

Ordinary Pairing-Friendly Genus 2 Hyperelliptic Curves with Absolutely Simple Jacobians

Georgios Fotiadis and Elisavet Konstantinou

Dept. of Information & Communication Systems Engineering
UNIVERSITY OF THE AEGEAN
Karlovassi, Samos 83200, GR
{gfotiadis,ekonstantinou}@aegean.gr

Abstract

We present a method for producing pairing-friendly, simple, ordinary Jacobian varieties of genus 2 hyperelliptic curves defined over a prime field \mathbb{F}_p . The proposed method heavily relies on the construction of a suitable p -Weil number and a corresponding quartic CM-field. Our Jacobians are absolutely simple and for this special class of Jacobians we give the first examples in the literature with ρ -values below 4, while previous results had in general ρ -values between 6 and 8. These examples derive from “families” of pairing-friendly Jacobians, which are basically polynomial representations of the Jacobian parameters.

Keywords: Pairing, hyperelliptic curves, Jacobian, embedding degree.

1 Introduction

An *asymmetric pairing* is a bilinear, non-degenerate, efficiently computable map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are cyclic groups of prime order r with $\mathbb{G}_1 \neq \mathbb{G}_2$. A crucial cryptographic requirement is that the discrete logarithm problem (DLP) is computationally infeasible in all *pairing groups* $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$. We call $\mathbb{G}_1, \mathbb{G}_2$ the *source groups* and \mathbb{G}_T the *target group*. Initially the source groups were set as r -order subgroups of ordinary elliptic curves over a finite field, while the target group was an r -order subgroup of a finite field.

Since elliptic curves are genus 1 algebraic curves, an obvious question is whether pairings on higher genus curves can be also used in implementations. In this case \mathbb{G}_1 and \mathbb{G}_2 consist of elements in the Jacobian variety of a genus g hyperelliptic curve defined over a finite field. By [Ber06, Lan06], this can be an advantageous choice especially when $g = 2$, since genus 2 curves and their Jacobians:

1. are competitive to elliptic curves in performance and security [Ber06, Lan06].
2. result in efficient Tate pairing calculations [FL06].
3. have efficient CM-constructions [LS13, Wen02] and point operations [Can87].
4. have points with smaller size.

This is our motivation for constructing “pairing-friendly”, ordinary Jacobians of genus 2 hyperelliptic curves over a prime field \mathbb{F}_p , called the *base field*.

An affine genus 2 hyperelliptic curve C over \mathbb{F}_p is defined by the equation $C/\mathbb{F}_p : y^2 = F(x)$, where $F(x) \in \mathbb{F}_p[x]$ is monic with $\deg F \in \{5, 6\}$. For any extension \mathbb{k} of \mathbb{F}_p , we denote by $C(\mathbb{k})$ the set of all points with coordinates in \mathbb{k} satisfying the hyperelliptic curve equation. Unlike the genus 1 case this set is not a group and hence we cannot define DLP-based protocols on $C(\mathbb{k})$. However, to each such curve we associate a special object called the Jacobian [Kob89]

of C/\mathbb{F}_p , denoted by $J(\mathbb{F}_p)$. This is a 2-dimensional abelian variety, hence an algebraic group, with order $\#J(\mathbb{F}_p) \approx p^2$. The elements of $J(\mathbb{F}_p)$ are equivalence classes of zero degree divisors, defined over \mathbb{F}_p , under the linear equivalence of divisors (see Section 2). This can be generalized to any extension \mathbb{k} of \mathbb{F}_p . In our context we assume that $J(\mathbb{F}_p)$ contains a cyclic subgroup of prime order r and that it is ordinary, simple and absolutely simple [Mil08] (see also Section 2).

For asymmetric pairings on Jacobians, the source groups are distinct r -order subgroups of $J(\mathbb{F}_{p^k})$ and the target group is an r -order subgroup of the multiplicative group of the extension field \mathbb{F}_{p^k} . In other words a pairing maps two divisors of order r , defined over \mathbb{F}_{p^k} , to an r th root of unity. This positive integer k is called the *embedding degree of $J(\mathbb{F}_p)$ with respect to r* and it is the smallest positive integer such that \mathbb{F}_{p^k} contains all r th roots of unity. In pairing-based applications such Jacobians are chosen according to the following rules:

1. The order of the Jacobian has a large prime factor r , i.e. $\#J(\mathbb{F}_p) = hr$, for $h \geq 1$. This ensures that $J(\mathbb{F}_p)$ (hence $J(\mathbb{F}_{p^k})$) contains points of order r .
2. The prime r is large enough, so that the DLP in $\mathbb{G}_1, \mathbb{G}_2$ is computationally hard. According to today's requirements, r should be at least 256 bit large, to avoid Pollard's rho attack, with running time $O(\sqrt{r})$.
3. The embedding degree k is large enough, so that the DLP in $\mathbb{G}_T \subset \mathbb{F}_{p^k}^*$ is as hard as in $\mathbb{G}_1, \mathbb{G}_2$. In practice \mathbb{F}_{p^k} must be resistant to the variants of the number field sieve (NFS) attack [EMJ17, KJ17, KB16].
4. k is relatively small, for efficient operations in \mathbb{G}_T . This means that the extension field must be as large as to ensure security and no larger.
5. The ρ -value $\rho = 2 \log p / \log r$ of the Jacobian is close to 1. This saves bandwidth by keeping the representation of Jacobian elements small. Examples with $\rho \approx 1$ are still absent for ordinary, absolutely simple Jacobians.

Hyperelliptic curves and the corresponding Jacobians satisfying these properties are called *pairing-friendly*.

We describe a method for producing pairing-friendly ordinary Jacobians of genus 2 hyperelliptic curves defined over prime fields. We present new examples of absolutely simple Jacobians, with the best reported ρ -values so far in the literature, for various embedding degrees. Particularly, our examples reduce the ρ -value to be up to 4, while previous results for the same embedding degrees have in general ρ -values between 6 and 8 [Fre08], or around 8 [LS13].

In Section 2 we present the necessary background for pairing-friendly 2-dimensional Jacobians and a summary of methods for their construction. We analyze our proposal and demonstrate our recommendations in Section 3. Numerical results of cryptographic value are provided in Section 4 and we conclude the paper in Section 5, summarizing our recommendations.

2 Background

Genus 2 Hyperelliptic Curves and Jacobians. Let C be a genus 2 hyperelliptic curve over a prime field \mathbb{F}_p and $C(\mathbb{k})$ the set of points on the curve with coordinates in an extension \mathbb{k} of \mathbb{F}_p . Since $C(\mathbb{k})$ is not a group, in hyperelliptic curve cryptography we are working with the Jacobian $J(\mathbb{F}_p)$ of C/\mathbb{F}_p [Kob89], which is a 2-dimensional abelian variety and hence an algebraic group [Mil08]. It is also a quotient group, whose elements are equivalence classes of zero degree divisors under the linear equivalence of divisors. In particular, two zero degree divisors are linearly equivalent, if their difference is a principal divisor, i.e. a divisor of a rational function in the function field of the curve C/\mathbb{F}_p [Mil08, OdJ08]. In dimension 2, each equivalence class consists of exactly two elements.

In this paper we are working with *simple* Jacobians which are also *absolutely simple*. A 2-dimensional Jacobian is simple if it does not split over \mathbb{F}_p to a product of elliptic curve groups

and it is absolutely simple, if it remains simple over $\overline{\mathbb{F}}_p$ [Mil08]. We denote by $\text{End}(J(\mathbb{F}_p))$ the *endomorphism ring* containing all homomorphisms from $J(\mathbb{F}_p)$ to itself. One of these elements is the *Frobenius endomorphism*, denoted by π , which acts by raising a divisor in $J(\mathbb{F}_p)$ to the p th power. When $J(\mathbb{F}_p)$ is simple, the Frobenius endomorphism satisfies a quartic, monic polynomial $P(x) \in \mathbb{Z}[x]$ called the *characteristic polynomial of Frobenius*:

$$P(x) = \prod_{i=1}^4 [x - \sigma_i(\pi)] = x^4 + Ax^3 + Bx^2 + Ap x + p^2, \quad (2.1)$$

where σ_i are the embeddings of the number field $K = \mathbb{Q}(\pi)$ into \mathbb{C} . Thus, π is an algebraic integer and also a *p-Weil number*, meaning $\pi\bar{\pi} = p$, where $\bar{\pi}$ is the complex conjugate of π . In our case, $J(\mathbb{F}_p)$ will be ordinary and K a quartic *CM-field*, i.e. an imaginary quadratic extension of a totally real field [Mil08].

The order of the Jacobian and $P(x)$ are related by $\#J(\mathbb{F}_p) = P(1)$ [CFA⁺06]. Additionally, $J(\mathbb{F}_p)$ is ordinary if $\gcd(B, p) = 1$ [HZ02] and it is simple if $P(x)$ is irreducible over $\mathbb{Z}[x]$ [OdJ08]. Finally, in order to check if $J(\mathbb{F}_p)$ is absolutely simple we use the next fact [HZ02].

Proposition 2.1. Let $J(\mathbb{F}_p)$ be a 2-dimensional Jacobian, with characteristic polynomial of Equation (2.1). Then exactly one of the following holds: (1) $J(\mathbb{F}_p)$ is absolutely simple. (2) $A = 0$. (3) $A^2 = p + B$. (4) $A^2 = 2B$. (5) $A^2 = 3B - 3p$. In cases (2), (3), (4) and (5), the smallest extension of \mathbb{F}_p over which $J(\mathbb{F}_p)$ splits, is quadratic, cubic, quartic and sextic respectively.

Proof. See Theorem 6, p. 145 in [HZ02]. □

Pairing-Friendly Conditions. Recall that for asymmetric pairings on Jacobians, $\mathbb{G}_1, \mathbb{G}_2$ are distinct subgroups of $J(\mathbb{F}_{p^k})$, while \mathbb{G}_T is an r -order subgroup of the multiplicative group of \mathbb{F}_{p^k} , where k is the embedding degree. This is the smallest positive integer such that \mathbb{F}_{p^k} contains the group μ_r of r th roots of unity. Equivalently, it is the smallest positive integer, such that $r \mid (p^k - 1)$ [Fre08].

Freeman et al. [FSS08] described the conditions for g -dimensional Jacobians to have embedding degree k . Here we are restricted to $g = 2$.

Proposition 2.2. Let $J(\mathbb{F}_p)$ be an ordinary 2-dimensional Jacobian with Frobenius endomorphism π and characteristic polynomial of Frobenius $P(x) \in \mathbb{Z}[x]$. Let k be a positive integer and $\Phi_k(x)$ the k th cyclotomic polynomial and suppose that $\gcd(r, p) = 1$ and $K = \mathbb{Q}(\pi)$ is a quartic CM-field. If

$$\#J(\mathbb{F}_q) = P(1) \equiv 0 \pmod{r} \quad \text{and} \quad \Phi_k(p) \equiv 0 \pmod{r}, \quad (2.2)$$

then $J(\mathbb{F}_p)$ has embedding degree k with respect to r .

Proof. See Proposition 2.1 in [FSS08]. □

Thus, in order to construct ordinary and simple 2-dimensional Jacobians over \mathbb{F}_p with embedding degree k and an r -order subgroup, it suffices to search for a Frobenius endomorphism $\pi \in \text{End}(J(\mathbb{F}_p))$ and a quartic CM-field $K = \mathbb{Q}(\pi)$, such that System (2.2) is satisfied. Note that the second equation in System (2.2) implies that p is a primitive k th root of unity in $(\mathbb{Z}/r\mathbb{Z})^*$.

As stated in Section 1, r must be a large prime so that the DLP in the r -order subgroups $\mathbb{G}_1, \mathbb{G}_2 \subseteq J(\mathbb{F}_{p^k})$ is computationally hard and the embedding degree k must be large enough so that the DLP in $\mathbb{G}_T \subseteq \mathbb{F}_{p^k}^*$ is approximately of the same difficulty as in $\mathbb{G}_1, \mathbb{G}_2$. Note that k should be the smallest such integer, since the extension field \mathbb{F}_{p^k} must not be unnecessarily

large. The ideal case appears when $\#J(\mathbb{F}_p)$ and r have approximately the same size. Since $\#J(\mathbb{F}_p) \approx p^2$, this means that the ρ -value $\rho = 2 \log p / \log r$ must be close to 1 [FSS08]. The recommended sizes of Jacobian parameters and the security levels that they provide are discussed in Section 4 (see also [BBC⁺09]). The simple and ordinary Jacobians having the properties we studied in this paragraph are called *pairing-friendly* [Fre08].

Parametric Families. The most common way to produce pairing-friendly Jacobians is to represent its parameters as polynomials, which when evaluated at certain integers will produce the actual Jacobian parameters. This idea was first introduced by Brezing and Weng [BW05] for elliptic curves and generalized by David Freeman [Fre08] for higher dimensional abelian varieties. In this case the Frobenius endomorphism is represented by a polynomial $\pi(x) \in K[x]$ with characteristic polynomial of Frobenius $P(t) \in \mathbb{Q}[t]$:

$$P(t) = \prod_{i=1}^4 [t - \sigma_i(\pi(x))] = t^4 + A(x)t^3 + B(x)t^2 + A(x)pt + p^2, \quad (2.3)$$

for the four embeddings $\sigma_i : K \rightarrow \mathbb{C}$ and some $A(x), B(x) \in \mathbb{Z}[x]$. Such a polynomial representation allows us to work with *polynomial families of pairing-friendly Jacobians*. The precise definition is the following [Fre08].

Definition 2.3. Let K be a quartic CM-field, $\pi(x) \in K[x]$ and $r(x) \in \mathbb{Q}[x]$. The pair $[\pi(x), r(x)]$ parametrizes a family of pairing-friendly Jacobians with embedding degree k , if the following conditions are satisfied:

1. $p(x) = \pi(x)\bar{\pi}(x) \in \mathbb{Q}[x]$ and $p(x)$ represents primes.
2. $r(x)$ is non-constant, irreducible, integer-valued, with $\text{lc}(r) > 0$.
3. $P(1) \equiv 0 \pmod{r(x)}$.
4. $\Phi_k(p(x)) \equiv 0 \pmod{r(x)}$, where $\Phi_k(x)$ is the k th cyclotomic polynomial.

By saying that $p(x)$ represents primes we mean that it is non-constant, irreducible, with $\text{lc}(p) > 0$ and it returns primes for finitely (or infinitely) many $x \in \mathbb{Z}$ [Fre08]. Condition (3) ensures that the Jacobian order factorizes as $\#J(\mathbb{F}_p) = h(x)r(x)$, for some $h(x) \in \mathbb{Q}[x]$, while condition (4) implies that $p(x)$ is a primitive k th root of unity in $\mathbb{Q}[x]/\langle r(x) \rangle$. Although $r(x)$ can be chosen as any polynomial with rational coefficients satisfying condition (2) of Definition 2.3, it is usually considered as the k th cyclotomic polynomial. Finally, the ρ -value of a polynomial family $[\pi(x), r(x)]$ is defined as the ratio:

$$\rho(\pi, r) = \lim_{x \rightarrow \infty} \frac{2 \log p(x)}{\log r(x)} = \frac{2 \deg p}{\deg r}.$$

Previous Constructions. Methods for constructing absolutely simple Jacobians are given in [Fre08, FSS08, LS13], with ρ -value in the range $6 \leq \rho \leq 8$. However better ρ -values can be achieved by non-absolutely simple Jacobians. For example see [Dry12, FS11, GV12, Kac10, KT08], with generic $\rho \leq 4$, where the best results appear in [Dry12], with $2 \leq \rho < 4$. Unfortunately there are still no examples with $\rho < 2$ for simple, ordinary Jacobians. All methods in [Dry12, Fre08, FS11, GV12, Kac10, KT08] use polynomial families of pairing-friendly Jacobians. An alternative approach is presented by Lauter–Shang in [LS13]. Representing the Frobenius element $\pi \in K$ in an appropriate form, they derive a system of three equations in four variables, whose solutions lead to few examples of absolutely simple Jacobians with $\rho \approx 8$.

Contribution. In this paper we focus on pairing-friendly 2-dimensional, absolutely simple and ordinary Jacobians. Their construction depends mainly on the choice of the quartic CM-field K and the representation of the Frobenius endomorphism π . We present a procedure for constructing polynomial families of pairing-friendly Jacobians based on Lauter-Shang’s [LS13], Dryło’s [Dry12] and new polynomial representations of the Frobenius endomorphism. In each case the problem of constructing the families is reduced to a system of three equations in four variables. By their solutions we produced polynomial families of 2-dimensional, absolutely simple Jacobians with the best ρ -values so far in the literature. In particular our families have in general $\rho(\pi, r) \leq 4$ for various embedding degrees, while previous results had $\rho(\pi, r)$ between 6 and 8. Using our families we produced various numerical examples of cryptographic value.

3 Constructing Pairing-Friendly Jacobians

Let C/\mathbb{F}_p be a genus 2 hyperelliptic curve for some prime p , with a simple and ordinary Jacobian $J(\mathbb{F}_p)$ and suppose that $\#J(\mathbb{F}_p) = hr$, for some prime r , with $\gcd(r, p) = 1$ and $h > 0$. Let also k be a positive integer and K a quartic CM-field. We can determine suitable parameters of a 2-dimensional Jacobian by searching for a Frobenius element $\pi \in K$, such that System (2.2) is satisfied:

$$P(1) \equiv 0 \pmod{r} \quad \text{and} \quad \Phi_k(p) \equiv 0 \pmod{r} \iff p = \pi\bar{\pi} \equiv \zeta_k \pmod{r}, \quad (3.1)$$

where $P(x) \in \mathbb{Z}[x]$ is the characteristic polynomial of Frobenius given by Equation (2.1) and ζ_k a primitive k th root of unity.

Since we will be working with polynomial families we need to transfer the above situation in terms of polynomial representations. This means that the Frobenius endomorphism is a polynomial $\pi(x) \in K[x]$, with characteristic polynomial of Frobenius $P(t) \in \mathbb{Z}[t]$ given by Equation (2.3). The complete process for constructing polynomial families of pairing-friendly, 2-dimensional Jacobians is described in Algorithm 1. We first fix an integer $k > 0$, a quartic

Algorithm 1 Constructing families of pairing-friendly 2-dimensional Jacobians.

Input: An integer $k > 0$, a quartic CM-field K , a number field L containing ζ_k, K .

Output: A polynomial family $[\pi(x), r(x)]$ of pairing-friendly, 2-dimensional Jacobian variety, with embedding degree k .

- 1: Find an $r(x) \in \mathbb{Q}[x]$ satisfying condition (2) of Definition 2.3, s.t. $L \cong \mathbb{Q}[x]/\langle r(x) \rangle$.
- 2: Let $u(x) \in \mathbb{Q}[x]$ be a primitive l th root of unity in $\mathbb{Q}[x]/\langle r(x) \rangle$.
- 3: For every $i = 1, \dots, \varphi(l) - 1$, such that $l/\gcd(i, l) = k$, do the following:
- 4: Find a polynomial $\pi(x) \in K[x]$, satisfying the following System:

$$\#J(\mathbb{F}_p) = P(1) \equiv 0 \pmod{r(x)} \quad \text{and} \quad p(x) = \pi(x)\bar{\pi}(x) \equiv u(x)^i \pmod{r(x)} \quad (3.2)$$

- 5: If $p(x) = \pi(x)\bar{\pi}(x)$ represents primes return the family $[\pi(x), r(x)]$.
-

CM-field K and set L as the number field containing ζ_k and K . Usually L is taken as the l th cyclotomic field $\mathbb{Q}(\zeta_l)$ for some $l \in \mathbb{Z}_{>0}$, such that $k \mid l$. In step 1, we construct the polynomial $r(x)$ such that it satisfies condition (2) of Definition 2.3. If $L = \mathbb{Q}(\zeta_l)$, then $r(x) = \Phi_l(x)$. With this choice we know that the polynomial $u(x) = x$ is a primitive l th root of unity in $\mathbb{Q}[x]/\langle r(x) \rangle$. Then the primitive k th roots of unity can be obtained by computing the powers $u(x)^i \pmod{r(x)}$, for every $i = 1, \dots, \varphi(l) - 1$, such that $l/\gcd(i, l) = k$. The fourth step is the most demanding since we are searching for the Frobenius polynomial $\pi(x) \in K[x]$, such that the family of Jacobians is pairing-friendly. To come to this conclusion we also need to verify

that the polynomial $p(x) = \pi(x)\bar{\pi}(x)$ represents primes (step 5). The output of Algorithm 1 is a polynomial family $[\pi(x), r(x)]$ of pairing-friendly 2-dimensional Jacobians with embedding degree k and ρ -value:

$$\rho(\pi, r) = \frac{2 \deg p}{\deg r} = \frac{2(\deg \pi + \deg \bar{\pi})}{\deg r} \leq \frac{2(2 \deg r - 2)}{\deg r} = 4 - \frac{4}{\deg r} < 4.$$

This is a significant improvement compared to [Fre08, FSS08, LS13], which for absolutely simple Jacobians have $6 \leq \rho(\pi, r) \leq 8$.

3.1 Lauter-Shang's Frobenius Elements

Lauter and Shang [LS13] considered quartic CM-fields $K = \mathbb{Q}(\eta)$, with positive and square-free discriminant Δ_K (primitive CM-fields), where η is:

$$\eta = \begin{cases} i\sqrt{a + b\sqrt{d}}, & \text{if } d \equiv 2, 3 \pmod{4} \\ i\sqrt{a + b\frac{-1 + \sqrt{d}}{2}}, & \text{if } d \equiv 1 \pmod{4} \end{cases} \quad (3.3)$$

for some $a, b, d \in \mathbb{Z}$, where d is positive and square-free. The Frobenius endomorphism π is an element of K and hence it is of the form:

$$\pi = X + Y\sqrt{d} + \eta(Z + W\sqrt{d}), \quad (3.4)$$

for $X, Y, Z, W \in \mathbb{Q}$ and since π is a p -Weil number, it must satisfy $\pi\bar{\pi} = p$, or:

$$(X^2 + dY^2 + \alpha(Z^2 + dW^2) + 2\beta dZW) + (2XY + 2\alpha ZW + \beta(Z^2 + dW^2))\sqrt{d} = p,$$

where $(\alpha, \beta) = (a, b)$, when $d \equiv 2, 3 \pmod{4}$ and $(\alpha, \beta) = ((2a - b)/2, b/2)$, when $d \equiv 1 \pmod{4}$. With this setting, the characteristic polynomial of Frobenius is:

$$P(x) = x^4 - 4Xx^3 + (2p + 4X^2 - 4dY^2)x^2 - 4Xpx + p^2.$$

By the first equation of System (3.2), the order of the Jacobian must be divisible by r . Combining the facts that p must be a prime integer, with $p \equiv \zeta_k \pmod{r}$ and $\#J(\mathbb{F}_p) = P(1)$, we are searching for solutions (X, Y, Z, W) of the system:

$$\left. \begin{aligned} X^2 + dY^2 + \alpha(Z^2 + dW^2) + 2\beta dZW &\equiv \zeta_k \pmod{r} \\ 2XY + 2\alpha ZW + \beta(Z^2 + dW^2) &= 0 \\ (\zeta_k + 1 - 2X)^2 - 4dY^2 &\equiv 0 \pmod{r} \end{aligned} \right\} \quad (3.5)$$

Remark 3.1. The first and third equation of System (3.5) are solved in $\mathbb{Z}/r\mathbb{Z}$ and the second in \mathbb{Q} . Such solutions are presented in [LS13], giving examples with $\rho \approx 8$. Alternatively, we can solve all equations modulo r and then search for lifts of X, Y, Z, W in \mathbb{Q} , such that the second equation is satisfied in \mathbb{Q} . \square

Since we are working with polynomial families, we transfer our analysis to $\mathbb{Q}[x]/\langle r(x) \rangle$, for an $r(x) \in \mathbb{Q}[x]$ satisfying condition (2) of Definition 2.3 and follow Algorithm 1. We first fix a number field $L = \mathbb{Q}(\zeta_l) \cong \mathbb{Q}[x]/\langle r(x) \rangle$ for $l \in \mathbb{Z}_{>0}$, such that $k \mid l$ and set $u(x), z(x), \eta(x)$ as the polynomials representing ζ_l, \sqrt{d}, η in $\mathbb{Q}[x]/\langle r(x) \rangle$ (see [MF05, SW06]). We set the Frobenius polynomial:

$$\pi(x) = X(x) + Y(x) + \eta(Z(x) + W(x)\sqrt{d}), \quad (3.6)$$

for some $X(x), Y(x), Z(x), W(x) \in \mathbb{Q}[x]/\langle r(x) \rangle$ and the characteristic polynomial of Frobenius is now expressed in $\mathbb{Q}[t]$, with coefficients in $\mathbb{Q}[x]$. In order to construct polynomial families of pairing-friendly Jacobians we work as follows. We first solve System (3.5) in $\mathbb{Z}/r\mathbb{Z}$ and obtain solutions $(X, Y, Z, W) \in \mathbb{Q}^4$. Then we represent these solutions as polynomials $[X'(x), Y'(x), Z'(x), W'(x)]$ in $\mathbb{Q}[x]/\langle r(x) \rangle$ and finally we take lifts $f_X(x), f_Y(x), f_Z(x), f_W(x) \in \mathbb{Q}[x]$, so that

$$2X(x)Y(x) + 2\alpha Z(x)W(x) + \beta [Z(x)^2 + dW(x)^2] = 0,$$

namely the second equation of System (3.5) is satisfied in $\mathbb{Q}[x]$, where:

$$\begin{aligned} X(x) &= f_X(x)r(x) + X'(x), & Y(x) &= f_Y(x)r(x) + Y'(x) \\ Z(x) &= f_Z(x)r(x) + Z'(x), & W(x) &= f_W(x)r(x) + W'(x) \end{aligned}$$

The field polynomial derives from $p(x) = \pi(x)\bar{\pi}(x)$ and it must represent primes, according to Definition 2.3. This is equivalent to finding $m, n \in \mathbb{Z}$, such that $p(mx + n) \in \mathbb{Z}[x]$ and contains no constant or polynomial factors.

Examples of Absolutely Simple Jacobians.

Let $K = \mathbb{Q}(\eta)$ be a primitive quartic CM-field and ζ_k a primitive k th root of unity. A solution of System (3.5) in $\mathbb{Z}/r\mathbb{Z}$ is represented by the quadruple:

$$(X, Y, Z, W) = \left(\frac{(\sqrt{\zeta_k} + 1)^2}{4}, \pm \frac{(\sqrt{\zeta_k} - 1)^2}{4\sqrt{d}}, \pm \frac{\zeta_k - 1}{4\eta}, \pm \frac{\zeta_k - 1}{4\eta\sqrt{d}} \right). \quad (3.7)$$

Below we give an example derived from the above solution, which first appeared in [Fre08]. Our method can be also extended for arbitrary polynomials $r(x)$ satisfying condition (2) of Definition 2.3.

Example 3.2. Set $l = k = 5$ and $K = \mathbb{Q}(i\sqrt{10 + 2\sqrt{5}})$. Take $L = \mathbb{Q}(\zeta_5)$ and $r(x) = \Phi_5(x)$, so that $u(x) = x$ is a primitive 5th root of unity in $\mathbb{Q}[x]/\langle r(x) \rangle$. The representation of $\sqrt{5}$ and η in $\mathbb{Q}[x]/\langle r(x) \rangle$ is:

$$z(x) = 2x^3 + 2x^2 + 1 \quad \text{and} \quad \eta(x) = -2x^3 + 2x^2.$$

For $i = 4$ in Algorithm 1, and for lifts $f_X(x) = 1/4$, $f_Y(x) = 1/20$, $f_Z(x) = 1/8$ and $f_W(x) = -1/40$, we get the following solution $[X(x), Y(x), Z(x), W(x)]$:

$$\begin{aligned} X(x) &= (x^4 + 2x^2 + 1)/4, & Y(x) &= (x^4 + 6x^3 + 6x^2 + 6x + 1)/20 \\ Z(x) &= (x^4 + x^3 + 2x^2 + x + 1)/8, & W(x) &= -(x^4 + 3x^3 + 2x^2 + 3x + 1)/40 \end{aligned}$$

By Equation (3.6) the Frobenius polynomial $\pi(x) \in K[x]$ is:

$$\pi(x) = X(x) + Y(x)\sqrt{5} + i\sqrt{10 + 2\sqrt{5}} \left(Z(x) + W(x)\sqrt{5} \right),$$

Setting the field polynomial as $p(x) = \pi(x)\bar{\pi}(x)$ we conclude to:

$$p(x) = \frac{1}{5}(x^8 + 2x^7 + 8x^6 + 9x^5 + 15x^4 + 9x^3 + 8x^2 + 2x + 1),$$

which is integer-valued for all $x \equiv 1 \pmod{5}$. The characteristic polynomial of Frobenius $P(t)$ has integer coefficients and it is irreducible over \mathbb{Z} . Additionally none of conditions (2)–(5) of Proposition 2.1 is satisfied and the middle coefficient $B(x)$ of $P(t)$ satisfies $\gcd[B(x), p(x)] = 1$. Thus the pair $[\pi(x), r(x)]$ represents a polynomial family of pairing-friendly, absolutely simple, ordinary, 2-dimensional Jacobian varieties with embedding degree $k = 5$ and $\rho(\pi, r) = 4$. \square

3.2 Generalized Dryło's Frobenius Elements

The following analysis is based on Dryło [Dry12]. Let $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, for a square-free $d > 0$ and some primitive s th root of unity ζ_s . For quartic CM-fields K there are two cases to consider:

1. If $\sqrt{-d} \notin \mathbb{Q}(\zeta_s)$, then $\varphi(s) = 2$ and so $s \in \{3, 4, 6\}$.
2. If $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$, then $\varphi(s) = 4$ and so $s \in \{5, 8, 10, 12\}$.

We take the Frobenius element $\pi \in K$ as a linear combination of ζ_s and $\sqrt{-d}$:

$$\pi = X + Y\sqrt{-d} + \zeta_s \left(Z + W\sqrt{-d} \right), \quad (3.8)$$

for some $X, Y, Z, W \in \mathbb{Q}$. Setting $X = Y = 0$ we recover Dryło's Frobenius elements [Dry12] leading to non-absolutely simple Jacobian varieties. We study the case $\sqrt{-d} \notin \mathbb{Q}(\zeta_s)$ and construct the equations derived from System (3.1).

Let ζ_s be a primitive s th root of unity where $s \in \{3, 4, 6\}$ and so $\varphi(s) = 2$. Condition $\pi\bar{\pi} = p$ of System (3.1) is equivalent to:

$$\begin{aligned} [X^2 + Z^2 + d(Y^2 + W^2) + (\zeta_s + \bar{\zeta}_s)(XZ + dYW)] \\ + [(\zeta_s - \bar{\zeta}_s)(XW - YZ)]\sqrt{-d} = p \end{aligned}$$

The coefficients A, B of the characteristic polynomial of Frobenius are:

$$A = -[4X + 2(\zeta_s + \bar{\zeta}_s)Z], \quad B = 2p + (A/2)^2 + d(\zeta_s - \bar{\zeta}_s)^2W^2$$

and so the second condition, namely $\#J(\mathbb{F}_p) \equiv 0 \pmod{r}$ implies:

$$[p + 1 + A/2]^2 + d(\zeta_s - \bar{\zeta}_s)^2W^2 \equiv 0 \pmod{r}$$

According to the above analysis, System (3.2) is transformed to:

$$\left. \begin{aligned} [X^2 + Z^2 + d(Y^2 + W^2) + (\zeta_s + \bar{\zeta}_s)(XZ + dYW)] &\equiv \zeta_k \pmod{r} \\ XW - YZ &= 0 \\ [p + 1 + A/2]^2 + d(\zeta_s - \bar{\zeta}_s)^2W^2 &\equiv 0 \pmod{r} \end{aligned} \right\} \quad (3.9)$$

We are working with polynomial families and so we fix the number field $L = \mathbb{Q}(\zeta_l) \cong \mathbb{Q}[x]/\langle r(x) \rangle$, where $r(x) = \Phi_l(x)$, for some $l > 0$, such that $\sqrt{d}, \zeta_s, \zeta_k \in L$. In particular this is done by setting $l = \text{lcm}(s, m, k)$, where m is the smallest positive integer such that $\sqrt{d} \in \mathbb{Q}(\zeta_m)$. Then the generalized Dryło Frobenius polynomial $\pi(x) \in K[x]$ becomes:

$$\pi(x) = X(x) + Y(x)\sqrt{-d} + \zeta_s \left(Z(x) + W(x)\sqrt{-d} \right), \quad (3.10)$$

for some $X(x), Y(x), Z(x), W(x) \in \mathbb{Q}[x]/\langle r(x) \rangle$ and its characteristic polynomial is $P(t) \in \mathbb{Q}[t]$ as in Equation (2.3), with coefficients in $\mathbb{Q}[x]$.

Examples of Absolutely Simple Jacobians with $s = 3$.

We give a few examples of polynomial families obtained by the solutions of System (3.9) for $s = 3$. Such a solution is the following:

$$\begin{aligned} X = Y &= [(\sqrt{3d} + 1)(\zeta_k - 1) + (\sqrt{-d} + \sqrt{-3})(\zeta_k + 1)]/[2\sqrt{-3}(d + 1)] \\ Z = W &= [(\zeta_k - 1) + (\zeta_k + 1)\sqrt{-d}]/[\sqrt{-3}(d + 1)] \end{aligned} \quad (3.11)$$

For the second equation of System (3.9) there is no need to take any lifts, since Solution (3.11) satisfies this equation in \mathbb{Q} . We then expect that the constructed Jacobian varieties will have $\rho(\pi, r) < 4$.

Remark 3.3. In the following examples the characteristic polynomial of Frobenius $P(t)$ satisfies $P(1) \equiv 0 \pmod{r(x)}$, but has rational coefficients. It can be transformed to a polynomial with integer coefficients by applying a linear transformation $t \rightarrow (MT + N)$, so that for every $t \equiv N \pmod{M}$, we have $P(t) \in \mathbb{Z}$. \square

Example 3.4. Let $l = 24$, so that $L = \mathbb{Q}(\zeta_{24})$. Set $r(x) = \Phi_{24}(x)$ and $u(x) = x$. For $s = 3$ and $d = 6$, the representation of $\sqrt{-6}$ and $\sqrt{-3}$ in $\mathbb{Q}[x]/\langle r(x) \rangle$ is:

$$z(x) = -2x^7 - x^5 + x^3 - x, \quad w(x) = 2x^4 - 1,$$

respectively. For $i = 3$ in Algorithm 1 we have $k = 8$ and by Solution (3.11):

$$\begin{aligned} X(x) &= Y(x) = (2x^7 - 3x^6 + 3x^5 - 2x^4 - x^3 + 3x^2 + 1)/21 \\ Z(x) &= W(x) = (-2x^7 - 3x^6 + 3x^5 + 2x^4 - 2x^3 - 3x - 4)/21 \end{aligned}$$

The Frobenius polynomial is represented by Equation (3.10), while the field polynomial is calculated by $p(x) = \pi(x)\bar{\pi}(x)$. We find that this is integer-valued for every $x \equiv \{7, 19\} \pmod{21}$. It is easy to verify that none of the conditions (2)–(5) of Proposition 2.1 is satisfied and also $\gcd[B(x), p(x)] = 1$. Thus the pair $[\pi(x), r(x)]$ represents a family of absolutely simple, ordinary, pairing-friendly, 2-dimensional Jacobians with embedding degree $k = 8$ and $\rho(\pi, r) = 3.5$. \square

In Table 1 we give more families derived by Solution (3.11). The integer $l > 0$ defined the

Table 1: Absolutely simple Jacobians from Solution (3.11).

l	k	d	i	x	$\rho(\pi, r)$
	3		16	$\{87, 144\} \pmod{147}$	
24	4	6	18	$\{5, 103\} \pmod{147}$	3.5000
	12		2	$\{16, 94, 104\} \pmod{147}$	
	24		17	$\{10, 20\} \pmod{21}$	

number field $L = \mathbb{Q}(\zeta_l)$ and the 2nd column is the embedding degree, obtained by taking the i th power (4th column) of ζ_l . The 3rd column is the square-free integer $d > 0$ defining the CM-field $K = \mathbb{Q}(\zeta_3, \sqrt{-d})$. The column x refers to the congruence that the inputs of $p(x)$ must satisfy, in order to obtain integer values. Finally the last column is the ρ -value of the family. In all cases of Table 1, the characteristic polynomial of Frobenius $P(t)$ has content equal to $1/7$, which disappears by setting $t \equiv N \pmod{7}$, for some $N \in \mathbb{Z}/7\mathbb{Z}$.

3.3 Alternative Representation

An alternative representation of a quartic CM-field is $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{-d_2})$, for some $d_1, d_2 \in \mathbb{Z}_{>0}$, with $d_1 \neq d_2$, such that $[K : \mathbb{Q}] = 4$. Additionally, K_2 is an imaginary quadratic extension of the totally real field K_1 . Then $\pi \in K$ is:

$$\pi = X + Y\sqrt{d_1} + \sqrt{-d_2} \left(Z + W\sqrt{d_1} \right), \quad (3.12)$$

for some $X, Y, Z, W \in \mathbb{Q}$. By the property of π being a Weil p -number, we get:

$$(X^2 + d_1Y^2 + d_2Z^2 + d_1d_2W^2) + (XY + d_2ZW)\sqrt{d_1} = p$$

and the characteristic polynomial of Frobenius is

$$P(x) = x^2 - 4Xx^3 + 4(X^2 - d_1Y^2)x^2 - 4Xpx + p^2. \quad (3.13)$$

Additionally, the condition $\#J(\mathbb{F}_q) = P(1) \equiv 0 \pmod{r}$ is equivalent to

$$(p + 1 + 2X)^2 - 4d_1Y^2 \equiv 0 \pmod{r}. \quad (3.14)$$

Using the fact that $p \equiv \zeta_k \pmod{r}$, we conclude to the following system:

$$\left. \begin{aligned} X^2 + d_1Y^2 + d_2Z^2 + d_1d_2W^2 &\equiv \zeta_k \pmod{r} \\ XY + d_2ZW &= 0 \\ (\zeta_k + 1 + 2X)^2 - 4d_1Y^2 &\equiv 0 \pmod{r} \end{aligned} \right\} \quad (3.15)$$

For polynomial families we set $L = \mathbb{Q}(\zeta_l) \cong \mathbb{Q}[x]/\langle r(x) \rangle$, where $l \in \mathbb{Z}_{>0}$ is an integer, such that $\sqrt{d_1}, \sqrt{-d_2}, \zeta_k \in \mathbb{Q}(\zeta_l)$. This is done by choosing $l = \text{lcm}(m_1, m_2, k)$, where m_1, m_2 are the smallest positive integers for which $\sqrt{d_1} \in \mathbb{Q}(\zeta_{m_1})$ and $\sqrt{-d_2} \in \mathbb{Q}(\zeta_{m_2})$. Then the Frobenius polynomial $\pi(x) \in K[x]$ is:

$$\pi(x) = X(x) + Y(x)\sqrt{d_1} + \sqrt{-d_2} \left(Z(x) + W(x)\sqrt{d_1} \right) \quad (3.16)$$

for $X(x), Y(x), Z(x), W(x) \in \mathbb{Q}[x]/\langle r(x) \rangle$. Note that we need to find the polynomial representation $z_1(x)$ and $z_2(x)$ of $\sqrt{d_1}$ and $\sqrt{-d_2}$ respectively in $\mathbb{Q}[x]/\langle r(x) \rangle$.

Absolutely Simple Jacobians.

We give a few examples of polynomial families obtained by solving System (3.15). Such a solution is:

$$\begin{aligned} X &= -d_2Z, & Z &= ((\zeta_k - 1) - (\zeta_k + 1)\sqrt{-d_2}) / (2(d_2 + 1)\sqrt{-d_2}) \\ Y &= W, & W &= -((\zeta_k + 1) + (\zeta_k - 1)\sqrt{-d_2}) / (2(d_2 + 1)\sqrt{d_1}) \end{aligned} \quad (3.17)$$

For the second equation of System (3.15) we do not need to take any lifts, since Solution (3.17) satisfies this equation in \mathbb{Q} . Again we expect that the Jacobian families will have ρ -values less than 4. Such examples are presented in Table 2.

Remark 3.5. Like Remark 3.3, in the examples of Table 2 $P(t)$ has rational coefficients. It can be transformed into a polynomial with integer coefficients by applying a linear transformation $t \rightarrow (MT + N)$, so that for every $t \equiv N \pmod{M}$, we have $P(t) \in \mathbb{Z}$. An analogous transformation is also required for $p(x)$. \square

Table 2: Absolutely simple Jacobians from Solution (3.17).

l	k	d_1	d_2	i	x	$\rho(\pi, r)$
56	7	7	2	8	$\{34, 58, 70\} \pmod{84}$	3.6667
	28			2	$\{5, 47, 70\} \pmod{84}$	
40	8	10	2	5	$\{5, 9, 21\} \pmod{30}$	3.7500
	20			18	$\{19, 25\} \pmod{30}$	

The 5th column refers to the powers i , so that $l/\text{gcd}(l, i) = k$, while the 6th column refers to the congruence that the inputs x of the field polynomial must satisfy, in order for $p(x)$ to be an integer.

4 Implementation and Numerical Examples

The process of generating suitable Jacobian parameters, given a polynomial family $[\pi(x), r(x)]$ is summarized in Algorithm 2. This involves a simple search for some $x_0 \in \mathbb{Z}$, such that $r(x_0)$ is a large prime of a desired size. Additionally we require $p(x_0)$ to be a large prime. In all inputs $[\pi(x), r(x)]$ of Algorithm 2 we need to ensure that $p(x)$ is integer-valued. This means that there must be integers $a, b \in \mathbb{Z}$, such that $p(x) \in \mathbb{Z}$, for all $x \equiv b \pmod{a}$. Algorithm 2 outputs the parameters (π, p, r) . Using these triples we can generate a 2-dimensional Jacobian $J(\mathbb{F}_p)$, with $r \mid \#J(\mathbb{F}_p)$ and Frobenius endomorphism π .

Algorithm 2 Generating suitable parameters for 2-dimensional Jacobians.

Input: A polynomial family $[\pi(x), r(x)]$ and a desired bit size S_r .

Output: A Frobenius element π , a prime p and a (nearly) prime r .

- 1: Find $a, b \in \mathbb{Z}$, such that $p(x) \in \mathbb{Z}$, for every $x \equiv a \pmod{b}$.
 - 2: Search for $x_0 \equiv b \pmod{a}$, such that $r(x_0) = nr$, for some prime r and $n \geq 1$.
 - 3: Set $\pi = \pi(x_0)$, $p = \pi(x_0)\bar{\pi}(x_0)$ and $r = r(x_0)/n$.
 - 4: If $\log r \approx S_r$ and p is prime, return (π, p, r) .
-

In all examples we considered pairing-friendly parameters of Jacobians providing a security level of at least 128 bits. These parameters are chosen according to Table 3, originally presented [BBC⁺09]. In this table we describe the sizes of the prime r , the extension field \mathbb{F}_{p^k} and

Table 3: Bit sizes of parameters and embedding degrees for various security levels.

Security Level	Subgroup Size	Extension Field Size	Embedding Degree		
			$\rho \approx 2$	$\rho \approx 3$	$\rho \approx 4$
128	256	3000 – 5000	12 – 20	8 – 13	6 – 10
192	384	8000 – 10000	20 – 26	13 – 17	10 – 13
256	512	14000 – 18000	28 – 36	18 – 24	14 – 18

the ρ -values, for which we achieve a specific security level. Note that we consider only ρ -values in the range $[2, 4]$, since examples of ordinary Jacobians with $\rho < 2$ are unknown. Below we give a few numerical results.

Example 4.1. By Example 3.4 for $K = \mathbb{Q}(\zeta_3, \sqrt{-6})$, with $l = 24$ and $k = 8$:

$$\begin{aligned}
 x_0 &= 4360331437 \equiv 7 \pmod{21}, & n &= 1, & \rho &= 3.4766, & \log r &= 256, & \log p &= 445 \\
 r &= 13066402029544023936014888184609183735900934642949490442553073853117 \\
 & \quad 4381452561 \\
 p &= 17104631628304699763110198214722643301043699660523612969956484320506 \\
 & \quad 5855733868250024048761970211501639650588258201899642085549804939611
 \end{aligned}$$

The Frobenius element is given by Equation (3.8), where:

$$\begin{aligned}
 X &= 19977689332165391591174792446457449401947760321021273055515383733481/7 \\
 &= Y \\
 Z &= -19977689345910463237518246909307679021587331482569818571002780858907/7 \\
 &= W
 \end{aligned}$$

Example 4.2. By Table 2 for $K = \mathbb{Q}(\sqrt{7}, \sqrt{-2})$, with $l = 56$ and $k = 7$:

$$\begin{aligned}
x_0 &= 2598994 \equiv 34 \pmod{84}, & n &= 1, & \rho &= 3.6438, & \log r &= 511, & \log p &= 931 \\
r &= 90224949054824406421561049829718588152075304690567472332332687394914 \\
&\quad 73066039292219239167201726638118449868190013063767741523986037176815 \\
&\quad 281479499089989361 \\
p &= 21239904668904333817709973155338690623300385802352294001328562007042 \\
&\quad 61835179582741593234260532283276861550703401273437279190497560011579 \\
&\quad 27702369069893259173431774628165850170870695988445770188791263194455 \\
&\quad 22756402197057566307655766948839347408923900736910854533045150375678 \\
&\quad 369784389
\end{aligned}$$

The Frobenius element is given by Equation (3.16), where:

$$\begin{aligned}
X &= - 25696905011664630705833341687313930844434718089380678968458180995099 \\
&\quad 2963637523888068136787166925109022918932740112208519677615493671272/3 \\
Y &= 95408680352830419349196275581747456931500685432234298288318648109643 \\
&\quad 04269787178041064158774558393289517649330206883526097646313691739567 \\
&\quad 6795/3 = W \\
Z &= 12848452505832315352916670843656965422217359044690339484229090497549 \\
&\quad 6481818761944034068393583462554511459466370056104259838807746835636/3
\end{aligned}$$

Example 4.3. By Table 1 for $K = \mathbb{Q}(\zeta_3, \sqrt{-6})$, with $l = 24$ and $k = 12$:

$$\begin{aligned}
x_0 &= 345544178999371 \equiv 16 \pmod{147}, & n &= 1, & \rho &= 3.4870, & \log r &= 386, & \log p &= 673 \\
r &= 20324910894606887240399630619505285158431171161301024701356843996833 \\
&\quad 9319902190248415883002212853851518240674936575281 \\
p &= 49425616831699737841023704220375574415231925088456164360663047426428 \\
&\quad 14180391704748985101035354501301286136788199848895195356498480763671 \\
&\quad 0392167837727193801811243040731972574701711205346152400140614733741
\end{aligned}$$

The Frobenius element is given by Equation (3.11), where:

$$\begin{aligned}
X &= 58820006615257915885458328313901928449890943678150596597746340772376 \\
&= 2779944351429654041129602047528721/7 = Y \\
Z &= 58820006615257859144034037707206747591416930807413746131814411489394 \\
&= 1258301910395154905139480417211818/7 = W
\end{aligned}$$

5 Conclusion

We presented a method for producing polynomial families of pairing-friendly Jacobians of dimension 2. We used different representations of the Frobenius element in a quartic CM-field from where we derived a system of three equations in four variables. Using the solutions of this system we constructed families of 2-dimensional, simple and ordinary Jacobians. Particularly, in this paper we focused on absolutely simple Jacobians, for which only few examples are known. The families we presented have the the best ρ -values so far in the literature. We argue though that the strategy we followed in this work can be used to produce families of non-absolutely simple Jacobians as well. Finally, we provided numerical examples of suitable parameters for a security level of at least 128 bits in r -order subgroups of a Jacobian $J(\mathbb{F}_{p^k})$ and in the extension field \mathbb{F}_{p^k} . More examples can be derived from our proposed families by using Algorithm 2.

References

- [BBC⁺09] J. Balakrishnan, J. Belding, S. Chisholm, K. Eisenträger, K. Stange, and E. Teske. Pairings on hyperelliptic curves. *Women in Numbers: Research Directions in Number Theory. Fields Institute Communications*, 60:87–120, 2009.
- [Ber06] D. Bernstein. Elliptic vs. hyperelliptic, part 1. Talk at ECC 2006, 2006.
- [BW05] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography*, 37(1):133–141, 2005.
- [Can87] David G. Cantor. Computing in the jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48(177):95–101, 1987.
- [CFA⁺06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications. Chapman & Hall/CRC Press, 2006.
- [Dry12] R. Drylo. Constructing pairing-friendly genus 2 curves with split jacobian. In S.D. Galbraith and M. Nandi, editors, *INDOCRYPT 2012*, volume 7668 of *LNCS*, pages 431–453. Springer, Berlin, Heidelberg, 2012.
- [EMJ17] N. El Mrabet and M. Joye. *Guide to pairing-based cryptography*. CRC Press, 2017.
- [FL06] G. Frey and T. Lange. Fast bilinear maps from the tate-lichtenbaum pairing on hyperelliptic curves. In F. Hess, S. Pauli, and M. Pohst, editors, *ANTS-VII 2006.*, volume 4076 of *LNCS*, pages 466–479. Springer, Berlin, Heidelberg, 2006.
- [Fre08] D. Freeman. A generalized brezing-weng algorithm for constructing pairing-friendly ordinary abelian varieties. In S.D. Galbraith and K.G. Paterson, editors, *Pairing 2008*, volume 5209 of *LNCS*, pages 431–453. Springer, Berlin, Heidelberg, 2008.
- [FS11] D.M. Freeman and S. Satoh. Constructing pairing-friendly hyperelliptic curves using weil restriction. *Journal of Number Theory*, 131(5):959–983, 2011.
- [FSS08] D. Freeman, P. Stevenhagen, and M. Streng. Abelian varieties with prescribed embedding degree. In A. Van der Poorten and A. Stein, editors, *ANTS-VIII 2008.*, volume 5011 of *LNCS*, pages 60–73. Springer, Berlin, Heidelberg, 2008.
- [GV12] A. Guillevic and D. Vergnaud. Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions. In M. Abdalla and T. Lange, editors, *Pairing 2012.*, volume 7708 of *LNCS*, pages 234–253. Springer, Berlin, Heidelberg, 2012.
- [HZ02] E.W. Howe and H.J. Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *Journal of Number Theory*, 92(1):139–163, 2002.
- [Kac10] E.J. Kachisa. Generating more kawazoe-takahashi genus 2 pairing-friendly hyperelliptic curves. In M. Joye, A. Miyaji, and A. Otsuka, editors, *Pairing 2010.*, volume 6487 of *LNCS*, pages 312–326. Springer, Berlin, Heidelberg, 2010.
- [KB16] T. Kim and R. Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In M. Robshaw and J. Katz, editors, *CRYPTO 2016.*, volume 9814 of *LNCS*, pages 543–571. Springer, Berlin, Heidelberg, 2016.
- [KJ17] T. Kim and J. Jeong. Extended tower number field sieve with application to finite fields of arbitrary composite extension degree. In M. Fehr, editor, *PKC 2017.*, volume 10174 of *LNCS*, pages 388–408. Springer, Berlin, Heidelberg, 2017.
- [Kob89] N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3):139–150, 1989.
- [KT08] M. Kawazoe and T. Takahashi. Pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$. In S.D. Galbraith and K.G. Paterson, editors, *Pairing 2008.*, volume 5209 of *LNCS*, pages 164–177. Springer, Berlin, Heidelberg, 2008.
- [Lan06] T. Lange. Elliptic vs. hyperelliptic, part 2. Talk at ECC 2006, 2006.
- [LS13] K. Lauter and N. Shang. Generating pairing-friendly parameters for the cm construction of genus 2 curves over prime fields. *Designs, Codes and Cryptography*, 67(3):341–355, 2013.
- [MF05] A. Murphy and N. Fitzpatrick. Elliptic curves for pairing applications. CiteSeer, 2005.
- [Mil08] J.S.: Milne. Abelian varieties., 2008.
- [OdJ08] F. Oort and A.J.: de Jong. Abelian varieties over finite fields. Seminar at Columbia University, September-December, 2008.

- [SW06] B.K. Spearman and K.S. Williams. Cyclic quartic fields with a unique normal integral basis. *Far east Journal of Mathematical Sciences*, 21:235–240, 2006.
- [Wen02] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(241):435–458, 2002.