A Remark on Implementing the Weil Pairing

Cheol Min Park[1⋆], Myung Hwan Kim[1] and Moti Yung[2]

[1] ISaC and Department of Mathematical Sciences,
Seoul National University, Korea
{mpcm,mhkim}@math.snu.ac.kr
[2] Department of Computer Science,
Columbia University, USA
moti@cs.columbia.edu

Abstract. We propose an improved implementation of modified Weil pairings. By reduction of operations in the extension field to those in the base field, we can save some operations in the extension field when computing a modified Weil pairing. In particular, computing $e_\ell(P, \phi(P))$ is the same as computing the Tate pairing without the final powering. So we can save about 50% of time for computing $e_\ell(P, \phi(P))$ compared with the standard Miller's algorithm.

keywords : pairing-based cryptosystem, Weil pairing, modified Weil pairing, separable endomorphism, distortion map

1 Introduction

Since Joux [16] proposed the one-round tripartite Diffie-Hellman protocol using pairings in 2000, a great deal of work on pairing-based cryptography has been done. An excellent reference to those work is Barreto's 'Pairing-Based Crypto Lounge' [3]. Due to the fact that pairings are now prevalent and applicable to many aspects of cryptography, it becomes important to implement pairings efficiently. The main strength of the Weil and the Tate pairings in cryptography is their bilinearity. In many cryptographic applications, however, another strong property, called non-degeneracy, is required. But the Weil and Tate pairings are trivial when applied to two dependent points. This problem can be solved using distortion maps, suggested by Verheul [25]. The pairings with distortion maps are called *modified pairings*.

Modified pairings are used in most pairing-based cryptography : tripartite Diffie-Hellman [16], identity-based encryption [5], identity-based signatures [9],[15], [22] ; short signatures [6, 27], identity-based chameleon hash [26], identification scheme [18], and so on. In particular, many pairing-based cryptographic applications require to compute special values of modified Weil pairing, namely, $e(P, \phi(P))$'s. See [15],[22],[18],[26],[27].

⋆ Part of this work was done while the first author was visiting Columbia University in 2004.

The methods that are employed in cryptography till now are the Weil and the Tate pairing algorithms whose implementations require quite extensive computations. To date, there are a few papers about implementing the Weil and Tate pairings. For examples,

- Miller's algorithm [21]
- Galbraith et al. on implementing the Tate pairing [14, 2]
- Barreto et al. on computing the Tate pairing [1, 2]
- Eisenträger et al. on improved Weil pairing evaluation [10] and on the squared Weil and Tate pairings [11]

Most works focused on speeding up the computation of the Tate pairing because the Weil pairing is more time-consuming. We need two Miller steps for computing the Weil pairing while computing the Tate pairing requires only one Miller step. One Miller step is called the Miller lite part and the other Miller step is called the full Miller part[24]. By comparing the exponentiation of the Tate pairing with the computation of the full Miller part, one can see a proper power of the Weil pairing can be computed faster than the Tate pairing at high security levels [19].

Our contribution : In this paper, we present an improved implementation of modified Weil pairings using distortion maps. When computing $e_\ell(P, \phi(Q))$, the full Miller part becomes the same as the Miller lite part. In particular, when computing $e_\ell(P, \phi(P))$, we just need to evaluate the Miller lite part. Computing $e_\ell(P, \phi(P))$ is the same as computing the Tate pairing without the final powering. So, we can save about 50% of time for computing $e_\ell(P, \phi(P))$ compared with the standard Miller's algorithm.

Outline of the paper : In Section 2, we review the definitions and basic properties of the Weil pairing and modified Weil pairings. In Section 3, we give definitions, propositions and examples of injective, separable distortion maps. In Section 4, we propose our methods computing general values and special values of a modified Weil pairing. Finally we conclude in Section 5.

2 The Weil pairing and modified Weil pairings

2.1 The Weil pairing

Let $\mathbb{F}_q$ denote the finite field containing q elements, where q is a prime power, and $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. An *elliptic curve* $E(\mathbb{F}_q)$ is the set of all solutions (x, y) over $\mathbb{F}_q$ to an equation

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

where $a_i \in \mathbb{F}_q$ for all i, together with the point at infinity O.

A *divisor* D on $E(\overline{\mathbb{F}}_q)$ is a finite linear combination of symbols (P) with integer coefficients:

$$D = \sum_{P \in E(\overline{\mathbb{F}}_q)} n_P(P) \ , \ n_P \in \mathbb{Z}.$$

The set $Div(E)$ of divisors is the free abelian group generated by the symbols (P). The *support* of a divisor $D = \sum_P n_P(P)$ is the set of points P with $n_P \neq O$. Let f be a nonzero rational function on $E(\overline{\mathbb{F}}_q)$. The *divisor* of a function f is

$$div(f) = \sum_P ord_P(f)(P),$$

where $ord_P(f) \in \mathbb{Z}$ is the order of zero or pole of f at P. Given a divisor $D = \sum_P n_P(P)$, we define

$$f(D) = \prod_P f(P)^{n_P}$$

For two divisors $D_1, D_2 \in Div(E)$, we say that D_1 and D_2 are *equivalent* (write $D_1 \sim D_2$) if $D_1 - D_2 = div(f)$ for some rational function f. The relation $\sim$ is an equivalence relation on $Div(E)$.

Let ℓ be a positive integer which is prime to $p = char(\mathbb{F}_q)$ and

$$E[\ell] = \{P \in E(\overline{\mathbb{F}}_q) | \ell P = O\}.$$

For $P, Q \in E[\ell]$, let A_P and A_Q be divisors which are equivalent to $(P) - (O)$ and $(Q) - (O)$, respectively, and have disjoint support. Then there exist rational functions f_{A_P} and f_{A_Q} such that $div(f_{A_P}) = \ell A_P$ and $div(f_{A_Q}) = \ell A_Q$. The Weil pairing of order ℓ is the map

$$e_\ell : E[\ell] \times E[\ell] \longrightarrow \mu_\ell$$

defined by

$$e_\ell(P, Q) = \frac{f_{A_P}(A_Q)}{f_{A_Q}(A_P)},$$

where μ_ℓ is the set of ℓ-th roots of unity.

2.2 Modified Weil pairings

Let $P \in E[\ell]$. Then the value of $e_\ell(P, P)$ is 1. If the point P and Q are linearly dependent, the value of $e_\ell(P, Q)$ is still 1 by the bilinearity of the Weil pairing. In many cryptographical applications, this causes some trouble. We can avoid this trouble using distortion maps of Verheul. A *distortion map* ϕ with respect to the point $P \in E(\mathbb{F}_q)$ is an endomorphism that maps P to $\phi(P) \in E(\mathbb{F}_{q^k})$ for some k which is linearly independent from P. By [25], distortion maps always exist on supersingular curves with only a finite number of exceptions but not on most

non-supersingular curves. Examples of distortion maps on supersingular curves are given in [17]. With respect to a distortion map ϕ, we define a modified Weil pairing $\hat{e}_\ell$ as follows:

$$\hat{e}_\ell(P, Q) = e_\ell(P, \phi(Q)).$$

Note that with a given point P, one can obtain a pair $(P, \phi(P))$ of points that are linearly independent. In many pairing-based cryptographic settings, a modified Weil pairing is defined on $G \times G$, where G is a cyclic group $\langle P \rangle$.

2.3 Miller's algorithm

The main part of computing the Weil/Tate pairing is to find the rational function f_{A_P} and evaluate $f_{A_P}(A_Q)$. We need to evaluate $f_{A_P}(A_Q)$ and $f_{A_Q}(A_P)$ for computing the Weil pairing. The evaluation of $f_{A_P}(A_Q)$, is called Miller lite part and the evaluation of $f_{A_Q}(A_P)$, is called the full Miller part. Let $g_{U,V}$ be the line passing through points $U, V \in E$ and g_U be the vertical line passing through points $U, -U$.

Theorem 1 *(Miller's formula) Let P be a point on elliptic curve and f_c be a rational function with divisor $(f_c) = c(P) - (cP) - (c-1)(O), c \in \mathbb{Z}$. For all $a, b \in \mathbb{Z}$ and $Q \in E$,*

$$f_{a+b}(Q) = f_a(Q) \cdot f_b(Q) \cdot g_{aP,bP}(Q)/g_{(a+b)P}(Q)$$

If $P \in E[\ell]$ and we choose $A_P = (P) - (O)$, then $f_{A_P} = f_l$. Hence we can compute the Weil pairing by combining the above formulas with the double-and-add method to compute lP. Note that if $P \in E(\mathbb{F}_q)$, then f_{A_P} is a rational function over the base field $\mathbb{F}_q$ and if $P \in E(\mathbb{F}_{q^k})$, then f_{A_P} is a rational function over the extension field $\mathbb{F}_{q^k}$. Since $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$, the full Miller part is more time-consuming than the Miller lite part.

3 Injective and separable distortion maps

Before we propose our methods computing modified Weil pairings, we need several definitions and propositions. Many of them are from [7].

3.1 A separable endomorphism

Let ϕ be an endomorphism and $P \in E(\mathbb{F}_q)$.

Definition 1. *The ramification index of ϕ at P is $e_\phi(P) = ord_P(u \circ \phi)$, where u is a uniformizing variable at $\phi(P)$.*

For the definition of the uniformizing variable, we refer the readers to [7]. It is well known that the values of $e_\phi(P)$ remains the same for all $P \in E(\mathbb{F}_q)$. We call this value the *ramification index* of ϕ, denoted by e_ϕ.

Definition 2. *For an endomorphism ϕ, we define $\phi^* : Div(E) \to Div(E)$ to be the homomorphism satisfying*

$$\phi^*((Q)) = \sum_{\phi(P)=Q} e_\phi(P).$$

Definition 3. *An endomorphism ϕ is called separable if $e_\phi = 1$, and inseparable if $e_\phi > 1$.*

Proposition 1. *Assume that ϕ is an endomorphism and that r is a nonzero rational function. Then*

$$div(r \circ \phi) = \phi^*(div(r))$$

Proof. See Proposition 11.9 of [7] or proposition 3.6(b) of [23].

¿From this proposition, we obtain the following.

Proposition 2. *Let $Q = \phi(P)$ and*

$$div(f_P) = \ell(P) - \ell(O) \quad div(f_Q) = \ell(Q) - \ell(O).$$

If ϕ is injective and separable, then

$$div(f_P) = div(f_Q \circ \phi).$$

Proof. By Proposition 1, the definition of ϕ^*, and the injectivity and separability of ϕ, we have

$$\begin{aligned} div(f_Q \circ \phi) &= \phi^*(div f_Q) \\ &= \phi^*(\ell(Q) - \ell(O)) \\ &= \ell\phi^*(Q) - \ell\phi^*(O) \\ &= \ell\left(\textstyle\sum_{\phi(X)=Q} e_\phi(X)\right) - \ell\left(\textstyle\sum_{\phi(Y)=O} e_\phi(Y)\right) \\ &= \ell(P) - \ell(O) \\ &= div(f_p). \end{aligned}$$

3.2 Examples of injective separable distortion maps

The following proposition helps finding injective separable distortion maps that are necessary in our algorithm.

Proposition 3. *An endomorphism ϕ is inseparable if and only if*

$$\phi(x, y) = (u(x^p, y^p), v(x^p, y^p))$$

for some rational functions u and v, where p is the characteristic of $\mathbb{F}_q$.

Proof. See Corollary 12.10 of [7].

Char.	Ext. Deg. ($q = p^m$)	Curve	Emb. Deg	ϕ
$p = 2$	Odd m	$y^2 + y = x^3$	2	ϕ_1
$p = 2$	$m \equiv \pm 1(8)$ $m \equiv \pm 3(8)$	$y^2 + y = x^3 + x + b$	4	ϕ_2
$p = 3$	$m \equiv \pm 1(12)$ $m \equiv \pm 5(12)$	$y^2 = x^3 + 2x + 1$	6	ϕ_3
$p = 3$	$m \equiv \pm 1(12)$ $m \equiv \pm 5(12)$	$y^2 = x^3 + 2x - 1$	6	ϕ_4
$p > 3$ ($p \equiv 2(3)$)	$m = 1$	$y^2 = x^3 + a$	2	ϕ_5
$p > 3$ ($p \equiv 3(4)$)	$m = 1$	$y^2 = x^3 + ax$	2	ϕ_6

Table 1. Examples of distortion maps

The following are examples of injective separable distortion maps.

$$
\begin{aligned}
&\phi_1(x, y) = (\zeta x, y), && \text{where } \zeta^2 + \zeta + 1 = 0\\
&\phi_2(x, y) = (x + s^2, y + sx + t), && \text{where } s^4 + s = 0,\ t^2 + t + s^6 + s^2 = 0\\
&\phi_3(x, y) = (-x + r, iy), && \text{where } r^3 + 2r + 2 = 0,\ i^2 + 1 = 0\\
&\phi_4(x, y) = (-x + r, iy), && \text{where } r^3 + 2r - 2 = 0,\ i^2 + 1 = 0\\
&\phi_5(x, y) = (\zeta x, y), && \text{where } \zeta^2 + \zeta + 1 = 0\\
&\phi_6(x, y) = (-x, iy), && \text{where } i^2 + 1 = 0.
\end{aligned}
$$

It can be easily checked that these distortion maps are indeed injective and separable by Proposition 3. Note that ϕ_1 is used in [5].

4 Computation of modified Weil pairings

In this section, we propose a method of computing modified Weil pairings more efficiently than existing algorithms.

4.1 Computing $e_\ell(P, \phi(Q))$

Before we apply our algorithm to the Weil pairing, we need a new definition of the Weil pairing.

Proposition 4. *Let D_P and D_Q be divisors $(P) - (O)$ and $(Q) - (O)$, respectively, and f_P, f_Q be rational functions such that $div(f_P) = \ell D_P$, $div(f_Q) =$*

ℓD_Q. *Then for random point* R,

$$e_\ell(P,Q) = \frac{f_P(Q+R)}{f_P(R)}\frac{f_Q(-R)}{f_Q(P-R)}.$$

Proof. Let $A_P = (P+S_1)-(S_1)$ and $A_Q = (Q+S_2)-(S_2)$ which have disjoint supports, where S_1 and S_2 are points of the underlying elliptic curve. Then

$$e_\ell(P,Q) = \frac{f_{A_P}(Q+S_2)}{f_{A_P}(S_2)}\frac{f_{A_Q}(S_1)}{f_{A_Q}(P+S_1)}.$$

Let $g(X) = f_p(X - S_1)$. Then

$$div(g) = \ell(P+S_1) - \ell(S_1) = \ell A_P = div(f_{A_P}).$$

Hence $f_{A_P}(X) = \lambda_1 g(X)$ for some constant λ_1. So

$$\frac{f_{A_P}(Q+S_2)}{f_{A_P}(S_2)} = \frac{\lambda_1 g(Q+S_1)}{\lambda_1 g(S_2)} = \frac{f_P(Q+S_2-S_1)}{f_P(S_2-S_1)}.$$

Similarly,

$$\frac{f_{A_Q}(S_1)}{f_{A_Q}(P+S_1)} = \frac{f_Q(S_1-S_2)}{f_Q(P+S_1-S_2)}.$$

Let $S_2 - S_1 = R$. Then the proposition is followed.

Corollary 2 *For an injective, separable distortion map* ϕ,

$$e_\ell(P,\phi(Q)) = \frac{f_P(\phi(Q)+R)}{f_P(R)}\frac{f_Q(-\phi^{-1}(R))}{f_Q(\phi^{-1}(P-R))}$$

Proof. By proposition 2, $div(f_Q) = div(f_{\phi(Q)} \circ \phi)$. Hence $f_{\phi(Q)} = \lambda f_Q \circ \phi^{-1}$ for some constant λ. If we combine this fact with the result of proposition 4, we can obtain this corollary.

Note that $P, Q \in E(\mathbb{F}_q)$, but $\phi(Q) \in E(\mathbb{F}_{q^k})$. If we apply the above corollary to compute the Weil pairing, we can reduce the full Miller part to the Miller lite part.

4.2 Computing $e_\ell(P, \phi(P))$

Lemma 1. *Given a rational function* $f : E \to F_{q^k}$ *with a pole of order* ℓ *at* O. *Define* $g(X) = \frac{f(-X)}{f(\phi(X))}$ *where* $\phi(X)$ *is a distortion map. Then*

$$g(O) = {c_\phi}^l$$

where c_ϕ *is constant depending on the distortion map and* l *is the order of pairing.*

Proof. This proof is similar to that of Lemma 1 of [11].
Consider the rational function $h(x) = \frac{x(X)}{y(X)}$ which has a zero of order 1 at $X = O$. Since f has a pole of order ℓ at O, the function $f_1 = \frac{f}{h^l}$ has neither a pole nor a zero at $X = O$, so $f_1(O)$ is finite and nonzero. By the same reason, $\psi_\phi(O)$ is finite and nonzero for the rational function $\psi_\phi(X) = \frac{h(-X)}{h(\phi(X))}$. Let $\psi_\phi(O)$ be c_ϕ. Hence $g(X) = \frac{f(-X)}{f(\phi(X))} = \frac{h(-X)^l f_1(-X)}{h(\phi(X))^l f_1(\phi(X))} = \psi_\phi(X)^l \frac{f_1(-X)}{f_1(\phi(X))}$, and $g(O) = {c_\phi}^l$.

In [21], it is claimed that $f_P(O)/f_Q(O) = 1$ if f_P and f_Q are normalized. While this normalization depends on the point P and Q, the constant c_ϕ only depends on the distortion map. So it can be precomputed. For distortion maps in the table 1, we compute the value of c_ϕ in the following lemma .

Lemma 2. $c_{\phi_1} = c_{\phi_5} = -1/\zeta$, $c_{\phi_2} = 1$, $c_{\phi_3} = c_{\phi_4} = c_{\phi_6} = i$

Proof. Since $-(x, y) = (x, -y)$ over the field of the characteristic $p \neq 2$ and $-(x, y) = (x, y + 1)$ over the field of the characteristic 2,

$$\psi_{\phi_1}(X) = \psi_{\phi_5}(X) = \frac{x}{-y} / \frac{\zeta x}{y} = -1/\zeta$$
$$\psi_{\phi_2}(X) = \frac{x}{y+1} / \frac{x + s^2}{y + sx + t} = \frac{xy + sx^2 + tx}{xy + x + s^2 y + s^2}$$
$$\psi_{\phi_3}(X) = \psi_{\phi_4}(X) = \frac{x}{-y} / \frac{-x + r}{iy} = \frac{-ix}{-x + r}$$
$$\psi_{\phi_6}(X) = \frac{x}{-y} / \frac{-x}{iy} = i$$

Hence

$$c_{\phi_1} = c_{\phi_5} = -1/\zeta,\ c_{\phi_2} = 1,\ c_{\phi_3} = c_{\phi_4} = c_{\phi_6} = i.$$

Proposition 5. *Let $Q = \phi(P)$. Then for an injective separable distortion map ϕ,*

$$e_\ell(P, \phi(P)) = {c_\phi}^\ell \frac{f_Q(\phi(Q))}{f_Q(P)} = {c_\phi}^\ell \frac{f_P(Q)}{f_P(\phi^{-1}(P))}.$$

Proof. By proposition 2 and 4,

$$e_\ell(P, \phi(P)) = e_\ell(P, Q) = \frac{(f_Q \circ \phi)(Q + R)}{(f_Q \circ \phi)(R)} \frac{f_Q(-R)}{f_Q(P - R)}$$

We can consider $e_\ell(P, Q)$ as a rational function in the variable R. Then $e_\ell(P, Q)$ only has zeros or poles in the following cases.

$$\{\phi(Q + R) = Q \text{ or } O\}, \{\phi(R) = Q \text{ or } O\}, \{-R = Q \text{ or } O\}, \{P - R = Q \text{ or } O\}$$

Since ϕ is injective and $Q = \phi(P)$, we have

$$R = P - Q, P, -Q, \text{ or } O.$$

But the zeros and poles cancel each other out at each of these points. So the rational function $e_\ell(P,Q)$ has neither zeros nor poles and hence $e_\ell(P,Q)$ must be a constant function. If we choose $R = O$, then

$$\frac{f_Q(-R)}{f_Q(\phi(R))} = {c_\phi}^\ell$$

by Lemma 1. Hence

$$e_\ell(P,\phi(P)) = {c_\phi}^\ell \frac{f_Q(\phi(Q))}{f_Q(P)}.$$

If we apply the proposition 2 again,

$${c_\phi}^\ell \frac{f_Q(\phi(Q))}{f_Q(P)} = {c_\phi}^\ell \frac{f_P(Q)}{f_P(\phi^{-1}(P))}$$

When computing $e_\ell(P,\phi(P))$, therefore, the Weil pairing is the same as the Tate pairing without the final powering. Hence we need only one Miller's algorithm to compute the Weil pairing. Moreover it is possible to make a deterministic Miller's algorithm according to the above result. In Miller's algorithm, $f_P(Q)$ is computed by multiplications of and divisions by $g(Q)$'s, where g's are lines passing through some multiples of P. Since $\{P,\phi(P)\}$ are linearly independent, these lines cannot pass through the point $\phi(P)$ and hence no $g(\phi(P))$'s are zero. Since the same holds when computing $f_Q(\phi(Q))$, no division by zero can occur during the computation of $e_\ell(P,\phi(P))$.

4.3 Analysis of computational savings

The main advantage of computing $f_Q(\phi^{-1}(R))$ instead of $f_{\phi(Q)}(R)$ is that we can replace the point multiplication in the extension field with the point multiplication in the base field. For computing the Weil pairing with order l, we need a point doubling or addition of P and $\phi(Q)$ in the Miller lite and the full Miller part, respectively, until we obtain lP and $l\phi(Q)$. After we double and add point Q, we apply the distortion map to doubling and addition of Q for doubling and addition of $\phi(Q)$. But we can't save multiplication in the extension field F_{q^k} for each step by computing the distortion map. Usually we must calculate one multiplication in the extension field. For distortion map $\phi(x,y) = (x+s^2, y+sx+t)$ which is used in supersingular curve over a field of characteristic 2, one squaring and one multiplication in the extension field are necessary. Hence we can save about $log(l)$ multiplications in the extension field by replacing the full Miller part with the Miller lite part. Another savings are obtained in computing the slope of the $g_{U,V}$. The slope λ of $g_{U,V}$ is $\frac{y(U)-y(V)}{x(U)-x(V)}$ and the tangent line slope is $\frac{3x(U)^2+a}{2y(U)}$ for the elliptic curves $y^2 = x^3 + ax + b$. So we need one inversion for $g_{U,V}$, one squaring and one inversion for $g_{U,U}$. If we compute $f_Q(\phi^{-1}(R))$ instead of $f_{\phi(Q)}(R)$, we can reduce $\frac{3\ell}{2}$ divisions and ℓ squarings in the extension

field to the same number of divisions and squarings in the base field. Finally, the inversion of a distortion map in computing $f_Q(\phi^{-1}(R))$ does not influence the operation count. The computation of the inversion of distortion map is easy. For example, $\phi_1^{-1}(x,y) = (\zeta^2 x, y)$ and $\phi_2^{-1}(x,y) = (x+s^2, y+sx+t+1)$. Moreover $\phi^{-1}(R)$ is evaluated just one time in the Miller's algorithm.
In particular, when computing $e_\ell(P, \phi(P))$, we don't need to evaluate the full Miller part. We reduce two Miller part to one Miller part. Hence we can save 50% of time.

5 Conclusions

In this paper, we proposed an improved implementation of the modified Weil pairings. When computing $e_\ell(P, \phi(Q))$, we can save some operations in the extension field by reduction the full Miller part to the Miller lite part. In [19], there is a comparison between the operation count of the full Miller's part and that of the exponentiation at the end of Tate pairing computation. We can choose the better one according to this comparison. But we must compare the operation counts of the Miller lite part with that of the exponentiation at the end of Tate pairing in case of supersingular curve with distortion map. This means we must reexamine the relative speed of the Tate and Weil pairing computations which is referred as the sixth open problems in [19]. When computing $e_\ell(P, \phi(P))$, the computation of the Weil pairing is the same as that of the Tate pairing without the final powering. So our algorithm saves about 50% of the computation cost compared to Miller's algorithm. Our method can be also applied to any Weil pairing method using a distortion map such as the parabola method[10] and the squared Weil pairing[11].

References

1. P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," Advances in Cryptology – Crypto 2002, Lecture Notes on Computer Science 2442, Springer-Verlag (2002), pp. 354–368.
2. P. S. L. M. Barreto, S. D. Galbraith, C. O'hEigeartaigh and M. Scott, "Efficient Pairing Computation on Supersingular Abelian Varieties," Cryptology ePrint Archive, Report 2004/375.
3. Available from http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html
4. I. Blake, G. Seroussi, N. Smart, "Elliptic Curves in Cryptography," Cambridge University Press, 1999.
5. D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology – Crypto 2001, Lecture Notes on Computer Science 2139, Springer-Verlag (2001), pp. 213–229.
6. D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," Advances in Cryptology – Asiacrypt 2001, Lecture Notes on Computer Science 2248, Springer-Verlag (2002), pp. 514–532.
7. L. S. Charlap, D. P. Robbins, "An elementary introduction to elliptic curves," CRD Expository Report No. 31, December 1988.

8. L. S. Charlap, R. Coley, "An elementary introduction to elliptic curves II," CCR Expository Report No. 34, July 1990.
9. J. C. Cha, J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," Practice and Theory in Public Key Cryptography – PKC 2003, Lecture Notes on Computer Science 2567, Springer-Verlag (2003), pp. 18–30.
10. K. Eisentrager, K. Lauter, P. L. Montgomery, "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," CT-RSA 2003, pp. 343-354.
11. K. Eisentrager, K. Lauter, P. L. Montgomery, "Improved Weil and Tate Pairings for Elliptic and Hyperelliptic Curves," ANTS 2004, pp.169-183.
12. G. Frey, M. Muller, H. Ruck, "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems," IEEE Transactions on Information Theory 45(5) (1999), pp. 1717–1719.
13. S. D. Galbraith, "Supersingular curves in cryptography," Advances in Cryptology – Asiacrypt 2001, Lecture Notes on Computer Science 2248, Springer-Verlag (2002), pp. 495–513.
14. S. D. Galbraith, K. Harrison, D. Soldera, "Implementing the Tate pairing," Algorithmic Number Theory Symposium – ANTS-V, Lecture Notes on Computer Science 2369, Springer-Verlag (2002), pp. 324–337.
15. F. He, "Efficient Identity Based Signature Schemes Based on Pairings," Selected Areas in Cryptography – SAC 2002, Lecture Notes on Computer Science 2595, Springer-Verlag (2003), pp. 310–324.
16. A. Joux, "A one-round protocol for tripartite Diffie-Hellman," Algorithm Number Theory Symposium – ANTS-IV, Lecture Notes on Computer Science 1838, Springer-Verlag (2000), pp. 385–394.
17. A. Joux, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems," Algorithm Number Theory Symposium – ANTS-V, Lecture Notes on Computer Science 2369, Springer-Verlag (2002), pp. 20–32.
18. M. Kim, H. Kim, K. Kim, "A New Identification Scheme based on the Gap Diffie-Hellman Problem," 2002 Symposium on Cryptography and Information Security (SCIS2002), Shirahama, Japan, Jan. 29 – Feb. 1, 2003, vol. 1/2, pp. 349–352.
19. N. Koblitz, A.J. Menezes, "Pairing-Based Cryptography at High Security Levels," Cryptology ePrint Archive, Report 2005/76.
20. A.J. Menezes, "Elliptic Curve Public Key Cryptosystems," Kluwer International Series in Engineering and Computer Science, 1993.
21. V. Miller, "The Weil Pairing, and Its Efficient Calculation," Journal of Cryptology, 17, 2004.
22. K. G. Paterson, "ID-based signatures from pairings on elliptic curves," Electronics Letters 38(18) (2002), pp. 1025–1026.
23. J.H. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.
24. J.Solinas,"ID-based digital signature algorithms," 2003, http://www.cacr.math.uwaterloo.ca/conferences/2003/ecc2003/solinas.pdf.
25. E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," Advances in Cryptology - Eurocrypt 2001, Lecture Notes in Computer Science 2045 (2001), pp. 195-210.
26. F. Zhang, R. Safavi-Naini, W. Susilo, "ID-Based Chameleon Hashes from Bilinear Pairings," Cryptology ePrint Archive, Report 2003/208.
27. F. Zhang, R. Safavi-Naini, W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications," Practice and Theory in Public Key Cryptography – PKC 2004, Singapore(SG), March 2004, Lecture Notes on Computer Science 2947, Springer-Verlag (2004), pp. 277–290.