Optimal Eta Pairing on Supersingular Genus-2 Binary Hyperelliptic Curves

Diego F. Aranha[1⋆], Jean-Luc Beuchat[2], Jérémie Detrey[3], and Nicolas Estibals[3]

[1] Institute of Computing, University of Campinas
Av. Albert Einstein, 1251, CEP 13084-971, Campinas, Brazil
dfaranha@ic.unicamp.br
[2] Graduate School of Systems and Information Engineering, University of Tsukuba,
1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan
beuchat@risk.tsukuba.ac.jp
[3] CARAMEL project-team, LORIA, INRIA / CNRS / Nancy Université,
Campus Scientifique, BP 239, 54506 Vandœuvre-lès-Nancy Cedex, France
jeremie.detrey@loria.fr   nicolas.estibals@loria.fr

Abstract. This article presents a novel pairing algorithm over supersingular genus-2 binary hyperelliptic curves. Starting from Vercauteren's work on optimal pairings, we describe how to exploit the action of the 2^{3m}-th power Verschiebung in order to reduce the loop length of Miller's algorithm even further than the genus-2 η_T approach.
As a proof of concept, we detail an optimized software implementation and an FPGA accelerator for computing the proposed optimal Eta pairing on a genus-2 hyperelliptic curve over $\mathbb{F}_{2^{367}}$, which satisfies the recommended security level of 128 bits. These designs achieve favourable performance in comparison with the best known implementations of 128-bit-security Type-1 pairings from the literature.

Keywords: Optimal Eta pairing, supersingular genus-2 curve, software implementation, FPGA implementation.

1 Introduction

The Weil and Tate pairings were independently introduced in cryptography by Frey & Rück [18] and Menezes, Okamoto & Vanstone [34] as tools to attack the discrete-logarithm problem on some classes of elliptic curves defined over finite fields. The discovery of constructive properties by Joux [29], Mitsunari, Sakai & Kasahara [37], and Sakai, Oghishi & Kasahara [41] initiated the proposal of an ever-increasing number of protocols based on bilinear pairings: identity-based encryption [10], short signature [12], and efficient broadcast encryption [11], to mention but a few. However, such protocols rely critically on efficient implementations of pairing primitives at high security levels on a wide range of targets.

⋆ This work was performed while the author was visiting University of Waterloo.

Miller described the first iterative algorithm to compute the Weil and Tate pairings back in 1986 [35, 36]. The Tate pairing seems to be more suited to efficient implementations (see for instance [25, 30]), and has therefore attracted a lot of interest from the research community. A large number of articles, culminating in the η_T pairing algorithm [5], focused on shortening the loop of Miller's algorithm in the case of supersingular abelian varieties. The Ate pairing, introduced by Hess *et al.* [28] for elliptic curves and by Granger *et al.* [24] in the hyperelliptic case, generalizes the η_T approach to ordinary curves. Eventually, several variants of the Ate pairing aiming at reducing the loop length of Miller's algorithm have been proposed in 2008 [27, 31, 43].

In this work, we target the AES-128 security level. When dealing with ordinary elliptic curves defined over a prime finite field $\mathbb{F}_p$, the family of curves introduced by Barreto & Naehrig (BN) [6] is a nearly optimal choice for the 128-bit security level. Their embedding degree $k = 12$ perfectly balances the security between the ℓ-torsion and the group of ℓ-th roots of unity, where ℓ is a prime number dividing the cardinality of the curve $\#E(\mathbb{F}_p)$. The latest software implementation results on these curves by Aranha *et al.* report computation times below one millisecond on a single core of an Intel Core i7 processor [1].

Supersingular curves over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$ are better suited to hardware implementation, and offer more efficient point doubling and tripling formulae than BN-curves. Moreover, supersingularity allows the use of a distortion map and thus provides Type-1 (or symmetric) pairings [19], which cannot be obtained with ordinary curves. However, the embedding degree of a supersingular elliptic curve is always less than or equal to 6 [34]. As a consequence, the security on the curve is too high with respect to the security of the group of ℓ-th roots of unity, and one has to consider curves defined over very large finite fields. Therefore, most of the hardware accelerators are struggling to achieve the AES-128 level of security (see for instance [9] for a comprehensive bibliography). Software implementations at this security level have for instance been reported in [3, 8]. However, the computation of a pairing is at least 6 times faster on a BN curve [7].

To mitigate the effect of the bounded embedded degree, Estibals proposed to consider supersingular elliptic curves over field extensions of moderately-composite degree [17]. Curves are then vulnerable to Weil descent attacks [22], but a careful analysis allowed him to maintain the security above the 128-bit threshold. As a proof of concept, he designed a compact Field-Programmable Gate Array (FPGA) accelerator for computing the Tate pairing on a supersingular elliptic curve defined over $\mathbb{F}_{3^{5\cdot 97}}$. Even though he targeted his architecture to low-resource hardware, his timings are very close to those of software implementations of BN curves.

Yet another way to reduce the size of the base field of the Tate pairing in the supersingular case is to consider a genus-2 binary hyperelliptic curve with embedding degree $k = 12$ [20, 40], which is the solution investigated in this work. We indeed show that, thanks to a novel pairing algorithm, these curves can be actually made very effective in the context of software implementations and hardware accelerators for embedded systems.

This paper is organized as follows: after a general reminder on the hyperelliptic Tate pairing (Section 2) and on the Eta pairing on in the case of those particular curves (Section 3), we describe a novel optimal[1] Eta pairing algorithm that further reduces the loop length of Miller's algorithm compared to the η_T approach [5] (Section 4). We then present an optimized software implementation (Section 5) and a low-area FPGA accelerator (Section 6) for the proposed pairing algorithm. We discuss our results and conclude in Section 7.

2 Background Material and Notations

In this section, we briefly recall a few definitions and results about hyperelliptic curves, and more precisely the Tate pairing on such curves. For more details, we refer the interested reader to [16, 24].

2.1 Reminder on Hyperelliptic Curves

Let C be an imaginary nonsingular hyperelliptic curve of genus g defined over the finite field $\mathbb{F}_q$, where $q = p^m$ and p is a prime, and whose affine part is given by the equation $y^2 + h(x)y = f(x)$, where $f,\ h \in \mathbb{F}_q[x]$, $\deg f = 2g + 1$, and $\deg h \leq g$.

For any algebraic extension $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$, we define the set of $\mathbb{F}_{q^d}$-rational points of C as $C(\mathbb{F}_{q^d}) = \{(x, y) \in \mathbb{F}_{q^d} \times \mathbb{F}_{q^d} \mid y^2 + h(x)y = f(x)\} \cup \{P_\infty\}$, where P_∞ is the point at infinity of the curve. For simplicity's sake, we also write $C = C(\overline{\mathbb{F}}_q)$. Additionally, denoting by ϕ_q the q-th power Frobenius morphism $\phi_q : C \to C$, $(x, y) \mapsto (x^q, y^q)$, and $P_\infty \mapsto P_\infty$, note that a point $P \in C$ is $\mathbb{F}_{q^d}$-rational if and only if $\phi_q^d(P) = P$.

We then denote by Jac_C the Jacobian of C, which is an abelian variety of dimension g defined over $\mathbb{F}_q$, and whose elements are represented by the divisor class group of degree-0 divisors $\mathrm{Pic}_C^0 = \mathrm{Div}_C^0 / \mathrm{Princ}_C$. In other words, two degree-0 divisors D and D' belong to the same equivalence class $\overline{D} \in \mathrm{Jac}_C$ if and only if there exists a non-zero rational function $z \in \overline{\mathbb{F}}_q(C)^*$ such that $D' = D + \mathrm{div}(z)$. Naturally extending the Frobenius map to divisors as $\phi_q : \sum_{P \in C} n_P(P) \mapsto \sum_{P \in C} n_P(\phi_q(P))$, we say that D is $\mathbb{F}_{q^d}$-rational if and only if $\phi_q^d(D) = D$.

It can also be shown that any divisor class $\overline{D} \in \mathrm{Jac}_C(\mathbb{F}_{q^d})$ can be uniquely represented by an $\mathbb{F}_{q^d}$-rational reduced divisor $\rho(\overline{D}) = \sum_{i=1}^{r}(P_i) - r(P_\infty)$, with $r \leq g$, $P_i \neq P_\infty$, and $P_i \neq -P_j$ for $i \neq j$, where the negative of a point $P = (x, y)$ is given via the hyperelliptic involution by $-P = (x, -y - h(x))$. In the following, we also denote by $\epsilon(\overline{D}) = \sum_{i=1}^{r}(P_i)$ the effective part of $\rho(\overline{D})$.

Using the Mumford representation, any non-zero $\mathbb{F}_{q^d}$-rational reduced divisor $D = \rho(\overline{D})$ (and therefore any non-zero element of the Jacobian $\mathrm{Jac}_C(\mathbb{F}_{q^d})$) can be associated with a unique pair of polynomials $[u(x), v(x)]$, with $u,\ v \in \mathbb{F}_{q^d}[x]$

[1] Here the "optimal" qualifier is to be understood more as a reference to Vercauteren's work [43] than an actual claim of optimality.

and such that u is monic, $\deg(v) < \deg(u) = r \leq g$, and $u \mid v^2 + vh - f$. Furthermore, given two reduced divisors D_1 and D_2 in Mumford representation, Cantor's algorithm [13] can be used to compute the Mumford representation of $\rho(D_1 + D_2)$, the reduced divisor corresponding to their sum on the Jacobian.

2.2 Hyperelliptic Tate Pairing

Let ℓ be a prime dividing $\#\operatorname{Jac}_C(\mathbb{F}_q)$ and coprime to q. Let also k be the corresponding embedding degree, *i.e.*, the smallest integer such that $\ell \mid q^k - 1$. We denote by $\operatorname{Jac}_C(\mathbb{F}_{q^k})[\ell]$ the $\mathbb{F}_{q^k}$-rational ℓ-torsion subgroup of Jac_C. The Tate pairing on C is then the well-defined, non-degenerate, and bilinear map

$$\langle .,. \rangle_\ell : \operatorname{Jac}_C(\mathbb{F}_{q^k})[\ell] \times \operatorname{Jac}_C(\mathbb{F}_{q^k})/\ell \operatorname{Jac}_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell,$$

defined as $\langle \overline{D}_1, \overline{D}_2 \rangle_\ell \equiv f_{\ell,D_1}(D_2)$, where D_1 and D_2 represent the divisor classes $\overline{D}_1$ and $\overline{D}_2$, respectively, with disjoint supports: $\operatorname{supp}(D_1) \cap \operatorname{supp}(D_2) = \emptyset$. Moreover, for any integer n and any $\mathbb{F}_{q^k}$-rational divisor D, the notation $f_{n,D}$ denotes the Miller function in $\mathbb{F}_{q^k}(C)^*$ which is defined (up to a non-zero constant multiple) by its divisor such that $\operatorname{div}(f_{n,D}) = nD - [n]D$, where $[n]D = \rho(nD)$. In the case of the Tate pairing, since $\overline{D}_1 \in \operatorname{Jac}_C[\ell]$, we have $[\ell]D_1 = 0$ and $\operatorname{div}(f_{\ell,D_1}) = \ell D_1$.

So as to obtain a unique value for the Tate pairing, we also define the reduced Tate pairing as $e : (\overline{D}_1, \overline{D}_2) \mapsto \langle \overline{D}_1, \overline{D}_2 \rangle_\ell^{(q^k-1)/\ell} \in \mu_\ell$, with $\mu_\ell \subseteq \mathbb{F}_{q^k}^*$ the subgroup of ℓ-th roots of unity. Note that for any L such that $\ell \mid L \mid q^k - 1$, we also have $e(\overline{D}_1, \overline{D}_2) = \langle \overline{D}_1, \overline{D}_2 \rangle_L^{(q^k-1)/L}$.

Ensuring that there are no elements of order ℓ^2 in $\operatorname{Jac}_C(\mathbb{F}_{q^k})$, we can also show that there is a natural isomorphism between the quotient $\operatorname{Jac}_C(\mathbb{F}_{q^k})/\ell \operatorname{Jac}_C(\mathbb{F}_{q^k})$ and $\operatorname{Jac}_C(\mathbb{F}_{q^k})[\ell]$. We can then identify these two groups, and define the Tate pairing on the domain $\operatorname{Jac}_C(\mathbb{F}_{q^k})[\ell] \times \operatorname{Jac}_C(\mathbb{F}_{q^k})[\ell]$.

The actual computation of the (reduced) Tate pairing is achieved thanks to Miller's algorithm [35, 36], which is based on the observation that, for any integer n, n', and for any $\mathbb{F}_{q^k}$-rational divisor D, one can take the function $f_{n+n',D} = f_{n,D} \cdot f_{n',D} \cdot g_{[n]D,[n']D}$, where $g_{[n]D,[n']D} \in \mathbb{F}_{q^k}(C)^*$ is such that $\operatorname{div}(g_{[n]D,[n']D}) = [n]D + [n']D - [n+n']D$. Note that the function $g_{[n]D,[n']D}$ can be explicitly obtained from the computation of $[n+n']D = \rho([n]D + [n']D)$ by Cantor's algorithm. See for instance [24, Algorithm 2] for more details. Therefore, computing $f_{\ell,D_1}(D_2)$ is tantamount to computing $[\ell]D_1$ on $\operatorname{Jac}_C(\mathbb{F}_{q^k})$ by means of any suitable scalar multiplication algorithm (*e.g.*, addition chain or double-and-add) while keeping track of the $g_{[n]D_1,[n']D_1}$ functions given by Cantor's algorithm and evaluating them at the divisor D_2. Miller's algorithm, based on the double-and-add approach, thus has a complexity of $\lfloor \log_2(\ell) \rfloor + \operatorname{wg}(\ell) - 1$ iterations (*i.e.*, evaluations of such $g_{[n]D_1,[n']D_1}$ functions), where $\operatorname{wg}(\ell)$ denotes the Hamming weight of ℓ.

Finally, let u_∞ be an $\mathbb{F}_q$-rational uniformizer at P_∞ (*i.e.*, $\operatorname{ord}_{P_\infty}(u_\infty) = 1$). For any function $z \in \overline{\mathbb{F}}_q(C)^*$, we denote by $\operatorname{lc}_\infty(z) = (u_\infty^{-\operatorname{ord}_{P_\infty}(z)} \cdot z)(P_\infty)$

the leading coefficient of z expressed as a Laurent series in u_∞. Restricting the domain of the Tate pairing to $\overline{D}_1 \in \mathrm{Jac}_C(\mathbb{F}_q)[\ell]$, one can easily check that $\mathrm{lc}_\infty(f_{\ell,D_1}) \in \mathbb{F}_q^*$ with $D_1 = \rho(\overline{D}_1)$. We can then apply [24, Lemma 1] to show that we can simply compute the Tate pairing as $\langle \overline{D}_1, \overline{D}_2 \rangle_\ell = f_{\ell,D_1}(\epsilon(\overline{D}_2))$, as long as $\mathrm{supp}(D_1) \cap \mathrm{supp}(\epsilon(\overline{D}_2)) = \emptyset$. This last condition is ensured by taking $\overline{D}_2 \in \mathrm{Jac}_C(\mathbb{F}_{q^k})[\ell] \setminus \mathrm{Jac}_C(\mathbb{F}_q)[\ell]$.

3 Eta Pairing on Supersingular Genus-2 Binary Curves

3.1 Curve Definition and Basic Properties

In this work, we consider the family of supersingular genus-2 hyperelliptic curves defined over $\mathbb{F}_2$ by the equation $C_d : y^2+y = x^5+x^3+d$, where $d \in \mathbb{F}_2$. Because of their supersingularity, which provides them with a very efficient arithmetic, along with their embedding degree of 12, which is the highest among all supersingular genus-2 curves, these curves are a target of choice for implementing pairing-based cryptography. They have therefore already been studied in this context in several articles [5, 14, 20, 32, 39, 40].

For m a positive integer coprime to 6, the cardinality L of the Jacobian of C_d over $\mathbb{F}_{2^m}$ is $L = \#\,\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m}) = 2^{2m} + \delta 2^{(3m+1)/2} + 2^m + \delta 2^{(m+1)/2} + 1$, where the value of δ is

$$\delta = \begin{cases} (-1)^d & \text{when } m \equiv 1,\ \ 7,\ 17, \text{ or } 23 \pmod{24}, \text{ and} \\ -(-1)^d & \text{when } m \equiv 5,\ 11,\ 13, \text{ or } 19 \pmod{24}. \end{cases}$$

The embedding degree of C_d is $k = 12$, and $\#\,\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m}) \mid 2^{12m} - 1$. The Tate pairing and its variants will then map into the degree-12 extension $\mathbb{F}_{2^{12m}}$, which we represent as the tower field $\mathbb{F}_{2^{12m}} \cong \mathbb{F}_{2^m}[\tau, s_{\tau,0}]$ where $\tau \in \mathbb{F}_{2^6}$ is such that $\tau^6+\tau^5+\tau^3+\tau^2+1 = 0$, and $s_{\tau,0} \in \mathbb{F}_{2^{12}}$ is such that $s_{\tau,0}^2+s_{\tau,0}+\tau^5+\tau^3 = 0$.

3.2 Distortion Maps

Since C_d is supersingular, it has non-trivial distortion maps [21, 44] embedding $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})$ into distinct subgroups of $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^{12m}})$. Such a distortion map will then allow us to construct Type-1 pairings [19], such as the modified Tate pairing described in the next section. An exhaustive study of the distortion maps of Jac_{C_d} is given by Galbraith *et al.* in [21], of which we now recall the key results.

From [21, Sec. 8], the automorphisms of C_d are of the form

$$\sigma_\omega : (x, y) \mapsto (x + \omega, y + s_{\omega,2}x^2 + s_{\omega,1}x + s_{\omega,0}),$$

where ω is a root of the polynomial $x^{16} + x^8 + x^2 + x$, $s_{\omega,2} = \omega^8 + \omega^4 + \omega$, $s_{\omega,1} = \omega^4 + \omega^2$, and $s_{\omega,0}$ is a root of $y^2 + y + \omega^5 + \omega^3$.

Considering τ as above, we also define $\theta = \tau^4 + \tau^2 + \tau$ and $\xi = \tau^4 + \tau^2$. One easily checks that τ, θ, and ξ are all roots of $x^{16} + x^8 + x^2 + x$. Let us now take $s_{\tau,0}$ as above, along with $s_{\theta,0} = s_{\tau,0}+\tau^5+\tau^2+\tau+1$ and $s_{\xi,0} = \tau^4+\tau^2$. Verifying that $s_{\omega,0}^2 + s_{\omega,0} + \omega^5 + \omega^3 = 0$ holds for all $\omega \in \{\tau, \theta, \xi\}$, we can now define the three corresponding automorphisms of C_d, namely σ_τ, σ_θ, and σ_ξ, along with their natural extension to its Jacobian Jac_{C_d}.

From [21, Prop. 8.1], all possible distortion maps can be found in $\mathbb{Z}[\phi_{2^m}, \sigma_\tau, \sigma_\theta]$, where ϕ_{2^m} is the 2^m-th power Frobenius map. Furthermore, $\mathbb{Q}[\phi_{2^m}, \sigma_\tau, \sigma_\theta]$ is a 16-dimensional vector space with the direct sum decomposition

$$\mathbb{Q}[\phi_{2^m}, \sigma_\tau, \sigma_\theta] = \mathbb{Q}(\phi_{2^m}) \oplus \sigma_\tau \mathbb{Q}(\phi_{2^m}) \oplus \sigma_\theta \mathbb{Q}(\phi_{2^m}) \oplus \sigma_\xi \mathbb{Q}(\phi_{2^m}).$$

In other words, the four endomorphisms of Jac_{C_d} 1, σ_τ, σ_θ, and σ_ξ are linearly independent over $\mathbb{Q}(\phi_{2^m})$, and any distortion map can be expressed as a $\mathbb{Q}(\phi_{2^m})$-linear combination of these endomorphisms.

Finally, a tedious computation—which, fortunately, can easily be checked using any computer algebra system—gives the three following equalities over $\mathrm{End}(\mathrm{Jac}_{C_d})$:

$$\begin{aligned} \phi_{2^m} \sigma_\tau \phi_{2^m}^{-1} &= \quad [2^m] \sigma_\tau \phi_{2^m}^{-2} + [\epsilon 2^{2m}] \sigma_\theta \phi_{2^m}^{-4}, \\ \phi_{2^m} \sigma_\theta \phi_{2^m}^{-1} &= [-2^{3m}] \sigma_\theta \phi_{2^m}^{-6}, \text{ and} \\ \phi_{2^m} \sigma_\xi \phi_{2^m}^{-1} &= \quad [2^{4m}] \sigma_\xi \phi_{2^m}^{-8} + [\epsilon 2^{5m}] \phi_{2^m}^{-10}, \end{aligned}$$

where $\epsilon = (-1)^e$ and $e = 0$ when $m \equiv 1$ or $11 \pmod{12}$, and 1 otherwise.

3.3 Modified Tate Pairing on C_d

Let ℓ be a large (odd) prime dividing $L = \#\,\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})$. After ensuring that there are no points of order ℓ^2 in $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^{12m}})$, we can restrict the domain of the Tate pairing to $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] \times \mathrm{Jac}_{C_d}(\mathbb{F}_{2^{12m}})[\ell]$, as detailed in Section 2.2. Using a non-trivial distortion map ψ which maps $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell]$ to a subgroup $\psi(\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell]) \subset \mathrm{Jac}_{C_d}(\mathbb{F}_{2^{12m}})[\ell]$ such that $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] \cap \psi(\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell]) = \{\overline{0}\}$, we can then define the reduced modified Tate pairing as the non-degenerate, bilinear map

$$\begin{aligned} \hat{e} \ : \ \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] \times \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] &\longrightarrow \mu_\ell \subseteq \mathbb{F}_{2^{12m}}^* \\ (\quad \overline{D}_1 \quad , \quad \overline{D}_2 \quad) &\longmapsto \langle \overline{D}_1, \psi(\overline{D}_2) \rangle_\ell^{(2^{12m}-1)/\ell} \\ &= \langle \overline{D}_1, \psi(\overline{D}_2) \rangle_L^{(2^{12m}-1)/L}, \end{aligned}$$

where $\langle \overline{D}_1, \psi(\overline{D}_2) \rangle_L = f_{L,D_1}(\epsilon(\psi(D_2)))$, the divisor classes $\overline{D}_1$ and $\overline{D}_2$ being represented by the $\mathbb{F}_{2^m}$-rational reduced divisors $D_1 = \rho(\overline{D}_1)$ and $D_2 = \rho(\overline{D}_2)$. As long as $\overline{D}_1$ and $\overline{D}_2$ are not both trivial, the distortion map ψ ensures that the affine supports of D_1 and $\psi(D_2)$ are disjoint.

At this stage, we have to point out that, in this case, the $g_{[n]D_1,[n']D_1}$ functions required by Miller's algorithm in the computation of the Tate pairing can be simplified. Indeed, from Cantor's algorithm, most of these functions involve vertical lines, which all pass through multiples of the $\mathbb{F}_{2^m}$-rational reduced divisor D_1, meaning that their equations will also be $\mathbb{F}_{2^m}$-rational. Furthermore, noticing that the x-coordinate of $\psi(P)$ is always in $\mathbb{F}_{2^{6m}}$ when P is $\mathbb{F}_{2^m}$- or $\mathbb{F}_{2^{2m}}$-rational, we can conclude that the evaluation of those vertical lines at $\epsilon(\psi(D_2))$

for any $\mathbb{F}_{2^m}$-rational reduced divisor D_2 will also be in $\mathbb{F}_{2^{6m}}^*$ and therefore annihilated by the final exponentiation to the $(2^{12m}-1)/L$-th power. We can then safely ignore the computation of those vertical lines.

3.4 Choosing an Efficient Pairing

Action of the Frobenius ϕ_{2^m}. Following the papers on hyperelliptic Ate and optimal Ate pairings [24, 43], a natural choice is to study the action of ϕ_{2^m}, the 2^m-th power Frobenius map, over $\mathrm{Jac}_{C_d}[\ell]$ in order to reduce the number of iterations in Miller's algorithm.

To that intent, let us first consider a non-zero element $\overline{D}_1 \in \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell]$. Since the four endomorphisms 1, σ_τ, σ_θ, and σ_ξ are $\mathbb{Q}(\phi_{2^m})$-linearly independent as per [21, Prop. 8.1], this is also the case for the four elements $\overline{D}_1$, $\overline{D}_\tau = \sigma_\tau(\overline{D}_1)$, $\overline{D}_\theta = \sigma_\theta(\overline{D}_1)$, and $\overline{D}_\xi = \sigma_\xi(\overline{D}_1)$, which then form a basis $\mathcal{B} = (\overline{D}_1, \overline{D}_\tau, \overline{D}_\theta, \overline{D}_\xi)$ of the 4-dimensional ℓ-torsion $\mathrm{Jac}_{C_d}[\ell]$.

From the three equalities presented in Section 3.2, and noting that $\phi_{2^m}(\overline{D}_1) = \overline{D}_1$ since $\overline{D}_1$ is $\mathbb{F}_{2^m}$-rational, one then obtains the following matrix describing the action of ϕ_{2^m} on the ℓ-torsion in the basis $\mathcal{B}$:

$$\phi_{2^m} \equiv \begin{pmatrix} 1 & 0 & 0 & \epsilon 2^{5m} \\ 0 & 2^m & 0 & 0 \\ 0 & \epsilon 2^{2m} & -2^{3m} & 0 \\ 0 & 0 & 0 & 2^{4m} \end{pmatrix} \pmod{\ell}.$$

From this matrix, one can remark that it is not completely diagonal. In particular, the eigenspace of eigenvalue 2^m, which would allow one to construct the optimal Ate pairing described by Vercauteren in [43, Sec. IV-G], is not directly attainable using the distortion map σ_τ. This is not a problem in general, but since we want to construct a Type-1 pairing, we cannot avoid the use of distortion maps.

Diagonalizing the matrix shows that a way to map $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell]$ to this eigenspace would be to use the distortion map $\psi = (2^{3m} + \phi_{2^m})\sigma_\tau$, as one can rapidly check that $\phi_{2^m}(\psi(\overline{D}_1)) = [2^m]\psi(\overline{D}_1)$. However, contrary to the distortion maps σ_τ, σ_θ, and σ_ξ which are simple automorphisms of C_d, ψ only acts on its Jacobian. As this might have a negative impact on the performance of the corresponding hyperelliptic Ate pairing, we decide not to follow this option in this paper, even though we plan to investigate it in the near future.

Sticking now to the diagonal parts of the matrix, one might alternatively consider using the distortion map σ_θ, as it maps the $\mathbb{F}_{2^m}$-rational ℓ-torsion to the eigenspace of eigenvalue -2^{3m}. However, since $\ell \mid L \mid 2^{6m}+1$, the lattice in which to look for an optimal pairing over this eigenspace is only of dimension 2, which is no better that the Eta pairing that we propose at the end of this section.

Action of the Verschiebung $\hat{\phi}_{2^m}$. An alternative to relying on the action of the Frobenius map ϕ_{2^m} would be to use its dual $\hat{\phi}_{2^m}$, the 2^m-th power Verschiebung. However, the curve C_d is not superspecial, which means that $\hat{\phi}_{2^m}$, albeit purely inseparable, is not a map of C_d but only of Jac_{C_d}: the conditions of [24, Lemma 5] are not met, and we are therefore unable to construct a non-degenerate pairing from such a map.

Action of the Verschiebung $\hat{\phi}_{2^{3m}}$. Nevertheless, as already noted by Barreto *et al.* in [5], the 2^{3m}-th power Verschiebung $\hat{\phi}_{2^{3m}}$ can be used instead of $\hat{\phi}_{2^m}$. We detail this construction in the following paragraphs.

First, let $P = (x_P, y_P)$ be a point of C_d distinct from P_∞, and $D = (P) - (P_\infty)$ be the corresponding degenerate divisor. Its Mumford representation is then $D = [x + x_P, y_P]$. Doubling and reducing D three times via Cantor's algorithm, we obtain $[8]D = \rho(8D) = [x + x_P^{64} + 1, x_P^{128} + y_P^{64} + 1]$. Note that the divisor $[8]D$ is also degenerate, as $[8]D = ([8]P) - (P_\infty)$, and corresponds to the point $[8]P = (x_P^{64} + 1, x_P^{128} + y_P^{64} + 1) \in C_d$.

Octupling therefore acts not only on Jac_{C_d} but also on the curve C_d itself, and in fact restricts to a morphism of curves from C_d to itself, defined over $\mathbb{F}_2$ as $[8] = \sigma_1 \phi_8^2$ with σ_1 the automorphism $(x, y) \mapsto (x + 1, x^2 + y + 1)$ and ϕ_8 the 8th power Frobenius map $(x, y) \mapsto (x^8, y^8)$.

Iterating this octupling m times, we obtain the $\mathbb{F}_2$-rational map $[2^{3m}]$ on C_d defined as $[2^{3m}] = \gamma \phi_{2^{3m}}^2$, with $\gamma = \sigma_1^m : (x, y) \mapsto (x + 1, x^2 + y + \nu)$ and $\nu = (m + 1)/2 \bmod 2$. Note that γ, $\phi_{2^{3m}}$, and $[2^{3m}]$ can be naturally extended to Jac_{C_d}, where the latter corresponds to the multiplication by 2^{3m}.

Furthermore, since $\phi_{2^{3m}}$ is a degree-2^{3m} isogeny of Jac_{C_d}, we know that $\hat{\phi}_{2^{3m}} \phi_{2^{3m}} = [2^{3m}]$. Since $[2^{3m}] = \gamma \phi_{2^{3m}}^2$, we then have $\hat{\phi}_{2^{3m}} = \gamma \phi_{2^{3m}}$ and can thus verify that $\hat{\phi}_{2^{3m}}$ is also a degree-2^{3m} purely inseparable endomorphism of the curve C_d. We are therefore in the conditions of [24, Lemma 5], from which we get that, for any reduced divisor D, $\hat{\phi}_{2^{3m}}(D)$ is also reduced and we have the equality of Miller functions (up to a non-zero constant multiple)

$$f_{n, \hat{\phi}_{2^{3m}}(D)} \circ \hat{\phi}_{2^{3m}} = f_{n,D}^{2^{3m}}. \tag{1}$$

Let us now consider the action of $\hat{\phi}_{2^{3m}}$ on the ℓ-torsion $\mathrm{Jac}_{C_d}[\ell]$. Noting that $\phi_{2^{3m}}^4$ is the identity over the ℓ torsion since $\mathrm{Jac}_{C_d}[\ell] \subseteq \mathrm{Jac}_{C_d}(\mathbb{F}_{2^{12m}})$, we obtain the following diagonal matrix in the basis $\mathcal{B}$:

$$\hat{\phi}_{2^{3m}} = [2^{3m}] \phi_{2^{3m}}^{-1} \equiv [2^{3m}] \phi_{2^{3m}}^3 \equiv \begin{pmatrix} 2^{3m} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2^{3m} \end{pmatrix} \pmod{\ell}.$$

From this matrix, it appears that $\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell]$ is in the eigenspace of eigenvalue 2^{3m}, while $\psi(\mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell])$ is in the eigenspace of eigenvalue 1, where the distortion map ψ is either σ_τ or σ_θ. In other words, for any $\mathbb{F}_{2^m}$-rational ℓ-torsion element $\overline{D}$, $\hat{\phi}_{2^{3m}}(\overline{D}) = [2^{3m}]\overline{D}$ and $\hat{\phi}_{2^{3m}}(\psi(\overline{D})) = \psi(\overline{D})$.

3.5 Eta Pairing on C_d

We now follow the construction of Barreto *et al.* [5] in order to obtain the η_T pairing with $T = 2^{3m}$. Remarking indeed that $\ell \mid L \mid N$ for $N = 2^{12m} - 1 = T^4 - 1$, and taking $M = N/L$, we can write

$$\hat{e}(\overline{D}_1, \overline{D}_2)^M = f_{L,D_1}(\epsilon(\psi(D_2)))^{M(2^{12m}-1)/L} = f_{N,D_1}(\epsilon(\psi(D_2)))^{(2^{12m}-1)/L}.$$

As $\ell \mid N$, we can then take the Miller function

$$f_{N,D_1} = f_{N+1,D_1} = f_{T^4,D_1} = \prod_{i=0}^{3} f_{T,[T^i]D_1}^{T^{3-i}} = \prod_{i=0}^{3} f_{2^{3m},[2^{i\cdot 3m}]D_1}^{2^{(3-i)\cdot 3m}}.$$

Furthermore, since D_1 and D_2 are $\mathbb{F}_{2^m}$-rational reduced divisors, we also have that $[2^{i\cdot 3m}]D_1 = \hat{\phi}^i_{2^{3m}}(D_1)$ and $\epsilon(\psi(D_2)) = \hat{\phi}^i_{2^{3m}}(\epsilon(\psi(D_2)))$ for all i. Iterating (1) then yields

$$\begin{aligned} f_{2^{3m},[2^{i\cdot 3m}]D_1}(\epsilon(\psi(D_2))) &= \left(f_{2^{3m},\hat{\phi}^i_{2^{3m}}(D_1)} \circ \hat{\phi}^i_{2^{3m}}\right)(\epsilon(\psi(D_2))) \\ &= f_{2^{3m},D_1}(\epsilon(\psi(D_2)))^{2^{i\cdot 3m}}. \end{aligned}$$

Putting it all together, we finally obtain

$$\hat{e}(\overline{D}_1, \overline{D}_2)^M = f_{2^{3m},D_1}(\epsilon(\psi(D_2)))^{4\cdot 2^{3\cdot 3m}\cdot(2^{12m}-1)/L},$$

and, as $\ell \nmid 4 \cdot 2^{3\cdot 3m}$,

$$f_{2^{3m},D_1}(\epsilon(\psi(D_2)))^{(2^{12m}-1)/L} = \hat{e}(\overline{D}_1, \overline{D}_2)^{M\cdot(4\cdot 2^{3\cdot 3m})^{-1} \bmod L}.$$

From the bilinearity and the non-degeneracy of the Tate pairing, we can then conclude that the η_T pairing defined as follows is also bilinear and non-degenerate [5]:

$$\begin{array}{rcccccl} \eta_T & : & \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] \times \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] & \longrightarrow & \mu_\ell \subseteq \mathbb{F}^*_{2^{12m}} \\ & & (\overline{D}_1, \overline{D}_2) & \longmapsto & f_{2^{3m},D_1}(\epsilon(\psi(D_2)))^{(2^{12m}-1)/L}. \end{array}$$

4 Optimal Eta Pairing on C_d

4.1 Construction and Definition

In order to further decrease the loop length in Miller's algorithm, we adapt in this work the optimal pairing technique as introduced by Vercauteren [43] to the case of the action of the 2^{3m}-th power Verschiebung $\hat{\phi}_{2^{3m}}$ and the Eta pairing detailed in the previous section.

To that intent, let us consider the 2-dimensional lattice spanned by the rows of the matrix

$$\mathfrak{L} = \begin{pmatrix} L & 0 \\ -2^{3m} & 1 \end{pmatrix}.$$

Note that since $\ell \mid L \mid 2^{6m}+1$, we know that $2^{6m} \equiv -1 \pmod{\ell}$, meaning that there is no need to look for 2^{3m}-ary expansions of multiples of L having more than two digits.

A shortest vector of $\mathfrak{L}$ is $[c_0, c_1] = [\delta 2^{(m-1)/2}+1, 2^m + \delta 2^{(m-1)/2}]$, which corresponds to taking the multiple $N' = c_1 2^{3m} + c_0 = M'L$ with $M' = 2^{2m} - \delta 2^{(3m-1)/2} - \delta 2^{(m-1)/2} + 1$.

We then have the M'-th power of the reduced modified Tate pairing

$$\hat{e}(\overline{D}_1, \overline{D}_2)^{M'} = f_{N',D_1}(\epsilon(\psi(D_2)))^{(2^{12m}-1)/L},$$

for which we can take the Miller function

$$\begin{aligned} f_{N',D_1} &= f_{c_1 2^{3m},D_1} \cdot f_{c_0,D_1} \cdot g_{[c_0]D_1,[c_1 2^{3m}]D_1} \\ &= f^{c_1}_{2^{3m},D_1} \cdot f_{c_1,[2^{3m}]D_1} \cdot f_{c_0,D_1} \cdot g_{[c_0]D_1,[c_1 2^{3m}]D_1}. \end{aligned}$$

Remarking that $c_1 2^{3m} \equiv -c_0 \pmod{\ell}$, $g_{[c_0]D_1,[c_1 2^{3m}]D_1}$ actually corresponds to the vertical lines passing through $[c_0]D_1$ and $[-c_0]D_1$, which can simply be ignored. Furthermore, exploiting the action of the Verschiebung $\hat{\phi}_{2^{3m}}$, we can rewrite $f_{c_1,[2^{3m}]D_1}(\epsilon(\psi(D_2)))$ as $f^{2^{3m}}_{c_1,D_1}(\epsilon(\psi(D_2)))$. Finally, also note that $f_{2^{3m},D_1}(\epsilon(\psi(D_2)))^{c_1 \cdot (2^{12m}-1)/L}$ is actually a power of the Eta pairing $\eta_T(\overline{D}_1, \overline{D}_2)$ defined in the previous section.

Consequently, let $\eta_{[c_0,c_1]} : \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] \times \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell] \to \mu_\ell$ be the optimal Eta pairing defined as

$$\eta_{[c_0,c_1]} \quad : \quad (\overline{D}_1, \overline{D}_2) \quad \longmapsto \quad \left(f^{2^{3m}}_{c_1,D_1} \cdot f_{c_0,D_1}\right)(\epsilon(\psi(D_2)))^{(2^{12m}-1)/L}.$$

From the previous considerations, we thus have that

$$\hat{e}(\overline{D}_1, \overline{D}_2)^{M'} = \eta_{[c_0,c_1]}(\overline{D}_1, \overline{D}_2) \cdot \eta_T(\overline{D}_1, \overline{D}_2)^{c_1},$$

whence $\eta_{[c_0,c_1]}(\overline{D}_1, \overline{D}_2) = \hat{e}(\overline{D}_1, \overline{D}_2)^W$ with

$$\begin{aligned} W &= M' - c_1 M \cdot (4 \cdot 2^{3 \cdot 3m})^{-1} \bmod L \\ &= 2^{2m} + \delta 2^{(3m-1)/2} + 2^m + \delta 2^{(m-1)/2} + 1. \end{aligned}$$

Finally, as $\ell \nmid W$, we show that the optimal Eta pairing $\eta_{[c_0,c_1]}$ is also bilinear and non-degenerate.

Note that the η_T pairing introduced in [5] with $T = -\delta 2^{(3m+1)/2} - 1$ corresponds to the lattice vector $[-\delta 2^{(3m+1)/2} - 1, -1] \in \mathfrak{L}$.

4.2 Computing $\eta_{[c_0,c_1]}$

The computation of the optimal Eta pairing $\eta_{[c_0,c_1]}$ defined in the previous section relies on the evaluation of the two Miller functions f_{c_0,D_1} and f_{c_1,D_1} at $\epsilon(\psi(D_2))$. With $[c_0, c_1] = [\delta 2^{(m-1)/2}+1, 2^m + \delta 2^{(m-1)/2}]$, we can take the following functions

$$\begin{cases} f_{c_0,D_1} = f_{\delta 2^{(m-1)/2},D_1} \cdot g_{[\delta 2^{(m-1)/2}]D_1,D_1} \quad \text{and} \\ f_{c_1,D_1} = f_{2^m,D_1} \cdot f_{\delta 2^{(m-1)/2},D_1} \cdot g_{[2^m]D_1,[\delta 2^{(m-1)/2}]D_1}. \end{cases}$$

Since we are ignoring the vertical lines, we can further rewrite

$$f_{\delta 2^{(m-1)/2},D_1} = f_{2^{(m-1)/2},[\delta]D_1} \quad \text{and}$$
$$f_{2^m,D_1} = f_{\delta 2^{(m-1)/2}\cdot\delta 2^{(m+1)/2},D_1} = f^{\delta 2^{(m+1)/2}}_{2^{(m-1)/2},[\delta]D_1} \cdot f_{2^{(m+1)/2},[2^{(m-1)/2}]D_1},$$

which finally gives

$$\begin{cases} f_{c_0,D_1} = f_{2^{(m-1)/2},[\delta]D_1} \cdot g_{[\delta 2^{(m-1)/2}]D_1,D_1} \quad \text{and} \\ f_{c_1,D_1} = f^{\delta 2^{(m+1)/2}+1}_{2^{(m-1)/2},[\delta]D_1} \cdot f_{2^{(m+1)/2},[2^{(m-1)/2}]D_1} \cdot g_{[2^m]D_1,[\delta 2^{(m-1)/2}]D_1}. \end{cases}$$

The computation of $\eta_{[c_0,c_1]}$ therefore chiefly involves the evaluation of the two Miller functions $f_{2^{(m-1)/2},[\delta]D_1}$ and $f_{2^{(m+1)/2},[2^{(m-1)/2}]D_1}$ of loop length $(m-1)/2$ and $(m+1)/2$, respectively. This represents a saving of 33% with respect to the η_T pairing presented in [5] whose Miller's loop length is $(3m+1)/2$.

Note that in order to exploit the octupling formula, we have to consider two cases, depending on the value of m mod 6, as described in Algorithm 1.

- When $m \equiv 1 \pmod 6$, then $(m-1)/2$ is a multiple of 3, and $f_{2^{(m-1)/2},[\delta]D_1}$ can be computed via $(m-1)/6$ octuplings, whereas $f_{2^{(m+1)/2},[2^{(m-1)/2}]D_1}$ can be computed by means of another $(m-1)/6$ octuplings and one extra doubling.
- When $m \equiv 5 \pmod 6$, $(m-1)/2$ is not a multiple of 3, but $(m+1)/2$ is. We then compute $\eta^2_{[c_0,c_1]} = \eta_{[2c_0,2c_1]}$ instead, with the Miller functions

$$\begin{cases} f_{2c_0,D_1} = f_{2^{(m+1)/2},[\delta]D_1} \cdot f_{2,D_1} \cdot g_{[\delta 2^{(m+1)/2}]D_1,[2]D_1} \quad \text{and} \\ f_{2c_1,D_1} = f^{\delta 2^{(m+1)/2}+1}_{2^{(m+1)/2},[\delta]D_1} \cdot f_{2^{(m+1)/2},[2^{(m+1)/2}]D_1} \cdot g_{[2^{m+1}]D_1,[\delta 2^{(m+1)/2}]D_1}. \end{cases}$$

The two $f_{2^{(m+1)/2},D}$ functions are then evaluated using $(m+1)/6$ octuplings each, whereas f_{2,D_1} only require one doubling.

Finally, one should note that, in our case, since the curve C_d is supersingular, the final exponentiation step is much simpler than for ordinary curves such as BN curves. Indeed, the exponent is

$$(2^{12m}-1)/L = (2^{6m}-1)(2^{2m}+1)(2^{2m}-\delta 2^{(3m+1)/2}+2^m-\delta 2^{(m+1)/2}+1),$$

whose regular form can be exploited to devise an efficient *ad-hoc* exponentiation algorithm, of negligible complexity when compared to Miller's loop.

4.3 Evaluation of the Complexity

From the above description of the optimal Eta pairing $\eta_{[c_0,c_1]}$, we can see that most of its computational cost lies in the iterated octuplings of D_1 and the evaluation of the corresponding Miller functions of the form $f_{8,[\pm 8^i]D_1}$ at the effective divisor $\epsilon(\psi(D_2))$. Here, we denote by $[\pm 8^i]D_1$ a reduced divisor representing one of the iterated octuples of D_1 or of $[\delta]D_1$ as required in the evaluation of $\eta_{[c_0,c_1]}$.

Algorithm 1 Computation of the optimal Eta pairing.

Input: $\overline{D}_1$ and $\overline{D}_2 \in \mathrm{Jac}_{C_d}(\mathbb{F}_{2^m})[\ell]$ represented by the reduced divisors D_1 and D_2.
Output: $\eta_{[c_0,c_1]}(\overline{D}_1, \overline{D}_2)$ or $\eta_{[c_0,c_1]}(\overline{D}_1, \overline{D}_2)^2 \in \mu_\ell \subseteq \mathbb{F}^*_{2^{12m}}$, depending upon whether $m \equiv 1$ or $5 \pmod 6$, respectively.

if $m \equiv 1 \pmod 6$ **then** $m' \leftarrow m-1$ **else** $m' \leftarrow m+1$ **end if**
$G_1 \leftarrow 1$; $R_1 \leftarrow [\delta]D_1$; $E_2 \leftarrow \epsilon(\psi(D_2))$
for $i \leftarrow 1$ **to** $m'/6$ **do**
  $G_1 \leftarrow G_1^8 \cdot f_{8,R_1}(E_2)$
  $R_1 \leftarrow [8]R_1$
end for // $G_1 = f_{2^{m'/2},[\delta]D_1}(E_2)$ and $R_1 = [\delta 2^{m'/2}]D_1$.
$G_2 \leftarrow G_1^\delta$; $R_2 \leftarrow [\delta]R_1$
for $i \leftarrow 1$ **to** $m'/6$ **do**
  $G_2 \leftarrow G_2^8 \cdot f_{8,R_2}(E_2)$
  $R_2 \leftarrow [8]R_2$
end for // $G_2 = f_{2^{m'},D_1}(E_2)$ and $R_2 = [2^{m'}]D_1$.
if $m \equiv 1 \pmod 6$ **then**
  $G_2 \leftarrow G_2^2 \cdot f_{2,R_2}(E_2)$ // $G_2 = f_{2^m,D_1}(E_2)$.
  $F_0 \leftarrow G_1 \cdot g_{R_1,D_1}(E_2)$ // $F_0 = f_{c_0,D_1}(E_2)$.
  $F_1 \leftarrow G_1 \cdot G_2 \cdot g_{[2]R_2,R_1}(E_2)$ // $F_1 = f_{c_1,D_1}(E_2)$.
else
  $F_0 \leftarrow G_1 \cdot f_{2,D_1}(E_2) \cdot g_{R_1,[2]D_1}(E_2)$ // $F_0 = f_{2c_0,D_1}(E_2)$.
  $F_1 \leftarrow G_1 \cdot G_2 \cdot g_{R_2,R_1}(E_2)$ // $F_1 = f_{2c_1,D_1}(E_2)$.
end if
return $\left(F_1^{2^{3m}} \cdot F_0\right)^{(2^{12m}-1)/L}$

In that sense, since D_1 is defined over $\mathbb{F}_{2^m}$, then $[\pm 8^i]D_1$ is also $\mathbb{F}_{2^m}$-rational. Moreover, as octupling directly acts on the curve C_d, if D_1 is degenerate (*i.e.*, of the form $D_1 = (P) - (P_\infty)$), then so is $[\pm 8^i]D_1$. Finally, note that if D_2 is degenerate, then so is $\psi(D_2)$, meaning that $\epsilon(\psi(D_2))$ is of degree 1 and has only one point in its support.

Considering the Miller function for octupling, we rewrite $f_{8,D} = f_{4,D}^2 \cdot f_{2,[4]D}$. Each iteration of Miller's algorithm is then just a matter of evaluating $f_{4,[\pm 8^i]D_1}$ and $f_{2,[\pm 4 \cdot 8^i]D_1}$ at $\epsilon(\psi(D_2))$, squaring the former, and accumulating both into the running product via two successive multiplications[2] over $\mathbb{F}_{2^{12m}}$. The respective costs of these operations are given in terms of basic operations over the base field $\mathbb{F}_{2^m}$ in Table 1.

Note that in order to obtain these costs, we have constructed $\mathbb{F}_{2^{12m}}$ as the tower field $\mathbb{F}_{2^m}[i, \tau, s_{\tau,0}]$, where $i \in \mathbb{F}_{2^2}$ is such that $i^2+i+1=0$, $\tau \in \mathbb{F}_{2^6}$ is such that $\tau^3 + i\tau^2 + i\tau + i = 0$ (one can then check that we still have $\tau^6 + \tau^5 + \tau^3 + \tau^2 + 1 = 0$), and $s_{\tau,0}$ is defined as before. Using Karatsuba for the two quadratic extensions and Toom–Cook for the cubic one, we obtain the expected complexity of 45 multiplications over $\mathbb{F}_{2^m}$ for computing one product over $\mathbb{F}_{2^{12m}}$ [30].

[2] Note that these multiplications are sparser than a regular multiplication over $\mathbb{F}_{2^{12m}}$ if at least one of the two divisors D_1 or D_2 is degenerate.

Where relevant, several costs are given in Table 1, depending on whether D_1 and D_2 are general (Gen.) or degenerate (Deg.) divisors. Making this disctinction is particularly relevant, as some protocols might be able to constrain the domain of their pairing computations in order to benefit from a possible speedup of 2 when one argument is degenerate, or even 4 in the case of two. For instance, Chatterjee *et al.* [14] have proposed a variant of the BLS signature scheme [12] in which one argument of each pairing function is a degenerate divisor.

Table 1. Costs of various operations involved in the computation of the optimal Eta pairing in terms of basic operations (multiplication, addition, squaring, and inversion) over the base field $\mathbb{F}_{2^m}$.

Operation	D_1	D_2	**Operations over $\mathbb{F}_{2^m}$**			
			Mult.	**Add.**	**Sq.**	**Inv.**
Addition over $\mathbb{F}_{2^{12m}}$	—	—	0	12	0	0
Squaring over $\mathbb{F}_{2^{12m}}$	—	—	0	21	12	0
Multiplication over $\mathbb{F}_{2^{12m}}$	—	—	45	199	0	0
$[\pm 8^i]D_1 \mapsto [\pm 8^{i+1}]D_1$	Deg.	—	0	2	13	0
	Gen.	—	0	5	24	0
$f_{4,[\pm 8^i]D_1}(\epsilon(\psi(D_2)))$	Deg.	Deg.	3	11	1	0
	Gen.	Deg.	19	40	2	0
	Gen.	Gen.	83	247	17	0
$f_{2,[\pm 4\cdot 8^i]D_1}(\epsilon(\psi(D_2)))$	Deg.	Deg.	2	9	1	0
	Gen.	Deg.	16	34	2	0
	Gen.	Gen.	81	236	17	0
Miller iteration $\begin{cases} G_i \leftarrow G_i^8 \cdot f_{8,R_i}(E_2) \\ R_i \leftarrow [8]R_i \end{cases}$	Deg.	Deg.	61	315	68	0
	Gen.	Deg.	121	512	130	0
	Gen.	Gen.	254	949	160	0
Final exp. over $\mathbb{F}_{2^{367}}$	—	—	303	1 386	2 234	1
Optimal Eta pairing $\eta_{[c_0,c_1]}(\overline{D}_1, \overline{D}_2)$ over $C_0(\mathbb{F}_{2^{367}})$	Deg.	Deg.	7 894	40 356	11 571	1
	Gen.	Deg.	15 293	64 644	15 472	1
	Gen.	Gen.	31 644	118 382	19 161	1

In the two following sections, as a proof of concept, we detail the software and hardware implementation results of the proposed optimal Eta pairing $\eta_{[c_0,c_1]}$. The selected curve is C_0 (*i.e.*, $d = 0$) over the field $\mathbb{F}_{2^{367}}$. One can check that $\#\,\mathrm{Jac}_{C_0}(\mathbb{F}_{2^{367}}) = 13 \cdot 7170258097 \cdot \ell$, where ℓ is a 698-bit prime, while the finite field $\mathbb{F}_{2^{12\cdot 367}}$ ensures a security of 128 bits for the computation of discrete logarithms via the function field sieve. The costs of the optimal Eta pairing on $C_0(\mathbb{F}_{2^{367}})$ are also given in Table 1.

For comparison purposes, one might compare this with the costs for the η_T pairing over C_d presented in [14] and [32]. In the former, Chatterjee *et al.* report a cost of 15 111 $\mathbb{F}_{2^m}$-multiplications for an η_T pairing on two degenerate divisors over $C_0(\mathbb{F}_{2^{459}})$. Since the number of these multiplications scales linearly with the size of the field, their approach would entail roughly 12 000 multiplications over our curve. In [32], Lee and Lee require 11 488 multiplications for an η_T pairing on two general divisors over $C_d(\mathbb{F}_{2^{79}})$, which would scale to approximately 53 000 multiplications on our curve $C_0(\mathbb{F}_{2^{367}})$. When compared to the figures in Table 1, these costs reflect the 33% improvement achieved thanks to our proposed optimal Eta approach.

5 Software Implementation

A software implementation was realized to illustrate the performance of the proposed pairing. The C programming language was used in conjunction with compiler intrinsics for accessing vector instructions. The chosen compiler was GCC version 4.6.2 with compiler flags including optimization level `-O3`, loop unrolling and platform-dependent tuning with `-march=native`. For evaluation, we considered as target platforms the Core 2 Duo 45 nm (Penryn microarchitecture) and Core i5 32 nm (Nehalem microarchitecture), represented by an Intel Xeon X3320 2.5 GHz and a mobile Intel Core i5 540 2.53 GHz with Turbo Boost disabled, respectively. Field arithmetic was implemented following the vectorization-friendly formulation presented in [2], with the exception of the Core i5 platform, where multiplication in $\mathbb{F}_{2^{367}}$ was implemented with the help of the native binary field multiplier [26] following the guidelines suggested in [42], that is, a 128-bit granular organization consisting of 3-way and 2-way Karatsuba formulas. We obtained timings of 7, 41, 464 and 11162 cycles for addition, squaring, multiplication and inversion in the Core 2, respectively; and efficiency gains of 47% and 27% for multiplication and inversion in the Core i5, respectively.

Table 2 presents our timings in millions of cycles for the pairing computation at the 128-bit security level. Timings from several related works are also collected for direct comparison with our software implementation. Our implementation considers all the three possible choices of divisors: general × general (GG), general × degenerate (GD) and degenerate × degenerate (DD); and presents the proposed genus-2 optimal Eta pairing as a very efficient candidate among the Type-1 pairings defined on supersingular curves over small-characteristic fields. In particular, the proposed pairing is more efficient than all other Type-1 pairings when at least one of the arguments is degenerate. Considering the Nehalem microarchitecture as a trend for future 64-bit computing platforms, the proposed pairing computed with degenerate divisors is also the closest in terms of performance to the current speed record for Type-3 pairing computation [1].

Table 2. Software implementations of pairing at the 128-bit security level. Timings were obtained with the Turbo Boost feature turned off, and therefore are compatible with the timings in Table 4 of the extended version of [1].

Implementation	Curve	Pairing	Intel Core 2 ($\times 10^6$ cycles)	Intel Core Nehalem ($\times 10^6$ cycles)
Beuchat *et al.* [8]	$E(\mathbb{F}_{2^{1223}})$	η_T	23.03	—
	$E(\mathbb{F}_{3^{359}})$		15.13	—
Aranha *et al.* [3], [4]	$E(\mathbb{F}_{2^{1223}})$	η_T	18.76	8.28
Chatterjee *et al.* [14]	$E(\mathbb{F}_{2^{1223}})$	η_T	19.0	—
	$E(\mathbb{F}_{3^{359}})$		15.8	—
	$C_0(\mathbb{F}_{2^{439}})$	η_T (DD)	16.4	—
Naehrig *et al.* [38]	$E(\mathbb{F}_p)$	Opt. Ate	4.38	—
Beuchat *et al.* [7]	$E(\mathbb{F}_p)$	Opt. Ate	2.95	2.82*
Aranha *et al.* [1]	$E(\mathbb{F}_p)$	Opt. Ate	2.19	2.04*
This work	$C_0(\mathbb{F}_{2^{367}})$	**Opt. Eta (DD)**	**4.44**	**2.75**
		Opt. Eta (GD)	**8.37**	**5.04**
		Opt. Eta (GG)	**16.95**	**9.90**

*Results adjusted by the maximum overclocking rate to eliminate the effect of Turbo Boost.

6 FPGA Implementation

We detail here an FPGA accelerator for our optimal Eta pairing on the curve $C_0(\mathbb{F}_{2^{367}})$ when both inputs are general divisors (GG). In [9], Beuchat *et al.* have presented a coprocessor architecture for computing the final exponentiation of the η_T pairing over supersingular curves. The core of their arithmetic and logic unit is a parallel–serial multiplier processing D coefficients of the multiplicand at each clock cycle, along with a unified operator supporting addition, Frobenius map, and n-fold Frobenius map. Intermediate results are stored in a register file implemented by means of dual-ported RAM. We decided to adapt such a finite field coprocessor for implementing our optimal Eta pairing. In the case of the finite field $\mathbb{F}_{2^{367}}$, we selected the parameters $D = 16$ and $n = 3$ for this coprocessor (*cf.* Appendix A for the details of the architecture). We prototyped our architecture on several Xilinx FPGAs with average speedgrade (Table 3). Place-and-route results show for instance that our pairing accelerator uses 4518 slices and 20 RAM blocks of a Virtex-4 device clocked at 220 MHz. For comparison purposes, we also included recent hardware implementation results from the literature in Table 3. It appears that our design is very compact and that its computation time remains comparable to other 128-bit-security implementations. This is even more so when noting that our performance estimates are given for the pairing of two general divisors, and that a speedup of 2 or 4 might be expected from the use of one or two degenerate divisors, respectively.

Table 3. FPGA implementations of pairings at medium- and high-security levels.

Implementation	**Curve**	**Sec. (bits)**	**FPGA**	**Area (slices)**	**Freq. (MHz)**	**Time (μs)**	**Area×time (slices·s)**
Ronan *et al.* [39]	$C_0(\mathbb{F}_{2^{103}})$ (DD)	75	xc2vp100-6	30464	41	132	4.02
Beuchat *et al.* [9]	$E(\mathbb{F}_{2^{691}})$	105	xc4vlx200-11	78874	130	19	1.48
	$E(\mathbb{F}_{3^{313}})$	109	xc4vlx200-11	97105	159	17	1.64
Cheung *et al.* [15]	$E(\mathbb{F}_{p_{254}})$	126	xc6vlx240t-2	7032*	250	573	4.03
Ghosh *et al.* [23]	$E(\mathbb{F}_{2^{1223}})$	128	xc4vlx200-11	35458	168	286	10.14
			xc6vlx130t-3	15167	250	190	2.88
Estibals [17]	$E(\mathbb{F}_{3^{5\cdot 97}})$	128	xc4vlx25-11	4755	192	2227	10.59
			xc3s1000-5	4713	104	4113	19.38
This work	$C_0(\mathbb{F}_{2^{367}})$ **(GG)**	**128**	**xc2vp30-6**	**4646**	**176**	**4405**	**20.5**
			xc4vlx25-11	**4518**	**220**	**3518**	**15.9**
			xc3s1500-5	**4713**	**114**	**6800**	**32.0**

*Number of Virtex-6 slices; this design also uses 32 embedded DSP blocks.

7 Conclusion and Perspectives

We presented a novel optimal Eta pairing algorithm on supersingular genus-2 binary hyperelliptic curves. Starting from Vercauteren's work on optimal pairings [43], we described how to exploit the action of the 2^{3m}-th power Verschiebung in order to further reduce the loop length of Miller's algorithm with respect to the genus-2 η_T approach [5], thus resulting in a 33% improvement.

In order to demonstrate the efficiency of our approach, we implemented the optimal Eta pairing at the 128-bit security level in software and hardware. As far as Type-1 pairings are concerned, our results show that genus-2 curves are a very effective alternative to supersingular elliptic curves and can even compete with the Type-3 pairings provided by ordinary curves such as BN curves.

We have designed as well an FPGA coprocessor for computing the proposed pairing, which also compares very well against other hardware pairing implementations. Additionally, this is the first known hardware pairing implementation over a genus-2 hyperelliptic curve reaching 128 bits of security.

Building upon this work, we now plan to study more precisely the action of other purely inseparable maps on C_d along with the corresponding pairing algorithms, so as to identify which one is the most efficient from an implementation point of view. Indeed, apart from the presented optimal Eta pairing based on the action of $\hat{\phi}_{2^{3m}}$, one can also construct optimal Ate pairings using the action of $\phi_{2^{3m}}$, or that of ϕ_{2^m} under the distortion map σ_θ, the most promising candidate being the optimal Ate pairing for the action of ϕ_{2^m} under the distortion map $\psi = (2^{3m} + \phi_{2^m})\sigma_\tau$.

Furthermore, Lubicz & Robert have recently presented a novel technique for computing the Weil and Tate pairings over abelian varieties based on an efficient representation of their elements by means of theta functions [33]. We are planning to investigate the application of this method to the case of our proposed genus-2 optimal Eta pairing, as both software and hardware implementations might benefit from the faster arithmetic of theta functions.

Acknowledgments

First of all, the authors would like to express their deepest thanks to Guillaume Hanrot who advised us to have a go at genus-2 pairings. He shall receive here our utmost gratitude. The authors would also like to thank Pierrick Gaudry for the careful proof-reading of the technical sections of this paper, along with Gaëtan Bisson, Romain Cosset, and Emmanuel Thomé who were always available to provide some clear answers to our many questions. Last but definitely not least, the authors would like to thank the anonymous reviewers for their insightful comments and suggestions for improving this paper.

References

1. Aranha, D.F., Karabina, K., Longa, P., Gebotys, C., López, J.: Faster explicit formulas for computing pairings over ordinary curves. In: Paterson, K. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 48–68. Springer (2011)
2. Aranha, D.F., López, J., Hankerson, D.: Efficient software implementation of binary field arithmetic using vector instruction sets. In: Abdalla, M., Barreto, P. (eds.) LATINCRYPT 2010. LNCS, vol. 6212, pp. 144–161. Springer (2010)
3. Aranha, D.F., López, J., Hankerson, D.: High-speed parallel software implementation of the η_T pairing. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 89–105. Springer (2010)
4. Aranha, D.F., Menezes, A., Knapp, E., Rodríguez-Henríquez, F.: Parallelizing the Weil and Tate pairings. In: IMA-CC (2011), to appear.

5. Barreto, P., Galbraith, S., Ó Éigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular Abelian varieties. Des. Codes Crypt. 42, 239–271 (2007)
6. Barreto, P., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer (2006)
7. Beuchat, J.L., Díaz, J.G., Mitsunari, S., Okamoto, E., Rodríguez-Henríquez, F., Teruya, T.: High-speed software implementation of the optimal ate pairing over Barreto–Naehrig curves. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing 2010. pp. 21–39. No. 6487 in LNCS, Springer (2010)
8. Beuchat, J.L., López-Trejo, E., Martínez-Ramos, L., Mitsunari, S., Rodríguez-Henríquez, F.: Multi-core implementation of the Tate pairing over supersingular elliptic curves. In: Garay, J., Miyaji, A., Otsuka, A. (eds.) CANS 2009. pp. 413–432. No. 5888 in LNCS, Springer (2009)
9. Beuchat, J.L., Detrey, J., Estibals, N., Okamoto, E., Rodríguez-Henríquez, F.: Fast architectures for the η_T pairing over small-characteristic supersingular elliptic curves. Bruguera, J., Cornea, M., Das Sarma, D. (eds.) IEEE Trans. Comput. 60(2), 266–281 (2011)
10. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. pp. 213–229. No. 2139 in LNCS, Springer (2001)
11. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. pp. 258–275. No. 3621 in LNCS, Springer (2005)
12. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. pp. 514–532. No. 2248 in LNCS, Springer (2001)
13. Cantor, D.: Computing in the Jacobian of a hyperelliptic curve. Math. Comput. 48(177), 95–101 (1987)
14. Chatterjee, S., Hankerson, D., Menezes, A.: On the efficiency and security of pairing-based protocols in the type 1 and type 4 settings. In: Hasan, M., Helleseth, T. (eds.) WAIFI 2010. LNCS, vol. 6087, pp. 114–134. Springer (2010)
15. Cheung, R., Duquesne, S., Fan, J., Guillermin, N., Verbauwhede, I., Yao, G.: FPGA implementation of pairings using residue number system and lazy reduction. In: Preneel, B., Takagi, T. (eds.) CHES 2011. pp. 421–441. No. 6917 in LNCS, Springer (2011)
16. Cohen, H., Frey, G. (eds.): Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathematics and its Applications, Chapman & Hall/CRC (2006)
17. Estibals, N.: Compact hardware for computing the Tate pairing over 128-bit-security supersingular curves. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing 2010. pp. 397–416. No. 6487 in LNCS, Springer (2010)
18. Frey, G., Rück, H.G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comput. 62(206), 865–874 (1994)
19. Galbraith, S., Paterson, K., Smart, N.: Pairings for cryptographers. Discrete Applied Mathematics 156, 3113–3121 (2008)
20. Galbraith, S.: Supersingular curves in cryptography. In: Boyd, C. (ed.) ASIACRYPT 2001. pp. 495–513. No. 2248 in LNCS, Springer (2001)
21. Galbraith, S.D., Pujolàs, J., Ritzenthaler, C., Smith, B.: Distortion maps for genus two curves. J. Math. Cryptol. 3(1), 1–18 (2009)
22. Gaudry, P., Hess, F., Smart, N.: Constructive and destructive facets of Weil descent on elliptic curves. J. Cryptol. 15(1), 19–46 (2001)
23. Ghosh, S., Roychowdhury, D., Das, A.: High speed cryptoprocessor for η_T pairing on 128-bit secure supersingular elliptic curves over characteristic two fields. In: Preneel, B., Takagi, T. (eds.) CHES 2011. pp. 442–458. No. 6917 in LNCS, Springer (2011)

24. Granger, R., Hess, F., Oyono, R., Thériault, N., Vercauteren, F.: Ate pairing on hyperelliptic curves. In: Naor, M. (ed.) EUROCRYPT 2007. pp. 430–447. No. 4515 in LNCS, Springer (2007)
25. Granger, R., Page, D., Smart, N.: High security pairing-based cryptography revisited. In: Hess, F., Pauli, S., Pohst, M. (eds.) ANTS VII. pp. 480–494. No. 4076 in LNCS, Springer (2006)
26. Gueron, S., Kounavis, M.E.: Carry-less multiplication and its usage for computing the GCM mode. White paper (2010), `http://software.intel.com/file/24918`
27. Hess, F.: Pairing lattices. In: Galbraith, S., Paterson, K. (eds.) Pairing 2008. pp. 18–38. No. 5209 in LNCS, Springer (2008)
28. Hess, F., Smart, N., Vercauteren, F.: The Eta pairing revisited. IEEE Trans. Inf. Theory 52(10), 4595–4602 (2006)
29. Joux, A.: A one round protocol for tripartite Diffie–Hellman. In: Bosma, W. (ed.) ANTS IV. pp. 385–394. No. 1838 in LNCS, Springer (2000)
30. Koblitz, N., Menezes, A.: Pairing-based cryptography at high security levels. In: Smart, N. (ed.) IMA-CC. pp. 13–36. No. 3796 in LNCS, Springer (2005)
31. Lee, E., Lee, H.S., Park, C.M.: Efficient and generalized pairing computation on abelian varieties (2009)
32. Lee, E., Lee, Y.: Tate pairing computation on the divisors of hyperelliptic curves of genus 2. J. Korean Math. Soc. 45(4), 1057–1073 (2008)
33. Lubicz, D., Robert, D.: Efficient pairing computation with Theta functions. In: Hanrot, G., Morain, F., Thomé, E. (eds.) ANTS IX. LNCS, vol. 6197, pp. 251–269. Springer (2010)
34. Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curves logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory 39(5), 1639–1646 (1993)
35. Miller, V.: Short programs for functions on curves (1986), unpublished manuscript available at `http://crypto.stanford.edu/miller`
36. Miller, V.: The Weil pairing, and its efficient calculation. J. Cryptol. 17(4), 235–261 (2004)
37. Mitsunari, S., Sakai, R., Kasahara, M.: A new traitor tracing. IEICE Trans. Fundamentals E85–A(2), 481–484 (2002)
38. Naehrig, M., Niederhagen, R., Schwabe, P.: New software speed records for cryptographic pairings. In: Abdalla, M., Barreto, P. (eds.) LATINCRYPT 2010. pp. 109–123. No. 6212 in LNCS, Springer (2010)
39. Ronan, R., Ó hÉigeartaigh, C., Murphy, C., Scott, M., Kerins, T.: Hardware acceleration of the Tate pairing on a genus 2 hyperelliptic curve. J. Syst. Architect. 53, 85–98 (2007)
40. Rubin, K., Silverberg, A.: Using Abelian varieties to improve pairing-based cryptography. J. Cryptol. 22(3), 330–364 (2009)
41. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: SCIS 2000. pp. 26–28 (2000)
42. Taverne, J., Faz-Hernández, A., Aranha, D.F., Rodríguez-Henríquez, F., Hankerson, D., López, J.: Speeding scalar multiplication over binary elliptic curves using the new carry-less multiplication instruction. J. Cryptographic Engineering 1(3), 187–199 (2011)
43. Vercauteren, F.: Optimal pairings. IEEE Trans. Inf. Theory 56(1), 455–461 (2010)
44. Verheul, E.R.: Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. J. Cryptol. 17(4), 277–296 (2004)

A Architecture of the hardware accelerator

We present in this section the design of the coprocessor by Beuchat *et al.* that we used for the computation of our optimal Eta pairing [9]. In order to best fit the arithmetic of $\mathbb{F}_{2^{367}}$, we parametrised their architecture as follows:

- The multiplier processes $D = 16$ coefficients and thus performs a multiplication over $\mathbb{F}_{2^{367}}$ in 23 clock cycles.
- We chose to support the 3-fold Frobenius map (*i.e.* raising to the eighth power) in the unified operator.
- The register file can store up to 127 intermediate variables belonging to $\mathbb{F}_{2^{367}}$ (46 kbit of RAM), along with the constant 1.

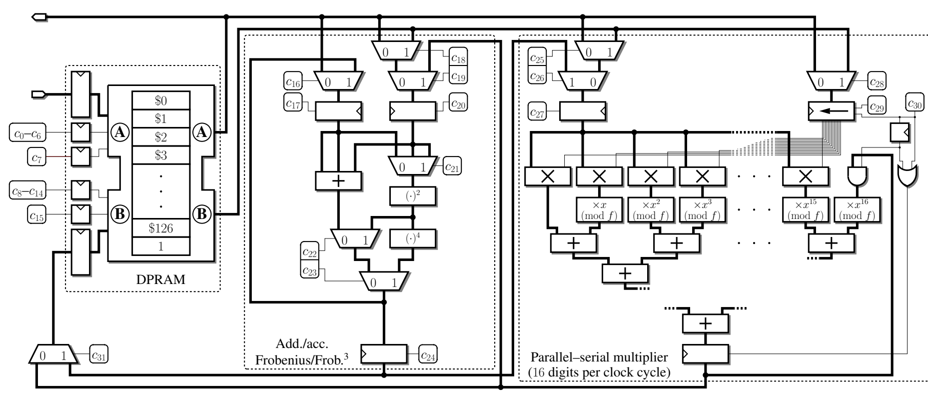

Fig. 1. A finite field coprocessor for $\mathbb{F}_{2^{367}}$.