Super-Isolated Elliptic Curves and Abelian Surfaces in Cryptography

Travis Scholl
Department of Mathematics
University of Washington
tscholl2@uw.edu

May 1, 2017

Abstract

We call a simple abelian variety over $\mathbb{F}_p$ *super-isolated* if its ($\mathbb{F}_p$-rational) isogeny class contains no other varieties. The motivation for considering these varieties comes from concerns about isogeny based attacks on the discrete log problem. We heuristically estimate that the number of super-isolated elliptic curves over $\mathbb{F}_p$ with prime order and $p \leq N$, is roughly $\tilde{\Theta}(\sqrt{N})$. In contrast, we prove that there are only 2 super-isolated surfaces of cryptographic size and near-prime order.

1 Introduction

The security of elliptic curve cryptography depends on the difficulty of the elliptic curve discrete log problem (ECDLP). Given an elliptic curve E over $\mathbb{F}_p$, a cyclic subgroup of $E(\mathbb{F}_p)$ generated by the point P, and a point $Q \in \langle P \rangle$, the ECDLP asks to find an integer k such that $Q = kP$. The fastest known generic algorithm to solve the ECDLP on an elliptic curve is Pollard's rho algorithm, which has an expected runtime of $\tilde{O}(\sqrt{p})$ [17, Ch. 3.6.3].

It is possible to transfer the ECDLP between curves via isogenies. If $\varphi : E \to E'$ is an isogeny[1] that restricts to an isomorphism $\langle P \rangle \to \langle \varphi(P) \rangle$, then $Q = kP$ if and only if $\varphi(Q) = k\varphi(P)$. This reduction is useful for solving the ECDLP if the time it takes to compute $\varphi(Q)$ and $\varphi(P)$, as well as to solve the ECDLP on E', is less than the time it takes to solve the ECDLP on E.

Concern about isogeny based attacks is partially motivated by the Gaudry-Hess-Smart (GHS) attack [9]. Over certain extension fields[2], Menezes and Teske in [15, Sec. 7] used the generalized GHS attack to show that there is a non-negligible proportion of "weak" curves, for which the ECDLP can be solved in significantly less time than it takes Pollard's rho. Under some reasonable assumptions, given a random elliptic curve E over such a field, one can find a chain of efficiently computable isogenies from E to a weak curve.

In [11, Sec. 11, Ex. 5], Koblitz, Koblitz, and Menezes observed that it is possible to use the complex multiplication (CM) method to construct elliptic curves $E/\mathbb{F}_p$ whose isogeny class is large ($\approx \sqrt{p}$), but contains no curves (besides E itself) whose *conductor gap* with E is small. The conductor gap between two curves measures the computational complexity in computing an isogeny between them. The curve E is called *isolated* because there are no other curves E' for which constructing an isogeny between E and E' is computationally feasible.

So far we have only mentioned elliptic curves, but the same ideas carry over to abelian surfaces. In [27], Wang gave a construction for isolated abelian surfaces that is analogous to the

[1] Unless otherwise noted, by isogeny we mean $\mathbb{F}_p$-rational isogeny.
[2] The attack described in [15] only applies to fields of the form $\mathbb{F}_2^{3\ell}$ with $53 \leq \ell \leq 200$.

one for curves given in [11]. Note that while these methods construct isolated varieties, they almost always have large isogeny classes.

In this paper, we focus on the special case of *super-isolated* abelian varieties. We call an abelian variety over a finite field super-isolated if its isogeny class contains a single isomorphism class. For increased security and efficiency, we focus on varieties of prime or near-prime order defined over a prime field.

Our main contributions are as follows. First, we outline practical algorithms that search for super-isolated elliptic curves and abelian surfaces. Second, we prove that only two super-isolated surfaces of cryptographic size and near-prime order exist, see Examples 35 and 36. Finally, we give some heuristics on the number of super-isolated varieties. Our results suggest that, unlike the case of surfaces, there are enough super-isolated elliptic curves of cryptographic size and prime order to use in cryptosystems that require ephemeral curves, such as [18].

The outline of the paper is as follows. Section 2 focuses on elliptic curves. Some background and notation is given in Section 2.1. In Section 2.2, we outline an algorithm to construct super-isolated elliptic curves of prime order over $\mathbb{F}_p$ with p of a given size. We heuristically estimate the number of such curves in Section 2.3. Section 3 focuses on surfaces. In Section 3.1, we show that finding super-isolated surfaces reduces to finding *super-isolated Weil numbers*, which are defined in that section. In Section 3.2, we outline an algorithm to search for super-isolated Weil numbers. We also prove the correctness and efficiency of the algorithm in the same section. Two examples of super-isolated surfaces of near-prime order and cryptographic size are given in Section 3.3. In Section 3.4, we prove these are the only such examples.

Acknowledgments

I would like to thank my advisor Neal Koblitz for all of his inspiration and guidance while working on this paper. I would also like to acknowledge the support from my graduate student peers, for which I am especially grateful.

2 Elliptic curves

2.1 Background and notation

Let p be a prime[3]. For any $t \in \mathbb{Z}$, let $I(t)$ denote the set of isomorphism classes of elliptic curves $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = p - t + 1$. A theorem of Tate says that the sets $I(t)$ are isogeny classes of elliptic curves over $\mathbb{F}_p$, see [22, Ch. 5]. The Hasse bound implies that $I(t)$ is empty when $t^2 > 4p$. An elliptic curve is *ordinary* if $t \not\equiv 0 \mod p$.

Definition 1. An elliptic curve $E/\mathbb{F}_p$ is *super-isolated* if there is only one isomorphism class in its isogeny class, i.e. $\#I(p + 1 - \#E(\mathbb{F}_p)) = 1$.

Definition 2. Let $\mathcal{O}$ be an order in a quadratic imaginary field, and let Δ be the discriminant of $\mathcal{O}$. The *Kronecker class number* $H(\Delta)$ *of* Δ is defined to be

$$H(\Delta) = \sum_{\mathcal{O}' \supseteq \mathcal{O}} h(\mathcal{O}')$$

where $h(\mathcal{O}')$ denotes the class number of the order $\mathcal{O}'$, and the sum is over all orders $\mathcal{O}'$ of $\mathcal{O} \otimes \mathbb{Q}$ such that $\mathcal{O}' \supseteq \mathcal{O}$.

Theorem 3 ([21, Thm. 4.6])**.** *If $t^2 < 4p$ and $t \not\equiv 0 \mod p$, then*

$$\#I(t) = H(t^2 - 4p).$$

[3]Many results in this paper can be extended to varieties over arbitrary finite fields $\mathbb{F}_q$, but we focus on the prime case because it is often more efficient in practice.

Remark 4. The Kronecker class number is defined differently in [21, Defn. 2.1], but the equivalence with the Definition 2 is proved in [21, Prop. 2.4].

Remark 5. If $t = p + 1 - \#E(\mathbb{F}_p) \equiv 0 \mod p$, then E is called *supersingular*. The reason that we focus on ordinary curves is because the ECDLP on supersingular curves is vulnerable to the Menezes-Okamoto-Vanstone attack [16]. There do exist super-isolated supersingular curves. For example, $y^2 + y = x^3 + x$ is the only curve over $\mathbb{F}_2$ with 5 points. See [21, Thm. 4.6, Pg. 194] for a detailed formula for $\#I(t)$ when $t \equiv 0 \mod p$. If $p \geq 5$ then any supersingular curve over $\mathbb{F}_p$ will have an even number of points. Hence we may ignore the supersingular case because we are interested in curves with prime order.

2.2 Super-isolated elliptic curves of prime order

In this section, we outline a simple method to search for super-isolated elliptic curves which have prime order. The reason for considering curves of prime order is that it increases the security and efficiency of the elliptic curve cryptosystem.

First we will use the results in Section 2.1 to give a simple characterization of super-isolated elliptic curves over prime fields.

Corollary 6. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with trace $t = p + 1 - \#E(\mathbb{F}_p)$. Then E is super-isolated if and only if*

$$t^2 - 4p \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

Proof. By Theorem 3, $\#I(t) = 1$ if and only if $t^2 - 4p$ is the discriminant of the maximal order of a quadratic imaginary field with class number 1. It is a well known theorem of Heegner and Stark that the numbers in the statement are precisely the discriminants of such fields [24]. □

Remark 7. Super-isolated elliptic curves are rare in the sense that if we choose a prime p at random, it is unlikely there exists such a curve over $\mathbb{F}_p$. Let $\pi_{SI}(x)$ denote the number of primes $p < x$ such that there exists a super-isolated elliptic curve over $\mathbb{F}_p$. Any such p must be of the form $t^2 + d/4$, where $-d$ is one of the numbers from Corollary 6 and t is an integer. This shows that $\pi_{SI}(x) = O(\sqrt{x})$.

Remark 8. Even when super-isolated curves exist over $\mathbb{F}_p$, such curves are rare in the set of all curves over $\mathbb{F}_p$. There are $2p + O(1)$ distinct isomorphism classes of elliptic curves over $\mathbb{F}_p$, but at most 18 are super-isolated. The number 18 is a rough overestimate that comes from the 9 values in Corollary 6, and then multiplying by 2 to account for quadratic twists. It is not hard to show that other twists will not be super-isolated.

Remark 9. Another way to view the condition in Corollary 6 is as follows. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with class number 1 and discriminant $-d$. Then we are searching for algebraic integers $\pi \in \mathcal{O}_K$ of the form $\pi = (t + \sqrt{-d})/2$ such that $\pi\overline{\pi} = (t^2 + d)/4 = p$ is prime and $\mathbb{Z}[\pi] = \mathcal{O}_K$.

Suppose that p, t, and $d = t^2 - 4p$ satisfy the condition in Corollary 6. The fact that $p = (t^2 + d)/4 \in \mathbb{Z}$ implies that $t \equiv d \mod 2$. So we may replace t with $2x$ or $2x + 1$ depending on $d \mod 2$. Then p and $N = p + 1 - t$ can be written as the following integral polynomials:

$$p = \begin{cases} x^2 + \frac{d}{4} & \text{if } -d \equiv 0 \mod 4 \\ x^2 + x + \frac{d+1}{4} & \text{if } -d \equiv 1 \mod 4 \end{cases}, \quad N = \begin{cases} (x-1)^2 + \frac{d}{4} & \text{if } -d \equiv 0 \mod 4 \\ x^2 - x + \frac{d+1}{4} & \text{if } -d \equiv 1 \mod 4 \end{cases} \tag{1}$$

We are interested in values of x such that p and N are simultaneously prime. Two necessary conditions for p and N to be simultaneously prime infinitely often are:

(i) p and N are irreducible over $\mathbb{Z}[x]$.

(ii) $\gcd_{a \in \mathbb{Z}} p(a)N(a) = 1$.

It is clear that condition (i) is satisfied for all values of d. From Table 1 below, condition (ii) holds for $d \in \{3, 19, 43, 67, 163\}$ (this can be checked using only a few consecutive values of a [3, Ex. 3.i, Pg. 19]).

We now give a simple description of our search method.

1. Choose $d \in \{3, 19, 43, 67, 163\}$ and let p, N be as in Table 2.
2. Choose random integers x in a predetermined range until $p(x)$ and $N(x)$ are both prime.
3. Use the CM method to recover a curve $E/\mathbb{F}_p$ with N points, see [6, Ch. 18.1].

Example 10. Let $d = 3$ and $x = 321438704914423479101766132343967029098$. Then $p = p(x)$ and $N = N(x)$ are both 256-bit primes. The curve $E/\mathbb{F}_p$ given by $y^2 = x^3 + 244944$ satisfies $\#E(\mathbb{F}_p) = N$. This value of x was found by a `Sage` [26] program that randomly sampled integers from the interval $[0, 2^{128}]$.

Example 11. Let $d = 3$ and $x = 2^{127} + 13906$. Then $p(x)$ and $N(x)$ are 255-bit primes. Moreover, their binary representations have a Hamming weight of 24 and 27 respectively. The CM method gives the curve $y^2 = x^3 + 279936$. Even though our search method does not have full control over the prime p, it is still possible to find primes with certain desirable properties, such as a low Hamming weight.

$-d$	$p(x)$	$N(x)$	$\gcd_{a\in\mathbb{Z}} p(a)N(a)$
3	$x^2 + x + 1$	$x^2 - x + 1$	1
4	$x^2 + 1$	$x^2 - 2x + 2$	2
8	$x^2 + 2$	$x^2 - 2x + 3$	6
7	$x^2 + x + 2$	$x^2 - x + 2$	4
11	$x^2 + x + 3$	$x^2 - x + 3$	3
19	$x^2 + x + 5$	$x^2 - x + 5$	1
43	$x^2 + x + 11$	$x^2 - x + 11$	1
67	$x^2 + x + 17$	$x^2 - x + 17$	1
163	$x^2 + x + 41$	$x^2 - x + 41$	1

Table 1: $\gcd_{a\in\mathbb{Z}} p(a)N(a)$ for values of d.

2.3 Estimating the number of super-isolated curves of prime order

In various applications, it is important to have some degree of randomness in the parameter selection. For example, a cryptosystem may require a distinct curve for each user, or use ephemeral keys such as in [18]. In this section, we estimate the number of super-isolated elliptic curves of prime order, as a way to measure the randomness in the selection of such a curve. We also give some numerical evidence supporting our estimates.

The Bateman-Horn conjecture [1] implies that if $p(x)$ and $N(x)$ are irreducible and satisfy $\gcd_{a\in\mathbb{Z}} p(a)N(a) = 1$, then the number of x, with $0 \le x \le M$, such that $p(x)$ and $N(x)$ are simultaneously prime is asymptotic to $\frac{C}{4}\int_2^M 1/\log^2(t)dt$ for a computable constant C. It is clear that $p(x)$ and $N(x)$ are irreducible, and we saw in Table 1 the values of d such that the second property holds. For each such d, Table 2 gives an approximation of the constant C.

Example 12. We ran 10000 iterations of the search in Example 10. The average number of x's sampled until $p(x)$ and $N(x)$ were both prime, was 10312. The heuristics above imply that the expected number of x's that need to be sampled is

$$\left(\frac{2.9}{4}\frac{1}{2^{128}}\int_2^{2^{128}} \frac{1}{\log^2 t}\, dt\right)^{-1} \approx 10610.$$

The percent difference between the observed and expected is -0.028.

$-d$	C
-3	≈ 2.9
-19	≈ 3.0
-43	≈ 10.6
-67	≈ 17.5
-163	≈ 44.8

Table 2: An approximation to the Bateman-Horn constant C.

Combining the heuristics above, we expect that the number of x with $0 \leq x \leq M$ such that $p(x)$ and $N(x)$ are prime for some $d \in \{3, 19, 43, 67, 163\}$ is approximately

$$19.7 \cdot \int_2^M \frac{1}{\log^2 t}\, dt.$$

Since $p(x)$ has degree 2, we can estimate the number of curves over $\mathbb{F}_p$ with $p \leq M$ by choosing x in the range $0 \leq x \leq \sqrt{M}$. Combined with above, we have the following estimate for the number of curves.

Heuristic 13. The number of super-isolated elliptic curves of prime order over $\mathbb{F}_p$ with $p \leq M$ is approximately

$$19.7 \int_2^{\sqrt{M}} \frac{1}{\log^2 t}\, dt.$$

3 Abelian surfaces

3.1 Super-isolated Weil numbers

We define *super-isolated* for an abelian variety as we did for an elliptic curve: an abelian variety whose isogeny class contains only one isomorphism class. Recall that finding a super-isolated elliptic curve over $\mathbb{F}_p$ is equivalent to finding an algebraic integer π in an imaginary quadratic field K of class number 1 such that $\pi\overline{\pi} = p$ and $\mathbb{Z}[\pi] = \mathcal{O}_K$ (see Remark 9). The general situation is similar, only we replace K with a CM field (defined below), and $\mathbb{Z}[\pi]$ with $\mathbb{Z}[\pi, \overline{\pi}]$.

Definition 14. A number field K is a *complex multiplication field*, or *CM field*, if K is a quadratic imaginary extension of a totally real field F. CM fields have a unique non-trivial automorphism fixing F, which we denote by $\alpha \mapsto \overline{\alpha}$ and refer to as complex conjugation.

Definition 15. For any $n \in \mathbb{Z}$, a *Weil n-number* is an algebraic integer that has absolute value $\sqrt{n}$ under every embedding to $\mathbb{C}$. A *Weil number* is a Weil n-number for some n. If K is a CM field, then $\alpha \in \mathcal{O}_K$ is a Weil number if and only if $\alpha\overline{\alpha} \in \mathbb{Z}$. It can be shown that if π is a Weil p-number for a prime p, then either $\mathbb{Q}(\pi)$ is a CM field or $\pi = \pm\sqrt{p}$.

Let $A/\mathbb{F}_p$ be a simple[4] abelian variety, and let f be the characteristic polynomial of the Frobenius endomorphism of A. It is well known that $\#A(\mathbb{F}_p) = f(1)$ and $f = h^e$ where h is irreducible and e is some integer. Moreover, any root π of f is a Weil p-number and $2 \dim A = e[\mathbb{Q}(\pi) : \mathbb{Q}]$ [28, Thm 8]. For cryptographic reasons, we are interested in varieties with prime or near-prime order, so we will mainly focus on the case where $e = 1$.

Theorem 16. *Let A be a simple abelian variety over $\mathbb{F}_p$, π be a root of the characteristic polynomial of the Frobenius endomorphism, and $K = \mathbb{Q}(\pi)$. Assume that $\pi \neq \pm\sqrt{p}$. Then A is super-isolated if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ and K has class number 1.*

[4] In this paper we use simple to mean simple over the base field. Other sources sometimes use the term to mean simple over the algebraic closure.

Proof. By [29, Thm. 3.5], the endomorphism ring of any variety isogenous to A is an order[5] in $\mathcal{O}_K$ containing $\mathbb{Z}[\pi, \overline{\pi}]$. Because the base field is $\mathbb{F}_p$ and $\pi \neq \pm\sqrt{p}$, the converse holds as well [29, Thm. 6.1]. That is, every order of $\mathcal{O}_K$ containing $\mathbb{Z}[\pi, \overline{\pi}]$ is the endomorphism ring of some variety isogenous to A. We call the set of varieties isogenous to A with endomorphism ring R the *endomorphism class* of R. So there is exactly one endomorphism class if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$. The proof of [29, Thm. 6.1] shows that the number of isomorphism classes in the endomorphism class of $\mathcal{O}_K$ is equal to the class number of K. Therefore, the entire isogeny class of A contains a single isomorphism class if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ and K has class number 1. □

Definition 17. A *super-isolated Weil number* is a Weil number π such that $K = \mathbb{Q}(\pi)$ has class number 1 and $\mathcal{O}_K = \mathbb{Z}[\pi, \overline{\pi}]$.

In this section we are mainly interested in surfaces. The reason for not considering higher dimensional abelian varieties is that the discrete log problem on jacobians[6] of curves of genus ≥ 3 can be solved faster than on comparably sized jacobians of curves of genus ≤ 2 [7, 8, 23]. This means that we would need to use a larger key size in order to achieve comparable security. Hence varieties of dimension ≥ 3 are less efficient in practice. Both genus 2 and 1 are still considered for cryptographic use and have comparable efficiency [2].

Remark 18. Another reason for focusing on curves and surfaces is that we do not expect many super-isolated varieties of dimension at least 3. In [25], Stark remarked that it is reasonable to believe that there are only finitely many CM fields of class number 1. This would imply that there is a finite list of fields which admit Weil numbers that could correspond to super-isolated varieties of near-prime order.

The following corollary specializes Theorem 16 to surfaces with $e = 1$.

Corollary 19. *Let A be an abelian surface over $\mathbb{F}_p$. Assume that the characteristic polynomial f of the Frobenius endomorphism of A is irreducible. Then A is super-isolated if and only if the roots of f are super-isolated Weil p-numbers.*

Proof. This follows from Theorem 16 after noting that, because f is irreducible, A is simple and $\pm\sqrt{p}$ can not be roots of f. □

Therefore, in order to find super-isolated surfaces of near-prime order (note that near-prime order implies the hypothesis in Corollary 19), it is sufficient to find all super-isolated Weil numbers π, such that $\pi\overline{\pi}$ is prime and $\mathbb{Q}(\pi)$ has degree 4. There are 91 quartic CM fields of class number 1, and they can be found in the literature [13, 30]. By [14, Cor. 2.10], if π is a Weil p-number whose minimal polynomial f has degree 4, then there is a simple abelian surface over $\mathbb{F}_p$ such that f is the characteristic polynomial of the Frobenius endomorphism of A. This is a special case of a theorem of Honda, which shows that every Weil p-number is a root of the characteristic polynomial of the Frobenius endomorphism of some simple abelian variety over $\mathbb{F}_p$ [10]. One can recover a representative of the isogeny class of A from π using the two dimensional analogue of the CM method [6, Ch. 18].

3.2 Search algorithm

In this section we describe an efficient algorithm for enumerating all super-isolated Weil numbers in a given field up to a certain bound. For the rest of the paper, unless otherwise stated, we will only consider super-isolated Weil numbers π such that $\mathbb{Q}(\pi)$ has degree 4 over $\mathbb{Q}$ and $\pi\overline{\pi}$ is prime.

[5] The statement of [29, Thm. 3.5] refers to an order in $\mathrm{End}_{\mathbb{F}_p} A \otimes \mathbb{Q}$, but this is the same as K since the base field is prime, see [29, Ch. 2].

[6] Cryptosystems usually use jacobians of hyperelliptic curves rather than arbitrary varieties because they provide efficient representations necessary for practical use [12].

Remark 20. Our methods are motivated by those Wang used in [27] to parameterize *isolated abelian surfaces*, which are analogues of the isolated elliptic curves described in Section 1.

Remark 21. A naive algorithm to find super-isolated Weil p-numbers is as follows. Fix a quartic CM field K with class number 1. For each prime p less than a certain bound, find all possible solutions π in $\mathcal{O}_K$ to the relative norm equation $\pi\overline{\pi} = p$. This can be done using standard algorithms, see [5, Ch. 7.5.4]. For each solution, check if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ by computing discriminants. This method is not practical because primes p which admit super-isolated Weil p-numbers are rare.

First, we will give an informal description of our algorithm. Let K be a quartic CM field with class number 1, and let $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ be a basis for $\mathcal{O}_K$. Then any $\pi \in \mathcal{O}_K$ can be written as $\sum a_i\alpha_i$ for some $a_i \in \mathbb{Z}$. We will show that π is a super-isolated Weil number if and only if the a_i satisfy the following properties:

(i) The condition that $\pi\overline{\pi} \in \mathbb{Z}$ is equivalent to $P_0(a_1, a_2, a_3, a_4) = 0$, where P_0 is the polynomial in Equation 5 below.

(ii) If (i) holds, then the condition that $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ is equivalent to the equations

$$f_1(a_1, a_2, a_3, a_4) = \pm 1 \quad \text{and} \quad f_2(a_1, a_2, a_3, a_4) = \pm 1,$$

where f_1 and f_2 are the polynomials in Equations (2,3).

(iii) The condition that $\pi\overline{\pi}$ is prime is equivalent to $P(a_1, a_2, a_3, a_4)$ being prime, where P is the polynomial in Equation 4 below.

These equivalences are shown in the proof of Theorem 30 below. Moreover, we will also show that if $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ are chosen in a certain way, then finding solutions to the equations $P_0 = 0$, $f_1 = \pm 1$, $f_2 = \pm 1$ essentially reduces to an instance of Pell's equation. Our algorithm starts by choosing such a basis, and proceeds to enumerate tuples (a_1, a_2, a_3, a_4) satisfying the conditions above.

3.2.1 The algorithm

The algorithm outlined below enumerates super-isolated Weil numbers in a certain field.

1. Choose a quartic CM field K of class number 1, and let F be the real quadratic subfield. Let Δ_K, Δ_F denote the respective discriminants.
2. Choose a basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of $\mathcal{O}_K$ such that $\alpha_1 = 1$ and $\{\alpha_1, \alpha_2\}$ form a basis for $\mathcal{O}_F$.
3. Choose non-conjugate embeddings $\phi_1, \phi_2 : K \hookrightarrow \mathbb{C}$.
4. Compute the coefficients of the following polynomials:

$$f_1 = \frac{1}{\sqrt{\Delta_F}} \sum_{i=1}^{4} (\phi_1(\alpha_i + \overline{\alpha}_i) - \phi_2(\alpha_i + \overline{\alpha}_i))x_i \tag{2}$$

$$f_2 = \frac{\Delta_F}{\sqrt{\Delta_K}} \sum_{1 \le i,j \le 4} \phi_1(\alpha_i - \overline{\alpha}_i)\phi_2(\alpha_j - \overline{\alpha}_j)x_i x_j \tag{3}$$

$$P = \frac{1}{2} \sum_{1 \le i,j \le 4} \left(\phi_1(\alpha_i\overline{\alpha}_j) + \phi_2(\alpha_i\overline{\alpha}_j)\right) x_i x_j \tag{4}$$

$$P_0 = \frac{1}{2\sqrt{\Delta_F}} \sum_{1 \le i,j \le 4} \left(\phi_1(\alpha_i\overline{\alpha}_j) - \phi_2(\alpha_i\overline{\alpha}_j)\right) x_i x_j \tag{5}$$

   By Lemma 25 below, $f_1 \in \mathbb{Z}[x_2, x_3, x_4]$, $f_2 \in \mathbb{Z}[x_3, x_4]$, and $P, P_0 \in \frac{1}{2}\mathbb{Z}[x_1, x_2, x_3, x_4]$.
5. Enumerate solutions $x_3 = a_3$, $x_4 = a_4$ to the equation

$$f_2(x_3, x_4) = \pm 1 \tag{6}$$

   up to a given bound. We do this as follows.

5.1 By Lemma 26 below, we may write $f_2 = ax_3^2 + bx_3x_4 + cx_4^2$ for $a, b, c \in \mathbb{Z}$ with $b^2 - 4ac = \Delta_F$. A straight-forward calculation shows that the $\mathbb{Z}$-module $I = a\mathbb{Z} + \frac{b+\sqrt{\Delta_F}}{2}\mathbb{Z}$ is an ideal of $\mathcal{O}_F$. Here we are abusing notation by writing $\sqrt{\Delta_F}$ as an element of F. Since K is a quartic CM field with class number 1, F has class number 1. So we can choose a principal generator γ for I. Let ϵ be a fundamental unit for F. One can find both γ and ϵ using standard algorithms, see [4, Ch. 4-5].

5.2 For each $i \in \mathbb{Z}$, with $|i|$ less than a predetermined bound, compute $\sigma = \pm\epsilon^i\gamma$ for each choice of sign.

5.3 For each σ, find a pair $a_3, a_4 \in \mathbb{Q}$ such that $a_3 a + a_4 \frac{b+\sqrt{\Delta_F}}{2} = \sigma$.

6. For each pair (a_3, a_4), find all a_2 such that $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ is a solution to

$$f_1(x_2, x_3, x_4) = \pm 1. \tag{7}$$

We can find a_2 as follows. By the choice of basis, the coefficient of x_2 in f_1 is non-zero. Thus, there are two possibilities for $a_2 \in \mathbb{Q}$, and they are each given by linear polynomials in a_3, a_4.

7. For each tuple (a_2, a_3, a_4), find all a_1 such that $x_1 = a_1$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ is a solution to

$$P_0(x_1, x_2, x_3, x_4) = 0. \tag{8}$$

This can be done as follows. A straightforward computation, using the fact that $\alpha_1 = 1$, shows that $2P_0 = g + f_1 x_1$ for some polynomial $g \in \mathbb{Z}[x_2, x_3, x_4]$. Since $f_1(a_2, a_3, a_4) = \pm 1$, we have $a_1 = \mp g(a_2, a_3, a_4)$.

8. For each tuple (a_1, a_2, a_3, a_4), if every a_i is integral and $P(a_1, a_2, a_3, a_4)$ is prime, then output

$$\pi = a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 + a_4\alpha_4.$$

3.2.2 Correctness

In this section, we will prove the correctness of the algorithm of Section 3.2.1. By correctness, we mean that if the algorithm outputs π, then π is a super-isolated Weil number. Conversely, if π is a super-isolated Weil number in K, then, given a large enough bound, the algorithm will eventually output π.

Remark 22. This section is solely focused on the correctness of the algorithm. For a discussion of the efficiency, see Section 3.2.3.

Our proof of correctness involves several computations, which have been broken down into several lemmas. The main idea is to find explicit polynomials representing the index of $\mathbb{Z}[\pi, \pi]$ in $\mathcal{O}_K$ and the value of $\pi\overline{\pi}$, both with respect to the basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$.

First, we will prove Lemmas 25 and 26, which were used in the description of the polynomials f_1, f_2, P, P_0 in the algorithm in Section 3.2.1. To prove these lemmas, we start with some facts from algebraic number theory.

Lemma 23. *Let K be a quartic CM field, F be the quadratic real subfield of K, and ϕ_1, ϕ_2 be non-conjugate embeddings $K \hookrightarrow \mathbb{C}$. If $\gamma \in \mathcal{O}_K$, then*

$$\phi_1(\gamma + \overline{\gamma}) + \phi_2(\gamma + \overline{\gamma}) \in \mathbb{Z}$$

and

$$\phi_1(\gamma + \overline{\gamma}) - \phi_2(\gamma + \overline{\gamma}) \in \sqrt{\Delta_F}\mathbb{Z}.$$

Proof. Note that $\gamma + \overline{\gamma} \in \mathcal{O}_F$, so $\phi_1(\gamma + \overline{\gamma})$ can be written as $a + b\sqrt{\Delta_F}$ for some $a, b \in \frac{1}{2}\mathbb{Z}$. Because $\phi_1(\sqrt{\Delta_F}) = -\phi_2(\sqrt{\Delta_F})$, the claim follows from noticing that

$$\phi_1(\gamma + \overline{\gamma}) + \phi_2(\gamma + \overline{\gamma}) = 2a$$
$$\phi_1(\gamma + \overline{\gamma}) - \phi_2(\gamma + \overline{\gamma}) = 2b\sqrt{\Delta_F}.$$

□

Lemma 24. *Let K be a quartic CM field with maximal totally real subfield F. If $\gamma \in \mathcal{O}_K$ and ϕ_1, ϕ_2 are any non-conjugate pair of embeddings $K \hookrightarrow \mathbb{C}$, then*

$$\phi_1(\gamma - \overline{\gamma})\phi_2(\gamma - \overline{\gamma}) \in \frac{\sqrt{\Delta_K}}{\Delta_F} \cdot \mathbb{Z}.$$

Proof. Let $\delta_{K/F}(\alpha)$ denote the relative different for any $\alpha \in \mathcal{O}_K$. Because K/F is a quadratic imaginary extension, we have that $\delta_{K/F}(\alpha) = \alpha - \overline{\alpha}$.

We may assume $K = F(\gamma)$ otherwise the claim is trivial as $\phi_1(\gamma - \overline{\gamma})\phi_2(\gamma - \overline{\gamma}) = 0$. From the proof of [20, Thm. III.2.5, Pg. 198],

$$\delta_{K/F}(\gamma)\mathcal{O}_K = \mathfrak{f}_{\mathcal{O}_F[\gamma]}\mathcal{D}_{K/F}$$

where $\mathfrak{f}_{\mathcal{O}_F[\gamma]} = \{\alpha \in K \colon \alpha\mathcal{O}_K \subseteq \mathcal{O}_F[\gamma]\}$ is the conductor of the order $\mathcal{O}_F[\gamma]$ in $\mathcal{O}_K$ and $\mathcal{D}_{K/F}$ is the relative different of the extension K/F.

Note that $\gamma + \overline{\gamma} \in \mathcal{O}_F$ implies that $\overline{\gamma} \in \mathcal{O}_F[\gamma]$, hence $\mathcal{O}_F[\gamma]$ is invariant under conjugation. It follows that $\mathfrak{f}_{\mathcal{O}_F[\gamma]}$ is invariant under conjugation, so we may write $\mathfrak{f}_{\mathcal{O}_F[\gamma]} = I \cdot \mathcal{O}_K$ for some ideal $I \subseteq \mathcal{O}_F$. Then

$$\begin{aligned}
\left(\phi_1(\gamma - \overline{\gamma})\phi_2(\gamma - \overline{\gamma})\right)^2 &= N_{K/\mathbb{Q}}\left(\gamma - \overline{\gamma}\right) \\
&= N_{K/\mathbb{Q}}\left(\delta_{K/F}(\gamma)\right) \\
&= N_{F/\mathbb{Q}}(I)^2 \cdot N_{K/\mathbb{Q}}(\mathcal{D}_{K/F}) \qquad (9)
\end{aligned}$$

The different and discriminant are related by the formula [20, Cor. III.2.10, Pg. 197]

$$\Delta_K = \Delta_F^2 N_{K/\mathbb{Q}}\left(\mathcal{D}_{K/F}\right). \qquad (10)$$

The claim follows from combining Equation 9 and Equation 10 and taking square roots. □

Lemma 25. *Let f_1, f_2, P, P_0 be the polynomials from Equations (2)-(5). Then*

(i) $f_1 \in \mathbb{Z}[x_2, x_3, x_4]$

(ii) $f_2 \in \mathbb{Z}[x_3, x_4]$

(iii) $P \in \frac{1}{2}\mathbb{Z}[x_1, x_2, x_3, x_4]$

(iv) $P_0 \in \frac{1}{2}\mathbb{Z}[x_1, x_2, x_3, x_4]$.

Proof. It is straightforward from the definition of f_1, f_2 and the choice of basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ that $f_1 \in \mathbb{C}[x_2, x_3, x_4]$ and $f_2 \in \mathbb{C}[x_3, x_4]$. So it remains to check the domain of the coefficients.

The claims for f_1, P, and P_0 all follow directly from Lemma 23. For f_2, note that the coefficient of $x_i x_j$ is $\phi_1(\delta_i)\phi_2(\delta_j) + \phi_1(\delta_j)\phi_2(\delta_i)$, where $\delta_i = \alpha_i - \overline{\alpha}_i$. The claim for f_2 follows from Lemma 24 and the fact that

$$\phi_1(\delta_i)\phi_2(\delta_j) + \phi_1(\delta_j)\phi_2(\delta_i) = \phi_1(\delta_i + \delta_j)\phi_2(\delta_i + \delta_j) - \phi_1(\delta_i)\phi_2(\delta_i) - \phi_1(\delta_j)\phi_2(\delta_j).$$

□

Lemma 26. *f_2 is a integral bilinear quadratic form in x_3, x_4 with discriminant Δ_F.*

Proof. It is clear from the definition that f_2 is a homogeneous polynomial of degree 2, and by Lemma 25, $f_2 \in \mathbb{Z}[x_3, x_4]$. So it remains to calculate the discriminant.

Let $\delta_i = \alpha_i - \overline{\alpha}_i$. By definition,

$$\begin{aligned}
\operatorname{disc} f_2 &= \frac{\Delta_F^2}{\Delta_K}\left(\left(\phi_1(\delta_3)\phi_2(\delta_4) + \phi_2(\delta_3)\phi_1(\delta_4)\right)^2 - 4\phi_1(\delta_3)\phi_2(\delta_3)\phi_1(\delta_4)\phi_2(\delta_4)\right) \\
&= \frac{\Delta_F^2}{\Delta_K}\left(\phi_1(\delta_3)\phi_2(\delta_4) - \phi_2(\delta_3)\phi_1(\delta_4)\right)^2.
\end{aligned}$$

Now we compute

$$\begin{aligned}\Delta_K &= \det \begin{pmatrix} 1 & \phi_1(\alpha_2) & \phi_1(\alpha_3) & \phi_1(\alpha_4) \\ 1 & \phi_1(\alpha_2) & \phi_1(\overline{\alpha_3}) & \phi_1(\overline{\alpha}_4) \\ 1 & \phi_2(\alpha_2) & \phi_2(\alpha_3) & \phi_2(\alpha_4) \\ 1 & \phi_2(\alpha_2) & \phi_2(\overline{\alpha}_3) & \phi_2(\overline{\alpha}_4) \end{pmatrix}^2 \\ &= (\phi_1(\alpha_2) - \phi_2(\alpha_2))^2 \left(\phi_1(\delta_3)\phi_2(\delta_4) - \phi_2(\delta_3)\phi_1(\delta_4)\right)^2 \\ &= \Delta_F \left(\phi_1(\delta_3)\phi_2(\delta_4) - \phi_2(\delta_3)\phi_1(\delta_4)\right)^2.\end{aligned}$$

□

Next we prove the correctness of step 5 using our previous lemmas.

Lemma 27. *If (a_3, a_4) is outputted in step 5 of the algorithm in Section 3.2.1, then $f_2(a_3, a_4) = \pm 1$. Moreover, if $x_3 = a_3$, $x_4 = a_4$ is an integral solution to $f_2(x_3, x_4) = \pm 1$, then, given a large enough bound, step 5 will eventually output the pair (a_3, a_4).*

Proof. Following the notation from the algorithm, let $f_2(x_3, x_4) = ax_3^2 + bx_3x_4 + cx_4^2$. Recall from Lemma 26 that $a, b, c \in \mathbb{Z}$ and $b^2 - 4ac = \Delta_F$. Note that $\{a, (b + \sqrt{\Delta_F})/2\}$ is a $\mathbb{Q}$-basis for F. Here we are abusing notation by writing $\sqrt{\Delta_F}$ as an element of F. So we can write any $\sigma \in F$ as

$$\sigma = ax + \frac{b + \sqrt{\Delta_F}}{2} y,$$

for some $x, y \in \mathbb{Q}$. Then the norm of σ is

$$\mathrm{Norm}_{F/\mathbb{Q}}(\sigma) = \left(ax + \frac{b + \sqrt{\Delta_F}}{2} y\right)\left(ax + \frac{b - \sqrt{\Delta_F}}{2} y\right) = a\left(ax^2 + bxy + cy^2\right) = af_2(x, y).$$

Therefore $f_2(x, y) = \pm 1$ if and only if the corresponding σ has norm $\pm a$. Moreover, $x, y \in \mathbb{Z}$ if and only if σ lies in the ideal $I = a\mathbb{Z} + (b + \sqrt{\Delta_F})/2\mathbb{Z}$ (one can show this is an ideal using the fact that $b^2 - 4ac = \Delta_F$). Because $\mathrm{Norm}_{F/\mathbb{Q}}(I) = |a|$, it follows that $x_3 = x, x_4 = y$ is an integral solution to $f_2(x_3, x_4) = \pm 1$ if and only if $\sigma\mathcal{O}_F = I$. Therefore, we have a bijection between integral solutions to $f_2(x_3, x_4) = \pm 1$ and generators of I.

The claim follows as steps (5.1)-(5.3) enumerate all generators σ for the ideal I, and compute the associated integral solution to $f_2 = \pm 1$. □

Now we will find an explicit $\mathbb{Z}$-basis for the order $\mathbb{Z}[\pi, \overline{\pi}]$. This will allow us to write down a formula for $\mathrm{disc}\,\mathbb{Z}[\pi, \overline{\pi}]$ in terms of the coefficients of π with respect to the basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ for $\mathcal{O}_K$. We will use this formula to determine when $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$.

Lemma 28. *Let K be a quartic CM field and let $\pi \in \mathcal{O}_K$ be an Weil p-number. Then $B = \langle 1, \pi, \overline{\pi}, \pi^2 \rangle$ generates $\mathbb{Z}[\pi, \overline{\pi}]$ as a $\mathbb{Z}$-module.*

Proof. We will show that any power of π or $\overline{\pi}$ is contained in $\mathrm{Span}(B)$. The claim will follow because $\pi\overline{\pi} \in \mathbb{Z}$, so any product $\pi^i\overline{\pi}^j$ can be rewritten as sums of powers of π or $\overline{\pi}$. Because K is a quartic extension, we only have to show $\pi^3, \overline{\pi}^2, \overline{\pi}^3 \in \mathrm{Span}(B)$.

First we will show that $\overline{\pi}^2 \in \mathrm{Span}(B)$. Let F be the real quadratic subfield of K. Note that $\pi + \overline{\pi} \in \mathcal{O}_F$, so it has a characteristic polynomial in F of the form $x^2 + ax + b$ for some $a, b \in \mathbb{Z}$. It follows that

$$\begin{aligned}(\pi + \overline{\pi})^2 &= -a(\pi + \overline{\pi}) - b \\ \pi^2 + \overline{\pi}^2 &= -a\pi - a\overline{\pi} - b - 2p \\ \overline{\pi}^2 &= -\pi^2 - a\pi - a\overline{\pi} - b - 2p. \end{aligned} \tag{11}$$

Now recall that the characteristic polynomial of π in K is of the form $x^4 - cx^3 + dx^2 - cpx + p^2$ for some $c, d \in \mathbb{Z}$. Using the fact that $\overline{\pi} = p/\pi$, this shows that

$$0 = \pi^4 - c\pi^3 + d\pi^2 - cp\pi + p^2$$
$$\pi^3 = c\pi^2 - d\pi + cp - p\overline{\pi} \tag{12}$$
$$\overline{\pi}^3 = c\overline{\pi}^2 + d\overline{\pi} + cp + p\pi. \tag{13}$$

It follows from Equations (11)-(13) that $\overline{\pi}^2, \pi^3, \overline{\pi}^3 \in \mathrm{Span}(B)$. □

Lemma 29. *Let K be a quartic CM field and let ϕ_1, ϕ_2 be non-conjugate embeddings $K \hookrightarrow \mathbb{C}$. If $\gamma \in \mathcal{O}_K$, then*

$$\mathrm{disc}(1, \gamma, \overline{\gamma}, \gamma^2) = \left(\phi_1(\gamma + \overline{\gamma}) - \phi_2(\gamma - \overline{\gamma})\right)^4 \left(\phi_1(\gamma - \overline{\gamma})\phi_2(\gamma - \overline{\gamma})\right)^2.$$

Proof. Let $\beta_1 = 1, \beta_2 = \gamma, \beta_3 = \overline{\gamma}, \beta_4 = \gamma^2$. Then $\mathrm{disc}(1, \gamma, \overline{\gamma}, \gamma^2) = \det \mathrm{tr}\, \beta_i\beta_j$. Let $\gamma_i = \phi_i(\gamma)$. Because K is a CM field, complex conjugation commutes with embeddings into $\mathbb{C}$, so $\phi_i(\overline{\gamma}) = \overline{\gamma}_i$. Using this, we can compute $\mathrm{tr}\, \beta_i\beta_j$ in terms of γ_1, γ_2. For example:

$$\mathrm{tr}_{K/\mathbb{Q}}\, \beta_3\beta_4 = \mathrm{tr}_{K/\mathbb{Q}}\, \gamma^2\overline{\gamma} = \gamma_1^2\overline{\gamma}_1 + \gamma_2^2\overline{\gamma}_2 + \gamma_1\overline{\gamma}_1^2 + \gamma_2\overline{\gamma}_2^2$$

A straightforward computation shows that $\det \mathrm{tr}\, \beta_i\beta_j$, when viewed as a polynomial in the ring $\mathbb{Z}[\gamma_1, \gamma_2, \overline{\gamma}_1, \overline{\gamma}_2]$, factors into the desired form. □

We are now ready to prove the correctness of the algorithm.

Theorem 30. *If the algorithm of Section 3.2.1 outputs π, then π is a super-isolated Weil number. Moreover, for any fixed super-isolated Weil number π, if the algorithm is given $K = \mathbb{Q}(\pi)$ and a large enough bound, then it will eventually output π.*

Proof. We will use the same notation as in Section 3.2.1. Let $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ and let $\pi = \sum a_i\alpha_i$. A straightforward computation, using Lemma 23, shows that

$$\phi_1(\pi\overline{\pi}) = P(a_1, a_2, a_3, a_4) \pm P_0(a_1, a_2, a_3, a_4)\sqrt{\Delta_F}.$$

It follows that π is a Weil p-number for a prime p if and only if the following hold:

(i) $P_0(a_1, a_2, a_3, a_4) = 0$

(ii) $P(a_1, a_2, a_3, a_4)$ is prime.

Next we will show that if (i) holds, then $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ if and only if the following hold:

(iii) $f_1(a_1, a_2, a_3, a_4) = \pm 1$

(iv) $f_2(a_1, a_2, a_3, a_4) = \pm 1$.

By Lemma 28, $B = \{1, \pi, \overline{\pi}, \pi^2\}$ spans $\mathbb{Z}[\pi, \overline{\pi}]$ as a $\mathbb{Z}$-module. Therefore $\mathbb{Z}[\pi, \overline{\pi}]$ is an order in K if and only if $\mathrm{disc}\, B \neq 0$, in which case B is basis for $\mathbb{Z}[\pi, \overline{\pi}]$. Hence $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ if and only if $\mathrm{disc}\, B = \Delta_K$. By Lemma 29 and the definition of f_1, f_2,

$$\mathrm{disc}\, B = \Delta_K f_1(a_1, a_2, a_3, a_4)^4 f_2(a_1, a_2, a_3, a_4)^2.$$

By Lemma 25, f_1 and f_2 are integer polynomials, so $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ if and only if $|f_1(a_1, a_2, a_3, a_4)| = |f_2(a_1, a_2, a_3, a_4)| = 1$.

We have shown that π is a super-isolated Weil number if and only if properties (i)-(iv) hold. Because the algorithm enumerates integral tuples (a_1, a_2, a_3, a_4) satisfying these properties, this shows that every algebraic integer the algorithm outputs is a super-isolated Weil number.

For the second claim, suppose that $\pi = \sum a_i\alpha_i$ is a super-isolated Weil number. Then by property (iv), $x_3 = a_3$, $x_4 = a_4$ is an integral solution to Equation 6. By Lemma 27, for a large enough bound, the algorithm will eventually enumerate a_3, a_4 in step 5. Recall that a_1, a_2 are essentially determined from a_3, a_4 (see steps 6 and 7). That is, for any given solution a_3, a_4 to Equation 6, there are two pairs (a_1, a_2) such that (a_1, a_2, a_3, a_4) satisfies Equations (6)-(8). Both pairs are found by the algorithm, so the algorithm will eventually output π. □

3.2.3 Efficiency

Recall that the algorithm in Section 3.2.1 enumerates solutions $x_1 = a_1$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ to Equations (6)-(8). For each integer i, chosen in step 5.2, the algorithm found several (possibly non-integral) solutions, see steps (5)-(7). In this section, we will show that the algorithm can find all solutions (a_1, a_2, a_3, a_4) with $P(a_1, a_2, a_3, a_4) \leq N$, by checking at most $O(\log N)$ values of i.

To prove the claim, we first show that the value of $|a_4|$ grows exponentially with $|i|$, i.e. $\log |a_4| = \Omega(|i|)$. Then we will show that the function $P(x_1, x_2, x_3, x_4)$, when restricted to solutions to Equations (6)-(8), is essentially bounded below by $|x_4|$.

Remark 31. The reason we choose a_4 instead of a_3 is that some of the equations turn out to be simpler. The same argument could be made with a_3 instead.

Lemma 32. *There are computable positive constants C_1, C_2, with $C_2 > 1$, such that if the integer i is chosen as in step 5.2, and the pair (a_3, a_4), with $a_4 \neq 0$, is computed as in step 5.3, then*

$$|a_4| \geq C_1 \cdot C_2^{|i|}.$$

The constants C_1, C_2 depend only on the basis chosen in step 2 and the generator chosen in step 5.1.

Proof. We will keep the notation from the algorithm in Section 3.2.1. Recall how the pair (a_3, a_4) is constructed from i in step 5. First we found an algebraic integer $\sigma \in \mathcal{O}_F$ of the form $\sigma = \pm\epsilon^i\gamma$ where γ generates the ideal $I = a\mathbb{Z} + (b + \sqrt{\Delta_F})/2\mathbb{Z}$, and ϵ is a fundamental unit of F. The pair a_3, a_4 are the coefficients of σ with respect to the $\mathbb{Z}$-basis $\{a, (b + \sqrt{\Delta_F})/2\}$ for I.

Using the quadratic formula and the fact that $a_3, a_4 \in \mathbb{Z}$, one can show that $f_2(a_3, a_4) = \pm 1$ implies that $|a_3| \leq C_0|a_4|$ for some constant C_0 that depends only on f_2 (hence C_0 depends on the basis chosen in step 2). So

$$\begin{aligned}
\left(|a|C_0 + \frac{|b| + \sqrt{\Delta_F}}{2}\right)|a_4| &\geq |a_3||a| + |a_4|\frac{|b| + \sqrt{\Delta_F}}{2} \\
&\geq \max\left(\left|\phi_1(\gamma\epsilon^i)\right|, \left|\phi_2(\gamma\epsilon^i)\right|\right) \\
&\geq \min\left(\left|\phi_1\left(\gamma\right)\right|, \left|\phi_2\left(\gamma\right)\right|\right) \cdot \max(\left|\phi_1(\epsilon^i)\right|, \left|\phi_2(\epsilon^i)\right|). \\
&= \min\left(\left|\phi_1\left(\gamma\right)\right|, \left|\phi_2\left(\gamma\right)\right|\right) \cdot \max(\left|\phi_1(\epsilon)\right|, \left|\phi_2(\epsilon)\right|)^{|i|}
\end{aligned}$$

The last step follows from the fact that $\phi_1(\epsilon)\phi_2(\epsilon) = \pm 1$. □

Next we want to show that, for all integral solutions $x_1 = a_1$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ to Equations (6)-(8), the value of $P(a_1, a_2, a_3, a_4)$ is essentially bounded below by $|a_4|$. Recall that Equations 6 and 7 involve a choice of sign. To simplify our argument, we will first restrict to a specific set of signs.

Let A be the set of rational tuples $(a_1, a_2, a_3, a_4) \in \mathbb{Q}^4$ such that $x_1 = a_1, x_2 = a_2, x_3 = a_3, x_4 = a_4$ is a solution to the following equations:

$$f_1(x_2, x_3, x_4) = 1 \tag{14}$$

$$P_0(x_1, x_2, x_3, x_4) = 0 \tag{15}$$

$$x_3 = \frac{-b + \sqrt{b^2 - 4a(c - 1/x_4^2)}}{2a} x_4. \tag{16}$$

Equation 16 comes from solving $f_2(x_3, x_4) = 1$ for x_3 (recall that $f_2 = ax_3^2 + bx_3x_4 + cx_4^2$ for integers a, b, c). Therefore, every tuple in A is a solution to Equations (6)-(8) with the positive signs. Note that every integral solution to Equations (6)-(8) lies in a set defined in a way similar to A, only with a possibly different choice of signs.[7] Our arguments in the lemmas below will not depend on the choice of sign, so they will apply to any such set.

[7] There are a total of 8 choices of signs we could use to define A. These come from the three choices of signs: one in Equation 6, one in Equation 7, and one from the quadratic formula when solving Equation 6 for x_3. Every solution to Equations (6)-(8) lies in one of these 8 sets.

Lemma 33. *There exists an explicit function $P_4(x_4)$ such that for every $(a_1, a_2, a_3, a_4) \in A$,*

$$P(a_1, a_2, a_3, a_4) = P_4(a_4),$$

where P is the polynomial from Equation 4.

Proof. To prove the claim, we first find functions $g_1(x_4), g_2(x_4), g_3(x_4)$ such that for all tuples $(a_1, a_2, a_3, a_4) \in A$, $a_i = g_i(a_4)$ for $i = 1, 2, 3$. Then we will substitute the g_i's into the polynomial P in order to construct $P_4(x_4)$.

By definition, if

$$g_3(x_4) = \frac{-b + \sqrt{b^2 - 4a(c - 1/x_4^2)}}{2a} x_4,$$

then $a_3 = g_3(a_4)$ for all $(a_1, a_2, a_3, a_4) \in A$.

Next we will find g_2. Recall that $f_1(x_2, x_3, x_4)$ is a linear polynomial with a non-zero coefficient of x_2 (see step 6 in the algorithm in Section 3.2.1). So we can use Equation 14 to write x_2 as a linear function of x_3 and x_4. By substituting g_3 for x_3, we obtain a function g_2 which satisfies $a_2 = g_2(a_4)$ for all $(a_1, a_2, a_3, a_3) \in A$.

Now we will find g_1. Recall that $P_0(x_1, x_2, x_3, x_4) = f_1 x_1 + g$ for some $g \in \mathbb{Z}[x_2, x_3, x_4]$ (see step 7). By Equations 14 and 15, $a_1 = -g(a_2, a_3, a_4)$ for all $(a_1, a_2, a_3, a_4) \in A$. By replacing x_2, x_3 in $-g$ with g_2, g_3 respectively, we obtain a function $g_1(x_4)$ such that $a_1 = g_1(a_4)$ for all $(a_1, a_2, a_3, a_4) \in A$.

Let

$$P_4(x_4) = P(g_1(x_4), g_2(x_4), g_3(x_4), x_4).$$

Note that P_4 has the desired property because for all $(a_1, a_2, a_3, a_4) \in A$, we have that $g_i(a_4) = a_i$ for $i = 1, 2, 3$. □

Theorem 34. *The algorithm in Section 3.2.1 can find all super-isolated Weil p-numbers with $p \leq N$ in $O(\log N)$ steps. That is, for each quartic CM field K of class number 1, there is at least one set of choices that can be made in steps 2 and 3 such that the algorithm only needs to check $O(\log N)$ values of $|i|$ in step 5.2. Here the implicit constant depends on the choices made.*

Sketch of proof. By Theorem 30, the algorithm will eventually output any specific super-isolated Weil number given a large enough bound. Therefore, it is sufficient to show that the value of $P(a_1, a_2, a_3, a_4)$ in step 8 grows exponentially in $|i|$. From Lemma 32, we know that $\log |a_4| = \Omega(|i|)$, so it is sufficient to show that $P(a_1, a_2, a_3, a_4) = \Omega(|a_4|)$.

Recall that there are only 91 such fields. For each one, we computed the function P_4 from Lemma 33 after choosing some random values in steps 2 and 3. We found that $|P_4(x_4)| = \Omega(x_4^4)$. We repeated the calculations for every alternative definition of the set A from Lemma 33, and found the same result (this property seems to always hold in practice). Some details for the case of $K = \mathbb{Q}(\zeta_5)$ are given in Appendix A. We also used these calculations in the proof of Theorem 37 below.

Let (a_1, a_2, a_3, a_4) be any integral solution to Equations (6)-(8). Then $P(a_1, a_2, a_3, a_4) = P_4(a_4)$ for some P_4 (recall the definition of P_4 depended on the set A, so there are 8 possibilities for P_4). Since $|P_4(x_4)| = \Omega(x_4^4)$, it follows that $P(a_1, a_2, a_3, a_4) = \Omega(a_4^4)$. □

3.3 Examples

We found the following super-isolated Weil numbers by using the algorithm in Section 3.2.1. Both generate non-normal quartic CM fields.

Example 35.

$$\pi = \frac{225058681}{16}\left(\sqrt{-19 - 8\sqrt{2}}\right)^3 + \frac{1}{16}\left(-19 - 8\sqrt{2}\right) + \frac{6822363251}{16}\sqrt{-19 - 8\sqrt{2}} - \frac{4404669978983883573}{16}.$$

Here $p = \pi\overline{\pi} = 75785615717819865717549739169971883$ is a 116 bit prime, and $N = \mathrm{Norm}_{K/\mathbb{Q}}(\pi - 1)$ factors as 31 times a 227 bit prime. The associated surface is the jacobian of the following hyperelliptic curve over $\mathbb{F}_p$:

$$\begin{aligned} y^2 = {} & 51897490505362555469478 0x^6 + 11029353551173568371106 20x^5 + 99128729223802494055581 2x^4 \\ & + 47858824978662143433307 6x^3 + 13027320350528120169454 4x^2 + 19179534443912344652288x \\ & + 1373526256863485541624. \end{aligned}$$

Example 36.

$$\pi = \frac{701408733}{8}\left(\sqrt{-13-2\sqrt{5}}\right)^3 - \frac{1}{8}\left(-13-2\sqrt{5}\right) + \frac{12255108743}{8}\sqrt{-13-2\sqrt{5}} + \frac{18762798022945344405}{8}.$$

Here $p = \pi\overline{\pi} = 55006654632787769594536175901603367 93$ is a 123 bit prime, and $N = \mathrm{Norm}_{K/\mathbb{Q}}(\pi - 1)$ factors as 521 times a 236 bit prime. The associated surface is the jacobian of the following hyperelliptic curve over $\mathbb{F}_p$:

$$\begin{aligned} y^2 = {} & 31665417744816510942301668704748396 14x^6 + 15345286707227323909002017203965541 6x^5 \\ & + 43971111064283255537684871237699538 29x^4 + 41364117070458720261568476176805867 20x^3 \\ & + 80164631936087980207811880168364936 6x^2 + 39583038852808864368114843064346933 99x \\ & + 23036392538868222355374330027643234 59. \end{aligned}$$

3.4 Main result

Our main result is that Examples 35 and 36 are the only examples of super-isolated surfaces with near-prime order and cryptographic size.

Theorem 37. *Examples 35 and 36 are the only super-isolated abelian surfaces $A/\mathbb{F}_p$ with the property that*

$$\#A(\mathbb{F}_p) = cr \text{ where } c \leq 1000, \ r \text{ is prime, and } 2^{160} \leq r \leq 2^{512}. \tag{17}$$

Sketch of proof. We will show that if A is an abelian surface satisfying property (17), then the roots of the characteristic polynomial of the Frobenius endomorphism of A are super-isolated Weil p-numbers with $p \leq 2^{261}$. The claim then follows by running the algorithm in Section 3.2.1 long enough to find all super-isolated Weil p-numbers with $p \leq 2^{261}$.

Let A be an abelian surface over $\mathbb{F}_p$ satisfying property (17). Recall from Section 3.1 that $\#A(\mathbb{F}_p) = f(1)$, where f is the characteristic polynomial of the Frobenius endomorphism of A. Using the well-known Hasse bound, it is not hard to show that property (17) implies that A is simple, because a product of elliptic curves does not have near-prime order. Hence $f = h^e$ for some irreducible polynomial h, see Section 3.1. But as $f(1)$ is near-prime, we must have $e = 1$, i.e. f is irreducible. So by Corollary 19, every root π of f is a super-isolated Weil p-number in the quartic CM field $K = \mathbb{Q}(\pi)$ of class number 1.

Next we will show that property 17 implies that $p \leq 2^{261}$. This is similar to using the Hasse bound above. Since the roots of f are Weil p-numbers, it follows that $f(x) = x^4 + ax^3 + bx^2 + pax + p^2$ with $|a| \leq 4\sqrt{p}$ and $|b| \leq 6p$. So

$$r \geq \frac{p^2 - 4p^{3/2} - 6p - 4\sqrt{p} - 1}{1000}.$$

A straightforward calculation shows that this inequality, when combined with the bound $r \geq 2^{512}$, implies that $p \leq 2^{261}$.

The next part of the proof is computational. We used `Sage` to compute the implicit constants in Section 3.2.3 that are used to bound the number of steps the algorithm must take in order to enumerate all super-isolated Weil p-numbers with $p \leq 2^{261}$ (see Theorem 34). Some details for the case of $K = \mathbb{Q}(\zeta_5)$ are given in Appendix A. Our results show that there are 282 conjugacy classes of such Weil numbers. Only those given in Examples 35 and 36 satisfy the properties in the claim. The source code is available at https://sites.math.washington.edu/~tscholl2/super-isolated. □

Remark 38. The bound $c \leq 1000$ used above is arbitrary. The smaller c is the more efficient the cryptosystem will be. The three smallest values of c were 31, 521, and 73399.

Remark 39. Note that the surfaces in Examples 35 and 36 provide 113 and 116 bits of security respectively (i.e. half the bitlength of the largest prime dividing the order). Recent standards suggest using between 128 and 256 bits of security [19]. While 113 bits should be fine in many cases, our result shows that we can increase the security without increasing the size of p or c, which would reduce the efficiency.

Remark 40. After running the algorithm to search all super-isolated Weil p-numbers π with $100 \leq p \leq 2^{10000}$, there was only one conjugacy class such that $\mathrm{Norm}(\pi - 1)$ was prime. In that case, $p \approx 2^{740}$. This prime is too large to be useful in most practical applications.

A Details for $\mathbb{Q}(\zeta_5)$

In this section, we provide a detailed example of the algorithm in Section 3.2.1, for the field $\mathbb{Q}(\zeta_5)$. We also show how long the algorithm must run in order to enumerate all super-isolated Weil p-numbers with $p \leq 2^{261}$. We will use the notation from Section 3.2.1 and the methods from Section 3.2.3.

Let $K = \mathbb{Q}(\zeta_5)$. Recall that step 2 of the algorithm chooses a basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ for $\mathcal{O}_K$ such that $\{\alpha_1, \alpha_2\}$ form a basis for $\mathcal{O}_F$ where F is the maximal real subfield of K. In this case, $F = \mathbb{Q}(\sqrt{5})$. We choose

$$\alpha_1 = 1, \quad \alpha_2 = -\zeta_5^3 - \zeta_5^2 + 2, \quad \alpha_3 = -3\zeta_5^2 - 2\zeta_5^2 - 2, \quad \alpha_4 = -2\zeta_5^3 + 3\zeta_5^2 - \zeta_5 - 1.$$

Let ϕ_1, ϕ_2 be the embeddings $K \hookrightarrow \mathbb{C}$ defined by

$$\phi_1(\zeta_5) = e^{2\pi i/5}, \quad \phi_2(\zeta_5) = e^{4\pi i/5}.$$

For reference, $\phi_1(\alpha_2) = \frac{5+\sqrt{5}}{2}$ and $\phi_2(\alpha_2) = \frac{5-\sqrt{5}}{2}$.

Next we compute the polynomials defined in Equations (2)-(5):

$$\begin{aligned}
f_1 &= 2x_2 + 5x_3 - 2x_4 \\
f_2 &= x_3^2 + 9x_3x_4 + 19x_4^2 \\
P &= x_1^2 + 5x_1x_2 + \frac{15}{2}x_2^2 - \frac{3}{2}x_1x_3 + \frac{5}{2}x_2x_3 + 9x_3^2 - 2x_1x_4 - \frac{15}{2}x_2x_4 + \frac{3}{2}x_3x_4 + \frac{37}{2}x_4^2 \\
P_0 &= x_1x_2 + \frac{5}{2}x_2^2 + \frac{5}{2}x_1x_3 + \frac{11}{2}x_2x_3 - 2x_3^2 - x_1x_4 - \frac{7}{2}x_2x_4 - \frac{7}{2}x_3x_4 - \frac{9}{2}x_4^2.
\end{aligned}$$

The next step is to enumerate all solutions to the equation $f_2(x_3, x_4) = \pm 1$. We do this following the method laid out in step 5.

Write $f_2 = ax_3^2 + bx_3x_4 + cx_4^2$, and then choose a generator γ for the ideal $I = a\mathbb{Z} + ((b + \sqrt{\Delta_F})/2)\mathbb{Z}$. Because in this case $I = \mathcal{O}_F$, we will choose $\gamma = 1$. A fundamental unit for $\mathcal{O}_F$ is

$$\epsilon = -\zeta_5^3 - \zeta_5^2 - 1.$$

Now for each choice of sign and value of i we compute $\sigma = \pm\epsilon^i\gamma$ and write

$$\sigma = a_3a + a_4\frac{b + \sqrt{\Delta_F}}{2}$$

as in step 5.3.

The remaining steps of the algorithm are straightforward, so we will skip ahead to compute the bound on i in order to find all super-isolated Weil p-numbers with $p \leq 2^{261}$. We first compute the constants from Section 3.2.3.

Notice that $f_2(a_3, a_4) = \pm 1$ implies that

$$\begin{aligned} a_3 &= \frac{-ba_4 \pm \sqrt{(ba_4)^2 - 4a(ca_4^2 \pm 1)}}{2a} \\ &= \frac{-ba_4 \pm |a_4|\sqrt{\Delta_F \pm 4a/a_4^2}}{2a}. \end{aligned}$$

Therefore we can bound $|a_3|$ from above by

$$\begin{aligned} |a_3| &\leq \frac{|b| + \sqrt{\Delta_F + 4|a|}}{2|a|}|a_4| \\ &= 6|a_4| \end{aligned}$$

Next we want to bound $|a_4|$ from below by an exponential function in i. Following the proof of Lemma 32,

$$\begin{aligned} \min(|\phi_1(\gamma)|, |\phi_2(\gamma|) \max(|\phi_1(\epsilon)|, |\phi_2(\epsilon)|)^{|i|} &\leq \max\left(|\phi_1(\gamma\epsilon^i)|, |\phi_2(\gamma\epsilon^i)|\right) \\ &\leq |a_3||a| + |a_4|\frac{|b| + \sqrt{\Delta_F}}{2} \\ &= |a_3| + \frac{9+\sqrt{5}}{2}|a_4| \\ &\leq 6|a_4| + \frac{9+\sqrt{5}}{2}|a_4| \\ &\leq 12|a_4| \end{aligned}$$

Since $\gamma = 1$ and $\max(|\phi_1(\epsilon)|, |\phi_2(\epsilon)|) = \frac{1+\sqrt{5}}{2} \geq 3/2$, we have

$$|a_4| \geq \frac{1}{12}\left(\frac{3}{2}\right)^{|i|}.$$

Next we want to bound $P(a_1, a_2, a_3, a_4)$ from below in terms of $|a_4|$. We follow the same steps as in the proof of Lemma 33. For simplicity, we will assume that (a_1, a_2, a_3, a_4) is a solution to Equations (14)-(16). In our case, these equations are

$$\begin{aligned} 1 &= 2x_2 + 5x_3 - 2x_4 \\ 0 &= x_1 + 5x_2^2 + 11x_2x_3 - 4x_3^2 - 7x_2x_4 - 7x_3x_4 - 9x_4^2 \\ x_3 &= \frac{-9 + \sqrt{5 + 4/x_4^2}}{2}x_4 \end{aligned}$$

Note that integral solutions to these equations exist, for example, $x_1 = 115, x_2 = -45, x_3 = 17, x_4 = -3$. This solution comes from setting $i = 7$.

By solving each of these constraints in terms of x_4, we have

$$\begin{aligned} x_1 &= \frac{5}{8}x_4^2 + \frac{1}{8}\left(5\,x_4^2 + 28\,x_4\right)\sqrt{5 + \frac{4}{x_4^2}} - 33\,x_4 - 1 \\ x_2 &= -\frac{5}{4}\,x_4\sqrt{5 + \frac{4}{x_4^2}} + \frac{49}{4}\,x_4 + \frac{1}{2} \\ x_3 &= \frac{1}{2}\,x_4\sqrt{5 + \frac{4}{x_4^2}} - \frac{9}{2}\,x_4 \end{aligned}$$

Substituting these into the polynomial $P(x_1, x_2, x_3, x_4)$ as in the proof of Lemma 33, we have

$$P_4(x_4) = \frac{75}{32}\,x_4^4 + \frac{55}{16}\,x_4^2 + \frac{5}{32}\left(5\,x_4^4 + 4\,x_4^2\right)\sqrt{5 + \frac{4}{x_4^2}} + 1$$

In particular,

$$P_4(x_4) \geq \frac{75}{32} x_4^4$$

for all $x_4 > 0$.

We saw above that for each integer i, any associated pair (a_3, a_4) (as computed in step 5 of the algorithm in Section 3.2.1) satisfies

$$|a_4| \geq \frac{1}{12} \left(\frac{3}{2}\right)^{|i|}.$$

If the tuple happens to satisfy Equations (14)-(16), then

$$P(a_1, a_2, a_3, a_4) \geq \frac{75}{32} \left(\frac{1}{12} \left(\frac{3}{2}\right)^{|i|}\right)^4.$$

So in order to capture all super-isolated Weil p-numbers with $p \leq 2^{261}$ which satisfy the constraints above, we have to check all i with $|i| \leq 118$. The bound for other choices of signs in Equations (14)-(16) can be computed similarly.

References

[1] Paul T. Bateman and Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[2] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Peter Schwabe. Kummer strikes back: new DH speed records. In *Advances in cryptology—ASIACRYPT 2014. Part I*, volume 8873 of *Lecture Notes in Comput. Sci.*, pages 317–337. Springer, Heidelberg, 2014.

[3] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[4] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[5] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[6] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[7] Andreas Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Math. Comp.*, 71(238):729–742, 2002.

[8] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.*, 76(257):475–492, 2007.

[9] Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *LNCS*, pages 19–34. Springer, Berlin, 2000.

[10] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[11] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes. Elliptic curve cryptography: the serpentine course of a paradigm shift. *J. Number Theory*, 131(5):781–814, 2011.

[12] Neal Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.

[13] Stphane Louboutin and Ryotaro Okazaki. Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one. *Acta Arith.*, 67(1):47–62, 1994.

[14] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[15] Alfred Menezes and Edlyn Teske. Cryptographic implications of Hess' generalized GHS attack. *Appl. Algebra Engrg. Comm. Comput.*, 16(6):439–460, 2006.

[16] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[17] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[18] Andrea Miele and Arjen K Lenstra. Efficient ephemeral elliptic curve cryptographic keys. In *Information Security: 18th International Conference, ISC 2015, Trondheim, Norway, September 9-11, 2015, Proceedings*, volume 9290 of *LNCS*, pages 524–547. Springer International Publishing, 2015.

[19] National Institute of Standards and Technology. Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-4, 2013.

[20] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[21] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[22] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[23] Benjamin Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. volume 22, pages 505–529. 2009.

[24] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[25] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.

[26] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5)*, 2017. `http://www.sagemath.org`.

[27] Wenhan Wang. *Isolated Curves for Hyperelliptic Curve Cryptography*. PhD thesis, University of Washington, 2012.

[28] W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[29] William C. Waterhouse. Abelian varieties over finite fields. volume 2, pages 521–560, 1969.

[30] Ken Yamamura. The determination of the imaginary abelian number fields with class number one. *Math. Comp.*, 62(206):899–921, 1994.