Algorithms and Arithmetic Operators for Computing the η_T Pairing in Characteristic Three

Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, *Member*, *IEEE*,
Eiji Okamoto, *Senior Member*, *IEEE*, Masaaki Shirase, and Tsuyoshi Takagi

Abstract—Since their introduction in constructive cryptographic applications, pairings over (hyper)elliptic curves are at the heart of an ever increasing number of protocols. With software implementations being rather slow, the study of hardware architectures became an active research area. In this paper, we discuss several algorithms to compute the η_T pairing in characteristic three and suggest further improvements. These algorithms involve addition, multiplication, cubing, inversion, and sometimes cube root extraction over $\mathbb{F}_{3^m}$. We propose a hardware accelerator based on a unified arithmetic operator able to perform the operations required by a given algorithm. We describe the implementation of a compact coprocessor for the field $\mathbb{F}_{3^{97}}$ given by $\mathbb{F}_3[x]/(x^{97}+x^{12}+2)$, which compares favorably with other solutions described in the open literature.

Index Terms—η_T pairing, finite field arithmetic, elliptic curve, hardware accelerator, FPGA.

1 Introduction

In 2001, Boneh et al. [1] proposed the BLS scheme, a remarkable short signature scheme whose principle is the following. They consider an additive group $G_1 = \langle P \rangle$ of prime order q and a map-to-point hash function $H : \{0,1\}^* \to G_1$. The secret key is an element x of $\{1, 2, \ldots, q-1\}$ and the public key is $xP \in G_1$ for a signer. Let $m \in \{0,1\}^*$ be a message, they compute the signature $xH(m)$. To do the verification, they use a map called bilinear pairing that we now define.

Let $G_1 = \langle P \rangle$ be an additive group and G_2 a multiplicative group with identity 1. We assume that the discrete logarithm problem is hard in both G_1 and G_2. A bilinear pairing on (G_1, G_2) is a map $e : G_1 \times G_1 \to G_2$ that satisfies the following conditions:

1. *Bilinearity.* For all Q, R, $S \in G_1$,
$$e(Q+R,S) = e(Q,S)e(R,S),$$
$$e(Q,R+S) = e(Q,R)e(Q,S).$$
2. *Nondegeneracy.* $e(P,P) \neq 1$.
3. *Computability.* e can be efficiently computed.

Modifications of the Weil and Tate pairings provide such maps.

The verification in the BLS scheme is done by checking if the values $e(P, xH(m))$ and $e(xP, H(m))$ coincide. Actually, if $x' \in \{1, 2, \ldots, q-1\}$ satisfies $e(xP, H(m)) = e(P, x'H(m))$, then we obtain $e(P, H(m))^x = e(P, H(m))^{x'}$ due to the bilinearity property of the pairing. From the nondegeneracy of the pairing, we know that $e(P, H(m))^x = e(P, H(m))^{x'}$ implies $x = x'$. The total cost is one hashing operation, one modular exponentiation, and two pairing computations, and the signature is twice as short as the one in DSA for similar level of security.

1.1 Pairings in Cryptology

Pairings were first introduced in cryptology by Menezes et al. [2] and Frey and Rück [3] for code-breaking purposes. Mitsunari et al. [4] and Sakai et al. [5] seem to be the first to have discovered their constructive properties. Since the foundational work of Joux [6], an already large and ever increasing number of pairing-based protocols has been found. Most of them are described in the survey by Dutta et al. [7]. As noticed in that survey, such protocols rely critically on efficient algorithms and implementations of pairing primitives.

According to [8], [9], when dealing with general curves providing common levels of security, the Tate pairing seems to be more efficient for computation than the Weil pairing and we now describe it.

Let E be a supersingular[1] elliptic curve over $\mathbb{F}_{p^m}$, where p is a prime and m is a positive integer, and let $E(\mathbb{F}_{p^m})$ denote the group of its points. Let $\ell > 0$ be an integer relatively prime to p. The *embedding degree* (or *security multiplier*) is the least positive integer k satisfying $p^{km} \equiv 1 \pmod{\ell}$. Let

1. See [10, Theorem V.3.1] for a definition.

- *J.-L. Beuchat and E. Okamoto are with the Graduate School of Systems and Information Engineering, Laboratory of Cryptography and Information Security, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan. E-mail: {beuchat, okamoto}@risk.tsukuba.ac.jp.*
- *N. Brisebarre is with Projet Arénaire, LIP, École Normale Supérieure de Lyon, 46, Allée d'Italie, F-69364 Lyon Cedex 07, France. E-mail: Nicolas.Brisebarre@ens-lyon.fr.*
- *J. Detrey is with the Cosec Group, Bonn-Aachen International Center for Information Technology (B-IT), Dahlmannstraße 2, D-53113 Bonn, Germany. E-mail: jdetrey@bit.uni-bonn.de.*
- *M. Shirase and T. Takagi are with the School of Systems Information Science, Future University-Hakodate, 116-2 Kamedanakano-cho, Hakodate, Hokkaido 041-8655, Japan. E-mail: {shirase, takagi}@fun.ac.jp.*

Manuscript received 1 Nov. 2007; revised 4 Mar. 2008; accepted 19 Mar. 2008; published online 27 June 2008.
Recommended for acceptance by R. Steinwandt, W. Geiselmann, and Ç.K. Koç. For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number TCSI-2007-11-0556.
Digital Object Identifier no. 10.1109/TC.2008.103.

$E(\mathbb{F}_{p^m})[\ell]$ denote the ℓ-torsion subgroup of $E(\mathbb{F}_{p^m})$, i.e., the set of elements P of $E(\mathbb{F}_{p^m})$ that satisfy $[\ell]P = \mathcal{O}$, where $\mathcal{O}$ is the point at infinity of the elliptic curve. Let $P \in E(\mathbb{F}_{p^m})[\ell]$ and $Q \in E(\mathbb{F}_{p^{km}})[\ell]$, let $f_{\ell,P}$ be a rational function on the curve with divisor $\ell(P) - \ell(\mathcal{O})$ (see [10] for an account of divisors), there exists a divisor D_Q equivalent to $(Q) - (\mathcal{O})$, with a support disjoint from the support of $f_{\ell,P}$. Then, the Tate pairing[2] of order ℓ is the map $e : E(\mathbb{F}_{p^m})[\ell] \times E(\mathbb{F}_{p^{km}})[\ell] \rightarrow \mathbb{F}^*_{p^{km}}$ defined by $e(P,Q) = f_{\ell,P}(D_Q)^{(p^{km}-1)/\ell}$. The kind of powering that occurs in this definition is called the final exponentiation; it makes it possible to get values in a multiplicative subgroup of $\mathbb{F}^*_{p^{km}}$ (which is required by most of the cryptographic applications) instead of a multiplicative subgroup of a quotient of $\mathbb{F}^*_{p^{km}}$.

In [11], Barreto et al. proved that this pairing can be computed as $e(P,Q) = f_{\ell,P}(Q)^{\frac{p^{km}-1}{\ell}}$, where $f_{\ell,P}$ is evaluated on a point rather than on a divisor. Due to a distortion map $\psi : E(\mathbb{F}_{p^m})[\ell] \rightarrow E(\mathbb{F}_{p^{km}})[\ell]$ (the concept of a distortion map was introduced in [12]), one can define the modified Tate pairing $\hat{e}$ by $\hat{e}(P,Q) = e(P, \psi(Q))$ for all $P, Q \in E(\mathbb{F}_{p^m})[\ell]$.

Miller [13], [14] proposed in 1986 the first algorithm for computing Weil and Tate pairings. Different ways for computing the Tate pairing can be found in [11], [15], [16], and [17]. In [18], Barreto et al. introduced the η_T pairing, which extended and improved the Duursma-Lee techniques [16]. It makes it possible to efficiently compute the Tate pairing. The η_T pairing is presented in Section 2 in which we recall the relation between it and the modified Tate pairing.

1.2 Implementation Challenges

With the software implementations of these successive algorithmic improvements being rather slow, the need for fine hardware implementations is strong. This is a critical issue to make pairings popular and of common use in cryptography and in particular in view of a successful industrial transfer. The papers [19], [20], [21], [22], [23], [24], [25], [26], and [27] address that problem.

In this paper, we deal with the characteristic three case, and given a positive integer m coprime to 6, we consider E, a supersingular elliptic curve over $\mathbb{F}_{3^m}$, defined by the equation $y^2 = x^3 - x + b$, with $b \in \{-1, 1\}$. Following the discussion at the beginning of [18, Section 5], there is no loss of generality from considering this case since these curves offer the same level of security for pairing applications as any supersingular elliptic curve over $\mathbb{F}_{3^m}$. The considered curve has an embedding degree of 6, which is the maximum value possible for supersingular elliptic curves and, hence, seems to be an attractive choice for pairing implementation.

1.3 Our Contribution

The algorithm given in [18] for computing the η_T pairing halves the number of iterations used in the approach by Duursma and Lee [16] but has the drawback of using inverse Frobenius maps. In [25], Beuchat et al. proposed a modified η_T pairing algorithm in characteristic three that does not require any inverse Frobenius map. Moreover, they designed a novel arithmetic operator implementing addition, cubing, and multiplication over $\mathbb{F}_{3^{97}}$, which performs in a fast and cheap way the step of final exponentiation [26]. Then, they extended in [27] this approach to the computation of the reduced η_T pairing (i.e., the combination of the η_T pairing and the final exponentiation).

In this paper, we present a synthesis and an improvement of the results in [25], [26], and [27]. The outline of this paper is given as follows: In Section 2, we define the η_T pairing and its reduced form, we give different algorithms to compute them, and we provide exact cost evaluations for these algorithms. Section 3 is dedicated to the presentation of a reduced η_T pairing coprocessor that is based on a unified arithmetic operator that implements the various required elementary operations over $\mathbb{F}_{3^m}$. We want to mention that all the material (i.e., algorithms and architectures) presented in this section can be easily adapted to work on any field $\mathbb{F}_p[x]/(f(x))$ for any prime p and any polynomial f irreducible over $\mathbb{F}_p$. We implemented our coprocessor on several Field-Programmable Gate Array (FPGA) families for the field $\mathbb{F}_{3^{97}}$ given by $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$. We provide the reader with a comprehensive comparison against state-of-the-art η_T pairing accelerators in Section 4 and conclude this paper in Section 5.

The appendices mentioned in the rest of the paper can be found in the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109.TC.2008.103.

2 Computation of the η_T Pairing in Characteristic Three

2.1 Preliminary Definitions

We use here the definition of the η_T pairing as introduced by Barreto et al. [18]. The interested reader shall find in that paper all the details related to the mathematical construction of the pairing, which we will deliberately not mention here for clarity's sake.

Let E be the supersingular elliptic curve defined by the equation $E : y^2 = x^3 - x + b$, where $b \in \{-1, 1\}$. Considering a positive integer m coprime to 6, the number of rational points of E over the finite field $\mathbb{F}_{3^m}$ is given by $N = \#E(\mathbb{F}_{3^m}) = 3^m + 1 + \mu b 3^{\frac{m+1}{2}}$, with

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

The embedding degree k of E is then 6.

Choosing $T = 3^m - N = -\mu b 3^{\frac{m+1}{2}} - 1$ and an integer ℓ dividing N, we define the η_T pairing of two points P and Q of the ℓ-torsion $E(\mathbb{F}_{3^m})[\ell]$ as

$$\eta_T(P,Q) = \begin{cases} f_{T,P}(\psi(Q)), & \text{if } T > 0 \text{ (i.e., } \mu b = -1), \\ f_{-T,-P}(\psi(Q)), & \text{if } T < 0 \text{ (i.e., } \mu b = 1), \end{cases}$$

where

- ψ is a distortion map from $E(\mathbb{F}_{3^m})[\ell]$ to $E(\mathbb{F}_{3^{6m}})[\ell]$ defined as $\psi(x,y) = (\rho - x, y\sigma)$ for all $(x,y) \in E(\mathbb{F}_{3^m})[\ell]$,

2. We give here the definition from [11], slightly different from the initial one given in [3].

as given in [11], where ρ and σ are elements of $\mathbb{F}_{3^{6m}}$ satisfying the equations $\rho^3-\rho-b=0$ and $\sigma^2+1=0$.

As already remarked in [20], this allows for representing $\mathbb{F}_{3^{6m}}$ as an extension of $\mathbb{F}_{3^m}$ using the basis $(1,\sigma,\rho,\sigma\rho,\rho^2,\sigma\rho^2)$: $\mathbb{F}_{3^{6m}}=\mathbb{F}_{3^m}[\sigma,\rho]\cong\mathbb{F}_{3^m}[X,Y]/(X^2+1,Y^3-Y-b)$. Hence, all the computations over $\mathbb{F}_{3^{6m}}$ can be replaced by computations over $\mathbb{F}_{3^m}$, as explicitly shown in Appendices E and F.

- $f_{n,P}$, for $n\in\mathbb{N}$ and $P\in E(\mathbb{F}_{3^m})[\ell]$, is a rational function defined over $E(\mathbb{F}_{3^{6m}})[\ell]$ with divisor $(f_{n,P})=n(P)-([n]P)-(n-1)(\mathcal{O})$.

In order to ensure that the obtained pairing values belong to the group of the ℓth roots of unity of $\mathbb{F}^*_{3^{6m}}$, we actually have to compute the *reduced* η_T pairing, defined as $\eta_T(P,Q)^M$, where

$$M=\frac{3^{6m}-1}{N}=(3^{3m}-1)(3^m+1)\left(3^m+1-\mu b3^{\frac{m+1}{2}}\right).$$

In the following, we will refer to this additional step as *final exponentiation*.

One should also note that, in characteristic 3, we have the following relation between the reduced η_T and modified Tate pairings:

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

with $L=-\mu b3^{\frac{m+3}{2}}$. Using v as a shorthand for $\eta_T(P,Q)^M$, we can compute the modified Tate pairing according to the following formula:

$$\hat{e}(P,Q)^M=v^{-2}\left(v^{3^{\frac{m+1}{2}}}\sqrt[3^m]{v^{3^{\frac{m-1}{2}}}}\right)^{-\mu b}.$$

Noting $T'=-\mu bT=3^{\frac{m+1}{2}}+\mu b$ and $P'=[-\mu b]P$, we now have to compute $\eta_T(P,Q)^M=f_{T',P'}(\psi(Q))^M$. Using the Duursma-Lee techniques [16] to simplify the computation of $f_{n,P}$ in Miller's algorithm, we obtain

$$f_{T',P'}(\psi(Q))=\left(\prod_{i=0}^{\frac{m-1}{2}}g_{[3^i]P'}(\psi(Q))^{3^{\frac{m-1}{2}-i}}\right)l_{P'}(\psi(Q)),$$

where

- g_V, for all $V=(x_V,y_V)\in E(\mathbb{F}_{3^m})[\ell]$, is the rational function introduced by Duursma and Lee [16], defined over $E(\mathbb{F}_{3^{6m}})[\ell]$ and having divisor $(g_V)=3(V)+([-3]V)-4(\mathcal{O})$. For all $(x,y)\in E(\mathbb{F}_{3^{6m}})[\ell]$, we have

$$g_V(x,y)=y_V^3y-\left(x_V^3-x+b\right)^2.$$

- l_V, for all $V=(x_V,y_V)\in E(\mathbb{F}_{3^m})[\ell]$, is the equation of the line corresponding to the addition of $[3^{\frac{m+1}{2}}]V$ with $[\mu b]V$, defined for all $(x,y)\in E(\mathbb{F}_{3^{6m}})[\ell]$:

$$l_V(x,y)=y-\lambda y_V(x-x_V)-\mu by_V,$$

with

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

We can also rewrite the equation of l_V as

$$l_V(x,y)=y+\lambda y_V(x_V-x-\nu b),$$

introducing

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

The remaining part of this section will present and discuss various algorithms that can be used to effectively compute the reduced η_T pairing. The next three sections will focus on the computation of $\eta_T(P,Q)$ only, the details of the final exponentiation being given in Section 2.5. Finally, cost evaluations and comparisons will be presented in Section 2.6.

2.2 Direct Approaches

2.2.1 Direct Algorithm

From the expression of $f_{T',P'}$, noting $\tilde{Q}=\psi(Q)$, we can write

$$f_{T',P'}(\tilde{Q})=\left(\cdots\left(g_{P'}(\tilde{Q})^3\cdot g_{[3]P'}(\tilde{Q})\right)^3\cdots\right)^3 g_{\left[3^{\frac{m-1}{2}}\right]P'}(\tilde{Q})\cdot l_{P'}(\tilde{Q}).$$

Noting $P'=(x_{P'},y_{P'})$ and $Q=(x_Q,y_Q)$, we have $[3^i]P'=(x_{P'}^{3^{2i}}-ib,(-1)^iy_{P'}^{3^{2i}})$ and $\tilde{Q}=\psi(Q)=(\rho-x_Q,y_Q\sigma)$. Injecting these in the expressions of $g_{[3^i]P'}$ and $l_{P'}$ and defining $m'=\frac{m-1}{2}$, we obtain

$$g_{[3^i]P'}(\tilde{Q})=(-1)^iy_{P'}^{3^{2i+1}}y_Q\sigma-\left(x_{P'}^{3^{2i+1}}+x_Q+(1-i)b-\rho\right)^2,$$
$$l_{P'}(\tilde{Q})=y_Q\sigma-(-1)^{m'}y_{P'}^{3^{2m'+1}}\left(x_{P'}^{3^{2m'+1}}+x_Q+(1-m')b-\rho\right).$$

An iterative implementation of the η_T pairing following this construction is given in Algorithm 1. The cost of each pseudo-code instruction is given as comments in terms of additions/subtractions (A), multiplications (M), and cubings (C) over the underlying field $\mathbb{F}_{3^m}$.

Algorithm 1 Direct algorithm for computing the η_T pairing.
Input: $P,Q\in E(\mathbb{F}_{3^m})[\ell]$.
Output: $\eta_T(P,Q)\in\mathbb{F}^*_{3^{6m}}$.

1. $y_P\leftarrow-\mu by_P$;
2. $x_P\leftarrow x_P^3$; $y_P\leftarrow y_P^3$; (2C)
3. $t\leftarrow x_P+x_Q+b$; $u\leftarrow y_Py_Q$; (1M, 2A)
4. $R\leftarrow(-t^2+u\sigma-t\rho-\rho^2)^3$; (1M, 2C, 3A)
5. $x_P\leftarrow x_P^9$; $y_P\leftarrow-y_P^9$; (4C)
6. $t\leftarrow x_P+x_Q$; $u\leftarrow y_Py_Q$; (1M, 1A)
7. $S\leftarrow-t^2+u\sigma-t\rho-\rho^2$; (1M)
8. $R\leftarrow R\cdot S$; (6M, 21A)
9. **for** $i\leftarrow 2$ **to** $\frac{m-1}{2}$ **do**
10. $R\leftarrow R^3$; (6C, 6A)
11. $x_P\leftarrow x_P^9-b$; $y_P\leftarrow-y_P^9$; (4C, 1A)
12. $t\leftarrow x_P+x_Q$; $u\leftarrow y_Py_Q$; (1M, 1A)
13. $S\leftarrow-t^2+u\sigma-t\rho-\rho^2$; (1M)
14. $R\leftarrow R\cdot S$; (12M, 59A)

15. **end for**
16. $S \leftarrow -y_P t + y_Q \sigma + y_P \rho$; (1M)
17. $R \leftarrow R \cdot S$; (12M, 51A)
18. **return** R;

A few remarks concerning this algorithm:

- The multiplication by $-\mu b$ on line 1 is for free. Indeed, $-\mu b$ being a constant (1 or -1) for fixed m and b, one can just compute the value of $-\mu b$ when those parameters are chosen, and propagate sign corrections on y_P throughout the whole algorithm.
- Similarly, multiplications by λ, ν, and b do not have any impact on the cost of the algorithm. The values of these constants are known in advance and actually only represent sign changes in the algorithm.
- Since the representation of $-t^2 + u\sigma - t\rho - \rho^2$ as an element of the tower field $\mathbb{F}_{3^{6m}}$ is sparse, the cubing on line 4 involves only one multiplication, two cubings, and three additions over $\mathbb{F}_{3^m}$, as detailed in Appendix E.2.
- Additionally, $(-t^2 + u\sigma - t\rho - \rho^2)^3$ has the same sparsity, and therefore, the product of R and S on line 8 can be computed by means of only six multiplications and 21 additions over $\mathbb{F}_{3^m}$, as per Appendix F.3.
- Inside the loop, the cubing of R on line 10 is computed in six cubings and six additions over $\mathbb{F}_{3^m}$ (Appendix E.1).
- The multiplication of R by S on line 14 involves only 12 multiplications and 59 additions over $\mathbb{F}_{3^m}$, as S is sparse (Appendix F.2,).
- The final product on line 17 is in turn computed by means of 12 multiplications and 51 additions, also due to the sparsity of S, as detailed in Appendix F.2.

2.2.2 Simplification Using Cube Roots

Cubing the intermediate result $R \in \mathbb{F}^*_{3^{6m}}$ at each iteration of Algorithm 1 is quite expensive. But, one can use the fact that, due to the bilinearity of the reduced η_T pairing,

$$\eta_T(P,Q)^M = \left(\eta_T\left(P, \left[3^{-\frac{m-1}{2}}\right]Q\right)^{3^{\frac{m-1}{2}}}\right)^M,$$

to compute instead

$$f_{T',P'}(\tilde{Q})^{3^{\frac{m-1}{2}}} = \left(\prod_{i=0}^{\frac{m-1}{2}} g_{[3^i]P'}(\tilde{Q})^{3^{m-1-i}}\right) l_{P'}(\tilde{Q})^{3^{\frac{m-1}{2}}},$$

with $\tilde{Q} = \psi([3^{-\frac{m-1}{2}}]Q) = (\rho - x_Q^3 - (\nu+1)b, -\lambda y_Q^3 \sigma)$.

Expanding everything, we obtain the following expressions, again with $m' = \frac{m-1}{2}$:

$$g_{[3^i]P'}(\tilde{Q})^{3^{m-1-i}} = -\lambda y_{P'}^{3^i} y_Q^{3^{-i}} \sigma - \left(x_{P'}^{3^i} + x_Q^{3^{-i}} - \nu b - \rho\right)^2,$$

$$l_{P'}(\tilde{Q})^{3^{\frac{m-1}{2}}} = y_Q^{3^{-m'}} \sigma + \lambda y_{P'}^{3^{m'}} \left(x_{P'}^{3^{m'}} + x_Q^{3^{-m'}} - \nu b - \rho\right).$$

This naturally gives another iterative method to compute $\eta_T(P,Q)$, presented in Algorithm 2. Here, the cubings over $\mathbb{F}_{3^{6m}}$ are traded for cube roots (noted R) over $\mathbb{F}_{3^m}$, which can be efficiently computed by means of a specific operator (see Section 3.5 for further details).

Algorithm 2 Simplified algorithm for computing the η_T pairing, with cube roots.
Input: $P, Q \in E(\mathbb{F}_{3^m})[\ell]$.
Output: $\eta_T(P,Q) \in \mathbb{F}^*_{3^{6m}}$.

1. $x_P \leftarrow x_P - \nu b$; (1A)
2. $y_P \leftarrow -\mu b y_P$;
3. $t \leftarrow x_P + x_Q$; $u \leftarrow y_P y_Q$; (1M, 1A)
4. $R \leftarrow -t^2 - \lambda u\sigma - t\rho - \rho^2$; (1M)
5. $x_P \leftarrow x_P^3$; $y_P \leftarrow y_P^3$; (2C)
6. $x_Q \leftarrow \sqrt[3]{x_Q}$; $y_Q \leftarrow \sqrt[3]{y_Q}$; (2R)
7. $t \leftarrow x_P + x_Q$; $u \leftarrow y_P y_Q$; (1M, 1A)
8. $S \leftarrow -t^2 - \lambda u\sigma - t\rho - \rho^2$; (1M)
9. $R \leftarrow R \cdot S$; (6M, 21A)
10. **for** $i \leftarrow 2$ **to** $\frac{m-1}{2}$ **do**
11. $x_P \leftarrow x_P^3$; $y_P \leftarrow y_P^3$; (2C)
12. $x_Q \leftarrow \sqrt[3]{x_Q}$; $y_Q \leftarrow \sqrt[3]{y_Q}$; (2R)
13. $t \leftarrow x_P + x_Q$; $u \leftarrow y_P y_Q$; (1M, 1A)
14. $S \leftarrow -t^2 - \lambda u\sigma - t\rho - \rho^2$; (1M)
15. $R \leftarrow R \cdot S$; (12M, 59A)
16. **end for**
17. $S \leftarrow \lambda y_P t + y_Q \sigma - \lambda y_P \rho$; (1M)
18. $R \leftarrow R \cdot S$; (12M, 51A)
19. **return** R;

2.2.3 Tabulating the Cube Roots

Even if cube roots can be computed with only a slight hardware overhead, it is sometimes advisable to restrict the hardware complexity of the arithmetic unit in order to achieve higher clock frequencies. The previous algorithm can easily be adapted to cube-root-free coprocessors by simply noticing that, as x_Q and $y_Q \in \mathbb{F}_{3^m}$, $x_Q^{3^{-i}} = x_Q^{3^{m-i}}$ and $y_Q^{3^{-i}} = y_Q^{3^{m-i}}$.

Therefore, computing the $m-1$ successive cubings of x_Q and y_Q, it is possible to tabulate the precomputed values of $x_Q^{3^{-i}}$ and $y_Q^{3^{-i}}$, which will be looked up on lines 6 and 12 of Algorithm 2 instead of computing the actual cube roots.

The $m-1$ cube roots of Algorithm 2 are hence traded for $2m-2$ cubings, at the expense of extra registers required to store the tabulated values as $m-1$ elements of $\mathbb{F}_{3^m}$.

This idea, originally suggested by Barreto et al. [18] was for instance applied by Ronan et al. [23] in the case $m \equiv 1 \pmod{12}$, although they curiously do not compute the actual η_T pairing, but the value

$$\eta_T(P, [3^{-m}]Q)^{3^{\frac{m-1}{2}}} = \eta_T(P,Q)^{3^{-\frac{m+1}{2}}}.$$

2.3 Reversed-Loop Approaches

In [18], Barreto et al. suggest reversing the loop to compute the η_T pairing. To that purpose, they introduce a new index $j = 3^{\frac{m-1}{2}} - i$ for the loop. Taking $\tilde{Q} = \psi(Q)$, we find

$$f_{T',P'}(\tilde{Q}) = l_{P'}(\tilde{Q}) \left(\prod_{j=0}^{\frac{m-1}{2}} g_{\left[3^{\frac{m-1}{2}-j}\right]P'}(\tilde{Q})^{3^j} \right).$$

2.3.1 Reversed-Loop Algorithm

Directly injecting the expression of $[3^{\frac{m-1}{2}-j}]P' = (x_{P'}^{3^{-2j-1}} - (\nu+1-j)b, -\lambda(-1)^j y_{P'}^{3^{-2j-1}})$ into the formulas, we obtain

$$l_{P'}(\tilde{Q}) = y_Q\sigma + \lambda y_{P'}\left(x_{P'} + x_Q - \nu b - \rho\right),$$
$$g_{\left[3^{\frac{m-1}{2}-j}\right]P'}(\tilde{Q})^{3^j} = -\lambda y_{P'}^{3^{-j}} y_Q^{3^j}\sigma - \left(x_{P'}^{3^{-j}} + x_Q^{3^j} - \nu b - \rho\right)^2.$$

Following this expression, a third iterative scheme for computing the η_T pairing can be directly devised, as detailed in Algorithm 3. In the case $m \equiv 1 \pmod{12}$, this is the exact same algorithm as described by Barreto et al. [18].

Algorithm 3 Reversed-loop algorithm for computing the η_T pairing, with cube roots.
Input: $P, Q \in E(\mathbb{F}_{3^m})[\ell]$.
Output: $\eta_T(P,Q) \in \mathbb{F}_{3^{6m}}^*$.

1. $x_P \leftarrow x_P - \nu b$; (1A)
2. $y_P \leftarrow -\mu b y_P$;
3. $t \leftarrow x_P + x_Q$; (1A)
4. $R \leftarrow (\lambda y_P t + y_Q\sigma - \lambda y_P\rho)\cdot(-t^2 - \lambda y_P y_Q\sigma - t\rho - \rho^2)$; (6M, 1C, 6A)
5. **for** $j \leftarrow 1$ **to** $\frac{m-1}{2}$ **do**
6. $x_P \leftarrow \sqrt[3]{x_P}$; $y_P \leftarrow \sqrt[3]{y_P}$; (2R)
7. $x_Q \leftarrow x_Q^3$; $y_Q \leftarrow y_Q^3$; (2C)
8. $t \leftarrow x_P + x_Q$; $u \leftarrow y_P y_Q$; (1M, 1A)
9. $S \leftarrow -t^2 - \lambda u\sigma - t\rho - \rho^2$; (1M)
10. $R \leftarrow R \cdot S$; (12M, 59A)
11. **end for**
12. **return** R;

It is to be noted that given the expression of its operands, the multiplication on line 4 is computed by means of only six multiplications, one cubing, and six additions over $\mathbb{F}_{3^m}$, as described in Appendix F.4.

As for Algorithm 2, Algorithm 3 also requires the computation of cube roots. A similar technique of precomputation and tabulation of the cube roots due to successive cubings of x_P and y_P can also be used, although we will not detail it here.

2.3.2 Eliminating the Cube Roots

The apparent duality between Algorithms 2 and 3 can be exploited to find another cube-free algorithm, still based on the reversed loop but similar to Algorithm 1.

For that purpose, we once again compute the reduced η_T pairing of P and Q as

$$\eta_T(P,Q)^M = \left(\eta_T\left(P, \left[3^{-\frac{m-1}{2}}\right]Q\right)^{3^{\frac{m-1}{2}}}\right)^M.$$

Noting $\tilde{Q} = \psi([3^{-\frac{m-1}{2}}]Q)$, the reversed loop becomes

$$\begin{aligned} f_{T',P'}(\tilde{Q})^{3^{\frac{m-1}{2}}} &= l_{P'}(\tilde{Q})^{3^{\frac{m-1}{2}}} \left(\prod_{j=0}^{\frac{m-1}{2}} g_{\left[3^{\frac{m-1}{2}-j}\right]P'}(\tilde{Q})^{3^{\frac{m-1}{2}+j}} \right) \\ &= l_{P'}(\tilde{Q})^{3^{\frac{m-1}{2}}} \left(\prod_{j=0}^{\frac{m-1}{2}} h_{j,P'}(\tilde{Q})^{3^{\frac{m-1}{2}-j}} \right) \\ &= \left(\cdots \left(\left(l_{P'}(\tilde{Q}) \cdot h_{0,P'}(\tilde{Q}) \right)^3 h_{1,P'}(\tilde{Q}) \right)^3 \cdots \right)^3 \\ &\quad \cdot h_{\frac{m-1}{2},P'}(\tilde{Q}), \end{aligned}$$

with the rational function $h_{j,P'}(\tilde{Q})$ defined as

$$h_{j,P'}(\tilde{Q}) = g_{\left[3^{\frac{m-1}{2}-j}\right]P'}(\tilde{Q})^{3^{2j}}.$$

We then compute the explicit expressions of $l_P(\tilde{Q})$ and $h_{j,P'}(\tilde{Q})$:

$$l_{P'}(\tilde{Q}) = -\lambda y_Q^3\sigma + \lambda y_{P'}\left(x_{P'} + x_Q^3 + b - \rho\right),$$
$$h_{j,P'}(\tilde{Q}) = (-1)^j y_{P'} y_Q^{3^{2j+1}}\sigma - \left(x_{P'} + x_Q^{3^{2j+1}} + (1-j)b - \rho\right)^2.$$

Algorithm 4 is a direct implementation of the previous computation of $\eta_T(P,Q)$. Similarly to Algorithm 1, it uses cubings over $\mathbb{F}_{3^{6m}}$ in order to avoid the cube roots of Algorithm 3. In the case $m \equiv 1 \pmod{12}$, this algorithm corresponds to the η_T pairing computation described by Beuchat et al. [25].

Algorithm 4 Cube-root-free reversed-loop algorithm for computing the η_T pairing.
Input: $P, Q \in E(\mathbb{F}_{3^m})[\ell]$.
Output: $\eta_T(P,Q) \in \mathbb{F}_{3^{6m}}^*$.

1. $x_P \leftarrow x_P + b$; (1A)
2. $y_P \leftarrow -\mu b y_P$;
3. $x_Q \leftarrow x_Q^3$; $y_Q \leftarrow y_Q^3$; (2C)
4. $t \leftarrow x_P + x_Q$; (1A)
5. $R \leftarrow (\lambda y_P t - \lambda y_Q\sigma - \lambda y_P\rho)\cdot(-t^2 + y_P y_Q\sigma - t\rho - \rho^2)$; (6M, 1C, 6A)
6. **for** $j \leftarrow 1$ **to** $\frac{m-1}{2}$ **do**
7. $R \leftarrow R^3$; (6C, 6A)
8. $x_Q \leftarrow x_Q^9 - b$; $y_Q \leftarrow -y_Q^9$; (4C, 1A)
9. $t \leftarrow x_P + x_Q$; $u \leftarrow y_P y_Q$; (1M, 1A)
10. $S \leftarrow -t^2 + u\sigma - t\rho - \rho^2$; (1M)
11. $R \leftarrow R \cdot S$; (12M, 59A)
12. **end for**
13. **return** R;

2.4 Loop Unrolling

Granger et al. [28] proposed a loop unrolling technique for the Duursma-Lee algorithm. They exploit the sparsity of g_V in order to reduce the number of multiplications over $\mathbb{F}_{3^m}$, exactly in the same way as we reduced the first two iterations of Algorithms 1 and 2.

By noting that $h_{j,P'}(\tilde{Q})^3$ is also as sparse as $h_{j,P'}(\tilde{Q})$ (for details, see Appendix E.2), we can apply the same approach to Algorithm 4.

In two successive iterations $2j'-1$ and $2j'$ of the loop, for $1 \le j' \le \lfloor \frac{m-1}{4} \rfloor$, we compute the new value of R as

$$R \leftarrow \left(R^3 \cdot h_{2j'-1,P'}(\tilde{Q})\right)^3 \cdot h_{2j',P'}(\tilde{Q}) = R^9 \cdot h_{2j'-1,P'}(\tilde{Q})^3 \cdot h_{2j',P'}(\tilde{Q}).$$

The values of $h_{2j'-1,P'}(\tilde{Q})$ and $h_{2j',P'}(\tilde{Q})$, computed at iterations $2j'-1$ and $2j'$, respectively, are both of the form $-t^2 + u\sigma - t\rho - \rho^2$. Therefore, given t and u, the computation of $h_{2j'-1,P'}(\tilde{Q})^3$ requires only one multiplication, two cubings, and three additions over $\mathbb{F}_{3^m}$, as per Appendix E.2. Similarly, the product of $h_{2j'-1,P'}(\tilde{Q})^3$ and $h_{2j',P'}(\tilde{Q})$ can be computed by means of only six multiplications and 21 additions, as explained in Appendix F.3. Finally, multiplying this product by R^9 requires a full $\mathbb{F}_{3^{6m}}$ multiplication, which can be performed with 15 multiplications and 67 additions over $\mathbb{F}_{3^m}$ (see Appendix F.1).

Hence, the cost of such a double iteration would be of 25 multiplications (neglecting the other operations), whereas two iterations of the original loop from Algorithm 4 cost $2 \times 14 = 28$ multiplications.

Following this, we can unroll the main loop of Algorithm 4 in order to save multiplications by computing two iterations at a time. The resulting scheme is shown in Algorithm 5, for the case where $\frac{m-1}{2}$ is even. If $\frac{m-1}{2}$ is actually odd, one just has to restrict the loop on j' from 1 to $\frac{m-3}{4}$ and compute the last product by an extra iteration of the original loop, for the additional cost of 14 multiplications, 10 cubings, and 68 additions over $\mathbb{F}_{3^m}$.

Algorithm 5 Unrolled loop for the computation of the η_T pairing when $\frac{m-1}{2}$ is even.
Input: $P, Q \in E(\mathbb{F}_{3^m})[\ell]$.
Output: $\eta_T(P,Q) \in \mathbb{F}^*_{3^{6m}}$.

1. $x_P \leftarrow x_P + b$; (1A)
2. $y_P \leftarrow -\mu b y_P$;
3. $x_Q \leftarrow x_Q^3$; $y_Q \leftarrow y_Q^3$; (2C)
4. $t \leftarrow x_P + x_Q$; (1A)
5. $R \leftarrow (\lambda y_P t - \lambda y_Q \sigma - \lambda y_P \rho) \cdot (-t^2 + y_P y_Q \sigma - t\rho - \rho^2)$; (6M, 1C, 6A)
6. **for** $j' \leftarrow 1$ **to** $\frac{m-1}{4}$ **do**
7. $R \leftarrow R^9$; (12C, 12A)
8. $x_Q \leftarrow x_Q^9 - b$; $y_Q \leftarrow y_Q^9$; (4C, 1A)
9. $t \leftarrow x_P + x_Q$; $u \leftarrow y_P y_Q$; (1M, 1A)
10. $S \leftarrow (-t^2 - u\sigma - t\rho - \rho^2)^3$; (1M, 2C, 3A)
11. $x_Q \leftarrow x_Q^9 - b$; $y_Q \leftarrow y_Q^9$; (4C, 1A)
12. $t \leftarrow x_P + x_Q$; $u \leftarrow y_P y_Q$; (1M, 1A)
13. $S' \leftarrow -t^2 + u\sigma - t\rho - \rho^2$; (1M)
14. $S \leftarrow S \cdot S'$; (6M, 21A)
15. $R \leftarrow R \cdot S$; (15M, 67A)
16. **end for**
17. **return** R;

It is to be noted that one could also straightforwardly apply a similar loop unrolling technique to Algorithm 1. However, we will not detail this point any further, for it is rigorously identical to the previous case.

2.5 Final Exponentiation

As already stated in Section 2.1, the η_T pairing has to be reduced in order to be uniquely defined and not only up to ℓth powers. This reduction is achieved by means of a final exponentiation, in which $\eta_T(P,Q)$ is raised to the Mth power, with

$$M = (3^{3m}-1)(3^m+1)\left(3^m + 1 - \mu b 3^{\frac{m+1}{2}}\right).$$

For this particular exponentiation, we use the scheme presented by Shirase et al. [29].

Taking $U = \eta_T(P,Q) \in \mathbb{F}^*_{3^{6m}}$, we first compute $U^{3^{3m}-1}$. Writing U as $U_0 + U_1\sigma$, where U_0 and $U_1 \in \mathbb{F}^*_{3^{3m}}$, and seeing that

$$U^{3^{3m}} = U_0 - U_1\sigma,$$
$$U^{-1} = \frac{U_0 - U_1\sigma}{U_0^2 + U_1^2},$$

we obtain the following expression for $U^{3^{3m}-1}$:

$$U^{3^{3m}-1} = \frac{(U_0^2 - U_1^2) + U_0U_1\sigma}{U_0^2 + U_1^2}.$$

This computation is directly implemented in Algorithm 6, where the multiplication (line 3), the squarings (lines 1 and 2), and the inversion (line 5) over $\mathbb{F}_{3^{3m}}$ are performed following the algorithms presented in Appendices B, C, and D (which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TC.2008.103), respectively.

Algorithm 6 Computation of $U^{3^{3m}-1}$ in $\mathbb{F}^*_{3^{6m}}$.
Input: $U = u_0 + u_1\sigma + u_2\rho + u_3\sigma\rho + u_4\rho^2 + u_5\sigma\rho^2 \in \mathbb{F}^*_{3^{6m}}$.
Output: $V = U^{3^{3m}-1} \in T_2(\mathbb{F}_{3^{3m}})$.

1. $m_0 \leftarrow (u_0 + u_2\rho + u_4\rho^2)^2$; (5M, 7A)
2. $m_1 \leftarrow (u_1 + u_3\rho + u_5\rho^2)^2$; (5M, 7A)
3. $m_2 \leftarrow (u_0 + u_2\rho + u_4\rho^2) \cdot (u_1 + u_3\rho + u_5\rho^2)$; 6M, 12A)
4. $a_0 \leftarrow m_0 - m_1$; $a_1 \leftarrow m_0 + m_1$; (6A)
5. $i \leftarrow a_1^{-1}$; (12M, 11A, 1I)
6. $V_0 \leftarrow a_0 \cdot i$; (6M, 12A)
7. $V_1 \leftarrow m_2 \cdot i$; (6M, 12A)
8. **return** $V_0 + V_1\sigma$;

One can then remark that

$$\frac{(U_0^2 - U_1^2)^2 + (U_0U_1)^2}{(U_0^2 + U_1^2)^2} = 1,$$

which means that $U^{3^{3m}-1}$ is in fact an element of $T_2(\mathbb{F}_{3^{3m}})$, where $T_2(\mathbb{F}_{3^{3m}}) = \{X_0 + X_1\sigma \in \mathbb{F}^*_{3^{6m}} : X_0^2 + X_1^2 = 1\}$ is the torus as introduced by Granger et al. for the case of the Tate pairing in [28].

This is a crucial point here, since arithmetic on the torus $T_2(\mathbb{F}_{3^{3m}})$ is much simpler than arithmetic on $\mathbb{F}^*_{3^{6m}}$. Thus, given $U \in T_2(\mathbb{F}_{3^{3m}})$, Algorithm 7 computes U^{3^m+1} in only nine multiplications and 18 or 19 (depending on the value of m modulo 6) additions over $\mathbb{F}_{3^m}$.

Algorithm 7 Computation of U^{3^m+1} in the torus $T_2(\mathbb{F}_{3^{3m}})$.
Input: $U = u_0 + u_1\sigma + u_2\rho + u_3\sigma\rho + u_4\rho^2 + u_5\sigma\rho^2 \in T_2(\mathbb{F}_{3^{3m}})$.
Output: $V = U^{3^m+1} \in T_2(\mathbb{F}_{3^{3m}})$.

1. $a_0 \leftarrow u_0 + u_1$; $a_1 \leftarrow u_2 + u_3$; $a_2 \leftarrow u_4 - u_5$; (3A)
2. $m_0 \leftarrow u_0 \cdot u_4$; $m_1 \leftarrow u_1 \cdot u_5$; $m_2 \leftarrow u_2 \cdot u_4$; (3M)
3. $m_3 \leftarrow u_3 \cdot u_5$; $m_4 \leftarrow a_0 \cdot a_2$; $m_5 \leftarrow u_1 \cdot u_2$; (3M)
4. $m_6 \leftarrow u_0 \cdot u_3$; $m_7 \leftarrow a_0 \cdot a_1$; $m_8 \leftarrow a_1 \cdot a_2$; (3M)
5. $a_3 \leftarrow m_5 + m_6 - m_7$; $a_4 \leftarrow -m_2 - m_3$; (3A)
6. $a_5 \leftarrow -m_2 + m_3$; $a_6 \leftarrow -m_0 + m_1 + m_4$; (3A)
7. **if** $m \equiv 1 \pmod 6$ **then**

TABLE 1
Cost of the Presented Algorithms for Computing the η_T Pairing and the Final Exponentiation, in Terms of Operations over the Underlying Field $\mathbb{F}_{3^m}$

		Additions	Multiplications	Cubings	Cube roots	Inversions
Direct loop	No cube root (Algorithm 1)	$67\frac{m-1}{2}+11$	$7m+2$	$5m-7$	0	0
	With cube roots (Algorithm 2)	$30m-15$	$7m+2$	$m-1$	$m-1$	0
Reversed loop	With cube roots (Algorithm 3)	$30m-22$	$7m-1$	m	$m-1$	0
	No cube root (Algorithm 4)	$67\frac{m-1}{2}+8$	$7m-1$	$5m-2$	0	0
Unrolled loop (Algorithm 5)	$\frac{m-1}{2}$ is even	$107\frac{m-1}{4}+8$	$25\frac{m-1}{4}+6$	$11\frac{m-1}{2}+3$	0	0
	$\frac{m-1}{2}$ is odd	$107\frac{m-3}{4}+76$	$25\frac{m-3}{4}+20$	$11\frac{m-1}{2}+2$	0	0
Final exp. (Algorithm 8)	$m \equiv 1 \pmod 6$	$3m+175$	73	$3m+3$	0	1
	$m \equiv 5 \pmod 6$	$3m+173$	73	$3m+3$	0	1

8. $v_0 \leftarrow 1 + m_0 + m_1 + ba_4$; (3A)
9. $v_1 \leftarrow bm_5 - bm_6 + a_6$; (2A)
10. $v_2 \leftarrow -a_3 + a_4$; (1A)
11. $v_3 \leftarrow m_8 + a_5 - ba_6$; (2A)
12. $v_4 \leftarrow -ba_3 - ba_4$; (1A)
13. $v_5 \leftarrow bm_8 + ba_5$; (1A)
14. **else if** $m \equiv 5 \pmod 6$ **then**
15. $v_0 \leftarrow 1 + m_0 + m_1 - ba_4$; (3A)
16. $v_1 \leftarrow -bm_5 + bm_6 + a_6$; (2A)
17. $v_2 \leftarrow a_3$;
18. $v_3 \leftarrow m_8 + a_5 + ba_6$; (2A)
19. $v_4 \leftarrow -ba_3 - ba_4$; (1A)
20. $v_5 \leftarrow -bm_8 - ba_5$; (1A)
21. **end if**
22. **return** $v_0 + v_1\sigma + v_2\rho + v_3\sigma\rho + v_4\rho^2 + v_5\sigma\rho^2$;

Finally, Algorithm 8 implements the complete final exponentiation. Given $U \in \mathbb{F}^*_{3^{6m}}$ as input, it first computes $U^{3^{3m}-1}$ due to Algorithm 6, then calls Algorithm 7 to obtain $U^{(3^{3m}-1)(3^m+1)}$. Then, $W = U^{(3^{3m}-1)(3^m+1)3^{(m+1)/2}}$ is computed by successive cubings over $\mathbb{F}_{3^{6m}}$, while $V = U^{(3^{3m}-1)(3^m+1)(3^m+1)}$ is obtained by a second call to Algorithm 7. The value to be computed is then

$$U^M = \begin{cases} V \cdot W^{-1}, & \text{when } \mu b = 1, \\ V \cdot W, & \text{when } \mu b = -1, \end{cases}$$

hence, the computation of $W' = W^{-\mu b}$ on line 8. When $\mu b = -1$, this is just a dummy operation, but it is an actual inversion when $\mu b = 1$. However, as $W \in T_2(\mathbb{F}_{3^{3m}})$, writing $W = W_0 + W_1\sigma$, we have

$$W^{-1} = \frac{W_0 - W_1\sigma}{W_0^2 + W_1^2} = W_0 - W_1\sigma.$$

Inversion over $T_2(\mathbb{F}_{3^{3m}})$ is therefore completely free, as it suffices to propagate the sign corrections in the final product $V \cdot W'$, implemented as a full multiplication over $\mathbb{F}^*_{3^{6m}}$.

Algorithm 8 Final exponentiation of the reduced η_T pairing [29].
Input: $U = u_0 + u_1\sigma + u_2\rho + u_3\sigma\rho + u_4\rho^2 + u_5\sigma\rho^2 \in \mathbb{F}^*_{3^{6m}}$.
Output: $U^M \in T_2(\mathbb{F}_{3^{3m}}) \subset \mathbb{F}^*_{3^{6m}}$, with the exponent $M = (3^{3m}-1)(3^m+1)(3^m+1-\mu b 3^{\frac{m+1}{2}})$.

1. $V \leftarrow U^{3^{3m}-1}$; (40M, 67A, 1I)
2. $V \leftarrow V^{3^m+1}$; (9M, 18 or 19A)
3. $W \leftarrow V$;
4. **for** $i \leftarrow 1$ **to** $\frac{m+1}{2}$ **do**
5. $W \leftarrow W^3$; (6C, 6A)
6. **end for**
7. $V \leftarrow V^{3^m+1}$; (9M, 18 or 19A)
8. $W' \leftarrow W^{-\mu b}$;
9. **return** $V \cdot W'$; (15M, 67A)

2.6 Overall Cost Evaluations and Comparisons

The costs of all the previously detailed algorithms are summarized in Table 1, in terms of additions (or subtractions), multiplications, cubings, cube roots, and inversions over $\mathbb{F}_{3^m}$.

From this table, we can see that the additional cost for cube-root-free algorithms is approximately $4m$ extra cubings and $7m/2$ extra additions, when compared to the equivalent algorithms with cube roots. The choice of a type of algorithm instead of the other will therefore depend on the practicality of the computation of cube roots in the given finite field $\mathbb{F}_{3^m}$ (see the discussion in Section 3.5).

This table also shows a slight superiority of reversed-loop algorithms versus direct-loop approaches. This is the reason why we chose to apply the loop unrolling technique to Algorithm 4.

The advantage of such a loop unrolling becomes also clearer when looking at Table 1. From Algorithm 4 to Algorithm 5, we trade approximately $27m/4$ additions and $3m/4$ multiplications for $m/2$ cubings over $\mathbb{F}_{3^m}$.

The costs of these algorithms for $m = 97$, on which we focus more closely in this paper, is given in Table 2. As detailed in Section 3.2, we can compute the inversion over $\mathbb{F}_{3^{97}}$ according to Fermat's little theorem in nine multiplications and 96 cubings, which allows us to express these costs in terms of additions, multiplications, cubings, and cube roots only. The total number of operations for the complete computation of the reduced η_T pairing, using Algorithm 5 for the η_T pairing and Algorithm 5 for the final exponentiation, is also given.

3 A Coprocessor for Arithmetic over $\mathbb{F}_{3^m}$

The η_T pairing calculation in characteristic three requires addition, multiplication, cubing, inversion, and sometimes

TABLE 2
Cost Evaluations of the Reduced η_T Pairing for $m = 97$

		A	M	C	R
Direct loop	(Algorithm 1)	3227	681	478	0
	(Algorithm 2)	2895	681	96	96
Reversed loop	(Algorithm 3)	2888	678	97	96
	(Algorithm 4)	3224	678	483	0
Unrolled loop	(Algorithm 5)	2576	606	531	0
Final exp.	(Algorithm 8)	466	82	390	0
Total	(Algorithms 5 and 8)	3042	688	921	0

Inversion over $\mathbb{F}_{3^{97}}$ is carried out according to Fermat's little theorem in nine multiplications and 96 cubings.

cube root extraction over $\mathbb{F}_{3^m}$. We propose here a unified arithmetic operator that implements the required operations and describe a hardware accelerator for pairing-based cryptography.

In the following, elements of the field extension $\mathbb{F}_{3^m}$ will be represented using a polynomial basis. Given a degree-m irreducible polynomial $f(x) \in \mathbb{F}_3[x]$, we have $\mathbb{F}_{3^m} \cong \mathbb{F}_3[x]/(f(x))$. Each element of $\mathbb{F}_{3^m}$ will then be represented as a polynomial $p(x)$ of degree $(m-1)$ and coefficients in $\mathbb{F}_3$:

$$p(x) = p_{m-1}x^{m-1} + \cdots + p_1 x + p_0.$$

Several researchers reported implementations of the Tate and η_T pairings on a supersingular curve defined on the field $\mathbb{F}_{3^{97}}$. Therefore, we discuss the implementation of Algorithm 5 for the field $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$ and the curve $y^2 = x^3 - x + 1$ (i.e., $b = 1$) on our coprocessor.

It is nonetheless important to note that the architectures and algorithms presented here can be easily adapted to different parameters. For instance, a different irreducible polynomial $f(x)$, a different field extension degree m, or even a different characteristic p (cubing and cube root extraction, being, respectively, Frobenius and inverse Frobenius maps in characteristic three, then replaced by raising to the pth power and pth root extraction).

3.1 Multiplication over $\mathbb{F}_{3^m}$

Three families of algorithms allow one to compute $d0(x) \cdot d1(x) \bmod f(x)$ (see, for instance, [30], [31], and [32] for an account of modular multiplication). In parallel-serial schemes, a single coefficient of the multiplier $d0(x)$ is processed at each step. This leads to small operators performing a multiplication in m clock cycles. Parallel multipliers compute a degree-$(2m-2)$ polynomial and carry out a final modular reduction. They achieve a higher throughput at the price of a larger circuit area. By processing D coefficients of an operand at each clock cycle, array multipliers, introduced by Song and Parhi [33], offer a good trade-off between computation time and circuit area and are at the heart of several pairing coprocessors (see, for instance, [19], [20], [22], [23], [25], and [34]).

Depending on the order in which coefficients of $d0(x)$ are processed, array multipliers can be implemented according to two schemes: most significant element (MSE) first and least significant element (LSE) first. Algorithm 9 summarizes the MSE-first scheme proposed by Shu et al. [22]. Fig. 1a illustrates the architecture of this operator for $D = 3$. It mainly consists of three Partial Product Generators (PPGs), three modulo $f(x)$ reduction units, a multioperand adder, and registers to store operands and intermediate results. Five bits allow for the control of the multiplier. If the irreducible polynomial over $\mathbb{F}_{3^m}$ is a trinomial or a pentanomial, modulo $f(x)$ operations are easy to implement. Consider for instance $f(x) = x^{97} + x^{12} + 2$ and let $u(x) = x \cdot d1(x)$ be a degree-97 polynomial. It suffices to remove $u_{97} \cdot f(x) = u_{97}x^{97} + u_{97}x^{12} + 2u_{97}$ from $u(x)$ to get $u(x) \bmod f(x)$. This involves only two multiplications and two subtractions over $\mathbb{F}_3$, namely $u_{12} - 1 \cdot u_{97}$ and $u_0 - 2 \cdot u_{97}$.

Algorithm 9 Multiplication over $\mathbb{F}_{3^m}$ [22].
Input: A degree-m monic polynomial $f(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_1 x + f_0$ and two degree-$(m-1)$ polynomials $d0(x)$ and $d1(x)$. A parameter D that defines the number of coefficients of $d0(x)$ processed at each clock cycle. The algorithm requires a degree-$(m-1)$ polynomial $a(x)$ for inter mediate computations.
Output: $p(x) = d0(x)d1(x) \bmod f(x)$
1. $p(x) \leftarrow 0$;
2. **for** $i \leftarrow \lceil m/D \rceil - 1$ **downto** 0 **do**
3. $\quad a(x) \leftarrow \sum_{j=0}^{D-1} (d0_{Di+j} \cdot d1(x) \cdot x^j) \bmod f(x)$;
4. $\quad p(x) \leftarrow a(x) + (p(x) \cdot x^D \bmod f(x))$;
5. **end for**
6. **return** $p(x)$;

Elements of $\mathbb{F}_3$ are often represented as 2-bit unsigned integers. Let $d0_i = 2d0_i^H + d0_i^L$ and $d1_j = 2d1_j^H + d1_j^L$. Multiplication over $\mathbb{F}_3 = \{0, 1, 2\}$ is then defined as follows:

$$d0_i \cdot d1_j = 2\left(d0_i^H d1_j^L \vee d0_i^L d1_j^H\right) + \left(d0_i^L d1_j^L \vee d0_i^H d1_j^H\right),$$

and can be implemented by means of two 4-input Lookup Tables (LUTs). Since $d0_i$ multiplies all coefficients of $d1$, the fan-out of our array multiplier is equal to $2m$.

However, a careful encoding of the elements of $\mathbb{F}_3$ can reduce the fan-out of the operator [35]. Since $2 \equiv -1 (\bmod 3)$, we take advantage of the borrow-save system [36] in order to represent the elements of $\mathbb{F}_3 = \{0, 1, -1\}$: $d0_i$ is encoded by a positive bit $d0_i^+$ and a negative bit $d0_i^-$ such that $d0_i = d0_i^+ - d0_i^-$. Multiplication over $\mathbb{F}_3$ is now defined by

$$\begin{aligned} d0_i \cdot d1_j = &\left(\left(1 - d1_j^-\right) d1_j^+ d0_i^+ \vee d1_j^- \left(1 - d1_j^+\right)\left(1 - d0_i^+\right)\right) \\ &- \left(\left(1 - d1_j^-\right) d1_j^+ d0_i^- \vee d1_j^- \left(1 - d1_j^+\right)\left(1 - d0_i^-\right)\right), \end{aligned}$$

and requires two 3-input LUTs: the first one depends on $d0_i^+$, and the second one on $d0_i^-$. Thus, the fan-out of the array multiplier is now equal to m. Since it is performed component-wise, addition over $\mathbb{F}_{3^m}$ is also a rather straightforward operation. If elements of $\mathbb{F}_3$ are represented by 2 bits, addition modulo 3 is, for instance, carried out by means of two 4-input LUTs.

3.2 Inversion over $\mathbb{F}_{3^m}$

The final exponentiation of the η_T pairing involves a single inversion over $\mathbb{F}_{3^m}$. Instead of designing a specific operator based on the Extended Euclidean Algorithm (EEA), we suggest to keep the circuit area as small as possible by performing this inversion according to Fermat's little

theorem and Itoh and Tsujii's work [37] (Algorithm 10). Since this scheme requires only multiplications and cubings over $\mathbb{F}_{3^m}$, we do not have to include dedicated hardware for inversion in our coprocessor.

Starting with an element d of $\mathbb{F}_{3^m}$, $d \neq 0$, we first raise it to the power of the base-3 repunit $(3^{m-1}-1)/2$ to obtain r. This particular powering can be achieved using only $m-2$ cubings over $\mathbb{F}_{3^m}$ and a few multiplications over $\mathbb{F}_{3^m}$ as detailed below. By cubing r and then multiplying the result by d, we successively obtain

$$u = d^{(3^{m-3})/2},$$
$$v = d^{(3^{m-1})/2}.$$

A final product gives us the result

$$u \cdot v = d^{(3^{m-3})/2} \cdot d^{(3^{m-1})/2} = d^{3^{m-2}} = d^{-1}.$$

Since $v \neq 0$ and $v^2 = d^{3^m-1} = 1$, $v \in \mathbb{F}_3$ and this operation could be performed in a single clock cycle at the price of a modification of our MSE-first multiplier: adding an extra control bit and a multiplexer allows one to select the value of the coefficient $d0_{3i}$ between its normal value (the D most significant coefficients of the multiplier) and the D least significant coefficients of the multiplier. Indeed, as $v \in \mathbb{F}_3$, its coefficients v_i are zero for all $i \neq 0$. Therefore, we only need v_0 to compute the final multiplication $u \cdot v = u \cdot v_0$. As our multiplier operates in a most-significant-coefficient-first fashion, instead of performing the full multiplication over $\mathbb{F}_{3^m}$, this multiplexer would allow us to bypass the whole shift register mechanism and compute the product $u \cdot v$ in a single iteration of the multiplier. Since we consider $m = 97$ for our implementation, this trick would allow us to save only $\lceil m/D \rceil - 1 = \lceil 97/3 \rceil - 1 = 32$ clock cycles at the price of a longer critical path and a larger control word. Thus, we do not include this modification in our coprocessor.

Algorithm 10 Inversion over $\mathbb{F}_{3^m}$.
Input: A positive integer m, and $d \in \mathbb{F}_{3^m}$, $d \neq 0$.
Output: $d^{-1} \in \mathbb{F}_{3^m}$.
1. $r \leftarrow d^{(3^{m-1}-1)/2}$; (see Algorithm 11)
2. $u \leftarrow r^3$; (1C)
3. $v \leftarrow u \cdot d$; (1M)
4. **return** $u \cdot v$; (1M)

As already shown in [38] and [39], addition chains can prove to be perfectly suited to raise elements of $\mathbb{F}_{3^m}$ to particular powers, such as the radix-3 repunit $(3^{m-1}-1)/2$ required by our inversion algorithm. In the following, we will restrict ourselves to Brauer-type addition chains,[3] whose definition follows.

A Brauer-type addition chain C of length l is a sequence of l integers $S = (j_1, \ldots, j_l)$ such that $0 \leq j_i < i$ for all $1 \leq i \leq l$. We can then construct another sequence $(n_0, \ldots, n_l)$ satisfying

$$\begin{cases} n_0 = 1, \\ n_i = n_{i-1} + n_{j_i}, \text{ for all } 1 \leq i \leq l. \end{cases}$$

3. Brauer-type addition chains are proved to be optimal for all numbers up to and including 12,508 [40], which is more than enough for our needs.

C is said to *compute* n_l, the last element of the sequence. From [40], we also have the following additional property, for all $1 \leq l' \leq l$:

$$\sum_{i=1}^{l'} n_{j_i} = n_{l'} - 1.$$

Moreover, we can see that we have, for $n \leq n'$,

$$d^{(3^{n+n'}-1)/2} = d^{(3^n-1)/2} \cdot \left(d^{(3^{n'}-1)/2}\right)^{3^n}.$$

Consequently, given a Brauer-type addition chain C of length l for $m-1$, we can compute the required $d^{(3^{m-1}-1)/2}$ as shown in Algorithm 11. This algorithm simply ensures that, for each iteration i, we have $z_i = d^{(3^{n_i}-1)/2}$, where $(n_0, \ldots, n_l)$ is the integer sequence associated with the addition chain C, verifying $n_l = m-1$. It requires l multiplications and $n_{j_1} + \cdots + n_{j_l} = m-2$ cubings over $\mathbb{F}_{3^m}$.

Algorithm 11 Computation of $d^{(3^{m-1}-1)/2}$ over $\mathbb{F}_{3^m}$.
Input: A positive integer m, $d \in \mathbb{F}_{3^m}$, $d \neq 0$, a Brauer-type addition chain $S = (j_1, \ldots, j_l)$ for $m-1$, and the integer sequence $(n_0, \ldots, n_l)$ associated with C.
Output: $d^{(3^{m-1}-1)/2} \in \mathbb{F}_{3^m}$.
1. $z_0 \leftarrow d$;
2. **for** $i \leftarrow 1$ **to** l **do**
3. $z_i \leftarrow z_{j_i} \cdot z_{i-1}^{3^{n_{j_i}}}$; (1M, n_{j_i}C)
4. **end for**
5. **return** z_l;

Therefore, our inversion scheme requires a total of $l+2$ multiplications and $m-1$ cubings over $\mathbb{F}_{3^m}$. For $m = 97$, an addition chain of length $l = 7$ allows us to compute $d^{(3^{96}-1)/2}$, and the overall cost of inversion is equal to nine multiplications and 96 cubings over $\mathbb{F}_{3^{97}}$.

3.3 Cubing over $\mathbb{F}_{3^m}$

Cubing over $\mathbb{F}_{3^m}$ consists in reducing the following expression modulo $f(x)$:

$$c(x) = d(x)^3 \bmod f(x) = \sum_{i=0}^{m-1} d_i x^{3i} \bmod f(x).$$

This general expression can be seen as a sum of D' elements of $\mathbb{F}_{3^m}$. The coefficients of those polynomials can be directly matched to the coefficients of the operand, possibly multiplied by 2. Thus, cubing requires a multi-operand adder and some extra wiring for the permutation of the coefficients. Multiplication by 2 consists in swapping the positive and negative bits of an element of $\mathbb{F}_3$. For instance, if $f(x) = x^{97} + x^{12} + 2$, we have to compute a sum of $D' = 3$ operands:

$$\begin{aligned} \nu_0(x) &= d_{32}x^{96} + 2d_{60}x^{95} + d_{88}x^{94} + \cdots \\ &\quad + d_1x^3 + d_{33}x^2 + 2d_{61}x + d_0, \\ \nu_1(x) &= d_{64}x^{95} + d_{92}x^{94} + \cdots + d_{90}x^3 + d_{65}x + d_{89}, \\ \nu_2(x) &= d_{96}x^{94} + \cdots + d_{94}x^3 + d_{93}, \end{aligned}$$

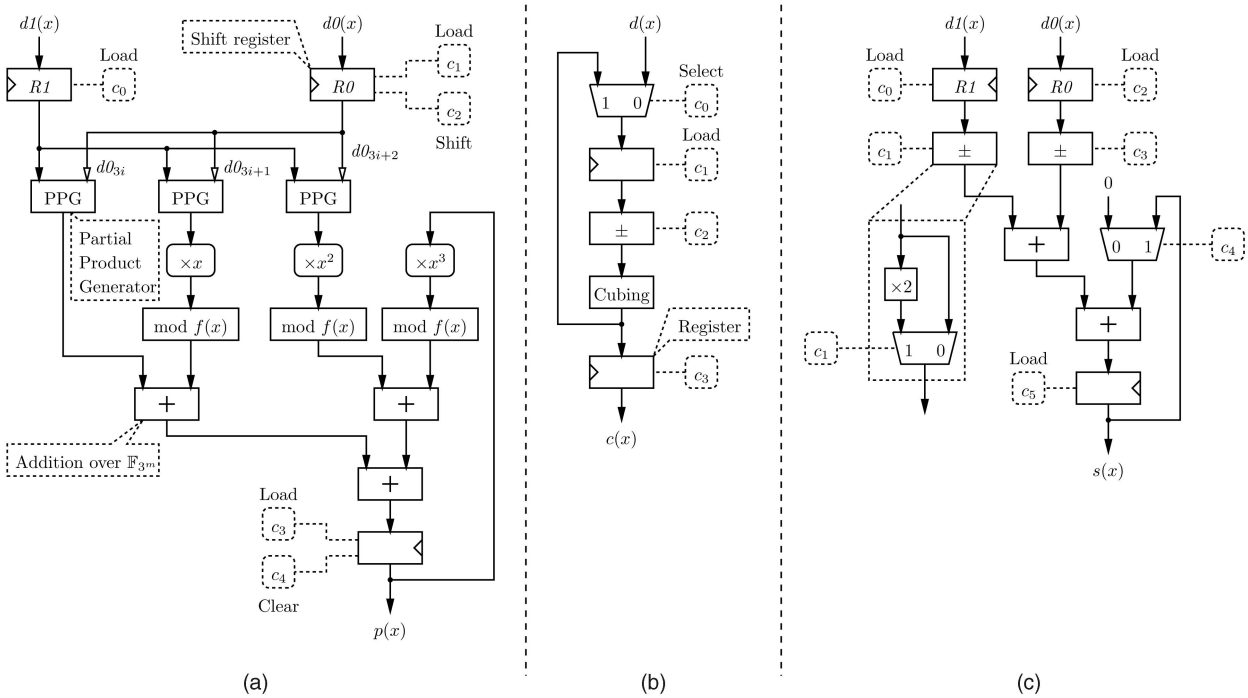

Fig. 1. Arithmetic operators over $\mathbb{F}_{3^m}$. (a) Multiplication ($D = 3$ coefficients of $d0(x)$ are processed at each clock cycle) [22]. (b) Cubing. (c) Addition/subtraction of two operands and accumulation. Boxes with rounded corners involve only wiring. The c_is denote control bits.

where $\nu_i(x) \in \mathbb{F}_{3^{97}}$, $0 \leq i \leq 2$, and

$$c(x) = d(x)^3 = \nu_0(x) + \nu_1(x) + \nu_2(x).$$

Recall that our inversion algorithm involves successive cubings. Since storing intermediate results in memory would be too time consuming, our cubing unit should include a feedback mechanism to efficiently implement Algorithm 11. Furthermore, cubing over $\mathbb{F}_{3^{6m}}$ requires the computation of $-u_5^3$, where $u_5 \in \mathbb{F}_{3^m}$ (for details, see Appendix E.1). These considerations suggest the design of the operator depicted in Fig. 1b.

If we have a closer look at the scheduling of the reduced η_T pairing algorithm, we note that there is no parallelism between multiplications and cubings over $\mathbb{F}_{3^m}$. If the array multiplier processes $D \geq D'$ coefficients at each clock cycle, we could take advantage of its multioperand adder to perform cubing. Fig. 2 describes how to modify the multiplier when $D = D' = 3$:

- The feedback loop responsible for the accumulation of partial products must be deactivated while cubing. An array of m AND gates performs this task and allows one to carry out the initialization step of the modular multiplication (instruction $p(x) \leftarrow 0$ in Algorithm 9).
- Multiplexers select the input of the multioperand adders between modulo $f(x)$ reduced partial products and the $\nu_i(x)$'s.
- The shift register of the multiplier and the PPGs allow for the control of cubing operations. If we store a control word in register $R0$ such that $d0_{3i} = d0_{3i+1} = d0_{3i+2} = -1$, the operator returns $-d1(x)^3$. If $d0_{3i} = d0_{3i+1} = d0_{3i+2} = 1$, we obtain $d1(x)^3$.

3.4 Addition over $\mathbb{F}_{3^m}$

The reduced η_T pairing algorithms discussed in this paper involve additions, subtractions, and accumulations over $\mathbb{F}_{3^m}$. Fig. 1c describes an operator implementing these functionalities. Again, a closer look at the reduced η_T pairing algorithms as well as at the algorithms for arithmetic over $\mathbb{F}_{3^{3m}}$ and $\mathbb{F}_{3^{6m}}$ indicates that there is almost no parallelism between additions and multiplications over $\mathbb{F}_{3^m}$. We suggest to further modify our array multiplier to include addition, subtraction, and accumulation (Fig. 3):

- An additional register is needed to store the second operand of an addition. Again, the shift register stores a control word to control additions. Assume for instance that we have to compute $-d2(x) + d1(x)$. We, respectively, load $d2(x)$ and $d1(x)$ in registers $R2$ and $R1$ and define a control word stored in $R0$ so that $d0_{3i=1}$, $d0_{3i+1} = 2$, and $d0_{3i+2} = 0$. We will thus compute $(d1(x) + 2 \cdot d2(x) + 0 \cdot d1(x)) \bmod f(x) = (d1(x) - d2(x)) \bmod f(x)$. Since the reduced η_T pairing algorithm involves successive additions and cubings, each control word loaded in the shift register manages a sequence of operations. Note that
  - while performing a multiplication or a cubing, registers $R1$ and $R2$ must store the same value;
  - $d0_{3i+2}$ is always equal to zero in the case of addition.
- A multiplexer in the accumulation loop allows one to select between the content of register $R3$ (accumulation) or the content of $R3$ shifted and reduced modulo $f(x)$ (multiplication).

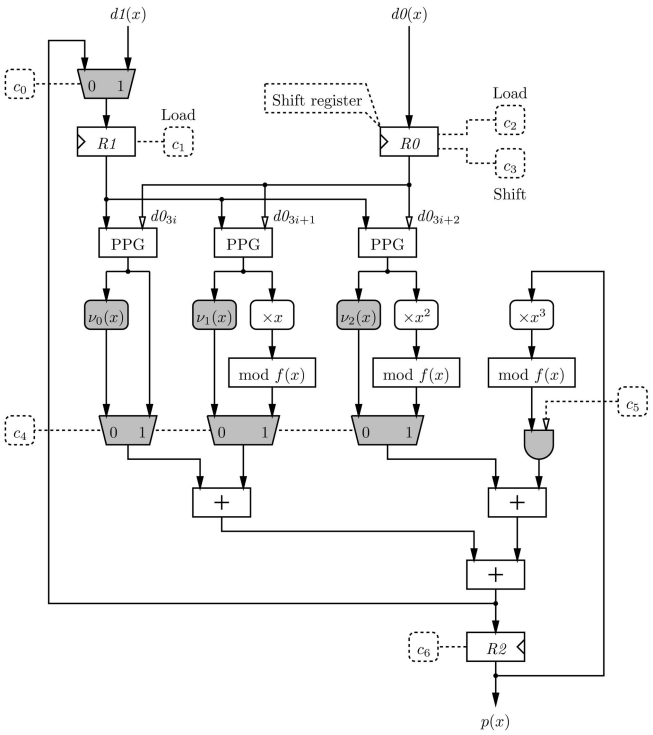

Fig. 2. Operator for multiplication and cubing over $\mathbb{F}_3[x]/(x^{97}+x^{12}+2)$. Boxes with rounded corners involve only wiring. The c_is denote control bits. Gray boxes outline the modifications of the array multiplier in Fig. 1a.

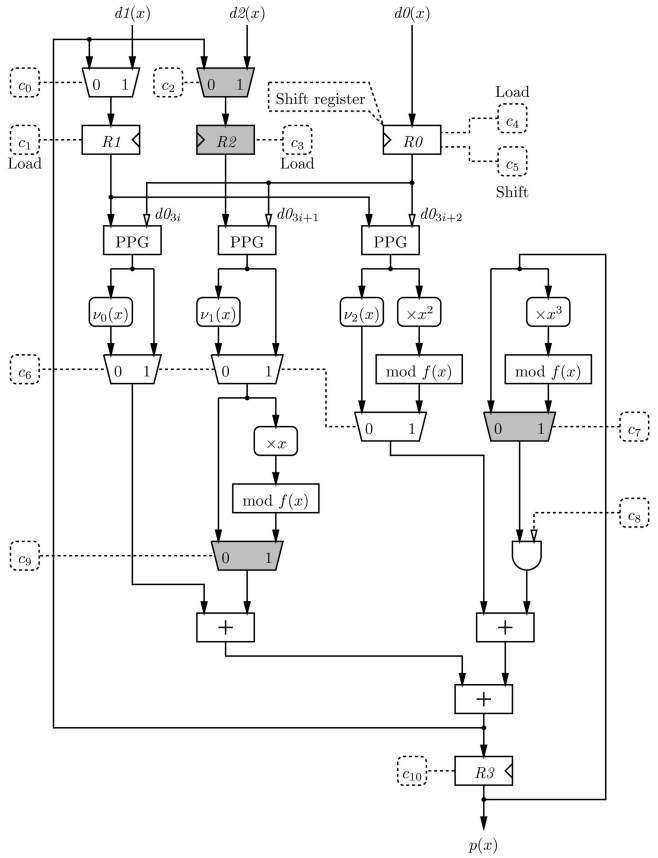

Fig. 3. Operator for addition, multiplication, and cubing over $\mathbb{F}_3[x]/(x^{97}+x^{12}+2)$. Boxes with rounded corners involve only wiring. The c_is denote control bits. Gray boxes outline the modifications of the operator in Fig. 2.

- An additional multiplexer is required to select the second input of the multioperand adder: $d2(x)$ (addition), $(d2(x) \cdot d0_{3i+1} \cdot x) \bmod f(x)$ (multiplication), or $\nu_1(x)$ (cubing).

3.5 Cube Root over $\mathbb{F}_{3^m}$

Some of the η_T pairing algorithms in characteristic three described in Section 2 involve cube roots over $\mathbb{F}_{3^m}$. This function is computed exactly in the same way as cubing: first, the normal form of $\sqrt[3]{d(x)} \bmod f(x)$ is obtained by solving the m-dimensional linear system given by the equation $(\sqrt[3]{d(x)})^3 \bmod f(x) = d(x)$. The result is then expressed as a sum of polynomials, each one being a permutation of the coefficients of the operand $d(x)$ multiplied by a constant. The number of polynomials we have to add depends on $f(x)$. Barreto gives a list of irreducible polynomials leading to efficient cube root operators in [41].

3.6 Architecture of the Coprocessor

Fig. 4 describes the architecture of our η_T pairing coprocessor. It consists of a single processing element (unified operator for addition, multiplication, and cubing), registers implemented by means of a dual-port RAM (six Virtex-II Pro SelectRAM+ blocks or 13 Cyclone II M4K memory blocks), and a control unit that consists of a Finite State Machine (FSM) and an instruction memory (ROM). Each instruction consists of four fields: an 11-bit word that specifies the functionality of the processing element, address and write enable signal for port B of the dual-port RAM, address for port A of the dual-port RAM, and a 6-bit control word that manages jump instructions and indicates how many times an instruction must be repeated. This approach makes it possible for instance to execute the consecutive steps appearing in the multiplication over $\mathbb{F}_{3^m}$ with a single instruction.

The architecture described in Fig. 4 was captured in the VHDL language and prototyped on several Altera and Xilinx FPGAs. We selected the following parameters: $m = 97$, $b = 1$, and $f(x) = x^{97} + x^{12} + 2$. Both synthesis and place-and-route steps were performed with Quartus II 7.1 Web Edition and ISE WebPACK 9.2i. The implementation on this coprocessor of the reduced η_T pairing (using Algorithm 5 for the η_T pairing and Algorithm 8 for the final exponentiation) takes 900 instructions, which are executed in 27,800 clock cycles. Table 3 summarizes the area (in slices on Xilinx FPGAs and Logic Elements (LEs) on the Altera device) and the calculation time.

It is worth noticing that an operator for inversion over $\mathbb{F}_{3^{97}}$ based on the EEA occupies 3,422 LEs on a Cyclone-II device [42] and 2,210 slices on a Virtex-II FPGA [43]. The implementation of the algorithm based on Itoh and Tsujii's work requires 394 clock cycles on our coprocessor for $m = 97$. The EEA needs $2m = 194$ clock cycles to return the inverse. Therefore, introducing specific hardware for inversion would double the circuit area while reducing the calculation time by less than 1 percent.

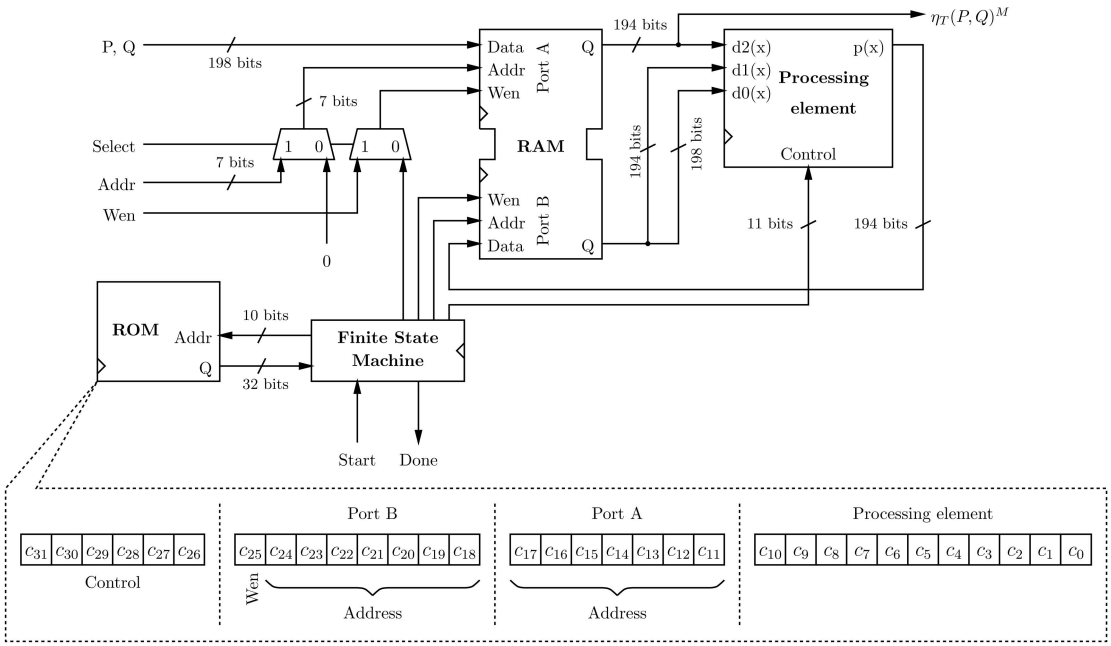

Fig. 4. Architecture of the coprocessor for arithmetic over $\mathbb{F}_{3^m}$.

We also described a naive coprocessor embedding the multiplier, the cubing unit, and the adder depicted in Fig. 1. The outputs of these operators are connected to the register file by means of a three-input multiplexer controlled by two additional bits. Place-and-route results indicate that such a coprocessor (without control unit) occupies 2,199 slices on a Spartan-3 FPGA and 3,345 LEs on a Cyclone-II device. Furthermore, we need 17 bits to control this ALU. Thus, our unified operator reduces both the area of the coprocessor and the width of the control words.

In order to guarantee the security of pairing-based cryptosystems in a near future, larger extension degrees will probably have to be considered, thus raising the question of designing such a unified operator for other extension fields. For this purpose, we wrote a C++ program that automatically generates a synthesizable VHDL description of a unified operator according to the characteristic and the irreducible polynomial $f(x)$.

4 Comparisons

Grabher and Page designed a coprocessor dealing with arithmetic over $\mathbb{F}_{3^m}$, which is controlled by a general purpose processor [19]. The ALU embeds an adder, a subtracter, a multiplier (with $D = 4$), a cubing unit, and a cube root operator based on the method highlighted by Barreto [41]. This architecture occupies 4,481 slices and allows one to perform the Duursma-Lee algorithm and its final exponentiation in 432.3 μs. The main advantage is that the control can be compiled using a retargeted GCC tool chain and other algorithms should easily be implemented on this architecture. Our approach leads however to a much simpler control unit and allows us to divide the number of slices by 2.4.

Another implementation of the Duursma-Lee algorithm was proposed by Kerins et al. [20]. It features a parallel multiplier over $\mathbb{F}_{3^{6m}}$ based on Karatsuba-Ofman's scheme. Since the final exponentiation requires a general multiplication over $\mathbb{F}_{3^{6m}}$, the authors cannot take advantage of the optimizations described in this paper and in [21] for the pairing calculation. Therefore, the hardware architecture consists of 18 multipliers and six cubing circuits over $\mathbb{F}_{3^{97}}$, along with, quoting [20], "a suitable amount of simpler $\mathbb{F}_{3^m}$ arithmetic circuits for performing addition, subtraction, and negation." Since the authors claim that roughly 100 percent of available resources are required to implement their pairing accelerator, the cost can be estimated as 55,616 slices [22]. The approach proposed in this paper reduces the area and the computation time by 30 and 4.4, respectively. Note that a multiplier over $\mathbb{F}_{3^{6m}}$ based on the fast Fourier transform [44] would save three multipliers over $\mathbb{F}_{3^m}$. Since all multiplications over

TABLE 3
Area and Calculation Time of an $\mathbb{F}_{3^{97}}$ Reduced η_T Pairing Coprocessor

	Virtex-II Pro 4	Virtex-4 LX 15	Spartan-3 200	Cyclone-II 5
Area	1833 slices	1851 slices	1857 slices	3216 LEs
Clock cycles	27800 cycles			
Clock frequency	145 MHz	203 MHz	100 MHz	152 MHz
Calculation time	192 μs	137 μs	278 μs	183 μs

TABLE 4
FPGA-Based Accelerators over $\mathbb{F}_{3^{97}}$ in the Literature

	Grabher and Page [19]	Kerins *et al.* [20]	Beuchat *et al.* [25], [26]
Algorithm	Modified Tate pairing	Modified Tate pairing	Reduced η_T pairing
FPGA	Virtex-II Pro 4	Virtex-II Pro 125	Cyclone II 35
Multiplier(s)	1 ($D = 4$)	18 ($D = 4$)	9 ($D = 3$)
Area	4481 slices	55616 slices	$\sim$ 18000 LEs
Clock cycles	59946	12866	4849
Clock frequency	150 MHz	15 MHz	149 MHz
Calculation time	432.3 μs	Estimated to 850 μs	33 μs

	Ronan *et al.* [23]		Jiang [24]
Algorithm	Reduced η_T pairing	Reduced η_T pairing	Reduced η_T pairing
FPGA	Virtex-II Pro 100	Virtex-II Pro 100	Virtex-4 LX200
Multiplier(s)	5 ($D = 4$)	8 ($D = 4$)	($D = 7$)
Area	10540 slices	15401 slices	74105 slices
Clock cycles	15853	15529	1627
Clock frequency	84.8 MHz	84.8 MHz	77.7 MHz
Calculation time	187 μs	183 μs	20.9 μs

The parameter D refers to the number of coefficients processed at each clock cycle by a multiplier.

$\mathbb{F}_{3^m}$ are performed in parallel, this approach would only slightly reduce the circuit area without decreasing the calculation time.

Beuchat et al. described a fast architecture for the computation of the η_T pairing [25]. The authors introduced a novel multiplication algorithm over $\mathbb{F}_{3^{6m}}$, which takes advantage of the constant coefficients of S. Thus, this design must be supplemented with a coprocessor for final exponentiation and the full pairing accelerator requires around 18,000 LEs on a Cyclone II FPGA [26]. The computation of the pairing and the final exponentiation require 4,849 and 4,082 clock cycles, respectively. Since both steps are pipelined, we can consider that a new result is returned after 4,849 clock cycles if we perform a sufficient amount of consecutive full η_T pairings. In order to compare our accelerator against this architecture, we implemented it on an Altera Cyclone II 5 FPGA with Quartus II 7.1 Web Edition. Our design occupies 3,216 LEs and the maximal clock frequency of 152 MHz allows one to compute a pairing in 183 μs. The architecture proposed in this paper is therefore 6 times slower but 5.6 times smaller.

In order to study the trade-off between circuit area and calculation time of the η_T pairing, Ronan et al. wrote a C program that automatically generates a VHDL description of a coprocessor and its control unit according to the number of multipliers over $\mathbb{F}_{3^m}$ to be included and the parameter D [23]. An architecture embedding five multipliers processing $D = 4$ coefficients at each clock cycle computes for instance a full pairing in 187 μs. Though slightly faster, this design requires five times the amount of slices of our pairing accelerator. Our approach offers a better compromise between area and calculation time (Table 4).

To our best knowledge, the fastest η_T pairing processor described in the open literature was designed by Jiang [24]. Unfortunately, Jiang does not give any detail about his architecture. Since a pairing is computed in 1,627 clock cycles and that multiplication over $\mathbb{F}_{3^m}$ is based on an LSE array multiplier processing $D = 7$ coefficients at each clock cycle, we can however guess that the design includes a hardwired multiplier over $\mathbb{F}_{3^{6m}}$. Though 6.5 faster than the coprocessor based on our unified arithmetic operator, the design by Jiang requires 40 times more slices.

5 Conclusion

We have discussed several algorithms to compute the η_T pairing and its final exponentiation in characteristic three. We proposed a compact implementation of the reduced η_T pairing in characteristic three over $\mathbb{F}_3[x]/(x^{97} + x^{12} + 2)$. Our architecture is based on a unified arithmetic operator that leads to the smallest circuit proposed in the open literature while demonstrating competitive performances.

Future works should include studies of the η_T pairing in characteristic two, where the wired multipliers embedded in most of the current FPGAs should allow for cheaper and faster array—and even fully parallel multipliers over $\mathbb{F}_{2^m}$. Such more efficient architectures would then allow us to investigate the η_T pairing over hyperelliptic curves.

The study of the Ate pairing [45] would also be of interest, for it presents a large speedup when compared to the Tate pairing and also supports nonsupersingular curves.

Acknowledgments

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

REFERENCES

[1] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," *Advances in Cryptology—Proc. ASIACRYPT '01,* C. Boyd, ed., pp. 514-532, 2001.

[2] A. Menezes, T. Okamoto, and S.A. Vanstone, "Reducing Elliptic Curves Logarithms to Logarithms in a Finite Field," *IEEE Trans. Information Theory,* vol. 39, no. 5, pp. 1639-1646, Sept. 1993.

[3] G. Frey and H.-G. Rück, "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," *Math. Computation,* vol. 62, no. 206, pp. 865-874, Apr. 1994.

[4] S. Mitsunari, R. Sakai, and M. Kasahara, "A New Traitor Tracing," *IEICE Trans. Fundamentals,* vol. E85-A, no. 2, pp. 481-484, Feb. 2002.

[5] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems Based on Pairing," *Proc. Symp. Cryptography and Information Security (SCIS '00),* pp. 26-28, Jan. 2000.

[6] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman," *Proc. Algorithmic Number Theory—ANTS IV,* W. Bosma, ed., pp. 385-394, 2000.

[7] R. Dutta, R. Barua, and P. Sarkar, *Pairing-Based Cryptographic Protocols: A Survey,* cryptology ePrint Archive, Report 2004/64, 2004.

[8] R. Granger, D. Page, and N.P. Smart, "High Security Pairing-Based Cryptography Revisited," *Proc. Algorithmic Number Theory —ANTS VII,* F. Hess, S. Pauli, and M. Pohst, eds., pp. 480-494, 2006.

[9] N. Koblitz and A. Menezes, "Pairing-Based Cryptography at High Security Levels," *Cryptography and Coding,* N.P. Smart, ed., pp. 13-36, Springer, 2005.

[10] J.H. Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[11] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," *Advances in Cryptology—Proc. CRYPTO '02,* M. Yung, ed., pp. 354-368, 2002.

[12] E.R. Verheul, "Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems," *J. Cryptology,* vol. 17, no. 4, pp. 277-296, 2004.

[13] V.S. Miller, *Short Programs for Functions on Curves,* http://crypto.stanford.edu/miller, 1986.

[14] V.S. Miller, "The Weil Pairing, and Its Efficient Calculation," *J. Cryptology,* vol. 17, no. 4, pp. 235-261, 2004.

[15] S.D. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate Pairing," *Algorithmic Number Theory—Proc. ANTS V,* C. Fieker and D. Kohel, eds., pp. 324-337, 2002.

[16] I. Duursma and H.S. Lee, "Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$," *Advances in Cryptology—Proc. ASIACRYPT '03,* C.S. Laih, ed., pp. 111-123, 2003.

[17] S. Kwon, "Efficient Tate Pairing Computation for Elliptic Curves over Binary Fields," *Information Security and Privacy—Proc. ACISP '05,* C. Boyd and J.M. González Nieto, eds., pp. 134-145, 2005.

[18] P.S.L.M. Barreto, S.D. Galbraith, C. Ó hÉigeartaigh, and M. Scott, "Efficient Pairing Computation on Supersingular Abelian Varieties," *Designs, Codes and Cryptography,* vol. 42, no. 3, pp. 239-271, Mar. 2007

[19] P. Grabher and D. Page, "Hardware Acceleration of the Tate Pairing in Characteristic Three," *Cryptographic Hardware and Embedded Systems—Proc. CHES '05,* J.R. Rao and B. Sunar, eds., pp. 398-411, 2005.

[20] T. Kerins, W.P. Marnane, E.M. Popovici, and P. Barreto, "Efficient Hardware for the Tate Pairing Calculation in Characteristic Three," *Cryptographic Hardware and Embedded Systems—Proc. CHES '05,* J.R. Rao and B. Sunar, eds., pp. 412-426, 2005.

[21] G. Bertoni, L. Breveglieri, P. Fragneto, and G. Pelosi, "Parallel Hardware Architectures for the Cryptographic Tate Pairing," *Proc. Third Int'l Conf. Information Technology: New Generations (ITNG),* 2006.

[22] C. Shu, S. Kwon, and K. Gaj, "FPGA Accelerated Tate Pairing Based Cryptosystem over Binary Fields," *Proc. IEEE Int'l Conf. Field Programmable Technology (FPT '06),* pp. 173-180, 2006.

[23] R. Ronan, C. Murphy, T. Kerins, C. Ó hÉigeartaigh, and P.S.L.M. Barreto, "A Flexible Processor for the Characteristic 3 η_T Pairing," *Int'l J. High Performance Systems Architecture,* vol. 1, no. 2, pp. 79-88, 2007.

[24] J. Jiang, "Bilinear Pairing (η_T Pairing) IP Core," technical report, Dept. of Computer Science, City Univ. of Hong Kong, May 2007.

[25] J.-L. Beuchat, M. Shirase, T. Takagi, and E. Okamoto, "An Algorithm for the η_T Pairing Calculation in Characteristic Three and Its Hardware Implementation," *Proc. 18th IEEE Symp. Computer Arithmetic (ARITH '07),* P. Kornerup and J.-M. Muller, eds., pp. 97-104, 2007.

[26] J.-L. Beuchat, N. Brisebarre, M. Shirase, T. Takagi, and E. Okamoto, "A Coprocessor for the Final Exponentiation of the η_T Pairing in Characteristic Three," *Proc. First Int'l Workshop Arithmetic of Finite Fields (WAIFI '07),* C. Carlet and B. Sunar, eds., pp. 25-39, 2007.

[27] J.-L. Beuchat, N. Brisebarre, J. Detrey, and E. Okamoto, "Arithmetic Operators for Pairing-Based Cryptography," *Cryptographic Hardware and Embedded Systems—Proc. CHES '07,* P. Paillier and I. Verbauwhede, eds., pp. 239-255, 2007.

[28] R. Granger, D. Page, and M. Stam, "On Small Characteristic Algebraic Tori in Pairing-Based Cryptography," *LMS J. Computation and Math.,* vol. 9, pp. 64-85, Mar. 2006.

[29] M. Shirase, T. Takagi, and E. Okamoto, "Some Efficient Algorithms for the Final Exponentiation of η_T Pairing," *Proc. Third Int'l Information Security Practice and Experience Conf. (ISPEC '07),* E. Dawson and D.S. Wong, eds., pp. 254-268, May 2007.

[30] J.-L. Beuchat, T. Miyoshi, J.-M. Muller, and E. Okamoto, "Horner's Rule-Based Multiplication over $\mathrm{GF}(p)$ and $\mathrm{GF}(p^n)$: A Survey," *Int'l J. Electronics,* to appear.

[31] S.E. Erdem, T. Yamk, and Ç.K. Koç, "Polynomial Basis Multiplication over $\mathrm{GF}(2^m)$," *Acta Applicandae Math.,* vol. 93, nos. 1-3, pp. 33-55, Sept. 2006.

[32] J. Guajardo, T. Güneysu, S. Kumar, C. Paar, and J. Pelzl, "Efficient Hardware Implementation of Finite Fields with Applications to Cryptography," *Acta Applicandae Math.,* vol. 93, nos. 1-3, pp. 75-118, Sept. 2006.

[33] L. Song and K.K. Parhi, "Low Energy Digit-Serial/Parallel Finite Field Multipliers," *J. VLSI Signal Processing,* vol. 19, no. 2, pp. 149-166, July 1998.

[34] R. Ronan, C. Ó hÉigeartaigh, C. Murphy, M. Scott, T. Kerins, and W. Marnane, "An Embedded Processor for a Pairing-Based Cryptosystem," *Proc. Third Int'l Conf. Information Technology: New Generations (ITNG),* 2006.

[35] G. Meurice de Dormale, personal communication.

[36] J.-C. Bajard, J. Duprat, S. Kla, and J.-M. Muller, "Some Operators for On-Line Radix-2 Computations," *J. Parallel and Distributed Computing,* vol. 22, pp. 336-345, 1994.

[37] T. Itoh and S. Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in $\mathrm{GF}(2^m)$ Using Normal Bases," *Information and Computation,* vol. 78, pp. 171-177, 1988.

[38] J. von zur Gathen and M. Nöcker, "Computing Special Powers in Finite Fields," *Math. Computation,* vol. 73, no. 247, pp. 1499-1523, 2003.

[39] F. Rodríguez-Henríquez, G. Morales-Luna, N.A. Saqib, and N. Cruz-Cortés, "A Parallel Version of the Itoh-Tsujii Multiplicative Inversion Algorithm," *Reconfigurable Computing: Architectures, Tools and Applications—Proc. ARC '07,* P.C. Diniz, E. Marques, K. Bertels, M.M. Fernandes, and J.M.P. Cardoso, eds., pp. 226-237, 2007.

[40] D.E. Knuth, *The Art of Computer Programming,* third ed. Addison-Wesley, 1998.

[41] P.S.L.M. Barreto, *A Note on Efficient Computation of Cube Roots in Characteristic 3,* 2004 cryptology ePrint Archive, Report 2004/305.

[42] A. Vithanage, personal communication.

[43] T. Kerins, E. Popovici, and W. Marnane, "Algorithms and Architectures for Use in FPGA Implementations of Identity Based Encryption Schemes," *Field-Programmable Logic and Applications,* J. Becker, M. Platzner, and S. Vernalde, eds., pp. 74-83, Springer, 2004.

[44] E. Gorla, C. Puttmann, and J. Shokrollahi, "Explicit Formulas for Efficient Multiplication in $\mathbb{F}_{3^{6m}}$," *Selected Areas in Cryptography—Proc. SAC '07,* C. Adams, A. Miri, and M. Wiener, eds., pp. 173-183, 2007.

[45] F. Hess, N. Smart, and F. Vercauteren, "The Eta Pairing Revisited," *IEEE Trans. Information Theory,* vol. 52, no. 10, pp. 4595-4602, Oct. 2006.

Jean-Luc Beuchat received the MSc and PhD degrees in computer science from the Swiss Federal Institute of Technology, Lausanne, Switzerland, in 1997 and 2001, respectively. He is an associate professor in the Graduate School of Systems and Information Engineering, University of Tsukuba. His current research interests include computer arithmetic and cryptography.

Nicolas Brisebarre received the PhD degree in pure mathematics from the Université Bordeaux I, Talence, France, in 1998. He is a *chargé de recherche* (junior researcher) at the Centre National de la Recherche Scientifique (CNRS), France, and a member of the Laboratoire de l'Informatique du Parallélisme (LIP), which is a joint computer science laboratory of CNRS, the École Normale Supérieure de Lyon, Institut National de Recherche en Informatique et Automatique (INRIA), and the Université Claude Bernard Lyon 1. His research interests are in computer arithmetic and number theory.

Jérémie Detrey received the MSc and PhD degrees in computer science from the École Normale Supérieure de Lyon (ENS Lyon), Lyon, France, in 2003 and 2007, respectively, under the supervision of Florent de Dinechin and Jean-Michel Muller. He is currently a postdoctoral fellow in the Cosec Group, Bonn-Aachen International Center for Information Technology (B-IT), Bonn, Germany. His research interests cover the various hardware aspects of computer arithmetic, from floating-point and elementary functions to finite fields and cryptography. He is a member of the IEEE and the IEEE Computer Society.

Eiji Okamoto received the BS, MS, and PhD degrees in electronics engineering from Tokyo Institute of Technology, in 1973, 1975, and 1978, respectively. He worked and studied communication theory and cryptography for NEC central research laboratories since 1978. From 1991, he became a professor at Japan Advanced Institute of Science and Technology, then at Toho University. He is currently a professor in the Graduate School of Systems and Information Engineering, University of Tsukuba. His research interests are cryptography and information security. He is a co-editor-in-chief of the *International Journal of Information Security*. He is a senior member of the IEEE.

Masaaki Shirase received the BSc degree in mathematics from Ibaraki University in 1994 and the MIS and DrIS degrees from Japan Advanced Institute of Science and Technology (JAIST), in 2003 and 2006, respectively. He is currently a postdoctoral fellow in the School of Systems Information Science, Future University-Hakodate. He is currently interested in the implementation of cryptographic algorithms.

Tsuyoshi Takagi received the BSc and MSc degrees in mathematics from Nagoya University in 1993 and 1995, respectively, and the Drrernat degree from the Technische Universität Darmstadt in 2001. He engaged in research on network security at NTT Laboratories from 1995 to 2001. He was an assistant professor in the Department of Computer Science at the Technische Universität Darmstadt until 2005. He is currently a professor in the School of Systems Information Science, Future University-Hakodate. His current research interests are information security and cryptography. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), and the International Association for Cryptographic Research (IACR).