Ate Pairing on Hyperelliptic Curves

R. Granger[1*], F. Hess[2], R. Oyono[3], N. Thériault[4**], and F. Vercauteren[5***]

[1] Dept. Computer Science, University of Bristol
MVB, Woodland Road, Bristol, BS8 1UB, United Kingdom
granger@cs.bris.ac.uk
[2] Technische Universität Berlin,
Fakultät II, Institut für Mathematik Sekr. MA 8-1,
Strasse des 17. Juni 136, D-10623 Berlin, Germany.
hess@math.tu-berlin.de
[3] University of Waterloo,
Department of Combinatorics and Optimization,
Waterloo, Ontario, N2L 3G1, Canada.
royono@uwaterloo.ca
[4] Instituto de Matemática y Física,
Universidad de Talca, Casilla 747, Talca, Chile.
ntheriau@inst-mat.utalca.cl
[5] Department of Electrical Engineering, Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
frederik.vercauteren@esat.kuleuven.be

Abstract. In this paper we show that the Ate pairing, originally defined for elliptic curves, generalises to hyperelliptic curves and in fact to arbitrary algebraic curves. It has the following surprising properties: The loop length in Miller's algorithm can be up to g times shorter than for the Tate pairing, with g the genus of the curve, and the pairing is automatically reduced, i.e. no final exponentiation is needed.
Keywords: Tate pairing, Ate pairing, hyperelliptic curves, finite fields.

1 Introduction

Pairings in cryptography have received a fast growing interest in the past six years and are currently a major topic in cryptologic research. Investigations are carried out regarding the use of pairings in cryptographic protocols on one side and regarding mathematical, algorithmic foundations of pairings on the other side.

The present paper conducts investigations of the latter type. Building on and generalising ideas from [5, 7, 4, 10, 17] into a common framework, the main result of the paper consists in providing new classes of efficient non-degenerate pairings on higher genus algebraic curves, called Ate pairings and superspecial Ate

* Funded by the EPSRC
** This work was done in part while the author was at the Fields Institute, Toronto, Canada
*** Postdoctoral Fellow of the Research Foundation - Flanders (FWO)

pairings, which feature some surprising properties. These pairings are different from the well known Weil and Tate pairings in that they are defined by much simpler algebraic expressions. Of course, for prime order groups any pairing can be obtained as a suitable power of any fixed non-degenerate pairing, and we also exhibit these powers for our pairings in relation to the Tate pairing.

The surprising properties of the Ate and superspecial Ate pairings are the following: Firstly, the loop length in Miller's algorithm for evaluating the pairing function is up to g times shorter than for the corresponding Tate pairing, where g is the genus of the underlying curve C. Secondly, the pairing is automatically reduced, that is, the final exponentiation required by the Tate pairing can be omitted.

There are constructive and destructive aspects regarding the relevance of our pairings to cryptography. A discussion of constructive aspects of the Tate pairing in higher genus has been carried out in [8]. The main point here is that pairings in higher genus can make use of degenerate divisors $D_2 = (Q)$, leading to more efficient evaluation and possibly some bandwidth savings due to compression. While this gives an improvement of a factor of up to g in comparison with general D_2 of degree g, the efficiency comparison with the Ate pairing in genus one is less favourable as indicated in Appendix A.

The destructive aspects of our pairings concern pairing inversion and the difficulty of the computational Diffie-Hellman problem in finite fields. In [24] it was shown that the computational Diffie-Hellman problem in the two domains of the pairing as well as in the codomain can be efficiently reduced to the problem of computing preimages of pairing values for each argument, given a fixed opposite argument. The absence of the final powering in our pairings and the fact that the degree of the pairing function is independent of the prime group order, and can hence be very small, raises questions about the hardness of pairing inversion. What can be stated at the moment is that Ate and thus Tate pairing inversion for small q, solving for degenerate divisors $D_2 = (Q)$ in the second argument, is actually efficient and straightforward (roughly as hard as computing the roots of a polynomial of degree qg over an extension of degree about gk of $\mathbb{F}_q$ where k is the embedding degree). In protocols it is hence prudent to restrict to public degenerate divisors. As of now, the precise security implications of our pairings are unknown and much more research is needed for an assessment.

Although we state most results for hyperelliptic curves only, the theory and proofs do actually not require the hyperellipticity and readily apply to general non-singular curves with a distinguished point P_∞, once the definition of "reduced divisor" has been adopted accordingly (see for example [15]). We leave these details to the interested reader.

The remainder of this paper is organised as follows: Section 2 recalls basic properties of hyperelliptic curves and the Tate-Lichtenbaum pairing. Section 3 defines the Ate pairing on all curves and proves that it is well-defined. This is then adapted in Section 4 to superspecial curves. Finally, Section 5 concludes the paper and Appendix A provides detailed performance estimates.

2 Mathematical Background

In this section, we briefly recall arithmetic on hyperelliptic curves, the definition of the Tate-Lichtenbaum pairing and Miller's algorithm to compute it.

2.1 Hyperelliptic Curves

Let C be a nonsingular hyperelliptic curve of genus g defined over a finite field $\mathbb{F}_q$ with $q = p^n$ elements. In the remainder of the paper, we will assume that C is an imaginary hyperelliptic curve and thus has only one point P_∞ at infinity and its affine part is given by

$$y^2 + h(x)y = f(x) \ ,$$

with $h, f \in \mathbb{F}_q[x]$, $\deg h \leq g$, f monic and $\deg f = 2g + 1$.

For any algebraic extension K of $\mathbb{F}_q$ consider the set

$$C(K) := \{(x, y) \in K \times K \mid y^2 + h(x)y = f(x)\} \cup \{P_\infty\} \ ,$$

called the set of K-rational points on C. The hyperelliptic involution ι defined by $\iota(x, y) = (x, -y-h(x))$ acts on the set $C(K)$. However, unlike elliptic curves, the set $C(K)$ for $g \geq 2$ does not form a group, but we can embed C into an abelian variety of dimension g called the Jacobian of C and denoted by J_C. As usual, we will represent elements of $J_C(K)$ by elements of the divisor class group of degree 0 divisors $\mathrm{Div}_C^0(K)/\mathrm{Prin}_C(K)$, the definition of which is recalled in the following paragraphs.

A divisor D on C is a formal sum of points over the algebraic closure $\overline{\mathbb{F}}_q$

$$D = \sum_{P \in C(\overline{\mathbb{F}}_q)} c_P(P)$$

with only finitely many non-zero coefficients $c_P \in \mathbb{Z}$. The set of all divisors on C is denoted Div_C and clearly forms a group under formal addition. The degree of D is defined as $\deg(D) = \sum_{P \in C(\overline{\mathbb{F}}_q)} c_P$ and the subgroup of degree 0 divisors is denoted by Div_C^0. The support $\mathrm{supp}(D)$ of a divisor D is the set of points P with $c_P \neq 0$ and we define $\mathrm{ord}_P(D) = c_P$.

Let φ be the Frobenius morphism $\varphi : C \to C$ given by $\varphi(x, y) = (x^q, y^q)$ and define

$$\varphi(D) = \sum_{P \in C(\overline{\mathbb{F}}_q)} c_P(\varphi(P)),$$

then D is called $\mathbb{F}_{q^k}$-rational if and only if $\varphi^k(D) = D$. The set of $\mathbb{F}_{q^k}$-rational divisors is denoted by $\mathrm{Div}_C(\mathbb{F}_{q^k})$ and similarly for the degree 0 divisors. To each non-constant rational function $f \in \overline{\mathbb{F}}_q(C)^*$, we can associate the divisor $\mathrm{div}(f) = \sum_{P \in C(\overline{\mathbb{F}}_q)} \mathrm{ord}_P(f)(P)$, where $\mathrm{ord}_P(f)$ denotes the order of vanishing of f at P, i.e. $\mathrm{ord}_P(f) \neq 0$ if and only if f has either a zero or pole at P and

$\text{ord}_P(f)$ then equals the multiplicity of f at P. One can prove that only finitely many $\text{ord}_P(f)$ are non-zero and furthermore, that $\deg(\text{div}(f)) = 0$. Any divisor of the form $\text{div}(f)$ with $f \in \overline{\mathbb{F}}_q(C)^*$ is called a principal divisor and the set of all these divisors is denoted Prin_C. By definition we have $J_C = \text{Div}_C^0/\text{Prin}_C$ and $J_C(\mathbb{F}_{q^k}) = \text{Div}_C^0(\mathbb{F}_{q^k})/\text{Prin}_C(\mathbb{F}_{q^k})$, where $\text{Prin}_C(\mathbb{F}_{q^k}) = \text{Prin}_C \cap \text{Div}_C^0(\mathbb{F}_{q^k})$. Given a degree 0 divisor D, we will denote by $\overline{D}$ the corresponding divisor class in J_C.

Each divisor class $\overline{D}$ can be uniquely represented by a so called reduced divisor, i.e. a divisor of the form

$$\sum\nolimits_{i=1}^{m}(P_i) - m(P_\infty) \ , \qquad m \leq g$$

with $P_i = (x_i, y_i) \in C(\overline{\mathbb{F}}_q)$, $P_i \neq P_\infty$ and $P_i \neq \iota(P_j)$ for $i \neq j$. For notational convenience, we introduce two maps on J_C: given a divisor class $\overline{D}$, we define $\rho(\overline{D})$ the unique reduced divisor in $\overline{D}$ and $\epsilon(\overline{D})$ the effective part of $\rho(\overline{D})$, i.e. $\rho(\overline{D}) = \epsilon(\overline{D}) - \deg(\epsilon(\overline{D}))(P_\infty)$. Note that the sets $\rho(J_C)$ and $\epsilon(J_C)$ can be endowed with a group law $\oplus$ by defining: $\rho(\overline{D}_1) \oplus \rho(\overline{D}_2) := \rho(\overline{D}_1 + \overline{D}_2)$ and similarly, $\epsilon(\overline{D}_1) \oplus \epsilon(\overline{D}_2) := \epsilon(\overline{D}_1 + \overline{D}_2)$. Furthermore, the notion of rationality is well defined since $P_\infty \in C(\mathbb{F}_q)$.

It is not difficult to show that any reduced $\mathbb{F}_q$-rational divisor admits a Mumford representation $[u(x), v(x)]$, i.e. a pair of polynomials $u, v \in \mathbb{F}_q[x]$, with $u = \prod_{i=1}^{m}(x - x_i)$, $\deg v < \deg u \leq g$ and $u | v^2 + vh - f$. Cantor's algorithm [6] can be used to compute the Mumford representation of the sum of two reduced divisors or for small genera, explicit formulae exist [3, 14, 18].

Given a divisor D representing a divisor class $\overline{D}$ in J_C and an integer n, we denote $[n]D := \rho(n\overline{D})$, i.e. the unique reduced divisor equivalent with nD. Finally, for D an $\mathbb{F}_{q^k}$-rational divisor, we denote by $f_{n,D} \in \mathbb{F}_{q^k}(C)$ any function (determined up to non-zero constant multiple) for which $\text{div}(f_{n,D}) = nD - [n]D$.

2.2 Tate-Lichtenbaum Pairing

In this section, we briefly recall the definition of the Tate-Lichtenbaum pairing as it is usually stated in the literature and discuss the various alternatives for the domain of the pairing.

Let r be a prime with $r \mid \#J_C(\mathbb{F}_q)$ and $\gcd(r, q) = 1$ and let k be the smallest integer such that $r \mid (q^k - 1)$, then k is called the embedding degree (dependent on r). Note that this implies that the r-th roots of unity μ_r are contained in $\mathbb{F}_{q^k}$ and in no strictly smaller extension of $\mathbb{F}_q$. Note that $r > k$, since k is the order of q modulo r and hence $k \mid r - 1$ holds. Denote with $J_C(\mathbb{F}_{q^k})[r]$ the r-torsion points on J_C defined over $\mathbb{F}_{q^k}$. The Tate-Lichtenbaum pairing is a well defined, non-degenerate, bilinear pairing [9, 16]

$$\langle \cdot, \cdot \rangle_r : J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \ ,$$

which is defined as follows: let $\overline{D}_1 \in J_C(\mathbb{F}_{q^k})[r]$ and $\overline{D}_2 \in J_C(\mathbb{F}_{q^k})$ and let $\overline{D}_1$ be represented by a divisor D_1 and $\overline{D}_2$ by a divisor D_2 with $\text{supp}(D_1) \cap$

$\operatorname{supp}(D_2) = \emptyset$. Since $\overline{D}_1$ has order r, the function $f_{r,D_1} \in \mathbb{F}_{q^k}(C)^*$ has divisor $\operatorname{div}(f_{r,D_1}) = rD_1 - [r]D_1 = rD_1$. The Tate-Lichtenbaum pairing of the divisor classes $\overline{D}_1$ and $\overline{D}_2$ is then defined by

$$\langle \overline{D}_1, \overline{D}_2 \rangle_r \equiv f_{r,D_1}(D_2) = \prod_{P \in C(\overline{\mathbb{F}}_q)} f_{r,D_1}(P)^{\operatorname{ord}_P(D_2)} \ ,$$

where $\equiv$ means equality up to r-th powers. Note that since D_2 has degree 0, multiplying f_{r,D_1} by a non-zero constant will give the same result.

In implementations, one works with the Mumford representation, i.e. with reduced divisors D_1 and D_2, but the Tate pairing cannot be computed as $f_{r,D_1}(D_2)$, since $P_\infty \in \operatorname{supp}(D_1) \cap \operatorname{supp}(D_2)$. The following lemma shows that if the function f_{r,D_1} is properly normalised, the Tate pairing can simply be computed as $f_{r,D_1}(\epsilon(\overline{D}_2))$. To state the lemma, we need the notion of leading coefficient: let u_∞ be a fixed $\mathbb{F}_q$-rational uniformizer at P_∞, then for any function $f \in \overline{\mathbb{F}}_q(C)^*$ we define $\operatorname{lc}_\infty(f)$ to be the leading coefficient of f as a Laurent series in u_∞. Note that when f is defined at P_∞ we simply have $f(P_\infty) = \operatorname{lc}_\infty(f)$ independent of the uniformizer chosen.

Lemma 1. *Let* $\overline{D}_1 \in J_C(\mathbb{F}_{q^k})[r]$, $D_1 = \rho(\overline{D}_1)$ *and* $\overline{D}_2 \in J_C(\mathbb{F}_{q^k})$ *and assume that* $\operatorname{supp}(D_1) \cap \operatorname{supp}(\epsilon(\overline{D}_2)) = \emptyset$, *then*

$$\langle \overline{D}_1, \overline{D}_2 \rangle_r \equiv f_{r,D_1}(\epsilon(\overline{D}_2))$$

if and only if $\operatorname{lc}_\infty(f_{r,D_1}) \in (\mathbb{F}_{q^k}^*)^r$. *Furthermore,* $\operatorname{lc}_\infty(f_{r,D_1})$ *being an r-th power is independent of the uniformizer chosen.*

Proof: Let $D_2 = \rho(\overline{D}_2)$ and choose $h \in \mathbb{F}_{q^k}(C)$ such that $D_1' = D_1 + \operatorname{div}(h)$ satisfies $\operatorname{supp}(D_1') \cap \operatorname{supp}(D_2) = \emptyset$, then by definition we have

$$\langle \overline{D}_1, \overline{D}_2 \rangle_r \equiv f_{r,D_1'}(D_2) \ .$$

Since $D_1' = D_1 + \operatorname{div}(h)$, we can take $f_{r,D_1'} = f_{r,D_1} h^r$ (in fact we could multiply $f_{r,D_1'}$ with a constant c, but this would give the same result as remarked before) and thus

$$\langle \overline{D}_1, \overline{D}_2 \rangle_r \equiv (f_{r,D_1} h^r)(D_2) \equiv \frac{(f_{r,D_1} h^r)(\epsilon(\overline{D}_2))}{\operatorname{lc}_\infty(f_{r,D_1} h^r)^{m_2}} \equiv \frac{f_{r,D_1}(\epsilon(\overline{D}_2))}{\operatorname{lc}_\infty(f_{r,D_1})^{m_2}} \ ,$$

with $m_2 = \deg(\epsilon(\overline{D}_2))$. Finally, $\gcd(m_2, r) = 1$ implies that $\operatorname{lc}_\infty(f_{r,D_1})^{m_2}$ is an r-th power if and only if $\operatorname{lc}_\infty(f_{r,D_1})$ is an r-th power. Furthermore, since $\operatorname{ord}_{P_\infty}(f_{r,D_1}) = -\deg(\epsilon(\overline{D}_1))r$, i.e. a multiple of r, the property of $\operatorname{lc}_\infty(f_{r,D_1})$ being an r-th power does not depend on the uniformizer chosen. $\square$

In practice, one often requires a unique pairing value instead of a whole coset; therefore one defines the reduced Tate-Lichtenbaum pairing as

$$e(\overline{D}_1, \overline{D}_2) = \langle \overline{D}_1, \overline{D}_2 \rangle_r^{(q^k-1)/r} \in \mu_r \subset \mathbb{F}_{q^k}^* \ .$$

It is easy to see that for any positive integer N with $r|N$ and $N|q^k - 1$ we have

$$e(\overline{D}_1, \overline{D}_2) = \langle \overline{D}_1, \overline{D}_2 \rangle_r^{(q^k-1)/r} = \langle \overline{D}_1, \overline{D}_2 \rangle_N^{(q^k-1)/N} \quad . \tag{1}$$

For $k > 1$ and $\overline{D}_1 \in J_C(\mathbb{F}_q)$, the reduced Tate-Lichtenbaum pairing can be computed as in Lemma 1, but without the need for normalisation. Indeed, since $\rho(\overline{D}_1)$ is $\mathbb{F}_q$-rational, we conclude that $f_{r,D_1} \in \mathbb{F}_q(C)$ and thus $\mathrm{lc}_\infty(f_{r,D_1}) \in \mathbb{F}_q^* \subset (\mathbb{F}_{q^k}^*)^r$. For elliptic curves, this simplification was first noticed in [5] using a more direct proof than that of Lemma 1.

For efficiency reasons, one restricts the domain of the Tate-Lichtenbaum pairing to the groups $\mathbb{G}_1 = J_C[r] \cap \mathrm{Ker}(\varphi - [1])$ and the group $\mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}(\varphi - [q])$, i.e. the eigenspaces of the Frobenius endomorphism on $J_C[r]$. Note that $\mathbb{G}_1 \subset J_C(\mathbb{F}_q)$ and $\mathbb{G}_2 \subset J_C(\mathbb{F}_{q^k})$, since for $\overline{D} \in \mathbb{G}_2$ we have $\varphi^k(\overline{D}) = [q^k]\overline{D} = \overline{D}$, because $\overline{D} \in J_C[r]$ and $q^k \equiv 1 \bmod r$. This also shows that k is the smallest integer such that the q-eigenspace of the Frobenius in $J_C[r]$ is $\mathbb{F}_{q^k}$-rational.

Remark 1. In the remainder of the paper we will assume that any representative D_1 of $\overline{D}_1 \in \mathbb{G}_1$ (resp. D_2 of $\overline{D}_2 \in \mathbb{G}_2$) is chosen to be $\mathbb{F}_q$-rational (resp. $\mathbb{F}_{q^k}$-rational).

Remark 2. In general, the smallest extension degree d such that the whole r-torsion $J_C[r]$ is $\mathbb{F}_{q^d}$-rational is larger than k [9]. This is obvious for $g \geq 2$, since $J_C[r] \simeq (\mathbb{Z}/r\mathbb{Z})^{2g}$, but even for elliptic curves, this phenomenon occurs: consider an elliptic curve $E/\mathbb{F}_q$ with $r \mid \#E(\mathbb{F}_q)$ and $r \mid q-1$, but such that $r^2 \nmid \#E(\mathbb{F}_q)$. In this case $E(\mathbb{F}_q)[r]$ is both the 1-eigenspace and q-eigenspace and the minimal d such that $E[r] \subset E(\mathbb{F}_{q^d})$ is equal to r.

Finally, we note that the group $\mathbb{G}_2$ already occurs in the original paper [9] disguised as a Galois cohomology group $H^1(G, J_C)[r]$, with G the absolute Galois group of $\mathbb{F}_q$. In fact, in [2][Section 6.3.1] one finds that the Tate-Lichtenbaum pairing has as domain $\mathbb{G}_2 \times J_C(\mathbb{F}_q)/rJ_C(\mathbb{F}_q)$, which is yet another choice of subgroups.

2.3 Miller's Algorithm

In [20] (see also [21]), Miller described a fast algorithm to compute evaluations of the form $f_{r,D_1}(D_2)$ for divisors on elliptic curves. The algorithm easily generalises to hyperelliptic curves as follows: by definition of the group law $\oplus$ on J_C, there exists a function $G_{D_a,D_b} \in \mathbb{F}_{q^k}(C)^*$ with $\mathrm{div}(G_{D_a,D_b}) = D_a + D_b - (D_a \oplus D_b)$ where $D_a \oplus D_b$ is reduced. As such we can take the function

$$f_{i+j,D} = f_{i,D} f_{j,D} G_{[i]D,[j]D} \quad .$$

This immediately leads to Algorithm 1 and the more detailed version given in Algorithm 2.

Algorithm 1 Miller's algorithm for hyperelliptic curves

Inputs: $n \in \mathbb{N}$ and $D_a, D_b \in J_C$ with disjoint support
Outputs: $f_{n,D_a}(D_b)$

Write n as $\sum_{j=0}^{s} n_j 2^j$, with $n_j \in \{0,1\}$ and $n_s = 1$.
$D \leftarrow D_a$, $c \leftarrow 1$.
for $j = s-1$ down to 0 **do**
  Compute $D \leftarrow [2]D$ and extract $G_{D,D}$.
  $c \leftarrow c^2 \cdot G_{D,D}(D_b)$.
  if $n_j = 1$ **then**
    Compute $D \leftarrow D \oplus D_a$ and extract G_{D,D_a}.
    $c \leftarrow c \cdot G_{D,D_a}(D_b)$.
  end if
end for
Return c.

3 Ate Pairing on Hyperelliptic Curves

In this section, we first recall the Ate pairing for elliptic curves and then show that with a minor, but important change, it can be extended to hyperelliptic curves.

The two main ideas of the Ate pairing are that the domain of the pairing is $\mathbb{G}_2 \times \mathbb{G}_1$ and that the loop length in Miller's algorithm is much shorter than for the Tate-Lichtenbaum pairing. The result is summarised in the following theorem from [17].

Theorem 1. *Let E be an elliptic curve over $\mathbb{F}_q$, r a large prime with $r \mid \#E(\mathbb{F}_q)$ and denote the trace of Frobenius with t, i.e. $\#E(\mathbb{F}_q) = q+1-t$. For $T = t-1$, $Q \in \mathbb{G}_2 = E[r] \cap \operatorname{Ker}(\varphi - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap \operatorname{Ker}(\varphi - [1])$, we have the following:*

1. *$f_{T,Q}(P)$ defines a bilinear pairing, called the Ate pairing*
2. *let $N = \gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$, with k the embedding degree, then*
$$e(Q,P)^L = f_{T,Q}(P)^{c(q^k-1)/N}$$
where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv k q^{k-1} \bmod r$
3. *for $r \nmid L$, the Ate pairing is non-degenerate*

The reason why this construction works is the compatibility of the scalar $T = t-1$ and the action of the Frobenius on $\mathbb{G}_2$. Indeed, by definition of $\mathbb{G}_2$ we have $\varphi(Q) = [q]Q$, and since $r | \#E(\mathbb{F}_q) = q+1-t$ it follows that $\varphi(Q) = [T]Q$. This last equality also determines the loop length in Miller's algorithm, i.e. $\lceil \log_2 |T| \rceil$.

For a hyperelliptic curve C with $g > 1$, the situation is somewhat different. Indeed, in this case $r | \#J_C(\mathbb{F}_q) = q^g + a_1(q^{g-1}+1) + a_2(q^{g-2}+1) + \cdots + a_g$, so in general q cannot be replaced by a smaller equivalent. However, note that for $g > 1$ and $r \approx \#J_C(\mathbb{F}_q)$, the bit length of q itself is already g times shorter than the bit length of r, again resulting in a shorter loop in Miller's algorithm. The possibility of using $T = q$ is already present in [7], but for a very restricted family of curves. This observation leads to the following theorem.

Theorem 2. *Let C be a hyperelliptic curve over $\mathbb{F}_q$ and $r \mid \#J_C(\mathbb{F}_q)$ a large prime. Let $\mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}(\varphi - [q])$ and $\mathbb{G}_1 = J_C[r] \cap \mathrm{Ker}(\varphi - [1])$, then*

$$a(\cdot,\cdot) : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r : (\overline{D}_2, \overline{D}_1) \mapsto f_{q,D_2}(D_1)$$

with $D_2 = \rho(\overline{D}_2)$ and $D_1 \in \overline{D}_1$ such that $\mathrm{supp}(D_1) \cap \mathrm{supp}(D_2) = \emptyset$, *defines a non-degenerate, bilinear pairing called the hyperelliptic Ate pairing. Furthermore, the relation with the reduced Tate-Lichtenbaum pairing is as follows:*

$$e(\overline{D}_2, \overline{D}_1) = a(\overline{D}_2, \overline{D}_1)^{kq^{k-1}} . \tag{2}$$

Note that in Theorem 2, the divisor D_2 is assumed to be reduced and the function f_{q,D_2} is evaluated at the divisor D_1 and not only at $\epsilon(\overline{D}_1)$ (but see Lemma 6). Furthermore, the image of the hyperelliptic Ate pairing already is μ_r so no final exponentiation is required. The proof of Theorem 2 follows from the following four lemmata. The first lemma shows that the Ate pairing indeed maps into μ_r.

Lemma 2. *Let $\overline{D}_2 \in \mathbb{G}_2$, $D_2 = \rho(\overline{D}_2)$ and $\overline{D}_1 \in \mathbb{G}_1$, $D_1 \in \overline{D}_1$ with* $\mathrm{supp}(D_1) \cap \mathrm{supp}(D_2) = \emptyset$, *then we have $f_{q,D_2}(D_1) \in \mu_r$.*

Proof: Let $h \in \mathbb{F}_q(C)^*$ with $\mathrm{supp}(\mathrm{div}(h)) \cap \mathrm{supp}(\mathrm{div}(f_{q,D_2})) = \emptyset$, then using Weil reciprocity we obtain

$$\begin{aligned} f_{q,D_2}(\mathrm{div}(h)) &= h(\mathrm{div}(f_{q,D_2})) \\ &= h(qD_2 - [q]D_2) = h(qD_2 - \varphi(D_2)) \\ &= \frac{h(qD_2)}{h(\varphi(D_2))} = \frac{h(D_2)^q}{h(D_2)^q} = 1 \ , \end{aligned}$$

therefore

$$f_{q,D_2}(D + \mathrm{div}(h)) = f_{q,D_2}(D) f_{q,D_2}(\mathrm{div}(h)) = f_{q,D_2}(D) \ . \tag{3}$$

As D_1 is defined over $\mathbb{F}_q$ and $\overline{D}_1 \in \mathbb{G}_1$, we obtain

$$f_{q,D_2}(D_1)^r = f_{q,D_2}(rD_1) = f_{q,D_2}(0) = 1$$

since $rD_1 \sim 0$. Using (3) again, we conclude that $f_{q,D_2}(D_1)$ only depends on $\overline{D}_1$ and not on the representative chosen. □

The following three lemmata show that the Ate pairing can indeed be related to the reduced Tate pairing.

Lemma 3. *Given $\overline{D}_1, \overline{D}_2 \in J_C(\mathbb{F}_{q^k})[r]$, $D_2 = \rho(\overline{D}_2)$ and $D_1 \in \overline{D}_1$ such that* $\mathrm{supp}(D_1) \cap \mathrm{supp}(D_2) = \emptyset$, *we have*

$$e(\overline{D}_2, \overline{D}_1) = f_{q^k,D_2}(D_1) \ .$$

Proof: By definition of the reduced Tate-Lichtenbaum pairing, we have to compute

$$e(\overline{D}_2, \overline{D}_1) = f_{r,D_2}(D_1)^{(q^k-1)/r} = f_{q^k-1,D_2}(D_1) \ ,$$

where the last equality follows from (1) with $N = q^k - 1$. Up to this point the divisor D_2 does not even have to be reduced: indeed, take $D_2' = D_2 + \mathrm{div}(h)$ for some $h \in \mathbb{F}_{q^k}(C)$, then $f_{q^k-1,D_2'} = c f_{q^k-1,D_2} h^{q^k-1}$ for some constant factor $c \in \mathbb{F}_{q^k}$. Since D_1 has degree 0, the constant c is irrelevant and the factor $h^{q^k-1}(D_1)$ clearly equals 1 since $h(D_1) \in \mathbb{F}_{q^k}^*$.

When D_2 is reduced, we have that $\mathrm{div}(f_{q^k,D_2}) = q^k D_2 - [q^k]D_2 = (q^k-1)D_2$ and $\mathrm{div}(f_{q^k-1,D_2}) = (q^k-1)D_2 - [q^k-1]D_2 = (q^k-1)D_2$ since $D_2 \in J_C[r]$, so without loss of generality we can take $f_{q^k-1,D_2} = f_{q^k,D_2}$, which ends the proof. □

An easy calculation [4, Lemma 2] proves the following lemma.

Lemma 4. *For any divisor D we can choose $f_{q^k,D}$ such that*

$$f_{q^k,D} = \prod_{i=0}^{k-1} \left(f_{q,[q^i]D}\right)^{q^{k-i-1}} \ . \tag{4}$$

For $D_2 = \rho(\overline{D}_2)$ with $\overline{D}_2 \in \mathbb{G}_2$, each of the factors in the right hand side of (4) can be expressed in terms of f_{q,D_2}. To see this, note that $\varphi(D_2) = [q]D_2$ and $\varphi^i(D_2) = [q^i]D_2$, so it suffices to relate $f_{q,\varphi^i(D_2)}$ with f_{q,D_2} as in the following lemma.

Lemma 5. *Let D be a reduced divisor and ψ a purely inseparable map on C with $\psi(P_\infty) = P_\infty$. Then $\psi(D)$ is also reduced and we can take*

$$f_{n,\psi(D)} \circ \psi = f_{n,D}^{\deg(\psi)} \ .$$

Proof: Let $D = \sum_{i=1}^m (P_i) - m(P_\infty)$ be reduced then $\psi(D) = \sum_{i=1}^m (\psi(P_i)) - m(P_\infty)$, where we used the fact that $\psi(P_\infty) = P_\infty$. Since ψ is assumed to be purely inseparable we have $\psi(P_i) \neq P_\infty$ and $\psi(P_i) \neq \iota(\psi(P_j))$ for $i \neq j$, i.e. $\psi(D)$ is again reduced. By definition we have $\mathrm{div}(f_{n,\psi(D)}) = n(\psi(D)) - ([n]\psi(D))$. Since ψ is purely inseparable we have

$$\begin{aligned}\psi^*\left(\mathrm{div}(f_{n,\psi(D)})\right) &= n\psi^*(\psi(D)) - \psi^*([n]\psi(D)) = n(\deg\psi)D - \psi^*(\psi([n]D)) \\ &= n(\deg\psi)D - (\deg\psi)([n]D) = \mathrm{div}(f_{n,D}^{\deg(\psi)}) \ .\end{aligned}$$

The non-trivial part is the equality $[n]\psi(D) = \psi([n]D)$, which follows from the fact that both sides are reduced divisors (since ψ maps a reduced divisor to a reduced divisor) and that they are linearly equivalent. Indeed,

$$\begin{aligned}[n]\psi(D) &= n\psi(D) + \mathrm{div}(h_n) = \psi(nD) + \mathrm{div}(h_n) \\ &= \psi([n]D + \mathrm{div}(g_n)) + \mathrm{div}(h_n) = \psi([n]D) + \mathrm{div}(\psi_* g_n) + \mathrm{div}(h_n) \,,\end{aligned}$$

for suitable functions $h_n, g_n \in \overline{\mathbb{F}}_q(C)$. Furthermore,

$$\psi^* \left(\mathrm{div}(f_{n,\psi(D)})\right) = \mathrm{div}\left(\psi^*(f_{n,\psi(D)})\right) = \mathrm{div}(f_{n,\psi(D)} \circ \psi) \ ,$$

so we can take $f_{n,\psi(D)} \circ \psi = f_{n,D}^{\deg(\psi)}$. □

Proof of Theorem 2: Since $D_1 \in \mathbb{G}_1$ and fixed under φ, and $D_2 \in \mathbb{G}_2$ is reduced (so $\varphi(D_2) = [q]D_2$), Lemma 5 implies

$$f_{q,[q^i]D_2}(D_1) = f_{q,\varphi^i(D_2)}(D_1) = f_{q,\varphi^i(D_2)}(\varphi^i(D_1)) = (f_{q,D_2}(D_1))^{q^i} \ ,$$

and using Lemma 4, we obtain

$$f_{q^k,D_2}(D_1) = \prod\nolimits_{i=0}^{k-1} \left(f_{q,[q^i]D_2}(D_1)\right)^{q^{k-i-1}} = (f_{q,D_2}(D_1))^{kq^{k-1}} \ . \tag{5}$$

Substituting the above in Lemma 3, we recover Equation (2)

$$e(\overline{D}_2, \overline{D}_1) = (f_{q,D_2}(D_1))^{kq^{k-1}}$$

This equation shows that $f_{q,D_2}(D_1)$ defines a non-degenerate bilinear pairing, since $e(\overline{D}_2, \overline{D}_1)$ is non-degenerate and bilinear. Furthermore, since $f_{q,D_2}(D_1) \in \mu_r$ by Lemma 2, the hyperelliptic Ate pairing is automatically reduced, i.e. no final exponentiation is needed. □

An important remark is that all optimisations that rely on the final powering, such as denominator elimination and ignoring the point at infinity in the evaluation, should be reexamined. It is not hard to see that the first simply no longer holds, whereas the second can be salvaged if the function f_{q,D_2} is properly normalised as in the following lemma.

Lemma 6. *Let $\overline{D}_2 \in \mathbb{G}_2$ and $\overline{D}_1 \in \mathbb{G}_1$ with $\mathrm{supp}(\epsilon(\overline{D}_1)) \cap \mathrm{supp}(\epsilon(\overline{D}_2)) = \emptyset$ and let $D_2 = \rho(\overline{D}_2)$, then if $\mathrm{lc}_\infty(f_{q,D_2}) = 1$ with respect to any $\mathbb{F}_q$-rational uniformizer u_∞ then*

$$a(\overline{D}_2, \overline{D}_1) = f_{q,D_2}(\epsilon(\overline{D}_1)) \ . \tag{6}$$

Proof: By definition we have $\mathrm{div}(f_{q,D_2}) = qD_2 - [q]D_2 = qD_2 - \varphi(D_2)$ since $D_2 \in \mathbb{G}_2$ is reduced and thus $\mathrm{ord}_{P_\infty}(f_{q,D_2}) = -m_2(q-1)$, with $m_2 = \deg(\epsilon(\overline{D}_2))$. This implies that $\mathrm{lc}_\infty(f_{q,D_2}) = 1$ is independent of the choice of $\mathbb{F}_q$-rational uniformizer. Indeed, let u'_∞ be any other $\mathbb{F}_q$-rational uniformizer, then

$$\mathrm{lc}'_\infty(f_{q,D_2}) = \mathrm{lc}_\infty(u'_\infty)^{m_2(q-1)} \mathrm{lc}_\infty(f_{q,D_2}) = \mathrm{lc}_\infty(f_{q,D_2}) \ .$$

Let $D'_1 \in \overline{D}_1$ such that $\mathrm{supp}(D'_1) \cap (\mathrm{supp}(\mathrm{div}(f_{q,D_2})) \cup \mathrm{supp}(\mathrm{div}(u_\infty)))$ and define $\tilde{f}_{q,D_2} = f_{q,D_2} \cdot u_\infty^{m_2(q-1)}$. The divisor of $\tilde{f}_{q,D_2}$ is

$$\mathrm{div}(\tilde{f}_{q,D_2}) = q\epsilon(\overline{D}_2) - \epsilon(\varphi(\overline{D}_2)) + m_2(q-1) \cdot (\mathrm{div}(u_\infty) - P_\infty)$$

which does not contain P_∞, and it is easy to adapt the proof of Lemma 2 to show that $\tilde{f}_{q,D_2}(\overline{D}_1)$ does not depend on the choice of representative of $\overline{D}_1$.

By construction of D_1', both $f_{q,D_2}(D_1')$ and $\tilde{f}_{q,D_2}(D_1')$ are well defined and

$$\tilde{f}_{q,D_2}(D_1') = f_{q,D_2}(D_1') \cdot (u_\infty(D_1'))^{m_2(q-1)} = f_{q,D_2}(D_1')$$

since $u_\infty(D_1')$ is in $\mathbb{F}_q$. From this, we obtain

$$\begin{aligned} a(\overline{D}_2, \overline{D}_1) &= f_{q,D_2}(D_1') = \tilde{f}_{q,D_2}(D_1') = \tilde{f}_{q,D_2}(\overline{D}_1) \\ &= \frac{f_{q,D_2}(\epsilon(\overline{D}_1)) \cdot (u_\infty^{m_2}(\epsilon(\overline{D}_1)))^{q-1}}{\mathrm{lc}_\infty(\tilde{f}_{q,D_2})^{\deg(\epsilon(\overline{D}_1))}} = f_{q,D_2}(\epsilon(\overline{D}_1)) \end{aligned}$$

since $\mathrm{lc}_\infty(\tilde{f}_{q,D_2}) = \mathrm{lc}_\infty(f_{q,D_2}) = 1$ by construction of $\tilde{f}_{q,D_2}$. □

4 Ate Pairing on Superspecial Curves

In this section, we investigate whether the hyperelliptic Ate pairing can also be defined on $\mathbb{G}_1 \times \mathbb{G}_2$. Recall that a curve C is said to have p-rank zero if $J_C[p] = \{0\}$, i.e. the p-torsion is trivial. An immediate consequence of the absence of p-torsion is that the dual of Frobenius $\hat{\varphi}$ (also called Verschiebung) is purely inseparable. Indeed, $\mathrm{Ker}(\hat{\varphi}) \subset J_C[q]$ since $\hat{\varphi}$ has degree q and thus $\mathrm{Ker}(\hat{\varphi}) = \{0\}$. Since $\hat{\varphi} \circ \varphi = [q]$, we conclude that $\hat{\varphi}$ acts as $\hat{\varphi}(\overline{D}_1) = [q]\overline{D}_1$ for $\overline{D}_1 \in \mathbb{G}_1$ and $\hat{\varphi}(\overline{D}_2) = \overline{D}_2$ for $\overline{D}_2 \in \mathbb{G}_2$.

However, p-rank zero is not restrictive enough for our purposes, since Lemma 5 holds for a purely inseparable map on the curve C, whereas Verschiebung is defined on the Jacobian. A curve C is called superspecial when its Jacobian J_C is isomorphic to E^g with E a supersingular elliptic curve. Note that this is more restrictive than supersingularity, since this only requires J_C to be isogenous to E^g. As an example of superspecial curves we mention the family described by Duursma-Lee [7].

For a superspecial curve, we can write $\hat{\varphi} = \varphi \circ \alpha$ for an automorphism $\alpha \in \mathrm{Aut}(C)$. Note that this automorphism is necessarily defined over $\mathbb{F}_q$, since $\varphi = \hat{\hat{\varphi}} = \hat{\alpha} \circ \hat{\varphi}$ and thus $\alpha \circ \varphi = \varphi \circ \alpha$.

Analysing the various lemmata used in proving Theorem 2, we immediately run into a problem since Lemma 2 is no longer valid. Indeed, let $D_1 = \rho(\overline{D}_1)$ with $D_1 \in \overline{D}_1$ and let $h \in \mathbb{F}_{q^k}(C)^*$, then

$$f_{q,D_1}(\mathrm{div}(h)) = h(qD_1 - [q]D_1) = h(qD_1 - \hat{\varphi}(D_1)) = \frac{h(D_1)^q}{h(\alpha(D_1))}\,.$$

This shows that even if h would be $\mathbb{F}_q$-rational, $f_{q,D_1}(\mathrm{div}(h))$ still is not 1, so $f_{q,D_1}(D_2)$ with $D_2 \in \overline{D}_2$ is not independent of the representative chosen.

On the other hand, it is easy to verify that Lemma 3 and 4 remain valid when D_1 and D_2 are swapped. Furthermore, since $\hat{\varphi}$ is given by purely inseparable map on C, Lemma 5 still applies. As a result we can prove the following theorem, circumventing the fact that Lemma 2 no longer holds.

Theorem 3. *Let C be a superspecial curve over $\mathbb{F}_q$ and r a large prime with $r \mid \#J_C(\mathbb{F}_q)$. Let $\mathbb{G}_1 = J_C[r] \cap \mathrm{Ker}(\varphi - [1])$ and $\mathbb{G}_2 = J_C[r] \cap \mathrm{Ker}(\varphi - [q])$, then*

$$\hat{a}(\cdot,\cdot) : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (\overline{D}_1, \overline{D}_2) \mapsto f_{q,D_1}(\epsilon(\overline{D}_2))^d$$

with $D_1 = \rho(\overline{D}_1)$, $d = \gcd(k, q^k - 1)$, $\mathrm{lc}_\infty(f_{q,D_1}) = 1$ and assuming that $\mathrm{supp}(D_1) \cap \mathrm{supp}(\epsilon(\overline{D}_2)) = \emptyset$, defines a non-degenerate, bilinear pairing called the superspecial Ate pairing. Furthermore, the relation with the reduced Tate-Lichtenbaum pairing is as follows:

$$e(\overline{D}_1, \overline{D}_2) = \hat{a}(\overline{D}_1, \overline{D}_2)^{(k/d)q^{k-1}} \,. \tag{7}$$

Proof: Combining Lemma 1, Lemma 3 and Lemma 4 it suffices to compute

$$e(\overline{D}_1, \overline{D}_2) = f_{q^k,D_1}(\epsilon(\overline{D}_2)) = \prod_{i=0}^{k-1} \left(f_{q,[q^i]D_1}(\epsilon(\overline{D}_2))\right)^{q^{k-i-1}} \,, \tag{8}$$

where $D_1 = \rho(\overline{D}_1)$. Applying Lemma 5 to $\hat{\varphi}^i$ we conclude that $f_{q,\hat{\varphi}^i(D_1)} \circ \hat{\varphi}^i = f_{q,D_1}^{q^i}$. Since D_1 is reduced and $\overline{D}_1 \in \mathbb{G}_1$, we have $\hat{\varphi}^i(D_1) = [q^i]D_1$. Furthermore, let $D_2 = \rho(\overline{D}_2)$, then since D_2 is reduced and $\overline{D}_2 \in \mathbb{G}_2$, we have $\hat{\varphi}(D_2) = D_2$. Combined with $\hat{\varphi}(P_\infty) = P_\infty$, we conclude that $\hat{\varphi}(\epsilon(\overline{D}_2)) = \epsilon(\overline{D}_2)$. Substituting this in (8) leads to

$$e(\overline{D}_1, \overline{D}_2) = f_{q,D_1}(\epsilon(\overline{D}_2))^{kq^{k-1}} = f_{q,D_1}(\epsilon(\overline{D}_2))^{d\cdot(k/d)q^{k-1}} \,.$$

Since the left hand side is an r-th root of unity and $\gcd((k/d)q^{k-1}, q^k - 1) = 1$, we conclude that $f_{q,D_1}(\epsilon(\overline{D}_2))^d$ also is an r-th root of unity. Furthermore, $e(\overline{D}_1, \overline{D}_2)$ is non-degenerate and bilinear, so we finally conclude that the superspecial Ate pairing also defines a non-degenerate bilinear pairing. □

The above theorem has been proved by Galbraith et al. [10] in the special case of supersingular elliptic curves in characteristic 2 and 3 using explicit computations.

5 Conclusion

In this paper we have introduced two new pairings on hyperelliptic curves, by generalising the Ate pairing on elliptic curves. The first version applies to all algebraic curves, whereas the second requires the curve to be superspecial, e.g. the Duursma-Lee curves. To prove that both versions are well-defined, we introduced a proper theoretical framework explaining several simpler results in the literature which were proved using ad hoc methods.

The most important property of the Ate pairings is that no final exponentiation is necessary. This raises security questions with respect to pairing inversion and Verheul's results on the computational Diffie-Hellman problem, especially when so-called degenerate divisors are used. The precise security implications of the Ate pairings are currently unknown and much more research is needed.

6 Acknowledgements

The authors would like to thank Bas Edixhoven and Ben Moonen for their expertise on superspecial curves. Robert Granger would like to thank Alfred Menezes for his invitation to visit the Centre for Applied Cryptographic Research at the University of Waterloo in May 2006, where this work was initiated.

References

1. R. Avanzi. Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementation. In M. Joye and J.-J. Quisquater, editor, *CHES*, volume 3156 of *Lecture Notes in Computer Science*, pages 133–147. Springer, 2004.
2. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.
3. R. Avanzi, N. Thériault, and Z. Wang. Rethinking low genus hyperelliptic jacobian arithmetic over binary fields: Interplay of field arithmetic and explicit formulae. Technical report, CACR, 2006. CACR 2006-07.
4. P. S. L. M. Barreto, S. Galbraith, C. O hEigeartaigh, and M. Scott. Efficient pairing computation on supersingular abelian varieties. *Designs, Codes and Cryptography*, to be published, 2005.
5. P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 354–368. Springer, 2002.
6. D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.
7. I. M. Duursma and Hyang-Sook Lee. Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$. In C.-S. Laih, editor, *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 111–123. Springer, 2003.
8. G. Frey and T. Lange. Fast Bilinear Maps from the Tate-Lichtenbaum Pairing on Hyperelliptic Curves. In F. Hess, S. Pauli, M. Pohst, editors, *ANTS VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 466–479. Springer, 2006.
9. G. Frey and H-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.
10. S. Galbraith, C. O hEigeartaigh, and C. Sheedy. Simplified pairing computation and security implications. To appear in *J. Math. Crypt.*, 2007.
11. P. Gaudry, F. Hess and N. P. Smart. Constructive and Destructive Facets of Weil Descent on Elliptic Curves. *J. Cryptology.*, 15(1):19–46, 2002.
12. P. Gaudry, E. Thomé, N. Thériault and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.*, 76(257), 475–492, 2007.
13. R. Granger, D. Page, and N. Smart. High security pairing-based cryptography revisited. In F. Hess, S. Pauli, M. Pohst, editors, *ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 480–494. Springer, 2006.
14. C. Guyot, K. Kaveh, and V. M. Patankar. Explicit algorithm for the arithmetic on the hyperelliptic Jacobians of genus 3. *J. Ramanujan Math. Soc.*, 19(2):75–115, 2004.
15. F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symb. Comp.*, 33(4):425-445, 2002.

16. F. Hess. A Note on the Tate Pairing of Curves over Finite Fields. *Arch. Math.*, 82:28-32, 2004.
17. F. Hess, N. Smart, and F. Vercauteren. The Eta-pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.
18. T. Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Appl. Algebra Engrg. Comm. Comput.*, 15(5):295–328, 2005.
19. N. Koblitz and A. Menezes. Pairing-Based Cryptography at High Security Levels. In Nigel Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36. Springer, 2005.
20. V. S. Miller. Short programs for functions on curves. Unpublished manuscript 1986. Available at `http://crypto.stanford.edu/miller/miller.pdf`.
21. V. S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.
22. J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
23. H. Stichtenoth. *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.
24. E. Verheul. Evidence that XTR is more Secure than Supersingular Elliptic Curve Cryptosystems. In B. Pfitzmann, editor, *EUROCRYPT*, volume of 2045 *Lecture Notes in Computer Science*, pages 195–210. Springer, 2001.
25. N. Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *J. Algebra*, 52(2):378–410, 1978.

A Performance Estimates

A.1 Miller's Algorithm

We here give an expanded version of Algorithm 1, tailored for the Ate pairing. From the point of view of computational efficiency, a good choice of uniformizer is $u_\infty = x^g/y$. Let $p(x)$ be a polynomial in x, then with this choice of u_∞ we have:

$$\mathrm{lc}_\infty(p(x)) = \mathrm{lc}(p(x))$$
$$\mathrm{lc}_\infty(y - p(x)) = \begin{cases} 1 & \text{if } \deg(p(x)) \leq g \\ -\mathrm{lc}(p(x)) & \text{if } \deg(p(x)) > g \end{cases}$$

where $\mathrm{lc}(p(x))$ is the leading coefficient (in the variable x) of $p(x)$. It is then easy to obtain $\mathrm{lc}_\infty(f_{q,D_2})$ from the computations in Miller's algorithm.

A more detailed description of Algorithm 1 is given in Algorithm 2. The computations coming from Cantor's algorithm can be replaced by explicit formulae, with some minor changes as $\tilde{v}_1(x)$ must be computed completely, both in the addition and the doubling formulae (in explicit formulae, the computation of $\tilde{v}_1(x)$ is avoided to reduce costs).

Remark 3. For genus 2, computing $res(c_i(x), u_b(x))$ is relatively inexpensive compared with polynomial operations, and it is more efficient to compute the resultant every time we accumulate on c_i rather than working with polynomials (squaring c_i in the doubling step will then become a single field operation). For all other genera, it is more efficient to accumulate c_1 and c_2 as polynomials and to compute resultants only in the final step of Algorithm 2.

Algorithm 2 Miller's algorithm for hyperelliptic curves (detailed)

Inputs: $n \in \mathbb{N}$ and $D_a, D_b \in J_C$ reduced with disjoint affine support, $D_a = [u_a(x), v_a(x)]$, $D_b = [u_b(x), v_b(x)]$

Outputs: $f_{n,D_a}(D_b)$

Write n as $\sum_{j=0}^{s} n_j 2^j$, with $n_j \in \{0,1\}$ and $n_s = 1$.
$D = [u(x), v(x)] \leftarrow D_a$, $c_1(x) \leftarrow 1$, $c_2(x) \leftarrow 1$, $c_3 \leftarrow 1$.
for $j = s-1$ down to 0 **do**
  $c_1(x) \leftarrow c_1(x)^2 \bmod u_b(x)$
  $c_2(x) \leftarrow c_2(x)^2 \bmod u_b(x)$
  $c_3 \leftarrow c_3^2$
  $d(x) \leftarrow \gcd(u(x), 2v(x) + h(x))$
  $[\tilde{u}_1(x), \tilde{v}_1(x)] \leftarrow 2D - \mathrm{div}(d(x))$
  $c_1(x) \leftarrow c_1(x) \cdot d(x) \bmod u_b(x)$
  $j \leftarrow 1$
  while $\deg(\tilde{u}_j) > g$ **do**
    $\tilde{u}_{j+1}(x) = Monic\left(\frac{\tilde{v}_j(x)^2 + h(x)\tilde{v}_j(x) - f(x)}{\tilde{u}_j(x)}\right)$.
    $\tilde{v}_{j+1}(x) = -\tilde{v}_j(x) - h(x) \bmod \tilde{u}_{j+1}(x)$.
    $c_1(x) \leftarrow c_1(x) \cdot (v_b(x) - \tilde{v}_j(x)) \bmod u_b(x)$
    $c_2(x) \leftarrow c_2(x) \cdot \tilde{u}_{j+1}(x) \bmod u_b(x)$
    $c_3 \leftarrow c_3 \cdot \mathrm{lc}_\infty(y - \tilde{v}_j)$
    $j \leftarrow j + 1$
  end while
  $D = [u(x), v(x)] \leftarrow [\tilde{u}_j(x), \tilde{v}_j(x)]$
  if $n_j = 1$ **then**
    $d(x) \leftarrow \gcd(u(x), u_a(x), v(x) + v_a(x) + h(x))$
    $[\tilde{u}_1(x), \tilde{v}_1(x)] \leftarrow D + D_a - \mathrm{div}(d(x))$
    $c_1(x) \leftarrow c_1(x) \cdot d(x) \bmod u_b(x)$
    $j \leftarrow 1$
    while $\deg(\tilde{u}_j) > g$ **do**
      $\tilde{u}_{j+1}(x) = Monic\left(\frac{\tilde{v}_j(x)^2 + h(x)\tilde{v}_j(x) - f(x)}{\tilde{u}_j(x)}\right)$.
      $\tilde{v}_{j+1}(x) = -\tilde{v}_j(x) - h(x) \bmod \tilde{u}_{j+1}(x)$.
      $c_1(x) \leftarrow c_1(x) \cdot (v_b(x) - \tilde{v}_j(x)) \bmod u_b(x)$
      $c_2(x) \leftarrow c_2(x) \cdot \tilde{u}_{j+1}(x) \bmod u_b(x)$
      $c_3 \leftarrow c_3 \cdot \mathrm{lc}_\infty(y - \tilde{v}_j)$
      $j \leftarrow j + 1$
    end while
    $D = [u(x), v(x)] \leftarrow [\tilde{u}_j(x), \tilde{v}_j(x)]$
  end if
end for
$c \leftarrow \frac{res(c_1(x), u_b(x))}{c_3 \cdot res(c_2(x), u_b(x))}$
Return c.

A.2 Operation Count

In general, one cannot assume that f_{q,D_2} obtained from the computations of Algorithm 1 is normalised to have $\mathrm{lc}_\infty(f_{q,D_2}) = 1$. The evaluation of $a(\overline{D}_2, \overline{D}_1)$ in Lemma 6 is then computed as

$$a(\overline{D}_2, \overline{D}_1) = \frac{f_{q,D_2}\left(\epsilon(\overline{D}_1)\right)}{\mathrm{lc}_\infty(f_{q,D_2})^{m_1}} \quad . \tag{9}$$

Tables 1 and 2 give the cost in field operations for the doubling and addition steps of Algorithm 2, for general divisors. The row "first & last" takes into account the cost of the resultants and final multiplications and inversion, as well as the operations saved by having $c_1 = c_2 = c_3 = 1$ in the first doubling step.

Table 1. Costs involved in Miller's algorithm to compute $a(\overline{D}_2, \overline{D}_1)$ using general divisors

		genus 2	genus 3
addition	$\mathbb{F}_q$	$7kM$	$32kM$
	$\mathbb{F}_{q^k}$	$1I + 29M + 5S$	$1I + 91M + 6S$
doubling	$\mathbb{F}_q$	$7kM$	$42kM$
	$\mathbb{F}_{q^k}$	$1I + 29M + 9S$	$1I + 88M + 22S$
first & last	$\mathbb{F}_q$	0	$-8kM$
	$\mathbb{F}_{q^k}$	$1I - 1M - 2S$	$1I + 7M - 13S$

Table 2. Costs involved in Miller's algorithm to compute $\hat{a}(\overline{D}_1, \overline{D}_2)$ for superspecial curves using general divisors

		genus 2	genus 3
addition	$\mathbb{F}_q$	$1I + (25 + 3k)M + 3S$	$1I + (67 + 12k)M + 6S$
	$\mathbb{F}_{q^k}$	$8M + 2S$	$44M$
doubling	$\mathbb{F}_q$	$1I + (25 + 3k)M + 6S$	$1I + (64 + 12k)M + 10S$
	$\mathbb{F}_{q^k}$	$8M + 4S$	$54M + 12S$
first & last	$\mathbb{F}_q$	$(k-1)M - 1S$	$(k-1)M - 1S$
	$\mathbb{F}_{q^k}$	$1I - 1M - 2S$	$1I - 1M - 12S$

Tables 3 and 4 give the cost in field operations for the doubling and addition steps of Algorithm 2, for degenerate divisors, i.e. for divisors whose support is a single point (together with the point at infinity).

Each addition (respectively doubling) step uses the fastest known explicit formulae in affine coordinates, adapted to include the computation of $\tilde{v}_1(x)$. For the genus three addition, we use the formulae of [14] with the resultant replaced by Cramer's rule (as was done for characteristic 2 in [3]). For the final computations with the resultants, we go back to the resultant computation of [14].

Table 3. Costs involved in Miller's algorithm to compute $a(\overline{D}_2, \overline{D}_1)$ using degenerate divisors

		genus 2	genus 3
addition	$\mathbb{F}_q$	$4kM$	$13kM$
	$\mathbb{F}_{q^k}$	$1I + 27M + 3S$	$1I + 69M + 6S$
doubling	$\mathbb{F}_q$	$4kM$	$13kM$
	$\mathbb{F}_{q^k}$	$1I + 27M + 7S$	$1I + 66M + 11S$
first & last	$\mathbb{F}_q$	$1M + 1S$	$2M + 2S$
	$\mathbb{F}_{q^k}$	$1I - 1M - 2S$	$1I - 1M - 2S$

Table 4. Costs involved in Miller's algorithm to compute $\hat{a}(\overline{D}_1, \overline{D}_2)$ for superspecial curves using degenerate divisors

		genus 2	genus 3
addition	$\mathbb{F}_q$	$1I + (25 + 4k)M + 3S$	$1I + (67 + 13k)M + 6S$
	$\mathbb{F}_{q^k}$	$2M$	$2M$
doubling	$\mathbb{F}_q$	$1I + (25 + 4k)M + 6S$	$1I + (64 + 13k)M + 6S$
	$\mathbb{F}_{q^k}$	$2M + 2S$	$2M + 2S$
first & last	$\mathbb{F}_q$	$(k - 1)M - 1S$	$(k - 1)M - 1S$
	$\mathbb{F}_{q^k}$	$1I - 1S$	$1I + 1M$

A.3 Performance Comparison

In this section we provide precise operation counts for three security levels: 80, 128 and 192-bit security. The sizes of the finite fields and the security parameters k are chosen such that both the DLP in the Jacobian of the curve $J_C(\mathbb{F}_q)$ and the DLP in the embedding field $\mathbb{F}_{q^k}$ are infeasible.

Following [13] we restrict to the use of so-called pairing friendly finite fields, i.e. $\mathbb{F}_q$ is a prime field with $q \equiv 1 \bmod 12$ and k of the form $2^i 3^j$. For these fields, the cost of the required operations of multiplication, squaring, and inversion can each be expressed simply in terms of base field operations [13], where m, s and i denote the cost of a multiplication, squaring and inversion respectively in $\mathbb{F}_q$.

Bearing in mind that for the same security, the base field will be smaller for higher genus, we must account for this in our cost estimates. We therefore express all costs in terms of the number of $\mathbb{F}_{q_3}$ multiplications we need to perform, where q_i is the base field cardinality of the genus i curve. Using basic Karatsuba, we thus have $M_{q_i} = (q_i/q_3)^{1.585} \cdot M_{q_3}$ for $i = 1, 2$. This estimate is likely to be slightly smaller than what is recorded in practice [1] and so will lead our results to underestimate the genus one operation counts slightly; however we believe they are sufficient for comparison purposes.

For simplicity we assume that a squaring costs the same as a multiplication, and that one inversion is equivalent to ten multiplications. We also assume half as many additions as doublings in Algorithm 2.

Table 5. Cost of $\mathbb{F}_{q^k}$ operations in terms of $\mathbb{F}_q$ operations

k	Mul	Sqr	Inv
6	$15m$	$15s$	$21m + 13s + i$
12	$45m$	$45s$	$51m + 43s + i$
16	$81m$	$81s$	$90m + 90s + i$
24	$135m$	$135s$	$141m + 133s + i$
32	$243m$	$243s$	$252m + 252s + i$
48	$405m$	$405s$	$411m + 403s + i$
54	$375m$	$375s$	$591m + 343s + i$

Table 6. Number of $\mathbb{F}_{q_3}$ multiplications to compute the Ate pairing

Security	g	q	k	MOV	number of $\mathbb{F}_{q_3}$ muls				
					ordinary	superspecial	ordinary degenerate	superspecial degenerate	fastest Ate
80	1	172	6	1032					3.12×10^4
	2	86	12	1032	3.79×10^5	1.21×10^5	3.34×10^5	4.92×10^4	
	3	64	16	1024	8.89×10^5	4.82×10^5	6.30×10^5	5.39×10^4	
128	1	256	12	3072					8.63×10^4
	2	128	24	3072	1.64×10^6	4.97×10^5	1.45×10^6	1.78×10^5	
	3	96	32	3072	3.91×10^6	2.12×10^6	2.80×10^6	1.89×10^5	
192	1	384	24	9216					3.87×10^5
	2	192	48	9216	6.68×10^6	1.99×10^6	5.94×10^6	6.60×10^5	
	3	152	54	8208	9.64×10^6	5.18×10^6	6.90×10^6	4.65×10^5	

Table 6 gives the results of our performance estimates. Of the right-most five columns, the left two are based on the formulae given in Table 1 and 2 and Algorithm 2, while the third and fourth are based on Table 3 and 4. The final column we computed using the estimates in [17], together with the final powering cost estimates from [13], taking the minimum over the choice of Ate or twisted Ate, average or small trace, and quadratic or sextic twist.

The table indicates that the Ate pairing for elliptic curves, can be an order of magnitude faster than the basic version of the Ate pairing described in this paper. The reason for the Ate pairing being particularly fast in the elliptic case is the availability of twists, as well as very short traces. Whether high degree twists can be utilised for the hyperelliptic Ate pairing remains open. When using degenerate divisors however, the Ate pairing for superspecial curves with genus two and three is certainly comparable to the genus one case.