

# PAIRINGS ON HYPERELLIPTIC CURVES

JENNIFER BALAKRISHNAN, JULIANA BELDING, SARAH CHISHOLM, KIRSTEN EISENTRÄGER,  
KATHERINE E. STANGE, AND EDLYN TESKE

*Dedicated to the memory of Isabelle Déchène (1974-2009)*

ABSTRACT. We assemble and reorganize the recent work in the area of hyperelliptic pairings: We survey the research on constructing hyperelliptic curves suitable for pairing-based cryptography. We also showcase the hyperelliptic pairings proposed to date, and develop a unifying framework. We discuss the techniques used to optimize the pairing computation on hyperelliptic curves, and present many directions for further research.

## 1. INTRODUCTION

Numerous cryptographic protocols for secure key exchange and digital signatures are based on the computational infeasibility of the discrete logarithm problem in the underlying group. Here, the most common groups in use are multiplicative groups of finite fields and groups of points on elliptic curves over finite fields. Over the past years, many new and exciting cryptographic schemes based on pairings have been suggested, including one-round three-way key establishment, identity-based encryption, and short signatures [3, 4, 43, 64]. Originally, the Weil and Tate (-Lichtenbaum) pairings on supersingular elliptic curves were proposed for such applications, providing non-degenerate bilinear maps that are efficient to evaluate. Over time potentially more efficient pairings have been found, such as the eta [2], Ate [41] and R-ate [53] pairings. Computing any of these pairings involves finding functions with prescribed zeros and poles on the curve, and evaluating those functions at divisors.

As an alternative to elliptic curve groups, Koblitz [47] suggested Jacobians of hyperelliptic curves for use in cryptography. In particular, hyperelliptic curves of low genus represent a competitive choice. In 2007, Galbraith, Hess and Vercauteren [29] summarized the research on hyperelliptic pairings to date and compared the efficiency of pairing computations on elliptic and hyperelliptic curves. In this rapidly moving area, there have been several new developments since their survey: First, new pairings have been developed for the elliptic case, including so-called optimal pairings by Vercauteren [71] and a framework for elliptic pairings by Hess [40]. Second, several constructions of ordinary hyperelliptic curves suitable for pairing-based cryptography have been found [19, 22, 67, 20].

In this paper, we survey

- the constructions of hyperelliptic curves suitable for pairings, especially in the ordinary case,
- the hyperelliptic pairings proposed to date, and
- the techniques to optimize computations of hyperelliptic pairings.

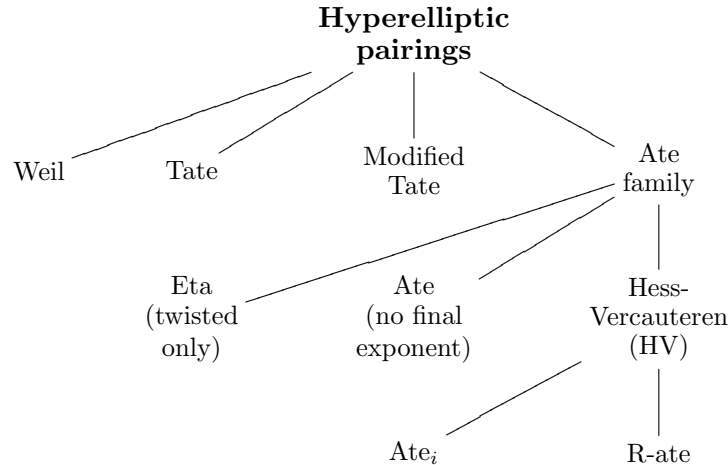
We also

---

*Date:* September 22, 2009.

*Key words and phrases.* Hyperelliptic curves, Tate pairing, Ate pairing.

FIGURE 1. Classification of hyperelliptic pairings



- give a unifying framework for hyperelliptic pairings which includes many of the recent variations of the Ate pairing, and
- present a host of potential further improvements.

In this paper, we do *not* provide any comparative implementation, or give recommendations on which pairings should be used to satisfy certain user-determined criteria; this is left for future work.

In our presentation, we focus on the case of genus 2 hyperelliptic curves and their Jacobians. Among all curves of higher genus, such curves are of primary interest for cryptographic applications: On the one hand, we find explicit formulae along with various optimizations (e.g., [50, 73]), providing for an arithmetic that is somewhat competitive with elliptic curves. On the other hand, the security is exactly the same as in the elliptic case, with the best attacks on the discrete logarithm problem in the Jacobian being square-root attacks based on the Pollard rho method (cf. [25]). However, Galbraith, Hess and Vercauteran [29, §10.1] argue that *pairing* computations on hyperelliptic curves will always be slow compared to elliptic curves: The most expensive part of a standard Tate pairing computation consists of repeatedly evaluating some function on a divisor and computing the product of the values obtained. Both in the elliptic and in the hyperelliptic case these divisors are defined over fields of the same size, but the functions in the hyperelliptic case are more complicated.

Figure 1 represents the collection of hyperelliptic pairings at a glance. For use in pairing-based applications, originally the Weil and Tate pairings were proposed. The Weil pairing is much more expensive to compute than the Tate pairing, so it is not used in practice. The pairings in the Ate family are potentially more efficient than the Tate pairing. Historically, the eta pairing was the first pairing to shorten the length of the Miller loop. It is defined on supersingular curves only and requires a final exponentiation. It gave rise to the Ate pairings which are defined for all curves. The hyperelliptic Ate pairing (which has a different definition than the elliptic Ate pairing!) has the advantage that its loop length is roughly half of the length of the Miller loop for the Tate pairing. It also is special in that it requires no final exponentiation (while the elliptic Ate pairing does require one). Other variations of the Ate pairing include the Hess-Vercauteran (HV) pairings. These are the pairings captured by our unifying framework, which generalizes work for the elliptic case by

Hess [40] and Vercauteren [71]. HV pairings also have potentially shorter Miller loops than the Ate pairing, depending on the embedding degree of the Jacobian. All of the HV pairings involve a final exponentiation. Two examples of HV pairings are the R-ate and the Ate<sub>i</sub> pairings. Table 5.6 in Section 5 gives more details about the differences and merits of each pairing.

Our paper is organized as follows. In Section 2 we review some of the background on Jacobians of hyperelliptic curves. Section 3 discusses hyperelliptic curves of low embedding degree and what is known about constructing them. Section 4 gives an overview of the different pairings on hyperelliptic curves following the classification in Figure 1. We also introduce the HV pairing framework, give a direct proof of the non-degeneracy and bilinearity of the pairings captured by this framework and discuss how the Ate and R-ate pairings fit in. Section 5 describes the adaptation of Miller's algorithm to the hyperelliptic setting, presents common optimizations and compares all pairings according to their key characteristics of loop length and final exponentiation. Section 6 presents numerous problems for future work.

## 2. JACOBIANS OF HYPERELLIPTIC CURVES

In this section, we fix some notation and terminology that will be used throughout the paper.

**2.1. Hyperelliptic curves.** A *hyperelliptic curve*  $C$  over a field  $K$  is a non-singular projective curve of the form

$$C : y^2 + H(x)y = F(x) \in K[x, y].$$

Let  $g$  be the genus of the curve. Throughout this paper, we restrict to the case where  $F$  is monic,  $\deg F(x) = 2g + 1$ , and  $\deg H(x) \leq g$ , so that  $C$  has one point at infinity, denoted  $P_\infty$ . When  $g = 1$ ,  $C$  is an *elliptic curve*. For significant parts of our discussion, we will consider the case where  $g = 2$ .

Although the points of a genus  $g \geq 2$  hyperelliptic curve do not form a group, there is an involution of the curve taking  $P = (x, y)$  to the point  $(x, -y - H(x))$ , which we will denote  $-P$ . Then, in accordance with the notation,  $-(-P) = P$ .

**2.2. Divisors and abelian varieties.** Let  $K$  be a field over which  $C$  is defined, and let  $\bar{K}$  its algebraic closure. A *divisor*  $D$  on the curve  $C$  is a formal sum over all symbols  $(P)$ , where  $P$  is a  $\bar{K}$ -point of the curve:

$$D = \sum_{P \in C(\bar{K})} n_P(P),$$

where all but finitely many of the coefficients  $n_P \in \mathbb{Z}$  are zero. The collection of divisors forms an abelian group  $\text{Div}(C)$ . The *degree* of a divisor is the sum

$$\sum_{P \in C(\bar{K})} n_P \in \mathbb{Z},$$

and the *support* of a divisor is the set of points of the divisor with non-zero coefficients  $n_P$ . For any rational function  $f$  on  $C$ , there is an associated divisor

$$\text{div}(f) = \sum_{P \in C(\bar{K})} \text{ord}_P(f)(P)$$

which encodes the number and location of its zeroes and poles. Any divisor which is the divisor of a function in this way is called a *principal divisor*.

An element  $\sigma$  in the Galois group of  $\bar{K}$  over  $K$ ,  $\text{Gal}(\bar{K}/K)$ , acts on a divisor as follows:

$$\left( \sum_{P \in C(\bar{K})} n_P(P) \right)^\sigma = \sum_{P \in C(\bar{K})} n_P(P^\sigma).$$

In particular, let  $L$  be any intermediate field  $K \subset L \subset \bar{K}$ . Consider a function  $f$  defined over  $L$ ; then  $\text{div}(f)$  is fixed by elements of  $\text{Gal}(\bar{K}/L)$ . In fact,  $\text{div}(f)^\sigma = \text{div}(f^\sigma)$ .

We give names to various sets of collections:  $\text{Div}(C)$  of divisors,  $\text{Div}^0(C)$  of degree zero divisors,  $\text{Ppl}(C)$  of principal divisors,  $\text{Div}_K(C)$  of divisors invariant under the action of  $\text{Gal}(\bar{K}/K)$ ,  $\text{Div}_K^0(C)$  of degree zero divisors invariant under the action of  $\text{Gal}(\bar{K}/K)$ , and  $\text{Ppl}_K(C)$  of principal divisors invariant under the action of  $\text{Gal}(\bar{K}/K)$ .

These are all abelian groups, which have the following subgroup relations:

$$\begin{array}{ccccc} \text{Div}(C) & \supset & \text{Div}^0(C) & \supset & \text{Ppl}(C) \\ \cup & & \cup & & \cup \\ \text{Div}_K(C) & \supset & \text{Div}_K^0(C) & \supset & \text{Ppl}_K(C). \end{array}$$

We make note of certain quotient groups:

$$\begin{array}{ll} \text{Pic}(C) := \text{Div}(C)/\text{Ppl}(C), & \text{Pic}^0(C) := \text{Div}^0(C)/\text{Ppl}(C), \\ \text{Pic}_K(C) := \text{Div}_K(C)/\text{Ppl}_K(C), & \text{Pic}_K^0(C) := \text{Div}_K^0(C)/\text{Ppl}_K(C). \end{array}$$

Elements of these quotient groups are equivalence classes of divisors. Divisors  $D_1$  and  $D_2$  of the same class are said to be *linearly equivalent*, and we write  $D_1 \sim D_2$ .

Recall that an elliptic curve is an example of an abelian variety. In general, an *abelian variety*  $A$  over  $K$  is a projective algebraic variety over  $K$  along with a group law  $\varphi : A \times A \rightarrow A$  and an inverse map  $\text{Inv} : A \rightarrow A$  sending  $x \mapsto x^{-1}$  such that  $\varphi$  and  $\text{Inv}$  are morphisms of varieties, both defined over  $K$ .

For an abelian variety  $A$ , a field  $K$  and an integer  $r$ , we let  $A(K)[r]$  denote the set of  $r$ -torsion points of  $A$  defined over  $K$ , that is, the set of points in  $A(K)$  of order dividing  $r$ . Now suppose  $A$  is an abelian variety over  $\mathbb{F}_q$ , with  $q = p^m$ . We say that  $A$  is *simple* if it is not isogenous over  $\mathbb{F}_q$  to a product of lower dimensional abelian varieties. We call  $A$  *absolutely simple* if it is simple over  $\bar{\mathbb{F}}_q$ . We say  $A$  is *supersingular* if  $A$  is isogenous over  $\bar{\mathbb{F}}_q$  to a power of a supersingular elliptic curve. (An elliptic curve  $E$  is supersingular if  $E(\bar{\mathbb{F}}_q)$  has no points of order  $p$ .) An abelian variety  $A$  of dimension  $g$  over  $\bar{\mathbb{F}}_q$  is *ordinary* if  $\#A(\bar{\mathbb{F}}_q)[p] = p^g$ . Note that for dimension  $g \geq 2$ , there exist abelian varieties that are neither ordinary nor supersingular.

There is a natural isomorphism between the degree zero part of the Picard group  $\text{Pic}^0(C)$  of a hyperelliptic curve  $C$  and its *Jacobian*  $\text{Jac}_C$ , which is an abelian variety into which the curve embeds (cf. [26]). For the remainder of this paper, we will identify the Picard group  $\text{Pic}^0(C)$  with  $\text{Jac}_C$ .

**2.3. Arithmetic in the Jacobian.** We will work in the Jacobian  $\text{Jac}_C$  of a hyperelliptic curve  $C$  of genus  $g$ , whose elements are equivalence classes of degree-zero divisors. To do so, we choose a *reduced* representative in each such divisor class. A *reduced* divisor is one of the form

$$(P_1) + (P_2) + \cdots + (P_r) - r(P_\infty)$$

where  $r \leq g$ ,  $P_\infty$  is the point at infinity on  $C$ ,  $P_i \neq -P_j$  for distinct  $i$  and  $j$ , and no  $P_i$  satisfying  $P_i = -P_i$  appears more than once. Such a divisor is called *semi-reduced* if the condition  $r \leq g$  is omitted. Each equivalence class contains exactly one reduced divisor. For a divisor  $D$  we will denote by  $\rho(D)$  the reduced representative of its equivalence class. The action of Galois commutes with  $\rho$ , i.e.  $\rho(D^\sigma) = \rho(D)^\sigma$ , since the property of being reduced is preserved by the action of Galois.

To encode the reduced divisor in a convenient way, we write  $(u(x), v(x))$  where  $u(x)$  is a monic polynomial whose roots are the  $x$ -coordinates  $x_1, \dots, x_r$  of the  $r$  points

$$P_1 = (x_1, y_1), \dots, P_r = (x_r, y_r),$$

and where  $v(x_i) = y_i$  for  $i = 1, \dots, r$ . This so-called *Mumford representation* [59] is uniquely determined by and uniquely determines the divisor. To find this representation, it suffices to find  $u(x)$  and  $v(x)$  satisfying the following conditions:

- (1)  $u(x)$  is monic,
- (2)  $\deg(v(x)) < \deg(u(x)) \leq g$ , and
- (3)  $u(x) \mid F(x) - v(x)H(x) - v(x)^2$ ,

where  $F(x)$  and  $H(x)$  are the polynomials defining the curve  $C$  (defined in Section 2.1). When we add two reduced divisors  $D_1$  and  $D_2$  the result  $D_1 + D_2$  is not necessarily reduced. Beginning with two reduced divisors in Mumford representation, the algorithm to obtain the Mumford representation of the reduction of their sum can be explained in terms of the polynomials involved in the Mumford representation, without recourse to the divisor representation. This algorithm is originally due to Cantor [6], and in the form presented here to Koblitz [47]. The algorithm has two stages: in the first, we find a semi-reduced divisor  $D \sim D_1 + D_2$ , and in the second stage, we reduce  $D$ . Suppose that  $D_i$  has Mumford representation  $(u_i, v_i)$  for  $i = 1, 2$ .

STAGE 1:

- (1) Find  $d(x) = \gcd(u_1(x), u_2(x), v_1(x) + v_2(x) + H(x))$ . Finding this via the extended Euclidean algorithm gives  $s_1(x)$ ,  $s_2(x)$  and  $s_3(x)$  such that

$$d = s_1 u_1 + s_2 u_2 + s_3 (v_1 + v_2 + H).$$

- (2) Calculate the quantities

$$u = u_1 u_2 / d^2, \quad \text{and} \quad v = s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + F) / d \pmod{u(x)}.$$

(It is easily verified that the fraction on the right is defined since  $d(x)$  is a divisor of the numerator.)

At this point, the result  $(u, v)$  is a semi-reduced divisor linearly equivalent to  $D_1 + D_2$ . This stage corresponds to simply adding  $D_1$  and  $D_2$  and canceling any points with their negatives if applicable. In fact, we obtain

$$D' = D_1 + D_2 - \text{div}(d).$$

STAGE 2:

In this stage, if  $\deg(u) > g$  we can replace  $(u, v)$  with a divisor  $(u', v')$  satisfying  $\deg(u') < \deg(u)$ . This replacement is as follows. Set

$$u' = (F - vH - v^2)/u, \quad \text{and} \quad v' = -H - v \pmod{u'}.$$

This stage corresponds to simplifying the divisor using the geometric group law nicely described for genus 2 by Lauter [51]. At each application of this loop to a divisor  $D_3$ , we obtain a divisor  $D''$  satisfying<sup>1</sup>

$$D'' = D_3 - \text{div}((F - vH - v^2)/u').$$

Applying this loop finitely many times, beginning with the result  $D'$  of stage one, we eventually obtain a reduced divisor  $D$  linearly equivalent to  $D_1 + D_2$ .

This algorithm has been optimized to avoid the use of the extended Euclidean algorithm and in this form it is much more efficient [29]. An enhanced version of Cantor's Algorithm is given as Algorithm 2 in this paper; see Section 5.1. If steps 5 and 8 through 13 are removed from Algorithm 2 one has the Cantor's Algorithm discussed here.

### 3. HYPERELLIPTIC CURVES OF LOW EMBEDDING DEGREE

In this section we discuss hyperelliptic curves suitable for pairing-based cryptographic systems. The Jacobian varieties of such curves must have computable pairings, and computationally infeasible discrete logarithm problems. Specifically, we require low embedding degrees and large prime-order subgroups.

**3.1. Embedding degree and  $\rho$ -value.** Let  $r$  be a prime. Let  $C$  be a hyperelliptic curve over  $\mathbb{F}_q$  of genus  $g$  with Jacobian variety  $\text{Jac}_C(\mathbb{F}_q)$  such that  $r \mid \#\text{Jac}_C(\mathbb{F}_q)$  and  $\gcd(r, q) = 1$ . The *embedding degree* of  $\text{Jac}_C$  with respect to  $r$  is the smallest integer  $k$  such that  $r \mid (q^k - 1)$ . Equivalently, the embedding degree of  $\text{Jac}_C$  with respect to  $r$  is the smallest integer  $k$  such that  $\mathbb{F}_{q^k}^*$  contains the group of  $r^{\text{th}}$  roots of unity  $\mu_r$ . If  $\text{Jac}_C$  has embedding degree  $k$  with respect to  $r$ , then a pairing on  $C$ , such as the Weil pairing  $e_r : \text{Jac}_C(\mathbb{F}_q)[r] \times \text{Jac}_C(\mathbb{F}_q)[r] \rightarrow \mu_r$ , “embeds”  $\text{Jac}_C(\mathbb{F}_q)[r]$  (and any discrete logarithm problem in  $\text{Jac}_C(\mathbb{F}_q)[r]$ ) into  $\mathbb{F}_{q^k}^*$ , and  $\mathbb{F}_{q^k}$  is the smallest-degree extension of  $\mathbb{F}_q$  with this property; whence the name “embedding degree”. Hitt [42] shows that if  $q = p^m$  with  $m > 1$ , then  $\text{Jac}_C(\mathbb{F}_q)[r]$  may be embedded into a smaller field which is not an extension of  $\mathbb{F}_q$  but only an extension of  $\mathbb{F}_p$ . The smallest such field is the so-called *minimal embedding field*, which is  $\mathbb{F}_{p^{\text{ord}_r p}}$ .

We occasionally speak of the embedding degree of the hyperelliptic curve  $C$ , in which case we mean the embedding degree of its Jacobian.

Another important parameter is the  $\rho$ -value, which for a Jacobian variety of dimension  $g$  we define as  $\rho = g \log q / \log r$ . Since  $\#\text{Jac}_C(\mathbb{F}_q) = q^g + O(q^{g-1/2})$ , the  $\rho$ -value measures the ratio of the bit-sizes of  $\#\text{Jac}_C(\mathbb{F}_q)$  and the subgroup order  $r$ . Jacobian varieties with a prime number of points have the smallest  $\rho$ -values:  $\rho \approx 1$ . We call a hyperelliptic curve, and its Jacobian variety, *pairing-friendly* if the Jacobian variety has small embedding degree and a large prime-order subgroup. In practice, we want  $k \leq 60$  and  $r > 2^{160}$ .

Since the embedding degree  $k$  is the order of  $q$  in the multiplicative group  $(\mathbb{Z}/r\mathbb{Z})^*$ , and typically elements in  $(\mathbb{Z}/r\mathbb{Z})^*$  have large order, we expect that for a random Jacobian over  $\mathbb{F}_q$  with order- $r$  subgroup, the embedding degree is approximately of the same size as  $r$ . (This reasoning has been

<sup>1</sup>In general,  $u'$  is a product of lines  $L_i$  whose divisors are  $(P_i) + (-P_i) - 2(P_\infty)$  for  $i = 1, \dots, r$  and  $\text{div}(F - vH - v^2)$  is the sum of the intersection points of  $C$  and a unique curve intersecting  $C$  at  $3g$  points including  $P_1, \dots, P_r$ .

made more precise for elliptic curves, by Balasubramanian and Koblitz [1] and Luca, Mireles and Shparlinski [57].) With  $r > 2^{160}$ , this means that evaluating a pairing for a *random* hyperelliptic curve becomes a computationally infeasible task. Just as in the case of elliptic curves, pairing-friendly hyperelliptic curves are rare and require special constructions.

**3.2. Embedding degrees required for various security levels.** For cryptographic applications, the discrete logarithm problems in  $\text{Jac}_C(\mathbb{F}_q)$  and in the multiplicative group  $\mathbb{F}_{q^k}^*$  must both be computationally infeasible. For Jacobian varieties of hyperelliptic curves of genus 2 the best known discrete logarithm (DL) algorithm is the parallelized Pollard rho algorithm [70, 65], which has running time  $O(\sqrt{r})$  where  $r$  is the size of the largest prime-order subgroup of  $\text{Jac}_C(\mathbb{F}_q)$ . For Jacobian varieties of dimensions 3 and 4 there exist index calculus algorithms of complexities  $O(q^{4/3+\varepsilon}) = O(|\text{Jac}_C|^{4/9+\varepsilon})$  and  $O(q^{3/2+\varepsilon}) = O(|\text{Jac}_C|^{3/8+\varepsilon})$ , respectively [35]. How this compares to the parallelized Pollard rho algorithm depends on the relative size of the subgroup order  $r$  – more precisely, only if  $\rho < 9/8$  (genus 3 case) or  $\rho < 4/3$  (genus 4 case) will the index calculus approach be superior to Pollard rho.

In any case, the best DL algorithms for genus 2, 3, and 4 are of exponential running time. On the other hand, the best algorithm for DL computation in finite fields is the index calculus attack (e.g., [62]) which has running time subexponential in the field size. Thus to achieve the same level of security in both groups, the size  $q^k$  of the extension field must be significantly larger than  $r$ . Table 3.1 shows sample subgroup sizes, extension field sizes, and embedding degrees with which to achieve common levels of security, for various cases  $r \approx q^{g/\rho}$ . The listed sizes for the prime-order subgroups and the extension fields (of large characteristic) follow the recommendations by NIST [61, Table 2].

TABLE 3.1. Embedding degrees for hyperelliptic curves of genus  $g = 2$  required to obtain commonly desired levels of security.

Security level (bits)	Subgroup size ( $r$ )	Extension field size ( $q^k$ )	Embedding degree ( $k$ )					
			$\rho \approx 1$	$\rho \approx 2$	$\rho \approx 3$	$\rho \approx 4$	$\rho \approx 6$	$\rho \approx 8$
80	160	1024	$6g$	$3g$	$2g$	$1.5g$	$g$	$0.8g$
112	224	2048	$10g$	$5g$	$3.3g$	$2.5g$	$1.6g$	$1.3g$
128	256	3072	$12g$	$6g$	$4g$	$3g$	$2g$	$1.5g$
192	384	7680	$20g$	$10g$	$6.6g$	$5g$	$3.3g$	$2.5g$
256	512	15360	$30g$	$15g$	$10g$	$7.5g$	$5g$	$3.8g$

While Table 3.1 as such is for genus 2 only, it can easily be adapted to the cases of genus 3 and 4: Only in the case that the Jacobian has almost prime order ( $\rho \approx 1$ ) we need to compensate for the aforementioned index-calculus algorithms in  $\text{Jac}_C$ . For this, if  $g = 3$ , multiply the second column entries by  $9/8$  and the fourth column entries by  $8/9$ ; if  $g = 4$  multiply the second column entries by  $4/3$  and the fourth column entries by  $3/4$ .

**3.3. Ordinary hyperelliptic curves of low embedding degree.** While there are numerous constructions for pairing-friendly elliptic curves – see e.g. the survey by Freeman, Scott and Teske [21] – there are not nearly as many constructions for hyperelliptic curves of low embedding degree and large prime-order subgroup. In this section, we discuss the case of ordinary Jacobians; see Section 3.4 for the supersingular case. We keep the discussion result-oriented, and refer the reader to the corresponding original papers for details on the specific constructions and the theory underneath.

Galbraith, McKee and Valença [32] argue that heuristically, for any fixed embedding degree  $k$  with  $\varphi(k) \geq 4$  ( $\varphi(k)$  = the Euler phi-function) and for any bound  $M$  on the field size  $q$ , there exist about as many genus 2 curves over  $\mathbb{F}_q$  of embedding degree  $k$  (any  $\rho$ -value) as there exist elliptic curves over  $\mathbb{F}_q$  of embedding degree  $k$ , namely  $\Theta(M^{1/2}/\log M)$ . For embedding degrees  $k = 5, 10$ , they identify several quadratic polynomials  $q(x)$  parameterizing field sizes such that genus 2 curves over  $\mathbb{F}_{q(x)}$  exist with embedding degree  $k$  (any  $\rho$ -value). (They also show that for  $k = 8, 12$ , such quadratic polynomials  $q(x)$  do not exist.)

Freeman [18] was the first to actually construct ordinary genus 2 curves of low embedding degree. His construction is based on the Cocks-Pinch method [11][21, Theorem 4.1], which produces pairing-friendly *elliptic* curves over prime fields of any prescribed embedding degree and with  $\rho \approx 2$ . In the genus-2 case, Freeman obtains curves over prime fields  $\mathbb{F}_q$  of any prescribed embedding degree  $k$  and  $\rho$ -value 8, that is,  $r \approx q^{1/4}$  (where  $r$  denotes the prime subgroup order of the Jacobian).

Freeman [18, Proposition 2.3] further shows that the resulting Jacobian varieties have the property that  $\text{Jac}_C(\mathbb{F}_{q^k})$  always contains two linearly independent  $r$ -torsion points. For an elliptic curve  $E/\mathbb{F}_q$ , the corresponding result implies that the entire  $r$ -torsion group is contained in  $E(\mathbb{F}_{q^k})$ , but this is not necessarily the case for higher dimensional abelian varieties. This phenomenon gives rise to the notion of the *full* embedding degree, which is the smallest integer  $k$  such that all  $r$ -torsion points of  $\text{Jac}_C$  are defined over  $\mathbb{F}_{q^k}$ . Freeman [18, Algorithm 5.1] gives a construction of genus 2 curves of prescribed full embedding degree  $k$  (necessarily even), which may be useful in cryptographic applications that require more than two linearly independent  $r$ -torsion points (see Section 6.8). Again, this construction yields curves with  $\rho$ -value 8.

Note that an essential part of either construction [18] is the use of the complex multiplication (CM) method to compute the actual curve. In genus 2, this includes computation of the Igusa class polynomials (e.g., [72]) of the CM field  $K = \text{End}(\text{Jac}_C) \otimes \mathbb{Q}$ , which is currently feasible for CM fields  $K$  with class numbers less than 100 [49]. (Here,  $\text{End}(\text{Jac}_C)$  denotes the set of all endomorphisms of  $\text{Jac}_C$  defined over  $\mathbb{F}_q$ .)

Freeman, Steinhagen and Steng [22, Algorithm 2.12] present a generalization of the Cocks-Pinch method, which, when coupled with complex multiplication methods, produces pairing-friendly abelian varieties over prime fields, of dimension  $g$  with  $\rho$ -values  $\approx 2g^2$ . This algorithm works for any prescribed embedding degree  $k$ , and applies to arbitrary genus  $g \geq 2$ . (However note that complex multiplication methods are available for special CM fields only if  $g = 3$ , and are completely undeveloped for  $g \geq 4$ .) In addition to explicit genus 2 examples with  $\rho \approx 8$ , a cryptographically interesting example is given for genus 3 ( $k = 17$  and  $\rho \approx 17.95$ ).

In the case of pairing-friendly *elliptic* curves, the method by Brezing and Weng [5] is a generalization of the Cocks-Pinch method [11] and produces elliptic curves over prime fields with  $1 < \rho < 2$  for many embedding degrees. Freeman [19, Algorithm 3.8] combines the Brezing-Weng approach with the method from Freeman, Steinhagen and Steng [22] to construct so-called *families* of abelian varieties over prime fields with  $\rho$ -values strictly less than  $2g^2$ . An explicit construction for genus 2, embedding degree  $k = 5$  and  $\rho = 4$  is given – note that an instantiation with a 224-bit prime subgroup order  $r$  would exactly meet the 112-bit security level requirements (cf. Table 3.1). Other examples (for genus 2) include:  $k = 6$ ,  $\rho = 7.5$ ;  $k = 8$ ,  $\rho = 7.5$ , and  $k = 10$ ,  $\rho = 6$  (able to exactly meet the 256-bit security level requirements) [19, 17]. In the case of genus 3, a construction yielding  $k = 7$  and  $\rho = 12$  is obtained.

All constructions mentioned so far in this section produce absolutely simple Jacobians. When considering simple abelian varieties  $A$  that are isogenous over some extension field  $\mathbb{F}_{q^a}$  ( $q$  a prime)



to a product of two elliptic curves, smaller  $\rho$ -values have been obtained:

Kawazoe and Takahashi [45] specialize to hyperelliptic curves with curve equation  $y^2 = x^5 + ax$  over a prime field  $\mathbb{F}_q$ . For the cardinalities of the Jacobians of such curves, closed formulae exist. These formulae are exploited in adaptations of the Cocks-Pinch method (producing Jacobians with  $\rho$ -values around 4), and Brezing-Weng-type methods (for embedding degree divisible by 8, producing Jacobian varieties with  $3 < \rho < 4$ ). The Jacobians split over  $\mathbb{F}_{q^d}$ ,  $d \in \{2, 4\}$ .

Satoh [67] considers hyperelliptic curves  $C$  of the form  $y^2 = x^5 + ax^3 + bx$  over  $\mathbb{F}_q$ , such that  $\text{Jac}_C$  splits over  $\mathbb{F}_{q^2}$ . This construction works for many embedding degrees and produces  $\rho$ -values  $< 4$ . More generally, Freeman and Satoh [20] show that if  $E$  is defined over  $\mathbb{F}_q$ , and  $A$  is an abelian variety isogenous over  $\mathbb{F}_{q^d}$  to  $E \times E$ , then  $A$  is isogenous over  $\mathbb{F}_q$  to a primitive subvariety of the Weil restriction of  $E$  from  $\mathbb{F}_{q^d}$  to  $\mathbb{F}_q$ . Thus, pairing-friendly abelian varieties of this type can be built from elliptic curves  $E/\mathbb{F}_q$  that are not pairing-friendly over  $\mathbb{F}_q$ , but are pairing-friendly when base-extended to  $\mathbb{F}_{q^d}$ . The elliptic curves can be constructed via Cocks-Pinch or Brezing-Weng type methods. The generic  $\rho$ -value for Jacobians of genus 2 produced in this manner is 4. With the Brezing-Weng method,  $\rho$ -values between 2 and 4 can be obtained. This approach not only contains the constructions by Kawazoe and Takahashi [45] and Satoh [67] but also produces the lowest ever recorded  $\rho$ -values for ordinary genus 2 curves. Explicit examples of cryptographically interesting genus 2 curves are given, such as a  $k = 9$ ,  $\rho \approx 8/3$  curve and a  $k = 27$ ,  $\rho \approx 20/9$  curve.

In conclusion, to date, the best we can achieve for pairing-friendly ordinary genus 2 curves with arbitrary prescribed embedding degree  $k$  is a  $\rho$ -value of 4; and  $\rho \approx 8$  if one insists on absolutely simple Jacobians. (Although to date, there is no apparent reason why Jacobians that split over small-degree extensions should be more vulnerable to DL attacks than the absolutely simple ones.) We have no constructions of ordinary hyperelliptic curves of genus  $g \geq 2$  with  $\rho$ -values less than 2. In particular, we have no constructions of higher-dimensional pairing-friendly ordinary Jacobian varieties with a prime number of points. This is in sharp contrast to the elliptic case, where  $\rho \approx 2$  can be achieved for any prescribed embedding degree,  $1 < \rho < 2$  for selected embedding degrees, and constructions for prime-order elliptic curves exist for embedding degrees  $k = 3, 4, 6, 10$ , and 12 (cf. [21]).

**3.4. Supersingular curves.** Supersingular hyperelliptic curves over  $\mathbb{F}_q$  are always pairing-friendly. In fact, Galbraith [28] shows that there exists a constant  $k(g)$  such that the embedding degree of any supersingular abelian variety of dimension  $g$  over any finite field  $\mathbb{F}_q$  is bounded by  $k(g)$ . Rubin and Silverberg [66] prove that for simple supersingular abelian varieties, for  $g \leq 6$  we have  $k(g) \leq 7.5g$ .

Specifically, for dimension  $g = 2$ , the embedding degree is bounded by 12, where  $k = 12$  can only happen if  $\mathbb{F}_q$  is a binary field  $\mathbb{F}_{2^m}$  with  $m$  odd. If  $q$  is a square, or if  $q = p^m$  with  $m$  odd and  $p \neq 2, 3$ , then the largest embedding degree is  $k = 6$ . If  $\mathbb{F}_q = \mathbb{F}_{3^m}$  with  $m$  odd, the embedding degree is always bounded by 4. (In the case of dimension  $g = 3$ , the embedding degree is bounded by 18, and the bound for the dimension 4 case is 30. In both cases, this bound is achieved only in characteristic three. Over prime fields  $\mathbb{F}_p$  with  $p \geq 11$ , there are no simple supersingular abelian varieties of dimension  $g = 3$ , while the largest embedding degree for dimension  $g = 4$  is  $k = 12$ .)

As Rubin and Silverberg show [66, Corollaries 13,14], not all embedding degrees below these bounds are possible. For example, in the dimension 2 case and if  $q = p^m$  with  $m$  odd, then for  $p = 2$  we have  $k \in \{1, 3, 6, 12\}$ ; if  $p = 3$ , we have  $k \in \{1, 3, 4\}$ ; if  $p = 5$  we have  $k \in \{1, 3, 4, 5, 6\}$  and if  $p \geq 7$  we have  $k \in \{1, 3, 4, 6\}$ .

Cryptographically interesting supersingular hyperelliptic curves can be explicitly constructed. For example, Galbraith et al. [33] give curve equations for various field characteristics that yield simple

supersingular Jacobians of dimension  $g = 2$  and of embedding degrees  $k \in \{4, 5, 6, 12\}$ . By carefully choosing the underlying fields,  $\rho$ -values close to 1 can be readily obtained.

**3.5. Supersingular versus ordinary hyperelliptic curves.** While the embedding degrees of supersingular abelian varieties are limited to a few, small values, their advantage is that they can achieve  $\rho$ -values significantly smaller than their ordinary counterparts. For example, let us consider the 112-bit security level (cf. Table 3.1). One could use the construction by Freeman and Satoh [20] of an ordinary absolutely simple hyperelliptic Jacobian of dimension 2, with embedding degree  $k = 6$  and  $\rho$ -value 2.976, with a 230-bit prime-order subgroup, working over a finite field  $\mathbb{F}_q$  with 342-bit  $q$ . Alternatively, one could use the embedding-degree 12 supersingular curve  $y^2 + y = x^5 + x^3 + b$  ( $b \in \{0, 1\}$ ) over  $\mathbb{F}_{2^m}$  with  $m \geq 250$  chosen such that its Jacobian contains a subgroup of prime order  $r > 2^{224}$ . (Note that Coppersmith’s algorithm [12] for DL computation in finite fields of small characteristic requires to embed the Jacobian into a 3000-bit binary field  $\mathbb{F}_{2^{12m}}$ , to obtain roughly the same level of security provided by a 2048-bit field  $\mathbb{F}_{q^{12}}$  with  $q$  large, cf. [55].) If  $m$  is chosen smaller than 342, this would result in bandwidth advantages for the supersingular Jacobian, given that in cryptographic applications the values that are transmitted are elements in  $\text{Jac}_C(\mathbb{F}_q)$ . However, already at the 128-bit security level the advantage of supersingular curves disappears, in the light of the recent work by Freeman and Satoh [20]: this security level can be achieved with 256-bit prime-order subgroups either of an ordinary Jacobian over a 341-bit  $\mathbb{F}_q$ , with  $k = 9$  and  $\rho = 8/3$ , or of a supersingular Jacobian over  $\mathbb{F}_{2^m}$  with  $m \geq 375$ , of embedding degree 12 (again,  $m$  is chosen in response to Coppersmith’s DL algorithm [12]: a 4500-bit binary field roughly provides the same security as a 3072-bit field of large characteristic). At high security levels ordinary curves are definitely preferable. For example, at the 256-bit level, a genus 2 curve with embedding degree  $k = 27$  and (optimal to date)  $\rho$ -value of 20/9 (cf. [20]) requires a 568-bit field, while a binary supersingular curve of embedding degree 12 requires a 1875-bit field.

#### 4. PAIRINGS FOR HYPERELLIPTIC CURVES

In this section, we give an overview of the different pairings on hyperelliptic curves, as well as introduce the more general framework of *HV pairings* which unify the recent variations on the Ate pairing. In particular, we present a direct proof of bilinearity and non-degeneracy for these pairings and describe how the Ate<sub>*i*</sub> and R-ate pairings fit into the framework.

We begin by introducing the historically most important pairings for hyperelliptic curves, the Tate-Lichtenbaum and Weil pairings. In what follows, let  $r$  be a positive integer and assume that  $C$  is defined over a finite field  $\mathbb{F}_q$ . Suppose that  $K = \mathbb{F}_{q^k}$  is an extension of  $\mathbb{F}_q$  such that  $r \mid (q^k - 1)$ . Throughout the section, we will use  $D$  to mean both a divisor and the divisor class represented by  $D$ .

For a positive integer  $s$ , a *Miller function*  $f_{s,D}$  is a function with divisor

$$(f_{s,D}) = sD - \rho(sD),$$

uniquely defined up to scalar multiplication by elements of  $K^*$ . The *Miller loop length* of such a function is  $\log_2 s$  and measures how quickly the function can be evaluated via Miller’s algorithm (see Algorithm 1). The benefit of recent variations on the Tate-Lichtenbaum pairing is a reduction in Miller loop length, which is sometimes accomplished by combining several Miller functions (see Section 5).

**4.1. Tate-Lichtenbaum pairing.** For  $D_1 \in \text{Jac}_C(K)[r]$ , the divisor  $rD_1$  is linearly equivalent to zero, hence there is some function whose divisor is  $rD_1$ , namely the Miller function  $f_{r,D_1}$  defined above. Let  $D_2$  be a divisor class, with representative  $D_2 = \sum_P n_P(P)$  disjoint from  $D_1$ . We define a pairing called the *Tate-Lichtenbaum pairing* as follows

$$\begin{aligned} \tau : \text{Jac}_C(K)[r] \times \text{Jac}_C(K)/r\text{Jac}_C(K) &\rightarrow K^*/(K^*)^r \\ (D_1, D_2) &\mapsto f_{r,D_1}(D_2) = \prod_P f_{r,D_1}(P)^{n_P}. \end{aligned}$$

This pairing is bilinear, non-degenerate and the result is independent of the choice of representatives of the divisor classes.

**4.2. The Weil pairing.** For  $D_1, D_2 \in \text{Jac}_C(\bar{K})[r]$ , the *Weil pairing* is given by

$$\begin{aligned} e_r : \text{Jac}_C(\bar{K})[r] \times \text{Jac}_C(\bar{K})[r] &\rightarrow \mu_r \\ (D_1, D_2) &\mapsto \tau(D_1, D_2)\tau(D_2, D_1)^{-1} \end{aligned}$$

which can be computed via two Tate-Lichtenbaum pairings. It is bilinear, alternating, and non-degenerate.

**4.3. The modified Tate-Lichtenbaum pairing.** If  $\text{Jac}_C(K)$  contains no elements of order  $r^2$ , then there is an isomorphism

$$\text{Jac}_C(K)[r] \cong \text{Jac}_C(K)/r\text{Jac}_C(K).$$

Under this identification, we define the *modified (or reduced) Tate-Lichtenbaum pairing* to be

$$\begin{aligned} t : \text{Jac}_C(K)[r] \times \text{Jac}_C(K)[r] &\rightarrow \mu_r \\ (D_1, D_2) &\mapsto \tau(D_1, D_2)^{(q^k-1)/r}. \end{aligned}$$

Since elements of  $K^*$  have order dividing  $q^k-1$  and  $r \mid (q^k-1)$ , the  $r^{\text{th}}$  powers which are the quotients of distinct representatives of the coset of  $\tau(D_1, D_2)$  are removed by this *final exponentiation*, leaving a unique result lying in  $\mu_r \subset K$ .

Other powers of the Tate-Lichtenbaum pairing can also give non-degenerate bilinear pairings into  $\mu_r$  which may yield shorter Miller loops (for example, with the use of efficiently computable automorphisms of  $C$  [16]; see Section 6.2).

**4.4. Hyperelliptic Ate pairing.** More generally, a *bilinear pairing* is a map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$$

where  $\mathbb{G}_i$  are abelian groups, in additive notation, and  $\mathbb{G}_3$  is a cyclic group, written multiplicatively, and for all  $p_1, p_2 \in \mathbb{G}_1$ ,  $q_1, q_2 \in \mathbb{G}_2$ , we have

$$\begin{aligned} e(p_1 + p_2, q_1) &= e(p_1, q_1)e(p_2, q_1), \\ e(p_1, q_1 + q_2) &= e(p_1, q_1)e(p_1, q_2). \end{aligned}$$

Let  $r$  be a prime dividing  $\#\text{Jac}_C(\mathbb{F}_q)$  and let  $k$  be the embedding degree of  $\text{Jac}_C(\mathbb{F}_q)$  with respect to  $r$ . We are interested in pairings where  $\mathbb{G}_1$  and  $\mathbb{G}_2$  are subgroups of  $\text{Jac}_C(K)$ , where  $K = \mathbb{F}_{q^k}$ . In particular, a number of more convenient and faster pairings are known when

$$(4.1) \quad \begin{aligned} \mathbb{G}_1 &= \text{Jac}_C(K)[r] \cap \ker(\pi - [1]), \\ \mathbb{G}_2 &= \text{Jac}_C(K)[r] \cap \ker(\pi - [q]), \end{aligned}$$

where  $\pi$  is the  $q^{\text{th}}$  power Frobenius automorphism. Since  $r$  divides  $\#\text{Jac}_C(\mathbb{F}_q)$ , the group  $\mathbb{G}_1$ , being the eigenspace of 1, is at least 1-dimensional over  $\mathbb{Z}/r\mathbb{Z}$ . Since the eigenvalues of the Frobenius come in pairs  $(\lambda, q/\lambda)$  [27, §5.2.3],  $q$  is also an eigenvalue of  $\pi$  on  $\text{Jac}_C[r]$ , and thus there exists a divisor  $D$  such that  $\pi(D) = qD$ . This implies that  $\pi^k D = q^k D = D$ , since  $r|(q^k - 1)$  and  $rD = 0$ . Consequently,  $D \in \text{Jac}_C(\mathbb{F}_{q^k})$ , and the group  $\mathbb{G}_2$  is also at least 1-dimensional over  $\mathbb{Z}/r\mathbb{Z}$ . If  $k > 1$ , then  $\mathbb{G}_1 \neq \mathbb{G}_2$  and  $\mathbb{G}_1 \times \mathbb{G}_2 \subset \text{Jac}_C(\mathbb{F}_{q^k})[r]$  is at least 2-dimensional over  $\mathbb{Z}/r\mathbb{Z}$ . (Recall that for genus  $g$ , the group  $\text{Jac}_C(\overline{K})[r]$  is  $2g$ -dimensional over  $\mathbb{Z}/r\mathbb{Z}$ .)

In the remainder of this section,  $\mathbb{G}_1$  and  $\mathbb{G}_2$  always denote the groups defined in (4.1).

The most basic pairing defined for divisors in  $\mathbb{G}_1, \mathbb{G}_2$  is the *hyperelliptic Ate pairing* [36]:

$$\begin{aligned} a : \mathbb{G}_2 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (D_2, D_1) &\mapsto f_{q, \rho(D_2)}(D_1), \end{aligned}$$

where  $\rho(D_2)$  is the reduced divisor class representative. Since the Frobenius  $\pi$  acts as  $[q]$  on  $D_2$ , we have  $f_{q, \rho(D_2)}(D_1) \in \mu_r$  and no final exponentiation is required [36, Lemma 2]. This is different from the elliptic Ate pairing [41], where a final exponentiation is always required. Another important difference of the hyperelliptic Ate pairing is that to obtain a well-defined value, one *must* use the reduced divisor  $\rho(D_2)$ , not simply any representative of the class  $D_2$ . The Miller loop length for the hyperelliptic Ate pairing is  $\log_2 q$ , in contrast to the elliptic case where the Miller loop length is  $\log_2(t - 1)$  with  $t$  the trace of Frobenius.

**4.5. The Hess-Vercauteren (HV) framework for pairings on Frobenius eigenspaces.** Since 2007, several variations of the Ate pairing have been proposed for elliptic and hyperelliptic curves, exploiting the fact that products and ratios of bilinear, non-degenerate pairings on  $\mathbb{G}_2 \times \mathbb{G}_1$  are also bilinear pairings, but not necessarily non-degenerate [75]. The key is to find combinations of pairings which are both non-degenerate and computable using shorter Miller loops. Following the work of Hess [40] and Vercauteren [71] in the elliptic curve case, we unify these various pairings on  $\mathbb{G}_2 \times \mathbb{G}_1$  in a more general framework, which we call *HV pairings*. The main benefit of this framework is that the criteria for non-degeneracy are more straightforward to verify, giving a direct way to create new pairings. Further investigation of this framework and possible extensions seems likely to be fruitful (see Section 6.1 and (1) in Section 6.9).

Let  $D$  be any divisor in  $\text{Jac}_C(K)[r]$ , and  $s$  an integer. Recall that any divisor  $D$  is equivalent to a unique reduced divisor which we denote  $\rho(D)$ . Let  $h(x) \in \mathbb{Z}[x]$  be a polynomial of the form  $h(x) = \sum_{i=0}^n h_i x^i$  satisfying  $h(s) \equiv 0 \pmod{r}$ . Define a *generalized Miller function*  $f_{s, h, D}$  to be any function with divisor

$$(4.2) \quad \sum_{i=0}^n h_i \rho(s^i D).$$

To see that this divisor is principal, consider the principal divisor

$$\sum_{i=0}^n h_i (s^i D - \rho(s^i D)),$$

which differs by  $(\sum_{i=0}^n h_i s^i)D$  from (4.2). Since  $h(s) \equiv 0 \pmod{r}$ , this is an integer multiple of  $rD$ , which is linearly equivalent to zero by assumption, and thus the divisor (4.2) is principal. As with the standard Miller function, the function  $f_{s, h, D}$  is only defined up to scalar multiples. Also, we note that the Miller function  $f_{r, D}$  for the Tate-Lichtenbaum pairing is equal to  $f_{s, h, D}$  for the constant function  $h(x) = r$  and arbitrary integer  $s$ .

**Theorem 4.1.** *Let  $s \equiv q^j \pmod{r}$  for some  $j \in \mathbb{Z}$ . Let  $h(x) \in \mathbb{Z}[x]$  with  $h(s) \equiv 0 \pmod{r}$ . Then*

$$\begin{aligned} a_{s,h} : \mathbb{G}_2 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (D_2, D_1) &\mapsto f_{s,h,D_2}(D_1)^{(q^k-1)/r} \end{aligned}$$

is a bilinear pairing satisfying

$$a_{s,h}(D_2, D_1) = t(D_2, D_1)^{h(s)/r} \text{ and } a_{s,h}(D_2, D_1) = a(D_2, D_1)^{kq^{k-1}h(s)/r}$$

where  $t$  is the modified Tate-Lichtenbaum pairing and  $a$  is the hyperelliptic Ate pairing. The pairing  $a_{s,h}$  is non-degenerate if and only if  $h(s) \not\equiv 0 \pmod{r^2}$ .

**Remark 4.2.** We note that since  $k$  is the embedding degree of  $\text{Jac}_C(\mathbb{F}_q)$  with respect to  $r$ , in Theorem 4.1  $s$  will be a  $k^{\text{th}}$  root of unity modulo  $r$  since  $q$  is a primitive  $k^{\text{th}}$  root. In Hess's framework, there is the additional condition that  $s$  be a primitive  $k^{\text{th}}$  root of unity modulo  $r^2$ . This requirement is necessary to show the existence of pairings such that the function  $f_{s,h,D}$  is of "lowest degree" (see [40, §3]), but is not required for the result above.

*Proof.* First we show that the pairing is well-defined on divisor classes. Suppose that  $D'_2 \sim D_2$ . Then

$$\text{div}(f_{s,h,D'_2}/f_{s,h,D_2}) = \sum_{i=1}^n h_i(\rho(s^i D'_2) - \rho(s^i D_2)) = \emptyset.$$

This demonstrates well-definition in the factor  $\mathbb{G}_2$ . For the factor  $\mathbb{G}_1$ , it suffices to show that the pairing is trivial under the hypothesis that  $D_1$  is a principal divisor. Suppose  $D_1 = \text{div}(g)$ . For any  $D_2 \in \mathbb{G}_2$ , by the hypothesis that  $s \equiv q^j \pmod{r}$  and  $\rho(rD_2) = \emptyset$ , it is the case that

$$\rho(s^i D_2) = \rho(q^{ij} D_2) = \rho(\pi^{ij} D_2) = \pi^{ij} \rho(D_2) = q^{ij} \rho(D_2) = s^i \rho(D_2) + rD'$$

for some divisor  $D'$  defined over  $\mathbb{F}_q$ . Therefore,

$$\sum_{i=1}^n h_i \rho(s^i D_2) = \sum_{i=1}^n h_i s^i \rho(D_2) + rD''$$

for some  $D''$  defined over  $\mathbb{F}_q$ . Then by the hypothesis, this expression is an  $r$ -th multiple of another divisor  $D'''$  defined over  $\mathbb{F}_q$ . By Weil reciprocity,

$$f_{s,h,D_2}(D_1)^{(q^k-1)/r} = g(rD''')^{(q^k-1)/r} = g(D''')^{q^k-1} = 1,$$

as required.

We show bilinearity and non-degeneracy directly, in contrast to Hess's more general approach in the elliptic curve case [40, Theorem 1].

Let  $s = q^j + \ell r$ , for  $j, \ell \in \mathbb{Z}$ . Linearity in the second coordinate follows from the definition of evaluation of a function on a divisor. To show linearity in the first coordinate, let  $D_2, D_3 \in \mathbb{G}_2$  and  $D_1 \in \mathbb{G}_1$  be non-trivial reduced divisors. Then

$$(f_{s,h,D_2+D_3}) = \sum_{i=0}^n h_i \rho(s^i D_2 + s^i D_3) = \sum_{i=0}^n h_i \rho(s^i D_2) + \sum_{i=0}^n h_i \rho(s^i D_3) + \sum_{i=0}^n h_i (g_i)$$

where

$$(g_i) = \rho(s^i D_2 + s^i D_3) - \rho(s^i D_2) - \rho(s^i D_3).$$

Since  $rD_2 \sim 0$ ,  $rD_3 \sim 0$  and  $s = q^j + \ell r$ , the function  $g_i$  has divisor

$$(g_i) = \rho(q^{ij} D_2 + q^{ij} D_3) - \rho(q^{ij} D_2) - \rho(q^{ij} D_3).$$

Since  $D_2, D_3 \in \mathbb{G}_2$ , the  $q$ -eigenspace of the Frobenius  $\pi$ , and since  $\rho$  commutes with  $\pi$ , we have

$$(g_i) = \rho(D_2 + D_3)^{\pi^{ij}} - \rho(D_2)^{\pi^{ij}} - \rho(D_3)^{\pi^{ij}}.$$

Then  $(g_i) = (m)^{\pi^{ij}}$  where  $m$  is the function with divisor

$$(m) = \rho(D_2 + D_3) - \rho(D_2) - \rho(D_3).$$

As  $f_{s,h,D_2+D_3}$  is evaluated at the divisor  $D_1 \in \mathbb{G}_1$ , which is fixed by  $\pi$ , the value  $g_i(D_1)$  equals  $m(D_1)^{\pi^{ij}} = m(D_1)^{q^{ij}}$ . Thus,

$$\prod_{i=0}^n g_i(D_1)^{h_i} = \prod_{i=0}^n m(D_1)^{h_i q^{ij}} = m(D_1)^{\sum_{i=0}^n h_i q^{ij}} = m(D_1)^{h(q^j)}.$$

Using the fact that  $s = q^j + \ell r$  and  $h(s) \equiv 0 \pmod{r}$ , we see that this value is eliminated by the final exponentiation of  $(q^k - 1)/r$ . Since

$$f_{s,h,D_2+D_3}(D_1) = f_{s,h,D_2}(D_1) f_{s,h,D_3}(D_1) \prod_{i=0}^n g_i(D_1)^{h_i},$$

the pairing  $a_{s,h}$  is linear with respect to the first coordinate.

We now show that

$$a_{s,h}(D_2, D_1) = t(D_2, D_1)^{h(s)/r}$$

using a similar argument. On the right, we have

$$t(D_2, D_1)^{h(s)/r} = \left( f_{r,D_2}(D_1)^{(q^k-1)/r} \right)^{h(s)/r}.$$

Since  $D_2 \in \mathbb{G}_2$ , we have  $\rho(rD_2) = 0$ , thus

$$(f_{r,D_2}^{h(s)/r}) = (h(s)/r)(rD_2 - \rho(rD_2)) = h(s)D_2 = \sum_{i=0}^n h_i s^i D_2.$$

On the left, we have

$$a_{s,h}(D_2, D_1) = f_{s,h,D_2}(D_1)^{(q^k-1)/r}.$$

where by definition

$$(f_{s,h,D_2}) = \sum_{i=0}^n h_i \rho(s^i D_2).$$

We can rewrite this as

$$(f_{s,h,D_2}) = \sum_{i=0}^n h_i s^i D_2 - \sum_{i=0}^n h_i (g_i),$$

where

$$(g_i) = s^i D_2 - \rho(s^i D_2).$$

Since we evaluate at  $D_1 \in \mathbb{G}_1$  fixed by  $\pi$  and  $s = q^j + \ell r$  for some  $\ell \in \mathbb{Z}$ , the contribution of the function with divisor  $(\sum_{i=0}^n h_i (g_i))$  is eliminated by raising to the power  $(q^k - 1)/r$ . Furthermore, we may choose any functions  $f_{r,D_2}$  and  $f_{s,h,D_2}$  with the above divisors, as any discrepancy from scalar multiples will be canceled out when evaluating at the degree zero divisor  $D_1$ . Thus,  $a_{s,h}(D_2, D_1) = t(D_2, D_1)^{h(s)/r}$ .

We have that  $t$  is a non-degenerate pairing and  $h(s) \equiv 0 \pmod{r}$ . Therefore, by the relationship between  $a_{s,h}$  and  $t$ , we conclude that  $a_{s,h}$  is non-degenerate if and only if  $h(s) \not\equiv 0 \pmod{r^2}$ .

For the relationship with the hyperelliptic Ate pairing  $a$ , we use the fact that  $t(D_2, D_1) = a(D_2, D_1)^{kq^k-1}$  [29, Theorem 2].

□

**4.6. Examples of HV pairings.** In this section, we describe how the pairings in the current literature fit into the HV framework. While these pairings can be expressed as  $a_{s,h}$  for some  $s \in \mathbb{Z}$  and  $h(x) \in \mathbb{Z}[x]$ , their actual computation takes an alternate form in order to make use of shorter Miller loops.

- (1) The *generalized Ate pairing* or *Ate<sub>i</sub> pairing*, was defined by Zhang [74] as the analogue of the Ate<sub>i</sub> pairing for elliptic curves [76]. For  $s \equiv q^j \pmod{r}$ ,

$$\begin{aligned} a_s : \mathbb{G}_2 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (D_2, D_1) &\mapsto f_{s,D_2}(D_1)^{(q^k-1)/r}. \end{aligned}$$

Since  $r \mid (q^k - 1)$ , we may assume  $0 < j < k$ . Note that if  $s = q^j$  then no final exponentiation is needed, as is the case for the hyperelliptic Ate pairing. However, this choice of  $s$  is never an improvement over the Ate pairing as the Miller loop length is  $i \log_2 q \geq \log_2 q$ .

For  $s \not\equiv q^j \pmod{r^2}$ , it is straightforward to show this is the HV pairing  $a_{s,h}$  where  $h(x) = x - q^j$ . Writing  $s = q^j + \ell r$  for  $\ell \in \mathbb{Z}$ , we have  $(f_{s,D}) = sD - \rho(sD) = (f_{s,h,D}) + \ell rD$ . As  $\ell rD \sim 0$ , these functions differ only by a constant and thus give the same value after the final exponentiation.

- (2) The Ate pairings defined by Vercauteren [71, Theorem 1] for elliptic curves can be generalized directly to hyperelliptic curves. To define the pairing, we first choose an integer  $m$  relatively prime to  $r$  and express  $mr$  in base  $q$  as  $mr = \sum_{i=0}^n h_i q^i$ . We can decompose the  $m^{\text{th}}$  power of the Tate-Lichtenbaum pairing as

$$(4.3) \quad t(D_2, D_1)^m = f_{\sum_{i=0}^n h_i q^i, D_2}(D_1)^{(q^k-1)/r} = \left( \prod_{i=0}^n f_{h_i q^i, D_2}(D_1) \cdot \prod_{j=0}^{n-1} g_j(D_1) \right)^{(q^k-1)/r}$$

where the  $g_j$  ( $j = 0, \dots, n-1$ ) are auxiliary functions defined through

$$f_{\sum_{i=j}^n h_i q^i, D_2} = f_{\sum_{i=j+1}^n h_i q^i, D_2} f_{h_j q^j, D_2} g_j.$$

The pairing  $a_{[h_0, \dots, h_n]}$  is then defined as

$$\begin{aligned} a_{[h_0, \dots, h_n]} : \mathbb{G}_2 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (D_2, D_1) &\mapsto \left( \prod_{i=0}^n f_{h_i, D_2}(D_1)^{q^i} \cdot \prod_{j=0}^{n-1} g_j(D_1) \right)^{(q^k-1)/r}. \end{aligned}$$

It is easy to see that  $a_{[h_0, \dots, h_n]}(D_2, D_1)$  equals  $t(D_2, D_1)^m$ . Indeed, by definition of the Miller functions and the action of the Frobenius on  $D_1$  and  $D_2$ , we have that

$$f_{h_i, q^i, D_2}(D_1) = f_{q^i, D_2}(D_1)^{h_i} f_{h_i, q^i, D_2}(D_1) = f_{q^i, D_2}(D_1)^{h_i} f_{h_i, D_2}(D_1)^{q^i}$$

as in the proof of [71, Theorem 1]. While not explicitly noted in that proof, it is also true that

$$\left( \prod f_{q^i, D_2}(D_1)^{h_i} \right)^{(q^k-1)/r} = 1,$$

by an argument similar to that of Theorem 4.1. Therefore  $a_{[h_0, \dots, h_n]}(D_2, D_1) = t(D_2, D_1)^m$ . Thus, this pairing is simply the HV pairing  $a_{q,h}$  where  $h(x) = \sum_{i=0}^n h_i x^i$ .

The pairing  $a_{[h_0, \dots, h_n]}$  is computed as a product of many Miller functions, as well as the auxiliary functions, and the total sum of the lengths of the Miller loops of the functions is  $\sum_{i=0}^n \log_2 h_i$ . Thus, for efficiency, this pairing is fastest if the coefficients of  $mr$  in base  $q$  expansion are small. Vercauteren gives an algorithm to find suitable multiples of  $r$  by searching for shortest vectors in a lattice spanned by vectors involving powers of  $q$  [71, §3.3]. This is the “lattice” idea which was further generalized by Hess [40]. See Section 6.1 for a discussion of the smallest loop length possible.

- (3) The *R-ate pairing*, introduced by Lee, Lee and Park in 2008 [53], was the first pairing defined as a ratio of generalized Ate pairings. We give a specific instantiation as an example (cf. [53, Corollary 3.3(3)]). Let  $T_i \equiv q^i \pmod{r}$  and  $T_j \equiv q^j \pmod{r}$ , where  $0 < i < j < k$ , and write  $T_i = aT_j + b$  for some  $a, b \in \mathbb{Z}$ . Then the R-ate pairing is

$$\begin{aligned} R : \mathbb{G}_2 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (D_2, D_1) &\mapsto (f_{a, T_j D_2}(D_1) f_{b, D_2}(D_1) g(D_1))^M, \end{aligned}$$

where  $g$  is an auxiliary function with divisor  $aT_j D_2 + bD_2 - \rho(aT_j D_2 + bD_2)$  and  $M \in \mathbb{N}$  is a final exponent. (The function  $g$  is the analogue of the ratio of a linear and vertical function for the elliptic curve case.) Although it is ambiguous in the original paper, this pairing requires a final exponentiation to yield a unique value. The exponent  $M = (q^k - 1)/r$  is sufficient, though a smaller exponent may also work, depending on the multiplicative orders of  $T_i$  and  $T_j$  modulo  $r$  (see [53, Corollary 3.3(3)] for details). It is easy to work out ([53, Theorem 3.2]) that

$$R(D_2, D_1) = (f_{T_i, D_2}(D_1) / f_{T_j, D_2}(D_1)^a)^M,$$

and thus  $R$  is in fact a ratio of generalized Ate pairings. Since  $f_{a, T_j D_2}(D_1) = f_{a, D_2}(D_1)^{q^j}$  ([76, Theorem 1]), in practice, the R-ate pairing is computed as

$$R(D_2, D_1) = \left( f_{a, D_2}(D_1)^{q^j} f_{b, D_2}(D_1) g(D_1) \right)^M.$$

In this form, and with  $M = (q^k - 1)/r$ , it is a straightforward calculation to establish that  $R$  corresponds to the above Vercauteren pairing  $a_{[h_0, \dots, h_i, \dots, h_j]}$  with  $h_0 = b, h_i = -1, h_j = a$  and all other coefficients equal to zero: let  $\ell_i, \ell_j \in \mathbb{Z}$  such that  $T_i = q^i + \ell_i r$  and  $T_j = q^j + \ell_j r$ , and express the  $r$ -multiple  $(\ell_i - a\ell_j)r$  in base  $q$ , and use that  $f_{1, D_2}$  is a constant function and therefore eliminated by the final exponentiation. In other words,  $R$  is the HV-pairing  $a_{s, h}$  where  $s = q$  and  $h(x) = ax^j - x^i + b$ .

**4.7. Twisted Ate pairing.** In this section, we discuss the *twisted Ate pairing*  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mu_r$ . The twisted Ate pairings use the fact that in certain situations, there is a “twist” of the Frobenius  $\pi$  which acts as  $[q]$  on  $\mathbb{G}_1$  and  $[1]$  on  $\mathbb{G}_2$ , thereby reversing the roles of these groups in the Ate pairing. The main benefit of such pairings is that  $D_1 \in \mathbb{G}_1$  is defined over  $\mathbb{F}_q$ , which means computing the Miller function  $f_{s, D_1}$  is simpler. An added benefit is that the points in  $D_2 \in \mathbb{G}_2$  have  $x$ -coordinates in a subfield of  $\mathbb{F}_{q^k}$  which also may simplify the evaluation, as explained in Section 5.3.

Let  $C$  be a curve over a finite field  $K = \mathbb{F}_q$ . A *twist* of  $C$  is a curve  $C'$  over  $\mathbb{F}_q$  such that there exists an isomorphism  $\phi : C' \rightarrow C$  defined over  $\mathbb{F}_{q^\delta}$  for some  $\delta \in \mathbb{Z}^+$ . If  $\delta$  is the minimal degree extension of  $\mathbb{F}_q$  over which the isomorphism is defined, then the twist  $C'$  is of *degree*  $\delta$ . For more on twists of curves, see Silverman [69, §10.2].

Let  $\pi$  be the Frobenius of  $C$  and let  $\phi^\pi$  denote the isomorphism  $C' \rightarrow C$  obtained by  $\pi$  acting on the coefficients of  $\phi$ . Then  $\phi^\pi \circ \phi^{-1}$  is an automorphism of  $C$  of order  $\delta$  in  $\text{Aut}(C)$ . Thus to look at



twists of  $C$ , one needs to consider the automorphism group of  $C$ . For genus 2 hyperelliptic curves over  $\mathbb{F}_q$ ,  $\text{Aut}(C)$  is isomorphic to one of the following groups [7, 8]:

$$C_2, C_{10}, C_2 \times S_3, V_4, D_8, D_{12}, 2D_{12}, \tilde{S}_4, \tilde{S}_5, M_{32}, \text{ or } M_{160},$$

where  $C_n$  is the cyclic group of order  $n$ ,  $V_4$  is the Klein 4-group,  $D_n$  is the dihedral group of order  $n$ ,  $S_n$  is the symmetric group of order  $n$ ,  $M_n$  is the group of order  $n$  arising from a certain exact sequence [8, Equation 6], and  $2D_{12}, \tilde{S}_4, \tilde{S}_5$  are 2-coverings of  $D_{12}, S_4$ , and  $S_5$ , respectively. This implies that  $\delta$ , as the order of an element in  $\text{Aut}(C)$ , has to divide  $\#\text{Aut}(C)$  for one of the above automorphism groups.

If  $C$  has a twist of degree  $\delta$  with  $m = \gcd(k, \delta) > 1$ , then it is possible to define a non-degenerate, bilinear pairing on  $\mathbb{G}_1 \times \mathbb{G}_2$ . For applications to cryptography, we are interested in using the highest degree twist available, because elements of  $\mathbb{G}_2$  can then be represented as elements of the Jacobian of the twist  $C'$  defined over  $\mathbb{F}_{q^{k/m}}$ .

Given a curve  $C$ , let  $r \mid \#\text{Jac}_C(\mathbb{F}_q)$  be a large prime,  $k$  the embedding degree, and  $C'$  a degree  $\delta$  twist of  $C$ . We have an injection

$$\begin{aligned} [\cdot] : \mu_\delta &\rightarrow \text{Aut}(C) \\ \xi &\mapsto [\xi] \end{aligned}$$

where  $\xi$  is the automorphism defined by the twist. Then  $\mathbb{G}_2 = \text{Jac}_C(\mathbb{F}_q)[r] \cap \ker(\pi - [q]) = \text{Jac}_C(\mathbb{F}_q)[r] \cap \ker([\xi]\pi^{k/m} - 1)$ , and Zhang proved the following theorem ([74, Theorem 2]):

**Theorem 4.3.** *Let  $C$  be a hyperelliptic curve over  $\mathbb{F}_q$  with a twist of degree  $\delta$ . Let  $m = \gcd(k, \delta)$  and  $e = k/m$ . Then*

$$\begin{aligned} a^{\text{twist}} : \mathbb{G}_1 \times \mathbb{G}_2 &\rightarrow \mu_r \\ (D_1, D_2) &\mapsto f_{q^e, D_1}(D_2), \end{aligned}$$

where the representatives of  $D_1 \in \mathbb{G}_1$  and  $D_2 \in \mathbb{G}_2$  have disjoint support, defines a non-degenerate bilinear pairing called the hyperelliptic twisted Ate pairing.

**Remark 4.4.** For  $C$  with  $\gcd(k, \#\text{Aut}(C)) \neq 1$ , any pairing on  $\mathbb{G}_1, \mathbb{G}_2 \subset \text{Jac}_C(\mathbb{F}_q)$  in the HV framework has a twisted version,  $a_{s,h}^{\text{twist}} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mu_r$  [40, Theorem 1].

We now define the *eta pairing*, which is essentially the twisted Ate pairing on supersingular curves, although historically it was introduced before the Ate pairing. The eta pairing makes use of a *distortion map* on  $C$  instead of a twist. Let  $e(\cdot, \cdot)$  denote any bilinear, non-degenerate, Galois-invariant pairing on  $\text{Jac}_C(\mathbb{F}_q)[r]$ . A non-degenerate pairing ensures that given a non-zero divisor class  $D_1$  of order  $r$ , there exists  $D_2$  such that  $e(D_1, D_2) \neq 1$ . However, there are certain instances where a specific  $D_1$  and  $D_2$  pair to 1, for example, where  $D_1, D_2$  both are defined over  $\mathbb{F}_q$  and the embedding degree  $k > 1$ . To remedy this, we introduce distortion maps.

**Definition 4.5.** Let  $e$  be a non-degenerate pairing and  $D_1$  and  $D_2$  non-zero divisor classes of prime order  $r$  on  $C$ . A *distortion map* is an endomorphism  $\psi$  of  $\text{Jac}_C(\mathbb{F}_q)$  such that  $e(D_1, \psi(D_2)) \neq 1$ .

Galbraith et al. [33] proved that distortion maps always exist for supersingular abelian varieties:

**Theorem 4.6.** *Let  $A$  be a supersingular abelian variety of dimension  $g$  over  $\mathbb{F}_q$ , and let  $r$  be a prime not equal to the characteristic of  $\mathbb{F}_q$ . For every two non-trivial elements  $D_1$  and  $D_2$  of  $A(\mathbb{F}_q)[r]$ , there exists an endomorphism  $\psi$  of  $A$  such that  $e(D_1, \psi(D_2)) \neq 1$ .*

The *eta pairing* has been introduced in 2007 by Barreto et al. [2] for supersingular curves. It provides a generalization of the results of Duursma and Lee [14] for a specific instance of supersingular curves. Consider a supersingular curve  $C/\mathbb{F}_q$  (having one point at infinity) which has even embedding degree  $k > 1$ . Let  $D_1$  and  $D_2$  be reduced divisors of degree zero on  $C$  defined over  $\mathbb{F}_q$  representing divisor classes with order  $r$ . Assume that there exists a distortion map  $\psi$  which allows for *denominator elimination* (see Section 5.3), meaning the  $x$ -coordinates of points in  $\psi(D_2)$  lie in a subfield of  $\mathbb{F}_{q^k}$ .

**Definition 4.7.** For  $T \in \mathbb{Z}$ , the *eta pairing*  $\eta_T$  is given by

$$\begin{aligned} \eta_T : \mathbb{G}_1 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (D_1, D_2) &\mapsto f_{T, D_1}(\psi(D_2))^{(q^k - 1)/r}. \end{aligned}$$

Note that in the literature, the eta pairing is often defined without the final exponent, though it is necessary to obtain a unique value in  $\mu_r$ . In general, this pairing is not a non-degenerate, bilinear pairing, but Barreto et al. [2, Theorem 1] give sufficient conditions on  $T$  under which  $\eta_T(\cdot, \cdot)$  can be related to the modified Tate-Lichtenbaum pairing. In particular, this implies that for certain values of  $T$ , the eta pairing is indeed non-degenerate and bilinear. Moreover, the recent work of Lee, Lee and Lee [54, 52] allows us to compute the eta pairing on genus 2 curves for general divisors, which lifts an earlier restriction to the case of degenerate divisors (see Section 5.4).

## 5. FAST COMPUTATION OF HYPERELLIPTIC PAIRINGS

In this section, we summarize the state of the art for fast computation of pairings on hyperelliptic curves of genus 2.

**5.1. Miller’s algorithm.** The algorithm used to compute Weil and Tate-Lichtenbaum pairings on elliptic curves was devised by Victor Miller in 1985 [58] and can be adapted to all pairings discussed in this paper [15]. Referring to the pairing definitions of Section 4 one sees that to compute a pairing, it is necessary to evaluate a Miller function at a divisor. Algorithm 1, futheron referred to as “Miller’s algorithm”, computes such a value using the structure of an addition chain for  $s$ .

Usually, an addition chain takes the form of a double-and-add chain, as follows. Starting with the integer  $k = 0$ , at each step one performs one of two possible calculations to update the value of  $k$ : one either doubles to obtain  $k \rightarrow 2k$  or doubles-and-adds to obtain  $k \rightarrow 2k + 1$ . To determine the sequence of steps needed to obtain any desired integer  $s$  in this way, one reads the binary digits of  $s$  from left to right, doubling once for each ‘0’ and doubling-and-adding for each ‘1.’ (For example,  $5 = 101_2$  is obtained as  $0 \rightarrow 2(0) + 1 = 1 \rightarrow 2(1) = 2 \rightarrow 2(2) + 1 = 5$ .) Starting from 0, this algorithm computes  $s$  in  $\lfloor \log_2 s \rfloor + 1$  steps (each of which consists of either one or two additions).

Miller’s Algorithm computes  $f_{s,D}$  following this double-and-add process by computing the Miller function  $f_{k,D}$  at each step along the way, obtaining  $f_{s,D}$  at the end. A double step involves one addition, and a double-and-add step involves two. For each addition, we compute the new Miller function  $f_{i+j,D}$  from the previously computed  $f_{i,D}$  and  $f_{j,D}$  via the relationship

$$f_{i+j,D} = f_{i,D} f_{j,D} h_{iD,jD}, \quad i, j > 0,$$

where the auxiliary function  $h_{D',D''}$  is a function with divisor

$$\rho(D') + \rho(D'') - \rho(D' + D'').$$

The computation of  $h_{D',D''}$  is performed by an enhanced version of Cantor’s Algorithm (cf. Section 2.3), here Algorithm 2. It is called under the name `Cantor()` once (if doubling) or twice (if doubling and adding) in each for-loop of Miller’s Algorithm. Using the result of Algorithm 2, one calculates

$f_{2i,D}$  from  $f_{i,D}$  (“double”) or  $f_{2i+1,D}$  from  $f_{i,D}$  and  $f_{1,D}$  (“double and add”), where  $f_{1,D}$  is a constant function.

In order to compute the pairing value, the Miller function  $f_{s,D_2}$  must be evaluated a divisor  $D_1$ , but this evaluation is not possible unless  $D_1$  and  $D_2$  have disjoint support, which is not the case if both are reduced. However, using reduced divisors and Mumford representation is too useful to dispense with, so the solution is the following. Let  $z$  be a uniformizer at  $P_\infty$  (for example,  $z(x,y) = x^2/y$  is a convenient choice). Then, if  $f$  is a function with order  $-r$  at  $P_\infty$ , define the *leading coefficient* at  $P_\infty$  of  $f$ , denoted as  $\text{lc}_\infty(f)$ , to be  $(z^r f)(P_\infty)$ . Then the *normalization* of  $f$  is the scalar multiple  $f^{\text{norm}} = f/\text{lc}_\infty(f)$  which has leading coefficient 1. For the hyperelliptic Ate pairing [36, Lemma 6], when  $z$  is  $\mathbb{F}_q$ -rational,

$$f_{q,\rho(D_2)}(D_1) = f_{q,\rho(D_2)}^{\text{norm}}(\epsilon(D_1)).$$

The right-hand expression requires computing the leading coefficient, but solves the problem of non-disjoint supports of  $D_1$  and  $D_2$  without losing the usefulness of Mumford representation.

For HV Pairings and the modified Tate-Lichtenbaum pairing, the same solution is possible. Consider the computation of  $t(D_2, D_1) = f_{r,D_2}(D_1)^{(q^k-1)/r}$  where  $D_1, D_2$  are reduced. Let  $-b_i$  be the coefficient of  $P_\infty$  in  $D_i$  for  $i = 1, 2$ . (Note that  $b_i = -1$  or  $-2$ , depending on whether or not the reduced divisor  $D_i$  is degenerate.) The function  $f_{r,D_2}$  has divisor  $rD_2$  with order  $-b_2r$  at  $P_\infty$ . Therefore, if  $z$  is an  $\mathbb{F}_{q^k}$ -rational uniformizer at  $P_\infty$ ,

$$f_{r,D_2}(D_1) = f_{r,D_2}^{\text{norm}}(\epsilon(D_1))/z(P_\infty)^{b_1 b_2 r}.$$

Since  $b_1 b_2 r$  is a multiple of  $r$ , the contribution of  $z(P_\infty)^{b_1 b_2 r (q^k-1)/r}$  is 1, and thus

$$f_{r,D_2}(D_1)^{(q^k-1)/r} = f_{r,D_2}^{\text{norm}}(\epsilon(D_1))^{(q^k-1)/r}.$$

As the HV pairing  $a_{s,h}(D_2, D_1)$  is a simply a power of the modified Tate pairing  $t(D_2, D_1)$  (see Theorem 4.1), in whichever form the pairing  $a_{s,h}(D_2, D_1)$  is computed, evaluating normalized functions at effective divisors will give the pairing value.

In the elliptic curve case, it is more efficient to evaluate the Miller functions and the auxiliary functions  $h_{D',D''}$  at the desired divisor (denoted  $D_2$  in Miller’s Algorithm) at each step, instead of reserving the evaluation for the end. In order to allow for this,  $D_2$  is passed to Cantor’s Algorithm. We now turn to a discussion of this aspect in the case of hyperelliptic curves.

In Miller’s Algorithm, the current Miller function  $f$  is stored as two polynomials  $f_1$  and  $f_2$  such that  $f = f_1/f_2$ . Similarly, the auxiliary functions  $h$  are returned from Cantor’s Algorithm as  $h_1$  and  $h_2$ . It remains to explain how to evaluate a polynomial function  $g(x,y)$  on  $C$  at the effective part of a divisor given in Mumford representation  $(u(x), v(x))$  (we need only the effective part because of the preceding discussion and the computation of the leading coefficient). We need to evaluate  $G(x) = g(x, v(x))$  at the zeroes of  $u(x)$ . This is the same as computing the resultant  $\text{Res}(G(x), u(x))$ . Performing a resultant calculation is sufficiently costly that it is best left to the end of Miller’s Algorithm, as long as the size of the Miller functions can be kept low in the meantime. Fortunately, in preparation for the eventual final resultant, it suffices to compute the Miller functions in  $x$  and  $y$  modulo  $u(x)$ , while substituting  $y = v(x)$ , effectively capping their degrees.

If Steps 5 and 8 through 13 are removed from Cantor’s Algorithm and only  $(U, V)$  is returned, the algorithm computes  $\rho(D_1 + D_2)$  for any divisors  $D_1$  and  $D_2$  in Mumford representation (this is the usual meaning of “Cantor’s Algorithm” as in Section 2.3). If these steps are included, then Cantor’s Algorithm can also return  $f, g \pmod{u}$  such that  $f/g = h_{D_1, D_2}(x, v(x))$  for some specified divisor  $(u, v)$ . This is the form in which it is used in Miller’s Algorithm.

---

**Algorithm 1** Miller's Algorithm

---

**Input:**  $D_1 = (u_1, v_1)$ ,  $D_2 = (u_2, v_2)$ ,  $d$ ,  $s = \sum_{i=0}^N s_i 2^i$ **Output:**  $f_{s, D_1}^{\text{norm}}(\epsilon(D_2))^d$ 

```

1:  $D \leftarrow D_1$ 
2:  $f_1 \leftarrow 1, f_2 \leftarrow 1, f_3 \leftarrow 1$ 
3: for  $i = N - 1$  down to 0 do
4:    $f_1 \leftarrow f_1^2 \pmod{u_2}, f_2 \leftarrow f_2^2 \pmod{u_2}, f_3 \leftarrow f_3^2$ 
5:    $(D, h_1, h_2, h_3) \leftarrow \text{Cantor}(D, D, D_2)$ 
6:    $f_1 \leftarrow f_1 \cdot h_1 \pmod{u_2}, f_2 \leftarrow f_2 \cdot h_2 \pmod{u_2}, f_3 \leftarrow f_3 \cdot h_3$ 
7:   if  $s_i = 1$  then
8:      $(D, h_1, h_2, h_3) \leftarrow \text{Cantor}(D, D_1, D_2)$ 
9:      $f_1 \leftarrow f_1 \cdot h_1 \pmod{u_2}, f_2 \leftarrow f_2 \cdot h_2 \pmod{u_2}, f_3 \leftarrow f_3 \cdot h_3$ 
10:  end if
11: end for
12: return  $\left( \text{Res}(f_1, u_2) / (f_3^{\deg(u_2)} \cdot \text{Res}(f_2, u_2)) \right)^d$ 

```

---



---

**Algorithm 2** Cantor's Algorithm

---

**Input:**  $D_1 = (u_1, v_1)$ ,  $D_2 = (u_2, v_2)$ ,  $D' = (u, v)$ **Output:**  $\rho(D_1 + D_2), f(x, v(x)) \pmod{u}, g(x, v(x)) \pmod{u}, \text{lc}_\infty(h_{D_1, D_2})$  where  $h_{D_1, D_2} = f/g$ 

```

1: compute  $(d_1, e_1, e_2)$  such that  $d_1 = e_1 u_1 + e_2 u_2 = \gcd(u_1, u_2)$ 
2: compute  $(d, c_1, c_2)$  such that  $d = c_1 d_1 + c_2(v_1 + v_2 + H) = \gcd(d_1, v_1 + v_2 + H)$ 
3:  $s_1 \leftarrow c_1 e_1, s_2 \leftarrow c_1 e_2, s_3 \leftarrow c_2$ 
4:  $U \leftarrow (u_1 u_2) / d^2, V \leftarrow (s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + F)) / d \pmod{U}$ 
5:  $f \leftarrow d \pmod{u}, g \leftarrow 1, h \leftarrow 1$ 
6: while  $\deg(U) > g$  do
7:    $U' \leftarrow (F - V H - V^2) / U, V' \leftarrow (-H - V) \pmod{U'}$ 
8:    $f \leftarrow f \cdot (v - V) \pmod{u}$ 
9:    $g \leftarrow g \cdot U' \pmod{u}$ 
10:  if  $\deg(V) > g$  then
11:     $h \leftarrow -\text{leadingcoeff}(V) \cdot h$ 
12:  end if
13:   $U \leftarrow U', V \leftarrow V'$ 
14: end while
15: return  $(U, V), f, g, h$ 

```

---

In the case that we are pairing degenerate divisors (see Section 5.4), a norm computation may be preferred to the resultant method [29].

**5.2. Using effective divisors and the leading coefficient.** The leading coefficient of  $f_{s, D}$  is an element of the field of definition of the function. Therefore, in the case of twisted pairings, the leading coefficient of  $f_{s, D_1}$  is defined over  $\mathbb{F}_q$ . Therefore, if the pairing includes a final exponentiation, the leading coefficient will be eliminated and thus may be ignored in the computation of the pairing.

**5.3. Final exponentiation.** As described in Section 4, most of the hyperelliptic pairings involve a *final exponentiation* of a Miller function  $f_{s, D}(D')$  by  $(q^k - 1)/r$ , where  $D \in \text{Jac}_C(\mathbb{F}_q)[r]$  and  $D'$  is an arbitrary divisor in  $\text{Jac}_C(\mathbb{F}_{q^k})$ . As has been widely reported, this extra computation has its benefits,

in particular when  $k$  is even. Many of these are described by Scott [68] and Galbraith, Hess, and Vercauteren [29]; we summarize the main ones here.

When  $k$  is even, the field  $\mathbb{F}_{q^k}$  can be constructed as a degree two extension of  $\mathbb{F}_{q^\ell}$ , where  $2\ell = k$ . We can represent elements as  $a + ib$  with  $a, b \in \mathbb{F}_{q^\ell}$  and  $\gamma^2$  a quadratic non-residue over  $\mathbb{F}_{q^\ell}$ . It is straightforward to check that

$$(1/(a + \gamma b))^{q^\ell - 1} = (a - \gamma b)^{q^\ell - 1}$$

which means inversion can be replaced by conjugation since the result is the same after final exponentiation. In particular, this applies to any denominators of computations in Miller's algorithm.

There is a further optimization, *denominator elimination*, which in fact allows one to ignore all denominators in Miller's algorithm. In computing  $f_{s,D}(D')$  where  $D$  is a divisor defined over the base field  $\mathbb{F}_q$ , one computes the numerator and denominator values separately (see Algorithm 1). If  $D' = (u(x), v(x))$  has  $u(x)$  defined over  $\mathbb{F}_{q^\ell}$ , then the computation of the denominator involves only  $D$  and  $u(x)$  and therefore becomes trivial after final exponentiation. In the case of supersingular curves, for example, a suitable evaluation divisor can be found using a distortion map  $\psi$  (see Section 4.7) such that  $\psi(D')$  has  $x$ -coordinates in  $\mathbb{F}_{q^\ell}$  [33].

The final exponentiation is generally computed in multiple steps by writing  $(q^k - 1)/r$  as a product of polynomials in base  $q$  expansion and exploiting finite field constructions, in particular the  $q^{\text{th}}$  power of Frobenius, which speeds up computation [29]. Other methods for faster computation include signed sliding window methods [37], as well as trace and tori methods [34, 38].

**Remark 5.1.** As the Ate pairing does not require final exponentiation, these techniques are unavailable. Furthermore, as stated by Granger et al., there are also possible security implications; namely, the problem of *pairing inversion* (given  $\gamma$  and  $D_1$ , find  $D_2$  such that  $a(D_1, D_2) = \gamma$ ) may not be as hard (see [36, Intro.]). However, we remark that if  $r^2 \nmid (q^k - 1)$  and  $r$  is prime, a superfluous final exponentiation of the Ate pairing still gives a non-degenerate result.

**5.4. Degenerate divisors.** For a genus 2 curve, a general reduced divisor  $D$  is of the form  $D = (P_1) + (P_2) - 2(\infty)$  and a degenerate divisor is of the form  $D = (P) - (\infty)$ . As there are fewer points in the support, the arithmetic is faster when adding a general divisor to a degenerate divisor than when adding two general divisors. This speeds up the computation of the Miller function  $f_{s,D}$  where  $D$  is degenerate. Furthermore, the evaluation of a Miller function on a degenerate divisor is also faster by at least half, since there is only one affine point. Many of the fastest hyperelliptic pairing computations use degenerate divisors, including the examples noted with [a], [b] and [c] in the Table 5.6. We summarize here when it is possible to use degenerate divisors as either the first or second argument of a pairing.

Should  $\text{Jac}_C(\mathbb{F}_q)$  be of prime order  $r$ , then for any  $P \in C(\mathbb{F}_q)$ , the divisor  $D = (P) - (\infty)$  can be used as the first argument, regardless of the pairing. Furthermore, if  $C$  is supersingular, then using a distortion map  $\psi$  (see Section 4.7), we have that  $\psi(D)$  is also degenerate and pairs non-trivially with  $D$ . Hence, for supersingular curves with prime-order  $\text{Jac}_C(\mathbb{F}_q)$ , we can use degenerate divisors as both arguments of the Tate-Lichtenbaum pairing. This fact was originally exploited in the definition of the  $\eta_T$  pairing by Duursma and Lee [14]. In the more general situation where  $\#\text{Jac}_C(\mathbb{F}_q)$  is not prime and/or the curve  $C$  is not supersingular, using degenerate divisors is not as straightforward, as noted by Frey and Lange [24]. If  $\#\text{Jac}_C(\mathbb{F}_q) = nr$  where  $\gcd(n, r) = 1$ , there is no guarantee that there exists a degenerate divisor  $D$  of order  $r$ . The probability that a reduced divisor is of order  $r$  is  $1/n$  and the probability that a divisor is degenerate is roughly  $1/q$ , by the Hasse-Weil bounds on  $C(\mathbb{F}_q)$  and  $\text{Jac}_C(\mathbb{F}_q)$ . Therefore, assuming independence, a heuristic argument gives that the

probability a divisor is degenerate and order  $r$  is  $1/qn$ . This implies that using a degenerate divisor for the first argument is not necessarily possible.

However, Frey and Lange [24] show that for  $q$  large enough (as in a cryptographic setting), it is possible to use a degenerate divisor as the second argument. In other words, there exists  $D_2 = (P) - (\infty) \in \text{Jac}_C(\mathbb{F}_{q^k})$  such that for any  $D_1 \in \text{Jac}_C(\mathbb{F}_q)[r]$ , the Tate-Lichtenbaum pairing  $\tau(D_1, D_2)$  is non-trivial. The probability that  $P \in C(\mathbb{F}_{q^k})$  yields such a divisor  $D_2$  has a lower bound of  $1/k \log_2 q$ . Moreover, if  $k = 2d$  is even, it is possible to choose  $P = (x, y)$  with  $x \in \mathbb{F}_{q^d}$  and  $y \in \mathbb{F}_{q^k}$ , using a degenerate divisor on the quadratic twist of  $C/\mathbb{F}_{q^d}$ . This technique is used for example by Fan, Gong and Jao [16] and allows for denominator elimination.

**Remark 5.2.** As remarked by Galbraith, Hess and Vercauteren [29, §7], there are potential security implications with using degenerate divisors, depending on the application. While the discrete logarithm problem with a degenerate divisor as a base point is no easier than that with a general divisor [44], other hardness assumptions such as pairing inversion (see Remark 5.1) are potentially compromised, as Granger et al. have noted [36]. To our knowledge, the topic remains unresolved.

We also remark that there are protocols in which it may not always be possible to use degenerate divisors, for example, when computing a pairing where one input is required to be a random multiple of a divisor  $D$ .

**5.5. Rubin-Silverberg point compression.** Another method available to us in genus 2 is the point compression technique of Rubin and Silverberg [66], who note that supersingular abelian varieties can be identified with subvarieties of Weil restrictions of supersingular elliptic curves.

Recall that a *supersingular  $q$ -Weil number* is a complex number of the form  $\sqrt{q}\zeta$ , where  $\zeta$  is a root of unity and  $\sqrt{q}$  denotes the positive square root. Let  $m$  be the order of  $\zeta$ .

The following theorem allows us to define a useful invariant:

**Theorem 5.3** ([66]). *Suppose  $A$  is a simple supersingular abelian variety of dimension  $g$  over  $\mathbb{F}_q$ , where  $q$  is a power of a prime  $p$ , and  $P(x)$  is the characteristic polynomial of the Frobenius endomorphism of  $A$ . Then  $P(x) = G(x)^e$ , where  $G(x) \in \mathbb{Z}[x]$  is a monic irreducible polynomial with  $e = 1$  or  $2$ . All of the roots of  $G$  are supersingular  $q$ -Weil numbers.*

We call the roots of  $G$  the  *$q$ -Weil numbers* for  $A$ .

**Definition 5.4.** The *cryptographic exponent* of  $A$  is defined by

$$c_A = \begin{cases} \frac{m}{2} & , \text{ if } q \text{ is a square} \\ \frac{m}{\gcd(2, m)} & , \text{ if } q \text{ is not a square.} \end{cases}$$

Let  $\alpha_A = c_A/g$ ; it is the *security parameter* of  $A$ .

Now let  $\mathbb{F} \subset \mathbb{F}'$  be finite fields,  $E$  an elliptic curve over  $\mathbb{F}$ , and let  $Q \in E(\mathbb{F}')$ . Recall that the trace from  $\mathbb{F}'$  to  $\mathbb{F}$  is given by

$$\text{Tr}_{\mathbb{F}'/\mathbb{F}}(Q) = \sum_{\sigma \in \text{Gal}(\mathbb{F}'/\mathbb{F})} \sigma(Q).$$

Rubin and Silverberg prove the following result:

**Theorem 5.5** ([66]). *Let  $E$  be a supersingular elliptic curve over  $\mathbb{F}_q$ ,  $\pi$  a  $q$ -Weil number for  $E$  ( $\pi \notin \mathbb{Q}$ ). Fix  $r \in \mathbb{N}$  with  $\gcd(r, 2pc_E) = 1$ . Then there is a simple supersingular abelian variety  $A$  over  $\mathbb{F}_q$  having the following properties.*

- (1)  $\dim A = \varphi(r)$ .
- (2) For every primitive  $r^{\text{th}}$  root of unity  $\zeta$ ,  $\pi\zeta$  is a  $q$ -Weil number for  $A$ .
- (3)  $c_A = rc_E$ .
- (4)  $\alpha_A = (r/\phi(r))\alpha_E$ .
- (5) There is a natural identification of  $A(\mathbb{F}_q)$  with the following subgroup of  $E(\mathbb{F}_{q^r})$  :

$$\{Q \in E(\mathbb{F}_{q^r}) : \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_{q^{r/l}}}(Q) = 0 \text{ for every prime } l \mid r\}.$$

This theorem can be thought of as a form of point compression for supersingular elliptic curves. More concretely, the theorem allows us to replace the Jacobian of a hyperelliptic curve  $C$  over  $\mathbb{F}$  with an elliptic curve  $E$  over an extension  $\mathbb{F}'$  of  $\mathbb{F}$ , while still exploiting the per-bit security gain of higher genus hyperelliptic curves. From a security standpoint, there is no difference between working with  $E(\mathbb{F}')$  and working with  $\text{Jac}_C(\mathbb{F})$ . On the other hand, one needs fewer bits to represent divisors with support in  $C(\mathbb{F})$  than to represent points in  $E(\mathbb{F}')$ .

As noted by Galbraith [28], recent implementations [2] indicate that pairings on elliptic curves with the Rubin-Silverberg compression are, in general, more efficient than using the pairings on Jacobians of hyperelliptic curves. However, it seems that Rubin and Silverberg have initiated a promising investigation into the arithmetic geometry of abelian varieties and its applications to pairings. Much work remains to be done, in particular with respect to the torsion structure of these varieties.

**5.6. A comparison of pairings.** We conclude this section by summarizing in Table 5.6 all known variants of the Tate-Lichtenbaum pairing defined in Section 4, in terms of their loop length and whether or not there is a final exponent of  $(q^k - 1)/r$ . Note that if there is a final exponent, in the case of even embedding degree  $k$ , this allows for the optimizations described in Section 5.3. The last column gives references to specific examples of curves of genus 2 in the literature for which the efficiency of the pairing has been analyzed, either theoretically, via implementation or both.

All pairings in Table 5.6 except the Tate-Lichtenbaum pairing and the modified Tate-Lichtenbaum pairing are defined on  $\mathbb{G}_2 \times \mathbb{G}_1$ , but if  $\gcd(k, \#\text{Aut}(C)) \neq 1$ , then there exist the twisted versions on  $\mathbb{G}_1 \times \mathbb{G}_2$  which have the same final exponent and loop length.

TABLE 5.6. A comparison of pairings.

Pairing	Curves	Final Exponent	Loop Length	Examples for $g = 2$
Modified Tate	All	Yes	$\log_2 r$	$[16]^a$ , [39, §5], [10],
Ate [36]	All	No	$\log_2 q$	
Eta [2]	Supersingular	Yes	Varies ( $\log_2 q$ ) possible	$[2]^b$
HV [40, 71]	All	Yes	Varies ( $\log_2 r$ )/ $\varphi(k)$ possible	$[71, §4]^c$
Ate <sub><math>i</math></sub> [74]	All	Yes	$\log_2(q^i \pmod{r})$ ( $\log_2 r$ )/ $\varphi(k)$ possible	$[74, §5]^d$
R-ate [53]	All	Yes	Varies	$[53, §5]^e$ , [31, §4,5] <sup>f</sup>

- [a] Fan, Gong and Jao use efficiently computable automorphisms to compute a power of the modified Tate-Lichtenbaum pairing on two Kawazoe-Takahashi families of non-supersingular curves over prime fields. This algorithm allows for a theoretical reduction of up to one fourth in the length of the Miller loop ( $\log_2 r$ ). They implement this on curves over  $\mathbb{F}_p$  where  $p$  is a 329-bit prime and  $k = 4$  and compare this with pairings on a supersingular curve defined over  $\mathbb{F}_p$  with  $p$  a 256-bit prime and  $k = 4$ . Using all known optimizations (degenerate divisors, encapsulated group operations, final exponentiation, fast field arithmetic), the pairing computation on the non-supersingular curve is about 55.8% faster.
- [b] This is one of the fastest known pairing implementations on a hyperelliptic curve and makes use of many optimizations including degenerate divisors and a special octupling formula.
- [c] Vercauteren gives an example of a family of supersingular curves with  $k = 12$  such that the loop length is approximately  $\log_2 r / \varphi(k)$ .
- [d] Zhang gives examples of Kawazoe-Takahashi curves with  $k = 8, 24$  such that the twisted Ate pairing has loop length approximately  $\log_2 r / \varphi(k)$ .
- [e] Lee, Lee and Park show that for supersingular curves the loop length can theoretically be approximately  $(\log_2 q) / 2$ . They also compute an example on a Duursma-Lee curve with  $k = 5$ , achieving a loop length 21% shorter than the Ate.
- [f] Galbraith, Lin and Mireles Morales [31] describe how to use the R-ate pairing on a real model of a hyperelliptic curve of genus 2 over  $\mathbb{F}_p$  with  $k = 6$ . By using a distortion map  $\psi$  on  $\text{Jac}_C(\mathbb{F}_p)[r]$  such that the image of  $\mathbb{G}_1$  is in the  $p$ -eigenspace,  $\mathbb{G}_2$ , they are also able to make use of denominator elimination. They conclude that such pairings are theoretically competitive with both pairings on certain elliptic curves with  $k = 3$  and with hyperelliptic curves in the imaginary model with  $k = 4$ .

## 6. FUTURE WORK ON HYPERELLIPTIC PAIRINGS

In this section, we present possible areas for future work, expanding upon the list in the 2007 survey paper of Galbraith, Hess and Vercauteren [29]. We list some newer problems, mention some recent advancements in the elliptic curve case which may find generalizations in pairings for  $g \geq 2$ , and conclude by revisiting the 2007 list [29].

**6.1. Achieving optimal loop length.** Since 2007, there has been a flurry of new work to reduce the loop length in Miller’s algorithm using variants of the Ate pairing. In particular, the Ate pairing on hyperelliptic curves of genus  $g$  already reduces the loop length by up to a factor of  $g$  when compared to the Tate-Lichtenbaum pairing [36]. Vercauteren [71] uses the following definition to characterize pairings with certain loop lengths.

**Definition 6.1.** [71] Let  $e : \mathbb{G}_1 \times \mathbb{G}_2 \mapsto \mu_r \subset \mathbb{F}_{q^k}^*$  be a non-degenerate, bilinear pairing defined using a combination of Miller functions. We call  $e(\cdot, \cdot)$  an *optimal* pairing if it can be computed using  $(\log_2 r) / \varphi(k) + \varepsilon(k)$  Miller iterations, where  $\varphi$  is the Euler phi function and  $\varepsilon(k) \leq \log_2 k$ .

Note that this means a pairing is optimal if the total sum of all the loop lengths of the Miller functions is approximately  $(\log_2 r) / \varphi(k)$ .

For an HV pairing  $a_{s,h(x)}$  with  $h(x) = \sum_{i=0}^n h_i x^i$ , the total sum of loop lengths is  $\sum_{i=0}^n \log_2 h_i$ . Thus to be optimal, it is necessary but not sufficient that the coefficients of  $h$  are bounded by  $r^{\varphi(k)}$ . This can be achieved by finding the shortest vectors in a lattice spanned by vectors involving powers of  $s$  [71, §3.3]. Vercauteren and Zhang both give examples of genus 2 HV pairings (see Table 5.6) where the polynomial  $h(x)$  satisfies this bound and has only one coefficient which is not  $\pm 1$ , therefore



providing examples of optimal hyperelliptic pairings. It remains open whether given a hyperelliptic curve it is always possible to construct an optimal HV pairing. One direction would be to look at extending the method of Vercauteren [71] which constructs optimal pairings on *parameterized* families of elliptic curves.

Vercauteren also conjectures that for elliptic curves without efficiently computable automorphisms other than the Frobenius, no pairing can be better than optimal [71, §2]. More specifically, he conjectures that for such a curve, any non-degenerate pairing requires at least  $(1 - \delta) \log_2 r / \varphi(k)$  Miller iterations where  $0 < \delta < 1/4$ . For a curve with a set of efficiently computable endomorphisms  $\mathcal{E} \subset \text{End}(E)$ , Vercauteren defines a *superoptimal* pairing as one which can be computed using  $(\log_2 r) / \#\mathcal{E} + \varepsilon(k)$  Miller iterations. It remains to examine what is the best possible for genus 2 curves, both with and without the existence of efficiently computable endomorphisms (see also Section 6.2). Furthermore, it is not known whether there are other non-degenerate, bilinear hyperelliptic pairings on  $\mathbb{G}_1 \times \mathbb{G}_2$  which are not part of the HV framework.

Lastly, we remark that the computation of an HV pairing cannot be measured solely by the sum of loop lengths. There is also the cost of computing the auxiliary functions (see (2),(3) in Section 4.6). It remains to formally compare the cost of these additional computations with the benefit of a shorter total sum of Miller loop lengths.

**6.2. Using efficiently computable automorphisms.** One newer method to speed up computations is to use efficiently computable automorphisms of the curve  $C$  (beyond the Frobenius). For example, Fan, Gong and Jao use efficiently computable automorphisms in computing a power of the modified Tate-Lichtenbaum pairing on some specific non-supersingular genus 2 curves over prime fields [16]. An open task is to explore how far can this be generalized to other genus 2 curves.

Furthermore, Hess [40] extends his pairing framework for ordinary elliptic curves to exploit efficiently computable automorphisms. This does not generally give an improved loop length since  $\#\mathcal{E} \leq \varphi(k)$  for most ordinary elliptic curves. However, as hyperelliptic curves have a greater variety of  $\text{Aut}(C)$ , it would be worthwhile to examine what improvements in loop length can be made by extending the HV framework to exploit these automorphisms.

**6.3. Fast arithmetic and the embedding degree.** In the case of even embedding degree  $k$ , it is traditional to exploit the degree two subfield, as explained in Section 5.3. In fact, Koblitz and Menezes define *pairing friendly fields* to be finite fields of the form  $\mathbb{F}_{q^k}$  such that  $k = 2^i 3^j$  for  $0 \leq i, j \in \mathbb{Z}$  and  $q \equiv 1 \pmod{12}$  [48, §5]. (If  $k$  is strictly a power of 2 then it is only required that  $q \equiv 1 \pmod{4}$ .) By a theorem of Lidl and Niederreiter [56, Theorem 3.75] and more particularly, by a specific instance of this theorem given by Koblitz and Menezes [48, Theorem 2], we can construct the extension  $\mathbb{F}_{q^k}$  for  $k$  of this form using a tower of quadratic and cubic extensions. There are thus certain advantages we can make use of for  $k = 2^i 3^j$ . For instance, there exist fast arithmetic methods for degree 2 and 3 subextensions; namely, the Karatsuba method for quadratic subextensions and the Toom-Cook method for cubic subextensions [46, §4.3.3]. These methods are used to economize the arithmetic in the smaller fields which reduce the number of field multiplications. However, there are embedding degrees not of this form, particularly among recent constructions of non-supersingular curves, and hence it would be worthwhile to see if these ideas can be extended to embedding degrees  $k$  containing other prime factors.

**6.4. Degenerate divisors.** As discussed in Section 5.4, one common optimization is to use degenerate divisors. Frey and Lange [24] give a lower bound on the probability that  $P \in C(\mathbb{F}_{q^k})$  gives a non-trivial pairing value when used as a degenerate divisor in the second argument of the Tate-Lichtenbaum pairing. However, to our knowledge, there is no method to efficiently find such points beyond simple trial and error.

We also consider using degenerate divisors with Ate-type pairings  $a$  on  $\mathbb{G}_2 \times \mathbb{G}_1$  (or twisted Ate on  $\mathbb{G}_1 \times \mathbb{G}_2$ ). While a heuristic argument shows that the likelihood that a divisor of  $\mathbb{G}_1$  is degenerate is small, it would be useful to know if there are particular curves where this is more likely and if so, how to find such divisors. It also remains to analyze the likelihood that an element of  $\mathbb{G}_2$  is degenerate. We note that for  $D \in \mathbb{G}_2$ , if  $D = (P) - (\infty)$ , then  $\pi(D) = (\pi(P)) - (\infty)$  implies that the divisor class  $qD$  is also degenerate.

**6.5. Ignoring the last bit.** In the case of the modified Tate-Lichtenbaum pairing on elliptic curves, when computing  $f_{r,D_1}(D_2)$ , it is possible to ignore the last bit in the expansion of  $r$ . This follows from the fact that since  $r$  is odd, the last iteration of the Miller loop of the Tate-Lichtenbaum pairing is the evaluation at  $D_2$  of the line function corresponding to the line through  $(r-1)P$  and  $P$ . This is a vertical line and so by the choice of divisor  $D_2$  with  $x$ -coordinates lying over  $\mathbb{F}_{q^d}$ , this is eliminated by the final exponentiation. While this does not give a large improvement compared to other loop length reductions, it is worth verifying whether this trick might be used in the case of hyperelliptic curves.

**6.6. Compression and higher degree twists.** Galbraith and Lin [30] give explicit formula to compute the Weil pairing on elliptic curves given only  $x$ -coordinates, and the Tate-Lichtenbaum and Ate pairings given both  $x$ -coordinates but at most one  $y$ -coordinate. This form of point compression is advantageous for elliptic curve pairings with small embedding degree, where one would be working over a field of large order (and consequently, taking a square root to recover  $y$  could be expensive). The compression makes use of explicit recurrence formulas for elliptic curve point multiplication and for Miller functions in the case of embedding degree  $k = 2$ . As these recurrences are given solely in terms of the  $x$ -coordinate of the point, the pairings are also computed in terms of the  $x$ -coordinate of the points involved. Note, however, that neglecting the value of  $y$  introduces a sign ambiguity, but this is resolved by taking the trace of the pairing, which is independent of the sign of  $y$ . It is perhaps worth investigating if the analogous results may be obtained for hyperelliptic pairings (for curves of the form  $y^2 = F(x)$ ) of small embedding degree.

Another form of compression involves algebraic tori, which are  $d$ -dimensional generalizations of the multiplicative group  $\mathbb{G}_m$ . Naehrig, Barreto and Schwabe [60] use algebraic tori to compress computations, not just in the final exponentiation but also in the Miller loop of elliptic curve pairings. Their methods rely on explicit formulas for multiplication and squaring of torus elements and also exploit degree 6 twists. One might want to try similar methods for certain twists of hyperelliptic curves.

Another benefit of twists, as explained in Section 4.7, is that curves with a twist of degree  $d$  allow one to use the twisted versions of Ate-type pairings. This means one computes the Miller function  $f_{s,D_1}(D_2)$  for  $D_1 \in \mathbb{G}_1$  and the divisor  $D_2 = (u(x), v(x)) \in \mathbb{G}_2$  with  $u(x)$  defined over the subfield  $\mathbb{F}_{q^{k/(d,k)}}$ , as opposed to computing  $f_{s,D_2}(D_1)$ . Furthermore, the points of  $\mathbb{G}_2$  can be represented as points on the Jacobian of the twist  $C'$  which allows for faster computations in the group  $\mathbb{G}_2$ . The example of Zhang [74] uses a twist of degree 8; to our knowledge, pairings on curves with twists of degree 10 have not been implemented.

**6.7. Trace zero subvarieties.** For a hyperelliptic curve  $C$  of genus  $g$  defined over  $\mathbb{F}_q$ , a *trace zero subvariety* of  $C$  is a subgroup of the Jacobian of  $C$  whose construction is connected to the Weil restriction of scalars. The use of trace zero varieties for cryptographic applications was first suggested by Frey [23]. The trace zero subvariety of  $C$  over a field extension of degree  $\ell$  is a subgroup of  $\text{Jac}_C(\mathbb{F}_{q^\ell})$ , which is isomorphic to the quotient  $\text{Jac}_C(\mathbb{F}_{q^\ell})/\text{Jac}_C(\mathbb{F}_q)$ .

It can also be defined concretely as follows: Let  $\pi$  be the  $q^{\text{th}}$  power Frobenius. Let  $\ell$  be a prime and assume that  $\ell \nmid \#\text{Jac}_C(\mathbb{F}_q)$ . We define the trace zero subvariety  $G_\ell$  of  $\text{Jac}_C(\mathbb{F}_{q^\ell})$  to be the set of elements of trace zero. I.e.,

$$G_\ell(\mathbb{F}_q) := \{D \in \text{Jac}_C(\mathbb{F}_{q^\ell}) : D + \pi(D) + \cdots + \pi^{\ell-1}(D) = \mathcal{O}\}.$$

Since  $G_\ell(\mathbb{F}_q)$  is the kernel of the trace map, it is a subgroup of  $\text{Jac}_C(\mathbb{F}_{q^\ell})$ . To perform arithmetic in a trace zero subvariety one can use the algorithms that work in the whole Jacobian. So far, no specific algorithms for the group law are known that make use of the subgroup properties.

Since  $G_\ell(\mathbb{F}_q)$  is a subgroup of  $\text{Jac}_C(\mathbb{F}_{q^\ell})$ , we can define a Tate-Lichtenbaum pairing on it by restriction: suppose the order of  $G_\ell(\mathbb{F}_q)$  is divisible by a large prime factor  $r$ , but not by  $r^2$ . Let  $\mathbb{G}_1 := G_\ell[r] \cap \ker(\pi^\ell - [1])$  and  $\mathbb{G}_2 := G_\ell[r] \cap \ker(\pi^\ell - [q^\ell])$ . Then the Tate-Lichtenbaum pairing on  $G_\ell$  is a map

$$t : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mu_r.$$

On the points of  $\mathbb{G}_1$ ,  $\pi$  acts as multiplication by an integer  $s$  ([13]), and the same is true for the action of  $\pi$  on  $\mathbb{G}_2$  ([9, Proposition 3]). Cesena [9] gives a new algorithm for computing the Tate-Lichtenbaum pairing over trace zero subvarieties of supersingular elliptic curves by exploiting the action of the  $q$ -Frobenius. He uses the fact that the  $q$ -Frobenius  $\pi$  is an efficient endomorphism (rather than just the  $q^r$ -Frobenius), together with the fact that for particular supersingular elliptic curves the action of the Frobenius can be computed more efficiently [9, Lemmas 1–3]. For these curves, the action of  $\pi$  is (close to being) multiplication of a power of  $q$ .

Experimentally, Cesena's algorithm is as efficient as the Tate-Lichtenbaum pairing on supersingular elliptic curves, though less efficient than the eta pairing  $\eta_T$  or the optimal Ate pairing of Vercauteren. It remains to explore whether Cesena's algorithm generalizes to supersingular hyperelliptic curves or non-supersingular trace zero varieties.

**6.8. Exploiting torsion groups of dimension  $> 2$ .** If  $r$  is coprime with the characteristic of  $\mathbb{F}_q$ , the  $r$ -torsion group of a Jacobian variety of dimension  $g$  is isomorphic to  $(\mathbb{Z}/r\mathbb{Z})^{2g}$ . With the exception of the recent work by Okamoto and Takashima [63], all known pairing-based cryptographic applications require only two linearly independent torsion points and thus can be realized in the elliptic curve setting; in fact, also the Okamoto-Takashima protocols can as well be implemented using a product of two (supersingular) elliptic curves. It is an open problem to find a cryptographic application that uses curves of genus 2 (or larger) and that does *not* work using elliptic curves. Both for the ordinary and the supersingular case, constructions of Jacobians of dimension 2 with low *full* embedding degree (cf. Section 3.3) are available ([18, 63]).

**6.9. More Problems.** For completeness, we include the problems posed by Galbraith, Hess and Vercauteren [29], making note of any recent advancements:

- (1) *Construct pairing-friendly ordinary hyperelliptic curves with smaller  $\rho$ -values.* At this point in time, the smallest  $\rho$ -value obtained for an ordinary hyperelliptic curve of small embedding degree is  $\rho \approx 20/9$  (for  $g = 2$ ,  $k = 27$ ; cf. Section 3). It is highly desirable to have curves with  $\rho$ -value  $< 2$ .

- (2) *Curves with  $g \geq 3$ .* For curves with  $g \geq 3$ , is it possible to develop efficient pairing-based cryptosystems which are also secure against the index calculus attacks available for these curves?
- (3) *Pairings on real models of hyperelliptic curves.* There have been recent examples [31] of efficient pairing computations on real models of hyperelliptic curves, as remarked in Section 5.6. Are real models competitive with the imaginary models in general? Furthermore, are there efficient pairings on non-hyperelliptic curves?
- (4) *Torsion structure.* Is there an efficient method for selecting divisors from  $\text{Jac}_C(\mathbb{F}_{q^k})[r]$  for pairing computations? (See also Section 6.4.) Furthermore, if this group has more than two generators, what cryptographic applications are possible? (See also Section 6.8.)
- (5) *Rubin-Silverberg point compression and Weil restriction.* Can the Rubin-Silverberg method (see Section 5.5) be made more efficient in the elliptic curve case and/or generalized to Jacobians of curves of genus  $g \geq 2$ ?
- (6) *Weil restriction.* As in Rubin-Silverberg point compression, certain abelian varieties can be identified with subvarieties of the Weil restriction of supersingular elliptic curves. When the abelian variety is a Jacobian, are there explicitly computable homomorphisms between the elliptic curve and the Jacobian representation?

**Acknowledgments.** The authors are most grateful to David Freeman for his elaborate feedback on earlier versions of this paper, which significantly improved our work. The authors further thank Paulo S.L.M. Barreto, Anja Becker, Felix Fontein, Steven Galbraith, and Alfred Menezes for helpful discussions and comments on an earlier draft of the paper. Thanks to Alan Silverster for conscientious technical editing. Thanks to Jonathan Wise. The work of the first author has been supported by a National Science Foundation Graduate Research Fellowship. The third author has been supported by the Informatics Circle of Research Excellence Chair in Algorithmic Number Theory and Cryptography. The fourth author is partially supported by National Science Foundation grant DMS-0801123 and a Sloan Research Fellowship. The work of the fifth author has been supported by a National Science Foundation Fellowship (#0802915) and a National Science and Engineering Research Council Fellowship (#373333). The fifth author is also grateful to Harvard University and the Pacific Institute for the Mathematical Sciences UBC, where some of this work was conducted. Lastly, the sixth author acknowledges support by the National Science and Engineering Research Council of Canada, and by the Premier’s Research Excellence Award of the province of Ontario.

The idea for this paper was conceived during the workshop “Women in Numbers” at the Banff International Research Station in November 2008, where the authors formed a project group studying hyperelliptic pairings.

## REFERENCES

1. R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, Journal of Cryptology **11** (1998), no. 2, 141–145.
2. P.S.L.M. Barreto, S. Galbraith, C. Ó hÉigearthaigh, and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, Designs, Codes and Cryptography **42** (2007), 239–271.
3. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM Journal on Computing **32** (2003), no. 3, 586–615.
4. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Journal of Cryptology **17** (2004), no. 4, 297–319.
5. F. Brezing and A. Weng, *Elliptic curves suitable for pairing based cryptography*, Designs, Codes and Cryptography **37** (2005), 133–141.
6. D. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Mathematics of Computation **48** (1987), no. 177, 95–101.

7. G. Cardona, *On the number of curves of genus 2 over a finite field*, Finite Fields and Their Applications **9** (2003), no. 4, 505–526.
8. G. Cardona, E. Nart, and J. Pujolàs, *Curves of genus two over fields of even characteristic*, Mathematische Zeitschrift **250** (2005), no. 1, 177–201.
9. E. Cesena, *Pairing with supersingular trace zero varieties revisited*, Cryptology ePrint Archive Report 2008/404, <http://eprint.iacr.org/2008/404/>.
10. Y.-J. Choie and E. Lee, *Implementation of Tate pairing on hyperelliptic curves of genus 2*, ICISC 2003, LNCS, vol. 2971, Springer-Verlag, 2004, pp. 97–111.
11. C. Cocks and R.G.E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, unpublished manuscript, 2001.
12. D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic two*, IEEE Transactions on Information Theory **30** (1984), 587–594.
13. D. Doche and T. Lange, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, ch. 15 (Arithmetic of special curves), Chapman & Hall/CRC, 2006.
14. I. Duursma and H.-S. Lee, *Tate pairing implementation for hyperelliptic curves  $y^2 = x^p - x + d$* , Advances in Cryptology - Asiacrypt 2003, LNCS, vol. 2894, Springer-Verlag, 2003, pp. 111–123.
15. K. Eisenträger, K. Lauter, and P. Montgomery, *Improved Weil and Tate pairings for elliptic and hyperelliptic curves*, Algorithmic Number Theory ANTS-VI, LNCS, vol. 3076, Springer-Verlag, 2004, pp. 169–183.
16. X. Fan, G. Gong, and D. Jao, *Speeding up pairing computations on genus 2 hyperelliptic curves with efficiently computable automorphisms*, Pairing 2008, LNCS, vol. 5209, Springer-Verlag, 2008, pp. 243–264.
17. D. Freeman, *A generalized Brezing-Weng method for constructing pairing-friendly ordinary abelian varieties: Additional examples*, <http://theory.stanford.edu/~dfreeman/papers/gen-bw-examples.pdf>.
18. ———, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*, Pairing 2007, LNCS, vol. 4575, Springer-Verlag, 2007, pp. 152–176.
19. ———, *A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties*, Pairing 2008, LNCS, vol. 5209, Springer-Verlag, 2008, pp. 146–163.
20. D. Freeman and T. Satoh, *Constructing pairing-friendly hyperelliptic curves using Weil restriction*, Preprint August 2009, 28 pages.
21. D. Freeman, M. Scott, and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, Journal of Cryptology, published online June 18, 2009. DOI: 10.1007/s00145-009-9048-z (to appear in print).
22. D. Freeman, P. Steinhagen, and M. Streng, *Abelian varieties with prescribed embedding degree*, Algorithmic Number Theory ANTS-VIII, LNCS, vol. 5011, Springer-Verlag, 2008, pp. 60–73.
23. G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, Finite Fields and Applications – Proceedings of the Fifth International Conference on Finite Fields and Applications  $F_4^5$ , Augsburg, August 2-6, 1999, Springer, 2001, pp. 128–161.
24. G. Frey and T. Lange, *Fast bilinear maps from the Tate-Lichtenbaum pairing on hyperelliptic curves*, Algorithmic Number Theory ANTS-VII, LNCS, vol. 4076, Springer-Verlag, 2006, pp. 466–479.
25. ———, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, ch. 23 (Algebraic realizations of DL systems), Chapman & Hall/CRC, 2006.
26. ———, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, ch. 4 (Background on curves and Jacobians), Chapman & Hall/CRC, 2006.
27. ———, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, ch. 5 (Varieties over special fields), Chapman & Hall/CRC, 2006.
28. S. Galbraith, *Supersingular curves in cryptography*, Advances in Cryptology – ASIACRYPT 2001, LNCS, vol. 2248, Springer-Verlag, 2001, pp. 495–513.
29. S. Galbraith, F. Hess, and F. Vercauteren, *Hyperelliptic pairings*, Pairing 2007, LNCS, vol. 4575, Springer-Verlag, 2007, pp. 108–131.
30. S. Galbraith and X. Lin, *Computing pairings using  $x$ -coordinates only*, Designs, Codes and Cryptography **50** (2009), 305–324.
31. S. Galbraith, X. Lin, and D. Mireles Morales, *Pairings on hyperelliptic curves with a real model*, Pairing 2008, LNCS, vol. 5209, Springer-Verlag, 2008, pp. 265–281.
32. S. Galbraith, J. McKee, and P. Valença, *Ordinary abelian varieties having small embedding degree*, Proc. Workshop on Mathematical Problems and Techniques in Cryptology, CRM, Barcelona, 2005, pp. 29–45.
33. S. Galbraith, J. Pujolàs, C. Ritzenthaler, and B. Smith, *Distortion maps for genus two curves*, Journal of Mathematical Cryptology **3** (2009), 1–18.
34. S. Galbraith and M. Scott, *Exponentiation in pairing-friendly groups using homomorphisms*, Pairing 2008, LNCS, vol. 5209, Springer-Verlag, 2008, pp. 211–224.

35. P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Mathematics of Computation **76** (2007), 475–492.
36. R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren, *Ate pairing on hyperelliptic curves*, Advances in Cryptology - Eurocrypt 2007, LNCS, vol. 4515, Springer-Verlag, 2007, pp. 419–436.
37. R. Granger, D. Page, and N. P. Smart, *High security pairing-based cryptography revisited*, Algorithmic Number Theory ANTS-VII, LNCS, vol. 4076, Springer-Verlag, 2006, pp. 480–494.
38. R. Granger, D. Page, and M. Stam, *On small characteristic algebraic tori in pairing-based cryptography*, LMS Journal of Computation and Mathematics **9** (2006), 64–85.
39. C. Ó hÉigartaigh and M. Scott, *Pairing calculation on supersingular genus 2 curves*, Selected Areas in Cryptography - SAC 2006, LNCS, vol. 4356, Springer-Verlag, 2007, pp. 302–316.
40. F. Hess, *Pairing lattices*, Pairing 2008, LNCS, vol. 5209, Springer-Verlag, 2008, pp. 18–38.
41. F. Hess, N. Smart, and F. Vercauteren, *The Eta pairing revisited*, IEEE Trans. Information Theory **52** (2006), 4595–4602.
42. L. Hitt, *On the minimal embedding field*, Pairing 2007, LNCS, vol. 4575, Springer-Verlag, 2007, pp. 294–301.
43. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Journal of Cryptology **17** (2004), no. 4, 263–276.
44. M. Katagi, I. Kitamura, T. Akishita, and T. Takagi, *Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors*, WISA 2004, LNCS, vol. 3325, Springer-Verlag, 2005, pp. 345–359.
45. M. Kawazoe and T. Takahashi, *Pairing-friendly hyperelliptic curves of type  $y^2 = x^5 + ax$* , Pairing 2008, LNCS, vol. 5209, Springer-Verlag, 2008, pp. 164–177.
46. D. Knuth, *The Art of Computer Programming*, 3rd ed., vol. 2, Addison-Wesley, 1997.
47. N. Koblitz, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), no. 3, 139–150.
48. N. Koblitz and A. Menezes, *Pairing-based cryptography at high security levels*, Cryptography and Coding 2005, LNCS, vol. 3796, Springer-Verlag, 2005, pp. 13–36.
49. D. Kohel, *Quartic CM fields database*, <http://echidna.maths.usyd.edu.au/kohel/dbs/complex-multiplication2.html>.
50. T. Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Applicable Algebra in Engineering, Communication and Computing **15** (2005), 295–328.
51. K. Lauter, *The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves*, Topics in Algebraic and Noncommutative Geometry, Contemporary Mathematics, vol. 324, American Mathematical Society, 2003, pp. 165–171.
52. E. Lee, H.-S. Lee, and Y. Lee, *Eta pairing computation on general divisors over hyperelliptic curves  $y^2 = x^p - x + d$* , Journal of Symbolic Computation **43** (2008), 452–474.
53. E. Lee, H.-S. Lee, and C.-M. Park, *Efficient and generalized pairing computations on abelian varieties*, IEEE Transactions on Information Theory **55** (2009), 1793–1803.
54. E. Lee and Y. Lee, *Tate pairing computation on the divisors of hyperelliptic curves of genus 2*, J. Korean Math. Soc. **45** (2008), no. 4, 1057–1073.
55. A. K. Lenstra, *Unbelievable security. Matching AES security using public key cryptosystems*, Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, Springer-Verlag, 2001, pp. 67–86.
56. R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, 1997.
57. F. Luca, D. J. Mireles, and I. E. Shparlinski, *MOV attack in various subgroups on elliptic curves*, Illinois J. Math. **48** (2004), 1041–1052.
58. V. Miller, *The Weil pairing and its efficient calculation*, Journal of Cryptology **17** (2004), 235–261.
59. D. Mumford, *Tata Lectures on Theta I, II*, Birkhäuser, Boston, 1983/84.
60. M. Naehrig, P. Barreto, and P. Schwabe, *On compressible pairings and their computation*, AFRICACRYPT 2008, LNCS, vol. 5023, Springer-Verlag, 2008, pp. 371–388.
61. NIST, *Recommendation for key management - Part 1: General (revised)*, NIST Special Publication 800-57, May 2006, <http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf>.
62. A. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, Advances in Cryptology - Eurocrypt 1984, LNCS, vol. 209, Springer-Verlag, 1985, pp. 224–314.
63. T. Okamoto and K. Takashima, *Homomorphic encryption and signatures from vector decomposition*, Pairing 2008, LNCS, vol. 5209, Springer-Verlag, 2008, pp. 57–74.
64. K. Paterson, *Advances in Elliptic Curve Cryptography*, ch. X (Cryptography from pairings), Cambridge University Press, 2005.
65. J. M. Pollard, *Monte Carlo methods for index computation (mod  $p$ )*, Mathematics of Computation **32** (1978), no. 143, 918–924.
66. K. Rubin and A. Silverberg, *Supersingular abelian varieties in cryptology*, Advances in Cryptology - CRYPTO 2002, LNCS, vol. 2442, Springer-Verlag, 2002, pp. 336–353.

67. T. Satoh, *The Brezing-Weng-Freeman method for certain genus 2 hyperelliptic curves*, Advances in Cryptology – Eurocrypt 2009, LNCS, vol. 5479, Springer-Verlag, 2009, pp. 536–553.
68. M. Scott, *Implementing cryptographic pairings*, Pairing 2007, LNCS, vol. 4575, Springer-Verlag, 2007, pp. 177–196.
69. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.
70. P. C. van Oorschot and M. J. Wiener, *Parallel collision search with cryptanalytic applications*, Journal of Cryptology **12** (1999), 1–28.
71. F. Vercauteren, *Optimal pairings*, Cryptology ePrint Archive Report 2008/096, <http://eprint.iacr.org/2008/096/>.
72. A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Mathematics of Computation **72** (2003), 435–458.
73. T. Wollinger, J. Pelzl, and C. Paar, *Cantor versus Harley: Optimization and analysis of explicit formulae for hyperelliptic curve cryptosystem*, IEEE Transactions on Computers **54** (2005), 861–872.
74. F. Zhang, *Twisted Ate pairing on hyperelliptic curves and applications*, Cryptology ePrint Archive Report 2008/274, <http://eprint.iacr.org/2008/274/>.
75. C. Zhao, C. Zhang, and J. Huang, *All pairings are in a group*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E91-A** (2008), 3084–3087.
76. ———, *A note on the Ate pairing*, International Journal of Information Security **7** (2008), 379–382.

DEPT. OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139

*E-mail address:* [jen@math.mit.edu](mailto:jen@math.mit.edu)

DEPT. OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138

*E-mail address:* [jbelding@math.harvard.edu](mailto:jbelding@math.harvard.edu)

DEPT. OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CALGARY, CALGARY, ALBERTA, CANADA T2N 1N4

*E-mail address:* [chisholm@math.ucalgary.ca](mailto:chisholm@math.ucalgary.ca)

DEPT. OF MATHEMATICS, THE PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802

*E-mail address:* [eisentra@math.psu.edu](mailto:eisentra@math.psu.edu)

DEPT. OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, BRITISH COLUMBIA, CANADA V5A 1S6

*E-mail address:* [kestange@sfu.ca](mailto:kestange@sfu.ca)

DEPT. OF COMBINATORICS AND OPTIMIZATION, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA N2L 3G1

*E-mail address:* [eteske@uwaterloo.ca](mailto:eteske@uwaterloo.ca)