ddots \\
-q^{\varphi(k)-1} & 0\ 0 \cdots 1
\end{pmatrix}
$$

$$
= \left(c_0, \quad c_1, \cdots, c_\ell \right)
$$

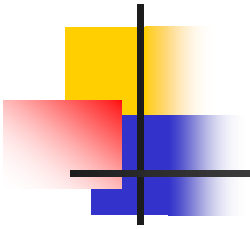
- $V = (c_0, c_1, \cdots c_\ell)$ with $\| V \| \leq r^{1/\varphi(k)}$



- $mr = c_0 + c_1 q + \cdots + c_\ell q^\ell$
- $a_{[c_0,c_1,\cdots,c_\ell]}(Q,P) = \prod (f_{c_i}^{qi}{}_{,Q}(P) \cdot G_{i,Q}(P))$: Pairing

  with $|c_i| \leq r^{1/\varphi(k)}$ for $0 \leq i \leq \ell = \varphi(k)-1$

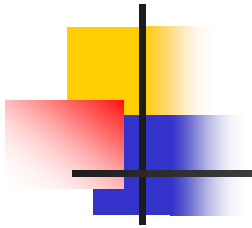
- For optimal pairing, we need to choose a short vector V with a minimal number of coordinates of size $r^{1/\varphi(k)}$



Conclusion & …

- R-ate pairing:
  - give pairings with low bound of Miller length when Ate_i pairings can't reach.
  - give more optimization for pairing computation in supersingular hyperelliptic curve with genus 2.
  - Higher genus curve or non-supersingular hyperelliptic curve?

  ➔ also applicable ➔ but is it efficient?



Thank you !