# On the Implementation of Tate Pairings

Soonhak Kwon
Dept. of Mathematics, Sungkyunkwan University, Korea
shkwon@skku.edu

Bilinear pairings were originally used as tools for attacking discrete logarithm problem for supersingular elliptic curves: MOV, and Frey and Rück Attack.

They become popular these days for identity-based encryption and signature schemes.

Tate pairing is a nicer candidate (computational advantage over Weil pairing).

**Some theoretical improvements of Tate Pairing have been proposed recently.**

Namely, Eta pairing and Ate pairing.

Explanation of the story

$$Tate \overset{HOW}{\longrightarrow} Eta \overset{HOW}{\longrightarrow} Ate$$

is our topic in this talk.

Let $E$ be an elliptic curve over $\mathbb{F}_q$ and $r$ be a (large) prime satisfying

$$r \mid \#E(\mathbb{F}_q)$$

The smallest positive integer $k$ satisfying $q^k \equiv 1 \pmod{r}$ is called an embedding degree (or security multiplier). If $k > 1$ and $(r, q) = 1$, then one has

$$E[r] \subset E(\mathbb{F}_{q^k})$$

$$\left( \iff \langle \mu_r \rangle \subset \mathbb{F}_{q^k} \right)$$

For integer $s$ and point $P \in E[r]$, one may consider the principal divisor

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

The Tate pairing is a non-degenerate bilinear pairing,

$$\langle \cdot, \cdot \rangle_r : E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^r$$

defined as $\langle P, Q \rangle_r = f_{r,P}(D_Q)$ where $D_Q$ is a divisor equivalent to $(Q) - (O)$ with $(f_{r,P})$ and $D_Q$ having disjoint supports.

More familiar Weil pairing $w(P, Q)$ can be interpreted as

$$w_r(P, Q) = \langle P, Q \rangle / \langle Q, P \rangle$$

which explains the computational advantage of Tate pairing over Weil pairing.

In many situations, one needs to determine unique $r$-th root of unity so one may define the reduced Tate pairing

$$e(P,Q) = \langle P,Q\rangle_r^{\frac{q^k-1}{r}} = f_{r,P}(D_Q)^{\frac{q^k-1}{r}}$$

Here, By Hasse's Theorem restricts the bound of $\#E(\mathbb{F}_q)$ as

$$\#E(\mathbb{F}_q) = q + 1 - t, \quad t \leq 2\sqrt{q}$$

Thus one needs roughly $\log_2 r \approx \log_2 q$ iterations (of divisor additions and doublings) for computing $f_{r,P}$.

A standard algorithm computing $f_{r,P}$ for given $P \in E[r]$ is so called Miller's algorithm, and speeding up Miller's algorithm has been quite an active research topic.

**Miller's Algorithm for Divisor Addition:** Thinking of reduced representations of divisors $D$ and $D'$,

$$D = (P) - (O) + (f) \quad \text{and} \quad D' = (P') - (O) + (f')$$

for some rational functions $f$ and $f'$, Miller's formula says

$$D + D' = (P + P') - (O) + (f f' \frac{\ell_{P,P'}}{\ell_{P+P'}})$$

$$s \to 1 \qquad \text{(I)}$$

$$s(P) - s(O) = ([s]P) - (O) + (f_{s,P}) \qquad \text{(II)}$$

$$s \to 2s \quad \text{or} \quad s \to 2s + 1 \qquad \text{((and apply Miller) III)}$$

$$r(P) - r(O) = (f_{r,P}) \qquad \text{(IV)}$$

**Recent Progress:** to name just few

BKLS Algorithm (2002, Barreto, Kim, Lynn, Scott)),

Duursma-Lee technique (2003, Duursma, Lee),

Eta pairing (2005, Barreto, Galbraith, O'hEigeartaigh, Scott),

Ate pairing (2006, Hess, Smart, Vercauteren)

are all concerned with the techniques of simplifying Miller's algorithm and finding suitable $T << r$ that may replace $r$ in computing Tate pairing.

**BKLS Algorithm:** $e(P,Q) = f_{r,P}(D_Q)^{\frac{q^k-1}{r}} \overset{modified}{\Longrightarrow} f_{r,P}(\psi Q)^{\frac{q^k-1}{r}}$

Using suitable automorphism $\psi$ (called distortion map), denominators $\ell_P$ can be eliminated after final exponentiation.

$D_Q$ can be replaced by $Q$

**Duursma-Lee Algorithm:**

Closed formula of Tate pairing for (hyper)elliptic case over cubic field

Find the following equality;

$$f_{r,P}(\psi Q)^{\frac{q^k-1}{r}} = f_{q^m+1,P}(\psi Q)^{q^m-1} = f_{q,P}(\psi Q)^{\square(q^m-1)}$$

where $m = k/2$

**Eta Pairing:**

Extension of Duursma-Lee Algorithm for supersingular curves

**Ate Pairing:**

Eliminates the use of distortion map $\psi$

Extension of Eta Pairing for supersingular and ordinary curves

## Idea of Ate Pairing

Introduce new (nicer) parameters $N$ and $T$ such that

$$r \rightsquigarrow N, \qquad q \rightsquigarrow T$$

Typical choice of $T$ is $T = t - 1$ where $t = \pi + \overline{\pi}$.

Here $T \equiv q \pmod{r}$, and $\pi$ is a Frobenius endomorphism of $E$ over $\mathbb{F}_q$,

$$\pi : E \longrightarrow E, \quad \pi(x, y) = (x^q, y^q)$$

Choose any $N > 0$ satisfying

$$r|N,\ N|q^k - 1 \text{ and } N|T^a \pm 1 \text{ for some } a.$$

Typical choice of $N$ is $N = gcd(T^k - 1, q^k - 1)$.

Write $T^k - 1 = LN$. Then

$$\begin{aligned} e(Q,P)^L = f_{r,Q}(P)^{L\cdot\frac{q^k-1}{r}} &= f_{N,Q}(P)^{L\cdot\frac{q^k-1}{N}} \\ &= f_{LN,Q}(P)^{\frac{q^k-1}{N}} \\ &= f_{T^k-1,Q}(P)^{\frac{q^k-1}{N}} \end{aligned}$$

Simple trick in Miller's algorithm imply

$$e(Q,P)^L = f_{T^k-1,Q}(P)^{\frac{q^k-1}{N}} = f_{T^k,Q}(P)^{\frac{q^k-1}{N}} \qquad \text{(Formula A)}$$

Duursma and Lee noticed

$$f_{T^k,Q} = \prod_{i=0}^{k-1} f_{T,T^iQ}^{T^{k-1-i}} = f_{T,Q}^{T^{k-1}} f_{T,TQ}^{T^{k-2}} f_{T,T^2Q}^{T^{k-3}} \cdots f_{T,T^{k-1}Q}$$

(Formula B)

Techniques of Ate pairing (we will explain soon) show

$$??? \quad f_{T,T^iQ} = f_{T,Q}^{h_i} \quad \text{for some } h_i \quad ???$$

and therefore Formula B implies (*usually, one has* $h_i = q^i$)

$$f_{T^k,Q} = f_{T,Q}^{\sum_{i=0}^{k-1} T^{k-1-i} h_i}$$

It will be shown the above properties hold if

(1) End($E$) has some nice elements

(2) Choose a proper domain for $Q$ and for $f$

Assume there is $\theta$ which is an

automorphism or purely inseparable endomorphism

In any case, it has separable degree one.

$$\text{i.e.} \quad \#\theta^{-1}(Q) = 1 = deg_s\theta$$

Then from $(f_{T,\theta Q}) = T(\theta Q) - (T\theta Q) - (T-1)(O)$, one has

$$\begin{aligned}(f_{T,\theta Q} \circ \theta) &= \theta^\star(f_{T,\theta Q}) = \theta^\star\{T(\theta Q) - (T\theta Q) - (T-1)(O)\} \\ &= e_\theta\{T(Q) - (TQ) - (T-1)(O)\} \\ &= e_\theta(f_{T,Q}) = (f_{T,Q})^{e_\theta}\end{aligned}$$

Thus one has the following up to constant multiple,

$$f_{T,\theta Q} \circ \theta = f_{T,Q}^{e_\theta} \qquad \text{(Formula C)}$$

We also want the condition $TQ = \theta Q$ to merge Formula C to Formula B

Formula A,B,C are TRUE

$$\text{for } \textit{any } Q \in E[r] \text{ and } \textit{any } P \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$$

But, from now on,

the condition of $P$ and $Q$,

and supersingular (or ordinary) properties of the curve $E$ do matters !!

For supersingular curves,

Eta pairing chooses $\theta = \gamma$ an automorphism,

which is related with a distortion map $\psi$ as

$$\gamma \circ \psi^{[q]} = \psi. \ (\psi^{[q]} \neq \psi \circ \cdots \circ \psi)$$

In this case, one has $e_\theta = 1$.

**Ate Pairing** introduces nice terminologies which are very convenient to understand and unify all previous ideas.

Let

$$G_1 = \{P \in E[r] | \pi P = P\} = E[r] \cap ker(\pi - 1)$$

and let

$$G_2 = \{Q \in E[r] | \pi Q = qQ\} = E[r] \cap ker(\pi - [q])$$

.

Then

$$E[r] = G_1 \oplus G_2$$

## Eta Pairing

Did not use $G_1$ and $G_2$ in the paper,

but in fact it was defined on $G_1 \times G_2$.

The existence of automorphism $\gamma$ of $E$ satisfying the condition

$$\gamma \circ \psi^{[q]}|_{G_1} = \psi|_{G_1}, \quad \text{and} \quad \gamma|_{G_1} = [q] \tag{1}$$

is crucial to find a nice form so called Eta pairing.

For each supersingular cases (binary, cubic, binary hyperelliptic), they constructed

explicit automorphism $\gamma$ satisfying above equation 1

For $P, R \in G_1$, using the equation 1 and Formula C,

$$f_{T,\gamma P}(\underline{\psi} R) = f_{T,\gamma P} \circ \underline{\gamma \circ \psi^{[q]}}(R) = f_{T,P} \circ \psi^{[q]}(R) = f_{T,P}(\psi R)^q \tag{2}$$

Since $T = t - 1 \equiv q \pmod{r}$,

$$f_{T,TP}(\psi R) = f_{T,\gamma P}(\psi R) = f_{T,P}(\psi R)^q$$

or more generally

$$f_{T,T^i P}(\psi R) = f_{T,P}(\psi R)^{q^i}$$

**— The End of Eta Pairing —**

For $R \in G_1$, the image of the distortion map, $\psi(R)$ is in $G_2$.

Thus letting $Q = \psi(R) \in G_2$, one has

$$Q = \psi(R) = \gamma \circ \psi^{[q]}(R) = \gamma \circ \pi(Q)$$

Therefore the automorphism $\gamma$ satisfies two conditions;

$$\gamma \circ \pi = 1 \quad (i.e.\ \gamma = [q]^{-1}) \quad \text{on} \quad G_2, \qquad \gamma = [q] \quad \text{on} \quad G_1$$

Rather than trying to find explicit automorphism $\theta = \gamma$ for each supersingular cases, Hess et al. used Frobenius endomorphism $\pi$ and the dual $\overline{\pi}$ (which are well-known more easier to deal with) and extended it to ordinary cases.

## Ate Pairing

Works for any cases (supersingular or ordinary) by choosing

$$\theta = \pi \text{ and considering Tate pairing on } G_2 \times G_1$$

Works for supersingular cases by choosing

$$\theta = \overline{\pi} \text{ and considering Tate pairing on } G_1 \times G_2,$$

which is analogous to Eta pairing (but not exactly same).

**Ate Pairing on $G_2 \times G_1$:** $\theta = \pi$ is used

Let $Q \in G_2$ and $P \in G_1$.

Then $\pi(P) = P$ and $\pi(Q) = qQ = TQ$. Thus defining $\theta = \pi$,

$$f_{T,TQ} \circ \pi = f_{T,\theta Q} \circ \theta = f_{T,Q}^{e_\theta} = f_{T,Q}^{q}$$

Thus

$$f_{T,TQ}(P) = f_{T,TQ} \circ \pi(P) = f_{T,Q}^{q}(P)$$

or more generally

$$f_{T,T^iQ}(P) = f_{T,Q}^{q^i}(P)$$

**Ate Pairing on $G_1 \times G_2$:** $\theta = \overline{\pi}$ is used

Same way let $Q \in G_2$ and $P \in G_1$.

Then $\overline{\pi}(P) = qP = TP$

$$\because \overline{\pi}(P) = \overline{\pi}\pi(P) = qP \text{ where } P \in G_1$$

and $\overline{\pi}(Q) = Q$

$$\because qQ = \overline{\pi}\pi Q = \overline{\pi}(qQ) = q\overline{\pi}Q \text{ where } Q \in G_2.$$

**1. Supersingular Case on $G_1 \times G_2$:**

$\overline{\pi}$ is purely inseparable of degree $q$

Thus by defining $\theta = \overline{\pi}$,

and since $\overline{\pi}$ is purely inseparable of degree $q$,

$$f_{T,TP} \circ \overline{\pi} = f_{T,\theta P} \circ \theta = f_{T,P}^{e_\theta} = f_{T,P}^{q}$$

Thus

$$f_{T,TP}(Q) = f_{T,TP} \circ \overline{\pi}(Q) = f_{T,P}^{q}(Q)$$

or more generally

$$f_{T,T^iP}(Q) = f_{T,P}^{q^i}(Q)$$

## 2. Ordinary Case on $G_1 \times G_2$ : $\overline{\pi}$ is separable of degree $q$

In this case, $\overline{\pi}$ is separable of degree $q$ and $ker(\overline{\pi}) = E[q] \cong \mathbb{Z}/q\mathbb{Z}$.

No obvious expression of $f_{T,T^iP}$ exists in terms of $f_{T,P}$ because

$$\begin{aligned}
(f_{T,TP}|_{G_2}) &= (f_{T,TP} \circ \overline{\pi}) \\
&= (f_{T,\overline{\pi}P} \circ \overline{\pi}) \\
&= \overline{\pi}^{\star}(f_{T,\overline{\pi}P}) \\
&= \overline{\pi}^{\star}\{T(\overline{\pi}P) - (T\overline{\pi}P) - (T-1)(O)\} \qquad (???) \\
&\neq (f_{T,P}|^{\square}_{G_2})
\end{aligned}$$

$(???)$ has complicated expression due to $\#\overline{\pi}^{-1}(\overline{\pi}P) = q$.

However using the theory of twists, one can also show there exists similar formulas.

Though this twisting technique is considered only for the Ate pairings of ordinary curves $E$, it can also be applied to supersingular cases.

**Summary:**

The advantage of Ate pairing is that one can replace

$$f_{q^k,P}(Q)$$

by

$$f_{T,P}(Q)^*$$

where $*$ is an integer depending on $q, k$, and $T = t - 1$ is roughly $\approx \sqrt{q}$.

It would be very good if one could find an improved version of the above idea or any new approach.

**—Thank You—**