

# A Comparison between Hardware Accelerators for the Modified Tate Pairing over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$

Jean-Luc Beuchat<sup>1</sup>, Nicolas Brisebarre<sup>2</sup>, Jérémie Detrey<sup>3</sup>,  
Eiji Okamoto<sup>1</sup>, and Francisco Rodríguez-Henríquez<sup>4</sup>

<sup>1</sup> Graduate School of Systems and Information Engineering,  
University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan

<sup>2</sup> LIP/Arénaire (CNRS – ENS Lyon – INRIA – UCBL), ENS Lyon,  
46, allée d'Italie, F-69364 Lyon Cedex 07, France

<sup>3</sup> Cospec group, B-IT, Dahlmannstraße 2, D-53113 Bonn, Germany

<sup>4</sup> Computer Science Section, Electrical Engineering Department, Centro de  
Investigación y de Estudios Avanzados del IPN, Av. Instituto Politécnico Nacional  
No. 2508, 07300 México City, México

**Abstract.** In this article we propose a study of the modified Tate pairing in characteristics two and three. Starting from the  $\eta_T$  pairing introduced by Barreto *et al.* [1], we detail various algorithmic improvements in the case of characteristic two. As far as characteristic three is concerned, we refer to the survey by Beuchat *et al.* [5]. We then show how to get back to the modified Tate pairing at almost no extra cost. Finally, we explore the trade-offs involved in the hardware implementation of this pairing for both characteristics two and three. From our experiments, characteristic three appears to have a slight advantage over characteristic two.

**Keywords:** Modified Tate pairing, reduced  $\eta_T$  pairing, finite field arithmetic, elliptic curve, hardware accelerator, FPGA.

## 1 Introduction

Over the past few years, bilinear pairings over elliptic and hyperelliptic curves have been the focus of an ever increasing attention in cryptology. Since their introduction to this domain by Menezes, Okamoto & Vanstone [23] and Frey & Rück [9], and the first discovery of their constructive properties by Mitsunari, Sakai & Kasahara [26], Sakai, Oghishi & Kasahara [31], and Joux [17], a large number of pairing-based cryptographic protocols have already been published. For those reasons, efficient computation of pairings is crucial and, according to the recommendations of [12, 21], the Tate pairing, rather than the Weil pairing, appears to be the most appropriate choice.

Miller [24, 25] proposed in 1986 the first algorithm for iteratively computing the Weil and Tate pairings. In the case of the Tate pairing, a further final exponentiation of the Miller's algorithm result is required to obtain a uniquely defined value. Various improvements were published in [2, 7, 10, 22] and we will

consider in this paper the modified Tate pairing as defined in [2]. Generalizing some results by Duursma & Lee [7], Barreto *et al.* then introduced the  $\eta_T$  pairing [1], in which the number of iterations in Miller’s algorithm is halved. This nondegenerate bilinear pairing can also be used as a tool for computing the modified Tate pairing, at the expense of an additional exponentiation.

General purpose microprocessors are intrinsically not suited for computations on finite fields of small characteristic, hence software implementations are bound to be quite slow and the need for special purpose hardware coprocessors is strong [5, 6, 11, 16, 18, 19, 20, 28, 29, 30, 33]. In this context, we extend here to the characteristic two the results by Beuchat *et al.* [5] in the case of the hardware implementation of the reduced  $\eta_T$  pairing in characteristic three.

In Section 2, we detail the algorithms required to compute the reduced  $\eta_T$  pairing in characteristic two. Some algorithmic improvements in both the pairing computation and the tower-field arithmetic are also presented, and an accurate cost analysis in terms of operations over the base field  $\mathbb{F}_{2^m}$  is given. We then study in Section 3 the relation between the  $\eta_T$  and Tate pairings, and show that the modified Tate pairing can be computed from the reduced  $\eta_T$  pairing at almost no extra cost in characteristics two and three. Section 4 gives hardware implementation results of the modified Tate pairing in both characteristics and for various field extension degrees. Comparisons between  $\mathbb{F}_{2^m}$  and  $\mathbb{F}_{3^m}$  are presented at equivalent levels of security and they show a slight advantage in favor of characteristic three. Finally, some comparisons with already published solutions are also given to attest the meaningfulness of our results. Supplementary material is available in a research report version of this paper [4].

## 2 Computation of the Reduced $\eta_T$ Pairing in Characteristic Two

### 2.1 Preliminary Definitions

We consider the supersingular curve  $E$  over  $\mathbb{F}_{2^m}$  defined by the equation

$$y^2 + y = x^3 + x + b, \tag{1}$$

where  $b \in \{0, 1\}$  and  $m$  is an odd integer. We define  $\delta = b$  when  $m \equiv 1, 7 \pmod{8}$ ; in all other cases,  $\delta = 1 - b$ . The number of rational points of  $E$  over  $\mathbb{F}_{2^m}$  is given by  $N = \#E(\mathbb{F}_{2^m}) = 2^m + 1 + \nu 2^{(m+1)/2}$ , where  $\nu = (-1)^\delta$  [2]. The embedding degree of this curve, which is the least positive integer  $k$  such that  $N$  divides  $2^{km} - 1$ , is 4.

Choosing  $T = 2^m - N$  and a prime  $\ell$  dividing  $N$ , Barreto *et al.* [1] defined the  $\eta_T$  pairing of two points  $P$  and  $Q \in E(\mathbb{F}_{2^m})[\ell]$  as:

$$\eta_T(P, Q) = f_{T', P'}(\psi(Q)),$$

where  $T' = -\nu T$ ,  $P' = [-\nu]P$ , and  $E(\mathbb{F}_{2^m})[\ell]$  denotes the  $\ell$ -torsion subgroup of  $E(\mathbb{F}_{2^m})$ . The distortion map  $\psi$  is defined from  $E(\mathbb{F}_{2^m})[\ell]$  to  $E(\mathbb{F}_{2^{4m}})[\ell]$  as

$$\psi(x, y) = (x + s^2, y + sx + t),$$

for all  $(x, y) \in E(\mathbb{F}_{2^m})[\ell]$  [1]. The elements  $s$  and  $t$  of  $\mathbb{F}_{2^{4m}}$  satisfy  $s^2 = s + 1$  and  $t^2 = t + s$ . This allows for representing  $\mathbb{F}_{2^{4m}}$  as an extension of  $\mathbb{F}_{2^m}$  using the basis  $(1, s, t, st)$ :  $\mathbb{F}_{2^{4m}} = \mathbb{F}_{2^m}[s, t] \cong \mathbb{F}_{2^m}[X, Y]/(X^2 + X + 1, Y^2 + Y + X)$ . Finally,  $f_{T', P'}$  is an element of  $\mathbb{F}_{2^m}(E)$ , where  $\mathbb{F}_{2^m}(E)$  denotes the function field of the curve, and is given by

$$f_{T', P'} : E(\mathbb{F}_{2^{4m}})[\ell] \longrightarrow \mathbb{F}_{2^{4m}}^* \\ \psi(Q) \longmapsto \left( \prod_{i=0}^{\frac{m-1}{2}} g_{[2^i]P'}(\psi(Q))^{2^{\frac{m-1}{2}-i}} \right) l_{P'}(\psi(Q)), \quad (2)$$

where:

- The point doubling formula is given by

$$[2^i]P' = \left( x_{P'}^{2^{2i}} + i, y_{P'}^{2^{2i}} + ix_{P'}^{2^{2i}} + \tau(i) \right),$$

with

$$\tau(i) = \begin{cases} 0 & \text{if } i \equiv 0, 1 \pmod{4}, \\ 1 & \text{otherwise.} \end{cases}$$

- $g_V$ , for all  $V = (x_V, y_V) \in E(\mathbb{F}_{2^m})[\ell]$ , is the rational function defined over  $E(\mathbb{F}_{2^{4m}})[\ell]$  corresponding to the doubling of  $V$ . For all  $(x, y) \in E(\mathbb{F}_{2^{4m}})[\ell]$ , we have  $g_V(x, y) = (x_V^2 + 1)(x_V + x) + y_V + y$  [1]. According to the equation of the elliptic curve (1),  $x_V^3 + x_V + y_V$  is equal to  $y_V^2 + b$  and we obtain [33]:

$$g_V(x, y) = x(x_V^2 + 1) + y_V^2 + y + b. \quad (3)$$

We considered both forms of  $g_V(x, y)$  when studying  $\eta_T$  pairing algorithms over  $\mathbb{F}_{2^m}$  and discovered that the second one always leads to the fastest algorithms.

- $l_V$ , for all  $V = (x_V, y_V) \in E(\mathbb{F}_{2^m})[\ell]$ , is the equation of the line corresponding to the addition of  $\left[2^{\frac{m+1}{2}}\right]V$  with  $[\nu]V$ , and defined for all  $(x, y) \in E(\mathbb{F}_{2^{4m}})[\ell]$  as follows:

$$l_V(x, y) = x_V^2 + (x_V + \alpha)(x + \alpha) + x + y_V + y + \delta + 1 + (x_V + x + 1 - \alpha)s + t, \quad (4)$$

where

$$\alpha = \begin{cases} 0 & \text{if } m \equiv 3 \pmod{4}, \\ 1 & \text{if } m \equiv 1 \pmod{4}. \end{cases}$$

### 2.2 Computation of the $\eta_T$ Pairing in Characteristic Two

Barreto *et al.* suggested reversing the loop to compute the  $\eta_T$  pairing [1]. They introduced the new index  $j = \frac{m-1}{2} - i$  and obtained

$$f_{T', P'}(\psi(Q)) = l_{P'}(\psi(Q)) \prod_{j=0}^{\frac{m-1}{2}} \left( g_{\left[2^{\frac{m-1}{2}-j}\right]P'}(\psi(Q)) \right)^{2^j}.$$

A tedious case-by-case analysis allows one to prove that:

$$\left( g_{\left[2^{\frac{m-1}{2}-j}\right]_{P'}}(\psi(Q)) \right)^{2^j} = (x_{P'}^{2^{-j}} + \alpha) \cdot (x_Q^{2^j} + \alpha) + y_{P'}^{2^{-j}} + y_Q^{2^j} + \beta + (x_{P'}^{2^{-j}} + x_Q^{2^j} + \alpha)s + t,$$

where

$$\beta = \begin{cases} b & \text{if } m \equiv 1, 3 \pmod{8}, \\ 1 - b & \text{if } m \equiv 5, 7 \pmod{8}. \end{cases}$$

This equation differs from the one given by Barreto *et al.* [1]: taking advantage of the second form of  $g_V$  (3), we obtain a slight reduction in the number of additions over  $\mathbb{F}_{2^m}$ .

We suggest a second improvement to save a multiplication over  $\mathbb{F}_{2^m}$ . At first glance multiplying  $l_{P'}(\psi(Q))$  by  $g_{\left[2^{\frac{m-1}{2}}\right]_{P'}}(\psi(Q))$  involves three multiplications over  $\mathbb{F}_{2^m}$ . However, when  $j = 0$ , we have:

$$g_{\left[2^{\frac{m-1}{2}}\right]_{P'}}(\psi(Q)) = (x_{P'} + \alpha)(x_Q + \alpha) + y_{P'} + y_Q + \beta + (x_{P'} + x_Q + \alpha)s + t.$$

Seeing that  $\alpha + \beta = \delta + 1$ , we rewrite  $l_{P'}(\psi(Q))$  as follows:

$$l_{P'}(\psi(Q)) = g_{\left[2^{\frac{m-1}{2}}\right]_{P'}}(\psi(Q)) + x_{P'}^2 + x_Q + \alpha + s.$$

Defining  $g_0 = (x_{P'} + \alpha)(x_Q + \alpha) + y_{P'} + y_Q + \beta$ ,  $g_1 = x_{P'} + x_Q + \alpha$ , and  $g_2 = x_{P'}^2 + x_Q + \alpha$ , we eventually obtain:

$$g_{\left[2^{\frac{m-1}{2}}\right]_{P'}}(\psi(Q)) = g_0 + g_1s + t \quad \text{and} \quad l_{P'}(\psi(Q)) = (g_0 + g_2) + (g_1 + 1)s + t.$$

The product  $l_{P'}(\psi(Q)) \cdot g_{\left[2^{\frac{m-1}{2}}\right]_{P'}}(\psi(Q))$  can be computed by means of two multiplications over  $\mathbb{F}_{2^m}$  (see [4, Appendix D.2]). Algorithm 1 describes the computation of the  $\eta_T$  pairing according to this construction. Addition over  $\mathbb{F}_{2^m}$  involves  $m$  bitwise exclusive-OR operations that can be implemented in parallel. We refer to this operation as addition (A) when we give the cost of an algorithm. However, the addition of an element of  $\mathbb{F}_2$  requires a single exclusive-OR operation, denoted by XOR. Additionally, M denotes multiplications, S squarings and R square roots. We also introduce  $\bar{\delta} = 1 - \delta$ .

The first step consists in computing  $P' = [-\nu]P$  (line 1). Multiplication over  $\mathbb{F}_{2^{4m}}$  usually requires nine multiplications and twenty additions over  $\mathbb{F}_{2^m}$ . However, the sparsity of  $G$  (as given line 13) allows one to compute the product  $F \cdot G$  (line 14) by means of only six multiplications and fourteen additions over  $\mathbb{F}_{2^m}$  (see [4, Appendix D.2] for further details). Contrary to what was suggested by Ronan *et al.* [29], the loop unrolling technique introduced by Granger *et al.* [13]

in the context of the Tate pairing in characteristic three turns out to be useless in our case. Let  $G_j$  and  $G_{j+1}$  denote the values of  $G$  at iterations  $j$  and  $j + 1$ , respectively. Algorithm 1 computes  $(F \cdot G_j) \cdot G_{j+1}$  by means of twelve multiplications and some additions over  $\mathbb{F}_{2^m}$ . The loop unrolling trick consists in taking advantage of the sparsity of  $G_j$  and  $G_{j+1}$ : only three multiplications over  $\mathbb{F}_{2^m}$  are required to compute the product  $G_j \cdot G_{j+1}$ . Unfortunately, the result is not a sparse polynomial, and the multiplication by  $F$  involves nine multiplications over  $\mathbb{F}_{2^m}$ . Thus, computing  $(G_j \cdot G_{j+1}) \cdot F$  instead of  $(F \cdot G_j) \cdot G_{j+1}$  does not decrease the number of multiplications over the underlying field.

---

**Algorithm 1.** Computation of the  $\eta_T$  pairing in characteristic two: reversed-loop approach with square roots.

---

**Input:**  $P, Q \in \mathbb{F}_{2^m}[\ell]$ .

**Output:**  $\eta_T(P, Q) \in \mathbb{F}_{2^{4m}}^*$ .

1.  $y_P \leftarrow y_P + \delta;$  ( $\bar{\delta}$  XOR)
  2.  $u \leftarrow x_P + \alpha; v \leftarrow x_Q + \alpha$  ( $2\alpha$  XOR)
  3.  $g_0 \leftarrow u \cdot v + y_P + y_Q + \beta;$  (1 M, 2 A,  $\beta$  XOR)
  4.  $g_1 \leftarrow u + x_Q; g_2 \leftarrow v + x_P^2;$  (1 S, 2 A)
  5.  $G \leftarrow g_0 + g_1s + t;$
  6.  $L \leftarrow (g_0 + g_2) + (g_1 + 1)s + t;$  (1 A, 1 XOR)
  7.  $F \leftarrow L \cdot G;$  (2 M, 1 S, 5 A, 2 XOR)
  8. **for**  $j = 1$  to  $\frac{m-1}{2}$  **do**
  9.  $x_P \leftarrow \sqrt{x_P}; y_P \leftarrow \sqrt{y_P}; x_Q \leftarrow x_Q^2; y_Q \leftarrow y_Q^2;$  (2 R, 2 S)
  10.  $u \leftarrow x_P + \alpha; v \leftarrow x_Q + \alpha$  ( $2\alpha$  XOR)
  11.  $g_0 \leftarrow u \cdot v + y_P + y_Q + \beta;$  (1 M, 2 A,  $\beta$  XOR)
  12.  $g_1 \leftarrow u + x_Q;$  (1 A)
  13.  $G \leftarrow g_0 + g_1s + t;$
  14.  $F \leftarrow F \cdot G;$  (6 M, 14 A)
  15. **end for**
  16. **return**  $F^M;$
- 

The square roots in Algorithm 1 could be computed according to the technique described by Fong *et al.* [8]. However, this approach would require dedicated hardware and could potentially slow down a pairing coprocessor. Thus, it is attractive to study square-root-free algorithms which allow one to design simpler arithmetic and logic units. Another argument preventing the usage of square roots is that the complexity of their computation heavily depends on the particular irreducible polynomial selected for representing the field  $\mathbb{F}_{2^m}$ . On the other hand, the complexity of squarings is somehow more independent of the irreducible polynomial [27, 32]. To get rid of the square roots, we remark that

$$\eta_T(P, Q) = \eta_T \left( \left[ 2^{-\frac{m-1}{2}} \right] P, Q \right)^{2^{\frac{m-1}{2}}}.$$

Let  $[2^j]Q = (x_{[2^j]Q}, y_{[2^j]Q})$ . Since

$$g_{\left[2^{\frac{m-1}{2}-j}\right]} \left( \left[2^{-\frac{m-1}{2}}\right]_{P'}(\psi(Q)) \right) = g_{[2^{-j}]P'}(\psi(Q)),$$

the  $\eta_T$  pairing is equal to

$$f_{T',P'}(\psi(Q)) = l_{\left[2^{-\frac{m-1}{2}}\right]_{P'}}(\psi(Q))^{2^{\frac{m-1}{2}}} \prod_{j=0}^{\frac{m-1}{2}} \left( (g_{[2^{-j}]P'}(\psi(Q)))^{2^{2j}} \right)^{2^{\frac{m-1}{2}-j}},$$

where

$$\begin{aligned} l_{\left[2^{-\frac{m-1}{2}}\right]_{P'}}(\psi(Q)) &= x_{P'}^2(x_{P'}^2 + x_Q + \alpha) + (\alpha + 1)x_{P'}^2 + y_{P'}^2 + y_Q + \\ &\quad \gamma + \delta + (x_{P'}^2 + x_Q)s + t, \\ (g_{[2^{-j}]P'}(\psi(Q)))^{2^{2j}} &= (x_{P'}^2 + 1) \cdot (x_{[2^j]Q} + 1) + \\ &\quad y_{P'}^2 + y_{[2^j]Q} + b + (x_{P'}^2 + x_{[2^j]Q} + 1)s + t, \end{aligned}$$

and

$$\gamma = \begin{cases} 0 & \text{if } m \equiv 1, 7 \pmod{8}, \\ 1 & \text{if } m \equiv 3, 5 \pmod{8}. \end{cases}$$

Again, one can simplify the computation of the product  $l_{\left[2^{-\frac{m-1}{2}}\right]_{P'}}(\psi(Q)) \cdot g_{P'}(\psi(Q))$ . Noting that  $\gamma + \delta = b$  and defining  $g'_0 = x_{P'}^2 x_Q + x_{P'}^2 + x_Q + y_{P'}^2 + y_Q + b + 1$ ,  $g'_1 = x_{P'}^2 + x_Q + 1$ , and  $g'_2 = x_{P'}^4 + x_Q + 1$ , we obtain

$$l_{\left[2^{-\frac{m-1}{2}}\right]_{P'}}(\psi(Q)) \cdot g_{P'}(\psi(Q)) = ((g'_0 + g'_2) + (g'_1 + 1)s + t) \cdot (g'_0 + g'_1 s + t).$$

An implementation of the  $\eta_T$  pairing following this construction is given in Algorithm 2.

We also studied direct approaches based on Equation (2). However, they turned out to be slower and we will not consider such algorithms in this paper (see [4, Appendix A] for details).

### 2.3 Final Exponentiation

The  $\eta_T$  pairing has to be reduced in order to be uniquely defined. We have to raise  $\eta_T(P, Q)$  to the  $M$ th power, where

$$M = \frac{2^{4m} - 1}{N} = (2^{2m} - 1)(2^m + 1 - \nu 2^{\frac{m+1}{2}}).$$

Two algorithms have been proposed in the open literature for  $\nu = 1$  and  $\nu = -1$ , respectively:

---

**Algorithm 2.** Computation of the  $\eta_T$  pairing in characteristic two: reversed-loop approach without square roots.

---

**Input:**  $P, Q \in \mathbb{F}_{2^m}[\ell]$ .

**Output:**  $\eta_T(P, Q) \in \mathbb{F}_{2^{4m}}^*$ .

1.  $y_P \leftarrow y_P + \delta;$  ( $\bar{\delta}$  XOR)
  2.  $x_P \leftarrow x_P^2; y_P \leftarrow y_P^2;$  (2 S)
  3.  $y_P \leftarrow y_P + b; u \leftarrow x_P + 1;$  ( $b + 1$  XOR)
  4.  $g_1 \leftarrow u + x_Q;$  (1 A)
  5.  $g_0 \leftarrow x_P \cdot x_Q + y_P + y_Q + g_1;$  (1 M, 3 A)
  6.  $x_Q \leftarrow x_Q + 1;$  (1 XOR)
  7.  $g_2 \leftarrow x_P^2 + x_Q;$  (1 S, 1 A)
  8.  $G \leftarrow g_0 + g_1s + t;$
  9.  $L \leftarrow (g_0 + g_2) + (g_1 + 1)s + t;$  (1 A, 1 XOR)
  10.  $F \leftarrow L \cdot G;$  (2 M, 1 S, 5 A, 2 XOR)
  11. **for**  $j \leftarrow 1$  to  $\frac{m-1}{2}$  **do**
  12.  $F \leftarrow F^2;$  (4 S, 4 A)
  13.  $x_Q \leftarrow x_Q^4; y_Q \leftarrow y_Q^4;$  (4 S)
  14.  $x_Q \leftarrow x_Q + 1; y_Q \leftarrow y_Q + x_Q;$  (1 A, 1 XOR)
  15.  $g_0 \leftarrow u \cdot x_Q + y_P + y_Q;$  (1 M, 2 A)
  16.  $g_1 \leftarrow x_P + x_Q;$  (1 A)
  17.  $G \leftarrow g_0 + g_1s + t;$
  18.  $F \leftarrow F \cdot G;$  (6 M, 14 A)
  19. **end for**
  20. **Return**  $F^M;$
- 

- Ronan *et al.* [29] assumed that  $\nu = 1$ , unrolled the different powering, and grouped the inversions together. Thus, their final exponentiation algorithm involves a single inversion over  $\mathbb{F}_{2^{4m}}$ .
- Shu *et al.* [33] noted that raising the  $\eta_T$  pairing to the power of  $2^{2m} - 1$  requires only one inversion over  $\mathbb{F}_{2^{2m}}$ . When  $\nu = -1$ , the second part of the final exponentiation consists in raising this intermediate result to the power of  $2^m + 1 + 2^{\frac{m+1}{2}}$ .

In the following, we show that the final exponentiation of the  $\eta_T$  pairing in characteristic two always involves a single inversion over  $\mathbb{F}_{2^{2m}}$ . Since  $M = (2^{2m} - 1)(2^m + 1) + \nu(1 - 2^{2m})2^{\frac{m+1}{2}}$ , we compute

$$\eta_T(P, Q)^M = \left(\eta_T(P, Q)^{2^{2m} - 1}\right)^{2^m + 1} \cdot \left(\eta_T(P, Q)^{\nu(1 - 2^{2m})}\right)^{2^{\frac{m+1}{2}}},$$

and we remark that the final exponentiation requires a single inversion over  $\mathbb{F}_{2^{2m}}$ . Let  $U = \eta_T(P, Q) \in \mathbb{F}_{2^{4m}}^*$ . Writing  $U = U_0 + U_1t$ , where  $U_0$  and  $U_1 \in \mathbb{F}_{2^{2m}}$  and noting that  $t^{2^{2m}} = t + 1$ , we obtain  $U^{2^{2m}} = U_0 + U_1 + U_1t$ . Therefore, we have:

$$\begin{aligned}
 U^{2^{2m}-1} &= \frac{U_0 + U_1 + U_1t}{U_0 + U_1t} = \frac{(U_0 + U_1 + U_1t)^2}{(U_0 + U_1t) \cdot (U_0 + U_1 + U_1t)} \\
 &= \frac{U_0^2 + U_1^2 + U_1^2s + U_1^2t}{U_0^2 + U_0U_1 + U_1^2s}, \text{ and} \\
 U^{1-2^{2m}} &= \frac{U_0 + U_1t}{U_0 + U_1 + U_1t} = \frac{U_0^2 + U_1^2s + U_1^2t}{U_0^2 + U_0U_1 + U_1^2s},
 \end{aligned}$$

where  $U_0^2 + U_0U_1 + U_1^2s \in \mathbb{F}_{2^{2m}}$ . Algorithm 3 summarizes the computation of the  $\eta_T(P, Q)^M$ :

- According to our notation, we have  $U = U_0 + U_1t$ , where  $U_0 = u_0 + u_1s$  and  $U_1 = u_2 + u_3s$ . Since  $s^2 = s + 1$ , we remark that:

$$\begin{aligned}
 U_0^2 &= (u_0^2 + u_1^2) + u_1^2s, \\
 U_1^2 &= (u_2^2 + u_3^2) + u_3^2s, \quad U_1^2s = u_3^2 + u_2^2s.
 \end{aligned}$$

Therefore, 4 squarings and 2 additions over  $\mathbb{F}_{2^m}$  allow us to get  $T_0 = U_0^2$ ,  $T_1 = U_1^2$ , and  $T_2 = U_1^2s$ .

- Multiplication over  $\mathbb{F}_{2^{2m}}$  on line 3 is performed according to the Karatsuba-Ofman’s scheme and involves three multiplications and four additions over  $\mathbb{F}_{2^m}$ :

$$T_3 = U_0U_1 = u_0u_2 + u_1u_3 + ((u_0 + u_1)(u_2 + u_3) + u_0u_2)s.$$

- Thanks to the tower field, inversion of  $D = U_0^2 + U_0U_1 + U_1^2s \in \mathbb{F}_{2^{2m}}$  is replaced by an inversion (denoted by I), a squaring, three multiplications, and two additions over  $\mathbb{F}_{2^m}$  (see [4, Appendix C] for details).
- The next step consists in computing  $V = V_0 + V_1t = U^{2^{2m}-1}$  and  $W = W_0 + W_1t = U^{\nu(1-2^{2m})}$ , where  $V_0, V_1, W_0,$  and  $W_1 \in \mathbb{F}_{2^{2m}}$ . Defining  $T_5 = \frac{U_0^2 + U_1^2s}{U_0^2 + U_0U_1 + U_1^2s}$  and  $T_6 = \frac{U_1^2}{U_0^2 + U_0U_1 + U_1^2s}$  (line 6), we easily check that  $U^{2^{2m}-1} = (T_5 + T_6) + T_6t$  and  $U^{1-2^{2m}} = T_5 + T_6t$ . Thus,

$$V_0 = T_5 + T_6, \quad W_0 = \begin{cases} T_5 + T_6 & \text{if } \nu = -1, \\ T_6 & \text{if } \nu = 1, \end{cases} \quad V_1 = W_1 = T_6.$$

- Raising  $V = V_0 + V_1t \in \mathbb{F}_{2^{4m}}^*$  to the  $(2^m + 1)$ th power over  $\mathbb{F}_{2^{4m}}$  (line 15) consists in multiplying  $V^{2^m}$  by  $V$ . This operation turns out to be less expensive than the usual multiplication over  $\mathbb{F}_{2^{4m}}$  (see [4, Appendix D.3] for details).

### 2.4 Overall Cost Evaluations

Table 1 summarizes the costs of the algorithms studied in this section in terms of arithmetic operations over  $\mathbb{F}_{2^m}$ . Software implementations benefit from the



---

**Algorithm 3.** Final exponentiation of the reduced  $\eta_T$  pairing.

---

**Input:**  $U = u_0 + u_1s + u_2t + u_3st \in \mathbb{F}_{2^{4m}}^*$ .

The intermediate variables  $m_i$  belong to  $\mathbb{F}_{2^m}$ . The  $T_i$ 's,  $V_i$ 's,  $W_i$ 's, and  $D$  belong to  $\mathbb{F}_{2^{2m}}$ .  $V$  and  $W \in \mathbb{F}_{2^{4m}}$ .

**Output:**  $V = U^M \in \mathbb{F}_{2^{4m}}^*$ , with  $M = (2^{2m} + 1)(2^m - \nu 2^{\frac{m+1}{2}} + 1)$ .

1.  $m_0 \leftarrow u_0^2; m_1 \leftarrow u_1^2; m_2 \leftarrow u_2^2; m_3 \leftarrow u_3^2;$  (4 S)
  2.  $T_0 \leftarrow (m_0 + m_1) + m_1s; T_1 \leftarrow (m_2 + m_3) + m_3s;$  (2 A)
  3.  $T_2 \leftarrow m_3 + m_2s; T_3 \leftarrow (u_0 + u_1s) \cdot (u_2 + u_3s);$  (3 M, 4 A)
  4.  $T_4 \leftarrow T_0 + T_2; D \leftarrow T_3 + T_4;$  (4 A)
  5.  $D \leftarrow D^{-1};$  (1 I, 3 M, 1 S, 2 A)
  6.  $T_5 \leftarrow T_1 \cdot D; T_6 \leftarrow T_4 \cdot D;$  (6 M, 8 A)
  7.  $V_0 \leftarrow T_5 + T_6;$  (2 A)
  8.  $V_1, W_1 \leftarrow T_5;$
  9. **if**  $\nu = -1$  **then**
  10.  $W_0 \leftarrow V_0;$
  11. **else**
  12.  $W_0 \leftarrow T_6;$
  13. **end if**
  14.  $V \leftarrow V_0 + V_1t; W \leftarrow W_0 + W_1t;$
  15.  $V \leftarrow V^{2^{m+1}}$  (5 M, 2 S, 9 A)
  16. **for**  $i \leftarrow 1$  **to**  $\frac{m+1}{2}$  **do**
  17.  $W \leftarrow W^2;$  (4 S, 4 A)
  18. **end for**
  19. **Return**  $V \cdot W;$  (9 M, 20 A)
- 

Extended Euclidean Algorithm (EEA) to perform the inversion over  $\mathbb{F}_{2^m}$ . However, supplementing a pairing coprocessor with dedicated hardware for the EEA is not the most appropriate solution. Computing the inverse of  $a \in \mathbb{F}_{2^m}$  by means of multiplications and squarings over  $\mathbb{F}_{2^m}$  according to Fermat's little theorem and Itoh and Tsujii's work [15] allows one to keep the circuit area as small as possible without impacting too severely on the performances [3]. Since  $a^{-1} = \left(a^{2^{m-1}-1}\right)^2$ , we first raise  $a$  to the power of  $2^{m-1} - 1$  using a Brauer-type addition chain for  $m - 1$ . Then, a squaring over  $\mathbb{F}_{2^m}$  suffices to obtain  $a^{-1}$ . We reported the cost of this inversion scheme for typical values of  $m$  in Table 2.

### 3 Computation of the Modified Tate Pairing

Several researchers designed hardware accelerators over  $\mathbb{F}_{2^m}$  and  $\mathbb{F}_{3^m}$  for the modified Tate pairing. According to Barreto *et al.* [1], a second exponentiation allows one to compute the modified Tate pairing from the reduced  $\eta_T$  pairing. Thus, the modified Tate pairing is believed to be slower and a comparison between architectures for the modified Tate and  $\eta_T$  pairings would be unfair. Here, we take advantage of the bilinearity of the reduced  $\eta_T$  pairing and show how to get the modified Tate pairing almost for free.

**Table 1.** Cost of the presented algorithms for computing the reduced  $\eta_T$  pairing in characteristic two in terms of operations over the underlying field  $\mathbb{F}_{2^m}$

	$\eta_T$ pairing with square roots (Algorithm 1)	$\eta_T$ pairing without square root (Algorithm 2)	Final Exponentiation (Algorithm 3)
<b>Additions</b>	$10 + 17 \cdot \frac{m-1}{2}$	$11m$	$2m + 53$
<b>XORs</b>	$3 + \bar{\delta} + (2\alpha + \beta) \cdot \frac{m+1}{2}$	$5 + \bar{\delta} + b + \frac{m-1}{2}$	–
<b>Multiplications</b>	$3 + 7 \cdot \frac{m-1}{2}$	$3 + 7 \cdot \frac{m-1}{2}$	26
<b>Squarings</b>	$m + 1$	$4m$	$2m + 9$
<b>Square roots</b>	$m - 1$	–	–
<b>Inversions</b>	–	–	1

**Table 2.** Cost of inversion over  $\mathbb{F}_{2^m}$  according to Itoh and Tsujii’s algorithm in terms of multiplications and squarings

Field	$\mathbb{F}_{2^{239}}$	$\mathbb{F}_{2^{251}}$	$\mathbb{F}_{2^{283}}$	$\mathbb{F}_{2^{313}}$
Cost	10 M, 238 S	10 M, 250 S	11 M, 282 S	10 M, 312 S

### 3.1 Modified Tate Pairing in Characteristic Two

The modified Tate pairing in characteristic two is given by  $\hat{e}(P, Q)^M = \eta_T(P, Q)^{MT}$ , where  $M = \frac{2^{4m}-1}{N}$  and  $T = 2^m - N$  [1]. Let  $V = \eta_T(P, Q)^M$ . We have  $V^N = \eta_T(P, Q)^{2^{4m}-1} = 1$ . Since  $\eta_T(P, Q)^M$  is a bilinear pairing, we obtain:

$$\hat{e}(P, Q)^M = V^T = V^{2^m-N} = V^{2^m} = \eta_T(P, Q)^{M \cdot 2^m} = \eta_T([2^m]P, Q)^M,$$

where  $[2^m]P = (x_P + 1, x_P + y_P + \alpha + 1)$ . Thus, it suffices to provide a hardware accelerator for the reduced  $\eta_T$  pairing with  $[2^m]P$  and  $Q$  to get the modified Tate pairing. Since this preprocessing step involves an XOR operation and an addition over  $\mathbb{F}_{2^m}$ , it can be computed in software. Conversely, a processor for the modified Tate pairing computes the  $\eta_T$  pairing if its inputs are  $[2^{-m}]P$  and  $Q$ :

$$\eta_T(P, Q)^M = \hat{e}([2^{-m}]P, Q)^M,$$

where  $[2^{-m}]P = (x_P + 1, x_P + y_P + \alpha)$ .

### 3.2 Modified Tate Pairing in Characteristic Three

The same approach allows one to compute the modified Tate pairing in characteristic three. Let  $m$  be a positive integer coprime to 6 and  $E$  be the supersingular elliptic curve defined by  $E : y^2 = x^3 - x + b$ , where  $b \in \{-1, 1\}$ . The number of

rational points of  $E$  over  $\mathbb{F}_{3^m}$  is given by  $N = \#E(\mathbb{F}_{3^m}) = 3^m + 1 + \mu b 3^{\frac{m+1}{2}}$  [2], with

$$\mu = \begin{cases} 1 & \text{if } m \equiv 1, 11 \pmod{12}, \\ -1 & \text{if } m \equiv 5, 7 \pmod{12}. \end{cases}$$

In characteristic three, we have the following relation between the reduced  $\eta_T$  and modified Tate pairings [1]:

$$(\eta_T(P, Q)^M)^{3T^2} = (\hat{e}(P, Q)^M)^L,$$

with  $M = \frac{3^{6m}-1}{N}$ ,  $T = 3^m - N$ , and  $L = -\mu b 3^{\frac{m+3}{2}}$ . Defining  $V = \eta_T(P, Q)^M \in \mathbb{F}_{3^{6m}}^*$  and seeing that  $V^N = 1$ , we obtain

$$V^{3T^2} = V^{3^{2m+1}-2 \cdot 3^{m+1} \cdot N+3N^2} = V^{3^{2m+1}}.$$

Dividing by  $L$  at the exponent level, we finally get the following relation between the reduced  $\eta_T$  and modified Tate pairings:

$$\begin{aligned} \hat{e}(P, Q)^M &= V^{\frac{3^{2m+1}}{L}} \\ &= V^{-\mu b 3^{\frac{3m-1}{2}}} = \eta_T\left(\left[-\mu b 3^{\frac{3m-1}{2}}\right] P, Q\right)^M, \end{aligned}$$

where  $\left[-\mu b 3^{\frac{3m-1}{2}}\right] P = (\sqrt[3]{x_P} - b, -\mu b \lambda \sqrt[3]{y_P})$  and

$$\lambda = (-1)^{\frac{m+1}{2}} = \begin{cases} 1 & \text{if } m \equiv 7, 11 \pmod{12}, \\ -1 & \text{if } m \equiv 1, 5 \pmod{12}. \end{cases}$$

Again, the overhead introduced is negligible compared to the calculation time of the reduced  $\eta_T$  pairing. Consider now the cube-root-free reversed-loop algorithm proposed by Beuchat *et al.* (Algorithm 4 in [5]). In this case, we suggest to compute  $\eta_T\left([- \mu b] P, \left[3^{\frac{3m-1}{2}}\right] Q\right)^M$ . Surprisingly, the modified Tate pairing in characteristic three turns out to be slightly less expensive than the  $\eta_T$  pairing: we save two cubings and one addition over  $\mathbb{F}_{3^m}$  (see [4, Appendix B] for details). Conversely, a processor for the modified Tate pairing provided with  $[-\mu b] P$  and  $\left[3^{\frac{-3m+1}{2}}\right] Q$  will return the reduced  $\eta_T$  pairing.

## 4 Implementation Results and Comparisons

### 4.1 A Unified Operator for the Arithmetic over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$

In [3], Beuchat *et al.* presented an FPGA-based accelerator for the computation of the  $\eta_T$  pairing in characteristic three. The coprocessor was based on a unified operator capable of handling all the necessary arithmetic operations over the base field  $\mathbb{F}_{3^m}$ . This streamlined design led to smaller circuits while retaining competitive performances with respect to the other published architectures.

For these reasons, we chose to use such a unified operator for our own implementations in characteristic three. We also adapted the operator for supporting finite-field arithmetic in characteristic two.

The core of this unified operator is an array multiplier [34] for computing the product of two elements of  $\mathbb{F}_{p^m}$  (where  $p = 2$  or  $3$ ), represented in a polynomial basis using a degree- $m$  polynomial  $f(x)$  irreducible over  $\mathbb{F}_p$ :  $\mathbb{F}_{p^m} \cong \mathbb{F}_p[x]/(f(x))$ .  $D$  coefficients of the multiplicand are processed at each clock cycle. The  $D$  corresponding partial products are then shifted and reduced modulo  $f(x)$  according to their respective weight, and finally summed into a register thanks to a tree of adders over  $\mathbb{F}_{p^m}$ . A feedback loop allows the accumulation of the previous partial products. A product over  $\mathbb{F}_{p^m}$  is therefore computed in  $\lceil m/D \rceil$  clock cycles.

With only slight modifications, it is possible for this multiplier to also support the other operations required by the computation of the modified Tate pairing. For instance, bypassing the shift/modulo- $f(x)$  reduction stage allows for additions, subtractions and accumulations. Similarly, the Frobenius endomorphism (*i.e.* squaring in characteristic two or cubing in characteristic three) only amounts to a linear combination of the coefficients of the polynomial. This linear combination can be computed at design time and then directly hard-wired as an alternative datapath during the shift/modulo stage.

## 4.2 Characteristic Two Versus Characteristic Three

It is common knowledge that arithmetic over  $\mathbb{F}_{2^m}$  is more compact and efficient than over  $\mathbb{F}_{3^m}$ . However, due to the different embedding degrees enjoyed by the elliptic curves of interest, competitive levels of security for pairing implementations in characteristic two are only achieved at the price of working over extension degrees much larger than what their counterparts in characteristic three require.

For a better understanding of this trade-off, we present here FPGA implementation results of a coprocessor for the modified Tate pairing in both characteristics two and three. The coprocessor is based on the previously described unified operator and implements the square- and cube-root-free reversed-loop algorithms (Algorithm 2, and Algorithm 4 in [5]) along with the corresponding final exponentiation. We also experimented with several values for  $D$ , aiming at a more exhaustive study of the trade-off between cost and performances.

Tables 3 and 4 present the post-place-and-route results for characteristic two and three respectively. These results were obtained for a Xilinx Virtex-II Pro 20 FPGA with average speedgrade, using the Xilinx ISE 9.2i tool suite. The two tables are also summarized in Figure 1.

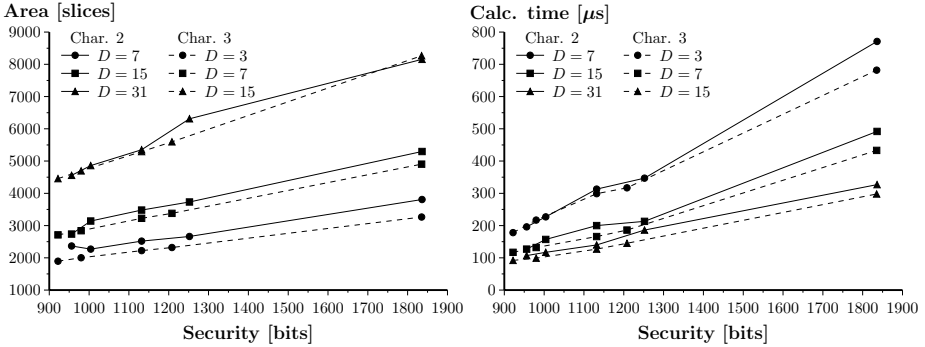
The given results show a slight advantage of characteristic three over characteristic two, for all the studied levels of security. This goes against the performances obtained by Barreto *et al.* in the case of software implementation [1], but also against the hardware results published by Shu *et al.* in [33]. Of course, this observation remains closely related to our unified architecture. However, as detailed in the following, our coprocessors perform better than the previously published solutions in terms of area-time product, which leads us to believe this observation to be accurate.

**Table 3.** Implementation results of the modified Tate pairing in characteristic two using our unified operator (on a Xilinx Virtex-II Pro xc2vp20, speedgrade -6)

Field	Security [bits]	$D$	Area [slices]	Frequency [MHz]	#cycles	Estimated calc. time [ $\mu$ s]
$\mathbb{F}_{2^{239}}$	956	7	2366	199	39075	196
		15	2736	165	20830	127
		31	4557	123	13147	107
$\mathbb{F}_{2^{251}}$	1004	7	2270	185	41969	227
		15	3140	145	22846	157
		31	4861	126	14794	117
$\mathbb{F}_{2^{283}}$	1132	7	2517	169	52820	313
		15	3481	140	27942	200
		31	5350	127	17765	140
$\mathbb{F}_{2^{313}}$	1252	7	2661	182	63167	347
		15	3731	156	33283	213
		31	6310	111	20831	186
$\mathbb{F}_{2^{459}}$	1836	7	3809	168	129780	771
		15	5297	135	66589	492
		31	8153	115	37601	327

**Table 4.** Implementation results of the modified Tate pairing in characteristic three using our unified operator (on a Xilinx Virtex-II Pro xc2vp20, speedgrade -6)

Field	Security [bits]	$D$	Area [slices]	Frequency [MHz]	#cycles	Estimated calc. time [ $\mu$ s]
$\mathbb{F}_{3^{97}}$	922	3	1896	156	27800	178
		7	2711	128	14954	117
		15	4455	105	9657	92
$\mathbb{F}_{3^{103}}$	980	3	2003	151	32649	217
		7	2841	126	16633	132
		15	4695	103	10227	99
$\mathbb{F}_{3^{119}}$	1132	3	2223	140	41788	299
		7	3225	125	20814	166
		15	5293	99	12607	127
$\mathbb{F}_{3^{127}}$	1208	3	2320	149	47234	317
		7	3379	129	24028	186
		15	5596	99	14349	145
$\mathbb{F}_{3^{193}}$	1835	3	3266	147	100668	682
		7	4905	111	48205	433
		15	8266	90	26937	298



**Fig. 1.** Area (left) and calculation time (right) for the modified Tate pairing on our unified operator, in both characteristics two and three, for various extension degrees and different values for the parameter  $D$

Moreover, the optimal number  $D$  of coefficients processed per clock cycle for the array multiplier appears to be 15 in characteristic two and 7 in characteristic three. However, modifying the value of this parameter changes only marginally the overall area-time product. According to the requirements of each application in terms of area and speed, one can then select the most appropriate value for  $D$ .

### 4.3 Comparisons

Tables 5, 6 and 7 present the cost and performances of other coprocessors for the computation of the modified Tate and reduced  $\eta_T$  pairings in characteristics two and three as published in the open literature. The results are summarized in Figure 2 as a comparison of these solutions against our proposed architecture in terms of their area-time product.

Despite its inherent lack of parallelism between operations, our unified operator greatly benefits from its compact design in order to reach higher frequencies. Combined with the algorithmic improvements described in this paper and in [5], this leads to competitive calculation times. Additionally, the streamlined design allows for reaching higher extension degrees and levels of security without risking to exhaust the FPGA resources: the slow increase of the area-time product with the security level of the system hints at the high scalability of the coprocessor.

Finally, the good performances of our solution against the previously published works vouches for a strong confidence in the outcome of our comparison between characteristics two and three for the hardware implementation of the modified Tate pairing.

## 5 Conclusion

We discussed several algorithms to compute the  $\eta_T$  pairing and its final exponentiation in characteristic two. We then showed how to get back to the modified

**Table 5.** FPGA-based accelerators for the modified Tate pairing over  $\mathbb{F}_{2^m}$  in the literature. The parameter  $D$  refers to the number of coefficients processed at each clock cycle by a multiplier. The architectures by Shu *et al.* [33] include four kinds of multipliers.

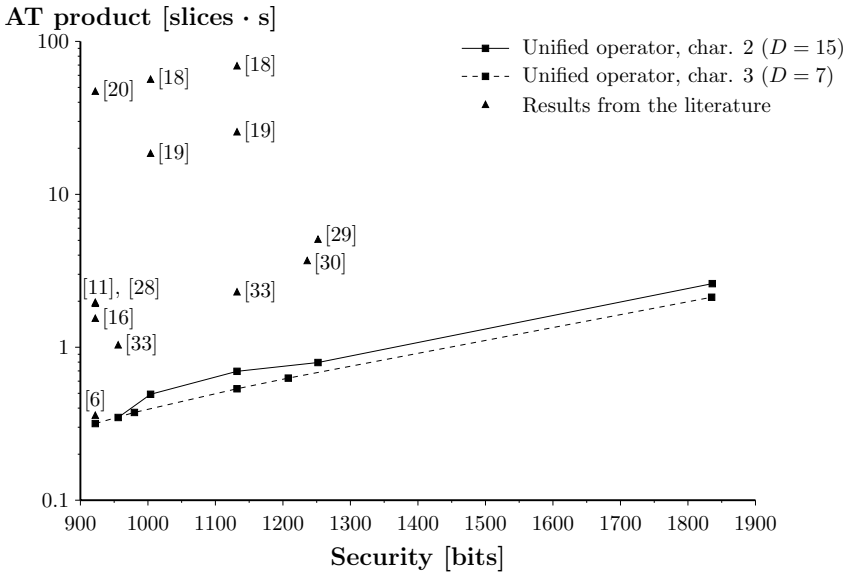
	Curve	FPGA	#mult.	$D$	Area [slices]	Freq. [MHz]	Calculation time [ $\mu$ s]	
Shu <i>et al.</i> [33]	$E(\mathbb{F}_{2^{239}})$	xc2vp100		6	16	25287	84	41
				1	4			
				1	1			
				1	2			
Keller <i>et al.</i> [18]	$E(\mathbb{F}_{2^{251}})$	xc2v6000	13	1	16621	50	6440	
				6	21955	43	2580	
				10	27725	40	2370	
Keller <i>et al.</i> [19]	$E(\mathbb{F}_{2^{251}})$	xc2v6000		1	6	3788	40	4900
				3	6	6181	40	3200
				9	6	13387	40	2600
Keller <i>et al.</i> [18]	$E(\mathbb{F}_{2^{283}})$	xc2v6000	13	1	18599	50	7980	
				4	22636	49	3230	
				6	24655	47	2810	
Keller <i>et al.</i> [19]	$E(\mathbb{F}_{2^{283}})$	xc2v6000		1	6	4273	40	6000
				3	6	6981	40	3800
				9	6	15065	40	3000
Shu <i>et al.</i> [33]	$E(\mathbb{F}_{2^{283}})$	xc2vp100		6	32	37803	72	61
				1	4			
				1	1			
				1	2			
Ronan <i>et al.</i> [29]	$E(\mathbb{F}_{2^{313}})$	xc2vp100	14	4	34675	55	203	
				8	41078	50	124	
				12	44060	33	146	
Ronan <i>et al.</i> [30]	$C(\mathbb{F}_{2^{103}})$	xc2vp100	20	4	21021	51	206	
				8	24290	46	152	
				16	30464	41	132	

**Table 6.** FPGA-based accelerators for the modified Tate pairing over  $\mathbb{F}_{3^m}$  in the literature. The parameter  $D$  refers to the number of coefficients processed at each clock cycle by a multiplier.

	FPGA	#mult.	$D$	Area [slices]	Freq. [MHz]	Calculation time [ $\mu$ s]
Grabher and Page [11]	xc2vp4	1	4	4481	150	432.3
Kerins <i>et al.</i> [20]	xc2vp125	18	4	55616	15	850

**Table 7.** FPGA-based accelerators for reduced  $\eta_T$  pairing over  $\mathbb{F}_{397}$  in the literature. The parameter  $D$  refers to the number of coefficients processed at each clock cycle by a multiplier.

	FPGA	#mult.	D	Area [slices]	Freq. [MHz]	Calculation time [ $\mu$ s]
Ronan <i>et al.</i> [28]	xc2vp100	5	4	10540	84.8	187
Jiang [16]	xc4vlx200	Not specified	7	74105	77.7	20.9
Beuchat <i>et al.</i> [5]	xc2vp4	1	3	1833	145	192
Beuchat <i>et al.</i> [6]	xc2vp30	9	3	10897	147	33.0
	xc4vlx25	9	3	11318	200	24.2



**Fig. 2.** Area-time product of the proposed coprocessor for the modified Tate pairing in characteristics two and three against the other solutions published in the literature

Tate pairing at almost no extra cost. Finally, we explored the trade-offs involved in the hardware implementation of the modified Tate pairing for both characteristic two and three. Our architectures are based on the unified arithmetic operator introduced in [3], and achieve a better area-time trade-off compared to previously published solutions [11, 16, 18, 19, 20, 28, 29, 30, 33].

Our modified Tate pairing coprocessors embed a single multiplier. A challenge consists in designing parallel architectures with the same (or even a smaller) area-time product. Future work should also include a study of the  $\eta_T$  pairing over genus-2 curves. The Ate pairing [14] would also be of interest, for it generalizes to ordinary curves the improvements introduced by the  $\eta_T$  pairing in the case of supersingular curves.



## Acknowledgment

The authors would like to thank Guillaume Hanrot and the anonymous referees for their valuable comments. This work was supported by the New Energy and Industrial Technology Development Organization (NEDO), Japan.

The authors would also like to express their deepest gratitude to the Carthusian Monks of the Grande Chartreuse in the French Alps for their succulent herbal products which fueled our efforts in writing this article.

## References

1. Barreto, P.S.L.M., Galbraith, S.D., ÓhÉigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular Abelian varieties. *Designs, Codes and Cryptography* 42, 239–271 (2007)
2. 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)
3. Beuchat, J.-L., Brisebarre, N., Detrey, J., Okamoto, E.: Arithmetic operators for pairing-based cryptography. In: Paillier, P., Verbauwhede, I. (eds.) *CHES 2007*. LNCS, vol. 4727, pp. 239–255. Springer, Heidelberg (2007)
4. Beuchat, J.-L., Brisebarre, N., Detrey, J., Okamoto, E., Rodríguez-Henríquez, F.: A comparison between hardware accelerators for the modified Tate pairing over  $\mathbb{F}_{2^m}$  and  $\mathbb{F}_{3^m}$ . *Cryptology ePrint Archive*, Report 2008/115 (2008)
5. Beuchat, J.-L., Brisebarre, N., Detrey, J., Okamoto, E., Shirase, M., Takagi, T.: Algorithms and arithmetic operators for computing the  $\eta_T$  pairing in characteristic three. *IEEE Transactions on Computers* 57(11) (November 2008) (to appear) An extended version is available as Report 2007/417 of the *Cryptology ePrint Archive*
6. Beuchat, J.-L., Shirase, M., Takagi, T., Okamoto, E.: An algorithm for the  $\eta_T$  pairing calculation in characteristic three and its hardware implementation. In: Kornerup, P., Muller, J.-M. (eds.) *Proceedings of the 18th IEEE Symposium on Computer Arithmetic*, pp. 97–104. IEEE Computer Society, Los Alamitos (2007)
7. Duursma, I., Lee, H.S.: Tate pairing implementation for hyperelliptic curves  $y^2 = x^p - x + d$ . In: Lai, C.S. (ed.) *ASIACRYPT 2003*. LNCS, vol. 2894, pp. 111–123. Springer, Heidelberg (2003)
8. Fong, K., Hankerson, D., López, J., Menezes, A.: Field inversion and point halving revisited. *IEEE Transactions on Computers* 53(8), 1047–1059 (2004)
9. Frey, G., Rück, H.-G.: A remark concerning  $m$ -divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation* 62(206), 865–874 (1994)
10. Galbraith, S.D., Harrison, K., Soldera, D.: Implementing the Tate pairing. In: Fieker, C., Kohel, D.R. (eds.) *ANTS 2002*. LNCS, vol. 2369, pp. 324–337. Springer, Heidelberg (2002)
11. Grabher, P., Page, D.: Hardware acceleration of the Tate pairing in characteristic three. In: Rao, J.R., Sunar, B. (eds.) *CHES 2005*. LNCS, vol. 3659, pp. 398–411. Springer, Heidelberg (2005)
12. Granger, R., Page, D., Smart, N.P.: High security pairing-based cryptography revisited. In: Hess, F., Pauli, S., Pohst, M. (eds.) *ANTS 2006*. LNCS, vol. 4076, pp. 480–494. Springer, Heidelberg (2006)

13. Granger, R., Page, D., Stam, M.: On small characteristic algebraic tori in pairing-based cryptography. *LMS Journal of Computation and Mathematics* 9, 64–85 (2006)
14. Hess, F., Smart, N., Vercauteren, F.: The Eta pairing revisited. *IEEE Transactions on Information Theory* 52(10), 4595–4602 (2006)
15. Itoh, T., Tsujii, S.: A fast algorithm for computing multiplicative inverses in  $\text{GF}(2^m)$  using normal bases. *Information and Computation* 78, 171–177 (1988)
16. Jiang, J.: Bilinear pairing (Eta-T Pairing) IP core. Technical report, City University of Hong Kong – Department of Computer Science (May 2007)
17. Joux, A.: A one round protocol for tripartite Diffie-Hellman. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 385–394. Springer, Heidelberg (2000)
18. Keller, M., Kerins, T., Crowe, F., Marnane, W.P.: FPGA implementation of a  $\text{GF}(2^m)$  Tate pairing architecture. In: Bertels, K., Cardoso, J.M.P., Vassiliadis, S. (eds.) ARC 2006. LNCS, vol. 3985, pp. 358–369. Springer, Heidelberg (2006)
19. Keller, M., Ronan, R., Marnane, W.P., Murphy, C.: Hardware architectures for the Tate pairing over  $\text{GF}(2^m)$ . *Computers and Electrical Engineering* 33(5–6), 392–406 (2007)
20. Kerins, T., Marnane, W.P., Popovici, E.M., Barreto, P.S.L.M.: Efficient hardware for the Tate pairing calculation in characteristic three. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 412–426. Springer, Heidelberg (2005)
21. Kobitz, N., Menezes, A.: Pairing-based cryptography at high security levels. In: Smart, N.P. (ed.) *Cryptography and Coding 2005*. LNCS, vol. 3796, pp. 13–36. Springer, Heidelberg (2005)
22. Kwon, S.: Efficient Tate pairing computation for elliptic curves over binary fields. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 134–145. Springer, Heidelberg (2005)
23. Menezes, A., Okamoto, T., Vanstone, S.A.: Reducing elliptic curves logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory* 39(5), 1639–1646 (1993)
24. Miller, V.S.: Short programs for functions on curves (1986), <http://crypto.stanford.edu/miller>
25. Miller, V.S.: The Weil pairing, and its efficient calculation. *Journal of Cryptology* 17(4), 235–261 (2004)
26. Mitsunari, S., Sakai, R., Kasahara, M.: A new traitor tracing. *IEICE Trans. Fundamentals* E85-A(2), 481–484 (2002)
27. Rodríguez-Henríquez, F., Morales-Luna, G., López, J.: Low-complexity bit-parallel square root computation over  $\text{GF}(2^m)$  for all trinomials. *IEEE Transactions on Computers* 57(4), 472–480 (2008)
28. Ronan, R., Murphy, C., Kerins, T., ÓhÉigeartaigh, C., Barreto, P.S.L.M.: A flexible processor for the characteristic 3  $\eta_T$  pairing. *Int. J. High Performance Systems Architecture* 1(2), 79–88 (2007)
29. Ronan, R., ÓhÉigeartaigh, C., Murphy, C., Scott, M., Kerins, T.: FPGA acceleration of the Tate pairing in characteristic 2. In: *Proceedings of the IEEE International Conference on Field Programmable Technology – FPT 2006*, pp. 213–220. IEEE, Los Alamitos (2006)
30. Ronan, R., ÓhÉigeartaigh, C., Murphy, C., Scott, M., Kerins, T.: Hardware acceleration of the Tate pairing on a genus 2 hyperelliptic curve. *Journal of Systems Architecture* 53, 85–98 (2007)
31. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: *2000 Symposium on Cryptography and Information Security (SCIS 2000)*, Okinawa, Japan, pp. 26–28 (January 2000)

32. Scott, M.: Optimal irreducible polynomials for  $\text{GF}(2^m)$  arithmetic. Cryptology ePrint Archive, Report 2007/192 (2007)
33. Shu, C., Kwon, S., Gaj, K.: FPGA accelerated Tate pairing based cryptosystem over binary fields. In: Proceedings of the IEEE International Conference on Field Programmable Technology – FPT 2006, pp. 173–180. IEEE, Los Alamitos (2006)
34. Song, L., Parhi, K.K.: Low energy digit-serial/parallel finite field multipliers. Journal of VLSI Signal Processing 19(2), 149–166 (1998)