# Constructing hidden order groups using genus three Jacobians

Steve Thakur

Axoni Research Group

**Abstract**

Groups of hidden order have gained a surging interest in recent years due to applications to cryptographic commitments, verifiable delay functions and zero knowledge proofs. Recently ([DG20]), the Jacobian of a genus three hyperelliptic curve has been suggested as a suitable candidate for such a group. While this looks like a promising idea, certain Jacobians are less secure than others and hence, the curve has to be chosen with caution. In this short note, we explore the types of Jacobians that would be suitable for this purpose.

## 1 Introduction

Finite abelian groups of hidden order have gained prominence within cryptography in the last few years. The adaptive root assumption in such groups yields a cryptographic accumulator which is universal and dynamic with batchable membership and non-membership proofs. A lot of these techniques were developed in [BBF19] where the authors constructed the first known Vector Commitment with constant-sized openings and a constant-sized public parameter. They subsequently designed a stateless blockchain that hinges on this Vector Commitment.

One of the best known verifiable delay functions is that constructed in [Wes18] which can be instantiated with any group of unknown order. Such groups also form the basis for the transparent polynomial commitment constructed in [BFS19]. This is a polynomial commitment with logarithmic size proofs and verification time and can be instantiated with any group of hidden order.

Until recently, the only widely known examples of groups of unknown order were RSA groups (which require a trusted setup) and class groups of number fields. In the latter case, only imaginary quadratic fields allow for efficient operations within class groups and even for this case, the group operations are roughly 10 times slower than those for RSA groups with the same security level. The recent paper by Dobson and Galbraith ([DG20] astutely observed that Jacobians of smooth curves over finite fields and in particular, Jacobians of genus three hyperelliptic curves can yield suitable candidates for groups of unknown order. These groups have a transparent setup unlike RSA groups and the group operations are believed to be 28 times faster than those in class groups of imaginary quadratic fields for the same level of security.

In this short note, we address a few issues surrounding the choice of the hyperelliptic curve. Broadly, it appears that the curves with the most "generic" behavior might be more suitable for our purpose since such curves do not appear vulnerable to the various point-counting algorithms than exists for certain families of curves.

## 2 Notations and background

### 2.1 The Honda-Tate correspondence

For an abelian variety $A$ over a field $F$, $\mathrm{End}(A)$ denotes its endomorphism ring and $\mathrm{End}^0(A)$ the endomorphism algebra of $A$ over the algebraic closure of the field of definition. By Honda-Tate theory, we have the well-known bijection

$$\{\text{Simple abelian varieties over } \mathbb{F}_q \text{ up to isogeny}\} \longleftrightarrow \{\text{Weil } q\text{-integers up to } \mathrm{Gal}_{\mathbb{Q}}\text{-conjugacy}\}$$

induced by the map sending an abelian variety to its Frobenius. For a Weil number $\pi$, we write $B_\pi$ for the corresponding simple abelian variety over $\mathbb{F}_q$. The dimension of $B_\pi$ is given by

$$2 \dim B = [\mathbb{Q}(\pi) : \mathbb{Q}][\mathrm{End}^0(B_\pi) : \mathbb{Q}(\pi)]^{1/2}.$$

Note that $\mathrm{End}^0(B_\pi)$ is a central division algebra over $\mathbb{Q}(\pi)$ and hence, $[\mathrm{End}^0(B_\pi) : \mathbb{Q}(\pi)]^{1/2}$ is an integer. The characteristic polynomial of $B_\pi$ on the Tate representation $V_l(A) := T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ (for any prime $l \neq p$) is independent of $l$ and is given by

$$P_{B_\pi}(X) := \prod_{\sigma \in \mathrm{Gal}_{\mathbb{Q}}} (X - \sigma(\pi))^{m_\pi}$$

where $m_\pi = [\mathrm{End}^0(B_\pi) : \mathbb{Q}(\pi)]^{1/2}$. We denote by $\mathcal{W}_{B_\pi}$ the set of Galois conjugates of $\pi$. Hence, $\mathbb{Q}(\mathcal{W}_{B_\pi})$ is the splitting field of $P_{B_\pi}(X)$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{B_\pi})/\mathbb{Q})$ is a subgroup of the wreath product $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$, the Galois group of the generic CM field of degree $2g$, where $g = [\mathbb{Q}(\pi + \overline{\pi}) : \mathbb{Q}]$.

**Definition 2.1.** An abelian variety $A$ over a field $F$ is *simple* if it does not contain a strict non-zero abelian subvariety. We say $A$ is *absolutely* or *geometrically* simple if the base change $A \times_F \overline{F}$ to the algebraic closure is simple. An abelian variety $A$ is *iso-simple* if it has a unique simple abelian subvariety up to isogeny.

We now state a few well-known facts about abelian varieties over finite fields which we will need in the subsequent sections. We refer the reader to the notes [Oo95] for proofs and further details.

**Proposition 2.1.** *For any simple abelian variety $B$ over a finite field $\mathbb{F}_q$, the abelian variety $B \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ is iso-simple.*

With this setup, let $\pi$ be a Weil number corresponding to $B$ and let $\widetilde{B}$ be the unique simple component (up to isogeny) of the base change $B \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ to the algebraic closure. Let $N$ be the smallest integer such that $\widetilde{B}$ has a model over the field $\mathbb{F}_{q^N}$. Then $\widetilde{B}$ corresponds to the Weil number $\pi^N$ and we have an isogeny

$$B \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q =_{\mathrm{isog}} \widetilde{B}^{(\dim B)/N}.$$

**Proposition 2.2.** *Let $\pi$ be a Weil $q$-integer and let $B_\pi$ be the corresponding simple abelian variety over $\mathbb{F}_q$. The following are equivalent:*
1. *$B_\pi \times_{\mathbb{F}_q} \mathbb{F}_{q^N}$ does not have any extra endomorphisms other than those of $B_\pi$ .*
2. *$\mathbb{Q}(\pi^N) = \mathbb{Q}(\pi)$.*

Thus, $B_\pi$ is absolutely simple if and only if $\mathbb{Q}(\pi^N) = \mathbb{Q}(\pi)$ for every integer $N$.

**Proposition 2.3.** *Let $\pi$ be a Weil $q$-integer and write $D_\pi := \mathrm{End}^0_{\mathbb{F}_q}(B_\pi)$. Then $D_\pi$ is a central division algebra over $\mathbb{Q}(\pi)$ and its Hasse invariants are given by*

$$\mathrm{inv}_v(D_\pi) = \begin{cases} 0 & \text{if } v \nmid q. \\ \frac{1}{2} & \text{if } v \text{ is real.} \\ [\mathbb{Q}(\pi)_v : \mathbb{Q}_p]\frac{v(\pi)}{v(q)} & \text{if } v | q. \end{cases}$$

In particular, $\mathrm{End}^0(B_\pi)$ is commutative if and only if the local degrees $[\mathbb{Q}(\pi)_v : \mathbb{Q}_p]$ annihilate the Newton slopes $\frac{v(\pi)}{v(q)}$. For instance, if $B_\pi$ is ordinary, the slopes $\frac{v(\pi)}{v(q)}$ are either 0 or 1 and hence, $\mathrm{End}^0(B_\pi)$ is commutative.

**Definition 2.2.** We say an abelian variety $B_\pi$ over $\mathbb{F}_q$ is of type $\mathrm{IV}(e,d)$ if the degree $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2e$ and the dimension $D_\pi$ is a $d^2$-dimensional division algebra central over $\mathbb{Q}(\pi)$ equipped with an involution of the second kind ($e, d \geq 1$). We say $B_\pi$ is *potentially* of type $\mathrm{IV}(e,d)$ if the base change $B_\pi \times_{\mathbb{F}_q} \mathbb{F}_q^j$ is simple and of type $\mathrm{IV}(e,d)$ for some extension $\mathbb{F}_q^j$.

The IV in the notation refers to Albert's classification of endomorphism algebras of simple abelian varieties.

**Proposition 2.4.** *Let $B_\pi$ be a simple abelian variety over a finite field $\mathbb{F}_q$ corresponding to a Weil number $\pi$ and let $l$ be a prime that does not divide $q$. The order $\left|B_\pi(\mathbb{F}_q)\right|$ of the group of $\mathbb{F}_q$-points is given by*

$$\left|B_\pi(\mathbb{F}_q)\right| = P_{B_\pi}(1) = \mathrm{Nm}(1-\pi)^{m_\pi}.$$

## 2.2 Newton Polygons

Let $B$ be an abelian variety over an algebraically closed field $k$ of characteristic $p > 0$. The group scheme $B[p^\infty]$ is a $p$-divisible group of rank $\leq \dim B$. Let $D(B[p^\infty])$ denote the Dieudonne module and $W(k)$ the Witt ring of $k$. Then $D(B[p^\infty]) \otimes_k W(k)[\frac{1}{p}]$ is a direct sum of pure isocrystals by the Dieudonne-Manin classification theorem. Let $\lambda_1 < \cdots < \lambda_r$ be the distinct slopes and let $m_i$ denote the multiplicity of $\lambda_i$. The sequence $m_1 \times \lambda_1, \cdots, m_r \times \lambda_r$ is called the *Newton polygon* of $B$. For a curve $C$ over a field of positive characteristic, we refer to the Newton polygon of the Jacobian $\mathrm{Jac}(C)$ as the Newton polygon of $C$.

**Definition 2.3.** A Newton polygon is *admissible* if it fulfills the following conditions:
1. The breakpoints are integral, meaning that for any slope $\lambda$ of multiplicity $m_\lambda$, we have $m_\lambda \lambda \in \mathbb{Z}$.
2. The polygon is *symmetric*, meaning that each slope $\lambda$, the slopes $\lambda$ and $1-\lambda$ have the same multiplicity.

Let $\pi$ be a Weil $q$-integer and let $B_\pi$ be the corresponding simple abelian variety over $\mathbb{F}_q$. Then the Newton slopes of $B_\pi$ are given by $\{v(\pi)/v(q)\}_v$ where $v$ runs through the places of $\mathbb{Q}(\pi)$ lying over $p$. In particular, the Newton polygon is symmetric and hence, all slopes lie in the interval $[0,1]$. The multiplicity of the slope 0 is called the $p$-rank of $B_\pi$. This is the $\mathbb{F}_p$-rank of the $p$-torsion group scheme $B_\pi[p]$

## 2.3 $l$-adic Galois representations

Let $A$ be an abelian variety over a field $F$. For any prime $l$ other than $\mathrm{char}(F)$, we have a Galois representation $\rho_{A,l} : \mathrm{Gal}_F \longrightarrow \mathrm{GL}_{2g}(\mathbb{Q}_l)$ induced by the $\mathrm{Gal}_F$-action on the $l$-adic Tate module of $A$. The Zariski closure $G_{A,l}$ of the image of $\rho_{A,l}$ is called the $l$-adic monodromy group of $A$. Let $G^0_{A,l}$ denote the connected component of $G_{A,l}$ containing the identity. This is a connected reductive subgroup (Falting's theorem) of the general symplectic group $\mathrm{GSp}_{2g}$. The index of $G^0_{A,l}$ in $G_{A,l}$ is finite and inddependent of the prime $l$. So after base change to a suitable extension $F_{A,\mathrm{conn}}$, the groups $G_{A,l}$ are connected reductive groups.

### 2.4 Cryptographic assumptions

**Assumption 2.5.** (Adaptive root assumption) *For a generic finite abelian group $\mathbb{G}$ of hidden order, it is infeasible for a probabilistic polynomial time algorithm to compute to compute $(g, h, l) \in \mathbb{G} \times \mathbb{G} \times \mathbb{Z} \setminus \{\pm 1\}$ such that $g^l = h$.*

Unlike in the case of class groups, it is possible to compute elements of small orders in Jacobians. But this can be remedied by replacing the Jacobian by an appropriate subgroup.

**Assumption 2.6.** *For a hyperelliptic curve of genus 2 or 3 over a finite field $\mathbb{F}_p$ for a sufficiently large $p$, we assume there exists an $N \in \mathbb{Z}$ such that it is infeasible for a probabilistic polynomial time algorithm to compute roots of the $l$-th division polynomials for $l > N$.*

For such an integer $N$, let $n := \mathrm{lcm}(1, \cdots, N)$. The subgroup $[n]\,\mathrm{Jac}(C)$ of $\mathrm{Jac}(C)$ is then expected to fulfill the adaptive root assumption. According to [DG20], the smooth integer $n := \mathrm{lcm}(1, \cdots, 60)$ is sufficient when $C$ is a genus three hyperelliptic curve.

## 3 Jacobians of curves

For a field $F$ of characteristic other than 2, a *hyperelliptic curve* $C$ of genus $g$ is the smooth completion of the affine curve given by $Y^2 = f(X)$ with $f$ monic, separable of degree $2g + 1$. A *divisor* $D$ is a formal sum $\sum_{m_P \in \mathbb{Z}, P \in C} m_P[P]$ of points on $C$ with all but finitely many of the multiplicities $m_P$ zero.

The *degree* $\deg(D)$ is the sum $\sum_P m_P$. The degree zero divisors $\mathrm{Div}^0(C)$ form an abelian group under addition. The *principal divisors* $\mathcal{P}(C)$ of $C$ are the divisors of the form $(f) := \mathrm{ord}_P(f)[P]$ where $f \in \bar{F}(C)$ and $\mathrm{ord}_P(f)$ is the order of the zero or the pole of $F$ at $P$. The quotient $\mathrm{Div}^0(C)/\mathcal{P}(C)$ is called the *Jacobian* of $C$. This is endowed with the structure of a principally polarized abelian variety over the field $F$.

In genus two, every smooth projective curve is hyperelliptic. On the other hand, the hyperelliptic locus of genus three curves is of codimension 1, which means that almost all genus three curves are non-hyperelliptic. Since Jacobians of genus three non-hyperelliptic curves are far less secure, it is important to be careful with the choice of the curve. When it comes to candidates for groups of hidden order, we would ideally have genus three hyperelliptic cuves $C$ over finite fields $\mathbb{F}_p$ such that $\mathrm{Jac}(C)$ is an absolutely simple threefold with a commutative endomorphism algebra.

**Example.** Let $l$ be an odd prime. Consider the curve

$$C : y^2 = 1 - x^l$$

of genus $\frac{l-1}{2}$ over $\mathbb{Q}$. The curve and its Jacobian $\mathrm{Jac}(C)$ have good reduction away from the primes $\{2, l\}$. Let $\zeta_l$ be a primitive $l$-th root of unity. The automorphism

$$C \times_{\mathbb{Q}} \mathbb{Q}(\zeta_l) \longrightarrow C \times_{\mathbb{Q}} \mathbb{Q}(\zeta_l), \quad (x_1, y_1) \mapsto (x_1, \zeta_l y_1)$$

induces an embedding

$$\mathbb{Q}(\zeta_l) \hookrightarrow \mathrm{End}^0(\mathrm{Jac}(C) \times_{\mathbb{Q}} \mathbb{Q}(\zeta_l)).$$

Since $[\mathbb{Q}(\zeta_l) : \mathbb{Q}] = l - 1 = 2 \dim \mathrm{Jac}(C)$, it follows (by degree reasons) that $\mathrm{Jac}(C)$ is absolutely simple with CM by the field $\mathbb{Q}(\zeta_l)$.

Now, $\mathrm{Jac}(C)$ has good reduction away from $\{2, l\}$ and since it is an abelian variety with CM, it has potential good reduction everywhere. So, for any prime $p \neq 2, l$, the reduction $\mathrm{Jac}(C)_p$ is an abelian variety over the finite field $\mathbb{F}_p$. Furthermore, since the extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ is abelian, it follows from the theory of complex multiplication that the Newton slopes of $\mathrm{Jac}(C)_p$ are determined exlusively by the splitting of the prime $p$ in $\mathbb{Z}[\zeta_l]$, which is determined by the residue $p \pmod{l}$.

1. In particular, if $p \equiv 1 \pmod{l}$, $\mathrm{Jac}(C_p)$ is ordinary.

2. If $p$ has an even inertia degree in $\mathbb{Q}(\zeta_l)/\mathbb{Q}$, $\mathrm{Jac}(C)_p$ is supersingular. Over a suitable finite extension, it is isogenous to the $\frac{l-1}{2}$-th power of the supersingular elliptic curve.

3. If $l \equiv 3 \pmod{4}$ and $p$ has order $\frac{l-1}{2}$ in $\mathbb{F}_l^*$, the Jacobian $\mathrm{Jac}(C)_p$ has Newton polygon

$$\frac{l-1}{2} \times \frac{2}{l-1}, \quad \frac{l-1}{2} \times \frac{l-3}{l-1}.$$

Since the Newton polygon of any simple component of $\mathrm{Jac}(C)_p$ has integral breakpoints, it follows that $\mathrm{Jac}(C)_p$ must be absolutely simple. In particularm, setting $l = 7$ and choosing a prime $p \equiv 1 \pmod{7}$ yields a simple ordinary Jacobian $\mathrm{Jac}(C_p)$ with $\mathrm{End}^0(\mathrm{Jac}(C_p)) \cong \mathbb{Q}(\zeta_7)$.

As this example illustrates, if we start with a curve $C/\mathbb{Q}$ such that $\mathrm{Jac}(C)$ has complex multiplication (CM) by a known field $K$, any reduction $C_p$ is determined by the splitting of $p$ in the extension $K/\mathbb{Q}$. However, such Jacobians might be vulnerable to the point-counting algorithm of [Abe18] since - in particular- they would have RM by the maximal real subfield of $F$. So for the purpose of obtaining hidden order groups, we might be better off starting with a curve $C$ such that $\mathrm{Jac}(C)$ has no non-trivial endomorphisms.

## 3.1 A few preliminary results

**Proposition 3.1.** *Let $g$ be an odd prime and let $B$ be an absolutely simple abelian variety of genus $g$ over a finite field $\mathbb{F}_q$. Then the endomorphism algebra $\mathrm{End}^0(B)$ is either a CM field of degree $2g$ or a $g^2$-dimensional division algebra central over an imaginary quadratic field in which $p := \mathrm{char}(\mathbb{F}_q)$ splits.*

*Proof.* Let $\pi$ denote the Weil $q$-integer corresponding to the isogeny class of $B$. Then

$$2g = [\mathbb{Q}(\pi) : \mathbb{Q}][\mathrm{End}^0(B) : \mathbb{Q}(\pi)]^{\frac{1}{2}}.$$

Since $g$ is a prime, the only possibilitie for the degree $[\mathbb{Q}(\pi) : \mathbb{Q}]$ are $2g, 2$ and $1$. In the first case, $\mathbb{Q}(\pi)$ is a CM field of degree $2g$ and in the second case, $B$ is of type $\mathrm{IV}(1, g)$. The only remaining case is $\pi \in \mathbb{Q}$. But in this case, $B$ is supersingular and hence, cannot be absolutely simple. $\square$

**Proposition 3.2.** *For an odd prime $g$, let $B$ be simple $g$-dimensional abelian variety over $\mathbb{F}_p$. Then one of the following holds:*

*1. $B$ is absolutely simple.*

*2. $B \times_{\mathbb{F}_p} \mathbb{F}_{p^g} =_{\mathrm{isog}} E^g$ for some ordinary elliptic curve $E$ over $\mathbb{F}_{p^l}$ such that the class number of $\mathrm{End}^0(E)$ is divisible by $g$.*

*Proof.* It is a well-known consequence of Honda-Tate theory that every simple abelian variety over a finite field is iso-simple (see [CCO14]). So $A \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q =_{\text{isog}} A_0^e$ for some simple abelian varety $A_0$ over $\overline{\mathbb{F}}_q$ and integer $e \geq 1$. So $\dim A = e \dim A_0$. Since $g$ is a prime, it follows that either $e = 1$ in which case $A$ is absolutely simple or $e = \dim A$, in which case $A_0$ is an elliptic curve.

Let $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ be the prime decomposition of the ideal generated by $p$ in the imaginary quadratic field $K := \mathbb{Q}(\pi_1)$. Then

$$\pi_1 \mathcal{O}_K = \mathfrak{p}^j \overline{\mathfrak{p}}^{g-j}, \overline{\pi}_1 \mathcal{O}_K = \mathfrak{p}^{g-j} \overline{\mathfrak{p}}^j$$

for some integer $g \geq j \geq 0$. Now, if $j \notin \{0, g\}$, the Newton slopes $g \times \frac{j}{g}$, $g \times \frac{g-j}{g}$ of $B_{\pi_1}$ have least common denominator $g$ and hence, $B_{\pi_1}$ is of type $\text{IV}(1, g)$. In particular, $B_\pi$ is absolutely simple.

On the other hand, if $j \in \{0, g\}$, then $B_{\pi_1}$ has Newton slopes $g \times 0$, $g \times 1$, meaning it is ordinary. Furthermore, suppose by way of contradiction that the ideal $\mathfrak{p}$ is principal, say $\mathfrak{p} = \gamma \mathcal{O}_K$. Then we have $\gamma^g = \pi_1 \zeta$ where $\zeta$ is a unit in $\mathcal{O}_K$. But since $K$ is an imaginary quadratic field, the only units in $\mathcal{O}_K$ are the roots of unity. Let $N$ be the smallest integer such that $\zeta^N = 1$. Now, $\zeta = (\gamma/\pi)^g$ and hence, $\mathbb{Q}(\pi)$ contains the $Ng$-th roots of unity. Since $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2g$, we have a contradiction. Thus, $\mathfrak{p}$ is not principal and since $\mathfrak{p}^g$ is, it follows that $g$ divides the class number of $K$. $\square$

The next proposition confirms that simple abelian threefolds over $\mathbb{F}_p$ with non-commutative endomorphism rings are rare within the larger set of simple abelian threefolds. However, up to isogeny, the abelian varieties of type $\text{IV}(1, 3)$ are far larger in number than the supersingular abelian varieties. Since the number of $\mathbb{F}_{p^3}$-points on such abelian varieties is a perfect cube, it would desirable to choose curves whose Jacobians are not of this type. We will need the next lemma.

**Lemma 3.3.** *Let $B_1, B_2$ be abelian varieites of type* $\text{IV}(1, g)$ *over a finite field $\mathbb{F}_q$ of characteristic $p$ and set $D_i := \text{End}^0_{\overline{\mathbb{F}}_p}(B_i)$ (($i = 1, 2$). Then the following are equivalent:*

(1). *$B_1$ is isogenous to $B_2$ over $\overline{\mathbb{F}}_p$.*

(2). *$D_1 \cong D_2$.*

*Proof.* It suffices to show that (2) $\Rightarrow$ (1) since the other direction is obvious.

(2) $\Rightarrow$ (1): Let $\pi_1, \pi_2$ be the corresponding Weil $q$-integers. Then $K := \mathbb{Q}(\pi_1) \cong \mathbb{Q}(\pi_2)$ is an imaginary quadratic field in which $p$ splits. Let $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ be the prime decomposition of $p$ in $K$. Let $\frac{j}{g}, \frac{g-j}{g}$ be the Hasse invariants of $D$ at $\mathfrak{p}, \overline{\mathfrak{p}}$ respectively. Then we have $\pi_1 \mathcal{O}_K = \mathfrak{p}^{dj} \overline{\mathfrak{p}}^{d(g-j)}$ where $d := \log_p(q)$. Since $D_2$ has the same Hasse invariants, it follows that $\pi_2 \mathcal{O}_K = \mathfrak{p}^{dj} \overline{\mathfrak{p}}^{d(g-j)}$ and hence, $\pi_1$, $\pi_2$ genrate the same ideal in $\mathcal{O}_K$. Since $K$ is an imaginary quadratic field, it has no torsion-free units and hence, $\pi_2 = \pi_1 \zeta$ where $\zeta^N = 1$ for some integer $N$. Thus, $B_1$, $B_2$ are isogenous over the extension $\mathbb{F}_{q^N}$. $\square$

**Proposition 3.4.** *The number of $\overline{\mathbb{F}}_p$-isogeny classes of simple principally polarized abelian threefolds $B$ over $\mathbb{F}_p$ with the endomorphism algebra $\text{End}^0_{\overline{\mathbb{F}}_p}(B)$ non-commutative is asymptotically $\mathbf{O}(\sqrt{p} \log(p))$.*

*Proof.* We first count the isogeny classes of the supersingular abelian varieties of genus 3. Let $\pi$ be a Weil number corresponding to this isogeny class. Then $\pi^N \in \mathbb{Z}$ for some integer $N$ and $[\mathbb{Q}(\pi) : \mathbb{Q}]$ divides 6. So $\pi = \sqrt{p}\zeta$ where $\zeta$ is a root of unity. The only possibilities for this are those afforded by $\zeta^6 = 1$. Hence, the number of simple supersingular abelian varieties of genus three up to isogeny is asymptotically $\mathbf{O}(1)$.

From Honda-Tate theory, it is immediate that $\mathrm{End}^0_{\overline{\mathbb{F}}_p}(B)$ is either a degree 6 CM field or a 9-dimensional division algebra central over an imaginary quadratic field. We consider the latter case. Let $\pi$ be an ordinary Weil $p$-integer. Let $\widetilde{\pi} := \sqrt[3]{\pi^2\overline{\pi}} = \sqrt[3]{p\pi} \in \overline{\mathbb{Q}}$ be one of the cube roots of $p\pi$. Then $\widetilde{\pi}$ is a Weil $p$-integer with $\mathbb{Q}(\widetilde{\pi})$ a CM field of degree 6. Thus, $B_{\widetilde{\pi}}$ is a simple genus three abelian variety over $\mathbb{F}_p$. Furthermore, $\widetilde{\pi}^3$ is a Weil $p^3$-integer with $\mathbb{Q}(\widetilde{\pi}^3) = \mathbb{Q}(\pi)$, an imaginary quadratic field. So $B_{\widetilde{\pi}^3}$ is a simple abelian variety over $\mathbb{F}_{p^3}$ with Newton slopes $3 \times \frac{1}{3}$, $3 \times \frac{2}{3}$.

Conversely, let $\pi$ be a Weil $p$-integer such that $B_\pi$ is potentially of type $\mathrm{IV}(1,3)$. Let $K$ be the imaginary quadratic field contained in $\mathbb{Q}(\pi)$ and let $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ be the factorization of $p\mathcal{O}_K$ into prime ideals. Then $\pi^3\mathcal{O}_K = \mathfrak{p}^2\overline{\mathfrak{p}}$ or $\mathfrak{p}\overline{\mathfrak{p}}^2$ and by symmetry, we may assume it is the former. Thus,

$$\pi^3\mathcal{O}_K = \mathfrak{p}^2\overline{\mathfrak{p}} = \mathfrak{p}(p\mathcal{O}_K)$$

and hence, $\mathfrak{p}, \overline{\mathfrak{p}}$ are principal ideals. Since $K$ is an imaginary quadratic field, $\mathcal{O}_K$ has no torsion-free units and every principal ideal of $\mathcal{O}_K$ has a unique generator up to multiplication by a root of unity $\zeta_N$ for some $N \in \{1, 2, 3, 4, 6\}$. Let $\pi_1$ be a generator for $\mathfrak{p}$. Then $\pi^3 = \pi_1^2\overline{\pi}_1\zeta$ where $\zeta^{12} = 1$.

Now, for two abelian varieties of type $\mathrm{IV}(1,3)$, the endomorphism algebras are isomorphic if and only if the abelian varieties are isogenous over some finite extension. Hence, there is a 2-to-1 map between the $\overline{\mathbb{F}}_p$-isogeny classes of simple threefolds of type $\mathrm{IV}(1,3)$ and the ordinary elliptic curves over $\mathbb{F}_p$ up to $\overline{\mathbb{F}}_p$-isogeny. Since the number of isogeny classes of ordinary eliptic curves over $\mathbb{F}_p$ is $\mathbf{O}(\sqrt{p}\log(p))$, this completes the proof. □

The number of isomorphism classes is a more subtle question and would entail looking at the class numbers of the endomorphism rings. But since we are only concerned with the number of points on the Jacobian - which only depends on the isogeny class, it suffices to study the isogeny classes for now.

**Corollary 3.5.** *The number of absolutely simple genus three Jacobians* $\mathrm{Jac}(C)$ *over* $\mathbb{F}_p$ *with* $\mathrm{End}^0(\mathrm{Jac}(C))$ *non-commutative is asymptotically* $\mathbf{O}(\sqrt{p}\log(p))$.

*Proof.* Let $B$ be any abelian variety over $\mathbb{F}_p$ with Newton polygon $3 \times \frac{1}{3}$, $3 \times \frac{2}{3}$. Since $B$ has a principally polarized abelian variety in its isogeny class over $\mathbb{F}_p$, we may assume without loss of generality that $B$ is principally polarized. So $B$ is the Jacobian of some curve $\widetilde{C}$ over $\overline{\mathbb{F}}_p$ by Oort's aforementioned theorem. If $C$ is hyperelliptic, there exists a hyperelliptic curve $C$ over $\mathbb{F}_p$ such that $\mathrm{Jac}(C)$ is $\mathbb{F}_p$-isomorphic to $B$. On the other hand, if $\widetilde{C}$ is non-hyperelliptic, then there exists a curve $C$ over $\mathbb{F}_p$ such that $\mathrm{Jac}(C)$ is isomorphic to the quadratic twist of $B$. □

## 3.2 Types of curves to avoid

The following types of curves $C/\mathbb{F}_q$ are less desirable as candidates for producing Jacobians with an unknown number of $\mathbb{F}_q$-points.

1. Any curve over a non-prime field $\mathbb{F}_q$.

   Note that since we do not want $\#\,\mathrm{Jac}(C)(\mathbb{F}_q)$ to have any known divisors, $\mathrm{Jac}(C)(\mathbb{F}_q)$ should have no known subgroups. In particular, if $q$ is not a prime, we would have the added burden of making sure that $\mathrm{Jac}(C)$ does not have a model over any proper subfield of $\mathbb{F}_q$.

2. A curve $C$ such that $\mathrm{Jac}(C)$ is not absolutely simple.

Note that if $\mathrm{Jac}(C)$ has a simple component $B$ (up to isogeny) over an extension $\mathbb{F}_{q^k}$, then $\#B(\mathbb{F}_{q^k})$ divides $\#\,\mathrm{Jac}(C)(\mathbb{F}_{q^k})$. In particular, if an adversary computes an elliptic curve covered by $C$ (possibly after passing to a finite extension), that would undermine the security of the system.

3. A curve $C$ with Newton slopes $3 \times \frac{1}{3}$, $3 \times \frac{2}{3}$.

Although such a Jacobian is absolutely simple, after passing to a suitable finite extension (of degree at most 6), the number of points is the cube of an integer. This would necessitate a larger field of definition for the same security level.

4. A curve $C$ obtained by using the CM methods described in [Wen01] and [Lai15].

Note that such curves are obtained by sampling possible values of the Weil number $\pi$ and subjecting thse norm $\#B_\pi(\mathbb{F}_q) = \mathrm{Nm}_{\mathbb{Q}(\pi)/\mathbb{Q}}(1-\pi)$ to primality tests such as the Miller-Rabin test. While this construction is certainly useful for other purposes, it is clearly insecure for the purpose of producing groups of hidden order. In fact, as observed in [DG20], it is necessary that the curve is chosen through a nothing-up-my-sleeve construction.

5. A curve $C$ such that $\mathrm{Jac}(C)$ has action by either of the fields $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ or $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.

Any such Jacobian would be simple with $\mathrm{End}^0(\mathrm{Jac}(C))$ a degree 6 CM whose maximal real subfield is $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ or $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Such Jacobians are susceptible to the the point-counting technique in [Abe18]. For instance, this rules out the curves $Y^2 = X^7 + a$ since the Jacobians have action by $\mathbb{Q}(\zeta_7)$. It also rules out the (non-hyperelliptic) Picard curves $Y^3 := f(X)$ ($\deg(f) = 9$) since these have CM by $\mathbb{Q}(\zeta_9)$.

Furthermore, we note that Abelard's algorithm exploits Pila's algorithm for factorizing rational primes $l \equiv 1 \pmod{n}$ in the cyclotomic extension $\mathbb{Q}(\zeta_n)$. Since every abelian extension over $\mathbb{Q}$ is a subfield of some cyclotomic field (Kronecker-Weber), it seems feasible that the technique could be extended in the foreseeable future to Jacobians with real multiplication (RM) by any known totally real cubic field Galois over $\mathbb{Q}$. For this reason, when it comes to constructing Jacobians with a hidden number of $\mathbb{F}_p$-points, it might be prudent to avoid Jacobians with RM by such fields.

### 3.3 Reductions of generic Jacobians over $\mathbb{Q}$

In this section, we explore the types of curves that might be suitable for constructing Jacobians with a hidden number of $\mathbb{F}_q$-rational points. Since we are interested in hyperelliptic curves over a prime field $\mathbb{F}_p$, a natural place to look is the reductions of hyperelliptic curves over $\mathbb{Q}$ at the places of good reduction.

First, we note that if a curve $C$ over $\mathbb{Q}$ is such that $L \hookrightarrow \mathrm{Jac}(C)$ for some number field $L$, then we have $L \hookrightarrow \mathrm{Jac}(C_p)$ for any prime $p$ of good reduction. Since knowledge of the endomorphism algebra of $\mathrm{Jac}(C_p)$ makes point-counting algorithms more feasible, it seems more prudent to look for Jacobians over $\mathbb{Q}$ that have no endomorphisms other than those of the form

$$[N] : \mathrm{Jac}(C) \longrightarrow \mathrm{Jac}(C); \;\; P \longrightarrow [N]P \;\; (N \in \mathbb{Z}).$$

We recall a few relevant theorems here.

**Theorem 3.6.** (Zarhin) *Let $C : Y^2 = f(X)$ be a genus $g$ hyperelliptic curve over $\mathbb{Q}$ such that the Galois group of $f(X)$ is the symmetric group $S_{2g+1}$ or the alternating group $A_{2g+1}$. Then* $\mathrm{Jac}(C)$ *is an absolutely simple abelian variety over $\mathbb{Q}$ with* $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}(C)) = \mathbb{Z}$.

We refer the reader to [Zha00] for the proof. Recall that as consequence of Hilbert's irreducibility theorem, most polynomials of degree $N$ are irreducible with Galois group $S_N$. So the condition imposed on $f(X)$ is not particularly restrictive.

**Theorem 3.7.** (Serre's open image theorem) *Let $g$ be an odd integer or 2 or 6. Let $A$ be an abelian variety over $\mathbb{Q}$ with absolute endomorphism ring $\mathbb{Z}$. Then for any prime $l$, the image of the Galois representation $\rho_{A,l} : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}_l)$ is open of finite index in $\mathrm{GSp}_{2g}(\mathbb{Z}_l)$.*

This is a generalization of Serre's older and better-known open image theorem for elliptic curves. Chavdarov ([Cha97]) showed that when the $l$-adic monodromy groups are as large as possible, the reductions are almost always geometrically simple abelian varieties over finite fields. In fact, the statement of his theorem is a bit more precise.

**Theorem 3.8.** (Chavdarov) *Let $A$ be an abelian variety over a number field $F$ with absolute endomorphism ring $\mathbb{Z}$ and the $l$-adic mondomy group $\mathrm{GSp}_{2g,\mathbb{Q}_l}$ for any prime $l$. Suppose, furthermore, that $F$ is enlarged so that the $l$-adic monodromy groups $G_{A,l}$ are connected. Then, away from a set of primes of $F$ of Dirichlet density zero, the reduction $A_v$ at a prime $v$ is an absolutely simple abelian variety with $\mathrm{End}^0(A_v)$ a generic CM field of degree $2g$.*

Zywina ([Zyw14]) generalized Chavdarov's theorem to all abelian varieties fulfilling the Mumford-Tate conjecture. The smallest field extension $F_{A,\mathrm{conn}}$ such that the $l$-adic modoromy groups are connected can be alternatively describes as

$$F_{A,\mathrm{conn}} := \bigcap_l F(A[l^\infty])$$

where $F(A[l^\infty])$ is the extension of $F$ obtained by attaching all $l^N$-torsion points of $A$ (for every $N \in \mathbb{Z}$) and the intersection runs through all rational primes ([LP95]). So, choosing a curve $C$ over $\mathbb{Q}$ such that the field $\mathbb{Q}_{\mathrm{Jac}(C),\mathrm{conn}} = \mathbb{Q}$ would allow us to choose a place $v$ of $\mathbb{Q}_{\mathrm{Jac}(C),\mathrm{conn}}$ such that:

1. $v$ is of local degree on over $\mathbb{Q}$, meaning that the residue field $k_v$ is a field of size $p := \mathrm{char}(v)$.
2. $C \times_{\mathbb{Q}} \mathbb{Q}_{\mathrm{Jac}(C),\mathrm{conn}}$ and $\mathrm{Jac}(C) \times_{\mathbb{Q}} \mathbb{Q}_{\mathrm{Jac}(C),\mathrm{conn}}$ have good reduction at $v$. Note that away from a finite set of places, both the curve $C$ and the Jacobian $\mathrm{Jac}(C)$ will have good reduction.
3. $\mathrm{Jac}(C_v)$ is absolutely simple with $\mathrm{End}^0(\mathrm{Jac}(C_v)$ a generic CM field of degree $2g$. The ubiqitousness of such places $v$ is implied by the aforementioned theorems of Chavdarov.

The first condition ensures that the field of definition is a prime finite field and the second ensures that $\mathrm{Jac}(C_v)$ is the Jacobian of a hypereliptic curve. The third condition ensures that $\mathrm{Jac}(C_v)$ does not have RM by any totally real field of degree $g$ which is Galois over $\mathbb{Q}$. This is one way of making sure that the adaptive root assumption in the group $\mathrm{Jac}(C_v(\mathbb{F}_p))$ is not vulnerable to an attack using Abelard's techniques ([Abe18]). In particular, with this construction, $\mathrm{Jac}(C_v)$ would not have RM by any totally real field of degree $g$ which is Galois over $\mathbb{Q}$.

**Corollary 3.9.** *For an odd integer $g$, let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $2g+1$ with Galois group $S_{2g+1}$. Let $C : Y^2 = f(X)$ be the hypereliptic curve over $\mathbb{Q}$ with Jacobian $\mathrm{Jac}(C)$. Let $L := \mathbb{Q}_{\mathrm{Jac}(C),\mathrm{conn}}$ be the smallest field extension such that the $l$-adic monodromy groups of $\mathrm{Jac}(C)$ are connected. Then there exists a density one subset $\mathcal{S}$ of the primes of $L$ such that for any $v \in \mathcal{S}$:*

*- the residue field $k_v$ at $v$ is a prime field.*

*- the reduction $C_v$ is a smooth curve over $k_v$.*

*- the Jacobian $\mathrm{Jac}(C_v)$ is an absolutely simple abelian variety over $k_v$ with CM by a generic CM field of degree $2g$.*

*Proof.* Since the intersection of two sets of Dirichlet density one also has density one, it suffices to show that the sets of primes of $L$ fulfilling each of the three conditions have density one.

Note that any prime $v$ with local degree one over $\mathbb{Q}$ fulfills the first condition and by the Chebotarev density theorem, the Dirichlet density of such primes is one. Since the curve $C \times_{\mathbb{Q}} L$ has good reduction away from a finite set of primes, the second condition holds away from a set of density zero.

Since the Galois group of $f(X)$ is assumed to be the full symmetric group $S_{2g+1}$, Zarhin's theorem implies that the endomorphism ring $\mathrm{End}(\mathrm{Jac}(C))$ is trivial. Furthermore, by Chavdarov's theorem, away from a density zero set, $\mathrm{Jac}(C_v)$ is absolutely simple with $\mathrm{End}(\mathrm{Jac}(C_v))$ a generic CM field of degree $2g$, which completes the proof. □

Furthermore, the following proposition implies that for any fixed number field $L \neq \mathbb{Q}$, the reduction of the Jacobian at a randomly chosen prime is unlikely to have action by $L$.

**Proposition 3.10.** *For an odd integer $g$, let $C : Y^2 = f(X)$ be a hyperelliptic curve such that $f(X) \in \mathbb{Z}[X]$ is irreducible of degree $2g+1$ with Galois group $S_{2g+1}$. Let $L$ be any fixed number field other than $\mathbb{Q}$. Then away from a set of places of density zero, the Jacobian of the reduction $C_v$ does not have action by the field $L$.*

*Proof.* Let $\widetilde{L}$ denote the Galois closure of $L$ over $\mathbb{Q}$. By Zarhin's theorem, $A := \mathrm{Jac}(C)$ is absolutely simple of dimension three with endomorphism ring $\mathbb{Z}$. So $A$ fulfills the Mumford-Tate conjecture and its Mumford-Tate group is the general symplectic group $\mathrm{GSp}_{2g}$. It is well-known that the general symplectic group is split over $\mathbb{Q}$, i.e. it has a maximal split torus over $\mathbb{Q}$. Furthermore, the Weyl group $W(\mathrm{GSp}_{2g})$ of $\mathrm{GSp}_{2g}$ is the wreath product $\{\pm 1\}^g \rtimes S_g$. Hence, by ([Zyw14], Thm 1.5), there exists a density one subset $\mathcal{S}$ of $\Sigma_F$ such that

$$\mathrm{Gal}(\widetilde{L}(\mathcal{W}_{A_v})/\widetilde{L}) \cong W(\mathrm{GSp}_{2g}) \cong \{\pm 1\}^g \rtimes S_g, \ \ \forall\, v \in \mathcal{S}.$$

In particular, for any $v \in \mathcal{S}$, we the endomorphism algebra $\mathrm{End}^0(A_v)$ is linearly disjoint with $L$. □

Now, for an odd integer $g$, let $f(X) \in \mathbb{Z}[X]$ be any irreducible polynomial with Galois group $S_{2g+1}$. Let $C : Y^2 = f(X)$ be the hypereliptic curve over $\mathbb{Q}$ and $A := \mathrm{Jac}(C)$ its Jacobian. Then $A$ has absolute endomorphism ring $\mathbb{Z}$ and if $p$ is a randomly chosen rational prime of good reduction, then with overwhelming probability:

- the Jacobian $A_p = \mathrm{Jac}(C_p)$ is absolutely simple with $\mathrm{End}^0(B)$ a generic CM field of degree $2g$.
- $A_p$ does not have action by any *fixed* number field other than $\mathbb{Q}$.

## References


[Abe18] Abelard, *Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus*, Journal of Complexity, 57:101440, 2020

[BBF19] D. Boneh, B. Bunz, B. Fisch, *Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains.* In Alexandra Boldyreva and Daniele Micciancio, editors, Advances in Cryptology – CRYPTO 2019, pages 561–586, Cham, 2019. Springer International Publishing.

[BFS19] B. Bunz, B. Fisch, A. Szepieniec, *Transparent SNARKs from DARK Compilers*

[CFGKN20] M. Campanelli, D. Fiore, N. Greco, D. Kolonelos, L. Nizzardo *Vector Commitment Techniques and Applications to Verifiable Decentralized Storage*

[Can87] D. Cantor. *Computing in the Jacobian of a hyperelliptic curve. Mathematics of computation*, 48(177):95–101, 1987.

[Can94] D. Cantor. *On the analogue of the division polynomials for hyperelliptic curves*, Crelle's Journal, 447:91–146, 1994.

[CCO14] B. Conrad, C. Chai, F. Oort, *Complex Multiplication and Lifting Problems*

[Cha97] N. Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. Volume 87, Number 1 (1997), 151-180.

[DG20] S. Dobson, S. Galbraith, *Trustless Groups of Unknown Order with Hyperelliptic Curves*

[Hal11], C. Hall, *An open-image theorem for a general class of abelian varieties*, with an appendix by E. Kowalski, Bull. Lond. Math. Soc., Vol. 43, No. 4 (2011), 703–711.

[Koh96] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, 1996 Berkeley thesis

[Lai15] Kim H. M. Laine. *Security of Genus 3 Curves in Cryptography.* PhD thesis, University of California, Berkeley, 2015.

[LP95] M. Larsen, R. Pink, *A connectedness criterion for $l$-adic representations*, Israel J. of Math. 97, 1-10 (1997)

[Lee20] J. Lee, *The security of Groups of Unknown Order based on Jacobians of Hyperelliptic Curves*

[Mil86] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 167–212

[Oo95] F. Oort, *Abelian Varieties over finite fields*

[Rei75] I. Reiner, *Maximal Orders*, Academic Press, 1975

[Sch85] R. Schoof. *Elliptic curves over finite fields and the computation of square roots mod p.* Mathematics of computation, 44(170):483–494, 1985.

[ST66] J.P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2), 88, 1968

[Tat69] J. Tate, *Classes d'isogenie des varietes abeliennes sur un corps fini*

[Wen01] A. Weng. *A class of hyperelliptic CM-curves of genus three.* Journal of the Ramanujan Mathematical Society, 16, 01 2001.

[Wen03] A. Weng. *Constructing hyperelliptic curves of genus 2 suitable for cryptography.* Mathematics of Computation, 72(241):435–458, 2003.

[Wes19] B. Wesolowski, *Efficient verifiable delay functions.* In Yuval Ishai and Vincent Rijmen, editors, Advances in Cryptology – Eurocrypt 2019, pages 379–407, Cham, 2019. Springer International Publishing.

[Yui78] N. Yu, *On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic $p > 2$* , Journal of Algebra 52, 378-410 (1978)

[Zar00] Y. Zarhin, *Hyperelliptic jacobians without complex multiplication* Math. Res. Letters 7 (2000), 123–132

[Zyw14] D. Zywina, *The splitting of reductions of an abelian variety*, IMRN 18 (2014), 5042–5083. MR3264675

Steve Thakur

Axoni Research Group
New York City, NY
Email: stevethakur01@gmail.com