

# Implementing Cryptographic Pairings and the R-ate Pairing

Luis J Domínguez P

Dublin City University

March, 2009

<http://www.computing.dcu.ie/~ldominguez/pairings>



- 1 Pairings
  - Introduction
  - Tate pairing
  - ate pairing
- 2 R-ate pairing
  - Introduction
  - TiTj
- 3 R-ate parameters
  - k=18
  - k=36
  - BN
- 4 Conclusion

The computation of pairings basically involves two groups,  $G_1$  and  $G_2$ . These two groups are finite cyclic additively-written groups and at least one of which is of prime order  $r$ . The pairing will take an element from each of the two groups and map them to the third group  $G_T$ , which is a finite cyclic multiplicatively-written group also of prime order  $r$ . A useful cryptographic pairing satisfies the following properties:

- Bilinearity
- Non-degeneracy
- Computability

Let  $P \in E(\mathbb{F}_p)[r]$  and  $Q \in E(\mathbb{F}_{p^k})$ , consider the divisor  $D = (Q + S) - (S)$  with  $S$  a random point in  $E(\mathbb{F}_{p^k})$ . Let  $f_{a,P}$  be a function with a divisor  $(f_{a,P}) = a(P) - (aP) - (a-1)(\mathcal{O})$  for  $a \in \mathbb{Z}$ . A non degenerate bilinear Tate pairing can be defined as a map:

### Definition

$$e_r : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \rightarrow \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r$$

$$(P, Q) \mapsto \langle P, Q \rangle_r = f_{r,P}(D)$$

This value of the pairing is in an equivalence class,  $\mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r$ , for practical purposes it is preferred to raise the value of the pairing to the power of  $(p^k - 1)/r$  to obtain a unique representative of the class.

It is necessary to apply the double-and-add, line-and-tangent algorithm until the point  $P$ , on being multiplied by its order  $r$ , finally reaches the  $\mathcal{O}$ . It will arrive there after  $\lg(r - 1)$  iterations of the miller loop.

Implementing the Tate Pairing is almost as easy as implementing the miller loop.

The Ate pairing is a variant of Tate pairing and it is a generalisation of the Eta pairing to ordinary pairing-friendly elliptic curves.

To measure if the family of curves is ate-friendly, we use the parameter  $\omega = \frac{\deg r(x)}{\deg m(x)}$ .

In the case of the KSS: k=18 curves,  $m(x) = x^3 + 18$ , and  $\omega \approx 2$ . Giving a family of curves with efficient ate pairing.

This pairing is suitable to pairing-friendly curves with small values of trace of Frobenius.

Frobenius endomorphism:  $\pi_p$

$$\pi_p : E \mapsto E : (x, y) \mapsto (x^p, y^p).$$

We denote

$$G_1 = E[r] \cap \text{Ker}(\pi_p - [1]), G_2 = E[r] \cap \text{Ker}(\pi_p - [p]).$$

Let  $T = t - 1$ . Let  $N = \gcd(T^k - 1, p^k - 1)$ ,  $T^k - 1 = LN$ .

### The ate pairing

For  $Q \in G_2$  and  $P \in G_1$  Ate pairing is defined as:

$$a_T : (Q, P) \mapsto f_{T,Q}(P)^{c_T(p^k-1)/N}$$

where  $c_T = \sum_{i=0}^{k-1-i} p^i \equiv kp^{k-1} \pmod{r}$ . The ate pairing is a bilinear non-degenerate pairing if  $r \nmid L$ . The first parameter should be defined over the extension field, but will be over  $\mathbb{F}_{p^3}$  for compression.

The new R-ate pairing introduced by Lee, Lee and Park [29] is a generalisation of the ate [24] and  $\text{ate}_i$  [45] pairing improving its computation efficiency. It takes three (two) short *Miller loops* to calculate the pairing, that together requires a shorter loop than a single typical application of the ate pairing. The *R-ate* pairing can be regarded as a ratio of any two pairings, hence the name.

The definition of the *R-ate* pairing with  $A = aB + b$  where  $A, B, a, b, \in \mathbb{Z}$  is as follows:

$$e_{A,B}(P, Q) = f_{a,BP}(Q) \times f_{b,P}(Q) \times G_{aBP,bP}(Q)$$

Generally this definition does not always give a bilinear and non-degenerate pairing. However, with a careful choice of pairs  $A$  and  $B$  one can succeed. For efficiency, we look for a working and non-trivial combination of  $A$  and  $B$  that would give the shortest *Miller loop*.

The R-a pairing algorithm uses  $a$  and  $b$  as follows:

- $m_1 = \max\{a, b\}$
- $m_2 = \min\{a, b\}$
- $f\{a, b\}, \{a, b\}Q = \{m_1, m_2\}$

The  $m_1$  and  $m_2$  is the most confusing part of the R-ate pairing.

How much improvement do we get?

Miller-length in iterations		
Tate	$e_r(P, Q)$	377
Ate	$e_t(P, Q)$	254
R-ate	$e_{A,B}(P, Q)$	61

Table: Comparison of miller-loop length for a curve with  $\rho = 4/3$

In this case, we got a Miller length of 1/6 compared to the Tate pairing.

for a  $\text{Log}_2(p) \approx 512$

It has been stated that  $T_i \equiv p^i \pmod r$  and  $A = a.B + b$ . Then,  $T_i = a.T_j + b$ , similarly  $T_j \equiv p^j \pmod r$ . However, it is also possible to use  $(t-1)^i \pmod r$ .

To generate the  $T_i - T_j$  combinations (or  $A, B$  pair) we can follow:

- Define in polynomials  $p^i \pmod r$
- Divide two  $p^i \pmod r$  polynomials
- $a \leftarrow [p(x)^i \pmod r / p(x)^j \pmod r]$
- $b \leftarrow (p(x)^i \pmod r) \pmod (p(x)^j \pmod r)$

However, we must discard trivial combinations, like:  $1.T_1 + x$ . Also, a negative  $a, b$  may lead to inefficient R-ate implementation since it will mean a longer Miller loop.

Now, one can generate the  $T_i - T_j$  combinations, but which one to use? The shortest of course...

The 3 Miller loop calls are:

- $f_{m_2}, m_2 Q \leftarrow M(Q, P, m_2)$
- $f_{c, m_2}, c \cdot m_2 Q \leftarrow M(m_2 \cdot Q, P, c)$
- $f_d, dQ \leftarrow M(Q, P, d)$

You may notice, the 1st and the 3rd are quite similar. One can use the first and get a partial result, but why?

The Miller length is defined as:

- $c \leftarrow \left\lfloor \frac{m_1}{m_2} \right\rfloor$
- $d \leftarrow m_1 - c \cdot m_2$

Just compare  $\text{Log}_2(m_2)$  and  $\text{Log}_2(d)$ . Let's see a few curves.

The parameters of this type of curves is as follows:

- $t(x) = (x^4 + 16x + 7)/7$
- $p(x) = (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21$
- $r(x) = (x^6 + 37x^3 + 343)/343$
- $\rho = 4/3$
- $\omega = 2$
- $p(x)$  and  $r(x)$  represents primes and  $t(x)$  represents integers when  $x \equiv 14 \pmod{42}$

Miller-length in iterations					
A	B	loops	ham	m2	c
3	$x$	23	4	0	23
$5/7 * x$	$1/7 * x^2$	47	6	24	23
$8/7 * x$	$3/7 * x^2$	48	7	25	23
$3/7 * x$	$2/7 * x^2$	48	4	24	24
$5/49 * x^2$	$3/49 * x^2$	47	5	47	0
$5/49 * x^2$	$8/49 * x^2$	48	2	48	0
$5/14 * x$	$3/14 * x^2$	47	6	23	24
$8/49 * x^2$	$3/49 * x^2$	47	5	47	0
$4/7 * x$	$1/7 * x^2$	47	6	24	23
$3/7 * x$	$2/7 * x$	23	4	23	0

Table: BN Curves A,B parameters

Miller-length in iterations					
A	B	loops	ham	m2	c
$2/7 * x$	$3/7 * x$	23	4	23	0
$3/14 * x$	$1/14 * x^2$	46	8	23	23
$8/49 * x^2$	$5/49 * x^2$	48	2	48	0
$3/49 * x^2$	$8/49 * x^2$	47	5	47	0
$3/49 * x^2$	$5/49 * x^2$	47	5	47	0

Table: BN Curves A,B parameters

The parameters of this type of curves is as follows:

- $t(x) = (2x^7 + 757x + 259)/259$
- $p(x) = (x^{14} - 4x^{13} + 7x^{12} + 683x^8 - 2510x^7 + 4781x^6 + 117649x^2 - 386569x + 823543)/28749$
- $r(x) = (x^{12} + 683x^6 + 117649)/161061481$
- $\rho = 7/6$
- $\omega = 2$
- $p(x)$  and  $r(x)$  represents primes and  $t(x)$  represents integers when  $x \equiv 777 \pmod{287}$

The parameters of this type of curves is as follows:

- $t(x) = 6x^2 + 1$
- $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$
- $n(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$
- $\rho = 1$

Miller-length in iterations					
A	B	loops	ham	m2	c
$6x + 3$	$6x + 1$	60	4	60	0
$6x + 4$	$12x + 3$	60	4	60	0
$6x + 3$	$6x + 2$	60	4	60	0
$6x + 5$	$12x + 3$	60	4	60	0

Table: BN Curves A,B parameters

Yes, we may find a combination of parameters with a similar number of loops than the shortest one that bring us less additions. Also, maybe we can exploit some parallel computation: look combination  $5/14 * x - 3/14 * x^2$ , seems promising

Unfortunately, we haven't found any yet... ;(

20 / 20

Luis J  
Dominguez P

Pairings

Introduction  
Tate pairing  
ate pairing

R-ate pairing

Introduction  
TITj

R-ate  
parameters

k=18  
k=36  
BN

Conclusion

Questions?