High-Speed Software Implementation of the Optimal Ate Pairing over Barreto–Naehrig Curves

Jean-Luc Beuchat[1], Jorge E. González-Díaz[2], Shigeo Mitsunari[3],
Eiji Okamoto[1], Francisco Rodríguez-Henríquez[2], and Tadanori Teruya[1]

[1] Graduate School of Systems and Information Engineering, University of Tsukuba,
1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan
[2] Computer Science Department, Centro de Investigación y de Estudios Avanzados
del IPN, Av. Instituto Politécnico Nacional No. 2508, 07300 México City, México
[3] Cybozu Labs, Inc., Akasaka Twin Tower East 15F, 2-17-22 Akasaka, Minato-ku,
Tokyo 107-0052

Abstract. This paper describes the design of a fast software library for the computation of the optimal ate pairing on a Barreto–Naehrig elliptic curve. Our library is able to compute the optimal ate pairing over a 254-bit prime field $\mathbb{F}_p$, in just 2.33 million of clock cycles on a single core of an Intel Core i7 2.8GHz processor, which implies that the pairing computation takes 0.832msec. We are able to achieve this performance by a careful implementation of the base field arithmetic through the usage of the customary Montgomery multiplier for prime fields. The prime field is constructed via the Barreto–Naehrig polynomial parametrization of the prime p given as, $p = 36t^4 + 36t^3 + 24t^2 + 6t + 1$, with $t = 2^{62} - 2^{54} + 2^{44}$. This selection of t allows us to obtain important savings for both the Miller loop as well as the final exponentiation steps of the optimal ate pairing.

Keywords: Tate pairing, optimal pairing, Barreto–Naehrig curve, ordinary curve, finite field arithmetic, bilinear pairing software implementation.

1 Introduction

The protocol solutions provided by pairing-based cryptography can only be made practical if one can efficiently compute bilinear pairings at high levels of security. Back in 1986, Victor Miller proposed in [26, 27] an iterative algorithm that can evaluate rational functions from scalar multiplications of divisors, thus allowing to compute bilinear pairings at a linear complexity cost with respect to the size of the input. Since then, several authors have found further algorithmic improvements to decrease the complexity of Miller's algorithm by reducing its loop length [3, 4, 12, 20, 21, 38], and by constructing pairing-friendly elliptic curves [5, 14, 29] and pairing-friendly tower extensions of finite fields [6, 24].

M. Joye, A. Miyaji, and A. Otsuka (Eds.): Pairing 2010, LNCS 6487, pp. 21–39, 2010.

Roughly speaking, an asymmetric bilinear pairing can be defined as the non-degenerate bilinear mapping, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$, where both $\mathbb{G}_1$, $\mathbb{G}_2$ are finite cyclic additive groups with prime order r, whereas $\mathbb{G}_3$ is a multiplicative cyclic group whose order is also r. Additionally, as it was mentioned above, for cryptographic applications it is desirable that pairings can be computed efficiently. When $\mathbb{G}_1 = \mathbb{G}_2$, we say that the pairing is symmetric, otherwise, if $\mathbb{G}_1 \neq \mathbb{G}_2$, the pairing is asymmetric [15].

Arguably the η_T pairing [3] is the most efficient algorithm for symmetric pairings that are always defined over supersingular curves. In the case of asymmetric pairings, recent breakthroughs include the ate pairing [21], the R-ate pairing [25], and the optimal ate pairing [38].

Several authors have presented software implementations of bilinear pairings targeting the 128-bit security level [1,8,10,16,18,23,31,32]. By taking advantage of the eight cores of a dual quad-core Intel Xeon 45nm, the software library presented in [1] takes 3.02 millions of cycles to compute the η_T pairing on a supersingular curve defined over $\mathbb{F}_{2^{1223}}$. Authors in [8] report 5.42 millions of cycles to compute the η_T pairing on a supersingular curve defined over $\mathbb{F}_{3^{509}}$ on an Intel Core i7 45nm processor using eight cores. The software library presented in [32] takes 4.470 millions of cycles to compute the optimal ate pairing on a 257-bit BN curve using only one core of an Intel Core 2 Quad Q6600 processor.

This paper addresses the efficient software implementation of asymmetric bilinear pairings at high security levels. We present a library,[1] that performs the optimal ate pairing over a 254-bit Barreto–Naehrig (BN) curve in just 2.33 million of clock cycles on a single core of an Intel i7 2.8GHz processor, which implies that the optimal ate pairing is computed in 0.832msec. To the best of our knowledge, this is the first time that a software or a hardware accelerator reports a high security level pairing computation either symmetric or asymmetric, either on one core or on a multi-core platform, in less than one millisecond. After a careful selection of a pairing-friendly elliptic curve and the tower field (Sections 2 and 3), we describe the computational complexity associated to the execution of the optimal ate pairing (Section 4). Then, we describe our approach to implement arithmetic over the underlying field $\mathbb{F}_p$ and to perform tower field arithmetic (Section 5), and we give benchmarking results of our software library (Section 6).

2 Optimal Ate Pairing over Barreto–Naehrig Curves

Barreto and Naehrig [5] described a method to construct pairing-friendly ordinary elliptic curves over a prime field $\mathbb{F}_p$. Barreto–Naehrig curves (or BN curves) are defined by the equation $E : y^2 = x^3 + b$, where $b \neq 0$. Their embedding degree k is equal to 12. Furthermore, the number of $\mathbb{F}_p$-rational points of E, denoted by r in the following, is a prime. The characteristic p of the prime field, the group order r, and the trace of Frobenius t_r of the curve are parametrized as follows [5]:

[1] An open source code for benchmarking our software library is available at `http://homepage1.nifty.com/herumi/crypt/ate-pairing.html`

$$\begin{aligned} p(t) &= 36t^4 + 36t^3 + 24t^2 + 6t + 1, \\ r(t) &= 36t^4 + 36t^3 + 18t^2 + 6t + 1, \\ t_r(t) &= 6t^2 + 1, \end{aligned} \tag{1}$$

where $t \in \mathbb{Z}$ is an arbitrary integer such that $p = p(t)$ and $r = r(t)$ are both prime numbers. Additionally, t must be large enough to guarantee an adequate security level. For a security level equivalent to AES-128, we should select t such that $\log_2(r(t)) \geq 256$ and $3000 \leq k \cdot \log_2(p(t)) \leq 5000$ [14]. For this to be possible t should have roughly 64 bits.

Let $E[r]$ denote the r-torsion subgroup of E and π_p be the Frobenius endomorphism $\pi_p : E \to E$ given by $\pi_p(x, y) = (x^p, y^p)$. We define $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_p - [1]) = E(\mathbb{F}_p)[r]$, $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_p - [p]) \subseteq E(\mathbb{F}_{p^{12}})[r]$, and $\mathbb{G}_3 = \mu_r \subset \mathbb{F}^*_{p^{12}}$ (*i.e.* the group of r-th roots of unity). Since we work with a BN curve, r is a prime and $\mathbb{G}_1 = E(\mathbb{F}_p)[r] = E(\mathbb{F}_p)$. The optimal ate pairing on the BN curve E is a non-degenerate and bilinear pairing given by the map [30,32,38]:

$$\begin{aligned} a_{\mathrm{opt}} : \mathbb{G}_2 \times \mathbb{G}_1 &\longrightarrow \mathbb{G}_3 \\ (Q, P) &\longmapsto \big(f_{6t+2,Q}(P) \cdot l_{[6t+2]Q,\pi_p(Q)}(P) \cdot \\ &\qquad\qquad l_{[6t+2]Q+\pi_p(Q),-\pi_p^2(Q)}(P)\big)^{\frac{p^{12}-1}{r}}, \end{aligned}$$

where

- $f_{s,Q}$, for $s \in \mathbb{N}$ and $Q \in \mathbb{G}_2$, is a family of normalized $\mathbb{F}_{p^{12}}$-rational functions with divisor $(f_{s,Q}) = s(Q) - ([s]Q) - (s-1)(\mathcal{O})$, where $\mathcal{O}$ denotes the point at infinity.
- l_{Q_1,Q_2} is the equation of the line corresponding to the addition of $Q_1 \in \mathbb{G}_2$ with $Q_2 \in \mathbb{G}_2$.

Algorithm 1 shows how we compute the optimal ate pairing in this work. Our approach can be seen as a signed-digit version of the algorithm utilized in [32], where both point additions and point subtractions are allowed. The Miller loop (lines 3–10) calculates the value of the rational function $f_{6t+2,Q}$ at point P. In lines 11–13 the product of the line functions $l_{[6t+2]Q,\pi_p(Q)}(P) \cdot l_{[6t+2]Q+\pi_p(Q),-\pi_p^2(Q)}(P)$ is multiplied by $f_{6t+2,Q}(P)$. The so-called final exponentiation is computed in line 14. A detailed summary of the computational costs associated to Algorithm 1 can be found in Section 4.

The BN curves admit a sextic twist $E'/\mathbb{F}_{p^2} : y^2 = x^3 + b/\xi$ defined over $\mathbb{F}_{p^2}$, where $\xi \in \mathbb{F}_{p^2}$ is an element that is neither a square nor a cube in $\mathbb{F}_{p^2}$, and that has to be carefully selected such that $r | \#E'(\mathbb{F}_{p^2})$ holds. This means that pairing computations can be restricted to points P and Q' that belong to $E(\mathbb{F}_p)$ and $E'(\mathbb{F}_{p^2})$, respectively, since we can represent the points in $\mathbb{G}_2$ by points on the twist [5,21,38].

3 Tower Extension Field Arithmetic

Since $k = 12 = 2^2 \cdot 3$, the tower extensions can be created using irreducible binomials only. This is because $x^k - \beta$ is irreducible over $\mathbb{F}_p$ provided that $\beta \in \mathbb{F}_p$

Algorithm 1. Optimal ate pairing over Barreto–Naehrig curves.

```
Input: $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$.
Output: $a_{\mathrm{opt}}(Q, P)$.
Write $s = 6t + 2$ as $s = \sum_{i=0}^{L-1} s_i 2^i$, where $s_i \in \{-1, 0, 1\}$;
$T \leftarrow Q$, $f \leftarrow 1$;
for $i = L - 2$ to $0$ do
    $f \leftarrow f^2 \cdot l_{T,T}(P)$; $T \leftarrow 2T$;
    if $s_i = -1$ then
        $f \leftarrow f \cdot l_{T,-Q}(P)$; $T \leftarrow T - Q$;
    else if $s_i = 1$ then
        $f \leftarrow f \cdot l_{T,Q}(P)$; $T \leftarrow T + Q$;
    end if
end for
$Q_1 \leftarrow \pi_p(Q)$; $Q_2 \leftarrow \pi_{p^2}(Q)$;
$f \leftarrow f \cdot l_{T,Q_1}(P)$; $T \leftarrow T + Q_1$;
$f \leftarrow f \cdot l_{T,-Q_2}(P)$; $T \leftarrow T - Q_2$;
$f \leftarrow f^{(p^{12}-1)/r}$;
return $f$;
```

is neither a square nor a cube in $\mathbb{F}_p$ [24]. Hence, the tower extension can be constructed by simply adjoining a cube or square root of such element β and then the cube or square root of the previous root. This process should be repeated until the desired extension of the tower has been reached.

Accordingly, we decided to represent $\mathbb{F}_{p^{12}}$ using the same tower extension of [18], namely, we first construct a quadratic extension, which is followed by a cubic extension and then by a quadratic one, using the following irreducible binomials:

$$\begin{aligned} \mathbb{F}_{p^2} &= \mathbb{F}_p[u]/(u^2 - \beta), \text{ where } \beta = -5, \\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^2}[v]/(v^3 - \xi), \text{ where } \xi = u, \\ \mathbb{F}_{p^{12}} &= \mathbb{F}_{p^6}[w]/(w^2 - v). \end{aligned} \tag{2}$$

We adopted the tower extension of Equation (2), mainly because field elements $f \in \mathbb{F}_{p^{12}}$ can be seen as a quadratic extension of $\mathbb{F}_{p^6}$, and hence they can be represented as $f = g + hw$, with g, $h \in \mathbb{F}_{p^6}$. This towering will help us to exploit the fact that in the hard part of the final exponentiation we will deal with field elements $f \in \mathbb{F}_{p^{12}}$ that become *unitary* [35, 36], *i.e.*, elements that belong to the cyclotomic subgroup $\mathbb{G}_{\Phi_6}(\mathbb{F}_{p^2})$ as defined in [17]. Such elements satisfy, $f^{p^6+1} = 1$, which means that $f^{-1} = f^{p^6} = g - hw$. In other words, inversion of such elements can be accomplished by simple conjugation. This nice feature opens the door for using addition-subtraction chains in the final exponentiation step, which is especially valuable for our binary signed choice of the parameter t. We also stress that our specific t selection permits to use $\xi = u \in \mathbb{F}_p$, which will yield important savings in the arithmetic computational cost as discussed next.

3.1 Computational Costs of the Tower Extension Field Arithmetic

The tower extension arithmetic algorithms used in this work were directly adopted from [18]. Let (a, m, s, i), $(\tilde{a}, \tilde{m}, \tilde{s}, \tilde{i})$, and (A, M, S, I) denote the cost of field addition, multiplication, squaring, and inversion in $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, and $\mathbb{F}_{p^6}$, respectively. From our implementation (see Section 5), we observed experimentally that $m = s = 8a$ and $i = 48.3m$. We summarize the towering arithmetic costs as follows:

- In the field $\mathbb{F}_{p^2}$, we used Karatsuba multiplication and the complex method for squaring, at a cost of 3 and 2 field multiplications in $\mathbb{F}_p$, respectively. Inversion of an element $A = a_0 + a_1 u \in \mathbb{F}_{p^2}$, can be found from the identity, $(a_0 + a_1 u)^{-1} = (a_0 - a_1 u)/(a_0^2 - \beta a_1^2)$. Using once again the Karatsuba method, field multiplication in $\mathbb{F}_{p^6}$ can be computed at a cost of $6\tilde{m}$ plus several addition operations. All these three operations require the multiplication in the base field by the constant coefficient $\beta \in \mathbb{F}_p$ of the irreducible binomial $u^2 - \beta$. We refer to this operation as m_β Additionally, we sometimes need to compute the multiplication of an arbitrary element in $\mathbb{F}_{p^2}$ times the constant $\xi = u \in \mathbb{F}_p$ at a cost of one multiplication by the constant β. We refer to this operation as m_ξ, but it is noticed that the cost of m_ξ is essentially the same of that of m_β.
- Squaring in $\mathbb{F}_{p^6}$ can be computed via the formula derived in [9] at a cost of $2\tilde{m} + 3\tilde{s}$ plus some addition operations. Inversion in the sextic extension can be computed at a cost of $9\tilde{m} + 3\tilde{s} + 4m_\beta + 5\tilde{a} + \tilde{i}$ [34].
- Since our field towering constructed $\mathbb{F}_{p^{12}}$ as a quadratic extension of $\mathbb{F}_{p^6}$, the arithmetic costs of the quadratic extension apply. Hence, a field multiplication, squaring and inversion costs in $\mathbb{F}_{p^{12}}$ are, $3M + 5A$, $2M + 5A$ and $2M + 2S + 2A + I$, respectively. However, if $f \in \mathbb{F}_{p^{12}}$, belongs to the cyclotomic subgroup $\mathbb{G}_{\Phi_6}(\mathbb{F}_{p^2})$, its field squaring f^2 can be reduced to three squarings in $\mathbb{F}_{p^4}$ [17].

Table 1 lists the computational costs of the tower extension field arithmetic in terms of the $\mathbb{F}_{p^2}$ field arithmetic operations, namely, $(\tilde{a}, \tilde{m}, \tilde{s}, \tilde{i})$.

Table 1. Computational costs of the tower extension field arithmetic

Field	Add./Sub.	Mult.	Squaring	Inversion
$\mathbb{F}_{p^2}$	$\tilde{a} = 2a$	$\tilde{m} = 3m + 3a + m_\beta$	$\tilde{s} = 2m + 3a + m_\beta$	$\tilde{i} = 4m + m_\beta$ $+2a + i$
$\mathbb{F}_{p^6}$	$3\tilde{a}$	$6\tilde{m} + 2m_\beta + 15\tilde{a}$	$2\tilde{m} + 3\tilde{s} + 2m_\beta + 8\tilde{a}$	$9\tilde{m} + 3\tilde{s} + 4m_\beta$ $+4\tilde{a} + \tilde{i}$
$\mathbb{F}_{p^{12}}$	$6\tilde{a}$	$18\tilde{m} + 6m_\beta + 60\tilde{a}$	$12\tilde{m} + 4m_\beta + 45\tilde{a}$	$25\tilde{m} + 9\tilde{s} + 12m_\beta$ $+61\tilde{a} + \tilde{i}$
$\mathbb{G}_{\Phi_6}(\mathbb{F}_{p^2})$	$6\tilde{a}$	$18\tilde{m} + 6m_\beta + 60\tilde{a}$	$9\tilde{s} + 4m_\beta$ $+30\tilde{a}$	Conjugation

3.2 Frobenius Operator

Raising an element $f \in \mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[w]/(w^2 - v)$ to the p-power, is an arithmetic operation needed in the final exponentiation (line 14) of the optimal ate pairing (Algorithm 1). We briefly describe in the following how to compute f^p efficiently.

We first remark that the field extension $\mathbb{F}_{p^{12}}$ can be also represented as a sextic extension of the quadratic field, *i.e.*, $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[W]/(W^6 - u)$, with $W = w$. Hence, we can write $f = g + hw \in \mathbb{F}_{p^{12}}$, with g, $h \in \mathbb{F}_{p^6}$ such that, $g = g_0 + g_1 v + g_2 v^2$, $h = h_0 + h_1 v + h_2 v^2$, where $g_i, h_i \in \mathbb{F}_{p^2}$, for $i = 1, 2, 3$. This means that f can be equivalently written as, $f = g + hw = g_0 + h_0 W + g_1 W^2 + h_1 W^3 + g_2 W^4 + h_2 W^5$.

We note that the p-power of an arbitrary element in the quadratic extension field $\mathbb{F}_{p^2}$ can be computed essentially free of cost as follows. Let $b \in \mathbb{F}_{p^2}$ be an arbitrary element that can be represented as $b = b_0 + b_1 u$. Then, $(b)^{p^{2i}} = b$ and $(b)^{p^{2i-1}} = \bar{b}$, with $\bar{b} = b_0 - b_1 u$, for $i \in \mathbb{N}$.

Let $\bar{g}_i$, $\bar{h}_i$, denote the conjugates of g_i, h_i, for $i = 1, 2, 3$ respectively. Then, using the identity $W^p = u^{(p-1)/6} W$, we can write, $(W^i)^p = \gamma_{1,i} W^i$, with $\gamma_{1,i} = u^{i(p-1)/6}$, for $i = 1, \ldots, 5$. From the definitions given above, we can compute f^p as,

$$\begin{aligned} f^p &= \left(g_0 + h_0 W + g_1 W^2 + h_1 W^3 + g_2 W^4 + h_2 W^5\right)^p \\ &= \bar{g}_0 + \bar{h}_0 W^p + \bar{g}_1 W^{2p} + \bar{h}_1 W^{3p} + \bar{g}_2 W^{4p} + \bar{h}_2 W^{5p} \\ &= \bar{g}_0 + \bar{h}_0 \gamma_{1,1} W + \bar{g}_1 \gamma_{1,2} W^2 + \bar{h}_1 \gamma_{1,3} W^3 + \bar{g}_2 \gamma_{1,4} W^4 + \bar{h}_2 \gamma_{1,5} W^5. \end{aligned}$$

The equation above has a computational cost of 5 multiplications in $\mathbb{F}_p$ and 5 conjugations in $\mathbb{F}_{p^2}$. We can follow a similar procedure for computing f^{p^2} and f^{p^3}, which are arithmetic operations required in the hard part of the final exponentiation of Algorithm 1. For that, we must pre-compute and store the per-field constants $\gamma_{1,i} = u^{i \cdot (p-1)/6}$, $\gamma_{2,i} = \gamma_{1,i} \cdot \bar{\gamma}_{1,i}$, and $\gamma_{3,i} = \gamma_{1,i} \cdot \gamma_{2,i}$ for $i = 1, \ldots, 5$.

4 Computational Cost of the Optimal Ate Pairing

In this work we considered several choices of the parameter t, required for defining $p(t)$, $r(t)$, and $t_r(t)$ of Equation (1). We found 64-bit values of t with Hamming weight as low as 2 that yield the desired properties for p, r, and t_r. For example, the binomial $t = 2^{63} - 2^{49}$ guarantees that p and r as defined in Equation (1) are both 258-bit prime numbers. However, due to the superior efficiency on its associated base field arithmetic, we decided to use the trinomial $t = 2^{62} - 2^{54} + 2^{44}$, which guarantees that p and r as defined in Equation (1) are 254-bit prime numbers. Since the automorphism group $\mathrm{Aut}(E)$ is a cyclic group of order 6 [30], it is possible to slightly improve Pollard's rho attack and get a speedup of $\sqrt{6}$ [11]. Therefore, we achieve a 126-bit security level with our choice of parameters. The curve equation is $E : Y^2 = X^3 + 5$ and we followed the procedure outlined in [6, 36] in order to find a generator $P = (x_P, y_P) = (1, \sqrt{6})$ for the group $E(\mathbb{F}_p)$, and one generator $Q' = (x_{Q'}, y_{Q'})$ for the group $E'(\mathbb{F}_{p^2})[r]$, given as,

$$\begin{aligned}x_{Q'} &= \mathrm{0x}19B0BEA4AFE4C330DA93CC3533DA38A9F430B471C6F8A536E81962ED967909B5\\ &\quad + \mathrm{0x}A1CF585585A61C6E9880B1F2A5C539F7D906FFF238FA6341E1DE1A2E45C3F72u,\\ y_{Q'} &= \mathrm{0x}17ABD366EBBD65333E49C711A80A0CF6D24ADF1B9B3990EEDCC91731384D2627\\ &\quad + \mathrm{0x}EE97D6DE9902A27D00E952232A78700863BC9AA9BE960C32F5BF9FD0A32D345u.\end{aligned}$$

In this Section, we show that our selection of t yields important savings in the Miller loop and the hard part of the final exponentiation step of Algorithm 1.

4.1 Miller Loop

We remark that the parameter $6t + 2$ of Algorithm 1 has a bitlength $L = 65$, with a Hamming weight of 7. This implies that the execution of the Miller loop requires 64 doubling step computations in line 4, and 6 addition/subtraction steps in lines 6 and 8.

It is noted that the equation of the tangent line at $T \in \mathbb{G}_2$ evaluated at P defines a sparse element in $\mathbb{F}_{p^{12}}$ (half of the coefficients are equal to zero). The same observation holds for the equation of the line through the points T and $\pm Q$ evaluated at P. This sparsity allows us to reduce the number of operations on the underlying field when performing accumulation steps (lines 4, 6, 8, 12, and 13 of Algorithm 1).

We perform an interleaved computation of the tangent line at point T (respectively, the line through the points T and Q) evaluated at the base point P, with a point doubling (respectively, point addition) using the formulae given in [2]. We recall that the field extension $\mathbb{F}_{p^{12}}$ can be also represented as, $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[W]/(W^6 - u)$, with $W = w$.

Doubling step (line 4). We represent the point $T \in E'(\mathbb{F}_{p^2})$ in Jacobian coordinates as $T = (X_T, Y_T, Z_T)$. The formulae for doubling T, *i.e.*, the equations that define the point $R = 2T = (X_R, Y_R, Z_R)$ are,

$$X_R = 9X_T^4 - 8X_TY_T^2,\ Y_R = 3X_T^2(4X_TY_T^2 - X_R) - 8Y_T^4,\ Z_R = 2Y_TZ_T.$$

Let the point $P \in E(\mathbb{F}_p)$ be represented in affine coordinates as $P = (x_P, y_P)$. Then, the tangent line at T evaluated at P can be calculated as [32],

$$l_{T,T}(P) = 2Z_RZ_T^2y_P\ -\ (6X_T^2Z_T^2x_P)W\ +\ (6X_T^3 - 4Y_T^2)W^2 \in \mathbb{F}_{p^{12}}.$$

Hence, the computational cost of the interleaving computation of the tangent line and the doubling of the point T is, $3\tilde{m} + 8\tilde{s} + 16\tilde{a} + 4m$. Other operations included in line 4 are f^2 and the product $f^2 \cdot l_{T,T}(P)$, which can be computed at a cost of, $12\tilde{m} + 45\tilde{a} + 4m_\beta$ and $13\tilde{m} + 39\tilde{a} + 2m_\beta$, respectively. In summary, the computational cost associated to line 4 of Algorithm 1 is given as, $28\tilde{m} + 8\tilde{s} + 100\tilde{a} + 4m + 6m_\beta$.

Addition step (lines 6 and 8). Let $Q = (X_Q, Y_Q, Z_Q)$ and $T = (X_T, Y_T, Z_T)$ represent the points Q and $T \in E'(\mathbb{F}_{p^2})$ in Jacobian coordinates. Then the point $R = T + Q = (X_R, Y_R, Z_R)$, can be computed as,

$$\begin{aligned}X_R &= (2Y_QZ_T^3 - 2Y_T)^2 - 4(X_QZ_T^2 - X_T)^3 - 8(X_QZ_T^2 - X_T)^2X_T,\\ Y_R &= (2Y_QZ_T^3 - 2Y_T)(4(X_QZ_T^2 - X_T)^2X_T - X_R) - 8Y_T(X_QZ_T^2 - X_T)^3,\\ Z_R &= 2Z_T(X_QZ_T^2 - X_T).\end{aligned}$$

Once again, let the point $P \in E(\mathbb{F}_p)$ be represented in affine coordinates as $P = (x_P, y_P)$. Then, the line through T and Q evaluated at the point P is given as,

$$l_{T,Q}(P) = 2Z_Ry_P - 4x_P(Y_QZ_T^3 + Y_T)W + (4X_Q(Y_QZ_T^3X_Q - Y_T) - 2Y_QZ_R)W^2 \in \mathbb{F}_{p^{12}}.$$

The combined cost of computing $l_{T,Q}(P)$ and the point addition $R = T + Q$ is, $7\tilde{m} + 7\tilde{s} + 25\tilde{a} + 4m$. Finally we must accumulate the value of $l_{T,Q}(P)$ by performing the product $f \cdot l_{T,Q}(P)$ at a cost of, $13\tilde{m} + 39\tilde{a} + 2m_\beta$.

Therefore, the computational cost associated to line 6 of Algorithm 1 is given as, $20\tilde{m} + 7\tilde{s} + 64\tilde{a} + 4m + 2m_\beta$. This is the same cost of line 8.

Frobenius application and final addition step (lines 11–13). In this step we add to the value accumulated in $f = f_{6t+2,Q}(P)$, the product of the lines through the points $Q_1, -Q_2 \in E'(\mathbb{F}_{p^2})$, namely, $l_{[6t+2]Q,Q_1}(P) \cdot l_{[6t+2]Q+Q_1,-Q_2}(P)$.

The points Q_1, Q_2 can be found by applying the Frobenius operator as, $Q_1 = \pi_p(Q)$, $Q_2 = \pi_p^2(Q)$. The total cost of computing lines 11–13 is given as, $40\tilde{m} + 14\tilde{s} + 128\tilde{a} + 4m + 4m_\beta$.

Let us recall that from our selection of t, $6t + 2$ is a 65-bit number with a low Hamming weight of 7.[2] This implies that the Miller loop of the optimal ate pairing can be computed using only 64 point doubling steps and 6 point addition/subtraction steps. Therefore, the total cost of the Miller loop portion of Algorithm 1 is approximately given as,

$$\begin{aligned}\text{Cost of Miller loop} &= 64 \cdot (28\tilde{m} + 8\tilde{s} + 100\tilde{a} + 4m + 6m_\beta) +\\ &\quad 6 \cdot (20\tilde{m} + 7\tilde{s} + 64\tilde{a} + 4m + 2m_\beta) +\\ &\quad 40\tilde{m} + 14\tilde{s} + 128\tilde{a} + 14m + 4m_\beta\\ &= 1952\tilde{m} + 568\tilde{s} + 6912\tilde{a} + 294m + 400m_\beta.\end{aligned}$$

4.2 Final Exponentiation

Line 14 of Algorithm 1 performs the final exponentiation step, by raising $f \in \mathbb{F}_{p^{12}}$ to the power $e = (p^{12} - 1)/r$. We computed the final exponentiation by following the procedure described by Scott *et al.* in [36], where the exponent e is split into three coefficients as,

$$e = \frac{p^{12} - 1}{r} = (p^6 - 1) \cdot (p^2 + 1) \cdot \frac{p^4 - p^2 + 1}{r}. \tag{3}$$

[2] We note that in the binary signed representation with digit set $\{-1, 0, 1\}$, the integers $t = 2^{62} - 2^{54} + 2^{44}$ and $6t + 2 = 2^{64} + 2^{63} - 2^{56} - 2^{55} + 2^{46} + 2^{45} + 2$ have a signed bitlength of 63 and 65, respectively.

As it was discussed in Section 3, we can take advantage of the fact that raising f to the power p^6 is equivalent to one conjugation. Hence, one can compute $f^{(p^6-1)} = \bar{f} \cdot f^{-1}$, which costs one field inversion and one field multiplication in $\mathbb{F}_{p^{12}}$. Moreover, after raising to the power $p^6 - 1$, the resulting field element becomes a member of the cyclotomic subgroup $\mathbb{G}_{\Phi_6}(\mathbb{F}_{p^2})$, which implies that inversion of such elements can be computed by simply conjugation (see Table 1). Furthermore, from the discussion in Section 3.2 raising to the power $p^2 + 1$, can be done with five field multiplications in the base field $\mathbb{F}_p$, plus one field multiplication in $\mathbb{F}_{p^{12}}$. The processing of the third coefficient in Equation (3) is referred as the *hard part* of the final exponentiation, *i.e*, the task of computing $m^{(p^4-p^2+1)/r}$, with $m \in \mathbb{F}_{p^{12}}$. In order to accomplish that, Scott *et al.* described in [36] a clever procedure that requires the calculation of ten temporary values, namely,

$$m^t,\, m^{t^2},\, m^{t^3},\, m^p,\, m^{p^2},\, m^{p^3},\, m^{(tp)},\, m^{(t^2p)},\, m^{(t^3p)},\, m^{(t^2p^2)},$$

which are the building blocks required for constructing a vectorial addition chain whose evaluation yields the final exponentiation f^e, by performing 13 and 4 field multiplication and squaring operations over $\mathbb{F}_{p^{12}}$, respectively.[3] Taking advantage of the Frobenius operator efficiency, the temporary values m^p, m^{p^2}, m^{p^3}, $m^{(tp)}$, $m^{(t^2p)}$, $m^{(t^3p)}$, and $m^{(t^2p^2)}$ can be computed at a cost of just 35 field multiplications over $\mathbb{F}_p$ (see Section 3.2). Therefore, the most costly computation of the hard part of the final exponentiation is the calculation of $m^t, m^{t^2} = (m^t)^t, m^{t^3} = (m^{t^2})^t$. From our choice, $t = 2^{62} - 2^{54} + 2^{44}$, we can compute these three temporary values at a combined cost of $62 \cdot 3 = 186$ cyclotomic squarings plus $2 \cdot 3 = 6$ field multiplications over $\mathbb{F}_{p^{12}}$. This is cheaper than the t selection used in [32] that requires $4 \cdot 3 = 12$ more field multiplications over $\mathbb{F}_{p^{12}}$.

Consulting Table 1, we can approximately estimate the total computational cost associated to the final exponentiation as,

$$\begin{aligned}
\text{F. Exp. cost} &= (25\tilde{m} + 9\tilde{s} + 12m_\beta + 61\tilde{a} + \tilde{i}) + (18\tilde{m} + 6m_\beta + 60\tilde{a}) + \\
&\quad (18\tilde{m} + 6m_\beta + 60\tilde{a}) + 10m + \\
&\quad 13 \cdot (18\tilde{m} + 6m_\beta + 60\tilde{a}) + 4 \cdot (9\tilde{s} + 4m_\beta + 30\tilde{a}) + 70m + \\
&\quad 186 \cdot (9\tilde{s} + 4m_\beta + 30\tilde{a}) + 6 \cdot (18\tilde{m} + 6m_\beta + 60\tilde{a}) \\
&= 403\tilde{m} + 1719\tilde{s} + 7021\tilde{a} + 80m + 898m_\beta + \tilde{i}.
\end{aligned}$$

Table 2 presents a comparison of $\mathbb{F}_{p^2}$ arithmetic operations of our work against the reference pairing software libraries [18, 32]. From Table 2, we observe that our approach saves about 39.5% and 13% $\mathbb{F}_{p^2}$ multiplications when compared against [18] and [32], respectively. We recall that in our work, the cost of the operation m_ξ is essentially the same of that of m_β. This is not the case in [18,32], where the operation m_ξ is considerably more costly than m_β.

[3] We remark that the cost of the field squaring operations is that of the elements in the cyclotomic subgroup $\mathbb{G}_{\Phi_6}(\mathbb{F}_{p^2})$ listed in the last row of Table 1.

Table 2. A Comparison of arithmetic operations required by the computation of the ate pairing variants

		$\tilde{m}$	$\tilde{s}$	$\tilde{a}$	$\tilde{i}$	m_ξ
Hankerson *et al.* [18] R-ate pairing	Miller Loop	2277	356	6712	1	412
	Final Exp.	1616	1197	8977	1	1062
	Total	3893	1553	15689	2	1474
Naehrig *et al.* [32] Optimal ate pairing	Miller Loop	2022	590	7140		410
	Final Exp.	678	1719	7921	1	988
	Total	2700	2309	15061	1	1398
This work Optimal ate pairing	Miller Loop	1952	568	6912		400
	Final Exp.	403	1719	7021	1	898
	Total	2355	2287	13933	1	1298

5 Software Implementation of Field Arithmetic

In this work, we target the x86-64 instruction set [22]. Our software library is written in C++ and can be used on several platforms: 64-bit Windows 7 with Visual Studio 2008 Professional, 64-bit Linux 2.6 and Mac OS X 10.5 with gcc 4.4.1 or later, etc. In order to improve the runtime performance of our pairing library, we made an extensive use of Xbyak [28], a x86/x64 just-in-time assembler for the C++ language.

5.1 Implementation of Prime Field Arithmetic

The x86-64 instruction set has a **mul** operation which multiplies two 64-bit unsigned integers and returns a 128-bit unsigned integer. The execution of this operation takes about 3 cycles on Intel Core i7 and AMD Opteron processors. Compared to previous architectures, the gap between multiplication and addition/subtraction in terms of cycles is much smaller. This means that we have to be careful when selecting algorithms to perform prime field arithmetic: the schoolbook method is for instance faster than Karatsuba multiplication in the case of 256-bit operands.

An element $x \in \mathbb{F}_p$ is represented as $x = (x_3, x_2, x_1, x_0)$, where $x_i, 0 \leq i \leq 3$, are 64-bit integers. The addition and the subtraction over $\mathbb{F}_p$ are performed in a straightforward manner, *i.e.*, we add/subtract the operands followed by reduction into $\mathbb{F}_p$. Multiplication and inversion over $\mathbb{F}_p$ are accomplished according to the well-known Montgomery multiplication and Montgomery inversion algorithms, respectively [19].

5.2 Implementation of Quadratic Extension Field Arithmetic

This section describes our optimizations for some operations over $\mathbb{F}_{p^2}$ defined in Equation (2).

Multiplication. We implemented the multiplication over the quadratic extension field $\mathbb{F}_{p^2}$ using a Montgomery multiplication scheme split into two steps:

1. The straightforward multiplication of two 256-bit integers (producing a 512-bit integer), denoted as, **mul256**.
2. The Montgomery reduction from a 512-bit integer to a 256-bit integer. This operation is denoted by **mod512**.

According to our implementation, **mul256** (resp. **mod512**) contains 16 (resp. 20) **mul** operations and its execution takes about 55 (resp. 100) cycles.

Let $P(u) = u^2 + 5$ be the irreducible binomial defining the quadratic extension $\mathbb{F}_{p^2}$. Let $A, B, C \in \mathbb{F}_{p^2}$ such that, $A = a_0 + a_1 u$, $B = b_0 + b_1 u$, and $C = c_0 + c_1 u = A \cdot B$. Then, $c_0 = a_0 b_0 - 5 a_1 b_1$ and $c_1 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1$. Hence, in order to obtain the field multiplication over the quadratic extension field, we must compute three multiplications over $\mathbb{F}_p$, and it may seem that three **mod512** operations are necessary. However, we can keep the results of the products **mul256**(a_0, b_0), **mul256**(a_1, b_1), and **mul256**$(a_0 + a_1, b_0 + b_1)$ in three temporary 512-bit integer values. Then, we can add or subtract them without reduction, followed by a final call to **mod512** in order to get $c_0, c_1 \in \mathbb{F}_p$. This approach yields the saving of one **mod512** operation as shown in Algorithm 2. We stress that the **addNC**/**subNC** functions in lines 1, 2, 6, and 7 of Algorithm 2, stand for addition/subtraction between 256-bit or 512-bit integers without checking the output carry. We explain next the rationale for using addition/subtraction without output carry check.

The addition $x + y$, and subtraction $x - y$, of two elements x, $y \in \mathbb{F}_p$ include an unpredictable branch check to figure out whether $x + y \geq p$ or $x < y$. This is a costly check that is convenient to avoid as much as possible. Fortunately, our selected prime p satisfies $7p < N$, with $N = 2^{256}$, and the function **mod512** can reduce operands x, whenever, $x < pN$. This implies that we can add up to seven times without performing an output carry check. In line 8, d_0 is equal

Algorithm 2. Optimized multiplication over $\mathbb{F}_{p^2}$.

```
Input: $A$ and $B \in \mathbb{F}_{p^2}$ such that $A = a_0 + a_1 u$ and $B = b_0 + b_1 u$.
Output: $C = A \cdot B \in \mathbb{F}_{p^2}$.
 1. $s \leftarrow \mathbf{addNC}(a_0, a_1)$;
 2. $t \leftarrow \mathbf{addNC}(b_0, b_1)$;
 3. $d_0 \leftarrow \mathbf{mul256}(s, t)$;
 4. $d_1 \leftarrow \mathbf{mul256}(a_0, b_0)$;
 5. $d_2 \leftarrow \mathbf{mul256}(a_1, b_1)$;
 6. $d_0 \leftarrow \mathbf{subNC}(d_0, d_1)$;
 7. $d_0 \leftarrow \mathbf{subNC}(d_0, d_2)$;
 8. $c_1 \leftarrow \mathbf{mod512}(d_0)$;
 9. $d_2 \leftarrow 5 d_2$;
10. $d_1 \leftarrow d_1 - d_2$;
11. $c_0 \leftarrow \mathbf{mod512}(d_1)$;
12. return $C \leftarrow c_0 + c_1 u$;
```

to $(a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1 = a_0b_1 + a_1b_0 < 2p^2 < pN$. Hence, we can use **addNC/subNC** for step 1, 2, 6, and 7. In line 9, we multiply d_2 by the constant value 5, which can be computed with no carry operation. By applying these modifications, we manage to reduce the cost of the field multiplication over $\mathbb{F}_{p^2}$ from about 640 cycles (required by a non-optimized procedure) to just 440 cycles.

In line 10, $d_1 = a_0b_0 - 5a_1b_1$. We perform this operation as a 512-bit integer subtraction with carry operation followed by a **mod512** reduction. Let x be a 512-bit integer such that $x = a_0b_0 - 5a_1b_1$ and let t be a 256-bit integer. The aforementioned carry operation can be accomplished as follows: if $x < 0$, then $t \leftarrow p$, otherwise $t \leftarrow 0$, then $d_1 \leftarrow x + tN$, where this addition operation only uses the 256 most significant bits of x.

Squaring. Algorithm 3 performs field squaring where some carry operations have been reduced, as explained next. Let $A = a_0 + a_1u \in \mathbb{F}_{p^2}$, $C = A^2 = c_0 + c_1u$, and let $x = (a_0 + p - a_1)(a_0 + 5a_1)$. Then $c_0 = x - 4a_0a_1 \bmod p$. However, we observe that $x \leq 2p \cdot 6p = 12p^2 < N^2$ where $N = 2^{256}$. Also we have that,

$$x - 4a_0a_1 \geq a_0(a_0 + 5a_1) - 4a_0a_1 = a_0(a_0 + a_1) \geq 0,$$

which implies,

$$\begin{aligned}\max(x - 4a_0a_1) &= \max(a_0(a_0 + p) + 5a_1(p - a_1)) \\ &< p \cdot 2p + 5(p/2)(p - p/2) < pN.\end{aligned}$$

We conclude that we can safely add/subtract the operands in Algorithm 3 without carry check.

Fast reduction for multiplication by small constant values. The procedures of point doubling/addition and line evaluation in Miller loop, and the

Algorithm 3. Optimized squaring over $\mathbb{F}_{p^2}$.

```
Input: $A \in \mathbb{F}_{p^2}$ such that $A = a_0 + a_1u$.
Output: $C = A^2 \in \mathbb{F}_{p^2}$.
 1. $t \leftarrow$ addNC$(a_1, a_1)$;
 2. $d_1 \leftarrow$ mul256$(t, a_0)$;
 3. $t \leftarrow$ addNC$(a_0, p)$;
 4. $t \leftarrow$ subNC$(t, a_1)$;
 5. $c_1 \leftarrow 5a_1$;
 6. $c_1 \leftarrow$ addNC$(c_1, a_0)$;
 7. $d_0 \leftarrow$ mul256$(t, c_1)$;
 8. $c_1 \leftarrow$ mod512$(d_1)$;
 9. $d_1 \leftarrow$ addNC$(d_1, d_1)$;
10. $d_0 \leftarrow$ subNC$(d_0, d_1)$;
11. $c_0 \leftarrow$ mod512$(d_0)$;
12. return $C \leftarrow c_0 + c_1u$;
```

operations m_ξ, m_β in the tower field arithmetic, involve field multiplications of an arbitrary element $A \in \mathbb{F}_{p^2}$ by small constant values 3, 4, 5, and 8.

We first remark that m_ξ requires the calculation of a field multiplication by the constant u. Given $A = a_0 + a_1 u \in \mathbb{F}_{p^2}$, then $A \cdot u = \beta \cdot a_1 + a_0 u = -5a_1 + a_0 u$. Computing this operation using shift-and-add expressions such as $5n = n + (n \ll 2)$ for $n \in \mathbb{F}_p$ may be tempting as a means to avoid full multiplication calculations. Nevertheless, in our implementation we preferred to compute those multiplication-by-constant operations using the x86-64 **mul** instruction, since the cost in clock cycles of **mul** is almost the same or even a little cheaper than the one associated to the shift-and-add method.

Multiplications by small constant values require the reduction modulo p of an integer x smaller than $8p$. Note that we need five 64-bit registers to store $x = (x_4, x_3, x_2, x_1, x_0)$. However, one can easily see that $x_4 = 0$ or $x_4 = 1$, and then one can prove that x div $2^{253} = (x_4 \ll 3)|(x_3 \gg 61)$. Division by 2^{253} involves only three logical operations and it can be efficiently performed on our target processor. Furthermore, the prime p we selected has the following nice property:

$$(ip) \text{ div } 2^{253} = \begin{cases} i & \text{if } 0 \le i \le 9, \\ i+1 & \text{if } 10 \le i \le 14. \end{cases}$$

Hence, we built a small look-up table p-Tbl defined as follows:

$$p\text{-Tbl}[i] = \begin{cases} ip & \text{if } 0 \le i \le 9, \\ (i-1)p & \text{if } 10 \le i \le 14. \end{cases} \tag{4}$$

We then get $|x - p\text{-Tbl}[x \gg 253]| < p$. Algorithm 4 summarizes how we apply this strategy to perform a modulo p reduction.

Algorithm 4. Fast reduction $x \bmod p$.

Input: $x \in \mathbb{Z}$ such that $0 \le x < 13p$ and represented as $x = (x_4, x_3, x_2, x_1, x_0)$, where $x_i, 0 \le i \le 4$, are 64-bit integers. Let p-Tbl be the precomputed look-up table defined in Equation (4).

Output: $z = x \bmod p$.

```
$q \leftarrow (x_4 \ll 3)|(x_3 \gg 61)$;        $(q \leftarrow \lfloor x/2^{253} \rfloor)$
$z \leftarrow x - p$-Tbl$[q]$;
if $z < 0$ then
    $z \leftarrow z + p$;
end if
return $z$;
```

6 Implementation Results

We list in Table 3 the timings that we achieved on different architectures. Our library is able to evaluate the optimal ate pairing over a 254-bit prime field $\mathbb{F}_p$, in just 2.33 million of clock cycles on a single core of an Intel Core i7 2.8GHz processor, which implies that the pairing computation takes 0.832msec. To our best knowledge, we are the first to compute a cryptographic pairing in less than one millisecond at this level of security on a desktop computer.

According to the second column of Table 3, the costs (in clock cycles) that were measured for the $\mathbb{F}_{p^2}$ arithmetic when implemented in the Core i7 processor are $\tilde{m} = 435$ and $\tilde{s} = 342$. Additionally, we measured $\tilde{a} = 40$, and $\tilde{i} = 7504$. Now, from Table 2, one can see that the predicted computational cost of the optimal ate pairing is given as,

$$\begin{aligned}\text{Opt. ate pairing cost} &= 2355\tilde{m} + 2287\tilde{s} + 13933\tilde{a} + \tilde{i}\\ &= 2355 \cdot 435 + 2287 \cdot 342 + 13933 \cdot 40 + 7504\\ &= 2{,}371{,}403.\end{aligned}$$

We observe that the experimental results presented in Table 3 have a reasonable match with the computational cost prediction given in Section 4.

For comparison purpose, we also report the performance of the software library for BN curves developed by Naehrig *et al.* [32], which is the best software implementation that we know of.[4] Naehrig *et al.* combined several state-of-the art optimization techniques to write a software that is more than twice as fast as the previous reference implementation by Hankerson *et al.* [18]. Perhaps the most original contribution in [32] is the implementation of the arithmetic over the quadratic extension $\mathbb{F}_{p^2}$ based on a tailored use of SIMD floating point instructions. Working in the case of hardware realizations of pairings, Fan *et al.* [13] suggested to take advantage of the polynomial form of $p(t)$ and introduced a new hybrid modular multiplication algorithm. The operands a and $b \in \mathbb{F}_p$ are converted to degree-4 polynomials $a(t)$ and $b(t)$, and multiplied according to Montgomery's algorithm in the polynomial ring. Coefficients of the results must be reduced modulo t. Fan *et al* noticed that, if $t = 2^m + s$, where s is a small constant, this step consists of a multiplication by s instead of a division by t.

Table 4 summarizes the best results published in the open literature since 2007. All the works featured in Table 4, targeted a level of security equivalent to that of AES-128. Aranha *et al.* [1] and Beuchat *et al.* [8] considered supersingular elliptic curves in characteristic 2 and 3, respectively. All other authors worked with ordinary curves.

Several authors studied multi-core implementations of a cryptographic pairing [1, 8, 16]. In the light of the results reported in Table 4, it seems that the acceleration achieved by an n-core implementation is always less than the ideal $n\times$ speedup. This is related to the extra arithmetic operations needed to combine the partial results generated by each core, and the dependencies between the different operations involved in the final exponentiation. The question that arises is therefore: how many cores should be utilized to compute a cryptographic pairing? We believe that the best answer is the one provided by Grabher *et al.*: "if the requirement is for two pairing evaluations, the slightly moronic conclusion

[4] The results on the Core 2 Quad processor are reprinted from [32]. We downloaded the library [33] and made our own experiments on an Opteron platform.

Table 3. Cycle counts of multiplication over $\mathbb{F}_{p^2}$, squaring over $\mathbb{F}_{p^2}$, and optimal ate pairing on different machines

	Our results			
	Core i7[a]	Opteron[b]	Core 2 Duo[c]	Athlon 64 X2[d]
Multiplication over $\mathbb{F}_{p^2}$	435	443	558	473
Squaring over $\mathbb{F}_{p^2}$	342	355	445	376
Miller loop	1,330,000	1,360,000	1,680,000	1,480,000
Final exponentiation	1,000,000	1,040,000	1,270,000	1,081,000
Optimal ate pairing	2,330,000	2,400,000	2,950,000	2,561,000

	dclxvi [32,33]			
	Core i7	Opteron[b]	Core 2 Quad[e]	Athlon 64 X2[d]
Multiplication over $\mathbb{F}_{p^2}$	–	695	693	1714
Squaring over $\mathbb{F}_{p^2}$	–	614	558	1207
Miller loop	–	2,480,000	2,260,000	5,760,000
Final exponentiation	–	2,520,000	2,210,000	5,510,000
Optimal ate pairing	–	5,000,000	4,470,000	11,270,000

[a] Intel Core i7 860 (2.8GHz), Windows 7, Visual Studio 2008 Professional
[b] Quad-Core AMD Opteron 2376 (2.3GHz), Linux 2.6.18, gcc 4.4.1
[c] Intel Core 2 Duo T7100 (1.8GHz), Windows 7, Visual Studio 2008 Professional
[d] Athlon 64 X2 Dual Core 6000+(3GHz), Linux 2.6.23, gcc 4.1.2
[e] Intel Core 2 Quad Q6600 (2394MHz), Linux 2.6.28, gcc 4.3.3

Table 4. A comparison of cycles and timings required by the computation of the ate pairing variants. The frequency is given in GHz and the timings are in milliseconds.

	Algo.	**Architecture**	**Cycles**	**Freq.**	**Calc. time**
Devegili *et al.* [10]	ate	Intel Pentium IV	69,600,000	3.0	23.20
Naehrig *et al.* [31]	ate	Intel Core 2 Duo	29,650,000	2.2	13.50
Grabher *et al.* [16]	ate	Intel Core 2 Duo (1 core)	23,319,673	2.4	9.72
		Intel Core 2 Duo (2 cores)	14,429,439		6.01
Aranha *et al.* [1]	η_T	Intel Xeon 45nm (1 core)	17,400,000	2.0	8.70
		Intel Xeon 45nm (8 cores)	3,020,000		1.51
Beuchat *et al.* [8]	η_T	Intel Core i7 (1 core)	15,138,000	2.9	5.22
		Intel Core i7 (8 cores)	5,423,000		1.87
Hankerson *et al.* [18]	R-ate	Intel Core 2	10,000,000	2.4	4.10
Naehrig *et al.* [32]	a_{opt}	Intel Core 2 Quad Q6600	4,470,000	2.4	1.80
This work	a_{opt}	Intel Core i7	2,330,000	2.8	0.83

is that one can perform one pairing on each core [. . .], doubling the performance versus two sequential invocations of any other method that does not already use multi-core parallelism internally" [16].

7 Conclusion

In this paper we have presented a software library that implements the optimal ate pairing over a Barreto–Naehrig curve at the 126-bit security level. To the best of our knowledge, we are the first to have reported the computation of a bilinear pairing at a level of security roughly equivalent to that of AES-128 in less than one millisecond on a single core of an Intel Core i7 2.8GHz processor. The speedup achieved in this work is a combination of two main factors:

- A careful programming of the underlying field arithmetic based on Montgomery multiplication that allowed us to perform a field multiplication over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ in just 160 and 435 cycles, respectively, when working in an Opteron-based machine. We remark that in contrast with [32], we did not make use of the 128-bit multimedia arithmetic instructions.
- A binary signed selection of the parameter t that allowed us to obtain significant savings in both the Miller loop and the final exponentiation of the optimal ate pairing.

Our selection of t yields a prime $p = p(t)$ that has a bitlength of just 254 bits. This size is slightly below than what Freeman *et al.* [14] recommend for achieving a high security level. If for certain scenarios, it becomes strictly necessary to meet or exceed the 128-bit level of security, we recommend to select $t = 2^{63} - 2^{49}$ that produces a prime $p = p(t)$ with a bitlength of 258 bits. However, we warn the reader that since a 258-bit prime implies that more than four 64-bit register will be required to store field elements, the performance of the arithmetic library will deteriorate.

Consulting the cycle count costs listed in Table 3, one can see that for our implementation the cost of the final exponentiation step is nearly 25% cheaper than that of the Miller loop.

Authors in [13, 32] proposed to exploit the polynomial parametrization of the prime p as a means to speed up the underlying field arithmetic. We performed extensive experiments trying to apply this idea to our particular selection of t with no success. Instead, the customary Montgomery multiplier algorithm appears to achieve a performance that is very hard to beat by other multiplication schemes, whether integer-based or polynomial-based multipliers.

The software library presented in this work computes a bilinear pairing at a high security level at a speed that is faster than the best hardware accelerators published in the open literature (see for instance [7, 13, 23, 37]). We believe that this situation is unrealistic and therefore we will try to design a hardware architecture that can compute 128-bit security bilinear pairing in shorter timings. Our future work will also include a study of the parallelization possibilities on pairing-based protocols that specify the computation of many bilinear pairing during their execution.

Acknowledgements

We thank Michael Naehrig, Ruben Niederhagen, and Peter Schwabe for making their pairing software library [33] freely available for research purposes.

The authors also want to thank Diego Aranha, Paulo S.L.M. Barreto, Darrel Hankerson, Alfred Menezes, and the anonymous referees for their valuable comments.

References

1. Aranha, D.F., López, J., Hankerson, D.: High-speed parallel software implementation of the η_T pairing. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 89–105. Springer, Heidelberg (2010)
2. Arène, C., Lange, T., Naehrig, M., Ritzenthaler, C.: Faster computation of the Tate pairing. Cryptology ePrint Archive, Report 2009/155 (2009), `http://eprint.iacr.org/2009/155.pdf`
3. Barreto, P.S.L.M., Galbraith, S.D., Ó hÉigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular Abelian varieties. Designs, Codes and Cryptography 42, 239–271 (2007)
4. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–368. Springer, Heidelberg (2002)
5. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006)
6. Benger, N., Scott, M.: Constructing tower extensions for the implementation of pairing-based cryptography. Cryptology ePrint Archive, Report 2009/556 (2009), `http://eprint.iacr.org/2009/556.pdf`
7. Beuchat, J.-L., Detrey, J., Estibals, N., Okamoto, E., Rodríguez-Henríquez, F.: Fast architectures for the η_T pairing over small-characteristic supersingular elliptic curves. Cryptology ePrint Archive, Report 2009/398 (2009), `http://eprint.iacr.org/2009/398.pdf`
8. Beuchat, J.-L., López-Trejo, E., Martínez-Ramos, L., Mitsunari, S., Rodríguez-Henríquez, F.: Multi-core implementation of the Tate pairing over supersingular elliptic curves. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009. LNCS, vol. 5888, pp. 413–432. Springer, Heidelberg (2009)
9. Chung, J., Hasan, M.A.: Asymmetric squaring formulae. In: Kornerup, P., Muller, J.-M. (eds.) Proceedings of the 18th IEEE Symposium on Computer Arithmetic, pp. 113–122. IEEE Computer Society, Los Alamitos (2007)
10. Devegili, A.J., Scott, M., Dahab, R.: Implementing cryptographic pairings over Barreto–Naehrig curves. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 197–207. Springer, Heidelberg (2007)
11. Duursma, I., Gaudry, P., Morain, F.: Speeding up the discrete log computation on curves with automorphisms. In: Lam, K.-Y., Okamoto, E., Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 103–121. Springer, Heidelberg (1999)
12. Duursma, I., Lee, H.S.: Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In: Laih, C.S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 111–123. Springer, Heidelberg (2003)
13. Fan, J., Vercauteren, F., Verbauwhede, I.: Faster $\mathbb{F}_p$-arithmetic for cryptographic pairings on Barreto–Naehrig curves. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 240–253. Springer, Heidelberg (2009)
14. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of Cryptology 23(2), 224–280 (2010)

15. Galbraith, S., Paterson, K., Smart, N.: Pairings for cryptographers. Discrete Applied Mathematics 156, 3113–3121 (2008)
16. Grabher, P., Großschädl, J., Page, D.: On software parallel implementation of cryptographic pairings. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 34–49. Springer, Heidelberg (2008)
17. Granger, R., Scott, M.: Faster squaring in the cyclotomic subgroup of sixth degree extensions. Cryptology ePrint Archive, Report 2009/565 (2009), http://eprint.iacr.org/2009/565.pdf
18. Hankerson, D., Menezes, A., Scott, M.: Software implementation of pairings. In: Joye, M., Neven, G. (eds.) Identity-based Cryptography. Cryptology and Information Security Series, ch. 12, pp. 188–206. IOS Press, Amsterdam (2009)
19. Hankerson, D., Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer, New York (2004)
20. Hess, F.: Pairing lattices. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 18–38. Springer, Heidelberg (2008)
21. Hess, F., Smart, N., Vercauteren, F.: The Eta pairing revisited. IEEE Transactions on Information Theory 52(10), 4595–4602 (2006)
22. Intel Corporation. Intel 64 and IA-32 Architectures Software Developer's Manuals, http://www.intel.com/products/processor/manuals/
23. Kammler, D., Zhang, D., Schwabe, P., Scharwaechter, H., Langenberg, M., Auras, D., Ascheid, G., Mathar, R.: Designing an ASIP for cryptographic pairings over Barreto–Naehrig curves. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 254–271. Springer, Heidelberg (2009)
24. Koblitz, N., Menezes, A.: Pairing-based cryptography at high security levels. Cryptology ePrint Archive, Report 2005/076 (2005), http://eprint.iacr.org/2005/076.pdf
25. Lee, E., Lee, H.-S., Park, C.-M.: Efficient and generalized pairing computation on abelian varieties. Cryptology ePrint Archive, Report 2008/040 (2008), http://eprint.iacr.org/2008/040.pdf
26. Miller, V.S.: Short programs for functions on curves (1986), http://crypto.stanford.edu/miller
27. Miller, V.S.: The Weil pairing, and its efficient calculation. Journal of Cryptology 17(4), 235–261 (2004)
28. Mitsunari, S.: Xbyak: JIT assembler for C++, http://homepage1.nifty.com/herumi/soft/xbyak_e.html
29. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundamentals E84, 1234–1243 (2001)
30. Naehrig, M.: Constructive and Computational Aspects of Cryptographic Pairings. PhD thesis, Technische Universiteit Eindhoven (2009), http://www.cryptojedi.org/users/michael/data/thesis/2009-05-13-diss.pdf
31. Naehrig, M., Barreto, P.S.L.M., Schwabe, P.: On compressible pairings and their computation. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 371–388. Springer, Heidelberg (2008)
32. Naehrig, M., Niederhagen, R., Schwabe, P.: New software speed records for cryptographic pairings. Cryptology ePrint Archive, Report 2010/186 (2010), http://eprint.iacr.org/2010/186.pdf
33. Schwabe, P.: Software library of "New software speed records for cryptographic pairings", http://cryptojedi.org/crypto/#dclxvi (accessed June 4, 2010)

34. Scott, M.: Implementing cryptographic pairings. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 177–196. Springer, Heidelberg (2007)
35. Scott, M., Barreto, P.S.L.M.: Compressed pairings. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 140–156. Springer, Heidelberg (2004)
36. Scott, M., Benger, N., Charlemagne, M., Dominguez Perez, L.J., Kachisa, E.J.: On the final exponentiation for calculating pairings on ordinary elliptic curves. Cryptology ePrint Archive, Report 2008/490 (2008), `http://eprint.iacr.org/2008/490.pdf`
37. Shu, C., Kwon, S., Gaj, K.: Reconfigurable computing approach for Tate pairing cryptosystems over binary fields. IEEE Transactions on Computers 58(9), 1221–1237 (2009)
38. Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theory 56(1), 455–461 (2010)