Quantum Money from Class Group Actions on Elliptic Curves

Hart Montgomery
Linux Foundation
hart.montgomery@gmail.com

Shahed Sharif
CSU San Marcos
ssharif@csusm.edu

October 7, 2024

Abstract

We construct a quantum money/quantum lightning scheme from class group actions on elliptic curves over $\mathbb{F}_p$. Our scheme, which is based on the invariant money construction of Liu-Montgomery-Zhandry (Eurocrypt '23), is simple to describe. We believe it to be the most instantiable and well-defined quantum money construction known so far. The security of our quantum lightning construction is exactly equivalent to the (conjectured) hardness of constructing two uniform superpositions over elliptic curves in an isogeny class which is acted on simply transitively by an exponentially large ideal class group.

However, we needed to advance the state of the art of isogenies in order to achieve our scheme. In partcular, we show:

- An efficient (quantum) algorithm for sampling a uniform superposition over a cryptographically large isogeny class.
- A method for specifying polynomially many generators for the class group so that polynomial-sized products yield an exponential-sized subset of class group, modulo a seemingly very modest assumption.

Achieving these results also requires us to advance the state of the art of the (pure) mathematics of elliptic curves, and we are optimistic that the mathematical tools we developed in this paper can be used to advance isogeny-based cryptography in other ways.

1 Introduction

Quantum money is a way of implementing digital money where "banknotes" that represent the money are quantum states. The idea for quantum money was first sketched out by Wiesner [Wie83], and since then quantum money has captivated the quantum computing research community. In this work, we focus on *publicly verifiable* quantum money [Aar09], which means that any observer without privileged information can verify the correctness of the banknotes, and quantum lightning [Zha19], which guarantees that even the mint cannot cheat by producing duplicate banknotes.

Unfortunately, constructing publicly verifiable quantum money has proven to be rather elusive. Farhi, Gosset, Hassidim, Lutomirski, Nagaj, and Shor showed that, even with some natural modifications, Wiesner's quantum money scheme cannot be used to directly build a publicly verifiable scheme [FGH+10]. The first candidates for truly publicly verifiable quantum money were given by Aaronson [Aar09] and Aaronson and Christiano [AC12], and gave publicly verifiable quantum money constructions relative to quantum and classical oracles, respectively. Unfortunately, the proposed instantiations of oracles in both constructions were later broken [LAF+10] [CPDDF+19], casting doubt on the possibility that such oracles could be securely implemented in the real world. Zhandry's concrete construction of quantum lightning [Zha19] was also broken by Roberts [Rob21]. More recently, the lattice-based construction of Khesin, Lu, and Shor [KLS22] was broken by Liu, Montgomery, and Zhandry [LMZ23].

On the other hand, there are a handful of candidates have been proposed that have not been broken, including constructions from knots [FGH+12] and quaternion algebras [Kan18, KSS21]. In addition,

Zhandry [Zha19], as suggested by [BDS16], showed how to build publicly verifiable quantum money from quantum-secure indistinguishability obfuscation (iO). Unfortunately, none of these assumptions have received much cryptanalytic attention at all, and all known candidates of post-quantum iO [GGH15, BGMZ18, BDGM20, WW21] do not have strong connections to well-studied cryptographic assumptions.

Liu, Montgomery, and Zhandry recently showed a generic, oracle construction for quantum money that they called *invariant money* [LMZ23]. They showed a number of possible constructions, but all of these were either oracle constructions or schemes that were not known to be efficiently instantiable. In particular, they showed an uninstantiable construction from class group actions on elliptic curves. In particular, they mention how invariant money could potentially be instantiated from isogenies. However, they also comment, "We do not know if it is even possible to instantiate such a scheme, as it would likely require new ideas in isogeny-based cryptography."

Very recently, Zhandry [Zha24] showed how to build a construction of quantum money from regular group actions that was loosely based on the generic construction of [LMZ23]. While Zhandry's construction was the first instantiable construction from group actions, it unfortunately resorts to nonstandard assumptions that seem significantly stronger than the assumptions used in the invariant money construction would be for an instantiable construction.

1.1 Our Contributions

In this work, we prove new results in isogeny-based cryptography necessary to build quantum money from the invariant money framework of [LMZ23]. We use these results to build a new quantum money scheme based on class group actions on elliptic curves, sharing some features with a proposal in [LMZ23]. Rather than come up with a new verification algorithm like that of Zhandry [Zha24], we advance the state of the art in the mathematics of elliptic curves, which enables us to build a very simple construction with simple (although still non-standard) assumptions.

Our quantum money scheme is conceptually very simple (modulo the new mathematical techniques required for its construction) and has an extremely easy to state security assumption. For instance, for quantum lightning, the scheme is exactly as secure as the problem of sampling two uniform superpositions over all elliptic curves over $\mathbb{F}_p$ with N points, for some N corresponding to elliptic curves with large class group. We also show that this new assumption is hard assuming that it is hard to compute isogenies between random isogenous elliptic curves (which is a standard assumption in cryptography at this point) and a quantum knowledge assumption similar to the one proposed recently by Zhandry [Zha24].

Our quantum money/lightning scheme is the first fully instantiable construction with a simple, offline (albeit quantum) security assumption. We also believe it is the simplest scheme proposed so far, and the one that rests on assumptions that are closest to traditional cryptographic security assumptions.

To enable such a simple scheme with a very nice security assumption, we advance the state of the art in elliptic curve mathematics and algorithms. In particular, for the minting algorithm to be efficient, it is necessary that a random elliptic curve mod p has non-negligible probability of having large associated class group. Previous work has either relied on heuristic assumptions, or worked exclusively with supersingular elliptic curves. In our work, we give new explicit lower bounds on the number of elliptic curves whose endomorphism ring has large discriminant, which together with a result of Tatuzawa show that at least 14% of elliptic curves mod p have endomorphism ring with exponentially large class group. We also, to our knowledge, for the first time apply a heuristic model due to Erdös-Rényi on encodings of class group elements.

Heuristics on sizes of class groups and efficiency of encodings for class groups are ubiquitous in isogeny-based cryptography. Consequently our formalization of these heuristics should find other uses in cryptography and mathematics outside of quantum money.

1.2 Other Related Work

Quantum money has been a key primitive in quantum computing, especially as quantum money and quantum lightning are closely tied to numerous other areas in quantum computing. For instance, the first message in

the quantum key distribution protocol of Bennet and Brassard [BB87] is just a banknote in Wiesner's quantum money scheme. Recent works on copy protection [ALL+21, CLLZ21] [LLQZ22] require at a minimum a computational assumption that implies quantum money.[1]

In the isogeny realm, our work makes precise estimates used for parameter selection in CRS-style cryptosystems. Previous work (for example [Cou06], [RS06], [DKS18]) relies completely on heuristics that imply a randomly chosen elliptic curve mod p will have large associated class group. Those heuristics are made precise here. We also show that, under a very plausible heuristic assumption, with overwhelming probability every element of the class group has a compact encoding.

1.3 Outline

The rest of this paper proceeds as follows. In Section 2, we provide a brief technical overview of our construction and new isogeny results. We hope this enables the reader to understand our ideas at a high level. Then, in Section 3, we provide preliminary material. In Section 4, we build the mathematical tools we need for our constructions. We note this section utilizes math that is outside the scope of knowledge of most cryptographers, but we do our best to make it as accessible as possible. We then present our full algorithm for sampling a superposition of elliptic curves in Section 5 and our algorithm for verifying these superpositions in Section 6. We then have a proof that our superposition verification algorithm is correct in Section 7. This is somewhat analogous to a similar proof in [LMZ23], although our proof is much more detailed than theirs. We finally present our full quantum money construction in Section 8.

In Section 9, we prove the security of our quantum money scheme. In Section 10, we present some additional number theory background that will be useful for readers that aren't as familiar with mathematics to use as reference. Finally, in Section 11, we give evidence for an Assumption 4.19, which underlies our verification algorithm.

2 Technical Overview

In this section we explain our main results and contributions at a high level. We begin by giving an overview of the new mathematical tools that are needed for its construction. We then outline our new quantum money scheme.

2.1 New Techniques and Facts on Elliptic Curves

In [LMZ23], it is stated that "generating superpositions over X, where X is the set of all elliptic curves with some (even polynomially likely) property seems difficult. In fact, we do not even know how to generate a uniform superposition over all elliptic curves efficiently." Our minting algorithm solves this problem by first efficiently generating a uniform superposition over all elliptic curves, by encoding elliptic curves as pairs (j, b), where j is the j-invariant and b is *twisting data*. We then show how to efficiently generate the superposition over a random exponentially large isogeny class. Note that we believe generating a superposition over a *specified* exponentially large isogeny class is difficult, and indeed the security of our scheme depends on this being the case.

Passing from the uniform superposition over all elliptic curves over a particular finite field to a superposition over a large isogeny class is accomplished by an explicit estimate on sizes of class groups associated to elliptic curves. The previous literature either restricts to isogeny classes of supersingular elliptic curves (which constitute a negligible fraction of all elliptic curves mod p), or relies on heuristics stating that the class group associated to a random elliptic curve mod p has size $O(\sqrt{p})$. We make these heuristics precise by focusing on elliptic curves whose Frobenius discriminant (that is, the discriminant of the characteristic polynomial of Frobenius) is both square-free and $\geq 3p$. We show that for $p > 2^{63}$, at least 14% of elliptic curves mod p have such a Frobenius discriminant. We then use Tatuzawa's effective version of Siegel's Theorem [Tat51] to obtain the following:

[1] This holds true even for certain weaker versions such as copy *detection*, also known as infinite term secure software leasing.

Corollary 2.1. Let $p > 2^{63}$ be prime. Given an ordinary elliptic curve $E/\mathbb{F}_p$, let $\mathcal{O}$ be $\mathrm{End}(E)$. If an elliptic curve E is drawn from either the distribution $\mathscr{D}_p$ or the distribution $\mathscr{U}_p$, then with probability at least 14%, the class group of $\mathcal{O}$ and the isogeny class of E both have size at least

$$0.089\frac{\sqrt{p}}{\log p},$$

Here, $\mathscr{U}_p$ is the uniform distribution on elliptic curves, and $\mathscr{D}_p$ is a related distribution defined in §3.3.

In addition to [Tat51], the proof of Corollary 4.14 relies on statistical analysis of the trace of Frobenius due to Murty-Prabhu [MP19b], and statistical analysis of the values of $4p - t^2$, $1 \leq t < \sqrt{p}$, using methods of Friedlander-Iwaniec [FI10].

Finally, we give a new treatment of computations in class groups. Typically, one cannot directly compute ideals coming from random ideal classes, since these ideals can have exponentially large generators. Instead, one attempts to express ideal classes as products of prime ideals with small norm. By treating small norm prime ideals as random elements in the class group, we use results of Erdös-Rényi to show that with all but negligible probability, every ideal class can be represented by a product of distinct prime ideals of small norm; see §4.4 and §4.5.

2.2 Quantum Money from Class Group Actions on Elliptic Curves

As we have alluded before, our scheme generally falls into the invariant framework of [LMZ23]. However, other than the obvious choice of using isogeny classes (determined by the number of points on elliptic curves ($\#E(\mathbb{F}_p)$) as the invariant, essentially every other choice we make deviates from the suggestions of [LMZ23] for implementing invariant money using class group actions on elliptic curves, and, as we have previously mentioned, our scheme accomplishes or circumvents some tasks they find difficult or impossible.

Recall that, informally speaking, a (public key) quantum money scheme is a tuple of algorithms $(\mathsf{Gen}, \mathsf{Ver})$ where Gen creates a quantum money state $|\psi\rangle$ which we refer to as a banknote and a serial number σ, and Ver takes as input a banknote $|\psi\rangle$ and a serial number σ and outputs 0 or 1, depending on whether or not the quantum money state is valid.

We say that a money scheme satisfies *quantum money unforgeability* if, given a random valid banknote and serial number pair $(|\psi\rangle, \sigma)$ it is hard to generate *two* banknotes $|\psi'\rangle, |\psi''\rangle$ that both verify with serial number σ. A scheme constitutes secure quantum lightning if it is hard for an adversary to find two states $|\psi'\rangle, |\psi''\rangle$ that both verify for *any* serial number σ. We formally define quantum money and quantum lightning in §3 and, for familiar readers, note that we use the "mini-scheme" definition from [AC12].

Our Construction. For an elliptic curve E, let t be the trace of Frobenius acting on E, and define the *Frobenius discriminant* to be $\Delta_{\mathrm{Fr}}(E) = 4p - t^2$. (This is the negative of the usual definition.) Note that Δ in the elliptic curve literature designates the discriminant of E itself; that is, if E is given by $y^2 = x^3 + ax + b$, the discriminant is $4a^3 + 27b^2$. We use Δ_{Fr} exclusively for the Frobenius discriminant.

Suppose we let $\mathscr{E}_{\mathsf{sf},3p}$ represent the set of isomorphism classes of elliptic curves E over $\mathbb{F}_p$ for prime p with $\Delta_{\mathrm{Fr}}(E) \geq 3p$ and square-free, and let $\mathcal{I}_N$ denote the set of elliptic curves over $\mathbb{F}_p$ with N points. Recall that two elliptic curves over $\mathbb{F}_p$ are isogenous if and only if they have the same number of points.

Our construction at a high level works as follows:

Money States: a valid quantum money state is a uniform superposition over a single isogeny class in $\mathscr{E}_{\mathsf{sf},3p}$.

Gen**:** To generate a money state, at a high level we do the following:

1. Sample a uniform superposition of elliptic curves in $\mathscr{E}_{\mathsf{sf},3p}$, getting a state $|\psi\rangle = \sum |E\rangle$.
2. In superposition, compute, in an adjacent register, the number of points in $|E\rangle$ using Schoof's algorithm.

3. Measure this new adjacent register and denote its value as N.

4. Output the tuple $(|\psi\rangle, N)$ as the money state. Note that $|\psi\rangle$ will have been altered by the measurement.

We note that sampling such a superposition as we do in step (1) was previously unknown and listed as an open problem in [LMZ23], and it requires new results in number theory to solve; namely, we require precise lower bounds on the proportion of elliptic curves with $\Delta_{\text{Fr}}(E)$ large and square-free. This follows from our mathematical work that we explained earlier in this overview.

Ver: Let $|\mathcal{I}_N\rangle := \frac{1}{\sqrt{\#\mathcal{I}_N}} \sum_{E \in \mathcal{I}_N} |E\rangle$. In other words, $|\mathcal{I}_N\rangle$ is the state corresponding to a uniform superposition over all elliptic curves with N points. Our goal, similar to [LMZ23], is to compute an approximation of the projection-valued measure $V_N = |\mathcal{I}_N\rangle \langle \mathcal{I}_N|$.

To do this, we take a similar approach as both [LMZ23] and [FGH+12]. We simulate a (invertible) random walk in superposition over the isogeny class group and continually check to see if the state has changed using projection-valued measures. Intuitively, correct money states will not change when we compute invertible maps on the state since these maps will map uniform superpositions to uniform superpositions. On the other hand, most incorrect money states will have changed substantially by such a walk. For instance, a classical state consisting of a single elliptic curve will likely be completely different after a random walk and thus fail verification.

While our verification algorithm closely resembles that of the invariant money in [LMZ23] at a high level, we emphasize that we need substantially new techniques to make it work. Most notably, to our knowledge the fact that a random elliptic curve has large associated class group with non-negligible probability has never been formally shown.

Security. The security of our construction is based on a simple assumption:

Definition 2.1. The Elliptic Curve Superposition Collision Problem ($ECSCP_p$): The prime p is fixed. Create two (possibly entangled) quantum states that are each negligibly far from the superposition of all elliptic curves over $\mathbb{F}_p$ in some isogeny class with Frobenius discriminant $\Delta_{\text{Fr}} \geq 3p$ and square-free.

We justify below why mathematicians believe this to be a hard problem. An astute reader will note that this security assumption is tied very closely to our scheme itself, and a reduction is simple. This is true—see Section 9 for the formal reduction—but we believe this to be a positive facet of our construction, in the same vein as the fact that the security of ElGamal encryption trivially following from the DDH assumption is a positive of that scheme, too.

[LMZ23] and [Zha24] argue that their constructions are secure using quantum assumptions of knowledge, and we can actually argue that not just our construction but the security assumption of our construction that we informally mentioned above is secure using assumptions of knowledge. As in [LMZ23] and [Zha24], we use two problems to prove the security of the $ECSCP_p$. First, we assume that it is hard to compute isogenies between random isogenous elliptic curves (the group action discrete log problem [ADMP20] over isogeny class groups). Second, we make a quantum assumption of knowledge: we assume that if there exists an adversary that breaks our main assumption (generating two superpositions) with non-negligible probability, we assume that there also exists some adversary that breaks our main assumption with similar probability from whose state "paths" (isogenies) between elliptic curves that it uses can be extracted. This is a relatively new type of assumption and we defer to [Zha24] for an extensive discussion on this sort of quantum knowledge assumption.

Construction Rationale. An adversary can efficiently fabricate money states if they can solve the group action discrete log problem for ideal classes acting on elliptic curves; fortunately, this problem is believed to be hard. But the hardness requires that the ideal class group is large. By Tatuzawa's estimate [Tat51], with overwhelming probability it is sufficient that $\Delta_{\text{Fr}}(E)$ be large for any elliptic curve E in the isogeny class. Thus we choose only isogeny classes for which $\Delta_{\text{Fr}} \geq 3p$. (Note that as E varies over elliptic curves mod p,

by the Hasse-Weil bounds $\Delta_{\mathrm{Fr}}(E)$ varies between 0 and $4p$.) Finally, it may happen that the isogeny class is a disjoint union of sets, each acted upon by different a class group corresponding to a different choice of endomorphism ring inside a given imaginary quadratic field (for instance, elliptic curves with endomorphism ring isomorphic to $\mathbb{Z}[\sqrt{-3}]$ along with elliptic curves with endomorphism ring isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$). We introduce a square-freeness condition to guarantee that the entire isogeny class forms a single homogeneous space.

Comparison to Zhandry's Scheme [Zha24]. Zhandry's recent quantum money construction is also loosely based on the invariant money construction in [LMZ23]. However, his construction turns out to be very different from ours. Zhandry makes a very nice observation that the Fourier domain can be useful for creating verifiable quantum states over group actions and builds a quantum lightning scheme based on this observation. On the other hand, our construction is more closely tied in nature to the invariant money scheme itself, although we need to solve or formalize several open problems in the mathematics of elliptic curves in order to make the scheme work.

We also note that Zhandry's assumptions are more complicated and seemingly stronger than ours: he proves his scheme secure in two different ways: one way uses what he calls the "D2X" assumption, which is an interactive assumption that requires a quantum oracle, and the other uses a quantum knowledge assumption. On the other hand, we can prove our scheme secure using a simple, noninteractive (albeit quantum) assumption, and we can prove this assumption secure using a simpler knowledge assumption as compared to Zhandry.

3 Definitions

In this section we provide basic definitions. For our quantum notations and definitions, we mostly borrow from and mimic [LMZ23].

Basic Cryptographic Notation. When we say a function is *negligible*, we mean that it is (asymptotically) smaller than $\frac{1}{f(\lambda)}$ for any polynomial f and security parameter λ. When we say a function is non-negligible, we mean that there is some polynomial function f for which the function grows (asymptotically) faster than $\frac{1}{f(\lambda)}$ for security parameter λ.

3.1 Quantum Specifics

We attempt to avoid any complicated quantum specifics. For general background and notation on quantum computing, we highly recommend [NC10].

Notation. Following [LMZ23], for quantum notation, we denote $|\cdot\rangle$ as the notation for a pure state and $|\cdot\rangle\langle\cdot|$ for its density matrix. ρ denotes a general mixed state. We let "$\dagger$" denote the conjugate transpose.

Definition 3.1. A *projection-valued measure* on a Hilbert space $\mathcal{H}$ is a set of outcomes $i \in M$ and, for each outcome, a positive semi-definite matrices $\mathbf{P}_i$, such that:

1. $\sum_M \mathbf{P}_i = \mathbf{I}$,
2. each $\mathbf{P}_i$ is Hermitian,
3. $\mathbf{P}_i^2 = \mathbf{P}_i$ and $\mathbf{P}_i = \mathbf{P}_i^\dagger$, and
4. for $i \neq j \in M$, $\mathbf{P}_i\mathbf{P}_j = 0$.

We say that the probability of obtaining output i on a pure state $|\psi\rangle$ is just $\langle\psi|\mathbf{P}_i|\psi\rangle$, with the measured state collapsing to $\frac{\mathbf{P}_i|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_i|\psi\rangle}}$; the analogous result for a mixed state is defined in the natural way using the trace.

For simplicity, we will abuse notation and refer to a single PVM operator $\mathbf{P}_i$ as a measurement, and the complementary operator $\mathbf{I}-\mathbf{P}_i$ will be implicit. In this case, a "successful" measurement on a state $|\psi\rangle$ will result in the output $\frac{\mathbf{P}_i|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_i|\psi\rangle}}$; we will typically be less concerned about the output of "failed" measurements.

3.2 Quantum Money and Quantum Lightning

Here, we define public key quantum money and quantum lightning. We use the definitions of [LMZ23] verbatim. As they do, following Aaronson and Christiano [AC12], we will only consider so-called "mini-schemes", where there is only a single banknote.

Both quantum money and quantum lightning share the same syntax and correctness requirements. There are two quantum polynomial-time algorithms $\mathsf{Gen}, \mathsf{Ver}$ such that:

- $\mathsf{Gen}(1^\lambda)$ samples a classical serial number σ and a quantum state $|\psi\rangle$.
- $\mathsf{Ver}(\sigma, |\psi\rangle)$ outputs a bit 0 or 1, and, if the output bit is 1, also outputs a state $|\psi'\rangle$.

Definition 3.2. We say that our quantum money scheme is *correct* if there exists a negligible function negl such that, for any polynomially sized integer i, we have $\Pr[\mathsf{Ver}^i(\mathsf{Gen}(1^\lambda))] \geq 1-\mathsf{negl}(\lambda)$. In other words, a correctly generated money state can be verified any polynomial number of times and verification will still pass.

Where public key quantum money and quantum lightning differ is in security. The differences are analogous to the differences between one-way functions and collision resistance.

Definition 3.3 (Quantum Money Unforgeability)**.** $(\mathsf{Gen}, \mathsf{Ver})$ is *secure public key quantum money* if, for all quantum polynomial-time A, there exists a negligible negl such that A wins the following game with probability at most negl:

- The challenger runs $(\sigma, |\psi\rangle) \leftarrow \mathsf{Gen}(1^\lambda)$, and gives $\sigma, |\psi\rangle$ to A.
- A produces a potentially entangled joint state $\rho_{1,2}$ over two quantum registers. Let ρ_1, ρ_2 be the states of the two registers. A sends $\rho_{1,2}$ to the challenger.
- The challenger runs $b_1 \leftarrow \mathsf{Ver}(\sigma, \rho_1)$ and $b_2 \leftarrow \mathsf{Ver}(\sigma, \rho_2)$. A wins if $b_1 = b_2 = 1$.

Definition 3.4 (Quantum Lightning Unforgeability)**.** $(\mathsf{Gen}, \mathsf{Ver})$ is *secure quantum lightning* if, for all quantum polynomial-time A, there exists a negligible negl such that A wins the following game with probability at most negl:

- A, on input 1^λ, produces and sends to the challenger σ and $\rho_{1,2}$, where $\rho_{1,2}$ is a potentially entangled joint state over two quantum registers.
- The challenger runs $b_1 \leftarrow \mathsf{Ver}(\sigma, \rho_1)$ and $b_2 \leftarrow \mathsf{Ver}(\sigma, \rho_2)$. A wins if $b_1 = b_2 = 1$.

In summary, the difference between quantum lightning and quantum money is therefore that in quantum lightning, unclonability holds, even for adversarially constructed states.

3.3 Elliptic curves

Consider a large prime p. We represent isomorphism classes of elliptic curves over $\mathbb{F}_p$ by pairs $(j, b) \in \mathbb{F}_p \times \mathbb{Z}$, where $b \in \{0, 1\}$ except in the following cases:

- If $j \equiv 1728 \mod p$ and $p \equiv 1 \pmod 4$, then $0 \leq b \leq 3$.
- If $j \equiv 0 \mod p$ and $p \equiv 1 \pmod 3$, then $0 \leq b \leq 5$.

Fix $\alpha \in \mathbb{F}_p$ a quadratic nonresidue. When $j \neq 0, 1728$, define the elliptic curve associated to the pair (j, b) to be given by

$$y^2 = x^3 + \frac{3j\alpha^{2b}}{j - 1728}x + \frac{2j\alpha^{3b}}{j - 1728}.$$

If $j = 1728$, define (j, b) to be given by

$$y^2 = x^3 + \alpha^b x.$$

If $j = 0$ and $p \equiv 1 \pmod 3$, we require that α be both a quadratic and a *cubic* nonresidue. Then (j, b) is given by

$$y^2 = x^3 + \alpha^b.$$

There is a bijection between pairs (j, b) and $\mathbb{F}_p$-isomorphism classes of elliptic curves; see [Sil09, Cor. X.5.4.1]. In the literature, j is known as the *j-invariant* of the elliptic curve, and b enumerates *twists* of elliptic curves with given j.

Definition 3.5. Let $\mathscr{U}_p$ denote the uniform probability distribution on isomorphism classes of elliptic curves over $\mathbb{F}_p$, given by uniformly randomly choosing a pair (j, b) as above.

There are many statistical results in the literature which refer to a different distribution $\mathscr{D}_p$, defined as follows.

Definition 3.6. We say $(a, b) \in \mathbb{F}_p^2$ is a *Weierstrass pair* if $4a^3 + 27b^2 \neq 0$. We associate to the Weierstrass pair the elliptic curve given by $y^2 = x^3 + ax + b$. The *Weierstrass distribution* $\mathscr{D}_p$ is the probability distribution on isomorphism classes of elliptic curves over $\mathbb{F}_p$ induced by the uniform distribution on Weierstrass pairs (a, b).

Note that there are exactly p pairs (a, b) for which $4a^3 + 27b^2 = 0$: when $-3a$ is a quadratic residue, there are 2 values for b, plus the pair $(0, 0)$ yields $2 \cdot \frac{p-1}{2} + 1 = p$. Thus there are $p^2 - p$ pairs (a, b) yielding elliptic curves.

Looking ahead, in Lemma 4.11 we show that the distance between $\mathscr{U}_p$ and $\mathscr{D}_p$ is at most $2/p$, and hence is negligible.

Definition 3.7. For an elliptic curve $E/\mathbb{F}_p$, let $t = t(E) = p + 1 - \#E(\mathbb{F}_p)$ be the *trace of Frobenius* on E, let $\frac{t}{2\sqrt{p}}$ be the *normalized trace*, let $\Delta_{\mathrm{Fr}} := \Delta_{\mathrm{Fr}}(E)$ be $4p - t^2$ the *Frobenius discriminant*, let $K = K(E) = \mathbb{Q}(\sqrt{-\Delta_{\mathrm{Fr}}})$, and let $D = D(E)$ be the discriminant of K. Let $\mathscr{E}_{\mathsf{sf},3p}$ be the set of elliptic curves E over $\mathbb{F}_p$ such that $\Delta_{\mathrm{Fr}}(E) \geq 3p$ and $\Delta_{\mathrm{Fr}}(E)$ is square-free.

The trace t is an $\mathbb{F}_p$-isogeny invariant of E, and hence an invariant of the isomorphism class of E. Thus the derived invariants Δ_{Fr} and D depend only on the isomorphism class of E, not on the equation used to define E. Thus by abuse of notation, we write $E \in \mathscr{E}_{\mathsf{sf},3p}$ to mean that the isomorphism class of E is in $\mathscr{E}_{\mathsf{sf},3p}$.

Definition 3.8. Given an imaginary quadratic field K with discriminant D, let $\mathscr{O}_K$ be the ring of integers of K, and define the *Bach generating set* B_K to be the set of ideal classes of unramified primes $\mathfrak{l}$ of $\mathscr{O}_K$ with $N(\mathfrak{l}) < 6(\log D)^2$.

Bach [Bac90, p. 376] showed that, assuming GRH, B_K generates $\mathrm{Cl}(\mathscr{O}_K)$.

4 Isogeny Building Blocks

In this section we build the isogeny-related tools we will need for our quantum money construction. Some are already known, some have been folklore (but, to our knowledge, never formalized), and some are new. For example, the prior isogeny literature uses the heuristic that the size of the class group is proportional to $\sqrt{D}$, where D is the discriminant of $\mathrm{End}(E) \subset K$; in fact, the heuristic is sometimes made by precise by noting that the constant of proportionality is given by a certain infinite series depending on D. While this suffices if the elliptic curve E is fixed, it is not strong enough to give bounds across large sets of elliptic curves where D varies. In §4.1 we give, to our knowledge, the first precise lower bounds for the number of elliptic curves mod p having large class groups—see Corollary 4.14. As a consequence for our protocol, we will obtain that minting is efficient, and that forgery attacks which rely on solving the isogeny problem are hard.

Ideal classes are typically encoded as products of prime ideals with small norm. After giving an algorithm for enumerating these prime ideals, we give a new analysis for the effectiveness of these encodings in §4.4 and §4.5, specifically by proving an eigenvalue bound for the adjacency matrix of the associated Cayley graph in Prop. 4.22. Our quantum money verification algorithm utilizes the class group action on elliptic curves, and the eigenvalue bound guarantees that verification is efficient.

The results in this section often use number theory that is new to the cryptography literature; while this enables proofs of new results, there is no easy way to present this material to readers who do not have the requisite background in mathematics. However, we have done our best to make the mathematics readable to cryptographers and have also summarized the necessary number theory in Section 10. We encourage readers who are unfamiliar with the number theory to read that section, which is near the end of the paper.

4.1 Probability of Large Isogeny Class

The goal of this section is to prove Corollary 4.14, which shows that for large p, a random elliptic curve belongs to an exponentially large isogeny class with probability $\geq 14\%$.

Our estimate will be accomplished in three steps:

- In Theorem 4.1, we compute the probability that a random elliptic curve E has Frobenius discriminant in a specified range.
- We determine how likely a random number of the form $4p - t^2$ is square-free in Theorem 4.9, and combine this with Theorem 4.1 to obtain, in Corollary 4.12, that a random elliptic curve is in $\mathscr{E}_{\mathsf{sf},3p}$ with probability $\geq 14\%$.
- In Corollary 4.14, we use a result of Tatuzawa to show that for elliptic curves in $\mathscr{E}_{\mathsf{sf},3p}$, the size of the associated class group is at least $0.089\dfrac{\sqrt{p}}{\log p}$.

In the next result, we use the Weierstrass representation of elliptic curves, so a pair $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ corresponds to the elliptic curve $y^2 = x^3 + ax + b$.

Theorem 4.1. *Let $I \subset [-1, 1]$ be an interval, and let $\mu_{ST}(I) = \frac{2}{\pi}\int_I \sqrt{1 - X^2}\, dX$. Let $N_I(p)$ be the number of elliptic curves over $\mathbb{F}_p$, encoded as pairs (a, b) with $4a^3 + 27b^2 \neq 0$, with normalized Frobenius trace $\frac{t}{2\sqrt{p}} \in I$. Then*

$$\left|\frac{N_I(p)}{p^2} - \mu_{ST}(I)\right| \leq \frac{8}{3p^{1/4}} + \frac{4}{3p^{1/2}} + + \frac{4}{p^2} + \frac{4}{p^{9/4}} + \frac{4\log p}{p^{5/2}}.$$

The measure μ_{ST} is known as the *Sato-Tate measure*.

Proof. Birch [Bir68] showed that

$$\lim_{p\to\infty}\left|\frac{N_I(p)}{p^2} - \mu_{ST}(I)\right| = 0.$$

An asymptotic error bound for $|N_I(p)/p^2 - \mu_{ST}(I)|$ is given in [MP19b]; we follow that proof to compute the explicit constant. Our notation follows that of [MP19b], with one exception. Suppose that $I = [x_0, x_1] \subset [-1, 1]$, and define $J = [\alpha, \beta] \subset [0, 1]$ where $\cos \pi\alpha = x_1$, $\cos \pi\beta = x_0$. Let $\mu'_{ST}(J) = 2\int_J \sin^2 \pi\theta \, d\theta$. Murty-Prabhu [MP19b] work with the measure μ'_{ST} in place of μ_{ST}, but the substitution $x = \cos \pi\theta$ translates between the two.

Let $m \geq 2$ be an integer. For the elliptic curve $y^2 = x^3 + ax + b$, define $\theta_{a,b}$ as the angle in $[0, \pi]$ for which $\cos \theta_{a,b}$ is its normalized trace. If $m = 2k$ is even, we have

$$\sum_{\substack{a,b \in \mathbb{F}_p \\ 4a^3+27b^2 \neq 0}} \frac{\sin 2k\theta_{a,b}}{\sin \theta_{a,b}} = 0 \tag{1}$$

as follows. Fix $c \in \mathbb{F}_p$ a quadratic nonresidue. Consider the elliptic curve corresponding to (a, b), having Frobenius trace t. Then the elliptic curve corresponding to (c^2a, c^3b) has Frobenius trace $-t$. Thus $\theta_{ca,cb} = \pi - \theta_{a,b}$, and so the set of θ values appearing in the sum are symmetric with respect to $\theta \mapsto \pi - \theta$. But $\sin(\pi - \theta) = \sin \theta$, while $\sin 2k(\pi - \theta) = -\sin 2k\theta$. Therefore, $\sum \frac{\sin 2k\theta}{\sin \theta} = 0$.

Now suppose m is odd. By [DS05, Thm. 3.5.2], the dimension of the space of weight $m + 1$ cusp forms is $\leq \lfloor \frac{m+1}{12} \rfloor$. Let $T_{m+1}(p)$ be the p-Hecke operator acting on the latter space of cusp forms. By [Del74, Thm. 8.2], the eigenvalues of $T_{m+1}(p)$ all have magnitude $p^{m/2}$. Therefore the trace of $T_{m+1}(p)$ is bounded by $\frac{1}{12}(m + 1)p^{m/2}$. Substituting into the Eichler-Selberg trace formula appearing on [MP19b, p. 31] and combining with [MP19b, eq. (3.3)], we obtain

$$\left| \sum_{\substack{a,b \in \mathbb{F}_p \\ 4a^3+27b^2 \neq 0}} \frac{\sin m\theta_{a,b}}{\sin \theta_{a,b}} \right| \leq \frac{1}{6}(m + 1)p^{3/2} + 2p^{-\frac{m-3}{2}}. \tag{2}$$

Let $M \geq 2$ be an integer. Let $\widehat{S}^{\pm}_{J',M}$ denote the Fourier transform of the Mth Beurling-Selberg polynomial for the interval $J' = \frac{1}{2}J = [\frac{\alpha}{2}, \frac{\beta}{2}]$; see [MP19b, §2.3].[1] From [MP19b, p. 30, (c)], we have

$$\widehat{S}^{\pm}_{J',M}(0) = \frac{\beta - \alpha}{2} \pm \frac{1}{M + 1} \tag{3}$$

and, for $0 < m \leq M$,

$$\left| \widehat{S}^{\pm}_{J',M}(m) + \widehat{S}^{\pm}_{J',M}(-m) - \frac{\sin \pi m\beta - \sin \pi m\alpha}{\pi m} \right| \leq \frac{2}{M + 1}. \tag{4}$$

Since $\frac{2}{M+1} \leq \frac{2}{m}$ and $|\frac{\sin \pi m\beta - \sin \pi m\alpha}{\pi m}| \leq \frac{2}{m}$,

$$|\widehat{S}^{\pm}_{J',M}(m) + \widehat{S}^{\pm}_{J',M}(-m)| \leq \frac{4}{m}. \tag{5}$$

An elementary calculation shows that

$$\mu_{ST}(I) = (\beta - \alpha) - \frac{\sin 2\pi\beta - \sin 2\pi\alpha}{2\pi}. \tag{6}$$

From (3), (4) with $m = 2$, and (6),

$$\left| 2\widehat{S}^{\pm}_{J',M}(0) - \widehat{S}^{\pm}_{J',M}(2) - \widehat{S}^{\pm}_{J',M}(-2) - \mu_{ST}(I) \right| \leq \frac{4}{M + 1}. \tag{7}$$

[1] Note that there are several mistakes in the calculation of [MP19b], including an incorrect choice for J'. See the preprint version [MP19a] for a more accurate treatment.

From (1),

$$\left|(\widehat{S}^{\pm}_{J',M}(1)+\widehat{S}^{\pm}_{J',M}(-1))\sum_{4a^3+27b^2\neq 0}\frac{\sin 2\theta_{a,b}}{\sin\theta_{a,b}}\right|=0. \tag{8}$$

From (2) and (5),

$$\left|(\widehat{S}^{\pm}_{J',M}(2)+\widehat{S}^{\pm}_{J',M}(-2))\sum_{4a^3+27b^2\neq 0}\frac{\sin 3\theta_{a,b}}{\sin\theta_{a,b}}\right|\leq\frac{4}{3}p^{3/2}+4 \tag{9}$$

and

$$\left|(\widehat{S}^{\pm}_{J',M}(m)+\widehat{S}^{\pm}_{J',M}(-m))\sum_{4a^3+27b^2\neq 0}\left[\frac{\sin(m+1)\theta_{a,b}}{\sin\theta_{a,b}}-\frac{\sin(m-1)\theta_{a,b}}{\sin\theta_{a,b}}\right]\right| \leq\frac{4(m+2)}{3m}p^{3/2}+\frac{16}{m}p^{-\frac{m-2}{2}}. \tag{10}$$

From (10), we obtain

$$\sum_{3\leq m\leq M}\left|(\widehat{S}^{\pm}_{J',M}(m)+\widehat{S}^{\pm}_{J',M}(-m))\sum_{4a^3+27b^2\neq 0}\left[\frac{\sin(m+1)\theta_{a,b}}{\sin\theta_{a,b}}-\frac{\sin(m-1)\theta_{a,b}}{\sin\theta_{a,b}}\right]\right| \leq\frac{8}{3}Mp^{3/2}+16p^{-\frac{1}{2}}\log M. \tag{11}$$

Let

$$\begin{aligned}B^{\pm}=&p^2(2\widehat{S}^{\pm}_{J',M}(0)-\widehat{S}^{\pm}_{J',M}(2)-\widehat{S}^{\pm}_{J',M}(-2))\\&+\sum_{m=1}^{2}\left((\widehat{S}^{\pm}_{J',M}(m)+\widehat{S}^{\pm}_{J',M}(-m))\sum_{4a^3+27b^2\neq 0}\frac{\sin(m+1)\theta_{a,b}}{\sin\theta_{a,b}}\right)\\&+\sum_{m=3}^{M}\left((\widehat{S}^{\pm}_{J',M}(m)+\widehat{S}^{\pm}_{J',M}(-m))\sum_{4a^3+27b^2\neq 0}\frac{\sin(m+1)\theta_{a,b}}{\sin\theta_{a,b}}-\frac{\sin(m-1)\theta_{a,b}}{\sin\theta_{a,b}}\right).\end{aligned}$$

From [MP19a, eq. (6)], we have

$$B^-\leq N_I(p)\leq B^+. \tag{12}$$

Letting $M=\lfloor p^{1/4}\rfloor$, and putting together (7)–(12) we obtain the claim.

□

Next, we determine what portion of elliptic curves with $|t|<\sqrt{p}$ satisfy that $4p-t^2$ is square-free. The following argument through Corollary 4.10 is modeled after the proof of [FI10, Theorem 2.1].

Lemma 4.2 ([You91])**.** *Let $\gamma\approx 0.577$ be Euler's constant. Then for $x\geq 2$ an integer,*

$$\sum_{n=1}^{x}\frac{1}{n}\leq\log x+\gamma+\frac{1}{2x}$$

For $n\in\mathbb{N}$, let $\tau(n)$ be the number of positive divisors of n.

Lemma 4.3. *For $x\geq 2$,*

$$\sum_{d\leq x}\tau(d)\leq x\log x+(2\gamma-1)x+4\sqrt{x}.$$

Proof. Let $\{x\}$ denote $x - \lfloor x \rfloor$. According to the proof of [BKZ18, Theorem 2], we have

$$\sum_{d \le x} \tau(d) = 2 \sum_{d \le \sqrt{x}} \left\lfloor \frac{x}{d} \right\rfloor - \lfloor \sqrt{x} \rfloor^2.$$

Continuing with that proof, but keeping track of the error terms, we get

$$\begin{aligned} \sum_{d \le x} \tau(d) &\le 2 \sum_{d \le \sqrt{x}} \left(\frac{x}{d} + 1 \right) - (\sqrt{x} - \{\sqrt{x}\})^2 \\ &\le 2x \sum_{d \le \sqrt{x}} \frac{1}{d} + \sqrt{x} - x + 2\sqrt{x}. \end{aligned}$$

Simplifying and applying Lemma 4.2, the claim follows.

□

Let $\rho(n)$ be the number of solutions to $t^2 \equiv 4p \pmod{n}$ with $t \in \mathbb{Z}/n\mathbb{Z}$.

Lemma 4.4. *For $d \ge 1$, $\rho(d^2) \le 4\tau(d)$.*

Proof. Suppose the prime factorization of d is $q_1^{e_1} \cdots q_s^{e_s}$. By Sun Tzu's Theorem (Chinese Remainder Theorem), $\rho(d^2) = \prod_i \rho(q_i^{2e_i})$. Observe that $4p$ is not a square mod p^2, and hence $\rho(d^2) = 0$ if $q_i = p$ for any i. Assume $q_i \ne p$ for all i. If q_i is odd, then $\rho(q_i^{2e_i}) = \rho(q_i)$ by Hensel's Lemma, and $\rho(q_i) \le 2$. If $q_i = 2$, then $\rho(q_i^{2e_i}) \le 8$. Finally, observe that $2^s \le \tau(d)$, with equality precisely when $e_i = 1$ for all i. The claim follows.

□

Lemma 4.5. *If $2 \le Y < p$, then*

$$\sum_{d=1}^{Y} \rho(d^2) \le 4Y \log Y + (8\gamma - 4)Y + 16\sqrt{Y}.$$

Proof. Combine Lemmas 4.3 and 4.4.

□

Let $A(n)$ be the number of solutions to $t^2 \equiv 4p \pmod{n}$ with $1 \le t \le \sqrt{p}$.

Lemma 4.6. *For $d \ge 1$, $|A(d^2) - \rho(d^2)\frac{\sqrt{p}}{d^2}| \le \rho(d^2)$.*

Proof. Let $M = \lfloor \frac{\sqrt{p}}{d^2} \rfloor$. In each of the intervals $[1, d^2]$, $[d^2+1, 2d^2]$, $\ldots$, $[(M-1)d^2+1, Md^2]$, there are exactly $\rho(d^2)$ contributions to $A(d^2)$. In the interval $[Md^2+1, \frac{\sqrt{p}}{d^2}]$, there are at most $\rho(d^2)$ additional contributions.

□

Lemma 4.7. *If $2 \le Y < \sqrt{p}$, then* $\displaystyle\sum_{Y < d < \sqrt{p}} A(d^2) \le \frac{36p}{Y^2}$.

Proof. For positive integers κ, Y, let

$$\begin{aligned} N(\kappa) &= \#\{(t,d) \in \mathbb{Z}^2 : d > Y, 1 \le t \le \sqrt{p}, 4p - t^2 = \kappa d^2\} \\ &= \#\{(t,d) \in \mathbb{Z}^2 : d > Y, 1 \le t \le \sqrt{p}, \mathrm{Nm}_{\mathbb{Q}(\sqrt{-\kappa})/\mathbb{Q}}(t + d\sqrt{-\kappa}) = 4p\}. \end{aligned}$$

If (t,d) is a pair counted by $N(\kappa)$, then we have $\kappa = \frac{4p-t^2}{d^2}$, and hence $N(\kappa) = 0$ for $\kappa > \frac{4p}{Y^2}$. We have $\displaystyle\sum_{Y < d < \sqrt{p}} A(d^2) \le \sum_{1 \le \kappa \le \frac{4p}{Y^2}} N(\kappa)$. We claim that $N(\kappa) \le 9$, from which the lemma follows. To see this, suppose

that (2) and (p) each split as the product of two principal ideals in $\mathbb{Q}(\sqrt{-\kappa})$; say $(2) = \mathfrak{l}_1 \cdot \bar{\mathfrak{l}}_1$ and $(p) = \mathfrak{l}_2 \cdot \bar{\mathfrak{l}}_2$. Then (t, d) is counted by $N(\kappa)$ if and only if $t + d\sqrt{-\kappa}$ is a generator for an ideal of norm $4p$, which must lie in the list $\mathfrak{l}_1^2\mathfrak{l}_2, (2)\mathfrak{l}_2, \bar{\mathfrak{l}}_1^2\mathfrak{l}_2, \bar{\mathfrak{l}}_1^2\bar{\mathfrak{l}}_2, (2)\bar{\mathfrak{l}}_2, \mathfrak{l}_1^2\bar{\mathfrak{l}}_2$. Conjugation changes the sign of d, and since we only count $d > 0$, we need only consider half of the above ideals. The number of generators for each ideal is at most the size of the units in the ring of integers of $\mathbb{Q}(\sqrt{-\kappa})$, which is at most 6 (occurring when $\kappa = 3$). But multiplication by -1 only changes the sign of the pair (t, d), and so there are at most 3 generators per ideal which contribute to the count of $N(\kappa)$. Therefore $N(\kappa) \leq 9$.

Finally, if the splitting behavior of $(2), (p)$ differs from our assumption above, then $N(\kappa)$ can only shrink. □

Let $\mu(n)$ denote the Möbius function.

Lemma 4.8. *If $2 \leq Y < \sqrt{p}$ is an integer, then*

$$\left| \sum_{d>Y} \mu(d) \frac{\rho(d^2)}{d^2} \right| \leq 12Y^{-0.7}.$$

Proof. We have

$$\left| \sum_{d>Y} \mu(d) \frac{\rho(d^2)}{d^2} \right| \leq \sum_{d=Y+1}^{\infty} \frac{4\tau(d)}{d^2}.$$

The first displayed inequality in the proof of Lemma 5 from [NR83] yields $\tau(d) \leq 5d^{0.3}$. The result follows from the fact that $\displaystyle\sum_{d=Y+1}^{\infty} \frac{20}{d^{1.7}} \leq \int_Y^{\infty} 20x^{-1.7}\, dx$.

□

Theorem 4.9. *Let $C = \displaystyle\prod_{q \text{ prime}} \left(1 - \frac{2}{q^2}\right)$ and let p be an odd prime. Let n_p be the number of values of t for which $1 \leq t < \sqrt{p}$ and $4p - t^2$ is square-free. Then*

$$n_p \geq Cp^{\frac{1}{2}} - \frac{4}{3}p^{\frac{1}{3}} \log p - (8\gamma + 32)p^{\frac{1}{3}} - 12p^{\frac{4}{15}} - 16p^{\frac{1}{6}}.$$

Proof. By inclusion-exclusion, $n_p = \displaystyle\sum_{d=1}^{\infty} \mu(d)A(d^2)$. Let $Y = \sqrt[3]{p}$. Using Lemma 4.6, we have

$$\begin{aligned} \sum_{d=1}^{\infty} \mu(d)A(d^2) &= \sum_{d \leq Y} \mu(d)A(d^2) + \sum_{d>Y} \mu(d)A(d^2) \\ &\geq \sqrt{p} \sum_{d \leq Y} \mu(d) \frac{\rho(d^2)}{d^2} - \sum_{d \leq Y} \rho(d^2) - \sum_{d>Y} A(d^2) \end{aligned}$$

Additionally,

$$\sqrt{p} \sum_{d \leq Y} \mu(d) \frac{\rho(d^2)}{d^2} \geq \sqrt{p} \sum_{d=1}^{\infty} \mu(d) \frac{\rho(d^2)}{d^2} - \sqrt{p} \left| \sum_{d>Y} \mu(d) \frac{\rho(d^2)}{d^2} \right|.$$

Combining Lemmas 4.5, 4.7, and 4.8 with the fact that

$$\sum_{d=1}^{\infty} \mu(d) \frac{\rho(d^2)}{d^2} = \prod_{q \text{ prime}} \left(1 - \frac{\rho(q^2)}{q^2}\right) \geq C,$$

we obtain the result.

□

Corollary 4.10. *If $p > 2^{63}$ is prime, then the probability that $4p - t^2$ is square-free, where t is randomly chosen in $1 \le t < \sqrt{p}$, is at least 25%.*

Proof. We wish to bound $n_p/\sqrt{p}$. The *Feller-Tornier constant* [OEI24, Seq. A065493] is

$$\frac{1}{2} + \frac{1}{2} \prod_{q \text{ prime}} \left(1 - \frac{2}{q^2}\right) > .66,$$

from which it follows that $C > 0.32$. Thus by Theorem 4.9, $\frac{n_p}{\sqrt{p}} \ge 0.32 - \epsilon(p)$, where

$$\epsilon(p) = \frac{4}{3} p^{-\frac{1}{6}} \log p + (8\gamma + 32) p^{-\frac{1}{6}} + 12 p^{-\frac{7}{30}} + 16 p^{-\frac{1}{3}}.$$

Since $p > 2^{63}$, $\epsilon(p) \le \epsilon(2^{63}) < 0.07$, the claim follows. □

Recall from Definitions 3.5 and 3.6 the probability distributions $\mathscr{U}_p$ and $\mathscr{D}_p$ on the set of isomorphism classes of elliptic curves over $\mathbb{F}_p$.

Lemma 4.11. *For any prime $p \ge 5$, the ℓ_2 distance between the distributions $\mathscr{D}_p$ and $\mathscr{U}_p$ is $\le \frac{2}{p}$.*

Proof. In the distribution $\mathscr{D}_p$, we represent elliptic curves by the $p^2 - p$ pairs $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying $4a^3 + 27b^2 \neq 0$. As observed in [Bir68, §1], for each isomorphism class of elliptic curves, there are $\frac{(p-1)}{2}$ pairs (a, b) giving rise to it, except for the cases of $y^2 = x^3 + ax$ and $y^2 = x^3 + b$. For $y^2 = x^3 + ax$, there are $(p-1)/4$ pairs $(a, 0)$ if $p \equiv 1 \pmod 4$ for each of 4 isomorphism classes of elliptic curves, and $(p-1)/2$ pairs for each of 2 isomorphism class if $p \equiv 3 \pmod 4$. For $y^2 = x^3 + 1$, there are $(p-1)/6$ pairs if $p \equiv 1 \pmod 3$ yielding 6 isomorphism classes of elliptic curves, and $(p-1)/2$ pairs if $p \equiv 2 \pmod 3$ for 2 isomorphism classes of elliptic curves. Then $\mathscr{D}_p$ chooses isomorphism classes with $a, b \neq 0$ with probability $\frac{1}{2p}$; curves with $b = 0$ with probability between $\frac{1}{2p}$ and $\frac{1}{4p}$; and curves with $a = 0$ with probability between $\frac{1}{2p}$ and $\frac{1}{6p}$. The largest discrepancy from the uniform distribution $\mathscr{U}_p$ occurs when $p \equiv 1 \pmod{12}$. In this case, for $\mathscr{D}_p$ there are $2p - 2$ isomorphism classes of elliptic curves with $a, b \neq 0$, 4 with $b = 0$, and 6 with $a = 0$, while $\mathscr{U}_p$ is uniform across all $2p + 8$ isomorphism classes. A routine calculation now yields the result.

□

Corollary 4.12. *Let $p > 2^{63}$ be prime. The probability that an elliptic curve drawn from the distribution $\mathscr{D}_p$ lies in $\mathscr{E}_{\mathsf{sf},3p}$ is at least 14%. The same holds if we draw from the distribution $\mathscr{U}_p$.*

Proof. We first choose an elliptic curve according to $\mathscr{D}_p$. Note that $|\frac{t}{2\sqrt{p}}| < \frac{1}{2}$ implies that $\Delta_{\mathrm{Fr}}(E) \ge 3p$.

Next, we cannot directly use Corollary 4.10 since the distribution of t values is not uniform. But since the density function $\frac{d\mu_{ST}}{dX} = \frac{2}{\pi}\sqrt{1 - X^2}$ is decreasing as a function of $|X| = |\frac{t}{2\sqrt{p}}|$, the probability that $\Delta_{\mathrm{Fr}}(E)$ is square-free, given that $|t| < \sqrt{p}$, is lowest when all of the square-free values occur for $|t|$ as large as possible. (In fact, this will never occur, since even t values result in $4 \mid \Delta_{\mathrm{Fr}}(E)$; but the probability we obtain with this assumption will in any case be a lower bound for the true probability.) Via Corollary 4.10, we therefore assume that the elliptic curves with square-free t and $4p - t^2 \ge 3p$ occur when $0.75\sqrt{p} < |t| < \sqrt{p}$. Applying Theorem 4.1, we see that at least 14% of all elliptic curves mod p have trace t in this range.

The analogous results for $\mathscr{U}_p$ follow from applying Lemma 4.11.

□

Theorem 4.13. *Suppose $0 < \epsilon < \frac{1}{2}$ and K is an imaginary quadratic field. Let D be the absolute value of the discriminant of K, and h the class number of K. If $D > \max(e^{1/\epsilon}, e^{11.2})$, then $h > \frac{0.655\epsilon}{\pi} D^{\frac{1}{2}-\epsilon}$ except for at most* one *choice of K.*

Proof. See the remarks immediately following Theorem 2 in [Tat51]. The idea is that according to the Dirichlet class number formula, $h = \frac{1}{\pi}\sqrt{D} \cdot L_D(1)$, where L_D is the L-function associated to K (this is a power series related to the Riemann zeta function which encodes number theoretic information about K). Tatuzawa in [Tat51] provides lower bounds for $L_D(1)$.

□

For somewhat better bounds, see [Hof80, Theorem 1].

Corollary 4.14. *Let $p > 2^{63}$ be prime. Given an ordinary elliptic curve $E/\mathbb{F}_p$, let $\mathcal{O}$ be $\mathrm{End}(E)$. If an elliptic curve E is drawn from either the distribution $\mathscr{D}_p$ or the distribution $\mathscr{U}_p$, then with probability at least 14%, $E \in \mathscr{E}_{\mathsf{sf},3p}$ and both the class group of $\mathcal{O}$ and the isogeny class of E have size at least $0.089\frac{\sqrt{p}}{\log p}$.*

Proof. By Corollary 4.12, there is a probability of at least 14% such that $E \in \mathscr{E}_{\mathsf{sf},3p}$. For $E \in \mathscr{E}_{\mathsf{sf},3p}$, consider Fr the Frobenius endomorphism and $K = \mathbb{Q}(\mathrm{Fr})$. Since $\Delta_{\mathrm{Fr}}(E)$ is square-free, $\mathbb{Z}[\mathrm{Fr}] = \mathrm{End}(E) \cong \mathscr{O}_K$, and this must hold for any elliptic curve isogenous to E. Therefore $\Delta_{\mathrm{Fr}}(E) = D(E)$ and the isogeny class of E is acted upon simply transitively by the class group, and so has the same size as the class group.

For the size claim, choose $\epsilon = \frac{1}{\ln p}$ in Theorem 4.13. Note that the one possible exceptional K in that Theorem is subsumed by the round-off error in the probability calculation of Corollary 4.12.

□

4.2 The SEA isogeny algorithm

We recall the complex multiplication theory of elliptic curves. Given an imaginary quadratic number field K and an order $\mathscr{O} \subset K$, we say that E has complex multiplication by $\mathscr{O}$ if $\mathrm{End}(E) \cong \mathscr{O}$, or if $\mathscr{O}$ is isomorphic to a subring of $\mathrm{End}(E)$, and there is no larger order of K isomorphic to a subring of $\mathrm{End}(E)$; this second case is only necessary for supersingular elliptic curves.

Identify $\mathscr{O}$ with (the corresponding subring of) $\mathrm{End}(E)$. Given an integral ideal I of $\mathscr{O}$, define $E[I] = \{\cap \ker(\alpha) : \alpha \in I\}$; it is a subgroup of E of order the ideal norm $N(I)$. Write φ_I for the canonical isogeny $\varphi_I : E \to E_I := E/E[I]$. Observe that $\deg(\varphi_I) = N(I)$. The isomorphism class of E_I depends only on the ideal class of I. We let $M(p)$ be the complexity of one arithmetic operation in $\mathbb{F}_p$. Then we have

Theorem 4.15. *Let E be an elliptic curve over $\mathbb{F}_p$ with complex multiplication by $\mathscr{O}$, and let $\mathfrak{l} \subset \mathscr{O}$ be a prime ideal of norm ℓ, where ℓ is a rational prime. Then there is a classical algorithm which computes the isogeny $\varphi_\mathfrak{l}$ in time $O\left(\ell M(p) \log \ell \log\log \ell \log p\right)$.*

Proof. See [DKS18, p. 12], specifically "Elkies steps" (Algorithms 3 and 4). See Section 10 for more details.

□

As we'll see in §4.3, we will be concerned with the case where $\ell \leq 6\log^2(4p)$.

4.3 Building the Generating Set of Isogenies

Below we will give an algorithm to list prime ideal classes in B_K. We will omit prime ideals of the form $\ell\mathscr{O}_K$ for ℓ a rational prime, since such so-called *inert* primes are principal and hence yield the trivial class. (Additionally, the ideal norm of $\ell\mathscr{O}_K$ is ℓ^2, so the inert primes will quickly exceed the Bach bound.) The prime ℓ is inert if and only if $-D$ is a quadratic nonresidue mod ℓ. If ℓ is not inert and does not divide D, then ℓ factors as the product of a prime ideal, say $\mathfrak{l}$, and its conjugate.

We now give an algorithm to generate a list of prime ideals $\mathfrak{l}_i$ representing B_K.

Algorithm 4.1: Bach Generating Set Algorithm

Input: K an imaginary quadratic field with discriminant D
Output: $(\mathfrak{l}_i)$, list of primes in $\mathscr{O}_K$

1 Initialize $i = 1$ and $\ell = 2$.
2 Check if ℓ is inert by determining if the Legendre symbol $(\frac{-D}{\ell}) = -1$; if yes, go to step 5.
3 By enumeration, find the smallest positive x satisfying $x^2 \equiv -D \pmod{\ell}$. Let $\mathfrak{l} = (\ell, x + \sqrt{-D})$ and $\mathfrak{l}' = \overline{\mathfrak{l}_i} = (\ell, x - \sqrt{-D})$.
4 Check if the class of $\mathfrak{l}$ has already been generated by determining if $\mathfrak{l} \cdot \mathfrak{l}_j$ is a principal ideal for any $\mathfrak{l}_j$ with $j < i$. If yes, go to the next step. Otherwise, set $\mathfrak{l}_i = \mathfrak{l}$. Check if $\mathfrak{l}^2$ is principal, and if not, then also set $\mathfrak{l}_{i+1} = \mathfrak{l}'$. Increment i by 1 or 2 accordingly.
5 Increment ℓ to the next larger rational prime. If $\ell > 6(\log D)^2$, then output the list $(\mathfrak{l}_i)$ and terminate.

We remark on accomplishing each of these steps. Step 2 is clear. For step 3, such an x with $1 \leq x \leq \frac{\ell}{2}$ is guaranteed to exist, as the Legendre symbol is $+1$ and solutions come in additive inverse pairs. For step 4, take the pairwise products of the generators of $\mathfrak{l} \cdot \mathfrak{l}_j$, and let $\Lambda \subset \mathbb{C}$ be the lattice generated by these products (where we view $\mathbb{Q}(\sqrt{-D}) \subset \mathbb{C}$ using either field embedding). Then apply Lagrange-Gauss reduction to the lattice; $\mathfrak{l} \cdot \mathfrak{l}_j$ is principal if and only if $\lambda_1(\Lambda) = \ell \cdot \ell_j$.

Proposition 4.16. *If $\widetilde{B}_K$ is the output of Algorithm 4.1, then the map $\widetilde{B}_K \to B_K$ given by $\mathfrak{l} \mapsto [\mathfrak{l}]$ is a bijection. Furthermore, if $[\mathfrak{l}] \in B_K$, then $[\mathfrak{l}]^{-1} \in B_K$.*

Proof. The definition of B_K immediately yields that the map is well-defined and surjective. Let $\mathfrak{l} \in \widetilde{B}_K$ of norm ℓ. If $\mathfrak{l}^2$ is principal, then $[\mathfrak{l}]$ is its own inverse. Otherwise in step 4, we also have $\overline{\mathfrak{l}} \in \widetilde{B}_K$ and since

$$\mathfrak{l} \cdot \overline{\mathfrak{l}} = \ell \mathscr{O}_K$$

is principal, we get $[\mathfrak{l}]^{-1} = [\overline{\mathfrak{l}}] \in \widetilde{B}_K$. This proves the second claim.

For the first claim, it suffices to show that the map is injective. Step 4 of the algorithm shows that $\forall \mathfrak{l}, \mathfrak{l}' \in \widetilde{B}_K$, $\mathfrak{l} \cdot \mathfrak{l}'$ is not principal. Since $\widetilde{B}_K$ is closed under inversion, this implies that if $\mathfrak{l}_i, \mathfrak{l}_j \in \widetilde{B}_K$ with $i \neq j$, then $\mathfrak{l}_i \cdot \mathfrak{l}_j^{-1}$ is not principal; in other words, $[\mathfrak{l}_i] \cdot [\mathfrak{l}_j]^{-1} \neq [(1)]$, and hence $[\mathfrak{l}_i] \neq [\mathfrak{l}_j]$.

□

Proposition 4.17. *Algorithm 4.1 requires $O((\log D)^7)$ bit operations and uses $O((\log D)^2 \log\log D)$ bits of memory.*

Note that $\log D = O(\log p)$.

Proof. Each of the first three steps take $O((\log D)^2)$. The length of the generators for the lattice Λ in step 4 is $O(D)$, and hence Lagrange-Gauss take $O((\log D)^3)$. There are $O((\log D)^2)$ pairs to check in one invocation of step 4, and the algorithm repeats $O((\log D)^2)$ times, whence the time estimate.

Each prime is recorded as a pair of generators whose coefficients are of size $\log \ell = O(\log\log D)$. Since there are $O((\log D)^2)$ primes, the space complexity follows.

□

4.4 The Distribution of Class Group Generators

Let G be a finite abelian group. We say that a sequence $h_1, \ldots, h_t \in G$ is *weakly Erdös-Rényi* if, for every $g \in G$, $\exists e_1, \ldots, e_t \in \{0, 1\}$ such that $g = h_1^{e_1} h_2^{e_2} \cdots h_t^{e_t}$.

Definition 4.18. We define the *Bach-Erdös-Rényi game* as follows. Given a parameter λ, an adversary wins if it can find an imaginary quadratic field K with discriminant $D > 2^\lambda$ such that the classes $B_K \subset \mathrm{Cl}(\mathscr{O}_K)$ are not weakly Erdös-Rényi.

Assumption 4.19. *For every quantum polynomial time adversary, the probability of winning the Bach-Erdös-Rényi game is a negligible function of λ.*

Why should we believe this assumption? First, consider the following theorem.

Theorem 4.20 ([ER65], Theorem 2)**.** *If G is a finite abelian group, $\delta > 0$, and*

$$t \geq \log(\#G) + \log\log(\#G) - 2\log\delta + 5,$$

then a randomly chosen sequence $h_1, \ldots, h_t \in G$ is weakly Erdös-Rényi with probability at least $1 - \delta$.

Taking $G = \mathrm{Cl}(\mathscr{O}_K)$ and $\delta = \frac{1}{D}$, the assumption holds as long as B_K acts like a random set of elements from G. In Section 11, we give heuristic evidence that B_K acts "sufficiently randomly."

4.5 Eigenvalue bounds

A *vertex-transitive graph* Γ is one for which for every pair of vertices v, w, there is an automorphism of the graph γ such that $\gamma(v) = w$.

Proposition 4.21 (Lemma 6.1, [Bab91])**.** *Let Γ be a vertex-transitive graph of degree d and diameter δ. Then the second largest eigenvalue of the adjacency matrix of Γ is $\leq d - \frac{1}{16.5\delta^2}$.*

Fix an isogeny class $\mathcal{I}_N \subset \mathscr{E}_{\mathsf{sf},3p}$. Let X be the graph with vertex set $\mathcal{I}_N$ and for which E, E' are adjacent if and only if $\exists[\mathfrak{l}] \in B_K$ such that $[\mathfrak{l}] * E = E'$.

Proposition 4.22. *Suppose B_K is weakly Erdös-Rényi for $\mathrm{Cl}(\mathscr{O}_K)$, and let $r = \#B_K$. Then the second largest eigenvalue μ_2 of the adjacency matrix of X satisfies $\mu_2 \leq r - \frac{1}{16.5r^2}$.*

Proof. Let $E_1, E_2 \in \mathcal{I}_N$. Since $\Delta_{\mathrm{Fr}}(E_1), \Delta_{\mathrm{Fr}}(E_2)$ are square-free, we must have $\Delta_{\mathrm{Fr}}(E_1) = D(E_1) = \Delta_{\mathrm{Fr}}(E_2)$. Therefore $\exists c \in \mathrm{Cl}(\mathscr{O}_K)$ such that $c * E = E'$. Since B_K is weakly-Erdös-Rényi, $\exists[\mathfrak{l}_1], \ldots, [\mathfrak{l}_t] \in B_K$ such that $c = \prod[\mathfrak{l}_i]$. The map $E \mapsto (\prod[\mathfrak{l}_i]) * E$ yields an automorphism of X which sends E to E', and hence X is vertex-transitive.

Observe that X is a regular graph with degree equal to r. If B_K is weakly Erdös-Rényi, then the diameter of X is bounded above by r. The result now follows from the previous proposition.

□

5 Sampling a Superposition of Elliptic Curves over $\mathbb{F}_p$

Suppose p is a large prime. Recall that we represent elliptic curves over $\mathbb{F}_p$ by a pair (j, b) where $j \in \mathbb{F}_p$ and b is twisting data. In this subsection, we show how to sample a uniform superposition over elliptic curves over $\mathbb{F}_p$. To our knowledge, this is not known for *supersingular* elliptic curves [MMP22], and most "natural" ways of generating random elliptic curves run into the index erasure problem [AMRR11] when used to try to generate a superposition of elliptic curves.

Algorithm 5.1: Algorithm ECSupGen

Input: p a prime
Output: $|E\rangle$ a quantum state
Let $\mathcal{S}$ be a register that can store a pair (j, b), where $j \in \mathbb{F}_p$ and $0 \leq b \leq 5$.
Generate a uniform superposition $|\psi\rangle \in \mathcal{S}$ over all pairs (j, b), where

- If $j \not\equiv 0, 1728 \pmod{p}$, then $b = 0$ or 1.
- If $j \equiv 1728$ and $p \equiv 1 \pmod{4}$, then $0 \leq b \leq 3$. If $p \equiv 3 \pmod{4}$, then $b = 0$ or 1.
- If $j \equiv 0$ and $p \equiv 1 \pmod{3}$, then $0 \leq b \leq 5$. If $p \equiv 2 \pmod{3}$, then $b = 0$ or 1.

Proposition 5.1. *Let $|\psi\rangle$ be the output of Algorithm 5.1. Then $|\psi\rangle$ is a uniform superposition over all isomorphism classes of elliptic curves over $\mathbb{F}_p$. The algorithm takes time $O(\log p)$.*

Proof. The first claim is immediate from the discussion in §3.3. The complexity estimate comes from generating the superposition over all j, which dominates the conditional superposition over b-values. □

We remark that encoding a superposition using the Weierstrass encoding (a, b) (corresponding to the elliptic curve $y^2 = x^3 + ax + b$) is also possible. However, the Weierstrass encoding requires about twice as many qubits. Additionally, since there are $O(p)$ pairs (a, b) corresponding to the same isomorphism class, the group action will not be as nicely behaved; for instance, the set of elliptic curves is the disjoint union of $O(p)$ orbits under the class group action.

6 Verifying a Superposition of Elliptic Curves

In this section, we give an algorithm that verifies that a quantum state is negligibly close to a uniform superposition of elliptic curves over $\mathbb{F}_p$ with a given number of points. Our algorithm is based on the verification algorithm of [LMZ23] (which is in turn an abstraction of the verification procedure of [FGH+12]); at a high level, it is the same as that of [LMZ23], although we have made a number of changes that are specific to our scheme.

6.1 Overview of Verification Algorithm.

Let $\mathcal{I}_N$ denote the set of elliptic curves over $\mathbb{F}_p$ with N points, and let $|\mathcal{I}_N\rangle := \frac{1}{\sqrt{\#\mathcal{I}_N}} \sum_{E \in \mathcal{I}_N} |E\rangle$. In other words, $|\mathcal{I}_N\rangle$ is a uniform superposition over all elliptic curves with N points.

Our goal, similar to [LMZ23], is to compute an approximation of the projection-valued measure $V_N = |\mathcal{I}_N\rangle \langle \mathcal{I}_N|$. Unlike [LMZ23], for us there is only a single orbit in $\mathcal{I}_N$ (because the class group acts transitively on the isogeny class), so we can simplify our corresponding PVM relative to theirs.

Note that if we started with a uniform superposition $|\mathcal{I}_N\rangle$, then $V_N |\mathcal{I}_N\rangle = |\mathcal{I}_N\rangle$ immediately. If instead we compute $V_N |\psi\rangle$ for some superposition $|\psi\rangle$ that does not put much weight on $|\mathcal{I}_N\rangle$, we know that V_N is likely to reject. We emphasize that such a projection does not disturb a "correct" state $|\mathcal{I}_N\rangle$. We will show that our algorithm closely mimics the behavior of the PVM V_N.

At a rough level, our algorithm works as follows: we first check to make sure that we are given a state that contains a representation of a (possible) superposition of elliptic curves with N points. Then, as in [LMZ23], we mimic taking a random walk (in superposition) over all elliptic curves with N points. If we ensure that our "steps" in the random walk are invertible (i.e., the mapping is one-to-one), then we have the following nice property: if we start with $|\mathcal{I}_N\rangle$, then taking a step of our walk brings us to $|\mathcal{I}_N\rangle$, which is where we started. If, on the other hand, we started with, say, a single elliptic curve E, then taking a random walk would likely leave us with a different elliptic curve, which is a totally different state. As in previous work [FGH+12, LMZ23], we build this intuition into a full verification algorithm.

6.2 Verification Algorithm Definitions.

Definition 6.1. The Isogeny Computation σ_i. Fix $E_0 \in \mathscr{E}_{\mathsf{sf},3p}$, and let $\mathcal{I}_N$ be its isogeny class. Let $\mathcal{V} = \mathbb{C}^{\mathcal{I}_N}$; that is, the complex vector space with orthonormal basis given by $|E\rangle$ for $E \in \mathcal{I}_N$. Let $K = \mathrm{End}(E_0) \otimes \mathbb{Q}$. Let $\mathfrak{l}_1, ..., \mathfrak{l}_r$ denote prime ideals which form a system of representatives for the classes in B_K, as discussed in Section 10. For each $i \in [1, r]$ we let $\sigma_i : \mathcal{V} \to \mathcal{V}$ denote the unitary given by $\sigma_i |E\rangle = |\mathfrak{l}_i * E\rangle$.

Note that by giving only p and $N := \#E_0(\mathbb{F}_p)$, $\mathcal{I}_N$ is determined, while K, B_K can be efficiently computed.

Recall that if $[\mathfrak{l}] \in B_K$, then $[\mathfrak{l}]^{-1} \in B_K$ as well. Therefore the σ_i come in pairs which are inverses of each other.

Definition 6.2. The State $|\mathbf{1}_n\rangle$. If n is an integer, define the state $|\mathbf{1}_n\rangle := \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle$ and if $n' > n$, define $|\mathbf{1}_{n,n'}\rangle := \frac{1}{\sqrt{n'-n+1}} \sum_{i=n}^{n'} |i\rangle$.

Definition 6.3. For integers n and k, let $\mathbf{P}_{n,k} := |\mathbf{1}_n\rangle \langle \mathbf{1}_n| \otimes \mathbf{I}_k$, where $\mathbf{I}_k$ denotes the identity matrix acting on k qubits.

We view $\mathbf{P}_{n,k}$ as a projection-valued measure with outputs 0 and 1. By Definition 3.1, the probability of obtaining output 1 when we apply the operator $\mathbf{P}_{n,k}$ to a pure state $|\psi\rangle$ is $\langle\psi| \mathbf{P}_{n,k} |\psi\rangle$, with the measured state collapsing to $\frac{\mathbf{P}_{n,k}|\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_{n,k}|\psi\rangle}}$.

Lemma 6.4. *We have the following:*

1. *Each $\mathbf{P}_{n,k}$ is a positive semi-definite Hermitian matrix.*
2. $\mathbf{P}_{n,k}^2 = \mathbf{P}_{n,k}$.
3. $\mathbf{P}_{n,k} = \mathbf{P}_{n,k}^\dagger$, *where "$\dagger$" denotes conjugate transpose.*

Definition 6.5. Let $r = \#B_K$, $k = \#\mathcal{I}_N$, and $\mathcal{W} = \mathbb{C}^r \otimes \mathcal{V}$. Let $\mathbf{U} : \mathcal{W} \to \mathcal{W}$ be the unitary given by

$$\mathbf{U} := \sum_{i=1}^{r} |i\rangle \langle i| \otimes \sigma_i + \sum_{i=r+1}^{2r} |i\rangle \langle i| \otimes \mathbf{I}_k.$$

Equivalently, for $1 \le i \le r$ and $E \in \mathcal{I}_N$,

$$\mathbf{U}(|i, E\rangle) = |i, \mathfrak{l}_i * E\rangle \text{ and}$$
$$\mathbf{U}(|i + r, E\rangle) = |i + r, E\rangle .$$

Recall that instead of $\mathcal{V}$, we work in the larger vector space of all pairs (j, b). But if $E \notin \mathcal{I}_N$ (which can be efficiently determined via Schoof's algorithm), then we may define σ_i to act trivially on $|E\rangle$. However, valid bank notes lie in $\mathcal{V}$, which can be checked efficiently. Thus the action of σ_i on $|E\rangle$, $E \notin \mathcal{I}_N$, will not be relevant.

6.3 Verification Algorithm.

Algorithm 6.1: Algorithm ECSupVer

Input: a prime p, integers N and τ, and a quantum state $|\psi\rangle$ stored in a register $\mathcal{S}$

Output: a bit 0 or 1. If it returns 1, then ECSupVer alters $|\psi\rangle$ to a state $|\psi'\rangle$ which it then outputs.

1 Check that $|\psi\rangle$ is properly formatted as a superposition over pairs $(j, b) \in \mathbb{F}_p \times \{0, \ldots, 5\}$ with b following the restrictions of Algorithm 5.1, and that $4p - (p + 1 - N)^2 \ge 3p$ and is square-free. If not, output 0.

2 Use Schoof's algorithm to compute the number of points in the elliptic curve representation of $|\psi\rangle$ in a new register.

3 Measure the value in the new register. If it is *not* N, output 0 and terminate. From N, compute K, B_K with Algorithm 4.1, and $\mathbf{U}$ as in Definition 6.5. Then discard this register.

4 Let $r = \#B_K$. Using a new register, create the state $|\varphi\rangle := \mathbf{1}_{2r} \otimes |\psi\rangle \in \mathcal{W} := \mathbb{C}^{2r} \otimes \mathcal{V}$.

5 Repeat the following τ times:

1. Apply the unitary $\mathbf{U}$ to $|\varphi\rangle$.
2. Apply the projection-valued measurement corresponding to $\mathbf{P}_{2r,k}$ to the resulting state. If the measurement fails (i.e., we do not get a state lying in the set $\mathbf{1}_{2r} \otimes \mathcal{V}$) output 0 and terminate.

Discard the first register and output 1 as well as the resulting state.

We will say that ECSupVer "accepts" if it returns 1 and a state.

6.4 Verification Algorithm Efficiency

We next prove that our verification algorithm is efficient. We do this with the following lemma.

Lemma 6.6. *On input a prime p, integers N and τ, and a quantum state $|\psi\rangle$, the algorithm* ECSupVer *runs in time*

$$\max\left(O\left(\log^8 p\right), O\left(\tau\left(\log^3 p\right)\left(\log\log^2 p\right)\left(\log\log\log^2 p\right)\right)\right).$$

Proof. Note that Schoof's algorithm (see Theorem 10.1) used in step 2 takes time $O\left(\log^8 p\right)$, which dominates the running time of the algorithm before the loop in step 4.

Step 4 is dominated by the cost of step (a), which is the application of the unitary $\mathbf{U}$ which performs the isogeny computation. If we let $M(p)$ be the complexity of one arithmetic operation in $\mathbb{F}_p$, then we know from Theorem 4.15 that there is a classical algorithm which computes a degree ℓ isogeny in time $O\left(\ell M(p)\log\ell\log\log\ell\log p\right)$. Since, in our case, $\ell = O\left(\log^2 p\right)$ and $M\left(p\right) = O\left(\log^3 p\right)$, we know that each iteration of step 4 is upper-bounded by a function which is $O\left(\left(\log^5 p\right)\left(\log\log^2 p\right)\left(\log\log\log^2 p\right)\right)$. The claim follows.

□

7 Proof of Verification Algorithm.

We now argue that our verification algorithm accepts with all but negligible probability.

Definition 7.1. The Matrix M. Define a unitary operator $\mathbf{M} : \mathcal{V} \to \mathcal{V}$ by

$$\mathbf{M} := \frac{1}{r}\sum_{i=1}^{r}\sigma_i.$$

Equivalently, for $E \in \mathcal{I}_N$,

$$\mathbf{M}\left|E\right\rangle = \frac{1}{r}\sum_{i=1}^{r}\left|\mathfrak{l}_i * E\right\rangle.$$

The operator $\mathbf{M}$ is analogous to a similar operator in [LMZ23], and we can borrow from, and make more precise, their analysis and explanation.

Lemma 7.2. *The eigenvalues of $\mathbf{M}$ are real. The largest eigenvalue of $\mathbf{M}$ is 1; the corresponding eigenvector is precisely $|\mathcal{I}_N\rangle = \sum_{E\in\mathcal{I}_N}|E\rangle$. Furthermore, if B_K is weakly Erdös-Rényi $\mathrm{Cl}(\mathscr{O}_K)$, then the second largest eigenvalue λ_2 for $\mathbf{M}$ is at most $1 - \frac{1}{16.5r^3}$.*

Proof. Consider the graph Γ whose vertices are the elliptic curves in $\mathcal{I}_N$, and whose edges are all pairs $(E, \mathfrak{l}_i * E)$ for $E \in \mathcal{I}_N$, $1 \le i \le r$. If we identify $\mathbf{M}$ with the matrix representing it in the computational basis $\{|E\rangle : E \in \mathcal{I}_N\}$, then $r\mathbf{M}$ is precisely the adjacency matrix of Γ. Since the $\mathfrak{l}_i$ come in inverse pairs, it follows that $\mathbf{M}$ is real symmetric, and hence has real eigenvalues. As Γ is r-regular, the largest eigenvalue of the adjacency matrix is r with corresponding eigenvector $|\mathcal{I}_N\rangle = \sum_{E\in\mathcal{I}_N}|E\rangle$. Therefore the largest eigenvector of $\mathbf{M}$ is 1, with eigenvector $|\mathcal{I}_N\rangle$.

From Proposition 4.22, if B_K is weakly Erdös-Rényi, then the second largest eigenvalue λ_2 for the matrix M is at most $1 - \frac{1}{16.5r^3}$.

□

Let $|\psi_1\rangle, ..., |\psi_k\rangle$ be an eigenbasis for $\mathbf{M}$, where we let $|\psi_1\rangle = |\mathcal{I}_N\rangle$. For each j, let a_j denote the eigenvalue corresponding to the eigenstate $|\psi_j\rangle$; if B_K is weakly Erdös-Rényi, then $a_j \le 1 - \frac{1}{16.5r^3}$ for $j \ge 2$.

As in [LMZ23], we will begin by showing a simple example where the state $|\psi\rangle$ is an eigenvector state. In the following lemma we examine what the state will look like after one operation of the "loop" in our verification algorithm, assuming the first PVM accepts, which we can then reuse for other calculations.

Lemma 7.3. $\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle = \frac{1+a_j}{2}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle$.

Proof. By the definitions of $\mathbf{P}_{2r,k}$, $\mathbf{U}$ (Definition 6.5), $\mathbf{M}$, and a_j, and the facts that $\langle i|\left|\mathbf{1}_r\right\rangle = \langle i|\left|\mathbf{1}_{r+1,2r}\right\rangle = \frac{1}{\sqrt{r}}$ and $(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D}) = \mathbf{AC}\otimes\mathbf{BD}$, we have:

$$\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle = \left(\left|\mathbf{1}_{2r}\right\rangle\left\langle\mathbf{1}_{2r}\right|\otimes\mathbf{I}_k\right)\left[\sum_{i=1}^{r}\left|i\right\rangle\left\langle i\right|\otimes\sigma_i + \sum_{i=r+1}^{2r}\left|i\right\rangle\left\langle i\right|\otimes\mathbf{I}_k\right]\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle$$

$$= \frac{1}{\sqrt{2}}\left(\left|\mathbf{1}_{2r}\right\rangle\left\langle\mathbf{1}_{2r}\right|\otimes\mathbf{I}_k\right)\left[\sum_{i=1}^{r}\left|i\right\rangle\left\langle i|\mathbf{1}_r\right\rangle\otimes\sigma_i + \sum_{i=r+1}^{2r}\left|i\right\rangle\left\langle i|\mathbf{1}_{r+1,2r}\right\rangle\otimes\mathbf{I}_k\right]\left|\psi_j\right\rangle$$

$$= \frac{1}{\sqrt{2r}}\left(\left|\mathbf{1}_{2r}\right\rangle\left\langle\mathbf{1}_{2r}\right|\otimes\mathbf{I}_k\right)\left[\sum_{i=1}^{r}\left|i\right\rangle\otimes\sigma_i + \sum_{i=r+1}^{2r}\left|i\right\rangle\otimes\mathbf{I}_k\right]\left|\psi_j\right\rangle$$

$$= \frac{1}{\sqrt{2r}}\left(\left|\mathbf{1}_{2r}\right\rangle\left\langle\mathbf{1}_{2r}\right|\otimes\mathbf{I}_k\right)\left[\sum_{i=1}^{r}\left|i\right\rangle\otimes\sigma_i\left|\psi_j\right\rangle + \sum_{i=r+1}^{2r}\left|i\right\rangle\otimes\left|\psi_j\right\rangle\right]$$

$$= \frac{1}{2\sqrt{r}}\left|\mathbf{1}_{2r}\right\rangle\left[\sum_{i=1}^{r}\left\langle\mathbf{1}_r|i\right\rangle\otimes\mathbf{I}_k\sigma_i\left|\psi_j\right\rangle + \sum_{i=r+1}^{2r}\left\langle\mathbf{1}_{r+1,2r}|i\right\rangle\otimes\mathbf{I}_k\left|\psi_j\right\rangle\right]$$

$$= \frac{1}{2r}\left|\mathbf{1}_{2r}\right\rangle\left[\sum_{i=1}^{r}\sigma_i\left|\psi_j\right\rangle + r\left|\psi_j\right\rangle\right] = \frac{1}{2}\left|\mathbf{1}_{2r}\right\rangle\left[\mathbf{M}\left|\psi_j\right\rangle + \left|\psi_j\right\rangle\right] = \frac{1+a_j}{2}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle.$$

□

The next lemma extends Lemma 7.3.

Lemma 7.4. *The probability that algorithm* ECSupVer *does not fail in the first iteration of its loop on an input* $\left|\psi_j\right\rangle$ *is* $\left(\frac{1+a_j}{2}\right)^2$.

Proof. We note that the state at the first measurement by $\mathbf{P}_{2r,k}$ is $\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle$. Therefore, by Definition 6.3, this first measurement by $\mathbf{P}_{2r,k}$ outputs 1 with probability

$$\left\langle\psi_j\right|\left\langle\mathbf{1}_{2r}\right|\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle$$

which, since (by Lemma 6.4) $\mathbf{P}_{2r,k}$ is Hermitian and real, and $\mathbf{P}_{2r,k}^2 = \mathbf{P}_{2r,k}$, is

$$\left(\left\langle\psi_j\right|\left\langle\mathbf{1}_{2r}\right|\mathbf{U}^\dagger\mathbf{P}_{2r,k}^\dagger\right)\left(\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle\right),$$

which by Lemma 7.3 is

$$\left\langle\psi_j\right|\left\langle\mathbf{1}_{2r}\right|\left(\frac{1+a_j}{2}\right)^2\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle = \left(\frac{1+a_j}{2}\right)^2.$$

□

The next lemma extends Lemmas 7.3 and 7.4 to the operation of the entire ECSupVer algorithm, not just one loop. It holds for all states, not just eigenvectors.

Lemma 7.5. *If* $\left|\psi\right\rangle = \sum_{j=1}^{k}\alpha_j\left|\psi_j\right\rangle$ *with* $\alpha_j\in\mathbb{C}$, *then*

$$\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^\tau\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle = \left|\mathbf{1}_{2r}\right\rangle\otimes\sum_{j\in M}\alpha_j\left(\frac{1+a_j}{2}\right)^\tau\left|\psi_j\right\rangle.$$

Proof. It follows from Lemma 7.3 that

$$\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi_j\right\rangle = \left|\mathbf{1}_{2r}\right\rangle \otimes \sum_{j\in M} \alpha_j \left(\frac{1+a_j}{2}\right)\left|\psi_j\right\rangle.$$

Iterating this τ times gives the desired result.

□

We can now define the state of ECSupVer at a particular point in time.

Lemma 7.6. *Suppose that* ECSupVer *accepts for the first i iterations in the loop on some input $|\psi\rangle$. Then the state of the $\mathcal{R}\times\mathcal{S}$ registers after step i in the loop is:*

$$\frac{\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^i\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right|\left\langle\mathbf{1}_{2r}\right|\left(\mathbf{U}^\dagger\mathbf{P}_{2r,k}\right)^{i-1}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^{i-1}\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}}.$$

Proof. Recall that by Definition 6.3, assuming that the first measurement by $\mathbf{P}_{2r,k}$ of ECSupVer accepts, after that the $\mathcal{R}\times\mathcal{S}$ registers will be in a state

$$\frac{\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right|\left\langle\mathbf{1}_{2r}\right|\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}}.$$

The next iteration of the loop, as all of the interations of the loop do, involves multiplying by $\mathbf{U}$ and then taking the PVM $\mathbf{P}_{2r,k}$. Assuming ECSupVer accepts in the second round of the loop, this gives us the following state:

$$\frac{\mathbf{P}_{2r,k}\mathbf{U}\frac{\mathbf{P}_{2r,k}\mathbf{U}|\mathbf{1}_{2r}\rangle|\psi\rangle}{\sqrt{\langle\psi|\langle\mathbf{1}_{2r}|\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}|\mathbf{1}_{2r}\rangle|\psi\rangle}}}{\sqrt{\left(\frac{\mathbf{P}_{2r,k}\mathbf{U}|\mathbf{1}_{2r}\rangle|\psi\rangle}{\sqrt{\langle\psi|\langle\mathbf{1}_{2r}|\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}|\mathbf{1}_{2r}\rangle|\psi\rangle}}\right)^\dagger\mathbf{U}^\dagger\mathbf{P}_{2r,k}^\dagger\mathbf{U}\frac{\mathbf{P}_{2r,k}\mathbf{U}|\mathbf{1}_{2r}\rangle|\psi\rangle}{\sqrt{\langle\psi|\langle\mathbf{1}_{2r}|\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}|\mathbf{1}_{2r}\rangle|\psi\rangle}}}}.$$

Cancelling terms and simplifying gives

$$\frac{\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^2\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right|\left\langle\mathbf{1}_{2r}\right|\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}\mathbf{P}_{2r,k}\mathbf{U}\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}}.$$

After the ith step, we are left with the state

$$\frac{\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^i\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right|\left\langle\mathbf{1}_{2r}\right|\left(\mathbf{U}^\dagger\mathbf{P}_{2r,k}\right)^{i-1}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^{i-1}\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}}$$

as desired.

□

Lemma 7.7. *The probability that* ECSupVer *accepts with input $|\psi\rangle = \sum_{j=1}^k \alpha_j|\psi_j\rangle$ in the ith iteration is*

$$\frac{\sum_{j=1}^k|\alpha_j|^2\left(\frac{1+a_j}{2}\right)^{2i}}{\sum_{j=1}^k|\alpha_j|^2\left(\frac{1+a_j}{2}\right)^{2i-2}}.$$

Proof. First, recall that we do not need to condition this probability on accepting in previous rounds because ECSupVer aborts and outputs 0 if any PVMs fail. By Lemma 7.6, the state of the $\mathcal{R}\times\mathcal{S}$ registers at the $(i-1)$th step is

$$\frac{\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^{i-1}\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right|\left\langle\mathbf{1}_{2r}\right|\left(\mathbf{U}^\dagger\mathbf{P}_{2r,k}\right)^{i-2}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}\left(\mathbf{P}_{2r,k}\mathbf{U}\right)^{i-2}\left|\mathbf{1}_{2r}\right\rangle\left|\psi\right\rangle}}$$

Therefore the probability of the PVM $\mathbf{P}_{2r,k}$ accepting in the ith loop of ECSupVer is just

$$\left(\frac{(\mathbf{P}_{2r,k}\mathbf{U})^{i-1}|\mathbf{1}_{2r}\rangle|\psi\rangle}{\sqrt{\langle\psi|\langle\mathbf{1}_{2r}|(\mathbf{U}^\dagger\mathbf{P}_{2r,k})^{i-2}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}(\mathbf{P}_{2r,k}\mathbf{U})^{i-2}|\mathbf{1}_{2r}\rangle|\psi\rangle}}\right)^\dagger \mathbf{U}^\dagger\mathbf{P}_{2r,k}^\dagger\mathbf{U}$$

$$\cdot\left(\frac{(\mathbf{P}_{2r,k}\mathbf{U})^{i-1}|\mathbf{1}_{2r}\rangle|\psi\rangle}{\sqrt{\langle\psi|\langle\mathbf{1}_{2r}|(\mathbf{U}^\dagger\mathbf{P}_{2r,k})^{i-2}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}(\mathbf{P}_{2r,k}\mathbf{U})^{i-2}|\mathbf{1}_{2r}\rangle|\psi\rangle}}\right)$$

which is

$$\frac{\langle\psi|\langle\mathbf{1}_{2r}|\left(\mathbf{U}^\dagger\mathbf{P}_{2r,k}^\dagger\right)^{i-1}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}(\mathbf{P}_{2r,k}\mathbf{U})^{i-1}|\mathbf{1}_{2r}\rangle|\psi\rangle}{\langle\psi|\langle\mathbf{1}_{2r}|\left(\mathbf{U}^\dagger\mathbf{P}_{2r,k}^\dagger\right)^{i-2}\mathbf{U}^\dagger\mathbf{P}_{2r,k}\mathbf{U}(\mathbf{P}_{2r,k}\mathbf{U})^{i-2}|\mathbf{1}_{2r}\rangle|\psi\rangle}$$

By Lemma 7.5, this is

$$\frac{\sum_{j=1}^k\alpha_j\left(\frac{1+a_j}{2}\right)^i\langle\psi|\otimes\langle\mathbf{1}_{2r}|\mathbf{1}_{2r}\rangle\otimes\sum_{j=1}^k\alpha_j\left(\frac{1+a_j}{2}\right)^i|\psi\rangle}{\sum_{j=1}^k\alpha_j\left(\frac{1+a_j}{2}\right)^{i-1}\langle\psi|\otimes\langle\mathbf{1}_{2r}|\mathbf{1}_{2r}\rangle\otimes\sum_{j=1}^k\alpha_j\left(\frac{1+a_j}{2}\right)^{i-1}|\psi\rangle}$$

which is

$$\frac{\sum_{j=1}^k|\alpha_j|^2\left(\frac{1+a_j}{2}\right)^{2i}}{\sum_{j=1}^k|\alpha_j|^2\left(\frac{1+a_j}{2}\right)^{2i-2}}$$

as desired.

□

The following lemma extends Lemma 7.7:

Lemma 7.8. *Suppose that, on some inputs $|\psi\rangle$, N, and τ, the algorithm* ECSupVer *does not reject before it reaches the loop. Then the probability that algorithm* ECSupVer *accepts on this set of inputs is $\sum_{j=1}^k|\alpha_j|^2\left(\frac{1+a_j}{2}\right)^{2\tau}$, where we note that the weights α_j are the weights of $|\psi\rangle$ at the time the loop in* ECSupVer *starts.*[1]

Proof. First, note that the probability that ECSupVer accepts on an input $|\psi\rangle$ is just the product of the probabilities that it accepts in each of the τ steps of the loop. This is because we abort if we ever fail a measurement, so we do not need to worry about conditional probabilities. By Lemma 7.7, the probability that ECSupVer accepts in the ith step of the loop is

$$\frac{\sum_{j=1}^k|\alpha_j|^2\left(\frac{1+a_j}{2}\right)^{2i}}{\sum_{j=1}^k|\alpha_j|^2\left(\frac{1+a_j}{2}\right)^{2i-2}}.$$

The product of these terms as i runs from 1 to τ is a telescoping product, and gives the desired result.

□

The next result, which is the main result of this section, shows that Algorithm ECSupVer approximately implements the PVM V_j. Theorem 7.9 implies that "proper" money states (where $\alpha_1 = 1$) are always accepted, and "bad" money states (where α_1 is negligible) are not accepted with noticeable probability. Moreover, if we start with a "good enough" money state, we will still have one post-verification.

[1] Note that earlier measurements could have changed these weights.

Theorem 7.9. *Let p be a prime. Let N be a positive integer for which $D := 4p-(p+1-N)^2$ is square-free and larger than $3p$. Let $K = \mathbb{Q}(\sqrt{-D})$, B_K the Bach generating set for K, and suppose B_K is weakly Erdös-Rényi. Let $r = \#B_K$, and suppose $\tau = 33r^3\lambda$.*

1. *If $|\psi\rangle = \sum_{j=1}^{k} \alpha_j |\psi_j\rangle \in \mathcal{V}$ is an arbitrary state, then the probability that* ECSupVer *accepts on input $|\psi\rangle$ is at least $|\alpha_1|^2$ and at most $|\alpha_1|^2 + 2^{-\lambda}$.*
2. *If* ECSupVer *accepts on some input state $|\psi\rangle = \sum_{j=1}^{k} \alpha_j |\psi_j\rangle$, and $|\psi'\rangle = \sum_{j=1}^{k} \alpha'_j |\psi_j\rangle$ is the corresponding output of* ECSupVer*, then $|\alpha'_1| \geq \frac{|\alpha_1|}{\sqrt{|\alpha_1^2|+2^{-\lambda}}}$.*

Proof. By Lemma 7.8, the probability that ECSupVer accepts on input $|\psi\rangle$ is $\sum_{j=1}^{k} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau}$. By Lemma 7.2, we know that $\lambda_2(\mathbf{M}) \leq 1 - \frac{1}{16.5r^3}$, where $\lambda_2(\mathbf{M})$ is the second largest eigenvalue for the matrix $\mathbf{M}$. Thus,

$$\sum_{j\neq 1} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau} \leq \sum_{j\neq 1} |\alpha_j|^2 \left(1 - \frac{1}{33r^3}\right)^{2\tau} \leq \left(1 - \frac{1}{33r^3}\right)^{66r^3\lambda} \leq 2^{-\lambda}.$$

Since

$$\sum_{j=1}^{k} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau} = |\alpha_1|^2 + \sum_{j\neq 1} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau},$$

it is immediate that ECSupVer accepts with probability at least $|\alpha_1|^2$, and moreover, we obtain

$$\sum_{j=1}^{k} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau} \leq |\alpha_1|^2 + 2^{-\lambda}, \tag{13}$$

proving that ECSupVeraccepts with probability at most $|\alpha_1|^2 + 2^{-\lambda}$, which proves part (1).

For the second part, recall that Lemma 7.6 shows that, on an accepting input, just before discarding the $|\mathbf{1}_{2r}\rangle$ qubits at the end of algorithm ECSupVer, the $\mathcal{R}\times\mathcal{S}$ registers will be in state

$$\frac{(\mathbf{P}_{2r,k}\mathbf{U})^{\tau} |\mathbf{1}_{2r}\rangle |\psi\rangle}{\sqrt{\langle\psi| \langle\mathbf{1}_{2r}| (\mathbf{U}^{\dagger}\mathbf{P}_{2r,k})^{\tau-1} \mathbf{U}^{\dagger}\mathbf{P}_{2r,k}\mathbf{U} (\mathbf{P}_{2r,k}\mathbf{U})^{\tau-1} |\mathbf{1}_{2r}\rangle |\psi\rangle}},$$

which by Lemma 7.5 is

$$\frac{|\mathbf{1}_{2r}\rangle \otimes \sum_{j=1}^{k} \alpha_j \left(\frac{1+a_j}{2}\right)^{\tau} |\psi_j\rangle}{\sqrt{\langle\psi| \langle\mathbf{1}_{2r}| (\mathbf{U}^{\dagger}\mathbf{P}_{2r,k})^{\tau-1} \mathbf{U}^{\dagger}\mathbf{P}_{2r,k}\mathbf{U} (\mathbf{P}_{2r,k}\mathbf{U})^{\tau-1} |\mathbf{1}_{2r}\rangle |\psi\rangle}}.$$

After discarding the state in the $\mathcal{R}$-register (which is $|\mathbf{1}_{2r}\rangle$), the $\mathcal{S}$-register has the state:

$$|\psi'\rangle = \frac{\sum_{j=1}^{k} \alpha_j \left(\frac{1+a_j}{2}\right)^{\tau} |\psi_j\rangle}{\sqrt{\sum_{j=1}^{k} \alpha_j \left(\frac{1+a_j}{2}\right)^{\tau} \langle\psi| \otimes \langle\mathbf{1}_{2r}|\mathbf{1}_{2r}\rangle \otimes \sum_{j=1}^{k} \alpha_j \left(\frac{1+a_j}{2}\right)^{\tau} |\psi\rangle}},$$

which (using the argument in the proof of Lemma 7.7) is

$$\frac{\sum_{j=1}^{k} \alpha_j \left(\frac{1+a_j}{2}\right)^{\tau} |\psi_j\rangle}{\sqrt{\sum_{j=1}^{k} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau}}} = \frac{\alpha_1 |\psi_1\rangle + \sum_{j\neq 1} \alpha_j \left(\frac{1+a_j}{2}\right)^{\tau} |\psi_j\rangle}{\sqrt{|\alpha_1|^2 + \sum_{j\neq 1} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau}}}.$$

Since $|\psi'\rangle = \sum_{j=1}^{k} \alpha'_j |\psi_j\rangle$, we have

$$|\alpha'_1| \geq \frac{|\alpha_1|}{\sqrt{|\alpha_1|^2 + \sum_{j\neq 1} |\alpha_j|^2 \left(\frac{1+a_j}{2}\right)^{2\tau}}}$$

By (13) we now have

$$|\alpha'_1| \geq \frac{|\alpha_1|}{\sqrt{|\alpha_1^2| + 2^{-\lambda}}},$$

which is part (2).

□

8 The protocol

Our elliptic curve-related security parameter is a large prime p. We can derive this from the "true" security parameter λ, where $\lambda \approx \log p$. In general, the choice of p will be derived from security of elliptic curve isogeny-related problems.

Minting. The minting algorithm $\mathsf{Gen}\left(1^{\lambda}\right)$ takes as input parameter p (determined implicitly by the security parameter λ) and proceeds as follows.

Algorithm 8.1: Minting Algorithm $Mint$

Input: A prime $p \in \mathbb{Z}$
Output: $|\psi\rangle$, $\sigma \in \mathbb{Z}$

1. Let $\mathcal{S}$ be a quantum register that is capable of holding a representation of an elliptic curve. In $\mathcal{S}$, construct a superposition $\sum |E\rangle$ over all elliptic curves over $\mathbb{F}_p$ using the Algorithm 5.1.
2. Use Schoof's algorithm to compute the number of points in $|E\rangle$ in superposition, and store the result in a new register, yielding the state $\sum |E\rangle |\#E(\mathbb{F}_p)\rangle$
3. In superposition, compute $\Delta_{\mathrm{Fr}}(E)$, then set a third register to be 1 if $\Delta_{\mathrm{Fr}}(E)$ is square-free and $\Delta_{\mathrm{Fr}}(E) > 3p$, and 0 otherwise. Measure this last register; if the result is 0, start over at step 1.
4. Measure the 2nd register (containing $|\#E\left(\mathbb{F}_p\right)\rangle$), and output the resulting state, which we refer to as $|\psi\rangle$ and the measured value σ. The state $|\psi\rangle$ is the bank note and σ is the serial number.

Observe that the state is a superposition over elliptic curves in a specific isogeny class. Note that $\mathsf{Gen}\left(1^{\lambda}\right)$ outputs tuples of the form $\left(|\psi\rangle, \sigma\right)$ as desired.

Verification. The verification algorithm $\mathsf{Ver}\left(|\psi\rangle, \sigma\right)$ does the following. Recall that $|\psi\rangle$ is (supposed to be) a superposition of elliptic curves, and σ is supposed to be the number of points in each of the elliptic curves in superposition.

Algorithm 8.2: Verification Algorithm Ver

Input: $|\psi\rangle$, $\sigma \in \mathbb{Z}$
Output: $\{0, \perp\}$ or $\{1, |\psi'\rangle\}$

1. Run $\mathsf{ECSupVer}\left(|\psi\rangle, \sigma\right)$ and receive an output tuple $(|\psi'\rangle \in \mathcal{S}, b \in \{0,1\})$.
2. **if** $b = 0$ **then return** 0 and $\perp$ and discard $|\psi'\rangle$
3. **else return** 1 and $|\psi'\rangle$

We have deferred a considerable amount of complexity to the actual description of $\mathsf{ECSupVer}$ here which is located in §6.

8.1 Correctness of the Scheme

We next argue that our construction is correct and efficient. We note that this follows almost immediately from the analysis of our ECSupGen and ECSupVer algorithms, but we will present formal arguments here regardless. We start by arguing that, with all but negligible probability, our Gen and Ver algorithms are efficient.

Proposition 8.1. *Let $p > 2^{63}$. For some parameter λ, the minting algorithm* Gen *on inputs p and λ runs in time $O\left(3\lambda \log^8 p\right)$ with probability $1 - 2^{-\lambda}$.*

Proof. From Theorem 10.1, we know that Schoof's algorithm for point counting takes time $O\left(\log^8 p\right)$, and this dominates asymptotically the cost of minting. From Corollary 4.12, we know that the probability of failure in step 3 is at most 86%. Thus, the probability that the algorithm has not terminated after 3λ iterations of step 3 is less than $2^{-\lambda}$. □

We make one further (but important) note on the minting algorithm.

Proposition 8.2. *Let $p > 2^{63}$ be prime. Let $\mathcal{O}$ be $\mathrm{End}(E)$ for all E output by the minting algorithm. Then the class group of $\mathcal{O}$ and the isogeny class of E both have size at least $0.089\frac{\sqrt{p}}{\log p}$.*

Proof. This follows immediately from Corollary 4.14. □

Proposition 8.3. *The verification algorithm* Ver *on inputs $|\psi\rangle$ and σ runs in time*

$$max\left(O\left(\log^8 p\right), O\left(\tau\left(\log^5 p\right)\left(\log\log^2 p\right)\left(\log\log\log^2 p\right)\right)\right).$$

where we set $\tau = 33r^3\lambda$ for $r = \#B_K$.

Proof. This follows immediately from Lemma 6.6. □

Proposition 8.4. *Our quantum money/lightning protocol* (Gen, Ver) *is correct. More precisely, as required by Definition 3.2, for any polynomially sized (in λ) integer i, we have*

$$\mathsf{Ver}^k\left(\mathsf{Gen}\left(1^\lambda\right)\right) = \left(|\psi'\rangle, 1\right) \tag{14}$$

with probability at least $1 - i2^{-\lambda+1}$ for all $k \leq i$ for some state $|\psi'\rangle$.

Proof. This follows from our earlier results evaluating ECSupGen and ECSupVer. More precisely, from Lemma 4.11, we know that, for any prime $p \geq 5$, the algorithm ECSupGen outputs a state $|\psi\rangle$ that has distance $\leq \frac{2}{p}$ from the uniform superposition of all elliptic curves over $\mathbb{F}_p$. Therefore, if we write $|\psi\rangle$ in terms of an eigenbasis, the weight α_1 of the eigenstate $|\psi_1\rangle$ must be at least $\alpha_1 \geq \sqrt{1 - \frac{2}{p}}$.

From Theorem 7.9 we know that $\mathsf{Ver}\left(|\psi\rangle, j\right)$ accepts on an input with probability at least $|\alpha_1|^2$. Thus, Ver accepts on $\mathsf{Gen}\left(1^\lambda\right)$ with probability at least $1 - \frac{2}{p}$.

Also from Theorem 7.9, we know that the output state of ECSupVer (and thus Ver) on some input $|\psi\rangle$ can be written in eigenbasis form where the state $|\psi_1\rangle$ has weight at least $\sqrt{\frac{|\alpha_1|^2}{|\alpha_1|^2 + 2^{-\lambda}}}$. Note that, for $\frac{2^{-\lambda}}{|\alpha_1|^2} \geq 2$, we have

$$\sqrt{\frac{|\alpha_1|^2}{|\alpha_1|^2 + 2^{-\lambda}}} \geq \sqrt{1 - \frac{2^{-\lambda}}{|\alpha_1|^2}} \tag{15}$$

Therefore, in the output state $|\psi''\rangle = \mathsf{Ver}\left(\mathsf{Gen}\left(1^\lambda\right)\right)$, we have that $|\psi''\rangle$ contains the eigenstate $|\psi_1''\rangle$ with weight $\alpha_1'' \geq \sqrt{1 - \frac{2^{-\lambda}}{1 - \frac{2}{p}}}$. Note that this is exceptionally close to 1.

In particular, as long as $|\alpha_1|^2 \geq \frac{1}{2}$ for any $|\psi\rangle$ that is input to ECSupVer, we know that the output will be at most a distance of $2^{-\lambda+1}$ from $|\psi_1\rangle$. Through a simple inductive argument, we can see that this will always be the case. Therefore ECSupVer and, correspondingly, Ver will accept on an input from Gen with probability at least $1 - 2^{-\lambda+1}$ in each verification. The final result follows from a simple union bound.

□

9 Security of our Construction

In this section we discuss security and security proofs for our construction.

9.1 Security Proofs and Assumptions

Quantum Money. We begin by defining our immediate security assumption for quantum money. Looking ahead, this assumption is slightly more complicated than our immediate security assumption for quantum lightning (but also directly implied by it).

In Theorem 9.2 below we show that the security of our quantum money protocol from section 8 is equivalent to the difficulty of the following problem, which we call the Elliptic Curve Superposition Duplication Problem for a prime p.

Definition 9.1. Elliptic Curve Superposition Duplication Problem ($ECSDP_p$): The prime p is fixed. Suppose we consider an elliptic curve E_s sampled uniformly at random from all elliptic curves E over $\mathbb{F}_p$ with Frobenius discriminant $\Delta_{\mathrm{Fr}}(E) \geq 3p$ and square-free. Given a superposition $|\rho\rangle = \sum |E\rangle$ of all elliptic curves over $\mathbb{F}_p$ in the same isogeny class as E_s, create two (possibly entangled) quantum states that are negligibly far from $|\rho\rangle$.

The security of our construction in the quantum money game is equivalent to this hardness assumption, which we formalize in the following theorem.

Theorem 9.2. *Any adversary that can win the quantum money unforgeability game of Definition 3.3 with respect to the quantum money protocol in §8 on input value p with non-negligible advantage can be used to solve the $ECSDP_p$ with non-negligible advantage. Moreover, any adversary that can solve the $ECSDP_p$ with non-negligible advantage can be used to win the quantum money unforgeability game with respect to the quantum money protocol on input p with non-negligible advantage.*

Proof. We show both directions of the implication below.

The Forward Direction. First, suppose that there exists an adversary $\mathcal{A}$ that can solve the quantum money unforgeability game in Definition 3.3 with non-negligible probability. We show that the adversary $\mathcal{A}$ can be used to create a new adversary $\mathcal{A}'$ that solves the $ECSDP_p$ problem with non-negligible probability.

Recall that in the $ECSDP_p$ problem, for an elliptic curve E_s sampled uniformly at random from all elliptic curves over $\mathbb{F}_p$ with discriminant $\Delta_{\mathrm{Fr}} \geq 3p$ and square-free, the adversary $\mathcal{A}'$ will be given a superposition $|\rho\rangle$ of all elliptic curves over $\mathbb{F}_p$ in the same isogeny class as E_s. $\mathcal{A}'$ computes the number of points in the superposition $|\rho\rangle$ in an adjacent register using Schoof's algorithm, calls this number N, and measures this new register. Note that the measurement will not affect the state $|\rho\rangle$ because it is guaranteed by the definition of the $ECSDP_p$ problem that $|\rho\rangle$ contains only elliptic curves in the same isogeny class.

Then $\mathcal{A}'$ sends the tuple $(|\rho\rangle, N)$ to the adversary $\mathcal{A}$. Note that, by definition 3.3 and the description of our protocol 8 this is correct distribution of inputs that the quantum money unforgeability adversary $\mathcal{A}$ requires.

Next, $\mathcal{A}$ outputs two states $|\psi\rangle, |\psi'\rangle$ such that $\mathsf{Ver}(|\psi\rangle, N) = \mathsf{Ver}(|\psi'\rangle, N) = 1$ with non-negligible probability. Therefore, $|\psi\rangle$ and $|\psi'\rangle$ must be accepted by $\mathsf{ECSupVer}$ with non-negligible probability. As in §6, for a state $|\psi\rangle$, let $|\psi_1\rangle, ..., |\psi_k\rangle$ be an eigenbasis for $\mathbf{M}$ and write $|\psi\rangle = \sum_{j=1}^{k} \alpha_j |\psi_j\rangle$, where the α_js are listed in decreasing order of their norms. From Theorem 7.9, we know that $\mathsf{ECSupVer}$ can be run on these states to output a state $|\psi'\rangle$ where α_1' will be $\geq 1 - \mathsf{negl}(\lambda)$). Thus, $\mathcal{A}'$ only needs to run $\mathsf{ECSupVer}$ on the outputs it receives from $\mathcal{A}$ and then output these states, and this output will be two states that solve the $ECSDP_p$ with non-negligible probability.

The Reverse Direction. Next, suppose that there exists an adversary $\mathcal{A}$ that can solve the $ECSDP_p$ with non-negligible advantage. We show how to build an adversary $\mathcal{A}'$ that can solve the quantum money unforgeability problem for our protocol with non-negligible advantage.

So, suppose that $\mathcal{A}'$ is given an instance of the quantum money unforgeability problem, which consists of a tuple $(|\psi\rangle, N)$, where $|\psi\rangle$ represents a uniform superposition over all elliptic curves in $\mathscr{E}_{\mathsf{sf},3p}$ with N points. $\mathcal{A}'$ immediately forwards this to $\mathcal{A}$, which then outputs two states $|\psi'\rangle$, $|\psi''\rangle$ which are negligibly far from the uniform superposition over all elliptic curves in $\mathscr{E}_{\mathsf{sf},3p}$ with N points with non-negligible probability.

From Theorem 7.9, we know that $\mathsf{ECSupVer}$ (and thus Ver) accepts on some state $|\psi\rangle$ with probability $\alpha_1^2 + 2^{-\lambda}$. Since $|\psi'\rangle$ and $|\psi''\rangle$ are negligibly far from the uniform superposition over all elliptic curves in $\mathscr{E}_{\mathsf{sf},3p}$ with N points with non-negligible probability, we know that, respectively, α_1' and α_1'' are negligibly far from one. Therefore $\mathcal{A}'$ can immediately output the tuple $(|\psi'\rangle, |\psi''\rangle, N)$ and this will be a tuple that wins the quantum money unforgeability game with non-negligible probability.

Conclusion. Since we have shown both directions of our claim, we have completed the proof.

□

A Note on State Amplification. Once again, for a state $|\psi\rangle$, let $|\psi_1\rangle, ..., |\psi_k\rangle$ be an eigenbasis for $\mathbf{M}$ and write $|\psi\rangle = \sum_{j=1}^{k} \alpha_j |\psi_j\rangle$, where the α_js are listed in decreasing order of their norms. In the proof of Theorem 9.2, we used the fact that the algorithm $\mathsf{ECSupVer}$ could take a state $|\psi\rangle$ with a non-negligible weight α_1 and turn it into some state $|\psi''\rangle$ where all *but* non-negligible weight is on α_1''. Note that this means for the $ECSDP_p$ problem that we can turn states that are "somewhat" close to correct into states that are negligibly far from perfect. This observation may be useful for studying the hardness of the $ECSDP_p$ problem in the future.

Quantum Lightning. We next define our immediate security assumption for quantum lightning. In Theorem 9.4 below we show that the security of our quantum lightning protocol from §8 is equivalent to the difficulty of the following problem, which we call the Elliptic Curve Superposition Collision Problem for a prime p.

Definition 9.3. Elliptic Curve Superposition Collision Problem ($ECSCP_p$): The prime p is fixed. Create two (possibly entangled) quantum states that are each negligibly far from the superposition of all elliptic curves over $\mathbb{F}_p$ in some isogeny class with Frobenius discriminant $\Delta_{\mathrm{Fr}} \geq 3p$ and square-free.

Theorem 9.4. *Any adversary that can win the quantum lightning game of Definition 3.4 with respect to the protocol with respect to the quantum lightning protocol in §8 on input value p with non-negligible advantage can be used to solve the $ECSCP_p$ with non-negligible advantage. Moreover, any adversary that can solve the $ECSCP_p$ with non-negligible advantage can be used to win the quantum lightning game with respect to the quantum lightning protocol on input p with non-negligible advantage.*

Proof. Our proof here is essentially a simpler version of that of Theorem 9.2. This is because the quantum lightning security game can be thought of as similar to the quantum money game, except the adversary is not provided with an initial money state/elliptic curve superposition. We note that the fact that the adversary gets to choose the isogeny class in the lightning game does not change the logic of the reduction at all.

Thus, our logic for this proof follows from exactly the same reasoning as in 9.2, so we omit it here to avoid duplication.

□

9.2 Intuition for the Hardness of these Assumptions

In this subsection, we offer evidence as to why our assumptions might be hard. To start, suppose we consider the following problem: given N and $E_1 \in \mathcal{I}_N$, construct the superposition $|\mathcal{I}_N\rangle$. While assuming this problem is hard clearly implies a weaker assumption than what we need for security, examining it is intuitive. The only known method to accomplish this is some variant of Computing $|\mathcal{I}_N\rangle$ using the class group action, as follows.

We compute the ideal class group $\mathrm{Cl}(\mathcal{O})$ associated to K, and construct the superposition

$$\sum_{c \in \mathrm{Cl}(\mathcal{O})} |c\rangle .$$

Then in superposition we apply c to E_1 to obtain

$$\sum_{c} |c * E_1\rangle |c\rangle .$$

We uncompute and discard the second register. The resulting state is then $|\mathcal{I}_N\rangle$. (If we do not uncompute the second register, then the state will with overwhelming probability fail to verify; see below.)

But uncomputing c is exactly the elliptic curve isogeny problem for ordinary curves: given isogenous elliptic curves E, E_1, find c such that $c * E_1 = E$. This is precisely the problem underlying the security of CRS.

Of course if $\#\mathcal{I}_N$ is small, then we can uncompute c. But by Corollary 4.14, Algorithm 8.1 generates an isogeny class of size $\geq 0.089 \frac{\sqrt{p}}{\log p}$, which is superpolynomial.

Now consider our security problem 9.1. In that problem, the adversary is given one copy of $|\mathcal{I}_N\rangle$. By measuring, the adversary obtains a single elliptic curve $E_1 \in \mathcal{I}_N$. But then they must construct a superposition from E_1 as discussed above.

We now show that if we do *not* uncompute the second register of

$$\sum_{c \in \mathrm{Cl}(\mathscr{O})} |c * E_1\rangle |c\rangle ,$$

then verification fails with all but negligible probability. To take into account the additional register containing the class group data in our verification protocol, we replace $\mathbf{P}_{2r,k}, \mathbf{U}$ with $\mathbf{P}_{2r,k} \otimes I_k, \mathbf{U} \otimes I_k$, respectively. Note that $\mathbf{P}_{2r,k} \otimes I_k = \mathbf{P}_{2r,2k}$. Let $c_1, \ldots, c_k$ be the elements of $\mathrm{Cl}(\mathscr{O})$ with c_1 the identity, and let $E_j = c_j * E_1$, so that $\mathcal{I}_N = \{E_1, \ldots, E_k\}$.

Let $|\psi_1\rangle, \ldots, |\psi_k\rangle$ be as in our proof of the verification algorithm. As they are eigenvectors for the real symmetric matrix $\mathbf{M}$, we can additionally require that they form an orthonormal basis. Suppose

$$|\psi_i\rangle = \sum_{j=1}^{k} u_{ij} |E_j\rangle .$$

Set

$$|\varphi_i\rangle = \sum_{j=1}^{k} \overline{u_{ij}} |c_j\rangle .$$

Let δ_{ij} denote the Kronecker delta.

Lemma 9.5. *For all* $1 \leq r, s \leq k$,

$$\sum_{i=1}^{k} u_{ir} \overline{u_{is}} = \delta_{rs}.$$

Proof. Let Ψ be the matrix with entries given by the u_{ij}. The rows of Ψ are the coordinates of the $|\psi_i\rangle$. The $|\psi_i\rangle$ are orthonormal, so Ψ is unitary and therefore has orthonormal columns as well. The claim follows. □

Proposition 9.6.

$$\sum_{i=1}^{k} |E_i\rangle |c_i\rangle = \sum_{i=1}^{k} |\psi_i\rangle |\varphi_i\rangle .$$

Proof. For all $1 \leq r, s \leq k$, we have

$$\langle c_s| \langle E_r| \sum_i |E_i\rangle |c_i\rangle = \delta_{rs}.$$

On the other hand,

$$\begin{aligned}\langle c_s| \langle E_r| \sum_i |\psi_i\rangle |\varphi_i\rangle &= \sum_i \langle c_s| \langle E_r|\psi_i\rangle |\varphi_i\rangle \\ &= \sum_i u_{ir} \langle c_s|\varphi_i\rangle \\ &= \sum_i u_{ir}\overline{u_{is}} \\ &= \delta_{rs}.\end{aligned}$$

Since the $|E_r\rangle |c_s\rangle$ form a basis for the ambient vector space, the claim follows. □

Theorem 9.7. *Let p be a prime. Let N be a positive integer for which $D := 4p - (p+1-N)^2$ is square-free and larger than $3p$. Let $K = \mathbb{Q}(\sqrt{-D})$, B_K the Bach generating set for K, and suppose B_K is weakly Erdös-Rényi. Let $r = \#B_K$, and suppose $\tau = 33r^3\lambda$. If $|\beta\rangle = \frac{1}{\sqrt{k}} \sum_{i=1}^{k} |E_i\rangle |c_i\rangle$, then the probability that* ECSupVer *accepts on input $|\beta\rangle$, with the last register hidden, is at most $\frac{1}{k} + 2^{-\lambda}$.*

In particular, since k is superpolynomial in λ, the probability of acceptance is negligible.

Proof. From the previous proposition,

$$|\beta\rangle = \frac{1}{\sqrt{k}} \sum_{i=1}^{k} |\psi_i\rangle |\varphi_i\rangle .$$

As $P_{2r,2k}$ and $\mathbf{U} \otimes I_k$ act trivially on the last register of $\mathbf{1}_{2r} \otimes |\beta\rangle$, the analysis of Section 7 goes through. In particular, we can apply Theorem 7.9, where for $|\beta\rangle$, we have $\alpha_1 = \frac{1}{\sqrt{k}}$. The claim follows. □

9.3 Application of Proofs from [LMZ23] and [Zha24]

In [LMZ23], the authors showed that their generic construction of invariant money could be secure if two assumptions held: the "hardness of path finding" and "knowledge of path". Rather than spell these out generically, we will explain them in terms of elliptic curve isogenies (and later formally define them, of course). Informally, the "hardness of path assumption" translates to the hardness of the discrete log on class group actions in our setting, and the "knowledge of path" assumption translates to the assumption that if any adversary knows two elements in some isogeny class, it must know an isogeny (or set of isogenies) that represents a path between them.

Zhandry's Attack. In his very recent work [Zha24], Zhandry showed that the knowledge of path assumption did not hold over group actions. Instead, Zhandry created a new assumption that he called the *quantum modified knowledge of group element assumption* (q-mKGEA) and used this as one of the ways that he proved security of his construction. Informally speaking, this assumption stated that even if an adversary did create two group action set elements for which a "path" between them could not be inferred from its state, it wasn't useful for the adversary's final outputs, and there existed an equally powerful adversary that did not do this.

Our Extensions. In this subsection, we extend this line of reasoning to give evidence why our $ECSCP_p$ might be hard. In particular, we show that, informally speaking, that if the group action discrete log (GA-DLog) problem over isogeny class groups is hard, and a modification of the q-mKGEA assumption is hard, then the $ECSCP_p$ is hard. It is also possible to interpret these results as saying that, assuming the GA-DLog problem is hard (which seems likely to us), any adversary that solves the $ECSCP_p$ problem must exploit a peculiar quantum property in a way that would be very interesting in and of itself.

Below, we formally state our assumptions necessary for our proofs.

Definition 9.8. Arbitrary Isogeny Class Group Action Discrete Logarithm Problem with prime p ($AICGA$-$DLog_p$). Consider some prime p. The $AICGA$-$Dlog_p$ problem is defined between a challenger and an adversary as follows: the adversary picks an elliptic curve E over $\mathbb{F}_p$ such that $D \geq 3p$. The challenger selects two elliptic curves E_1 and E_2 uniformly at random from the isogeny class of E. The adversary wins the game if they can output an isogeny (or polynomially-sized path of isogenies) that map E_1 to E_2.

We note that this is very similar to traditional discrete log, with the exception that the adversary is allowed to choose the isogeny class from which the challenge is sampled. We note that this would be analogous to letting the adversary choose a particular group from a family of groups in the traditional, classical discrete log setting.

We next introduce our variant of Zhandry's q-mKGEA assumption. To do this, we will first need to define our analogue of *group action games*, which Zhandry also introduced in [Zha24].

Definition 9.9. Isogeny Class Group Action Game. A *one-round isogeny class group action game* with parameter p is given by an interactive algorithm called a challenger, which we will denote by Ch. In the game, Chsends a set of (classical) parameters derived from some setup algorithm taking as input a security parameter λ (and p) to an adversary $\mathcal{A}$ and then receives back a single quantum message from $\mathcal{A}$, before deciding if $\mathcal{A}$ wins and outputting 1 if this is the case. We denote such a game Ch^p and say that an adversary $\delta(\lambda)$-wins Ch^p if $\mathsf{Ch}^p(\lambda)$ outputs 1 with probability at least $\delta(\lambda)$ when interacting with $\mathcal{A}$.

With this in mind, we are ready to define our own variant of Zhandry's q-mKGEA assumption, which we call the q-$mKCGEA_p$ assumption. We note that our assumption is in a sense applying the principles of Zhandry's mKGEA assumption to the KGEA assumption from [LMZ23].

Definition 9.10. Quantum Modified Knowledge of Class Group Element Assumption with parameter p (q-$mKCGEA_p$). Fix a parameter p. The q-$mKGEA_p$ assumption holds if the following is true: consider a one-round isogeny class group action game Ch and any QPT adversary $\mathcal{A}$ that $\delta(\lambda)$ wins Ch for some non-negligible function δ.

Suppose we write the message from $\mathcal{A}$ to Ch as $\rho_{1,2,3}$, which we define as a joint system over two registers which we denote 1, 2, and 3, respectively. Consider measuring the first and second registers and suppose that we obtain elliptic curves E_1 and E_2. We can denote this process and output as $(E_1 E_2 |\psi\rangle) \leftarrow \left[\mathcal{A}'\left(1^\lambda\right) \leftrightarrow \mathsf{Ch}\left(1^\lambda\right)\right]$.

Then, for all such δ, $\mathcal{A}$, and Ch, there exists another non-negligible δ' and a QPT $\mathcal{A}'$ that δ'-wins Ch, and moreover there exists a QPT extractor $\mathcal{E}$ and function ϵ of λ such that the following holds:

$$\Pr\left[E_1, E_2 \in \mathscr{E}_{\mathsf{sf},3p} \text{ and } E_2 \neq \varphi(E_1) : \begin{array}{c}(E_1 E_2 |\psi\rangle) \leftarrow \left[\mathcal{A}'\left(1^\lambda\right) \leftrightarrow \mathsf{Ch}\left(1^\lambda\right)\right] \\ \varphi \leftarrow \mathcal{E}(E_1 E_2 |\psi\rangle)\end{array}\right] \leq \epsilon(\lambda) \tag{16}$$

What does this mean in words? Suppose there is some adversary that can win a isogeny class group action game. Then there must exist some other adversary that succeeds with similar advantage that knows isogenies between certain elliptic curves (possibly in superposition) in the adversary's final state. Zhandry [Zha24] discusses at length how this "patches" the knowledge of group element assumption (KGEA) from [LMZ23] and how it allows for many oblivious samplers of elliptic curves, which is not the case for the KGEA assumption, so we defer a length discussion on this assumption to that work.

Proof of Security. We are finally ready to show that the $ECSCP_p$ is hard assuming that $AICGA-DLog_p$ is hard and that the $q-MKCGEA_p$ assumption holds. Our proof mirrors that of the security proof for invariant money in [LMZ23], although we specifically tailor it to elliptic curve isogenies. We state this in the following theorem:

Theorem 9.11. *Suppose that the $AICGA_DLog_p$ problem as defined in definition 9.8 is hard and that the $q-mKCGEA_p$ assumption as defined in definition 9.10 holds true. It is the case that the $ECSCP_p$ as defined in definition 9.3 is hard.*

Proof. We will argue a proof by contradiction. So, suppose $\mathcal{A}$ is a QPT adversary that can solve the $ECSCP_p$ with non-negligible advantage ϵ. We note that we can effectively guarantee that $\mathcal{A}$ wins with all but negligible probability since we can just run $\mathcal{A}$ a total of $\frac{\lambda}{\epsilon}$ times, ensuring we get a success with high probability. Note that we can always check whether or not an attempt by $\mathcal{A}$ was successful by using the Ver algorithm. For simplicity and ease of understanding, we will assume the success probability is actually 1, incurring only a negligible error. Not assuming this would only complicate our expressions and not change anything fundamental about the proof.

By the deferred measurement principle, we may assume without loss of generality that $\mathcal{A}$ is unitary, so that the output is a pure state $\sum_{x,z,s}\alpha_{x,z,s}|x,z,s\rangle$, where the first two registers are the supposed quantum money states, and the last register is auxiliary state left over by running $\mathcal{A}$.

Suppose we let $|\psi'\rangle$ denote the uniform superposition of elliptic curves in $\mathscr{E}_{\mathsf{sf},3p}$ with j points. Since the output of $\mathcal{A}$ passes verification with probability $1-\mathsf{negl}$, we can instead write the output of $\mathcal{A}$ as something negligibly far from:

$$|S\rangle = \sum_s \beta_s |\psi_j\rangle |\psi_j\rangle |s\rangle \tag{17}$$

Let $\mathcal{E}$ be the extractor guaranteed by applying the $q-mKCGEA_p$ assumption to the adversary $\mathcal{A}$. Now consider measuring both of the registers containing $|\psi'\rangle$, getting elliptic curves E_1 and E_2, respectively, and leaving the auxiliary state as

$$\psi'' \propto \sum_s \beta'_s |s\rangle \tag{18}$$

Then we know that $\mathcal{E}(E_1, E_2, |\psi''\rangle)$ outputs φ such that, with overwhelming probability over E_1 and E_2, we have $E_2 = \varphi(E_1)$. Next, notice that for any E, E' in the set $\mathscr{E}_{\mathsf{sf},3p}$ with j points, the probability of obtaining E_1, E_2 in our measurement is identical to the probability of obtaining any other elliptic curves E, E', and the state $\psi'' \propto \sum_s \beta'_s |s\rangle$. In particular, we have that $\mathcal{E}(E_1, E_2, |\psi''\rangle)$ outputs an isogeny ψ such that $E_2 = \psi(E_1)$ with non-negligible probability.

We can use this observation to construct an adversary for the $AICGA-DLog_p$ problem, contradicting our assumptions and completing the proof.

Let $\mathcal{A}_D$ be the following $AICGA-DLog_p$ adversary:

- Run $\mathcal{A}$ and measure both registers containing $|\psi_j\rangle$, obtaining the state $|\psi''\rangle$.
- Send the elliptic curve E_1 to the challenger, obtaining two elliptic curves E, E in response.
- Run $\mathcal{E}(E, E', |\psi''\rangle)$ to get an output φ. Output φ.

Note that the probability of the measurement outputting E and E' is exactly the same as of it outputting E_1 and E_2. Therefore the extractor $\mathcal{E}$ should work with both sets of elliptic curves with equal probability, contradicting the $AICGA-DLog_p$ assumption, which completes the proof.

□

Comments on the Assumptions. We note that the $AICGA-DLog_p$ essentially boils down to the group action discrete log problem for isogenies, except that the adversary controls the isogeny class where the discrete log challenge happens. While in a traditional key exchange protocol the adversary would not get to pick the isogeny class, we note that if this assumption is not hard, then key exchange from isogeny class

groups is also very unlikely to be hard–the only way this would not be the case is if some isogeny classes where $\Delta_{\text{Fr}} \geq 3p$ and square-free were substantially harder than others, which would be quite surprising.

On the other hand, the $q - mKCGEA_p$ is very much an unstudied assumption and could certainly be false. Notably, as we mentioned earlier, Zhandry [Zha24] broke the analogous KGEA assumption in [LMZ23], which is why the assumption we use here takes its current form. What we can use this assumption to show, though, is that any adversary that solves the $ECSCP_p$ algorithm must most likely *not* remember the isogenies between elements in the isogeny class groups that it uses, which means that such an adversary must take considerably different form than most simple quantum algorithms today.

10 Additional number theory background

Given an elliptic curve $E/\mathbb{F}_p$, the Frobenius endomorphism satisfies a quadratic polynomial of the form $x^2 - tx + p$, where t is an integer, called the *Frobenius trace*, and $|t| < 2\sqrt{p}$. Two elliptic curves are isogenous over $\mathbb{F}_p$ if and only if their Frobenius traces are equal. The number of points $\#E(\mathbb{F}_p)$ is equal to $p + 1 - t$.

Theorem 10.1. *Given an elliptic curve $E/\mathbb{F}_p$, there is a classical algorithm for computing the trace of Frobenius t, and $\#E(\mathbb{F}_p)$, in time $O(\log^8 p)$.*

This is Schoof's point-counting algorithm; see [Sch95, p. 235].

We say E is *ordinary* if $t \neq 0$. Going forward, we will restrict our attention to ordinary elliptic curves since the isogeny classes in our protocol are always ordinary. Let K be the quadratic extension of $\mathbb{Q}$ generated by a root of $x^2 - tx + p$, and let $D = D(E)$ denote the absolute value of its discriminant. Write $\Delta_{\text{Fr}}(E) = 4p - t^2$, so that $\Delta_{\text{Fr}} = f^2 D$ for some integer f. Let Fr denote the Frobenius endomorphism of E. Then the endomorphism ring $\mathcal{O}$ of E is isomorphic to an order in K containing $\mathbb{Z}[\text{Fr}]$. We have $\mathbb{Z}[\text{Fr}]$ equals the maximal order of K if and only if $\Delta_{\text{Fr}} = D$. It follows that if Δ_{Fr} is square-free, then $\mathcal{O} = \mathbb{Z}[\text{Fr}] =$ the maximal order of K.

Let $\text{Cl}(\mathcal{O})$ denote the ideal class group of $\mathcal{O}$. The main theorem of complex multiplication states that $\text{Cl}(\mathcal{O})$ acts simply transitively on the set of isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}$. Therefore if $D(E) = \Delta_{\text{Fr}}(E)$, then $\text{Cl}(\mathcal{O})$ acts simply transitively on the entire isogeny class of E.

The proof of Theorem 4.1 makes reference to the theory of modular forms, an extremely technical and deep area of number theory. For our purposes, we will only need the following. Let $\mathbb{H} = \{z = x + yi \in \mathbb{C} : y > 0\}$. For an even positive integer k, a *cusp form of weight k* is a holomorphic function

$$f : \mathbb{H} \to \mathbb{C}$$

which can be written $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$, and such that if $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is a 2×2 integer matrix with determinant 1, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

For a given k, the space of weight k cusp forms S_k forms a vector space over $\mathbb{C}$. Given a prime p, there is a linear operator $T_k(p)$ called the *p-Hecke operator of weight k*,

$$T_k(p) : S_k \to S_k,$$

given by

$$T_k(p)(f) = p^{k-1} f(pz) + \frac{1}{p} \sum_{b=0}^{p-1} f\left(\frac{z+b}{p}\right).$$

For (much!) more background on modular forms, cusp forms, and Hecke operators and their uses, see [DS05]. For an application of modular forms to quantum money, see [KSS21].

The proof of Theorem 4.1 also makes use of *Beurling-Selberg polynomials*. For a given interval $I = [x_0, x_1]$, let χ_I be the characteristic, or indicator, function of I; that is, $\chi_I(x) = 1$ if $x \in I$ and $\chi_I(x) = 0$ otherwise.

For a positive integer M, the Beurling-Selberg polynomials $S^+_{M,I}$ and $S^-_{M,I}$ are degree M trigonometric polynomials giving close approximations to χ_I, and satisfying

$$S^-_{M,I}(x) \leq \chi_I(x) \leq S^+_{M,I}(x)$$

for all x. See Montgomery [Mon94, §1.2] for more information.

Recall that for $I \subset [-1,1]$, $\mu_{ST}(I) = \frac{2}{\pi}\int_I \sqrt{1-X^2}\,dX$. The measure μ_{ST} is known as the *Sato-Tate measure*, and appears in many statistical results in number theory.

Lemma 10.2 (Hensel's Lemma)**.** *Let p be prime, i a positive integer, and f an integer polynomial. If α is an integer satisfying $f(\alpha) \equiv 0 \pmod{p^i}$ and $f'(\alpha) \not\equiv 0 \pmod{p}$, then there exists unique $\beta \in \mathbb{Z}/p^{i+1}\mathbb{Z}$ satisfying $\beta \equiv \alpha \pmod{p^i}$ and $f(\beta) \equiv 0 \pmod{p^{i+1}}$.*

The Möbius function μ is defined as follows: if n is not square-free, then $\mu(n) = 0$. Otherwise, $\mu(n)$ is $(-1)^r$, where r is the number of prime factors of n.

SEA algorithm. Here, we elaborate on the proof of Theorem 4.15. In [DKS18, p. 12], the authors mention that the bottleneck in the SEA algorithm is computing the $\mathbb{F}_p$-rational roots of the modular polynomial $\Phi_\ell(x, j_0)$. This is a degree $\ell+1$ polynomial whose roots are the j-invariants of elliptic curves ℓ-isogenous to the curve with j-invariant j_0. In our protocol, Φ_ℓ will always have at most 2 roots. To compute these roots, we compute $\gcd(\Phi_\ell, x^p - x)$. To do this efficiently, use successive squaring to compute $x^p \pmod{\Phi_\ell}$; this take $O(\log p)$ steps. Each step involves multiplying polynomials of degree $O(\ell)$. Using the fast Fourier transform, each multiplication can be accomplished in time $O(M(p)\ell \log \ell \log\log \ell)$.

11 Heuristic for Erdös-Rényi assumption

We now give heuristic evidence for Assumption 4.19. The Chebotarev density theorem states that if we fix K, then asymptotically the classes of the primes are uniformly distributed in $\mathrm{Cl}(\mathscr{O}_K)$, giving evidence for random distribution. Unfortunately the primes contributing to B_K are small, so the asymptotic is not so helpful. However, Lagarias and Odlyzko prove an effective version of the Chebotarev density theorem that ensures a certain uniformity in the distribution of small primes, as follows. Let $\chi : \mathrm{Cl}(\mathscr{O}_K) \to \mathbb{Z}/n\mathbb{Z}$ be a surjective homomorphism for some small n. Lagarias and Odlyzko [LO77, Corollary 1.2] show that, assuming GRH, for each $i \in \mathbb{Z}/n\mathbb{Z}$, there is a prime $\mathfrak{l}$ of size $O(n^2(\log D)^2)$ with $\chi([\mathfrak{l}]) = i$. Taking n to be the product of small sets of small prime factors $p_1, \ldots, p_r$ of $\#\mathrm{Cl}(\mathscr{O}_K)$, this suggests that the distribution of classes in B_K in

$$\mathrm{Cl}(\mathscr{O}_K)/p_1\,\mathrm{Cl}(\mathscr{O}_K) \times \cdots \times \mathrm{Cl}(\mathscr{O}_K)/p_r\,\mathrm{Cl}(\mathscr{O}_K)$$

should look like a product of r independent distributions. It is in this sense that B_K looks like randomly sampled elements.

12 Acknowledgements

The authors would like to thank Alice Silverberg, Alina Bucur, and Mark Zhandry for helpful conversations. Thanks also to Neha Prabhu for assistance with the proof of Theorem 4.1, and to Henryk Iwaniec for assistance with the proofs of Lemmas 4.3, 4.4, and 4.5.

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Proceedings of the 2009 24th Annual IEEE Conference on Computational Complexity*, CCC '09, pages 229–242, Washington, DC, USA, 2009. IEEE Computer Society. 1

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In Howard J. Karloff and Toniann Pitassi, editors, *44th ACM STOC*, pages 41–60. ACM Press, May 2012. 1, 4, 7

[ADMP20] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 411–439. Springer, Heidelberg, December 2020. 5

[ALL+21] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 526–555, Virtual Event, August 2021. Springer, Heidelberg. 3

[AMRR11] Andris Ambainis, Loïck Magnin, Martin Roetteler, and Jérémie Roland. Symmetry-assisted adversaries for quantum state generation. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 167–177. IEEE, 2011. 17

[Bab91] László Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. In *23rd ACM STOC*, pages 164–174. ACM Press, May 1991. 17

[Bac90] Eric Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990. 8

[BB87] Charles H. Bennett and Gilles Brassard. Quantum public key distribution reinvented. *SIGACT News*, 18(4):51–53, July 1987. 3

[BDGM20] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Factoring and pairings are not necessary for iO: Circular-secure LWE suffices. Cryptology ePrint Archive, Report 2020/1024, 2020. https://eprint.iacr.org/2020/1024. 2

[BDS16] Shalev Ben-David and Or Sattath. Quantum tokens for digital signatures, 2016. https://arxiv.org/abs/1609.09047. 2

[BGMZ18] James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry. Return of GGH15: Provable security against zeroizing attacks. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018, Part II*, volume 11240 of *LNCS*, pages 544–574. Springer, Heidelberg, November 2018. 2

[Bir68] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *Journal of the London Mathematical Society*, s1-43(1):57–60, 01 1968. 9, 14

[BKZ18] Bruce C. Berndt, Sun Kim, and Alexandru Zaharescu. The circle problem of Gauss and the divisor problem of Dirichlet—still unsolved. *The American Mathematical Monthly*, 125(2):99–114, 2018. 12

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 556–584, Virtual Event, August 2021. Springer, Heidelberg. 3

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. https://eprint.iacr.org/2006/291. 3

[CPDDF+19] Marta Conde Pena, Raul Durán Díaz, Jean-Charles Faugère, Luis Hernández Encinas, and Ludovic Perret. Non-quantum cryptanalysis of the noisy version of Aaronson–Christiano's quantum money scheme. *IET Information Security*, 13(4):362–366, 2019. 1

[Del74] Pierre Deligne. La conjecture de Weil : I. *Publications Mathématiques de l'IHÉS*, 43:273–307, 1974. 10

[DKS18] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 365–394. Springer, Heidelberg, December 2018. 3, 15, 34

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer, 2005. 10, 33

[ER65] P. Erdös and A. Rényi. Probabilistic methods in group theory. *Journal d'Analyse Mathématique*, 14(1):127–138, Dec 1965. 17

[FGH+10] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, Daniel Nagaj, and Peter Shor. Quantum state restoration and single-copy tomography for ground states of hamiltonians. *Physical review letters*, 105(19):190503, 2010. 1

[FGH+12] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter W. Shor. Quantum money from knots. In Shafi Goldwasser, editor, *ITCS 2012*, pages 276–289. ACM, January 2012. 1, 5, 18

[FI10] J. B. Friedlander and H. Iwaniec. Square-free values of quadratic polynomials. *Proc. Edinb. Math. Soc. (2)*, 53(2):385–392, 2010. 4, 11

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 498–527. Springer, Heidelberg, March 2015. 2

[Hof80] Jeffrey Hoffstein. On the Siegel-Tatuzawa theorem. *Acta Arithmetica*, 38:167–174, 1980. 15

[Kan18] Daniel M. Kane. Quantum money from modular forms, 2018. https://arxiv.org/abs/1809.05925. 1

[KLS22] Andrey Boris Khesin, Jonathan Z Lu, and Peter W Shor. Publicly verifiable quantum money from random lattices, 2022. https://arxiv.org/abs/2207.13135v2. 1

[KSS21] Daniel M. Kane, Shahed Sharif, and Alice Silverberg. Quantum money from quaternion algebras. Cryptology ePrint Archive, Report 2021/1294, 2021. https://eprint.iacr.org/2021/1294. 1, 33

[LAF+10] Andrew Lutomirski, Scott Aaronson, Edward Farhi, David Gosset, Jonathan A. Kelner, Avinatan Hassidim, and Peter W. Shor. Breaking and making quantum money: Toward a new quantum cryptographic protocol. In Andrew Chi-Chih Yao, editor, *ICS 2010*, pages 20–31. Tsinghua University Press, January 2010. 1

[LLQZ22] Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 294–323. Springer, Heidelberg, November 2022. 3

[LMZ23] Jiahui Liu, Hart Montgomery, and Mark Zhandry. Another round of breaking and making quantum money: How to not build it from lattices, and more. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*, pages 611–638. Springer, Heidelberg, April 2023. 1, 2, 3, 4, 5, 6, 7, 18, 20, 30, 31, 32, 33

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London-New York, 1977. 34

[MMP22] Marzio Mula, Nadir Murru, and Federico Pintore. Random sampling of supersingular elliptic curves. Cryptology ePrint Archive, Report 2022/528, 2022. https://eprint.iacr.org/2022/528. 17

[Mon94] H.L. Montgomery. *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*. Conference board of the mathematical sciences regional conference series in mathematics. Conference Board of the Mathematical Sciences, 1994. 34

[MP19a] M. Ram Murty and Neha Prabhu. The error term in the Sato-Tate theorem of Birch, 2019. https://arxiv.org/abs/1906.03534. 10, 11

[MP19b] M. Ram Murty and Neha Prabhu. The error term in the Sato–Tate theorem of Birch. *Bulletin of the Australian Mathematical Society*, 100(1):27–33, 2019. 4, 10

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. 6

[NR83] J. L. Nicolas and G. Robin. Majorations explicites pour le nombre de diviseurs de n. *Canadian Mathematical Bulletin*, 26(4):485–492, 1983. 13

[OEI24] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences, 2024. Published electronically at http://oeis.org. 14

[Rob21] Bhaskar Roberts. Security analysis of quantum lightning. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 562–567. Springer, Heidelberg, October 2021. 1

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. https://eprint.iacr.org/2006/145. 3

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7(1):219–254, 1995. 33

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 8

[Tat51] Tikao Tatuzawa. On a theorem of Siegel. *Japanese journal of mathematics: transactions and abstracts*, 21:163–178, 1951. 3, 4, 5, 14

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983. 1

[WW21] Hoeteck Wee and Daniel Wichs. Candidate obfuscation via oblivious LWE sampling. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part III*, volume 12698 of *LNCS*, pages 127–156. Springer, Heidelberg, October 2021. 2

[You91] Robert M. Young. 75.9 Euler's constant. *The Mathematical Gazette*, 75(472):187–190, 1991. 11

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 408–438. Springer, Heidelberg, May 2019. 1, 2

[Zha24] Mark Zhandry. Quantum money from abelian group actions. In *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2024. 2, 5, 6, 30, 31, 33