QUANTUM MONEY FROM QUATERNION ALGEBRAS

DANIEL M. KANE, SHAHED SHARIF, AND ALICE SILVERBERG

Abstract. We propose a new idea for public key quantum money. In the abstract sense, our bills are encoded as a joint eigenstate of a fixed system of commuting unitary operators. We perform some basic analysis of this black box system and show that it is resistant to black box attacks. In order to instantiate this protocol, one needs to find a cryptographically complicated system of computable, commuting, unitary operators. To fill this need, we propose using Brandt operators acting on the Brandt modules associated to certain quaternion algebras. We explain why we believe this instantiation is likely to be secure.

1. Introduction

One of the main challenges to building a purely digital currency is that digital information can be copied, allowing adversaries to duplicate bills or more generally perform double spending attacks. Existing cryptocurrencies solve this problem by maintaining a tamper-proof ledger of all transactions to ensure that the same bill is not spent multiple times by the same actor. Essentially, in these schemes, money is not represented by a digital token so much as a number on this decentralized ledger.

Another idea for solving the bill copying problem is to make use of the quantum no-cloning principle and taking advantage of the idea that quantum information in general *cannot* be copied. A scheme to take advantage of this was proposed by Wiesner in [27]. His scheme involved the bank preparing a quantum state that was an eigenstate in a secret basis. The bank could verify the correctness of the state, but it was information-theoretically impossible for an adversary without possession of this secret to copy the state in question. Unfortunately, this scheme has the disadvantage that one needs to contact the bank in order to verify the legitimacy of a bill.

Since then, there has been an effort to develop schemes for public key quantum money—that is, a scheme by which there is a publicly known protocol for checking the validity of a bill. In such a system, the bank has a mechanism for producing valid bills, and there is a publicly known mechanism that, with high probability, non-destructively checks the validity of a given bill. It should be computationally infeasible to produce $n+1$ valid bills, given access to n valid bills, without access to the bank's secret information. Such schemes can at best be computationally secure rather than information theoretically secure, as it is a finite computational problem to construct a quantum state that reliably passes the publicly known verification procedure. There have been several proposals over the years for cryptographically

2010 *Mathematics Subject Classification.* 81P68, 94A60 (primary), 11R52, 11Y40, 11F11 (secondary).

Key words and phrases. quantum money, quaternion algebras.

secure quantum money based on ideas such as knot theory [10] and function obfuscation [1, 28].

In this paper, we give a new proposal for public-key quantum money using quaternion algebras, which the first author was led to from ideas about the theory of modular forms. We hope that the ideas and techniques of this paper could be used for other problems in cryptography and computer science. We also expect this paper to inspire work on the associated computational algebra problems.

This paper can be viewed as an extended version of [15]. While the title of [15] refers to modular forms, the proposed scheme did not use modular forms, but only quaternion algebras and Brandt operators. The known connection between quaternion algebras and modular forms leads one to wonder whether modular forms can be used cryptanalytically, and we address that question in the security section.

In his March 27, 2020 lecture at the Simons Institute for the Theory of Computing [23], Peter Shor listed Kane's quantum money scheme in [15] as one of very few quantum money proposals that had not yet been broken.

1.1. **Our Proposed Scheme.** The verification procedure for quantum money should ideally be non-destructive.[1] A natural way to achieve this goal is to make the state an eigenstate of some (commuting collection of) unitary operators, that is, consider a scheme where there is a set of commuting unitary operators $U_1, U_2, \ldots, U_t$, and a bill is a joint eigenstate $|\psi\rangle$. One can easily verify such a state is a valid bill and measure the corresponding eigenvalues of the U_j non-destructively. One can also produce a random joint eigenstate by starting with some arbitrary state $|\rho\rangle$ and measuring with respect to the eigenbasis of the U_j. In fact one can construct pairs of eigenstates with the same eigenvalues by starting with a maximally entangled state. However, there seems to be no obvious way to produce more than these two eigenstates with the same eigenvalues. This makes this into a scheme for *quantum lightning* (see [28]), which by standard methods can be turned into a quantum money protocol. In particular, to create quantum money, one merely needs the state $|\psi\rangle\,|\psi\rangle$ along with a classical digital signature certifying the sequence of eigenvalues. We show (in Theorem 4.1 below) that this quantum money scheme is secure if the U_j are implemented as oracles.

In order to obtain a practical version of this scheme, one needs to find explicit commuting operators U_j so that the joint eigenstates are cryptographically complicated. This is a non-trivial problem, but we have a candidate collection coming from Brandt matrices acting on the Brandt modules associated to certain quaternion algebras.

The action of the p-Brandt matrices on the Brandt modules associated to our maximal order $\mathcal{O}_N$ in a suitable quaternion algebra can be viewed as a computationally efficient way to implement the action of the Hecke operators T_p on a space of modular forms, namely, the space $S_2(\Gamma_0(N))$ of weight two cusp forms of level N, where for us, N is a large prime. Modular forms are spaces of highly symmetric analytic functions on the upper half of the complex plane with a storied mathematical history, finding applications in problems as diverse as the computation of partition numbers and the proof of Fermat's Last Theorem. The vector space $S_2(\Gamma_0(N))$ has dimension $\Theta(N)$, and the operators e^{iT_p} acting on this space are a

[1]Though as Zhandry [28, Remark 3.1] observes, if the verification procedure succeeds with high probability, then it can be modified to a new verification procedure that is non-destructive with high probability.

collection of commuting, unitary operators acting on a large, complex vector space. These operators seem relatively likely to be cryptographically complicated.

1.2. **Outline.** We discuss the details of the black box version of this protocol in Section 2, the related security problem in Section 3, and a proof of black box security in Section 4. In Section 5 we give details of our instantiation using quaternion algebras. We describe some of the relevant theory of quaternion orders and ideal class sets in Section 5.1, using [26] as a reference. We introduce the Brandt matrices in Section 5.2, obtain canonical encodings of ideal classes in Section 5.3 that help to make the Brandt matrices computationally tractable, and give additional information about the Brandt operators in Section 5.4. We provide an efficient algorithm to produce a maximally entangled state in Section 5.5. We formally instantiate the protocol in Section 5.6. In Section 6 we discuss the security of the instantiation. Theorem 6.2 reduces the security of the instantiation to the hardness of Problem 6.1, while Sections 6.2 to 6.6 give possible avenues of attack and why we do not expect them to succeed.

2. The Black Box Protocol

A *quantum money protocol* consists of a set B of *bills*, an efficient *verification algorithm* Verify, and an efficient *minting algorithm* Mint. The verification algorithm takes as input public parameters PP and a candidate bill x, and outputs True if and only if $x \in B$. The minting algorithm takes as input public and private parameters and outputs a bill $x \in B$.

Suppose V is an N-dimensional complex vector space, and $U_1, \ldots, U_t$ are commuting unitary operators on V. Since the U_j's commute, there exists an eigenbasis $\{|\psi_i\rangle\}_{i=1}^N$. Let z_{ij} denote the eigenvalue of U_j associated to the eigenvector $|\psi_i\rangle$, that is, $U_j |\psi_i\rangle = z_{ij} |\psi_i\rangle$. Set $v_i = (z_{i1}, \ldots, z_{it})$, the vector of eigenvalues for $|\psi_i\rangle$.

Definition 2.1. If $\varepsilon \in \mathbb{R}^{>0}$, we say that an eigenbasis $\{|\psi_i\rangle\}_i$ is **ε-separated** if $|v_k - v_j| \geq \varepsilon$ in the L_2-norm whenever $j \neq k$.

Given an oracle that can compute controlled versions of the U_j, we present the following quantum money protocol:

The public parameters consist of:

- an efficient digital signature algorithm and a verification key VK,
- an N-dimensional complex vector space V along with a computationally feasible basis for V,
- commuting unitary operators $U_1, U_2, \ldots, U_t$ on V, and
- a positive real number ε.

Assume there is an ε-separated eigenbasis $\{|\psi_i\rangle\}_{i=1}^N$. For each i, let v_i be the vector of eigenvalues for $|\psi_i\rangle$, as above. Then a *bill* consists of a triple $(|\psi\rangle, v, \sigma)$, called respectively the *note*, *serial number*, and *signature*, given as follows:

- the note $|\psi\rangle$ is $|\psi_i\rangle \otimes |\psi_i\rangle$ for some i,
- the serial number v is classical information providing an approximation of v_i to error less than $\varepsilon/3$, and
- σ is a digital signature of v signed with the signing key SK that corresponds to the verification key VK.

The verification algorithm $\mathsf{Verify}(\mathsf{PP}, (|\psi\rangle, v, \sigma))$ is as follows:

(1) Verify the digital signature σ of v.

(2) For each $j = 1, ..., t$, use phase estimation to verify that the note $|\psi\rangle$ is an eigenstate of $U_j \otimes I_N$ and of $I_N \otimes U_j$ with eigenvalues within $\varepsilon/2$ of those given by the entries of the serial number v (where I_N is the $N \times N$ identity matrix.

The minting algorithm $\mathsf{Mint}(\mathsf{PP}, \mathsf{SK})$ is as follows:

(1) Prepare a maximally entangled state $\frac{1}{\sqrt{N}} \sum_{i=1}^{N} |\psi_i\rangle |\psi_i\rangle$ for V that is the uniform superposition over all notes.
(2) Apply phase estimation with $U_j \otimes I_N$ for each j. Set $|\psi\rangle$ to be the resulting state, and set the jth entry of the serial number v to be an approximation to the eigenvalue.
(3) Set σ to be the digital signature of v with signing key SK.

Remark 2.2. There are a few important things to note about this protocol:

(1) The separation assumption implies that, up to scalar multiple, the eigenbasis $\{|\psi_i\rangle\}$ is unique. Therefore the verification algorithm is correct.
(2) If the bill is valid, verification does not change it.
(3) If the note was not an eigenstate of all the $U_j \otimes I_N$ and $I_N \otimes U_j$ before applying the verification algorithm, it will be after the phase estimation step.
(4) Due to the assumed separation of $\{|\psi_i\rangle\}$, every pair of bills that validate for the same serial number must (after verification) have notes that are the same eigenstate.

If the serial number is required to be an appropriate unique rounding of the eigenvalues of $|\psi_i\rangle$ rather than merely an approximation, this looks very much like a protocol for *quantum lightning* in the sense of [28], that is, a mechanism that can produce and label one of a number of states but for which it is hard even for an adversarial algorithm to produce multiple copies of the same such state. We chose to use arbitrary approximations so that one does not need to worry about precision errors if the true eigenvalues are near the boundary between two different roundings. However, our proposal should still give many of the applications of quantum lightning, including quantum money and verifiable randomness.

3. The Security Problem

What might an attack against this scheme look like? For quantum lightning, an attack would require a method for producing two copies of the same bolt (in this case a pair of identical eigenstates). We argue that any attack on our quantum money protocol should be able to do this. In fact it is enough to note that having four copies of the same eigenstate, one can throw away one to get three copies. Thus, we base our security on the following problem:

Problem 3.1. Given N, $V \cong \mathbb{C}^N$, and commuting unitary operators $U_1, \ldots, U_t$ on V, output a state of the form $|\psi\rangle |\psi\rangle |\psi\rangle$, where $|\psi\rangle$ is an eigenvector of all the U_j.

The black box version of the problem is when the adversary only has black box access to the U_j.

We claim that any agent capable of attacking this system must be capable of solving Problem 3.1. In particular, we consider three kinds of attacks on the system:

(1) Attacks by the mint: This would apply for systems where the mint creates a public registry of valid serial numbers (or perhaps puts them into a hash tree, publishing only the root). In such a system, the mint itself might try to cheat by creating multiple copies of bills appearing in the registry.
(2) Attacks by others: An attacker given access to some number of valid bills and perhaps a much larger number of valid serial number signatures finds some procedure to spend more bills than they initially had access to.
(3) Attacks on random instances: An attacker, for a random public key/private key pair for the digital signature scheme and making some number of calls to a signing oracle, finds some procedure to spend more bills than they initially had access to.

Theorem 3.2 below shows that an adversary who succeeds with any of the above types of attack can then solve Problem 3.1. Note the similarity between its proof and the security proof in [1, Theorem 14].

We note some differences between (2) and (3) of Theorem 3.2. Part (2) says that if you have an algorithm that attacks the given instance, then you can produce an algorithm that either attacks that instance of the digital signature scheme, or (with additional input of chosen signatures) solves Problem 3.1. While (2) addresses attacks on a specific system, it cannot be algorithmically hard, since there *is* an algorithm that forges signatures—namely, a signing algorithm that has the private key of the instance hard-coded. In contrast, (3) attacks a random instance of the protocol (which is what we might hope would be computationally hard), and the second conclusion of (3) is an unequivocal attack on Problem 3.1.

Theorem 3.2. *(1) If an adversary using a quantum computer and given the secret key to the signing protocol can in time T run a procedure that with probability at least p produces $n+1$ valid bills with at most n total serial numbers among them, then the adversary can with constant positive probability solve Problem 3.1 in time $O(T/p)$.*

(2) If an adversary, given n bills and s uniformly random valid signatures of serial numbers, but without access to the signing key, can in time T run a procedure that with probability at least p produces $n+1$ bills that pass the verification procedure, then the adversary in time $O(T)$ with probability p can, given $n+s$ chosen signatures, either:
- *produce a new valid signature without access to the signing key, or*
- *solve Problem 3.1.*

(3) Suppose there is a quantum algorithm that for a random instantiation of the quantum money protocol (i.e., a random choice of parameters for the digital signature scheme, but without access to the signing key), given n uniformly random bills and the signatures corresponding to s other uniformly random bills, can generate $n+1$ valid bills in time T with probability p (with the probability taken over both the space of measurement outcomes and the set of public key/private key pairs for the signature scheme). Then either:
- *there is a quantum algorithm that for a random instantiation of the digital signature scheme and given $n+s$ chosen signatures can in time $O(T)$ and with probability at least $\frac{p}{2}$ produce a new valid signature without access to the signing key, or*

- *there is a quantum algorithm that in time* $O(\frac{T+c(n+s)}{p})$ *and with probability at least* $\frac{1}{2}$ *solves Problem 3.1, where* c *is the time required to run the minting algorithm once.*

Proof. The argument for (1) is easy. By the pigeonhole principle, at least two of the bills produced must have the same serial number. Given the separation between the v_i, this must mean that the notes in question are both of the form $|\psi_i\rangle |\psi_i\rangle$ for the same value of i. Using one and a half of these, the adversary (i.e., the mint) has produced a state of the form $|\psi_i\rangle |\psi_i\rangle |\psi_i\rangle$. Thus, in time T the adversary can solve Problem 3.1 with probability at least p. Repeating $O(1/p)$ times yields a constant probability of success.

For (2), the adversary can use the chosen signatures and the minting algorithm to produce $n+s$ valid bills $x_1, \ldots, x_n, y_1, \ldots, y_s$; namely, to produce a bill, the adversary can produce a maximally entangled state $\sum_{i=1}^{N} |\psi_i\rangle \otimes |\psi_i\rangle$, measure with respect to the operators $I \otimes U_j$ for $j \in \{1, \ldots, t\}$, and then sign the tuple of eigenvalues resulting from the measurements using a single call to the signing algorithm (where N and t are as in Problem 3.1). For each k, let σ_k denote the signature for bill y_k. By hypothesis, using $x_1, \ldots, x_n, \sigma_1, \ldots, \sigma_s$, the adversary with probability at least p can in time T produce $n+1$ bills that pass the verification procedure. These bills along with $y_1, \ldots, y_s$ give $n+s+1$ valid bills. Thus either the adversary has produced a valid signature that is not one of the original $n+s$ signatures of valid bills (thus producing a new signature without the private key), or at least two of the $n+s+1$ bills have the same serial number, which implies that the adversary has three copies of the same eigenstate, and the adversary has solved Problem 3.1.

For (3), the desired quantum algorithm first generates an instance of the quantum money protocol, i.e., generates a public key/private key pair for the digital signature algorithm. As in (2), using $n+s$ calls to the signature algorithm, the algorithm with probability at least p either produces a new signature without using the private key, or solves Problem 3.1. If the former holds with probability at least $\frac{p}{2}$, then the first conclusion holds. Now suppose that is not the case. Then the algorithm solves Problem 3.1 with probability at least $p/2$. A solution to Problem 3.1 is independent of the signature keys. Repeat $O(1/p)$ times with $O(1/p)$ random instances of the signature key pair to obtain the second conclusion. □

3.1. **A $\sqrt{N}$ Attack.** There is an obvious $O(\sqrt{N})$ time attack on Problem 3.1:

- Produce $\sqrt{N}$ notes using the minting procedure.
- Search for pairs of notes with serial numbers sufficiently close to each other.

Each note is $|\psi_i\rangle |\psi_i\rangle$ for a uniform random value of i. By the birthday paradox, we expect to find a collision within the first $O(\sqrt{N})$ notes.

4. Black Box Security

One might worry about black box attacks against the proposed system, that is, attacks on Problem 3.1 that do not make use of any special structure of V or the U_j and only have black box access to the operators U_j. In this section we show that any such attack must have query complexity at least $\Omega((N/\log(N))^{1/3})$.

If $\mathcal{D}$ is a probability distribution over $(S^1)^t$, then for each N, we obtain an induced probability distribution over tuples of commuting $N \times N$ unitary operators $(U_1, \ldots, U_t)$ by letting $\{|\psi_i\rangle\}$ be a random orthonormal basis of $\mathbb{C}^N$ (under the

Haar measure), letting $v_i = (z_{i1}, \ldots, z_{it})$ be i.i.d. samples from $\mathcal{D}$ for $i = 1, \ldots, N$, and defining U_j by the equations $U_j |\psi_i\rangle = z_{ij} |\psi_i\rangle$.

Theorem 4.1. *Suppose $\mathcal{D}$ is any probability distribution over $(S^1)^t$ such that with high probability, any finite number of samples chosen from $\mathcal{D}$ are distinct. Then any circuit consisting of standard gates and controlled U_j gates that solves Problem 3.1 with constant positive probability for sets of operators $U_1, \ldots, U_t$ chosen according to $\mathcal{D}$ and with uniformly random eigenbasis $\{|\psi_i\rangle\}$ must have $\Omega((N/\log(N))^{1/3})$ controlled U_j gates.*

The hypothesis on $\mathcal{D}$ in Theorem 4.1 holds, for instance, if $\mathcal{D}$ is the uniform distribution over $(S^1)^t$. Additionally, for each small positive ε, if $t \gg \log(N)$, then the eigenvectors are ε-separated with high probability. This shows that Theorem 4.1 holds even when the eigenvectors are ε-separated (which implementations of our quantum money protocol require).

The proof of Theorem 4.1 will proceed in three steps:

(1) Replace Problem 3.1 with a refinement, Problem 4.2, that is equivalent when the eigenspaces are one-dimensional.
(2) Show that with degenerate eigenspaces (i.e., eigenspaces of dimension greater than one), Problem 4.2 is impossible to solve with constant positive probability even with an unbounded number of queries (with probability of success depending on how degenerate the eigenspaces are).
(3) Then define a family of input distributions parameterized by an integer M so that when M is large we have ε-separation with high probability and when M is small we do not. We use the bounds from (2) to show that the probability of success with small M is bounded and then use the polynomial method to show that unless we make a large number of queries, this implies that the probability of success is small even in the range where we do have ε-separation.

4.1. **Preliminary lemmas.** Consider the following refinement of Problem 3.1:

Problem 4.2. Given N, $V \cong \mathbb{C}^N$, and commuting unitary operators $U_1, \ldots, U_t$ on V, output a state of the form $|\psi_i\rangle |\psi_i\rangle |\psi_i\rangle$ for some $1 \leq i \leq N$, where $\{|\psi_i\rangle\}$ is a fixed secret eigenbasis of V for the operators U_j.

When the eigenbasis is ε-separated, then Problems 4.2 and 3.1 are equivalent. But if the eigenspaces are degenerate, then Problem 4.2 is impossible to solve. To see this, suppose that a circuit attempting to solve Problem 4.2 outputs a state $|\phi\rangle$, and think of the choice of basis $\{|\psi_i\rangle\}$ as a random variable. Then it suffices to show that the probability that $|\phi\rangle$ has a large component in any $|\psi_i\rangle |\psi_i\rangle |\psi_i\rangle$ direction is small. We first consider the case of a single, totally degenerate eigenspace; we will consider the general case in Claim 2 of the proof of Theorem 4.1.

Lemma 4.3. *If W is a complex vector space and $|\phi\rangle \in W \otimes W \otimes W$, then*

$$\mathop{\mathbf{E}}_{\{|\psi_i\rangle\} \text{ orthonormal basis of } W} \left[\sum_i |\langle\psi_i| \langle\psi_i| \langle\psi_i| |\phi\rangle|^2 \right] \leq \frac{3}{\dim(W)}.$$

Proof. Let $m = \dim(W)$. It suffices to show that

$$\mathop{\mathbf{E}}_{||\psi\rangle|_2=1} \left[|\langle\psi| \langle\psi| \langle\psi| |\phi\rangle|^2 \right] \leq \frac{3}{m^2}.$$

Rewrite $|\psi\rangle$ as $\frac{1}{\sqrt{m}}\sum_{i=1}^{m} x_i |\psi_i\rangle$ where $\{|\psi_i\rangle\}$ is a random orthonormal basis for W and x_i are i.i.d. ± 1 random variables. We claim that even after fixing the $|\psi_i\rangle$, the expectation over x_i is at most $3/m^2$. In particular let

$$|\phi\rangle = \sum_{1\le i,j,k\le m} a_{ijk} |\psi_i\rangle |\psi_j\rangle |\psi_k\rangle$$

where $\sum_{1\le i,j,k\le m} |a_{ijk}|^2 = 1$. Then the expectation over x_i is

$$\frac{1}{m^3} \mathop{\mathbf{E}}_{x_i}[|\sum_{1\le i,j,k\le m} a_{ijk} x_i x_j x_k|^2].$$

Collecting like terms this is

$$\frac{1}{m^3} \mathop{\mathbf{E}}_{x_i}[|\sum_{1\le i<j<k\le m} (a_{ijk}+a_{ikj}+a_{jik}+a_{jki}+a_{kij}+a_{kji}) x_i x_j x_k + \sum_{i=1}^{m} x_i (a_{iii} + \sum_{j=1, j\ne i}^{m} (a_{ijj}+a_{jij}+a_{jji}))|^2].$$

By orthogonality of the variables $x_i x_j x_k$ and x_i, this is

$$\frac{1}{m^3} \mathop{\mathbf{E}}_{x_i}[\sum_{1\le i<j<k\le m} |a_{ijk}+a_{ikj}+a_{jik}+a_{jki}+a_{kij}+a_{kji}|^2 + \sum_{i=1}^{m} |a_{iii} + \sum_{j=1, j\ne i}^{m} (a_{ijj}+a_{jij}+a_{jji})|^2]. \tag{4.1}$$

For each i, there are $3m-2$ terms in the sum $a_{iii} + \sum_{j=1,j\ne i}^{m}(a_{ijj}+a_{jij}+a_{jji})$. Thus by Cauchy-Schwartz, (4.1) is at most

$$\frac{1}{m^3}\left(\sum_{\substack{1\le i,j,k\le m\\ i\ne j\ne k}} 6|a_{ijk}|^2 + (3m-2)\sum_{i=1}^{m}\left(|a_{iii}|^2 + \sum_{j=1,j\ne i}^{m}(|a_{ijj}|^2+|a_{jij}|^2+|a_{jji}|^2)\right)\right).$$

Collecting terms, this is at most

$$\frac{1}{m^3}\sum_{i,j,k=1}^{m}(3m-2)|a_{ijk}|^2 \le \frac{3}{m^2},$$

as desired. □

Our proof of Theorem 4.1 in §4.2 will also make use of the following two lemmas.

Lemma 4.4. *Suppose $N, M \in \mathbb{Z}^{>0}$, and $M \le \frac{N}{16\log N}$. With the probability taken over the space of all functions $h : [N] \to [M]$, we have*

$$\Pr\left(\#(h^{-1}(j)) > \frac{N}{2M} \text{ for all } j\right) \ge 1 - \frac{1}{16N\log N}.$$

Proof. Fix $j \in [M]$. For $i \in [N]$, define a random variable X_i by

$$X_i = \begin{cases} 1 & h(i) = j, \\ 0 & h(i) \ne j. \end{cases}$$

The probability that $X_i = 1$ is $\frac{1}{M}$, and the X_i are independent. Let $X = \sum_{i=1}^{N} X_i$. Observe that $\mathop{\mathbf{E}}_{h}[X] = \frac{N}{M}$. By the Chernoff bounds,

$$\Pr\left(X \leq \frac{N}{2M}\right) \leq e^{-\frac{N}{8M}} \leq \frac{1}{N^2},$$

where the last inequality holds since $M \leq \frac{N}{16 \log N}$. By the union bound, we have

$$\Pr\left(\#(h^{-1}(j)) \leq \frac{N}{2M} \text{ for some } j\right) \leq \sum_{j=1}^{M} \Pr\left(X \leq \frac{N}{2M}\right) \leq \frac{M}{N^2} \leq \frac{1}{16N \log N}.$$

The claim now follows. □

Lemma 4.5. *If $i \in \mathbb{Z}^{\geq 1}$, then* $\left| \prod_{\substack{j \geq 1 \\ j \neq i}} \frac{(2j-1)^2}{(2j-1)^2 - (2i-1)^2} \right| = O\left(\frac{1}{i}\right).$

Proof. Let $f(z) := \prod_{j=1}^{\infty} \left(1 - \frac{z}{(2j-1)^2}\right) = \cos(\frac{\pi\sqrt{z}}{2})$. Then

$$\left| \prod_{\substack{j \geq 1 \\ j \neq i}} \frac{(2j-1)^2}{(2j-1)^2 - (2i-1)^2} \right| = \left| \frac{1}{(2i-1)^2 f'((2i-1)^2)} \right|$$

$$= O\left(\frac{1}{|(2i-1)\sin\left(\frac{(2i-1)\pi}{2}\right)|} \right) = O\left(\frac{1}{i}\right).$$

□

4.2. **Proof of Theorem 4.1.** Next, we use the polynomial method. Let C be any circuit consisting of standard gates and at most d controlled U_j gates. We show that under the correct distributions over U_j, any circuit with d too small will be unable to distinguish the cases where the eigenspaces of U_j are degenerate, and those where it is not.

Let $v_1, \ldots, v_N$ be i.i.d. samples from $\mathcal{D}$, let $\{|\psi_i\rangle\}$ be a random orthonormal basis, and let $(U_1, \ldots, U_t)$ be the operators determined by these choices. Since, by hypothesis, N samples chosen from $\mathcal{D}$ are with high probability distinct, every solution of Problem 3.1 is also a solution of Problem 4.2, and so the probability that circuit C solves Problem 3.1 is

$$\mathop{\mathbf{E}}_{|\psi_i\rangle, v_i} \left[\sum_i |\langle\psi_i| \langle\psi_i| \langle\psi_i| C(U_1, \ldots, U_t) |0\rangle|^2 \right],$$

where the expectation is over all choices of orthonormal basis $\{|\psi_i\rangle\}$ and tuples of eigenvalues $v_1, \ldots, v_N$. By the polynomial method [2, Lemma 4.2], this expectation is of the form $\mathop{\mathbf{E}}_{v_i}[p(z_{ij}, \overline{z_{ij}})]$, where p is some polynomial of degree at most $2d$ and $v_i = (z_{i1}, \ldots, z_{it})$.

For integers M, we define a slightly different probability distribution over the v_i. We let $h : [N] \to [M]$ be a function chosen uniformly at random, and let $v_i = u_{h(i)}$

where the u_j are i.i.d. elements of $\mathcal{D}$. We let

$$A_M = \mathop{\mathbf{E}}_{h,v_i}[p(z_{ij}, \overline{z_{ij}})]$$

where the h vary uniformly among functions $[N] \to [M]$ and the v_i are distributed as above, with $v_i = u_{h(i)}$ and the u_j distributed according to $\mathcal{D}$.

There are several things worth noting about this distribution. First, it is easy to see that our original probability of success is $\lim_{M\to\infty} A_M$. This is because for large M, with high probability h has no collisions and therefore the distribution over the v_i is arbitrarily close in total variational distance to i.i.d. copies of $\mathcal{D}$. Second, we have the following:

Claim 1. *For each N, there exists a polynomial $q_N(x)$ of degree at most $2d$ such that $A_M = q_N(1/M)$.*

Proof. Since $p(z_{ij}, \overline{z_{ij}})$ is a polynomial of degree at most $2d$, to prove the claim it suffices to show that if m is a monic monomial of degree e, then $\mathop{\mathbf{E}}_{h,u_i}[m(z_{ij}, \overline{z_{ij}})]$ is a polynomial in $1/M$ of degree at most e. Write $m(z_{ij}, \overline{z_{ij}}) = m_1(z_{ij})m_2(\overline{z_{ij}})$ with m_1 and m_2 monic. Observe that

$$\mathop{\mathbf{E}}_{v_i}[m(z_{ij}, \overline{z_{ij}})] = \begin{cases} 1 & \text{if } m_1 = m_2 \\ 0 & \text{if } m_1 \neq m_2. \end{cases}$$

Write u_{ij} for the jth component of u_i. Given h, define a ring homomorphism $H : \mathbb{C}[\{z_{ij}\}] \to \mathbb{C}[\{u_{ij}\}]$ by $H(z_{ij}) = u_{h(i)j}$. Then $\mathop{\mathbf{E}}_{h,u_i}[m(z_{ij}, \overline{z_{ij}})]$ equals the probability over the set of h's that $H \circ m_1 = H \circ m_2$. If $m_1 = m_2$, then this probability is 1. Now suppose that $m_1 \neq m_2$. For $k = 1$ and 2, let

$$B_k = \{z_{ij} \mid z_{ij} \text{ appears in } m_k \text{ with positive exponent}\}.$$

Since $z_{ij}\overline{z_{ij}} = 1$ whenever $z_{ij} \in S^1$, by cancelling such terms in m we may assume that $B_1 \cap B_2 = \emptyset$. Without loss of generality, $|B_1| \geq |B_2|$. If t is a surjective map $B_1 \twoheadrightarrow B_2$, say that h has *collision type* t if $H(z) = H(t(z))$ for all $z \in B_1$. There is a finite set T of collision types with the property that h has collision type in T if and only if $H \circ m_1 = H \circ m_2$. The number of h having collision type in the set T is given by an inclusion-exclusion formula. Each term in the inclusion-exclusion is given by the number of h having collision type t for all t in some subset $T' \subseteq T$. For a given collision type $t \in T$, the probability that h has type t is $\frac{1}{M^{|B_1|}}$. The probability that h has type t for every $t \in T'$ is of the form K/M^f for some constant K and some integer f. The maximum value of f occurs for the sets T' such that h has type t for all $t \in T'$ if and only if $H|_{B_1 \cup B_2}$ is a constant, in which case $f = |B_1| + |B_2| - 1$. Since $|B_1| + |B_2| \leq e$, Claim 1 follows. □

We next show:

Claim 2. *If $M \leq \frac{N}{16 \log N}$, then $q_N(1/M) = O(M/N)$.*

Proof. By the above discussion and Claim 1 we have:

$$q_N(1/M) = \mathop{\mathbf{E}}_{h,|\psi_i\rangle,v_i}\left[\sum_i |\langle\psi_i|\langle\psi_i|\langle\psi_i| C(U_1, \ldots, U_t) |0\rangle|^2\right], \tag{4.2}$$

where the h vary uniformly over functions from $[N]$ to $[M]$, the v_i are distributed according to h and $\mathcal{D}$ as above, and the sets $\{|\psi_i\rangle\}$ vary over random orthonormal

bases for V. Suppose $M \leq \frac{N}{16 \log N}$, and let h be a random function from $[N]$ to $[M]$. By Lemma 4.4, with probability at least $1 - \frac{1}{16N \log N}$, for every $j \in [M]$ we have $\#(h^{-1}(j)) = \Omega(N/M)$. Let $V_j = \operatorname{span}\{|\psi_i\rangle : h(i) = j\}$, so that with probability at least $1 - \frac{1}{16N \log N}$ we have $\dim V_j = \Omega(N/M)$. Fix both the values of the u_j and the spaces V_j. The V_j are eigenspaces for U_k with eigenvalues u_{jk}. The output of C depends only on the V_j and the u_j, but not on *which* basis of V_j is given by $\{|\psi_i\rangle : h(i) = j\}$. Thus the output is $\sum_j a_j |\phi_j\rangle$ for some $|\phi_j\rangle \in V_j^{\otimes 3}$ and $\sum_j |a_j|^2 = 1$. Therefore the right-hand side of (4.2) is

$$\mathop{\mathbf{E}}_{V_j, u_j} \sum_j |a_j|^2 \left[\mathop{\mathbf{E}}_{|\psi_i\rangle \text{ given } V_j} \left[\sum_{i : |\psi_i\rangle \in V_j} |\langle \psi_i| \langle \psi_i| \langle \psi_i| |\phi_j\rangle|^2 \right] \right].$$

Here, we vary over orthogonal decompositions $V = \oplus_{j=1}^M V_j$, tuples of eigenvalues u_j, and orthonormal bases $\{|\psi_i\rangle\}$ that are a union of orthonormal bases for the V_j. Note that h can be recovered from this data by defining $h(i) = j$ if and only if $|\psi_i\rangle \in V_j$. Thus varying over tuples $(\{|\psi_i\rangle\}, h, u_j)$ is the same as varying over tuples $(\{V_j\}, \{|\psi_i\rangle\}$ given $V_j, u_j)$, with an appropriate choice of distribution on the latter tuples. By Lemma 4.3, with probability at least $1 - \frac{1}{16N \log N}$ we have:

$$\begin{aligned} \sum_j |a_j|^2 \mathop{\mathbf{E}}_{|\psi_i\rangle \text{ given } V_j} \left[\sum_{i : |\psi_i\rangle \in V_j} |\langle \psi_i| \langle \psi_i| \langle \psi_i| |\phi_j\rangle|^2 \right] &= \sum_j |a_j|^2 O(1/\dim(V_j)) \\ &= O(M/N). \end{aligned}$$

By (4.2) we have $q_N(1/M) = O(M/N)$, as desired. □

We now proceed to prove Theorem 4.1 by contradiction. Suppose that for every $k > 0$ there is a circuit for which $d^3 < k \frac{N}{\log(N)}$. To prove Theorem 4.1, it suffices to show that for sufficiently large N the success probability of such a circuit is $O(k)$, where the implied constant is independent of N. By Claim 1, for each N the success probability is $\lim_{M \to \infty} A_M = q_N(0)$, so it suffices to show that $q_N(0) = O(k)$.

We may assume that $k < \frac{1}{16}$. For $i \in \{1, \ldots, 2d+1\}$, let

$$m_i = \frac{d^3}{(2i-1)^2} \text{ and } M_i = \lfloor m_i \rfloor \in \mathbb{Z}.$$

Then $M_i \leq d^3 < \frac{N}{16 \log N}$, so by Claim 2 we have $q_N(1/M_i) = O(M_i/N)$ for each i.

Using standard polynomial interpolation, we have:

$$q_N(0) = \sum_{i=1}^{2d+1} q_N(1/M_i) \prod_{j \neq i} \frac{1/M_j}{1/M_j - 1/M_i}.$$

We begin by bounding these expressions if the M_j were replaced by m_j:

$$\begin{aligned} \left| \prod_{j \neq i, j \leq 2d+1} \frac{1/m_j}{1/m_j - 1/m_i} \right| &= \left| \prod_{j \neq i, j \leq 2d+1} \frac{(2j-1)^2/d^3}{(2j-1)^2/d^3 - (2i-1)^2/d^3} \right| \\ &= \left| \prod_{j \neq i, j \leq 2d+1} \frac{(2j-1)^2}{(2j-1)^2 - (2i-1)^2} \right| \leq \left| \prod_{j \neq i} \frac{(2j-1)^2}{(2j-1)^2 - (2i-1)^2} \right|, \end{aligned}$$

where the final product is over all positive integers j. By Lemma 4.5, the latter product is $O(1/i)$. Since $M_i = \lfloor m_i \rfloor$, we have $1/M_i = 1/m_i + O(1/m_i^2)$. Thus,

$$\begin{aligned}
\left| \prod_{j \neq i} \frac{1/M_j}{1/M_j - 1/M_i} \right| &= \left| \prod_{j \neq i} \frac{1/m_j + O(1/m_j^2)}{1/m_j - 1/m_i + O(1/m_i^2 + 1/m_j^2)} \right| \\
&\leq \left| \prod_{j \neq i} \frac{1/m_j}{1/m_j - 1/m_i} \right| \prod_{j \neq i} \left(1 + \frac{O(1/m_i^2 + 1/m_j^2)}{|1/m_i - 1/m_j|} \right) \\
&= O(1/i) \exp\left(\sum_{j \neq i} O\left(\frac{i^4 + j^4}{(i^2 - j^2) d^3} \right) \right) \\
&\leq O(1/i) \exp\left(\sum_{j \neq i} O\left(\frac{\max(i,j)^4}{(\max(i,j)|i-j| d^3} \right) \right) \\
&\leq O(1/i) \exp\left(\sum_{j \neq i} O\left(\frac{\max(i,j)^3}{|i-j| d^3} \right) \right).
\end{aligned}$$

Now if $i \leq \sqrt{d}$, the terms with $j \leq 2i$ sum to at most $O(1/d)$, and the larger terms in the sum are $O\left(\frac{j^2}{d^3}\right)$, and therefore sum to $O(1)$. If $i \geq \sqrt{d}$, then the terms are $O\left(\frac{1}{|i-j|}\right)$, and thus sum to $O(\log(d))$. This implies that

$$\begin{aligned}
q_N(0) &= \sum_{i=1}^{2d+1} q_N(1/M_i) \prod_{j \neq i} \frac{1/M_j}{1/M_j - 1/M_i} \\
&= \sum_{i=1}^{\sqrt{d}} q_N(1/M_i) O(1/i) + \sum_{i=\sqrt{d}}^{2d+1} q_N(1/M_i) O(\log(d)/i) \\
&= \sum_{i=1}^{\sqrt{d}} O\left(\frac{M_i}{Ni} \right) + \sum_{i=\sqrt{d}}^{2d+1} O\left(\frac{\log(d) M_i}{Ni} \right) \\
&= \sum_{i=1}^{\sqrt{d}} O\left(\frac{d^3}{Ni^3} \right) + \sum_{i=\sqrt{d}}^{2d+1} O\left(\frac{d^3 \log(d)}{Ni^3} \right) \\
&= O(d^3 \log(d)/N).
\end{aligned}$$

Since $d^3 < \frac{kN}{\log(N)}$ and $k < 1/16$, it follows that for $N \geq 2$ we have $\frac{d^3 \log(d)}{N} < \frac{k \log(d)}{\log(N)} < k$, as desired.

Remark 4.6. The bound in Theorem 4.1 is nearly tight. In particular, if we assume ε-separation of the v_i's for the operators $U_1, \ldots, U_t$, then there is actually an algorithm for solving Problem 3.1 with constant probability in $O(N^{1/3} t/\varepsilon)$ queries, similar to the collision algorithm of [4]. The algorithm involves computing $N^{1/3}$ pairs $|\psi_i\rangle |\psi_i\rangle$, then preparing $N^{2/3}$ other maximally entangled states. These maximally entangled states can be thought of as being in a superposition of all combinations of $N^{2/3}$ pairs tensored together. There is a reasonable probability

that one of these $N^{2/3}$ pairs agrees with one of our $N^{1/3}$ pairs, and we can find the index of such a pair using Grover's algorithm by measuring the eigenvalues of only $O(N^{1/3})$ of our pairs. In order to compute the eigenvalues to sufficient accuracy takes only $O(t/\varepsilon)$ queries each. Thus, this algorithm has query complexity $O(N^{1/3})$, although the full complexity is $O(N^{2/3})$.

5. Instantiation using Quaternion Algebras

Above, we discussed a quantum money protocol that depends on having access to a number of black box, commuting operators. However, for our protocol to be cryptographically secure, we will need to implement it using operators that are cryptographically difficult to work with. This is a bit of an issue as most easily computable sets of commuting operators will not be secure in this way. For example, taking U_j to be the Pauli matrix on the jth qubit Z_j gives an easy set of commuting operators, but one for which it is easy to manufacture eigenstates (even with specified eigenvalues). We come up with a hopefully secure set of commuting operators using the theory of quaternion algebras.

5.1. **Quaternion Algebras.** Before we discuss our implementation in detail, we review some basic facts about orders in quaternion algebras, for which [26] can be used as a reference.

Given $a, b \in \mathbb{Q}$, define $H(a,b) = \mathbb{Q}+\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}ij$ to be the $\mathbb{Q}$-algebra with basis $\{1, i, j, ij\}$ and relations $i^2 = a$, $j^2 = b$, and $ji = -ij$. Then $H(a,b)$ has dimension four as a $\mathbb{Q}$-vector space, and $H(a,b)$ is a quaternion algebra over $\mathbb{Q}$. For example, $H(-1,-1)$ is the $\mathbb{Q}$-algebra of Hamilton quaternions.

For $z = x_0 + x_1 i + x_2 j + x_3 ij \in H(a,b)$ (with $x_i \in \mathbb{Q}$), its conjugate is $\bar{z} := x_0 - x_1 i - x_2 j - x_3 ij$ and its reduced norm is $\mathrm{nrd}(z) := z\bar{z}$.

A quaternion algebra H over $\mathbb{Q}$ is *ramified* at a prime N (respectively, at ∞) if the completion $H \otimes_{\mathbb{Q}} \mathbb{Q}_N$ (respectively, $H \otimes_{\mathbb{Q}} \mathbb{R}$) is a division algebra (equivalently, is not the matrix algebra $M_2(\mathbb{Q}_N)$, respectively $M_2(\mathbb{R})$). An *order* $\mathcal{O}$ in H is by definition a subring that is also a lattice (i.e., a finitely-generated $\mathbb{Z}$-submodule such that $\mathcal{O}\mathbb{Q} = H$).

From now on, suppose N is a prime number and $N \geq 5$. Let H_N be the unique quaternion algebra over $\mathbb{Q}$ ramified at N and ∞; see Proposition 5.1 of Pizer [21] for a and b such that $H_N = H(a,b)$. If $N \equiv 1 \pmod 6$ let $\mathcal{O}_N$ be the maximal order given explicitly in Proposition 5.2 of Pizer [21], and if $N \equiv 5 \pmod 6$ let $H_N = H(-3,-N)$ and $\mathcal{O}_N = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{j+ij}{2} + \mathbb{Z}\frac{i-ij}{3}$. (In particular, if $N \equiv 7 \pmod{12}$ then $H_N = H(-1,-N)$ and $\mathcal{O}_N = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{1+ij}{2}$.) Then $\mathcal{O}_N$ is an N-extremal maximal order in H_N, that is, a maximal order for which the unique ideal of reduced norm N is principal (see [26, Chapter 21]).

A (left) fractional ideal of $\mathcal{O}_N$ is by definition a (full-rank) lattice in H_N that is closed under left multiplication by elements of $\mathcal{O}_N$. Define the ideal class set $\mathrm{Cls}(\mathcal{O}_N)$ to be the set of fractional ideals of $\mathcal{O}_N$ modulo right multiplication, i.e., modulo the equivalence relation defined by $I \sim J$ if and only if there exists $z \in H_N$ such that $I = Jz$. The ideal class set $\mathrm{Cls}(\mathcal{O}_N)$ is finite (see [26, Chapter 21]). If I is a fractional ideal of $\mathcal{O}_N$, let $[I]$ denote its ideal class, i.e., the set of fractional ideals J of $\mathcal{O}_N$ such that $I = Jz$ for some $z \in H_N$.

If I is a left fractional $\mathcal{O}_N$-ideal, then the reduced norm $\mathrm{nrd}(I)$ is defined in [26, §16.3], and satisfies $I\bar{I} = \mathrm{nrd}(I)\mathcal{O}_N$. If $I \subset \mathcal{O}_N$ then $\mathrm{nrd}(I)^2 = [\mathcal{O}_N : I]$ (see [26, §16.4.8]).

The quaternion algebra $H(a, b)$ embeds in $\mathbb{R}^4$ via the homomorphism of abelian groups

$$x_0 + x_1 i + x_2 j + x_3 ij \mapsto (x_0, x_1\sqrt{|a|}, x_2\sqrt{|b|}, x_3\sqrt{|ab|}).$$

Identifying $H(a, b)$ with its image, for all $z \in H(a, b)$ we have $\mathrm{nrd}(z) = \|z\|^2$, where $\|\cdot\|$ denotes the Euclidean norm on $\mathbb{R}^4$. The image of $\mathcal{O}_N$ and of any left fractional ideal of $\mathcal{O}_N$ is a lattice in $\mathbb{R}^4$. We thus may represent a fractional ideal by a Minkowski reduced basis. Since every fractional ideal is a rank four lattice, given a $\mathbb{Z}$-basis, a Minkowski reduced basis can be computed in polynomial time [20]. In algorithms, we specify a fractional ideal for $\mathcal{O}_N$ by a Minkowski reduced basis for it.

5.2. **Normalized Brandt operators $T(p)$.**

Definition 5.1. If I is a left fractional $\mathcal{O}_N$-ideal, define its right order $\mathcal{O}_I := \{z \in H_N \mid Iz \subset I\}$ and its weight $w_I := \#(\mathcal{O}_I^\times/\{\pm 1\}) = \frac{1}{2}\#\mathcal{O}_I$.

Then $\mathcal{O}_I$ is a maximal order, and w_I depends only on the ideal class $[I]$. In Proposition A.7 in Appendix A we completely describe the w_I. Our choices for the maximal orders $\mathcal{O}_N$ were designed to give Proposition A.7 a clean statement.

Suppose p is a prime not equal to N, and suppose I and J are non-zero fractional ideals of $\mathcal{O}_N$. Define $a_p([I], [J])$ to be the number of fractional ideals $I' \subset J$ such that $I' \sim I$ and $J/I' \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Let $h = \#\mathrm{Cls}(\mathcal{O}_N)$ and let $T'(p)$ be the $h \times h$ matrix with $[I], [J]$-entry $a_p([I], [J])$. The matrix $T'(p)$ is the p-Brandt matrix for level N. The action of $T'(p)$ is self-adjoint for the pairing on $\mathbb{C}^{\mathrm{Cls}(\mathcal{O}_N)}$ given by

$$\left\langle (x_{[I]})_{[I]}, (y_{[I]})_{[I]} \right\rangle = \sum_{[I]} \frac{1}{w_I} x_{[I]} \overline{y_{[I]}}$$

(see [26, §41.1.9]). Let W be the diagonal $h \times h$ matrix whose $[I], [I]$-entry is $\sqrt{w_I}$, and let $T(p) = WT'(p)W^{-1}$. We call $T(p)$ the **normalized p-Brandt matrix** for level N. For example, if $N \equiv 1 \pmod{12}$, then $T(p) = T'(p)$. Let V_N be the subset of $\mathbb{C}^{\mathrm{Cls}(\mathcal{O}_N)}$ orthogonal (under the usual inner product) to the vector $(\sqrt{w_I})_{[I]}$. Then $T(p)$ acts on $\mathbb{C}^{\mathrm{Cls}(\mathcal{O}_N)}$, preserves V_N, and acts as a self-adjoint operator for the usual inner product. In our protocol, we will use the associated unitary operator $e^{iT(p)/\sqrt{p}}$.

In order to use the operators $T(p)$ in our quantum money scheme, we will need to find a way to make these operators computationally tractable. First, we will need to find a better way of representing our ideal classes. While it is easy to give a single fractional ideal in the class, it is important for us to find a canonical representation.

5.3. **Canonical encoding.** We next show how to obtain a canonical representation of an ideal class.

Algorithm 5.2.

INPUT: A prime number $N \geq 5$, an N-extremal maximal order $\mathcal{O}_N$ in H_N, and a left fractional $\mathcal{O}_N$-ideal I.

OUTPUT: A triple of integers (d, a, b) such that $\gcd(d, a, b) = 1$ and $b > a \geq 0$ and $d \geq 1$.

(1) *Apply a shortest vector algorithm such as Algorithm 2.7.5 of* [6] *to the lattice* I *to produce an element* $z \in I$ *of minimal non-zero reduced norm.*
(2) *Compute the ideal* $J_z := \frac{1}{\mathrm{nrd}(I)} I\bar{z}$.
(3) *Repeat steps (1) and (2) for each of the (at most six)* $z \in I$ *of minimal non-zero norm. Let* J *be the ideal* J_z *with lexicographically first encoding, and compute* $m := \mathrm{nrd}(J)$.
(4) *Compute the image* $\mathcal{I} \subset M_2(\mathbb{Z}/m\mathbb{Z})$ *of* $J/m\mathcal{O}_N$ *under the isomorphism* $f_{N,m} : \mathcal{O}_N/m\mathcal{O}_N \xrightarrow{\sim} M_2(\mathbb{Z}/m\mathbb{Z})$ *from the algorithm of Proposition A.4.*
(5) *Letting* $H \subset (\mathbb{Z}/m\mathbb{Z})^2$ *be the (cyclic) subgroup (of order* m*) generated by the rows of all the elements of* $\mathcal{I}$*, apply the algorithm of Proposition A.3 to obtain* $(d, c) \in \mathbb{Z}^2$ *that generates* H *and satisfies* $d \mid m$ *and* $\gcd(d, c) = 1$.
(6) *Compute* $b = m/d$ *and* $a = c \pmod{b}$. *Output* (d, a, b).

We call the triple (d, a, b) obtained in this way the *canonical encoding* of the ideal class of I. Theorem 5.3 below justifies the terminology and shows that the algorithm works.

Theorem 5.3. *In Algorithm 5.2, we have:*

(i) $m\mathcal{O}_N \subset J \subset \mathcal{O}_N$;
(ii) $N \nmid m$;
(iii) H *is a cyclic group of order* m;
(iv) $\gcd(d, a, b) = 1$;
(v) *if inputs* I *and* I' *are in the same ideal class in* $\mathrm{Cls}(\mathcal{O}_N)$*, then they output the same triple* (d, a, b)*, and produce the same* J*,* $\mathcal{I}$*, and* H;
(vi) *if the same triple is output by inputs* I *and* I'*, then* $[I] = [I']$*, and* I *and* I' *produce the same* J*,* $\mathcal{I}$*, and* H;
(vii) *Algorithm 5.2 is a quantum polynomial-time algorithm.*

Proof. If $\gamma \in H_N$ and I_0 is a left fractional $\mathcal{O}_N$-ideal, then

$$I_0\gamma \subset \mathcal{O}_N \text{ if and only if } \gamma \in I_0^{-1} = \overline{I_0}\mathrm{nrd}(I_0)^{-1}. \tag{5.1}$$

Since $\bar{z}/\mathrm{nrd}(I) \in \bar{I}\mathrm{nrd}(I)^{-1} = I^{-1}$, it follows that $J_z = I\bar{z}/\mathrm{nrd}(I) \subset \mathcal{O}_N$, so $J \subset \mathcal{O}_N$. Then $1 \in J^{-1} = \bar{J}m^{-1}$ by (5.1), so $m \in J$, so $m\mathcal{O}_N \subset J$, giving (i).

We claim that m is the minimum of the reduced norms of the integral ideals in $[I]$. Say $I' = I\gamma$. By (5.1), we have that $I\gamma \subset \mathcal{O}_N$ if and only if $\gamma = \bar{\alpha}/\mathrm{nrd}(I)$ with $\alpha \in I$. The reduced norm $\mathrm{nrd}(I\gamma) = \frac{\mathrm{nrd}(\alpha)}{\mathrm{nrd}(I)}$ is minimized when α is an element of I of minimal non-zero reduced norm. The minimality of m follows.

Since $\mathcal{O}_N$ is N-extremal, the Frobenius ideal of $\mathcal{O}_N$ is principal; let π be a generator. As in [26, 42.2.4], we have $J = \pi^r J'$ for some $r \in \mathbb{Z}^{\geq 0}$ and some ideal $J' \subset \mathcal{O}_N$ satisfying $N \nmid \mathrm{nrd}(J')$. Then $m = \mathrm{nrd}(J) = N^r\mathrm{nrd}(J')$ and $J' \in [J] = [I]$. By the minimality of m we have $N \nmid m$, giving (ii).

If r is a divisor of m, and $r \neq 1, m$, then $r\mathcal{O}_N \not\subset J$ and $J \not\subset r\mathcal{O}_N$. To see this, first suppose $J \subset r\mathcal{O}_N$. Then $r^{-1}J$ is an integral ideal in the ideal class of J, of strictly smaller norm, contradicting the minimality of m. If $r\mathcal{O}_N \subset J$, then $r \in J$, so by (5.1) with J in place of I, the ideal $J\bar{r}/m = Jr/m$ is integral. It is then an integral ideal of strictly smaller norm in the ideal class of J, contradicting the minimality of m. The map that sends a matrix to its rowspace induces a bijection from the set of left ideals of $M_2(\mathbb{Z}/m\mathbb{Z})$ to the set of subgroups of $(\mathbb{Z}/m\mathbb{Z})^2$ (Lemma A.5). It follows that $r(\mathbb{Z}/m\mathbb{Z})^2 \not\subset H$ and $H \not\subset r(\mathbb{Z}/m\mathbb{Z})^2$ for all non-trivial proper

divisors r of m, from which one can show that the subgroup H must be cyclic of order m, giving (iii).

Since $\gcd(d, c) = 1$, we have $\gcd(d, c, b) = 1$. Since $a \equiv c \pmod{b}$, we have (iv).

For (v), suppose that the inputs I and I' give J and J', respectively, in step (4) of the algorithm. Since J' is an integral ideal in $[I]$ with minimal norm, as shown in the second paragraph of this proof there is an element $z \in I$ of minimal non-zero norm such that $J' = I\bar{\alpha}/\mathrm{nrd}(I)$. Therefore when running the algorithm on input I, both J and J' appear in the list of ideals generated in step (3); by symmetry, the same occurs with input I'. Since both J and J' are lexicographically first, we have $J = J'$. Let H be as in step (5). By the last sentence of Proposition A.3, the integer d, and thus b, is uniquely determined. Suppose that (d, c) and (d, c') are two generators for H. Then there exists $\lambda \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $\lambda(d, c) = (d, c')$ in H. Since $\lambda d \equiv d \pmod{m}$, we have $\lambda \equiv 1 \pmod{b}$, so $c \equiv c' \pmod{b}$. Thus a is also unique.

For (vi), suppose that inputs $[I]$ and $[I']$ have the same output (d, a, b). The groups H and H' from step (5) of the algorithm are both subgroups of $(\mathbb{Z}/m\mathbb{Z})^2$, where $m = db$. The group H is generated by (d, c) for some c with $a = c \pmod{b}$ and $\gcd(d, c) = 1$, and H' is generated by (d, c') for some c' with $a = c' \pmod{b}$ and $\gcd(d, c') = 1$. By Lemma A.6 we have $H = H'$. Since (by Lemma A.5) the map that sends a matrix to its rowspace induces a bijection from the set of left ideals of $M_2(\mathbb{Z}/m\mathbb{Z})$ to the set of subgroups of $(\mathbb{Z}/m\mathbb{Z})^2$, we have $\mathcal{I} = \mathcal{I}'$. Then $J/m\mathcal{O}_N = J'/m\mathcal{O}_N$, so $J = J'$ and $[I] = [J] = [J'] = [I']$.

For (vii), the $\mathbb{Z}$-rank of I is 4, so step (1) runs in polynomial time.

Viewed as lattices in $\mathbb{R}^4$, the index $[\mathcal{O}_N : I]$ can be computed as the square root of a ratio of determinants. Since $\mathrm{nrd}(I) = \sqrt{[\mathcal{O}_N : I]}$, the reduced norm in step (2) can be computed in polynomial time.

In step (3), it is easy to compute all the elements of minimal non-zero norm from one of them, since each I has at most six z of minimal non-zero norm. To see this, observe that $z, z' \in I$ both have minimal norm if and only if $z' = uz$ for some unit $u \in \mathcal{O}_N^\times$. The proof of Proposition A.7 gives an explicit generator for $\mathcal{O}_N^\times$, which has order at most 6. If $N \equiv 1 \pmod{12}$, then $\mathcal{O}_N^\times = \{\pm 1\}$, so up to sign there is a unique $z \in I$ of minimal non-zero norm, and only one ideal J_z.

Thus all steps run in polynomial time, except that the invocation of Proposition A.4 in step (4) might necessitate the use of a quantum polynomial-time algorithm to factor m. □

Unfortunately, some triples (d, a, b) are not canonical encodings, as seen in the following example. Fortunately, we can detect when a triple is not canonical; we do that in the Algorithm 5.5 below.

Example 5.4. Let $N = 23$, so $H_{23} = H(-3, -23)$ and $\mathcal{O}_{23} = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{j+ij}{2} + \mathbb{Z}\frac{i-ij}{3}$. Let $\alpha = \frac{1+i}{2}$ and $\beta = \alpha + \frac{i-ij}{3} = \frac{3+5i-2ij}{6}$ and $I = (2, \beta)$. Then $\mathrm{nrd}(I) = 2$, and I, $I\alpha$, and $I\alpha^2$ are the only ideals in $[I]$ of minimal norm. Applying the algorithm of Proposition A.4 gives the isomorphism $\mathcal{O}_{23}/2\mathcal{O}_{23} \xrightarrow{\sim} M_2(\mathbb{Z}/2\mathbb{Z})$ that sends α to $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ and β to $\left[\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right]$. The image of I (resp., $I\alpha, I\alpha^2$) is the set of matrices with row space generated by $(1, 1)$ (resp., $(1, 0), (0, 1)$). It follows that exactly one of $(1, 1, 2)$, $(1, 0, 2)$, and $(2, 0, 1)$ (depending on which of $I, I\alpha, I\alpha^2$ is lexicographically first) can be a canonical encoding of an ideal class in $\mathrm{Cls}(\mathcal{O}_{23})$.

Algorithm 5.5. *INPUT: A prime $N \geq 5$, a $\mathbb{Z}$-bases $(\omega_1, \omega_2, \omega_3, \omega_4)$ for a maximal order $\mathcal{O}_N$ in H_N, and a triple of integers (d, a, b).*

OUTPUT: 1 *if (d, a, b) is the canonical encoding of some fractional ideal of $\mathcal{O}_N$, along with an ideal $J \subset \mathcal{O}_N$ whose canonical encoding is (d, a, b);* 0 *otherwise.*

1. *If $a \geq b$ or $a < 0$ or $d < 1$ or $b < 1$ or $\gcd(d, a, b) > 1$, output* 0 *and stop.*
2. *Apply the algorithm in Lemma A.2 to compute an integer c such that $\gcd(d, c) = 1$ and $c \equiv a \pmod{b}$.*
3. *Set $m = db$. Apply the algorithm of Proposition A.4 to obtain an isomorphism $f_{N,m} : \mathcal{O}_N/m\mathcal{O}_N \xrightarrow{\sim} M_2(\mathbb{Z}/m\mathbb{Z})$, let $\pi : \mathcal{O}_N \to \mathcal{O}_N/m\mathcal{O}_N \to M_2(\mathbb{Z}/m\mathbb{Z})$ be the composition of reduction mod N with $f_{N,m}$, and compute $\pi(\omega_i)$ for each i.*
4. *Compute $x_i \in \mathbb{Z}$ such that $\sum_{i=1}^4 x_i \pi(\omega_i) = \left[\begin{smallmatrix} d & c \\ 0 & 0 \end{smallmatrix}\right]$.*
5. *Compute $\alpha = \sum_{i=1}^4 x_i \omega_i$ and compute a $\mathbb{Z}$-basis for the ideal $J \subset \mathcal{O}_N$ generated by m and α.*
6. *Apply Algorithm 5.2 to compute the canonical encoding (d', a', b') of J.*
7. *Output* 1 *and the ideal J if $(d', a', b') = (d, a, b)$, and otherwise output* 0.

Proposition 5.6. *Algorithm 5.5 is correct and runs in quantum polynomial time.*

Proof. Suppose that I is a left fractional ideal of $\mathcal{O}_N$ and suppose that (d, a, b) is its canonical encoding. Let c, $m = db$, and J be as in Algorithm 5.5 with input (d, a, b). To show correctness, by Theorem 5.3(v) it suffices to show that $[I] = [J]$.

Let J', c', and $H' = \langle (d, c') \rangle$ be as in steps (3) and (5) of Algorithm 5.2 with input I. Let H be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^2$ generated by (d, c). Then $\gcd(d, c) = 1 = \gcd(d, c')$ and $c \equiv c' \pmod{b}$. By Lemma A.6 we have $H = H'$. Since J (resp., J') is the inverse image, under the composition $\mathcal{O}_N \to \mathcal{O}_N/m\mathcal{O}_N \xrightarrow{\sim} M_2(\mathbb{Z}/m\mathbb{Z})$, of the set of matrices whose rows are in $H = H'$, we have $J = J'$, so $[J] = [J'] = [I]$.

Steps (4) and (5) are linear algebra. All steps run in polynomial time, except that steps (3) and (6) might necessitate the use of a quantum polynomial-time algorithm to factor m. □

We will need to bound the size of m that we may need to deal with.

Lemma 5.7. *Suppose z is an element of minimal non-zero norm in a fractional ideal I for $\mathcal{O}_N$. Let $J = \frac{1}{\mathrm{nrd}(I)} I\bar{z}$ and $m = \mathrm{nrd}(J)$. Then $m \leq \sqrt{2}\sqrt{N}$.*

Proof. Let $\lambda_1(I)$ denote the length of a shortest non-zero vector in the lattice I, and let D denote the discriminant of I. By the Hermite bound we have $\lambda_1(I)^4 \leq 2|\det(I)| = 2\sqrt{D}$. But $\mathrm{nrd}(z) = \lambda_1(I)^2$, so $\mathrm{nrd}(z) \leq \sqrt{2}\sqrt[4]{D}$.

By Lemma 15.2.15 and Proposition 16.4.3 of [26] we have $\mathrm{nrd}(I) = \sqrt[4]{D}/\sqrt{N}$. Thus $m = \mathrm{nrd}(z)/\mathrm{nrd}(I) = \mathrm{nrd}(z)\sqrt{N}/\sqrt[4]{D} \leq \sqrt{2}\sqrt{N}$. □

5.4. **Computation of normalized Brandt Operators $T(p)$.** Given an ideal class $[J]$, we will need to find the multiset of ideal classes $[I]$ with non-zero $a_p([I], [J])$-entries. This is relatively straightforward as we need to find $I \supset J \supset pI$ that are invariant under left multiplication by $\mathcal{O}_N$, or equivalently we need to find $J/pI \subset I/pI$ that are invariant under $\mathcal{O}_N/p\mathcal{O}_N$. It is a standard fact that the action of $\mathcal{O}_N/p\mathcal{O}_N$ on I/pI is isomorphic to the action of $M_2(\mathbb{Z}/p\mathbb{Z})$ on itself. Once such isomorphisms are computed using the algorithm of Proposition A.4 in Appendix A, the invariant elements of I/pI correspond to $\{A \in M_2(\mathbb{Z}/p\mathbb{Z}) \mid Av = 0\}$ for v some non-zero element in $(\mathbb{Z}/p\mathbb{Z})^2$. Since these sets are invariant under scaling of v, there are exactly

$p+1$ such J's, and they are computable in a straightforward manner. Furthermore, since J is a small index sublattice of I, from a reduced basis of I it is relatively simple to compute a reduced basis for J and thus, the appropriate canonical representation for $[J]$. This allows us to compute the non-zero entries of a row of the Brandt matrix $T'(p)$. Proposition A.7 in Appendix A gives the w_I, and hence the normalized Brandt matrix $T(p)$. Then, using standard Hamiltonian simulation algorithms, it is straightforward to approximate the action of $e^{iT(p)/\sqrt{p}}$ on V_N. By [3, Theorem 1], $e^{iT(p)/\sqrt{p}}$ can be computed with gate complexity polynomial in p and $\log(N)$.

If p is small compared to N, then $T(p)$ is a sparse matrix, since each column has at most $p+1$ non-zero entries and the matrix is $h \times h$ with $h = O(N/12)$.

5.5. **Producing Maximally Entangled States.** There is one additional difficulty in implementing our scheme in this context. Namely, there is no obvious way to produce a maximally entangled state for $V_N \otimes V_N$. In this section, we provide an efficient algorithm for doing this.

In order to produce this representation, we first note that it suffices to produce a state that is a uniform superposition of the representatives for the elements of $\mathrm{Cls}(\mathcal{O}_N)$. In order to do this, we begin by providing a different representation of such elements.

The following algorithm efficiently produces a superposition over canonical encodings of ideal classes.

Algorithm 5.8.

INPUT: A prime number $N \geq 5$ and an N-extremal maximal order $\mathcal{O}_N$.

OUTPUT: Either a quantum state proportional to $\sum |d,a,b\rangle$, where (d,a,b) varies over the canonical encodings of the elements in $\mathrm{Cls}(\mathcal{O}_N)$, or else $\perp$.

1. *Prepare a state $|\psi\rangle$ proportional to $\sum_{d=1}^{\lfloor\sqrt{2N}\rfloor} \frac{1}{\sqrt{d}} |d\rangle$.*
2. *Apply to $|\psi\rangle$ the linear map that sends $|d\rangle$ to*
$$|d\rangle \otimes \left(\frac{1}{\sqrt{C_d}} \sum_{i=1}^{C_d} |i\rangle \right)^{\otimes 2},$$
where $C_d = \lfloor \sqrt{2N}/d \rfloor$, and call the resulting state $|\psi_1\rangle$.
3. *Writing f for a function that implements Algorithm 5.5, apply to $|\psi_1\rangle |0\rangle$ the operator that sends $|d,a,b\rangle |0\rangle$ to $|d,a,b\rangle |f(d,a,b)\rangle$, and call the resulting state $|\psi_2\rangle$.*
4. *Measure the last register of the quantum state $|\psi_2\rangle$. If the result is 0, output $\perp$. Otherwise, output $|\psi_2\rangle$.*

If the algorithm outputs $\perp$, we say it fails; otherwise we say it succeeds.

Theorem 5.9. *Algorithm 5.8 succeeds with probability at least $(1 - \frac{1}{N}) \frac{1}{32\pi^2}$.*

Proof. Step (1) can be implemented by first preparing the state $\frac{1}{\sqrt{M}} \sum_{m=1}^{M} |m\rangle$ where $M := \lfloor \log_2(\sqrt{2N}) \rfloor$, then appending a zero qubit to this state and applying the operator defined by

$$|m0\rangle \mapsto \sum_{d=2^m}^{2^{m+1}} \left[\frac{1}{\sqrt{d}} |d0\rangle + \sqrt{\frac{1}{2^m} - \frac{1}{d}} |d1\rangle \right],$$

and then measuring the last qubit. If the result is 1, start over. If the result is 0, step (1) has succeeded. One can compute that the success probability for step (1) is at least $\frac{1}{2}$.

For each d let C'_d be the least power of 2 larger than C_d. To implement step (2), consider the following procedure. First, apply the operator defined by $|d0\rangle \mapsto \frac{1}{\sqrt{C'_d}} |d\rangle \sum_{i=1}^{C'_d} |i\rangle$. Define $B(d,i) := 0$ if $i > C_d$ and $B(d,i) := 1$ if $i \leq C_d$. Apply the operator defined by $|di\rangle \mapsto |di\rangle |B(d,i)\rangle$ and measure the last register. If the result is 0, reject and start over. Rejection occurs with probability $\leq \frac{1}{2}$. If the result is 1, discarding the last register leaves a state of the form $\frac{1}{\sqrt{C_d}} |d\rangle \sum_{i=1}^{C_d} |i\rangle$. Applying the above procedure twice produces the output of step (2). The success probability for step (2) is $\geq \frac{1}{4}$.

Step (2) outputs a state that approximates the uniform distribution of $|d,a,b\rangle$ for (d,a,b) running over positive integers with $da, db \leq \sqrt{2N}$. By Lemma 5.7, these triples include all the canonical encodings of elements of $\mathrm{Cls}(\mathcal{O}_N)$. The number of states in this distribution is thus

$$\sum_{d=1}^{\lfloor\sqrt{2N}\rfloor} \left(\frac{\sqrt{2N}}{d}\right)^2 \leq 2N \sum_{d=1}^{\infty} \frac{1}{d^2} = \frac{\pi^2 N}{3}.$$

The number of triples (d,a,b) that are canonical encodings is $\#\mathrm{Cls}(\mathcal{O}_N) \geq (N-1)/12$. Thus the success probability in step (4) is at least $((N-1)/12)/(\pi^2 N/3) = (1-\frac{1}{N})\frac{1}{4\pi^2}$. The claim follows. □

Using Algorithm 5.8, we can next obtain a maximally entangled state by applying a controlled-NOT operator. We implement this in the next section in our instantiation of the minting algorithm.

5.6. **Instantiation of protocol.** Algorithm 5.10 below is our instantiation of the minting algorithm using normalized Brandt operators. Fix N, $H_N, \mathcal{O}_N$, and V_N as before, and choose primes $p_1, \ldots, p_t$ distinct from N. Let $T(p_j)$ be the normalized p_j-Brandt matrix for level N (as defined in §5.2) and let $U_j = e^{iT(p_j)/\sqrt{p_j}}$. Recall that §5.4 allows one to compute $T(p_j)$ and the action of U_j on V_N. Let $\{|\psi_i\rangle\}$ be a joint eigenbasis for the U_j's, and fix ε for which $\{|\psi_i\rangle\}$ is ε-separated. Set the public parameters PP to be $(N, H_N, \mathcal{O}_N, p_1, \ldots, p_t, \varepsilon)$. Let SK be a signing key for a fixed digital signature algorithm. The Mint algorithm is as follows.

Algorithm 5.10. *INPUT:* PP, SK

OUTPUT: a uniformly random valid bill $(|\psi\rangle, v, \sigma)$ *with* $|\psi\rangle \in V_N$.

1. *Apply Algorithm 5.8 to obtain the superposition* $\sum |d,a,b\rangle$*, where the sum is over all the canonical encodings of the elements of* $\mathrm{Cls}(\mathcal{O}_N)$.
2. *Append an ancillary register initialized to* 0 *and apply controlled-NOT operators to obtain the quantum state* $\sum(|d,a,b\rangle \otimes |d,a,b\rangle)$.
3. *Apply phase estimation with the operators* $U_j \otimes I_h$ *and* $I_h \otimes U_j$ *for* $j = 1, \ldots, t$*. Let* $|\psi\rangle$ *be the resulting quantum state and* v *the tuple of eigenvalues.*
4. *If* $v_j = e^{i(p_j+1)/\sqrt{p_j}}$ *for all* j*, output* $\perp$*. Otherwise, let* σ *be the signature of* v*, and output* $(|\psi\rangle, v, \sigma)$.

This instantiation of the minting algorithm is essentially the same as the black box Mint algorithm of §2, except that it takes place in the subspace V_N, not in all of $\mathbb{C}^{\mathrm{Cls}(\mathcal{O}_N)}$.

Theorem 5.11. *The* Mint *Algorithm 5.10 has correct output with probability at least* $\frac{1}{32\pi^2}(1-\frac{1}{N})(1-\frac{12}{N})$*, and runs in quantum polynomial time.*

Proof. The subspace V_N is the orthogonal complement of the span of $|\psi_0\rangle := \sum \frac{1}{w_I}|d,a,b\rangle$, where the sum is over the canonical encodings of the elements of $\mathrm{Cls}(\mathcal{O}_N)$, and $w_I = \#\mathcal{O}_I^\times/\{\pm 1\}$ where $\mathcal{O}_I$ is the right order of any ideal I with canonical encoding (d,a,b). As $|\psi_0\rangle$ is itself an eigenvector for the normalized Brandt operators, in the minting protocol it suffices to check that the output is not $|\psi_0\rangle \otimes |\psi_0\rangle$. (When $N \equiv 1 \pmod{12}$, then $|\psi_0\rangle \otimes |\psi_0\rangle$ is the maximally entangled state as in Step 2 of Algorithm 5.10.) Since $T(p)|\psi_0\rangle = (p+1)|\psi_0\rangle$, we have $U_p|\psi_0\rangle = e^{i(p+1)/\sqrt{p}}|\psi_0\rangle$. By ε-separation, step (4) outputs $\perp$ if and only if $|\psi\rangle = |\psi_0\rangle \otimes |\psi_0\rangle$; otherwise, the output is a valid bill with a note in V_N.

By Theorem 5.9, step (1) succeeds with probability bounded below by $\frac{1}{32\pi^2}(1-\frac{1}{N})$. The state proportional to

$$\sum(|d,a,b\rangle \otimes |d,a,b\rangle)$$

is a uniform superposition of all of the eigenstates of the form $|\psi_i\rangle \otimes |\psi_i\rangle$. Since there are at least $N/12$ such states, the probability of obtaining the state $|\psi_0\rangle \otimes |\psi_0\rangle$ is at most $\frac{12}{N}$. The claim follows. □

Remark 5.12. Our motivation for working in V_N instead of $\mathbb{C}^{\mathrm{Cls}\mathcal{O}_N}$ is that $|\psi_0\rangle \otimes |\psi_0\rangle$ is an easy state to manufacture, so allowing this state to be a valid note would permit easy attacks by the mint or by others as in §3.

The instantiation of the verification algorithm Verify is identical to the black box algorithm of §2.

5.7. **ε-separation.** Our quantum money protocol instantiation requires that the eigenbasis for the operators $e^{iT(p)/\sqrt{p}}$ be ε-separated. Table 1 in Appendix B gives experimental data that suggests that the eigenbasis is ε-separated even for ε quite large; for instance, $\varepsilon = 1/(4\log_2(N))$ works for all N in Table 1, where we use $e^{iT(p)/\sqrt{p}}$ for all primes $p < \log_2(N)$.

For the normalized Brandt operators $T(p)$, rather than $e^{iT(p)/\sqrt{p}}$, Goldfeld and Hoffstein [11] obtain ε-separation when the number of operators m is $O(N\log N)$, and obtain a bound for m that is polylog(N) if they assume a version of the Riemann hypothesis. However, the ε is not explicit. Note that Goldfeld and Hoffstein, as well as Serre's result below, deal with the Brandt operators $T'(p)$, but since $T(p)$ and $T'(p)$ are similar, the eigenvalues are identical, and so these results apply to $T(p)$ as well.

Theorem 5.13 ([11], Theorems 3 and 2)**.** *Let $N \geq 5$ be a prime. For each prime $p \neq N$, let $T(p)$ be the normalized p-Brandt matrix for level N. Then:*

(1) There exist a constant $K = O(N\log N)$ and $\varepsilon > 0$ such that if $p_1, \ldots, p_t$ is the list of primes $\leq K$ with $p_i \neq N$, then every eigenbasis for the operators $T(p_1), \ldots, T(p_t)$ is ε-separated.

(2) *If the Riemann hypothesis for Rankin-Selberg zeta functions holds, then there exist a constant* $K = O((\log N)^2(\log\log N)^4)$ *and* $\varepsilon > 0$ *such that if* $p_1, \ldots, p_t$ *is the list of primes* $\leq K$ *with* $p_i \neq N$*, then every eigenbasis for the operators* $T(p_1), \ldots, T(p_t)$ *is* ε*-separated. If* $N > e^{15}$*, one can take* $K = 16(\log N)^2(\log\log N)^4$.

Proposition 5.14. *Suppose* $p_1 \ldots, p_t, N$ *are distinct prime numbers with* $N \geq 5$*. Then every eigenbasis with respect to* $T(p_1), \ldots, T(p_t)$ *that is* ε*-separated for some* $\varepsilon > 0$ *is also an eigenbasis with respect to* $\left\{e^{\frac{i}{\sqrt{p_j}}T(p_j)}\right\}$ *that is* ε'*-separated for some* ε' *such that* $0 < \varepsilon' = O(\varepsilon/\sqrt{\max_j\{p_j\}})$.

Proof. Let $U_j = e^{\frac{i}{\sqrt{p_j}}T(p_j)}$ and $K = \max_j\{p_j\}$. By Deligne's proof of the Weil conjectures [8], the eigenvalues of $T(p_j)$ lie in the interval $[-2\sqrt{p_j}, 2\sqrt{p_j}]$, so the eigenvalues of $\frac{1}{\sqrt{p_j}}T(p_j)$ lie in $[-2, 2]$. Let $H = \{z \in S^1 \mid -2 \leq \arg(z) \leq 2\}$. The map on t-tuples $\rho : [-2, 2]^t \to H^t$ given coordinate-wise by $\lambda \mapsto e^{i\lambda}$ sends tuples of eigenvalues with respect to the $\frac{1}{\sqrt{p_j}}T(p_j)$ to the corresponding tuple of eigenvalues with respect to the U_j. Since ρ^{-1} is Lipschitz continuous, there exists $M > 0$ such that for all $v_1, v_2 \in [-2, 2]^t$ we have $|v_1 - v_2| \leq M|\rho(v_1) - \rho(v_2)|$. If v_1 and v_2 are two distinct tuples of eigenvalues for $\frac{1}{\sqrt{p_j}}T(p_j)$, then $|v_1 - v_2| > \frac{1}{\sqrt{p_j}}\varepsilon$. It follows that with respect to the U_j's our joint eigenbasis is ε'-separated for $\varepsilon' = \frac{1}{M\sqrt{K}}\varepsilon$. □

Theorem 5.15 below gives heuristic evidence that a "random" eigenbasis will most likely be ε-separated for a large value of ε. Fix primes $p_1, \ldots p_t$. As before, for each prime N distinct from $p_1, \ldots, p_t$, let $\{v_{i,N}\}_{i=1}^h$ denote the set of vectors of eigenvalues for an eigenbasis for $\{\frac{1}{\sqrt{p_j}}T(p_j)\}_{j=1}^t$, where $T(p_j)$ is the normalized p_j-Brandt matrix for level N and $h = \#\mathrm{Cls}(\mathcal{O}_N)$. On the interval $[-2, 2]$, let μ_p denote the probability measure

$$\frac{p+1}{\pi} \cdot \frac{(1 - x^2/4)^{1/2}}{(\sqrt{p} + \frac{1}{\sqrt{p}})^2 - x^2} dx.$$

Theorem 5.15 (Théorème 3, [22])**.** *The distribution of vectors* $\{v_{i,N}\}_{i=1}^h \subset [-2, 2]^t$*, where* N *is a prime not equal to* $p_1, \ldots, p_t$*, approaches the product measure* $\prod_{i=1}^t \mu_{p_i}$ *as* N *goes to infinity.*

For p large, μ_p approaches the distribution $\frac{1}{2\pi}\sqrt{4 - x^2}dx$. Thus the distribution of the eigenvalues of the $U_j = e^{iT(p_j)/\sqrt{p_j}}$ in the subset of S^1 with argument $x \in [-2, 2]$ will approach the distribution $\frac{1}{2\pi}\sqrt{4 - x^2}dx$. A more precise statement on the distribution of eigenvalues is given in [19, Theorem 19].

Remark 5.16. In light of Theorem 5.15, a natural assumption is that the $v_{i,N}$ act like independent random samples drawn from the distribution $\prod_{i=1}^t \mu_{p_i}$. Under this assumption, if $0 < \varepsilon < 1$, then for t larger than a sufficiently large multiple of $\log N$, with high probability the eigenbasis for the U_j is ε-separated.

6. Security of the Instantiation

In Theorem 6.2 we reduce the security of the instantiation to the hardness of Problem 6.1 below.

As the operators U_j in the instantiation are no longer black box, one must now consider additional attacks. In §§6.2–6.6 we note some of the most obvious attacks on Problem 6.1, and reasons we do not expect them to work. In each case, instead of an attacker with only black box access to the U_j we consider an attacker that uses some property of the instantiation.

6.1. **Security Reduction.** The following problem restates Problem 3.1 in the setting of our instantiation.

Problem 6.1. Given a prime $N \geq 5$, and operators $U_j = e^{iT(p_j)/\sqrt{p_j}}$, where the $T(p_j)$ are the normalized Brandt matrices acting on V_N corresponding to distinct primes $p_1, \ldots, p_t$ not equal to N, output a state of the form $|\psi\rangle\,|\psi\rangle\,|\psi\rangle$, where $|\psi\rangle$ is an eigenvector for all the U_j's.

The following result shows that our quantum money proposal is secure if Problem 6.1 is hard and the digital signature algorithm is secure.

Theorem 6.2. *(1) If an adversary using a quantum computer and given the secret key to the signing protocol can in time T run a procedure that with probability at least p produces $n+1$ valid bills with at most n total serial numbers among them, then the adversary can with constant positive probability solve Problem 6.1 in time $O(T/p)$.*

(2) If an adversary, using a quantum computer and given n bills and s uniformly random valid signatures of serial numbers, but without access to the signing key for the signatures, can in time T run a procedure that with probability at least p produces $n+1$ bills that pass the verification procedure, then with constant positive probability the adversary in time $O(T/p)$ and given $n+s$ valid bills can either produce a new valid signature without access to the private key, or else solve Problem 6.1.

Proof. The proof is word for word the same as that of Theorem 3.2, with Problem 6.1 in place of Problem 3.1. □

6.2. **Use of Other U_j.** An attacker will have access not just to the U_j used in the quantum money protocol but also to $e^{iT(p)/\sqrt{p}}$ for any reasonably sized prime p. Since the black box lower bound from Theorem 4.1 does not depend on the number of operators, its conclusion still holds, if one were to treat the U_j as black box operators.

6.3. **Other Powers of $e^{iT(p)/\sqrt{p}}$.** An attacker will be able to apply arbitrary powers of the U_j, by computing $e^{i\gamma T(p)/\sqrt{p}}$ for any $\gamma \in \mathbb{R}$. The following modification of Theorem 4.1 shows that this does not help.

Theorem 6.3. *Suppose $\mathcal{A}$ is an algorithm that, on input a real number $\gamma \in \mathbb{R}$ and a black-box unitary operator e^T, outputs a black-box unitary operator that approximates $e^{\gamma T}$. Suppose $\mathcal{D}$ is any probability distribution over $(S^1)^t$ such that with high probability, any finite number of samples chosen from $\mathcal{D}$ are distinct. Then any circuit consisting of standard gates and controlled $\mathcal{A}(\gamma, U_j)$ gates that solves Problem 3.1 with constant positive probability for sets of operators $U_1, \ldots, U_t$ chosen according to $\mathcal{D}$ and with uniformly random eigenbasis $\{|\psi_i\rangle\}$ must have $\Omega((N/\log(N))^{1/3})$ controlled $\mathcal{A}(\gamma, U_j)$ gates.*

The only difference between the proofs of Theorems 6.3 and 4.1 is that the calls to $\mathcal{A}$ might give a different distribution $\mathcal{D}$ of eigenvalues. We may assume that the γ chosen in Theorem 6.3 all satisfy $0 < \gamma \leq 1$. Then the distribution induced by replacing each sample from $\mathcal{D}$ with its γth power for some $0 < \gamma \leq 1$ also has the property that with high probability, any finite number of samples are distinct.

6.4. **Sparse Logarithms.** The matrices $T(p)$ are too large to be able to directly compute their eigenvectors via classical algorithms from linear algebra. However, the $\log(U_j) = \frac{1}{\sqrt{p_j}}T(p_j)$ used in our protocol are sparse operators. One might potentially take advantage of this. A potential worry is that one might use an HHL-like quantum algorithm [13] to find eigenvectors (one cannot use HHL directly as the matrix used would not be invertible). Since an HHL-like algorithm would deal with $e^{itT(p)}$ for $t \in \mathbb{R}$ via Hamiltonian simulation, rather than directly with the sparse matrices $\frac{1}{\sqrt{p}}T(p)$, this would be covered by our black box lower bounds. It is not clear how else an attack might make use of the sparsity of each $\frac{1}{\sqrt{p}}T(p)$.

6.5. **Quantum State Restoration.** A technique in [9] was developed to break a number of quantum money schemes that look superficially like ours. These schemes use eigenstates of some operator H where the state itself has some clean (but secret) product representation. They show in [9] that if one is given a state $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \in V_A \otimes V_B$ and can compute a measurement of whether we are in state $|\psi\rangle$, we can produce a duplicate of the state $|\psi_B\rangle$ in time $\text{poly}(\dim(V_B))$. If the supposedly secure state is a tensor product of many small pieces, this can be used to recover the individual pieces one at a time.

However, we have no reason to believe that the eigenstates involved in our algorithm can be decomposed as such tensor products, so this class of attacks seems unlikely to work. In fact, it is unclear if there is even any natural way to write V_N as a tensor product.

6.6. **Modular Forms and Elliptic Curves.** The system of operators $T(p)$ acting on V_N is isomorphic to the system of Hecke operators T_p acting on the space $S_2(\Gamma_0(N))$ of weight two cusp forms of level N (see [21, 18]). Further, there is an equivalence of categories between classes of left ideals in a fixed maximal order in a quaternion algebra of prime discriminant p and isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (see for example [26, Chapter 42]).

We do not see a way to use these relationships between quaternion algebras and modular forms, or between quaternion algebras and elliptic curves, to provide an attack. Since one uses quaternion algebras to make computations associated with modular forms easier [21, 26, 16], it seems unlikely that it would be helpful to use modular forms to attack a protocol based on quaternion algebras. Below, we attempt to use the theory of modular forms to attack our instantiation, and give a more detailed explanation as to why we think that a modular forms approach is likely to be fruitless. Here we focus on using the theory of modular forms, but one could equivalently phrase this using elliptic curves, via the equivalence given in [18]. A reference for the theory of modular forms is [17].

To try to solve Problem 6.1, one could try to directly manufacture a specific eigenstate $|\psi\rangle$ three times in succession to obtain a solution to Problem 6.1. We next consider two "direct manufacture" problems.

Cusp forms are typically encoded as power series $f(q) = \sum_{n=1}^{\infty} a_n q^n$. If f is a simultaneous eigenvector of all the Hecke operators T_p, normalized so that $a_1 = 1$, then the eigenvalue of T_p is a_p. Such a cusp form f is called an *eigenform* for the Hecke operators.

Problem 6.4. Given a prime N and a normalized eigenform $f \in S_2(\Gamma_0(N))$ for the Hecke operators T_p with corresponding eigenvalue a_p for all primes p, output a simultaneous eigenstate $|\psi\rangle$ of $e^{iT(p)/\sqrt{p}}$ for all primes p, such that the corresponding eigenvalue is $e^{ia_p/\sqrt{p}}$.

Problem 6.5. Given a prime $N \geq 5$, complex numbers $\alpha_1, \ldots, \alpha_t$, operators $U_j = e^{iT(p_j)/\sqrt{p_j}}$, where the $T(p_j)$ are the normalized Brandt matrices acting on V_N corresponding to distinct primes $p_1, \ldots, p_t$ not equal to N, and a promise that there is a simultaneous eigenstate of $U_1, \ldots, U_t$ such that U_j has eigenvalue α_j for each j, output such a simultaneous eigenstate $|\psi\rangle$ of $U_1, \ldots, U_t$ with eigenvalues $\alpha_1, \ldots, \alpha_t$, respectively.

Lemma 6.6.

(i) Every solution to Problem 6.4 is unique (up to scalar).

(ii) If every instance of Problem 6.5 with fixed choice of N and $U_1, \ldots, U_t$ as part of the input has a solution that is unique up to scalar, then every eigenbasis for this choice of $N, U_1, \ldots, U_t$ is ε-separated for some $\varepsilon > 0$.

(iii) Given N and $U_1, \ldots, U_t$, if there is an ε-separated eigenbasis for the U_j's for some $\varepsilon > 0$, then every solution to Problem 6.5 with these N and $U_1, \ldots, U_t$ as part of the input is unique (up to scalar).

Proof. For (i), fix an instance N and $f = \sum a_n q^n$ of Problem 6.4, and suppose $|\psi\rangle$ and $|\psi'\rangle$ are simultaneous eigenstates for $e^{iT(p)/\sqrt{p}}$ with eigenvalue $e^{ia_p/\sqrt{p}}$ for all primes p. Then for each prime p, the states $|\psi\rangle$ and $|\psi'\rangle$ are simultaneous eigenvectors for the operators $T(p)$. The eigenvalue for $T(p)$ of $|\psi\rangle$ is $\frac{a_p}{p_j} + 2\pi k_p$ for some $k_p \in \mathbb{Z}$. Since $T(p)$ is an integer matrix, its eigenvalues, including a_p, are algebraic numbers. Therefore $2\pi k_p$ is also algebraic, so $k_p = 0$ for all p. Thus, a_p is the eigenvalue for the operator $T(p)$ of $|\psi\rangle$, and similarly of $|\psi'\rangle$. By the multiplicity one theorem for weight two cusp forms of prime level, two normalized eigenforms in $S_2(\Gamma_0(N))$ with the same eigenvalues for all the Hecke operators T_p must be equal. Since the system of Hecke operators T_p acting on $S_2(\Gamma_0(N))$ is isomorphic to the system of operators $T(p)$ acting on V_N, it follows that $|\psi\rangle$ and $|\psi'\rangle$ are scalar multiples, giving (i).

For (ii), suppose $\{|\psi_i\rangle\}_{i=1}^h$ is an eigenbasis that is not ε-separated for any ε, with eigenvalues z_{ij} satisfying $U_j |\psi_i\rangle = z_{ij} |\psi_i\rangle$ for $i = 1, \ldots, h$ and $j = 1, \ldots, t$. Then there exist $k \neq \ell$ such that $z_{kj} = z_{\ell j}$ for all j. Set $\alpha_j = z_{kj}$ for each j. Then $|\psi_k\rangle$ and $|\psi_\ell\rangle$ are linearly independent solutions to Problem 6.5, for the given $N, U_1, \ldots, U_t$. This gives (ii).

For (iii), suppose $\{|\psi_i\rangle\}_{i=1}^h$ is an ε-separated eigenbasis for some $\varepsilon > 0$, with eigenvalues z_{ij} satisfying $U_j |\psi_i\rangle = z_{ij} |\psi_i\rangle$, and suppose $|\psi\rangle$ and $|\psi'\rangle$ are two solutions to Problem 6.5. Write $|\psi\rangle = \sum c_i |\psi_i\rangle$ and $|\psi'\rangle = \sum c_i' |\psi_i\rangle$ with $c_i, c_i' \in \mathbb{C}$. Applying U_j to both equations gives $c_i \alpha_j = c_i z_{ij}$ and $c_i' \alpha_j = c_i' z_{ij}$ for all i and j. Choose k so that $c_k \neq 0$. Then $\alpha_j = z_{kj}$ for all j. Suppose $i \neq k$. Since $\{|\psi_i\rangle\}$ is ε-separated, there exists j such that $z_{ij} \neq z_{kj} = \alpha_j$. It follows that $c_i = c_i' = 0$ for all $i \neq k$. Thus both $|\psi\rangle$ and $|\psi'\rangle$ are non-zero multiples of $|\psi_k\rangle$, giving (iii). $\square$

In the next result, "with complexity T" for classical algorithms means in time T, and for quantum algorithms means with gate complexity T.

Proposition 6.7. *Suppose there are an algorithm B that on input N can solve Problem 6.5 with complexity B_N, and an algorithm C that on input N with complexity C_N outputs a positive number ε and a list of primes $p_1(N), \ldots, p_{t_N}(N)$ such that there is an ε-separated eigenbasis for $\{e^{iT(p_j(N))/\sqrt{p_j(N)}}\}_{j=1}^{t_N}$. Let $g_{N,p}$ be the complexity of computing $e^{iT(p)/\sqrt{p}}$. Then there is an algorithm that can solve Problem 6.4 on input N with complexity $B_N + C_N + \sum_{j=1}^{t_N} g_{N,p_j(N)}$.*

Proof. Given an instance (N, f) of Problem 6.4, run algorithm C with input N to obtain $\varepsilon > 0$ and primes $p_1(N), \ldots, p_{t_N}(N)$. Set $U_j = e^{iT(p_j(N))/\sqrt{p_j(N)}}$ and $\alpha_j = e^{ia_{p_j(N)}/\sqrt{p_j(N)}}$, and run algorithm B with inputs $N, \alpha_1, \ldots, \alpha_{t_N}, U_1, \ldots, U_{t_N}$ to obtain output $|\psi\rangle$. Suppose $|\psi_0\rangle$ is a solution to Problem 6.4; a solution exists since V_N acted on by the $T(p)$ is isomorphic to $S_2(\Gamma_0(N))$ acted on by the T_p. For each j the state $|\psi_0\rangle$ is an eigenvector for U_j with eigenvalue α_j. By Lemma 6.6(iii), $|\psi\rangle$ is a non-zero scalar multiple of $|\psi_0\rangle$, so it is a solution to Problem 6.4.

For the complexity, algorithms B and C are each run once, and each U_j is computed once. □

Theorem 5.13 and Proposition 5.14 guarantee that ε and the list of primes $p_1(N), \ldots, p_{t_N}(N)$ as in the above proof exist. As in §5.4, each U_j can be computed via a quantum algorithm with gate complexity that is polynomial in $p_j(N)$ and $\log(N)$.

Proposition 6.8. *An adversary that can solve Problem 6.4 and has a simultaneous eigenform f for the Hecke operators can solve Problem 6.1.*

Proof. Solve Problem 6.4 with input f three times in succession. □

There is no known efficient algorithm for solving Problems 6.4 or 6.5. Also, there is no known algorithm that runs in time polynomial in $\log(N)$ for finding a simultaneous eigenform f for the Hecke operators. Indeed, a standard method for finding such forms is to compute eigenvectors of the Brandt matrices (see [18, §2.3], [7]). As mentioned in §6.4, directly computing eigenvectors is difficult since the $T(p)$ are large matrices.

7. Conclusion

We have presented what seems like it should be a fairly efficient quantum money protocol. As far as we can tell, there are no subexponential attacks on this protocol, and so it should be possible to implement securely with only a few hundred qubits.

8. Acknowledgments

Kane would like to thank Scott Aaronson for his help with the presentation of [15]. Sharif and Silverberg would like to thank John Voight for helpful discussions. Kane was supported by NSF Award CCF-1553288 (CAREER), NSF Award CCF-2107547, a Sloan Research Fellowship, and a grant from CasperLabs. Silverberg was supported by NSF Award CNS-1703321 and a grant from the Alfred P. Sloan Foundation.

Appendix A. Arithmetic lemmas

Lemma A.1. *There is a deterministic polynomial-time algorithm that, given positive integers m, e, and r such that $e \mid m$ and $\gcd(r, e) = 1$, computes $k \in \mathbb{Z}$ such that $k \equiv r \pmod{e}$ and $\gcd(k, m) = 1$.*

Proof. For $i = 1, 2, \ldots$ compute $d_i := \gcd(e^i, m)$ until $d_i = d_{i+1}$, and fix that i. Then $\gcd(d_i, m/d_i) = 1$. Compute k such that $k \equiv r \pmod{d_i}$ and $k \equiv 1 \pmod{m/d_i}$. Since $i \leq \log_2 m$, the algorithm runs in polynomial time. □

Lemma A.2. *There is a deterministic polynomial-time algorithm that, given positive integers d, a, and b such that $\gcd(d, a, b) = 1$, computes $c \in \mathbb{Z}$ such that $c \equiv a \pmod{b}$ and $\gcd(d, c) = 1$.*

Proof. Let $e = \gcd(d, b)$. By hypothesis, $\gcd(a, e) = 1$. Apply the algorithm in Lemma A.1 to compute $c' \in \mathbb{Z}$ such that $c' \equiv a \pmod{e}$ and $\gcd(c', d) = 1$. Since $c' \equiv a \pmod{e}$, we can apply the Chinese Remainder Theorem to compute $c \in \mathbb{Z}$ such that $c \equiv c' \pmod{d}$ and $c \equiv a \pmod{b}$. Then $\gcd(d, c) = \gcd(d, c') = 1$. □

Proposition A.3. *There is a deterministic polynomial-time algorithm that, given a positive integer m and a cyclic subgroup $H \subset (\mathbb{Z}/m\mathbb{Z})^2$ of order m, computes $(d, c) \in \mathbb{Z}^2$ that generates H and satisfies $d \mid m$ and $\gcd(d, c) = 1$. The integer d is the unique divisor of m such that (d, γ) generates H for some $\gamma \in \mathbb{Z}$.*

Proof. Theorem 2.6.9 of [5] gives a deterministic polynomial-time algorithm that given m and H, produces $(d', c') \in \mathbb{Z}^2$ that generates H. Since H has order m we have $\gcd(d', c', m) = 1$. Let $d = \gcd(d', m)$. Compute integers r, s such that $d = rd' + sm$. Letting $e = m/d$, then $\gcd(r, e) = 1$. Apply the algorithm in Lemma A.1 to compute $k \in \mathbb{Z}$ such that $k \equiv r \pmod{e}$ and $\gcd(k, m) = 1$. Then $kd' \equiv rd' \pmod{md'/d}$, so $kd' \equiv rd' \equiv d \pmod{m}$. Let $c = kc' \pmod{m}$. Then $(d, c) = k(d', c')$ generates H. Since $d \mid m$ we have $\gcd(d, c) = \gcd(d, c, m) = 1$. Since $i \leq \log_2 m$, the algorithm runs in polynomial time.

Projecting H onto the first component gives a cyclic subgroup of $\mathbb{Z}/m\mathbb{Z}$ of order m/d, for which d is the unique generator that divides m. □

The next result gives an algorithm that computes an isomorphism $\mathcal{O}_N/m\mathcal{O}_N \xrightarrow{\sim} M_2(\mathbb{Z}/m\mathbb{Z})$, where $\mathcal{O}_N$ is a maximal order and the prime $N \nmid m$. For our purposes, it is important that the algorithm produce the same isomorphism each time it is given the same inputs N, $\mathcal{O}_N$, and m. The algorithm invokes a polynomial-time quantum algorithm to factor m. As such, there is some small failure probability. After that, it uses a classical polynomial-time algorithm due to Voight to deterministically construct isomorphisms $\mathcal{O}_N/p^r\mathcal{O}_N \xrightarrow{\sim} M_2(\mathbb{Z}/p^r\mathbb{Z})$ for each prime divisor p of m, where $p^r || m$.

Proposition A.4. *There is an algorithm in complexity class BQP that, given a positive integer m, a prime N that does not divide m, a maximal order $\mathcal{O}_N$ in H_N, and a $\mathbb{Z}$-basis for $\mathcal{O}_N$, produces an isomorphism*

$$f_{N,m} : \mathcal{O}_N/m\mathcal{O}_N \xrightarrow{\sim} M_2(\mathbb{Z}/m\mathbb{Z}).$$

Proof. Factor m (for example using Shor's algorithm). For each prime divisor p of m, with $p^r || m$, apply Proposition 4.8 of [25] and the results mentioned in the paragraph after Problem 4.9 of [25] to obtain an isomorphism $\mathcal{O}_N/p^r\mathcal{O}_N \xrightarrow{\sim} M_2(\mathbb{Z}/p^r\mathbb{Z})$. Then apply the Chinese Remainder Theorem. □

Lemma A.5. *Fix $m \in \mathbb{Z}^{>0}$. Let f denote the map from the set of left ideals of $M_2(\mathbb{Z}/m\mathbb{Z})$ to the set of subgroups of $(\mathbb{Z}/m\mathbb{Z})^2$ induced by sending a matrix to its rowspace. Then f is a bijection, and its inverse is the map g that sends a subgroup H to the set of matrices whose rows are in H.*

Proof. Suppose that H is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^2$. The left action of $M_2(\mathbb{Z}/m\mathbb{Z})$ on H is by row operations, so if $A \in M_2(\mathbb{Z}/m\mathbb{Z})$ and $B \in g(H)$, then the rows of AB are linear combinations of the rows of B, so $AB \in g(H)$. Thus $g(H)$ is a left ideal, and fg is the identity.

To show that gf is the identity, suppose $\mathcal{I}$ is a left ideal of $M_2(\mathbb{Z}/m\mathbb{Z})$ and let $H = f(\mathcal{I})$. Then $\mathcal{I} \subset g(H)$. To show $g(H) \subset \mathcal{I}$, suppose $(x, y) \in H$. By the definition of H, there are matrices $A_1, ..., A_r \in \mathcal{I}$ and for each i a row a_i of A_i such that $(x, y) = \sum_{i=1}^{r} a_i$. Left-multiplying A_i by $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ if necessary, we may assume that a_i is the top row of A_i. Then $\left[\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] \sum_{i=1}^{r} A_i \in \mathcal{I}$, and $\left[\begin{smallmatrix} 0 & 0 \\ x & y \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right] \in \mathcal{I}$. Since such matrices generate $g(H)$, we have $g(H) \subset \mathcal{I}$. □

Lemma A.6. *Suppose that $d, b \in \mathbb{Z}^{>0}$, that $c, c' \in \mathbb{Z}$, that $c = c' \pmod b$, and that $\gcd(d, c) = 1 = \gcd(d, c')$. Let $m = db$ and suppose that H and H' are the subgroups of $(\mathbb{Z}/m\mathbb{Z})^2$ generated by (d, c) and by (d, c'), respectively. Then $H = H'$.*

Proof. Since $\gcd(d, c) = 1$, there exist integers x and y such that $cx = 1 + dy$. Setting $\lambda = 1 + x(c' - c)$, then $\lambda c = c' + yd(c' - c)$, and since $c' \equiv c \pmod b$ it follows that $\lambda c \equiv c' \pmod m$ and $\lambda d \equiv d \pmod m$. Thus $\lambda(d, c) = (d, c')$ in $(\mathbb{Z}/m\mathbb{Z})^2$, so $H' \subset H$. By symmetry, $H \subset H'$, so $H = H'$. □

Recall (Definition 5.1) that if I is a left fractional $\mathcal{O}_N$-ideal of the quaternion algebra H_N, then we let $\mathcal{O}_I$ be its right order and we let $w_I = \#(\mathcal{O}_I^\times/\{\pm 1\}) = \frac{1}{2}\#\mathcal{O}_I^\times$. An integral solution to $x^2 - 3y^2 = -N$ can be found in polynomial time by [24].

Proposition A.7. *We have $w_I = 1$ for all $[I] \in \mathrm{Cls}(\mathcal{O}_N)$, with the following exceptions:*

(1) If $N \equiv 5 \pmod{12}$, then $w_I = 3$ for all $I \in [\mathcal{O}_N]$.
(2) If $N \equiv 7 \pmod{12}$, then $w_I = 2$ for all $I \in [\mathcal{O}_N]$.
(3) Suppose $N \equiv 11 \pmod{12}$. Let $(a, b) \in \mathbb{Z}^2$ be a solution to $x^2 - 3y^2 = -N$. Let $\alpha := \frac{a}{3b}i + \frac{1}{3b}ij$ and $\hat{\mathcal{O}} := \mathbb{Z} + \frac{1+j}{2}\mathbb{Z} + \alpha\mathbb{Z} + \frac{\alpha - \alpha j}{2}\mathbb{Z}$. Then $w_I = 3$ for all $I \in [\mathcal{O}_N]$, and $w_I = 2$ for all $I \in [\mathcal{O}_N \cdot \hat{\mathcal{O}}]$.

Proof. Table 1.3 of [12] shows that $w_I = 1$ for all $[I]$, with the following exceptions: when $N \equiv 5 \pmod{12}$ one ideal class satisfies $w_I = 3$; when $N \equiv 7 \pmod{12}$ one ideal class satisfies $w_I = 2$; and when $N \equiv 11 \pmod{12}$ there are two ideal classes $[I]$ and $[J]$ such that $w_I = 3$ and $w_J = 2$. If $N \equiv 7 \pmod{12}$ then $i^2 = -1$ so $i \in \mathcal{O}_N^\times$ has order 4, and hence $w_{\mathcal{O}_N} = 2$. If $N \equiv 5 \pmod 6$ then $i^2 = -3$ so $\frac{1+i}{2} \in \mathcal{O}_N^\times$ has order 6, and hence $w_{\mathcal{O}_N} = 3$. Now suppose $N \equiv 11 \pmod{12}$. One can check that $\hat{\mathcal{O}}$ is a maximal order, and $\hat{\mathcal{O}}$ is the right order of the ideal $\mathcal{O}_N \cdot \hat{\mathcal{O}}$. We have $\alpha^2 = \frac{-(a^2+N)}{3b^2} = -1$, so $\alpha \in \hat{\mathcal{O}}^\times$ has order 4 and hence $w_{\mathcal{O}_N \cdot \hat{\mathcal{O}}} = 2$. □

See also [14], where $\mathcal{O}_N$ is denoted $\mathcal{O}(3)$ when $N \equiv 5 \pmod 6$, and $\hat{\mathcal{O}}$ is denoted $\mathcal{O}'(1)$.

TABLE 1. ε-separation for $\{e^{iT(p)/\sqrt{p}} \mid p < \log_2(N)\}$

N	ε
547	0.4824236848637427
557	0.7199773703667618
563	0.7553525215246627
569	0.9200347021863563
571	0.48205861423463164
577	0.40674046098264244
587	0.7982583121867862
593	0.9266761931828437
599	0.62563971482572
601	0.7182238262429224
607	0.7313809878961292
613	0.768492003890778
617	0.5983414655675874
619	0.6187541297546084
631	0.45419000886679206
641	0.43490142944562354
643	0.6346083766649872
647	0.7432521901131
653	0.5063114409620633
659	0.6777125171096566

N	ε
12569	0.22159756788222007
12577	0.22690747823008486
12583	0.2774346724081338
12589	0.22865081262562248
12601	0.25482871813162855
12611	0.16451483770778993
12613	0.09017383560136713
12619	0.18211198468203824
12637	0.16246553818517484
12641	0.19366213429958556
20011	0.34309639146812015
20021	0.3536950173591149
20023	0.2610129987276544
20029	0.19283243271645334
20047	0.30798681044672843
20051	0.2711650765294632
20063	0.21456144876447153
20071	0.3506564319413416
20089	0.2942067355453101

APPENDIX B. ε-SEPARATION DATA

For each prime N in Table 1, let $p_1, \ldots, p_t$ be the primes less than $\log_2(N)$, and set $U_j = e^{iT(p_j)/\sqrt{p_j}}$. Letting $|\psi_1\rangle, \ldots, |\psi_h\rangle \in V_N$ be the simultaneous eigenvectors for the U_j's, we used Sage to compute the corresponding tuples of eigenvalues $v_1, \ldots, v_h$, and the minimum Euclidean distance between pairs of tuples of eigenvalues. In Table 1, the value ε is the minimum Euclidean distance $|v_i - v_j|$ for $i \neq j$, and therefore is the largest value of ε for which the eigenbasis is ε-separated. Sage code used to generate the table is available at `https://github.com/ssharif/QuantumMoneyCode`.

REFERENCES

[1] Scott Aaronson and Paul Christiano, *Quantum money from hidden subspaces*, in STOC '12: Proceedings of the forty-fourth annual ACM Symposium on Theory of Computing (2012), 41–60, `https://doi.org/10.1145/2213977.2213983` and in Theory of Computing **9** (2013), 349–401, `http://www.theoryofcomputing.org/articles/v009a009/v009a009.pdf`.

[2] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf, *Quantum Lower Bounds by Polynomials*, in 39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8–11, 1998, Palo Alto, California, USA (pp. 352–361). IEEE Computer Society.

[3] D. W. Berry, A. M. Childs, and R. Kothari, *Hamiltonian Simulation with Nearly Optimal Dependence on all Parameters*, in 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (2015), pp. 792–809, `https://doi.org/10.1109/FOCS.2015.54`.

[4] Gilles Brassard, Peter Høyer, and Alain Tapp, *Quantum cryptanalysis of hash and claw-free functions*, in LATIN'98: Theoretical Informatics, Lecture Notes in Computer Science **1380** (1998) Springer-Verlag, 163–169, https://doi.org/10.1007/BFb0054319.

[5] Iuliana Ciocănea-Teodorescu, *Algorithms for finite rings*, PhD thesis, Université de Bordeaux and Universiteit Leiden, 2016, https://tel.archives-ouvertes.fr/tel-01378003v2/document.

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

[7] Alex Cowan, *Computing newforms using supersingular isogeny graphs*, preprint (2020), https://arxiv.org/abs/2010.10745.

[8] Pierre Deligne, *La conjecture de Weil. I*, Publications Mathématiques de l'IHÉS **43**, (1974), 273–307, https://doi.org/10.1007/BF02684373.

[9] 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*, Phys. Rev. Lett. **105**, 190503 (2010), http://doi.org/10.1103/PhysRevLett.105.190503.

[10] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor, *Quantum money from knots*, in ITCS '12: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (2012), 276–289, https://doi.org/10.1145/2090236.2090260.

[11] Dorian Goldfeld and Jeffrey Hoffstein, *On the number of Fourier coefficients that determine a modular form*, in A Tribute to Emil Grosswald: Number Theory and Related Analysis, Contemporary Math. **143**, AMS, 1993, 385–393.

[12] Benedict H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc. **7**, AMS, 1987, 115–187.

[13] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd, *Quantum Algorithm for Linear Systems of Equations*, Phys. Rev. Lett. **103** (2009), 150502, https://doi.org/10.1103/PhysRevLett.103.150502.

[14] Tomoyoshi Ibukiyama, *On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings*, Nagoya Mathematical Journal **88** (1982), 181–195, https://doi.org/10.1017/S002776300002016X.

[15] Daniel M. Kane, *Quantum Money from Modular Forms*, preprint (2018), https://arxiv.org/abs/1809.05925.

[16] David R. Kohel, *Computing modular curves via quaternions*, Fourth CANT Conference: Number Theory and Cryptography, University of Sydney, 3–5 Dec. 1997, preprint, https://wstein.org/papers/bib/kohel-sydney.pdf.

[17] Serge Lang, Introduction to Modular Forms, Grundlehren der mathematischen Wissenschaften **222**, Springer-Verlag Berlin Heidelberg, 1987.

[18] Jean-François Mestre, *La méthode des graphes. Exemples et applications*, in Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, 217–242.

[19] M. Ram Murty and Kaneenika Sinha, *Effective equidistribution of eigenvalues of Hecke operators*, J. Number Theory **129** (2009), no. 3, 681–714.

[20] Phong Nguyen and Damien Stehlé, *Low-Dimensional Lattice Basis Reduction Revisited*, ACM Transactions on Algorithms **5**, Issue 4, Article No.: 46 (2009), https://doi.org/10.1145/1597036.1597050; Extended Abstract in Proceedings of ANTS-VI, Lecture Notes in Computer Science **3076** (2004), Springer-Verlag, 338–357.

[21] Arnold Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, Journal of Algebra **64**, Issue 2 (1980), 340–390, https://doi.org/10.1016/0021-8693(80)90151-9.

[22] Jean-Pierre Serre, *Répartition asymptotique des valeurs propres de l'opérateur de Hecke* T_p, J. Amer. Math. Soc. **10**, no. 1 (1997), 75–102, https://doi.org/10.1090/S0894-0347-97-00220-8.

[23] Peter W. Shor, *Quantum Money*, March 27th, 2020 virtual lecture at workshop on Lattices: New Cryptographic Capabilities, at Simons Institute for the Theory of Computing, https://simons.berkeley.edu/talks/quantum-money-based-lattices.

[24] Denis Simon, *Solving Quadratic Equations Using Reduced Unimodular Quadratic Forms*, in Math. of Comp **74** (2005), 1531–1543.

[25] John Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, in Quadratic and higher degree forms, Developments in Math. **31**, Springer, New York, 2013, 255–298.
[26] John Voight, Quaternion Algebras, Graduate Studies in Mathematics **288**, Springer International Publishing, 2021. https://math.dartmouth.edu/~jvoight/quat-book.pdf.
[27] Stephen Wiesner, *Conjugate coding*, ACM SIGACT News (1983), 78–88, https://doi.org/10.1145/1008908.1008920.
[28] Mark Zhandry, *Quantum Lightning Never Strikes the Same State Twice*, in Advances in Cryptology—EUROCRYPT 2019, Lect. Notes in Comp. Sci. **11478**, Springer, (2019), 408–438, https://doi.org/10.1007/978-3-030-17659-4_14, full version available at https://eprint.iacr.org/2017/1080.

Mathematics Department, UCSD, La Jolla, CA 92093
Email address: dakane@ucsd.edu

Mathematics Department, California State University, San Marcos, CA 92096
Email address: ssharif@csusm.edu

Mathematics Department, University of California, Irvine, CA 92697
Email address: asilverb@uci.edu