THEORY OF COMPUTING, Volume 9 (9), 2013, pp. 349–401
www.theoryofcomputing.org

Quantum Money from Hidden Subspaces

Scott Aaronson* Paul Christiano†

Received April 21, 2012; Revised September 17, 2012; Published March 11, 2013

Abstract: Forty years ago, Wiesner pointed out that quantum mechanics raises the striking possibility of money that cannot be counterfeited according to the laws of physics. We propose the first quantum money scheme that is

1. *public-key*—meaning that anyone can verify a banknote as genuine, not only the bank that printed it, and
2. *cryptographically secure*, under a "classical" hardness assumption that has nothing to do with quantum money.

Our scheme is based on *hidden subspaces*, encoded as the zero-sets of random multivariate polynomials. A main technical advance is to show that the "black-box" version of our scheme, where the polynomials are replaced by classical oracles, is *unconditionally* secure. Previously, such a result had only been known relative to a *quantum* oracle (and even there, the proof was never published).

Even in Wiesner's original setting—quantum money that can only be verified by the bank—we are able to use our techniques to patch a major security hole in Wiesner's scheme. We give the first private-key quantum money scheme that allows unlimited verifications and that remains unconditionally secure, even if the counterfeiter can interact adaptively with the bank.

*This material is based upon work supported by the National Science Foundation under Grant No. 0844626. Also supported by a DARPA YFA grant, an NSF STC grant, a TIBCO Chair, and a Sloan Fellowship.

†This work was done while the author was a student at MIT.

ACM Classification: F.1.2, E.3

AMS Classification: 81P68, 94A60

Key words and phrases: electronic cash, multivariate polynomials, quantum cryptography, quantum lower bounds

© 2013 Scott Aaronson and Paul Christiano
Licensed under a Creative Commons Attribution License (CC-BY) DOI: 10.4086/toc.2013.v009a009

Our money scheme is simpler than previous public-key quantum money schemes, including a knot-based scheme of Farhi et al. The verifier needs to perform only two tests, one in the standard basis and one in the Hadamard basis—matching the original intuition for quantum money, based on the existence of complementary observables.

Our security proofs use a new variant of Ambainis's quantum adversary method, and several other tools that might be of independent interest.

Contents

1 Introduction

"Information wants to be free"—this slogan expresses the idea that classical bits, unlike traditional economic goods, can be copied an unlimited number of times. The copyability of classical information is one of the foundations of the digital economy, but it is also a nuisance to governments, publishers, software companies, and others who wish to prevent copying. Today, essentially all electronic commerce involves a trusted third party, such as a credit card company, to mediate transactions. Without such a third party entering at *some* stage, it is impossible to prevent electronic cash from being counterfeited, regardless of what cryptographic assumptions one makes.[1]

Famously, though, quantum bits do *not* "want to be free" in the same sense that classical bits do: in many respects, they behave more like gold, oil, or other traditional economic goods. Indeed, the *No-Cloning Theorem*, which is an immediate consequence of the linearity of quantum mechanics, says that there is no physical procedure that takes as input an unknown[2] quantum pure state $|\psi\rangle$, and that produces as output two unentangled copies of $|\psi\rangle$, or even a close approximation thereof. The No-Cloning Theorem is closely related to the *uncertainty principle*, which says that there exist "complementary" properties of a quantum state (for example, its position and momentum) that cannot both be measured to unlimited accuracy.[3]

1.1 The history of quantum money

But can one actually *exploit* the No-Cloning Theorem to achieve classically-impossible cryptographic tasks? This question was first asked by Wiesner [42], in a remarkable paper written around 1970 (but only published in 1983) that arguably founded quantum information science. In that paper, Wiesner proposed a scheme for *quantum money* that would be physically impossible to clone. In Wiesner's scheme, each "banknote" would consist of a classical serial number s, together with a quantum state $|\psi_s\rangle$ consisting of n unentangled qubits, each one

$$|0\rangle, \quad |1\rangle, \quad \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \quad \text{or} \quad \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

with equal probability. The issuing bank would maintain a giant database, which stored a classical description of $|\psi_s\rangle$ for each serial number s. Whenever someone wanted to *verify* a banknote, he or she would take it back to the bank—whereupon the bank would use its knowledge of how $|\psi_s\rangle$ was prepared to measure each qubit in the appropriate basis, and check that it got the correct outcomes. On the other hand, it can be proved [33] that someone who did *not* know the appropriate bases could copy the banknote with success probability at most $(3/4)^n$.

Though historically revolutionary, Wiesner's money scheme suffered at least three drawbacks:

[1]The recent Bitcoin system is an interesting illustration of this principle: it gets rid of the centralized third party, but still uses a "third party" distributed over the community of Bitcoin users.

[2]The adjective "unknown" is needed because, if we knew a classical description of a procedure to *prepare* $|\psi\rangle$, then of course we could run that procedure multiple times to prepare multiple copies.

[3]Indeed, if we could copy $|\psi\rangle$, then we could violate the uncertainty principle by measuring one observable (such as position) on some copies, and a complementary observable (such as momentum) on other copies. Conversely, if we could measure all the properties of $|\psi\rangle$ to unlimited accuracy, then we could use the measurement results to create additional copies of $|\psi\rangle$.

(1) **The "Verifiability Problem":** The only entity that can verify a banknote is the bank that printed it.

(2) **The "Online Attack Problem":** A counterfeiter able to submit banknotes for verification, and get them back afterward, can easily break Wiesner's scheme ([30, 3]; see also Section 7).

(3) **The "Giant Database Problem":** The bank needs to maintain a database with an entry for every banknote in circulation.

In followup work in 1982, Bennett, Brassard, Breidbart, and Wiesner [15] (henceforth BBBW) at least showed how to eliminate the giant database problem: namely, by generating the state $|\psi_s\rangle = |\psi_{f_k(s)}\rangle$ using a *pseudorandom function* f_k, with key k known only by the bank. Unlike Wiesner's original scheme, the BBBW scheme is no longer *information-theoretically* secure: a counterfeiter can recover k given exponential computation time. On the other hand, a counterfeiter cannot break the scheme in polynomial time, unless it can *also* distinguish f_k from a random function.

These early ideas about quantum money inspired the field of *quantum cryptography* [14]. But strangely, the subject of quantum money itself lay dormant for more than two decades, even as interest in quantum computing exploded. However, the past few years have witnessed a "quantum money renaissance." Some recent work has offered partial solutions to the verifiability problem. For example, Mosca and Stebila [34] suggested that the bank use a *blind quantum computing* protocol to offload the verification of banknotes to local merchants, while Gavinsky [25] (see also followup work by Molina et al. [33] and Pastawski et al. [37]) proposed a variant of Wiesner's scheme that requires only *classical* communication between the merchant and bank.

However, most of the focus today is on a more ambitious goal: namely, creating what Aaronson [3] called *public-key quantum money*, or quantum money that *anyone* could authenticate, not just the bank that printed it. As with public-key cryptography in the 1970s, it is far from obvious *a priori* whether public-key quantum money is possible at all. Can a bank publish a description of a quantum circuit that lets people feasibly *recognize* a state $|\psi\rangle$, but does not let them feasibly prepare or even copy $|\psi\rangle$?

Aaronson [3] gave the first formal treatment of public-key quantum money, as well as related notions such as copy-protected quantum software. He proved that there exists a *quantum oracle* relative to which secure public-key quantum money is possible. Unfortunately, that result, though already involved, did not lead in any obvious way to an explicit (or "real-world") quantum money scheme.[4] He raised as an open problem whether secure public-key quantum money is possible relative to a *classical* oracle. In the same paper, Aaronson also proposed an explicit scheme, based on random stabilizer states, but could not offer any evidence for its security. And indeed, the scheme was broken about a year afterward by Lutomirski et al. [32], using an algorithm for finding planted cliques in random graphs due to Alon, Krivelevich, and Sudakov [8].

Recently, Farhi et al. [24] took a completely different approach to public-key quantum money. They proposed a quantum money scheme based on *knot theory*, where each banknote is a superposition over exponentially-many oriented link diagrams. Within a given banknote, all the link diagrams L have the

[4] Also, the proof of Aaronson's result never appeared—an inexcusable debt that this paper finally repays, with interest.

same Alexander polynomial $p(L)$ (a certain knot invariant).[5] This $p(L)$, together with a digital signature of $p(L)$, serves as the banknote's "classical serial number." Besides the unusual mathematics employed, the work of Farhi et al. [24] (building on [32]) also introduced an idea that will play a major role in our work. That idea is to construct public-key quantum money schemes by composing two "simpler" ingredients: first, objects that we call *mini-schemes*; and second, classical digital signature schemes.

The main disadvantage of the knot-based scheme, which it shares with every previous scheme, is that no one can say much about its security—other than that it has not yet been broken, and that various known counterfeiting strategies fail. Indeed, even characterizing *which quantum states Farhi et al.'s verification procedure accepts* remains a difficult open problem, on which progress seems likely to require major advances in knot theory! In other words, there might be states that look completely different from "legitimate banknotes," but are still accepted with high probability.

In followup work, Lutomirski [31] proposed an "abstract" version of the knot scheme, which gets rid of the link diagrams and Alexander polynomials, and simply uses a classical oracle to achieve the same purposes. Lutomirski raised the challenge of proving that this *oracle* scheme is secure—in which case, it would have yielded the first public-key quantum money scheme that was proven secure relative to a classical oracle. Unfortunately, proving the security of Lutomirski's scheme remains open, and seems hard.[6]

As alluded to earlier, there is already some research on ways to *break* quantum money schemes. Besides the papers by Lutomirski [30] and Lutomirski et al. [32] mentioned before, let us mention the beautiful work of Farhi et al. on *quantum state restoration* [23]. As we discuss in Section 7, quantum state restoration can be used to break many public-key quantum money schemes: roughly speaking, any scheme where the banknotes contain only limited entanglement, and where verification consists of a rank-1 projective measurement. This fact explains why our scheme, like the knot-based scheme of Farhi et al. [24], will require highly-entangled banknotes.

1.2 The challenge

Work over the past few years has revealed a surprising richness in the quantum money problem—both in the ideas that have been used to construct public-key quantum money schemes, *and* in the ideas that have been used to break them. Of course, this record also underscores the need for caution! To whatever extent we can, we ought to hold quantum money schemes to modern cryptographic standards, and not be satisfied with "we tried to break it and failed."

[5]Instead of knots, Farhi et al. [24] could also have used, say, superpositions over n-vertex *graphs* having the same eigenvalue spectrum. But in that case, their scheme would have been breakable, the reason being that the *graph isomorphism problem* is easy for random graphs. By contrast, it is not known how to solve *knot isomorphism* efficiently, even with a quantum computer and even for random knots.

[6]One way to understand the difficulty is that any security proof for Lutomirski's scheme would need to contain, as a special case, a quantum lower bound for the so-called *index erasure* problem [10]. In other words, any fast quantum algorithm for index erasure would imply a break of Lutomirski's scheme.

At present, the simplest known proof of a quantum lower bound for index erasure is via a reduction from Aaronson's quantum lower bound for the *collision problem* [1] (cf. [6]). The latter is proved using the polynomial method of Beals et al. [12]. In this work, by contrast, we will only manage to prove the security of *our* oracle scheme using a specially-designed variant of Ambainis's quantum adversary method [9]. There *is* a recent lower bound for the index erasure problem using the adversary method [10], but it is quite involved.

It is easy to see that, if public-key quantum money is possible, then it must rely on *some* computational assumption, in addition to the No-Cloning Theorem.[7] The best case would be to show that secure, public-key quantum money is possible, *if* (for example) there exist one-way functions resistant to quantum attack. Unfortunately, we seem a long way from showing anything of the kind. The basic problem is that *uncloneability* is a novel cryptographic requirement: something that would not even make sense in a classical context. Indeed, work by Farhi et al. [23] and Aaronson [3] has shown that it is sometimes possible to copy quantum banknotes, via attacks that do not even *measure* the banknotes in an attempt to learn a classical secret! Rather, these attacks simply perform some unitary transformation on a legitimate banknote $|\$\rangle$ together with an ancilla $|0\rangle$, the end result of which is to produce $|\$\rangle^{\otimes 2}$. Given such a strange attack, how can one deduce the failure of any "standard" cryptographic assumption?

Yet despite the novelty of the quantum money problem—or perhaps because of it—it seems reasonable to want *some* non-tautological evidence that a public-key quantum money scheme is secure. A minimal wish-list might include:

(1) Security under *some* plausible assumption, of a sort cryptographers know how to evaluate. Such an assumption should talk only about computing a classical output from a classical input; it should have nothing to do with cloning of quantum states.

(2) A proof that the money scheme is secure against *black-box counterfeiters*: those that do not exploit the structure of some cryptographic function f used in verifying the banknotes.

(3) A "simple" verification process, which accepts all valid banknotes $|\$\rangle$ with probability 1, and rejects all banknotes that are far from $|\$\rangle$.

1.3 Our results

Our main contribution is a new public-key quantum money scheme, which achieves all three items in the wish-list above, and which is the first to achieve (1) or (2). Regardless of whether our particular scheme stands or falls, we introduce at least four techniques that should be useful for the design and analysis of *any* public-key quantum money scheme. These are:

- The "inner-product adversary method," a new variant of Ambainis's quantum adversary method [9] that can be used to rule out black-box counterfeiting strategies.
- A formal proof that full-fledged quantum money schemes can be constructed out of two simpler ingredients: (a) objects that we call *mini-schemes*, and (b) conventional digital signature schemes secure against quantum attack. (Note that this construction itself, *sans* the analysis, was introduced in earlier work on quantum money, by Lutomirski et al. [32] and Farhi et al. [24].)
- A method to *amplify* weak counterfeiters into strong ones, so that one only needs to rule out the latter to show security.

[7] This is because a counterfeiter with unlimited time could simply search for a state $|\psi\rangle$ that the (publicly-known) verification procedure accepted.

- A new connection between (a) the security of quantum money schemes, and (b) the security of conventional cryptosystems against attacks that succeed with exponentially-small probabilities.

A second contribution is to construct the first *private*-key quantum money schemes that remain *unconditionally* secure, even if the counterfeiter can interact adaptively with the bank. This gives the first solution to the "online attack problem," a major security hole in the Wiesner [42] and BBBW [15] schemes pointed out by Lutomirski [30] and Aaronson [3]. These private-key schemes are direct adaptations of our public-key scheme.

In more detail, our quantum money scheme is based on *hidden subspaces* of the vector space $\mathbb{F}_2^n$. Each of our money states is a uniform superposition of the vectors in a random $n/2$-dimensional subspace $A \leq \mathbb{F}_2^n$. We denote this superposition by $|A\rangle$. Crucially, we can recognize the state $|A\rangle$ using only membership oracles for A and for its dual subspace $A^{\perp}$. To do so, we apply the membership oracle for A, then a Fourier transform, then the membership oracle for $A^{\perp}$, and then a second Fourier transform to restore the original state. We prove that this operation computes a rank-1 projection onto $|A\rangle$.

Underlying the security of our money schemes is the assertion that the states $|A\rangle$ are difficult to clone, even given membership oracles for A and $A^{\perp}$. Or more concretely: *any quantum algorithm that maps $|A\rangle$ to $|A\rangle^{\otimes 2}$ must make $2^{\Omega(n)}$ queries to the $A, A^{\perp}$ oracles.*

In order to prove this statement, we introduce a new method for proving lower bounds on quantum query complexity, which we call the *inner-product adversary method*. This technique considers a single counterfeiting algorithm being run in parallel to clone two distinct states $|A\rangle$ and $|A'\rangle$, with each having access to the membership oracles for $A, A^{\perp}$ or $A', A'^{\perp}$, as appropriate. To measure how much progress the algorithm has made, we consider the inner product between the states produced by the parallel executions: because $\langle A|^{\otimes 2} |A'\rangle^{\otimes 2} < \langle A|A'\rangle$ for many pairs of subspaces A, A', in order to succeed a counterfeiter will have to reduce this inner product substantially. We prove that when averaged over a suitable distribution of pairs A, A', the *expected inner product* between the two states produced by the counterfeiter cannot decrease too much with a single query to the membership oracles. We conclude that in order to produce $|A\rangle^{\otimes 2}$ given $|A\rangle$ and membership oracles for $A, A^{\perp}$, a counterfeiter must use exponentially many queries.

Having ruled out the possibility of nearly perfect cloning, we introduce a new amplification protocol, which allows us to transform a counterfeiter who succeeds with $\Omega(1/\mathrm{poly}(n))$ success probability into a counterfeiter who succeeds with probability arbitrarily close to 1. This technique is based on combining standard Grover search with a monotonic state amplification protocol of Tulsi, Grover, and Patel [41], to obtain monotonic convergence with the quadratic speedup of Grover search.[8] Combining this amplification with the inner-product adversary method, and applying a random linear transformation to convert the counterfeiter's worst case to its average case, we conclude that no counterfeiting algorithm can succeed with any non-negligible probability on a non-negligible fraction of states $|A\rangle$.

Using these results, how do we produce a secure quantum money scheme? We now need to step back, and discuss some general constructions that have nothing to do with hidden subspaces in particular. Before constructing full-fledged quantum money schemes, we find it useful—following [32, 24]—to construct simpler objects called *quantum money mini-schemes*, in which the bank issues only a single money state and maintains no secret information. Formally, a mini-scheme is a protocol Bank for outputting pairs

[8] Although the "quadratic speedup" part is not strictly necessary for us, it improves our lower bound on the number of queries the counterfeiter needs to make—to the tight one, in fact—and might be of independent interest.

(s, ρ_s) and a verification procedure Ver_s for identifying ρ_s. We say a mini-scheme is *complete* if the state ρ_s passes the verification Ver_s with high probability, and we say the scheme is *secure* if furthermore no counterfeiter can take a single state ρ_s, and produce two (possibly-entangled) states ρ_1 and ρ_2 which simultaneously pass the verification procedure with non-negligible probability.

In the case of hidden subspace money, for example, we can use our uncloneability result to produce a secure mini-scheme relative to a classical oracle. The algorithm Bank queries the classical oracle to obtain a serial number s and the description of a subspace A. Using this description, it prepares $|A\rangle$ and publishes $(s, |A\rangle)$. The verification procedure uses the serial number s as an index into another classical oracle, which allows it to test membership in A and $A^{\perp}$. We prove that the uncloneability of the states $|A\rangle$ implies that this mini-scheme is secure.

Using a construction introduced by Lutomirski et al. [32] and Farhi et al. [24], we also show that, given any mini-scheme $\mathcal{M}$, one can obtain a full-fledged quantum money scheme by combining $\mathcal{M}$ with any (classical) digital signature scheme secure against quantum attacks. In the construction of [32, 24], the issuing bank first uses the mini-scheme to produce a pair (s, ρ_s); then it digitally signs the serial number s and distributes $(s, \rho_s, \mathsf{Sign}(s))$ as its banknote. Our contribution is to prove rigorously that, *if* a counterfeiter can break the money scheme, then it must have been able to break either the underlying mini-scheme or else the signature scheme.

By combining this reduction with our mini-scheme, we are able to obtain a "black-box" public key quantum money scheme relative to a classical oracle, which is unconditionally secure:

Theorem (Security of Hidden Subspace Money)**.** Relative to some (classical) oracle A, there exists a secure public-key quantum money scheme.

More precisely, there is an algorithm KeyGen^A which outputs pairs $(k_{\text{private}}, k_{\text{public}})$ with security parameter n; an algorithm $\mathsf{Bank}^A(k_{\text{private}})$ which generates a "quantum banknote" $|\$\rangle$; and a verification algorithm $\mathsf{Ver}^A(k_{\text{public}}, |\$\rangle)$ which tests the authenticity of a purported banknote. These algorithms are polynomial-time and have the following properties:

Completeness: If $(k_{\text{private}}, k_{\text{public}})$ is produced by KeyGen^A, then $\mathsf{Ver}^A(k_{\text{public}}, \mathsf{Bank}^A(k_{\text{private}}))$ accepts with certainty.

Soundness: Suppose a would-be polynomial-time counterfeiter with access to A and k_{public} is given q valid banknotes. If this counterfeiter outputs any number of (possibly-entangled) quantum states, there is at most a $1/\exp(n)$ probability that Ver^A will accept more than q of them.

By adapting these ideas to the private-key setting, we are also able to provide the first *private*-key quantum money scheme that is unconditionally secure, even if the counterfeiter is able to interact adaptively with the bank. This patches a security hole in Wiesner's original scheme which was observed in [30, 3], but which has not previously been addressed in a provably-secure way.

Finally, we provide a candidate cryptographic protocol for obfuscating the indicator functions of subspaces $A \leq \mathbb{F}_2^n$. In order to obfuscate a membership oracle for A, we provide a random system of polynomials $p_1, \ldots, p_m$ that vanish on A. Membership in A can be tested by evaluating the p_i, but given only the p_i, we conjecture that it is difficult to recover A. Combining this protocol with the black-box money scheme, we obtain an *explicit* quantum money scheme. This scheme is also the first public-key quantum money scheme whose security can be based on a plausible "classical" cryptographic assumption. Here is the assumption:

Conjecture (*). Suppose A is a uniformly-random $n/2$-dimensional subspace of $\mathbb{F}_2^n$, and that $\{p_i\}_{1\le i\le 2n}$, $\{q_i\}_{1\le i\le 2n}$ are systems of degree-d polynomials from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, which vanish on A and $A^\perp$ respectively but are otherwise uniformly-random. Then for large enough constant d, there is no polynomial-time quantum algorithm that takes as input descriptions of the p_i and the q_i, and outputs a basis for A with success probability $\Omega\left(2^{-n/2}\right)$.

Note that we can trivially guess a *single* nonzero A element with success probability $2^{-n/2}$, but guessing a whole *basis* for A would succeed with probability only $2^{-\Omega(n^2)}$. Conjecture (*) asserts that it is harder to find many elements of A than to find just one element.

The following theorem says that, *if* a counterfeiter could break our quantum money scheme, then with nontrivial success probability, it could *also* recover a description of A from the p_i and the q_i alone—even without having access to a bank that provides a valid money state $|A\rangle$.

Theorem. Assuming Conjecture (*), there exists a public-key quantum money scheme with perfect completeness and $1/\exp(n)$ soundness error. That is, the verifier always accepts valid banknotes, and a would-be counterfeiter succeeds only with $1/\exp(n)$ probability.[9]

The problem of recovering a subspace A, given a system of equations that vanish on A, is closely related to *algebraic cryptanalysis*, and in particular to the so-called *polynomial isomorphism problem*. In the latter problem, we are given as input two polynomials $p,q:\mathbb{F}^n\to\mathbb{F}$ related by an unknown linear change of basis L; the challenge is to find L. When $\deg(p)=\deg(q)=3$, the best known algorithms for the polynomial isomorphism problem require exponential time [38, 26, 18]. An attacker *might* be able to use known techniques to effectively reduce the degree of the polynomials in our scheme by 1, at the expense of an exponentially reduced success probability [18]. Provided the degree is at least 4, however, recovering A seems to be well beyond existing techniques.

1.4 Motivation

Unlike the closely-related task of *quantum key distribution* [14] (which is already practical), quantum money currently seems to be a long way off. The basic difficulty is how to maintain the *coherence* of a quantum money state for an appreciable length of time. *All* money eventually loses its value unless it is spent, but money that decohered on a scale of microseconds would be an extreme example!

So one might wonder: why develop rigorous foundations for a cryptographic functionality that seems so far from being practical? One answer is that, just as quantum key distribution uses many of the same ideas as private-key quantum money, but without requiring long-lasting coherence, so it is not hard to imagine protocols that would use many of the same ideas as *public*-key quantum money without requiring long-lasting coherence. Indeed, depending on the problem, rapid decoherence might be a *feature* rather than a bug!

As one example, public-key quantum money that decohered quickly could be used to create **non-interactive uncloneable signatures**. These are n-qubit quantum states $|\psi\rangle$ that an agent can efficiently

[9]This theorem remains true even if the statement of Conjecture (*) is weakened by adding random noise to the p_i and the q_i, so that only a constant fraction of them vanish on A or $A^\perp$. The presence of noise interferes substantially with known techniques for solving systems of equations, though an attacker who was able to recover A from a *single* polynomial would of course not be hindered by such noise.

prepare using a private key, then freely hand out to passersby. By feeding $|\psi\rangle$, together with the agent's *public* key, into suitable measuring equipment, anyone can verify on the spot that the agent is who she says she is and not an impostor. Compared with *classical* identification protocols, the novel feature here is that the agent does not need to respond to a *challenge*—for example, digitally signing a random string—but can instead just hand out a fixed $|\psi\rangle$ non-interactively. Furthermore, because $|\psi\rangle$ decoheres in a matter of seconds, and recovering a classical *description* of $|\psi\rangle$ from measurements on it is computationally intractable, someone who is given $|\psi\rangle$ cannot use it later to impersonate the agent.

Of course, if an attacker managed to solve the technological problem of keeping $|\psi\rangle$ coherent for very long times, then he could break this system, by collecting one or more copies of $|\psi\rangle$ that an agent had handed out, and using them to impersonate the agent. But in that case, whatever method the attacker was using to keep the states coherent could *also*—once discovered—be used to create a secure public-key quantum money scheme!

However, we believe the "real" reason to study quantum money is basically the same as the "real" reason to study quantum computing as a whole—or for that matter, to study the many interesting aspects of *classical* cryptography that are equally far from application. As theoretical computer scientists, we are in the business of mapping out the inherent capabilities and limits of information processing.

In our case, what quantum money provides is a near-ideal playground for understanding the implications of the uncertainty principle and the No-Cloning Theorem. In the early days of quantum mechanics, Bohr [16] and others argued that the uncertainty principle requires us to change our conception of science itself—their basic argument being that, in physics, predictions are only ever as good as our knowledge of a system's initial state $|\psi\rangle$, but the uncertainty principle might mean that the initial state is unknowable even with arbitrarily-precise measurements.

But does this argument have any "teeth"? In other words: among the properties of a quantum state $|\psi\rangle$ that make the state impossible to learn precisely or to duplicate, can any of those properties ever *matter empirically*? To us, quantum money is interesting precisely because it gives one of the clearest examples where the answer to that question is yes.

2 Preliminaries

To begin, we fix some notation. Let $[N] = \{1,\ldots,N\}$. We call a function $\delta(n)$ *negligible* if $\delta(n) = o(1/p(n))$ for every polynomial p. Given a subspace S of a vector space V, let $S^\perp$ be the *orthogonal complement* of S: that is, the set of $y \in V$ such that $x \cdot y = 0$ for all $x \in S$. It is not hard to show that $S^\perp$ is also a subspace of V, that $\left(S^\perp\right)^\perp = S$, and that these properties hold even if $\cdot$ is "merely" a dot product rather than an inner product. As a word of warning, this paper will use the same notation $S^\perp$ in two very different contexts:

- When $V = \mathbb{C}^{2^n}$, the orthogonal complement $S^\perp$ of, e. g., the subspace $S \leq V$ spanned by a single computational basis state $|x\rangle$, has $2^n - 1$ dimensions and is spanned by all basis states $|y\rangle$ such that $y \neq x$.
- When $V = \mathbb{F}_2^n$, the orthogonal complement $S^\perp$ of, e. g., the subspace $S \leq V$ spanned by a single string $x = x_1 \ldots x_n$, has $n-1$ dimensions and consists of all strings $y = y_1 \ldots y_n$ such that $x_1 y_1 + \cdots + x_n y_n \equiv 0 \pmod 2$.

By a *classical oracle*, we will mean a unitary transformation of the form $|x\rangle \to (-1)^{f(x)} |x\rangle$, for some Boolean function $f : \{0,1\}^* \to \{0,1\}$. Note that, unless specified otherwise, even a classical oracle can be queried in quantum superposition. A *quantum oracle*, by contrast, is an arbitrary n-qubit unitary transformation U (or rather, a collection of such transformations U, one for each n) that a quantum algorithm can apply in a black-box fashion. Quantum oracles were defined and studied by Aaronson and Kuperberg [5].

2.1 Cryptography

Before we construct quantum money schemes, it will be helpful to have some "conventional" cryptographic primitives in our toolbox. Foremost among these is a *digital signature scheme secure against quantum chosen-message attacks*. We now define digital signature schemes—both for completeness, and to fix the quantum attack model that is relevant for us.

Definition 2.1 (Digital Signature Schemes)**.** A (classical, public-key) **digital signature scheme** $\mathcal{D}$ consists of three probabilistic polynomial-time classical algorithms:

- KeyGen, which takes as input a security parameter 0^n, and generates a **key pair** $(k_{\text{private}}, k_{\text{public}})$.
- Sign, which takes as input k_{private} and a message x, and generates a **signature** $\mathsf{Sign}(k_{\text{private}}, x)$.[10]
- Ver, which takes as input k_{public}, a message x, and a claimed signature w, and either accepts or rejects.

We say $\mathcal{D}$ has **completeness error** ε if $\mathsf{Ver}(k_{\text{public}}, x, \mathsf{Sign}(x, k_{\text{private}}))$ accepts with probability at least $1-\varepsilon$ for all messages x and key pairs $(k_{\text{private}}, k_{\text{public}})$. Here the probability is over the behavior of Ver and Sign.

Let C (the **counterfeiter**) be a quantum circuit of size $\operatorname{poly}(n)$ that takes k_{public} as input[11] and does the following:

(1) Probabilistically generates a classical list of messages $x_1, \ldots, x_m$, and submits them to a **signing oracle** $\mathcal{O}$.

(2) Gets back independently-generated signatures $w_1, \ldots, w_m$, where $w_i := \mathsf{Sign}(k_{\text{private}}, x_i)$.

(3) Outputs a pair (x, w).

We say C **succeeds** if $x \notin \{x_1, \ldots, x_m\}$ and $\mathsf{Ver}(k_{\text{public}}, x, w)$ accepts. We say $\mathcal{D}$ has **soundness error** δ if every counterfeiter C succeeds with probability at most δ. Here the probability is over the key pair $(k_{\text{private}}, k_{\text{public}})$ and the behavior of C, Sign, and Ver.

We call $\mathcal{D}$ **secure against nonadaptive quantum chosen-message attacks** if it has completeness error $\leq 1/3$ and negligible soundness error.

[10] We indulge in slight abuse of notation, since if Sign is randomized then the signature need not be a function of k_{private} and x.

[11] Actually, for our security proofs, it suffices to consider a weaker attack model, in which C only receives k_{public} at the same time as it receives $w_1, \ldots, w_m$. This model was called "existential unforgeability under *static* chosen-message attacks" by Cash et al. [20]. We thank an anonymous reviewer for this observation.

Intuitively, we call a signature scheme "secure" if no *quantum* counterfeiter with *nonadaptive, classical* access to a signing oracle $\mathcal{O}$ can forge a signature for any message that it did not submit to $\mathcal{O}$. Depending on the application, one might want to generalize Definition 2.1 in various ways: for example, by giving the counterfeiter *adaptive* or *quantum* access to $\mathcal{O}$, or by letting KeyGen, Sign, and Ver be quantum algorithms themselves. For this paper, however, Definition 2.1 provides all we need.

Do signature schemes secure against quantum attack exist? Naturally, signature schemes based on RSA or other number-theoretic problems can all be broken by a quantum computer. However, building on earlier work by Naor and Yung [35] (among many others), Rompel [40] showed that a secure public-key signature scheme can be constructed from *any* one-way function—not necessarily a trapdoor function. Furthermore, Rompel's security reduction, from breaking the signature scheme to inverting the one-way function, is *black-box*: in particular, nothing in it depends on the assumption that the adversary is classical rather than quantum. We therefore get the following consequence:

Theorem 2.2 (Quantum-Secure Signature Schemes [40])**.** *If there exists a (classical) one-way function f secure against quantum attack, then there also exists a digital signature scheme secure against quantum chosen-message attacks.*

Recently, Boneh et al. [17] proved several results similar to Theorem 2.2, and they needed nontrivial work to do so. However, a crucial difference is that Boneh et al. were (justifiably) concerned with quantum adversaries who can make *quantum* queries to the signing oracle $\mathcal{O}$. By contrast, as mentioned earlier, for our application it suffices to consider adversaries who query $\mathcal{O}$ *classically*—and in that case, the standard security reductions go through essentially without change.

Let us state another consequence of Theorem 2.2, which will be useful for our oracle construction in Section 5.

Theorem 2.3 (Relativized Quantum-Secure Signatures)**.** *Relative to a suitable oracle A, there exists a digital signature scheme secure against quantum chosen-message attacks.*

Proof sketch. It is easy to give an oracle $A : \{0,1\}^* \to \{0,1\}$ relative to which there exists a one-way function $f_n : \{0,1\}^n \to \{0,1\}^{p(n)}$ secure against quantum adversaries. Indeed, we can let A be a *random* oracle, and then define

$$f_n(x) := A(x,1)\ldots A(x,p(n))$$

directly in terms of A. Assume $p(n) \geq n$. Then the lower bound on the quantum query complexity of function inversion, proved by Bennett et al. [13] and Ambainis [9], straightforwardly implies that any quantum algorithm to invert f_n, with success probability $\varepsilon > 0$, must make $\Omega(2^{n/2}\sqrt{\varepsilon})$ quantum queries to A.

Now, the security reduction of Rompel [40] is not only black-box but *relativizing*: that is, it goes through if all legitimate and malicious parties have access to the same oracle A. So by Theorem 2.2, starting from $\{f_n\}$ one can construct a digital signature scheme relative to the same oracle A, which is secure against quantum chosen-message attacks. □

2.2 Quantum information

Let us collect a few facts about quantum pure and mixed states that are used in the paper. We assume basic familiarity with the formalism of bras, kets, density matrices, etc.; see Nielsen and Chuang [36] for a good overview.

Given two mixed states ρ and σ, their *trace distance* is defined as

$$D(\rho,\sigma) := \frac{1}{2}\sum_{i=1}^{N} |\lambda_i| ,$$

where $\lambda_1,\dots,\lambda_N$ are the eigenvalues of $\rho-\sigma$. Trace distance is a metric and satisfies $0 \le D(\rho,\sigma) \le 1$. Also, the *fidelity* $0 \le F(\rho,\sigma) \le 1$ is defined, in this paper, as the maximum of $|\langle\psi|\varphi\rangle|$ over all purifications $|\psi\rangle$ of ρ and $|\varphi\rangle$ of σ.[12] By extension, given a subspace S, we let $F(\rho,S)$ be the maximum of $|\langle\psi|\varphi\rangle|$ over all purifications $|\psi\rangle$ of ρ and all unit vectors $|\varphi\rangle \in S$. Trace distance and fidelity are related as follows [36]:

Proposition 2.4. *For all mixed states ρ,σ,*

$$D(\rho,\sigma) \le \sqrt{1-F(\rho,\sigma)^2},$$

with equality if ρ or σ is pure.

While fidelity is *not* a metric, it does satisfy the following inequality, which will be helpful in Section 5.

Lemma 2.5 ("Triangle Inequality" for Fidelity)**.** *Suppose $\langle\psi|\rho|\psi\rangle \ge 1-\varepsilon$ and $\langle\varphi|\sigma|\varphi\rangle \ge 1-\varepsilon$. Then $F(\rho,\sigma) \le |\langle\psi|\varphi\rangle| + 2\varepsilon^{1/4}$.*

Proof. By Proposition 2.4,

$$D(\rho,|\psi\rangle) \le \sqrt{1-\langle\psi|\rho|\psi\rangle} \le \sqrt{\varepsilon},$$

and likewise $D(\sigma,|\varphi\rangle) \le \sqrt{\varepsilon}$. Thus, since trace distance satisfies the triangle inequality,

$$\begin{aligned} D(\rho,\sigma) &\ge D(|\psi\rangle,|\varphi\rangle) - D(\rho,|\psi\rangle) - D(\sigma,|\varphi\rangle) \\ &\ge \sqrt{1-|\langle\psi|\varphi\rangle|^2} - 2\sqrt{\varepsilon}. \end{aligned}$$

Then

$$\begin{aligned} F(\rho,\sigma) &\le \sqrt{1-D(\rho,\sigma)^2} \\ &\le \sqrt{1-\left(\sqrt{1-|\langle\psi|\varphi\rangle|^2}-2\sqrt{\varepsilon}\right)^2} \\ &\le \sqrt{|\langle\psi|\varphi\rangle|^2+4\sqrt{\varepsilon}} \\ &\le |\langle\psi|\varphi\rangle| + 2\varepsilon^{1/4}. \end{aligned}$$

□

[12] Some authors instead define "fidelity" as the maximum of $|\langle\psi|\varphi\rangle|^2$.

Finally, the following lemma of Aaronson [2] will imply that, as long as a quantum money scheme has small *completeness error* (i.e., small probability of rejecting a valid banknote), the banknotes can be reused many times.

Lemma 2.6 ("Almost As Good As New Lemma" [2]). *Suppose a measurement on a mixed state ρ yields a particular outcome with probability $1-\varepsilon$. Then after the measurement, one can recover a state $\widetilde{\rho}$ such that $\|\widetilde{\rho}-\rho\|_{\mathrm{tr}} \leq \sqrt{\varepsilon}$.*

2.3 Quantum search

In our security proof for quantum money, an important step will be to *amplify* a counterfeiter who copies a banknote \$ with any non-negligible fidelity to a counterfeiter who copies \$ almost perfectly. Taking the contrapositive, this will imply that to rule out the former sort of counterfeiter, it suffices to rule out the latter.

In this section, we first review two variants of Grover's search algorithm [27] that are useful for amplifying the fidelity of quantum states. We then introduce a variant that combines the advantages of both.

Assume we are given a pure initial state $|\mathrm{Init}\rangle$, in some Hilbert space $\mathcal{H}$. Our goal is to map $|\mathrm{Init}\rangle$ to a final state $|\Psi\rangle$ that lies in (or close to) a "good subspace" $G \leq \mathcal{H}$. We have oracle access to two unitary transformations:

- U_{Init}, which maps $|\mathrm{Init}\rangle$ to $-|\mathrm{Init}\rangle$, and acts as the identity on all $|v\rangle$ orthogonal to $|\mathrm{Init}\rangle$.
- U_G, which maps $|v\rangle$ to $-|v\rangle$ for all $|v\rangle \in G$, and acts as the identity on all $|v\rangle$ orthogonal to G.

We are promised that the fidelity of the initial state with G,

$$F\left(|\mathrm{Init}\rangle, G\right) = \max_{|\psi\rangle \in G} \langle \mathrm{Init} | \psi \rangle ,$$

is at least some $\varepsilon > 0$.

In this scenario, *provided $F\left(|\mathrm{Init}\rangle, G\right)$ is known*, the amplitude amplification framework of Brassard, Høyer, Mosca, and Tapp [19] lets us prepare a state close to G using only $\Theta(1/\varepsilon)$ iterations:

Lemma 2.7 (Amplitude Amplification [19]). *Write $|\mathrm{Init}\rangle$ as $\sin\theta\,|\mathrm{Good}\rangle + \cos\theta\,|\mathrm{Bad}\rangle$, where $|\mathrm{Good}\rangle$ is the unit vector formed by projecting $|\mathrm{Init}\rangle$ onto G, and $|\mathrm{Bad}\rangle$ is orthogonal to $|\mathrm{Good}\rangle$. Then by using $O(T)$ oracle calls to U_{Init} and U_G, we can prepare the state*

$$|\Phi_T\rangle := \sin\left[(2T+1)\,\theta\right]|\mathrm{Good}\rangle + \cos\left[(2T+1)\,\theta\right]|\mathrm{Bad}\rangle .$$

Note that Grover's algorithm is simply a special case of Lemma 2.7, where $|\mathrm{Init}\rangle$ is the uniform superposition over N basis states $|1\rangle, \ldots, |N\rangle$, and G is the subspace spanned by "marked" states.

However, Lemma 2.7 has an annoying drawback, which it shares with ordinary Grover search. Namely, the algorithm does *not* converge monotonically toward the target subspace G, but could instead "wildly overshoot it," cycling around the 2-dimensional subspace spanned by $|\mathrm{Bad}\rangle$ and $|\mathrm{Good}\rangle$. If we know the fidelity $F(|\mathrm{Init}\rangle, G)$ in advance (rather than just a lower bound on the fidelity), *or* if we can prepare new copies of $|\text{Init}\rangle$ "free of charge" in case of failure, then this overshooting is not a serious problem. Alas, neither of those conditions will hold in our application.

Fortunately, for independent reasons, in 2005 Tulsi, Grover, and Patel [41] introduced a new quantum search algorithm that *does* guarantee monotonic convergence toward G, by alternating unitary transformations with measurements. (Their algorithm was later simplified and improved by Chakraborty, Radhakrishnan, and Raghunathan [21].)

Lemma 2.8 (Fixed-Point Quantum Search [41, 21])**.** *By using T oracle calls to U_{Init} and U_G, we can prepare a state $|\Psi\rangle$ such that $F(|\Psi\rangle, G) \geq 1 - \exp(-T\varepsilon^2)$.*

Rearranging, Lemma 2.8 lets us prepare a state $|\Psi\rangle$ such that $F(|\Psi\rangle, G) \geq 1 - \delta$ using

$$T = O\left(\frac{1}{\varepsilon^2} \log \frac{1}{\delta}\right)$$

iterations. On the positive side, the dependence on $1/\delta$ in this bound is logarithmic: we get not only monotonic convergence toward G, but *exponentially-fast* convergence. On the negative side, notice that the dependence on ε has worsened from $1/\varepsilon$ to $1/\varepsilon^2$—negating the quadratic speedup that was the original point of quantum search!

In the rest of this section, we give a "hybrid" quantum search algorithm that combines the advantages of Lemmas 2.7 and 2.8—i.e., it converges monotonically toward the target subspace G (rather than "overshooting" G), but *also* achieves a quadratic speedup. In the context of our security proof for quantum money, this hybrid algorithm will lead to a quadratically-better (and in fact, tight) lower bound on the number of queries that a counterfeiter needs to make, compared to what we would get from using Lemma 2.8 alone. While this quadratic improvement is perhaps only of moderate interest, we include the algorithm in the hope that it will find other applications.

We first give a technical lemma needed to analyze our algorithm.

Lemma 2.9. *For all L, β, η, γ, there are at most $(L/\beta + 1)(2\eta + 1)$ integers $T \in \{0, \ldots, L\}$ such that $|T - (\beta n + \gamma)| < \eta$ for some integer n.*

Proof. The real interval $[0, L]$ can intersect at most $L/\beta + 1$ intervals $(\beta n + \gamma - \eta, \beta n + \gamma + \eta)$, and each such interval can contain at most $2\eta + 1$ integer points. □

We now give our hybrid of Lemmas 2.7 and 2.8.

Theorem 2.10 (Faster Fixed-Point Search)**.** *Let $\delta \geq 2\varepsilon$. Then by using*

$$O\left(\frac{\log 1/\delta}{\varepsilon \delta^2}\right)$$

oracle calls to U_{Init} and U_G, we can prepare a state ρ such that $F(\rho, G) \geq 1 - \delta$.

Proof. Let $\xi := \arcsin \varepsilon$; note that $\varepsilon \leq \xi \leq \frac{\pi}{2}\varepsilon$. Also let $L := \lceil 100/\xi \rceil$ and $R := (25/\delta^2)(2 + \log(1/\delta))$. Then the algorithm is as follows:

(1) Choose an integer $T \in \{0, \ldots, L\}$ uniformly at random.

(2) Apply T iterations of amplitude amplification with $|\text{Init}\rangle$ as the initial state and G as the target subspace (as in Lemma 2.7), to obtain a state $|\Phi_T\rangle$.

(3) Apply R iterations of fixed-point quantum search with $|\Phi_T\rangle$ as the initial state and G as the target subspace (as in Lemma 2.8), to obtain a state $|\Psi_T\rangle$.

The final output of the above algorithm is

$$\rho = \operatorname*{E}_{T \in \{0,\ldots,L\}} \left[|\Psi_T\rangle \langle \Psi_T| \right].$$

Also, the total number of oracle calls to U_{Init} and U_G is

$$O(TR) = O\left(\frac{\log 1/\delta}{\varepsilon \delta^2} \right).$$

(The reason this number scales like TR rather than $T+R$ is that, in step (3), each time we reflect about the initial state $|\Phi_T\rangle$ we need to rerun step (2). Thus, we need $\Theta(T)$ oracle calls within each of the R iterations.)

By Lemma 2.7, after step (2) we have a state $|\Phi_T\rangle$ such that

$$F\left(|\Phi_T\rangle, G\right) = \left| \langle \Phi_T | \text{Good} \rangle \right| = \left| \sin\left[(2T+1)\xi \right] \right|.$$

So for any $\alpha \in (0,1)$,

$$\begin{aligned}
\Pr_{T \in \{0,\ldots,L\}} \left[F(|\Phi_T\rangle, G) < \alpha \right] &= \Pr_{T \in \{0,\ldots,L\}} \left[|\sin\left[(2T+1)\xi\right]| < \alpha \right] \\
&= \Pr_{T \in \{0,\ldots,L\}} \left[\exists n \in \mathbb{Z} : |(2T+1)\xi - \pi n| < \arcsin\alpha \right] \\
&\leq \frac{\left(\frac{L}{\pi/2\xi} + 1 \right)\left(\frac{\arcsin\alpha}{\xi} + 1 \right)}{L+1} \\
&\leq \frac{2}{\pi}\arcsin\alpha + \frac{2\xi}{\pi} + \frac{\arcsin\alpha}{100} + \frac{\xi}{100} \\
&\leq 1.02(\alpha + \varepsilon),
\end{aligned}$$

where the third line uses Lemma 2.9.

Now assume $F(|\Phi_T\rangle, G) \geq \alpha$. Then by Lemma 2.8, after step (3) we have a state $|\Psi_T\rangle$ such that

$$F(|\Phi_T\rangle, G) \geq 1 - \exp\left(-R\alpha^2\right).$$

Let us now make the choice $\alpha := \delta/5$. Then by the union bound, the "average" output $\rho = \operatorname{E}_T\left[|\Psi_T\rangle\langle\Psi_T|\right]$ satisfies

$$\begin{aligned}
1 - F(\rho, G) &\leq 1.02(\alpha+\varepsilon) + \exp\left(-R\alpha^2\right) \\
&\leq 0.204\delta + 0.51\delta + \exp\left(-\frac{R\delta^2}{25} \right) \\
&< \delta. \qquad \square
\end{aligned}$$

Note that our hybrid loses the property of *exponentially-fast* convergence toward the target subspace G, but that property will not be important for us anyway. We leave as an open problem whether there exists a hybrid algorithm with exponentially-fast convergence.

3 Formalizing quantum money

In this section, we first give a formal cryptographic definition of *public-key quantum money schemes*. Our definition is similar to that of Aaronson [3]. However, following [32, 24], we next define the notion of a *quantum money mini-scheme*, which is easier to construct and analyze than a full-blown quantum money scheme. A mini-scheme is basically a quantum money scheme where each banknote includes a classical serial number; where the only security requirement is that producing a second banknote with *the same serial number* is intractable; and where there is no public or private key (since given the lax security requirement, there is no need for one). We then prove two general results: the amplification of weak counterfeiters into strong ones (Theorem 3.5), and the construction of full-blown quantum money schemes from mini-schemes together with quantumly-secure digital signature schemes (Theorem 3.6).

3.1 Quantum money schemes

Intuitively, a *public-key quantum money scheme* is a scheme by which

(1) a trusted "bank" can feasibly generate an unlimited number of quantum banknotes,

(2) anyone can feasibly verify a valid banknote as having come from the bank, but

(3) no one besides the bank can feasibly map $q = \text{poly}(n)$ banknotes to $r > q$ banknotes with any non-negligible success probability.[13]

We now make the notion more formal.

Definition 3.1 (Quantum Money Schemes)**.** A **public-key quantum money scheme** $\mathcal{S}$ consists of three polynomial-time quantum algorithms:

- KeyGen, which takes as input a security parameter 0^n, and probabilistically generates a key pair $(k_{\text{private}}, k_{\text{public}})$.
- Bank, which takes as input k_{private}, and probabilistically generates a quantum state \$ called a **banknote**. (Usually \$ will be an ordered pair (s, ρ_s), consisting of a classical **serial number** s and a **quantum money state** ρ_s, but this is not strictly necessary.)
- Ver, which takes as input k_{public} and an alleged banknote ¢, and either accepts or rejects.

[13] Previously, Aaronson [3] required only that no polynomial-time counterfeiter could increase its *expected* number of valid banknotes. However, the stronger condition required here is both achievable, and seemingly more natural from the standpoint of security proofs.

We say $\mathcal{S}$ has **completeness error** ε if $\mathsf{Ver}\left(k_{\text{public}}, \$\right)$ accepts with probability at least $1-\varepsilon$ for all public keys k_{public} and valid banknotes \$. If $\varepsilon = 0$ then $\mathcal{S}$ has **perfect completeness**.

Let Count (the **money counter**) take as input k_{public} as well as a collection of (possibly-entangled) alleged banknotes $\cancel{\$}_1, \ldots, \cancel{\$}_r$, and output the number of indices $i \in [r]$ such that $\mathsf{Ver}\left(k_{\text{public}}, \cancel{\$}_i\right)$ accepts. Then we say $\mathcal{S}$ has **soundness error** δ if, given any quantum circuit $C\left(k_{\text{public}}, \$_1, \ldots, \$_q\right)$ of size $\operatorname{poly}(n)$ (called the **counterfeiter**), which maps $q = \operatorname{poly}(n)$ valid banknotes $\$_1, \ldots, \$_q$ to $r = \operatorname{poly}(n)$ (possibly-entangled) alleged banknotes $\cancel{\$}_1, \ldots, \cancel{\$}_r$,

$$\Pr\left[\mathsf{Count}\left(k_{\text{public}}, C\left(k_{\text{public}}, \$_1, \ldots, \$_q\right)\right) > q\right] \leq \delta.$$

Here the probability is over the key pair $\left(k_{\text{private}}, k_{\text{public}}\right)$, valid banknotes $\$_1, \ldots, \$_q$ generated by $\mathsf{Bank}\left(k_{\text{private}}\right)$, and the behavior of Count and C.

We call $\mathcal{S}$ **secure** if it has completeness error $\leq 1/3$ and negligible soundness error.

In Appendix A, we show that the completeness error in any quantum money scheme can be amplified to $1/2^{\operatorname{poly}(n)}$, at the cost of only a small increase in the soundness error. Note that, by Lemma 2.6 (the "Almost As Good As New Lemma"), once we make the completeness error exponentially small in n, we can also give our scheme the property that *any banknote* \$ *can be verified* $\exp(n)$ *times*, before \$ gets "worn out" by repeated measurements. This observation is part of what justifies our use of the term "money."[14]

In this paper, we will often consider **relativized** quantum money schemes, which simply means that the three procedures KeyGen, Bank, Ver—as well as the counterfeiter C—all get access to exactly the same oracle $A : \{0,1\}^* \to \{0,1\}$. We will also consider relativized digital signature schemes, etc., which are defined analogously.

A **private-key quantum money scheme** is the same as a public-key scheme, except that the counterfeiter C no longer gets access to k_{public}. (Thus, we might as well set $k := k_{\text{public}} = k_{\text{private}}$, since the public and private keys no longer play separate roles.) We call a private-key scheme **query-secure**—a notion "intermediate" between private-key and public-key—if the counterfeiter C is allowed to interact repeatedly with the bank. Given any alleged banknote σ, the bank runs the verification procedure $\mathsf{Ver}(k, \sigma)$, then returns to C both the classical result (i.e., accept or reject) *and* the post-measurement quantum state $\widetilde{\sigma}$.

3.2 Mini-schemes

While Definition 3.1 captures our intuitive requirements for a public-key quantum money scheme, experience has shown that it is cumbersome to work with in practice. So following Lutomirski et al. [32] and Farhi et al. [24], in this section we define a simpler primitive called *mini-schemes*. We also prove an amplification theorem for a large class of mini-schemes. Then, in Section 3.3, we will explain how mini-schemes can be generically combined with conventional digital signature schemes to create full public-key quantum money schemes.

Definition 3.2 (Mini-Schemes)**.** A (public-key) **mini-scheme** $\mathcal{M}$ consists of two polynomial-time quantum algorithms:

[14] By contrast, BBBW [15] introduced the term "subway tokens" for quantum money states that get destroyed immediately upon verification.

- Bank, which takes as input a security parameter 0^n, and probabilistically generates a banknote $\$ = (s, \rho_s)$, where s is a classical **serial number**, and ρ_s is a quantum money state.

- Ver, which takes as input an alleged banknote $₵$, and either accepts or rejects.

We say $\mathcal{M}$ has **completeness error** ε if $\mathsf{Ver}(\$)$ accepts with probability at least $1-\varepsilon$ for all valid banknotes \$. If $\varepsilon = 0$ then $\mathcal{M}$ has perfect completeness. If, furthermore, $\rho_s = |\psi_s\rangle\langle\psi_s|$ is always a pure state, and Ver simply consists of a projective measurement onto the rank-1 subspace spanned by $|\psi_s\rangle$, then we say $\mathcal{M}$ is **projective**.[15]

Let Ver_2 (the **double verifier**) take as input a single serial number s as well as two (possibly-entangled) states σ_1 and σ_2, and accept if and only if $\mathsf{Ver}(s, \sigma_1)$ and $\mathsf{Ver}(s, \sigma_2)$ both accept. We say $\mathcal{M}$ has **soundness error** δ if, given any quantum circuit C of size $\mathrm{poly}(n)$ (the **counterfeiter**), $\mathsf{Ver}_2(s, C(\$))$ accepts with probability at most δ. Here the probability is over the banknote \$ output by $\mathsf{Bank}(0^n)$, as well as the behavior of Ver_2 and C.

We call $\mathcal{M}$ **secure** if it has completeness error $\leq 1/3$ and negligible soundness error.

We observe a simple relationship between Definitions 3.1 and 3.2:

Proposition 3.3. *If there exists a secure public-key money scheme* $\mathcal{S} = (\mathsf{KeyGen}_{\mathcal{S}}, \mathsf{Bank}_{\mathcal{S}}, \mathsf{Ver}_{\mathcal{S}})$*, then there also exists a secure mini-scheme* $\mathcal{M} = (\mathsf{Bank}_{\mathcal{M}}, \mathsf{Ver}_{\mathcal{M}})$.

Proof. Each banknote output by $\mathsf{Bank}_{\mathcal{M}}(0^n)$ will have the form

$$\left(k_{\text{public}}, \mathsf{Bank}_{\mathcal{S}}\left(k_{\text{private}}\right)\right),$$

where $\left(k_{\text{private}}, k_{\text{public}}\right)$ is a key pair output by $\mathsf{KeyGen}_{\mathcal{S}}(0^n)$. Then $\mathsf{Ver}_{\mathcal{M}}(s, \rho_s)$ will accept if and only if $\mathsf{Ver}_{\mathcal{S}}(s, \rho_s)$ does. Any counterfeiter $C_{\mathcal{M}}$ against $\mathcal{M}$ can be converted directly into a counterfeiter $C_{\mathcal{S}}$ against $\mathcal{S}$. □

Call a mini-scheme $\mathcal{M} = (\mathsf{Bank}, \mathsf{Ver})$ **secret-based** if Bank works by first generating a uniformly-random classical string r, and then generating a banknote $\$_r := (s_r, \rho_r)$. Intuitively, in a secret-based scheme, the bank can generate many identical banknotes by simply reusing r, while in a non-secret-based scheme, *not even the bank* might be able to generate two identical banknotes. Here is an interesting observation:

Proposition 3.4. *If there exists a secure, secret-based mini-scheme, then there also exists a one-way function secure against quantum attack.*

Proof. The desired OWF is $\mathsf{SerialNum}(r) := s_r$. If there existed a polynomial-time quantum algorithm to recover r given s_r, then we could use that algorithm to produce an unlimited number of additional banknotes $\$_r$. □

[15] We similarly call a full quantum money scheme projective, if $\mathsf{Ver}(\$)$ consists of a measurement on one part of \$ in the computational basis, followed by a rank-1 projective measurement on the remaining part.

All of the mini-schemes developed in this paper will be secret-based. By contrast, the earlier schemes of Lutomirski et al. [32] and Farhi et al. [24] are non-secret-based, since the serial number s is only obtained as the outcome of a quantum measurement.

The following result is one of the most useful in the paper. Intuitively, it says that in projective mini-schemes, a counterfeiter that copies a banknote with *any* non-negligible fidelity can be "amplified" to a counterfeiter that copies the banknote almost *perfectly*—or conversely, that to rule out the former sort of counterfeiter, it suffices to rule out the latter. The proof makes essential use of the amplitude amplification results from Section 2.3.

Theorem 3.5 (Amplification of Counterfeiters)**.** *Let $\mathcal{M} = (\mathsf{Bank}, \mathsf{Ver})$ be a projective mini-scheme, and let $\$ = (s, \rho)$ be a valid banknote in $\mathcal{M}$. Suppose there exists a counterfeiter C that copies $\$$ with probability $\varepsilon > 0$: that is,*

$$\Pr\left[\mathsf{Ver}_2\left(s, C\left(\$\right)\right) \textit{ accepts}\right] \geq \varepsilon.$$

Then for all $\delta > 0$, there is also a modified counterfeiter C' (depending only on ε and δ, not $\$$), which makes

$$O\left(\frac{\log 1/\delta}{\sqrt{\varepsilon}\left(\sqrt{\varepsilon} + \delta^2\right)}\right)$$

queries to C, C^{-1}, and Ver *and which satisfies*

$$\Pr\left[\mathsf{Ver}_2\left(s, C'\left(\$\right)\right) \textit{ accepts}\right] \geq 1 - \delta.$$

Proof. Write $\$$ as a mixture of pure states:

$$\$ = \sum p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|.$$

By linearity, clearly it suffices to show that

$$\Pr\left[\mathsf{Ver}_2\left(s, C'\left(\left|\psi_i\right\rangle\right)\right) \text{ accepts}\right] \geq 1 - \delta$$

for all i such that $p_i > 0$. We focus on $\left|\psi\right\rangle := \left|\psi_1\right\rangle$ without loss of generality.

By assumption, there exists a subspace S such that

$$\Pr\left[\mathsf{Ver}\left(\rho\right) \text{ accepts}\right] = F\left(\rho, S\right)^2$$

for all ρ. Then $F\left(\$, S\right) = F\left(\left|\psi\right\rangle, S\right) = 1$.

Now, just as Ver is simply a projector onto S, so Ver_2 is a projector onto $S^{\otimes 2}$. Thus

$$F\left(C\left(\left|\psi\right\rangle\right), S^{\otimes 2}\right) \geq \sqrt{\varepsilon}.$$

So consider performing a fixed-point Grover search, with $C\left(\left|\psi\right\rangle\right)$ as the initial state and $S^{\otimes 2}$ as the target subspace. By Lemma 2.8, this will produce a state ρ such that $F\left(\rho, S^{\otimes 2}\right) \geq 1 - \delta$ using $O\left(\left(1/\varepsilon\right)\log(1/\delta)\right)$ Grover iterations. Each iteration requires a reflection about $C\left(\left|\psi\right\rangle\right)$ and a reflection about $S^{\otimes 2}$, which can be implemented using $O\left(1\right)$ queries to C, C^{-1} and Ver respectively. Therefore the number of queries to C, C^{-1} and Ver is $O\left(\left(1/\varepsilon\right)\log(1/\delta)\right)$ as well.

If δ is large compared to ε, then we can instead use Theorem 2.10, which produces a state ρ such that $F\left(\rho, S^{\otimes 2}\right) \geq 1-\delta$ using

$$O\left(\frac{1}{\sqrt{\varepsilon}\delta^2}\log\frac{1}{\delta}\right)$$

iterations. Taking the minimum of the two bounds gives us the claimed bound on query complexity. □

Theorem 3.5 is unlikely to hold for *arbitrary* (non-projective) mini-schemes, for the simple reason that we can always create a mini-scheme where Ver accepts *any* state with some small nonzero probability ε. We leave it as an open problem to find the largest class of mini-schemes for which Theorem 3.5 holds.

3.3 The standard construction

Following Lutomirski et al. [32] and Farhi et al. [24], we can now define a "standard construction" of public-key quantum money schemes from mini-schemes and digital signature schemes. Given a mini-scheme $\mathcal{M} = (\mathsf{Bank}_{\mathcal{M}}, \mathsf{Ver}_{\mathcal{M}})$, and a signature $\mathcal{D} = (\mathsf{KeyGen}_{\mathcal{D}}, \mathsf{Sign}_{\mathcal{D}}, \mathsf{Ver}_{\mathcal{D}})$, we define the quantum money scheme $\mathcal{S} = (\mathsf{KeyGen}_{\mathcal{S}}, \mathsf{Bank}_{\mathcal{S}}, \mathsf{Ver}_{\mathcal{S}})$ as follows:

- $\mathsf{KeyGen}_{\mathcal{S}}$ is simply $\mathsf{KeyGen}_{\mathcal{D}}$ from the digital signature scheme.
- $\mathsf{Bank}_{\mathcal{S}}$ first calls $\mathsf{Bank}_{\mathcal{M}}$ from the mini-scheme to obtain a banknote (s,ρ). It then outputs (s,ρ) together with a digital signature of the serial number s:
$$\mathsf{Bank}_{\mathcal{S}}\left(k_{\text{private}}\right) := \left(s, \mathsf{Sign}_{\mathcal{D}}\left(k_{\text{private}}, s\right), \rho\right).$$
- $\mathsf{Ver}_{\mathcal{S}}$ accepts an alleged banknote (s,w,σ), if and only if $\mathsf{Ver}_{\mathcal{M}}(s,\sigma)$ and $\mathsf{Ver}_{\mathcal{D}}\left(k_{\text{public}}, s, w\right)$ both accept.

We now prove the above construction's security.

Theorem 3.6 (Security of the Standard Construction)**.** *Suppose $\mathcal{M}$ is a secure mini-scheme, and $\mathcal{D}$ is a digital signature scheme secure against quantum chosen-message attacks. Then $\mathcal{S}$ is a secure public-key quantum money scheme.*

Proof. The intuition behind the proof is extremely simple: by requiring digital signatures for the serial numbers, we can force a counterfeiter to copy one of its *existing* banknotes, rather than creating a new banknote with a new serial number. In this way, we force the counterfeiter to break the underlying mini-scheme $\mathcal{M}$, rather than doing an "end run" around $\mathcal{M}$.

To formalize this intuition, suppose there exists a counterfeiter $C_{\mathcal{S}}$ against $\mathcal{S}$: that is, a polynomial-time quantum algorithm such that

$$\Pr\left[\mathsf{Count}\left(k_{\text{public}}, C_{\mathcal{S}}\left(k_{\text{public}}, \$_1, \ldots, \$_q\right)\right) > q\right] \geq \frac{1}{p(n)}.$$

Here $\$_i := (s_i, w_i, \rho_i)$ is a valid banknote, Count is the money counter from Definition 3.1, and p is some polynomial. Also, the probability is over the key pair $\left(k_{\text{private}}, k_{\text{public}}\right)$, the valid banknotes $\$_1, \ldots, \$_q$, and the behavior of Count and $C_{\mathcal{S}}$. Suppose further that $\mathcal{D}$ is secure. Then it suffices to show that, by using $C_{\mathcal{S}}$, we can construct a counterfeiter $C_{\mathcal{M}}$ against the underlying mini-scheme $\mathcal{M}$.

Let $\mathsf{New}\left(k_{\text{public}}, \$_1, \ldots, \$_q\right)$ be an algorithm that does the following:

(1) Records the serial numbers $s_1, \ldots, s_q$ of $\$_1, \ldots, \$_q$, and lets $U := \{s_1, \ldots, s_q\}$.

(2) Runs $C_{\mathcal{S}}(k_{\text{public}}, \$_1, \ldots, \$_q)$, and examines the output states $¢_1, \ldots, ¢_r$.

(3) Returns the number of $i \in [r]$ such that $\mathsf{Ver}_{\mathcal{S}}(¢_i)$ accepts, *and* $¢_i$'s serial number s'_i does not belong to U.

Then we claim that $\Pr[\mathsf{New}(k_{\text{public}}, \$_1, \ldots, \$_q) > 0]$ is negligibly small, where the probability is over the same variables as before. The proof is simply that, if this were not so, then we could easily create a counterfeiter $C_{\mathcal{D}}$ against the digital signature scheme $\mathcal{D}$. With non-negligible probability, $C_{\mathcal{D}}$ would generate a valid signature $\mathsf{Sign}_{\mathcal{D}}(k_{\text{private}}, s'_i)$, for a message s'_i for which $C_{\mathcal{D}}$ had never before seen a valid signature, by running $C_{\mathcal{S}}(k_{\text{public}}, \$_1, \ldots, \$_q)$, then measuring $¢_i = (s'_i, w'_i, \rho'_i)$ for a uniformly random $i \in [r]$. (Note that $C_{\mathcal{D}}$ can generate q money states $\$_1, \ldots, \$_q$, without knowledge of k_{private}, by generating the s_i and the ρ_i on its own, then calling the signing oracle $\mathcal{O}$ to get the w_i.)

But now we can define a counterfeiter $C_{\mathcal{M}}$ against the mini-scheme $\mathcal{M}$, which works as follows:

(i) Run $\mathsf{KeyGen}_{\mathcal{D}}(0^n)$, to generate a *new* key pair $\left(k'_{\text{private}}, k'_{\text{public}}\right)$.

(ii) Label the banknote to be copied (s_ℓ, ρ_ℓ), for some $\ell \in [q]$ chosen uniformly at random.

(iii) Repeatedly call $\mathsf{Bank}_{\mathcal{M}}(0^n)$ to generate $q-1$ serial numbers and quantum money states, labeled (s_i, ρ_i) for all $i \in [q] \setminus \{\ell\}$. Let $U := \{s_1, \ldots, s_q\}$.

(iv) Generate a digital signature $w_i := \mathsf{Sign}_{\mathcal{D}}\left(k'_{\text{private}}, s_i\right)$ for each $i \in [q]$. Let $\$_i := (s_i, w_i, \rho_i)$.

(v) Run the counterfeiter $C_{\mathcal{S}}(k_{\text{public}}, \$_1, \ldots, \$_q)$, to obtain $r > q$ alleged banknotes $¢_1, \ldots, ¢_r$ where $¢_j = \left(s'_j, w'_j, \rho'_j\right)$.

(vi) Choose $j, k \in [r]$ uniformly at random without replacement, and output $\left(\rho'_j, \rho'_k\right)$ as a candidate for two copies of ρ_ℓ.

Suppose that $\mathsf{Count} > q$, as happens with probability at least $1/p(n)$. Also suppose that $\mathsf{New} = 0$, as happens all but a negligible fraction of the time. Then by the pigeonhole principle, there must exist indices $j \neq k$ such that $s'_j = s'_k$. With probability at least $1/\binom{r}{2}$, the counterfeiter $C_{\mathcal{M}}$ will find such a (j,k) pair. Therefore $C_{\mathcal{M}}$ succeeds with overall probability $\Omega(1/\text{poly}(n))$. □

Theorem 3.6 reduces the construction of a public-key quantum money scheme to two "smaller" problems: constructing a mini-scheme, and constructing a signature scheme secure against quantum attacks. In practice, however, the situation is even better, since in this paper, all of our constructions of mini-schemes will *also* yield signature schemes "free of charge"! The following proposition explains why:

Proposition 3.7. *If there exists a secure, secret-based mini-scheme $\mathcal{M}$, then there also exists a secure public-key quantum money scheme $\mathcal{S}$.*

Proof. Starting from $\mathcal{M}$, we can get a one-way function secure against quantum attack from Proposition 3.4, and hence a digital signature scheme $\mathcal{D}$ secure against quantum chosen-message attack from Theorem 2.2. Combining $\mathcal{M}$ and $\mathcal{D}$ now yields $\mathcal{S}$ by Theorem 3.6. □

Finally, let us make explicit what Theorem 3.6 means for oracle construction.

Corollary 3.8. *Suppose there exists a mini-scheme $\mathcal{M}$ that is provably secure relative to some oracle $A_{\mathcal{M}}$ (i.e., any counterfeiter $C_{\mathcal{M}}$ against $\mathcal{M}$ must make superpolynomially many queries to $A_{\mathcal{M}}$). Then there exists a public-key quantum money scheme $\mathcal{S}$ that is provably secure relative to some other oracle $A_{\mathcal{S}}$.*

Proof. By Theorem 2.3, relative to a suitable oracle $A_{\mathcal{D}}$ (in fact, a *random* oracle suffices), there exists a signature scheme $\mathcal{D}$, such that any quantum chosen-message attack against $\mathcal{D}$ must make superpolynomially many queries to $A_{\mathcal{D}}$. The oracle $A_{\mathcal{S}}$ will simply be a concatenation of $A_{\mathcal{M}}$ with $A_{\mathcal{D}}$. Relative to $A_{\mathcal{S}}$, we claim that the mini-scheme $\mathcal{M}$ and signature scheme $\mathcal{D}$ are *both* secure—and therefore, by Theorem 3.6, we can construct a secure public-key quantum money scheme $\mathcal{S}$.

The only worry is that a counterfeiter $C_{\mathcal{M}}$ against $\mathcal{M}$ might gain some advantage by querying $A_{\mathcal{D}}$; or conversely, a counterfeiter $C_{\mathcal{D}}$ against $\mathcal{D}$ might gain some advantage by querying $A_{\mathcal{M}}$. However, this worry is illusory, for the simple reason that the oracles $A_{\mathcal{D}}$ and $A_{\mathcal{M}}$ are generated independently. Thus, if $C_{\mathcal{M}}$ can break $\mathcal{M}$ by querying $A_{\mathcal{D}}$, then it can *also* break $\mathcal{M}$ by querying a randomly-generated "mock-up" $A'_{\mathcal{D}}$ of $A_{\mathcal{D}}$; and conversely, if $C_{\mathcal{D}}$ can break $\mathcal{D}$ by querying $A_{\mathcal{M}}$, then it can also break $\mathcal{D}$ by querying a randomly-generated mock-up $A'_{\mathcal{M}}$ of $A_{\mathcal{M}}$. Regardless of the *computational* cost of generating these mock-ups, they give us a break against $\mathcal{D}$ or $\mathcal{M}$ that makes only $\operatorname{poly}(n)$ oracle queries, thereby giving the desired contradiction. □

4 Inner-product adversary method

At least in the black-box setting, our goal is to create quantum money (mini-)schemes that we can *prove* are secure—by showing that any counterfeiter would need to make exponentially many queries to some oracle. Proving security results of this kind turns out to require interesting quantum lower bound machinery. In this section, we introduce the *inner-product adversary method*, a new variant of Ambainis's quantum adversary method [9] that is well-adapted to proving the security of quantum money schemes, and that seems likely to find other applications.

Let us explain the difficulty we need to overcome. In a public-key quantum money scheme, a counterfeiter C has *two* powerful resources available:

(1) One or more copies of a "legitimate" quantum money state $|\psi\rangle$.

(2) Access to a *verification procedure* V, which accepts $|\psi\rangle$ and rejects every state orthogonal to $|\psi\rangle$.

Indeed, for us, the situation is even better for C (i.e., worse for us!), since C can query not only the verification procedure V itself, but also an underlying *classical* oracle U that the legitimate buyers and sellers use to implement V. But let us ignore that issue for now.

As a first step, of course, we should understand how to rule out counterfeiting given (1) or (2) separately. If C has a copy of $|\psi\rangle$, but no oracle access to V, then the impossibility of preparing $|\psi\rangle|\psi\rangle$

essentially amounts to the No-Cloning Theorem. Conversely, if C has oracle access to V, but no copy of $|\psi\rangle$, then given unlimited time, C *can* prepare as many copies of $|\psi\rangle$ as it wants, by using Grover's algorithm to search for a quantum state that V accepts. The problem is "merely" that, if $|\psi\rangle$ has n qubits, then Grover's algorithm requires $\Theta(2^{n/2})$ iterations, and the BBBV hybrid argument [13] shows that Grover's algorithm is optimal.

What we need, then, is a theorem showing that any counterfeiter needs exponentially many queries to V to prepare $|\psi\rangle|\psi\rangle$, *even if* the counterfeiter has a copy of $|\psi\rangle$ to start with. Such a theorem would contain both the No-Cloning Theorem and the BBBV hybrid argument as special cases. Aaronson [3] called the desired generalization the *Complexity-Theoretic No-Cloning Theorem*, and sketched a proof of it using Ambainis's adversary method. Based on that result, Aaronson also argued that there exists a *quantum oracle* (i.e., a black-box unitary transformation V) relative to which secure public-key quantum money is possible. However, the details were never published.

In this section, we prove a result—Theorem 4.2—that is much more general than Aaronson's previous Complexity-Theoretic No-Cloning Theorem [3]. Then, in Section 5, we apply Theorem 4.2 to prove the security of public-key quantum money relative to a *classical* oracle. In Appendix B, we also apply Theorem 4.2 to prove the "original" Complexity-Theoretic No-Cloning Theorem [3], which involves Haar-random n-qubit states $|\psi\rangle$, rather than superpositions $|A\rangle$ over subspaces $A \leq \mathbb{F}_2^n$.[16]

4.1 Idea of method

So, what *is* the inner-product adversary method? In Ambainis's adversary method [9]—like in the BBBV hybrid argument [13] from which it evolved—the basic idea is to upper-bound how much "progress" a quantum algorithm Q can make at distinguishing pairs of oracles, as the result of a single query. Let $\left|\Psi_t^U\right\rangle$ be Q's state after t queries, assuming that the oracle is U. Then *normally*, before any queries have been made, we can assume that $\left|\Psi_0^U\right\rangle = \left|\Psi_0^V\right\rangle$ for all oracles U and V. By contrast, after the final query T, for all oracle pairs (U,V) that Q is trying to distinguish, we must have (say) $\left|\left\langle\Psi_T^U|\Psi_T^V\right\rangle\right| \leq 1/2$. Thus, *if* we can show that the inner product $\left|\left\langle\Psi_t^U|\Psi_t^V\right\rangle\right|$ can decrease by at most ε as the result of a single query, then it follows that Q must make $\Omega(1/\varepsilon)$ queries.

But when we try to apply the above framework to quantum money, we run into serious difficulties. Most obviously, it is no longer true that $\left|\Psi_0^U\right\rangle = \left|\Psi_0^V\right\rangle$ for all oracles U,V. Indeed, before Q makes even a *single* query to its oracle V, it already has a great deal of information about V, in the form of a legitimate money state $|\psi\rangle$ that V accepts. The task is "merely" to prepare a second copy of a state that Q already has! Worse yet, once we fix two oracles U and V, we find that Q generally *can* exploit the "head start" provided by its initial state to decrease the inner product $\left|\left\langle\Psi_t^U|\Psi_t^V\right\rangle\right|$ by a constant amount, by making just a single query to U or V respectively.

Our solution is as follows. We first carefully choose a distribution $\mathcal{D}$ over oracle pairs (U,V). We then analyze how much the *expected* inner product

$$\mathop{\mathrm{E}}_{(U,V)\sim\mathcal{D}}\left[\left|\left\langle\Psi_t^U|\Psi_t^V\right\rangle\right|\right]$$

[16] For whatever it is worth, we get a lower bound of $\Omega(2^{n/2})$ on the number of queries needed to copy a Haar-random state, which is quadratically better than the $\Omega(2^{n/4})$ that we get for subspace states.

can decrease as the result of a single query to U or V. We will find that, even if Q can substantially decrease the inner product between $\left|\Psi_t^U\right\rangle$ and $\left|\Psi_t^V\right\rangle$ for *some* (U,V) pairs by making a single query, it cannot do so for *most* pairs.

To illustrate, let $|\psi\rangle$ and $|\varphi\rangle$ be two possible quantum money states, which satisfy (say) $\langle\psi|\varphi\rangle = 1/2$. Then if a counterfeiting algorithm succeeds perfectly, it must map $|\psi\rangle$ to $|\psi\rangle^{\otimes 2}$, and $|\varphi\rangle$ to $|\varphi\rangle^{\otimes 2}$. Since

$$\langle\psi|^{\otimes 2}|\varphi\rangle^{\otimes 2} = (\langle\psi|\varphi\rangle)^2 = \frac{1}{4},$$

this means that the counterfeiter must *decrease the corresponding inner product* by at least $1/4$. However, we will show that the *average* inner product can decrease by at most $1/\exp(n)$ as the result of a single query. From this it will follow that the counterfeiter needs to make $2^{\Omega(n)}$ queries.

Let us mention that today, there are several "sophisticated" versions of the quantum adversary method [10, 29], which *can* yield lower bounds for quantum state generation tasks not unlike the ones we consider. However, a drawback of these methods is that they are extremely hard to apply to concrete problems: doing so typically requires eigenvalue bounds, and often the use of representation theory. For this reason, even if one of the "sophisticated" adversary methods (or a variant thereof) could be applied to the quantum money problem, our approach might still be preferable.

4.2 The method

We now introduce the inner-product adversary method. Let $\mathcal{O}$ be a set of quantum oracles acting on n qubits each. For each $U \in \mathcal{O}$, assume there exists a subspace $S_U \leq \mathbb{C}^{2^n}$ such that

(i) $U|\psi\rangle = -|\psi\rangle$ for all $|\psi\rangle \in S_U$, and

(ii) $U|\eta\rangle = |\eta\rangle$ for all $|\eta\rangle \in S_U^{\perp}$.

Let $R \subset \mathcal{O} \times \mathcal{O}$ be a symmetric binary relation on $\mathcal{O}$, with the properties that

(i) $(U,U) \notin R$ for all $U \in \mathcal{O}$, and

(ii) for every $U \in \mathcal{O}$ there exists a $V \in \mathcal{O}$ such that $(U,V) \in R$.

Suppose that for all $U \in \mathcal{O}$ and all $|\eta\rangle \in S_U^{\perp}$, we have

$$\mathop{\mathrm{E}}_{V\,:\,(U,V)\in R}\left[F(|\eta\rangle, S_V)^2\right] \leq \varepsilon,$$

where $F(|\eta\rangle, S_V) = \max_{|\psi\rangle\in S_V} |\langle\eta|\psi\rangle|$ is the fidelity between $|\eta\rangle$ and S_V. Let Q be a quantum oracle algorithm, and let Q^U denote Q run with the oracle $U \in \mathcal{O}$. Suppose Q^U begins in the state $\left|\Psi_0^U\right\rangle$ (possibly already dependent on U). Let $\left|\Psi_t^U\right\rangle$ denote the state of Q^U immediately after the t^{th} query. Also, define a *progress measure* p_t by

$$p_t := \mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\left|\left\langle\Psi_t^U|\Psi_t^V\right\rangle\right|\right].$$

The following lemma bounds how much p_t can decrease as the result of a single query.

Lemma 4.1 (Bound on Progress Rate)**.**

$$p_t \geq p_{t-1} - 4\sqrt{\varepsilon}.$$

Proof. Let $\left|\Phi_t^U\right\rangle$ denote the state of Q^U immediately *before* the t^{th} query. Then for all t, it is clear that $\left\langle\Phi_t^U|\Phi_t^V\right\rangle = \left\langle\Psi_{t-1}^U|\Psi_{t-1}^V\right\rangle$: in other words, the unitary transformations that Q performs in between query steps have no effect on the inner products. So to prove the lemma, it suffices to show the following inequality:

$$\mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\left|\left\langle\Phi_t^U|\Phi_t^V\right\rangle\right|\right] - \mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\left|\left\langle\Psi_t^U|\Psi_t^V\right\rangle\right|\right] \leq 4\sqrt{\varepsilon}\,. \tag{*}$$

Let $\{|i\rangle\}_{i\in[B]}$ be an arbitrary orthonormal basis for Q's workspace register. Then we can write

$$\begin{aligned}\left|\Phi_t^U\right\rangle &= \sum_{i\in[B]} \alpha_{t,i}^U |i\rangle \left|\Phi_{t,i}^U\right\rangle \\ &= \sum_{i\in[B]} |i\rangle \left(\beta_{t,i}^U \left|\eta_{t,i}^U\right\rangle + \gamma_{t,i}^U \left|\psi_{t,i}^U\right\rangle\right),\end{aligned}$$

where $\left|\eta_{t,i}^U\right\rangle \in S_U^{\perp}$ and $\left|\psi_{t,i}^U\right\rangle \in S_U$. (By normalization, $\left|\beta_{t,i}^U\right|^2 + \left|\gamma_{t,i}^U\right|^2 = \left|\alpha_{t,i}^U\right|^2$.) A query transforms the above state to

$$\left|\Psi_t^U\right\rangle = \sum_{i\in[B]} |i\rangle \left(\beta_{t,i}^U \left|\eta_{t,i}^U\right\rangle - \gamma_{t,i}^U \left|\psi_{t,i}^U\right\rangle\right).$$

So for all $U,V \in \mathcal{O}$,

$$\begin{aligned}\left\langle\Phi_t^U|\Phi_t^V\right\rangle - \left\langle\Psi_t^U|\Psi_t^V\right\rangle &= \sum_{i\in[B]} \left(\overline{\beta}_{t,i}^U \left\langle\eta_{t,i}^U\right| + \overline{\gamma}_{t,i}^U \left\langle\psi_{t,i}^U\right|\right)\left(\beta_{t,i}^V \left|\eta_{t,i}^V\right\rangle + \gamma_{t,i}^V \left|\psi_{t,i}^V\right\rangle\right) \\ &\quad - \sum_{i\in[B]} \left(\overline{\beta}_{t,i}^U \left\langle\eta_{t,i}^U\right| - \overline{\gamma}_{t,i}^U \left\langle\psi_{t,i}^U\right|\right)\left(\beta_{t,i}^V \left|\eta_{t,i}^V\right\rangle - \gamma_{t,i}^V \left|\psi_{t,i}^V\right\rangle\right) \\ &= 2\sum_{i\in[B]} \left(\overline{\beta}_{t,i}^U \gamma_{t,i}^V \left\langle\eta_{t,i}^U|\psi_{t,i}^V\right\rangle + \overline{\gamma}_{t,i}^U \beta_{t,i}^V \left\langle\psi_{t,i}^U|\eta_{t,i}^V\right\rangle\right).\end{aligned}$$

By Cauchy-Schwarz, the above implies that

$$\left|\left\langle\Phi_t^U|\Phi_t^V\right\rangle\right| - \left|\left\langle\Psi_t^U|\Psi_t^V\right\rangle\right| \leq 2\max_{i\in[B]}\left|\left\langle\eta_{t,i}^U|\psi_{t,i}^V\right\rangle\right| + 2\max_{i\in[B]}\left|\left\langle\psi_{t,i}^U|\eta_{t,i}^V\right\rangle\right|.$$

Now fix $U \in \mathcal{O}$ and $i \in [B]$. Then again applying Cauchy-Schwarz,

$$\begin{aligned}\mathop{\mathrm{E}}_{V\,:\,(U,V)\in R}\left[\left|\left\langle\eta_{t,i}^U|\psi_{t,i}^V\right\rangle\right|\right] &\leq \sqrt{\mathop{\mathrm{E}}_{V\,:\,(U,V)\in R}\left[\left|\left\langle\eta_{t,i}^U|\psi_{t,i}^V\right\rangle\right|^2\right]} \\ &\leq \sqrt{\mathop{\mathrm{E}}_{V\,:\,(U,V)\in R}\left[\max_{|\psi\rangle\in S_V}\left|\left\langle\eta_{t,i}^U|\psi\right\rangle\right|^2\right]} \\ &\leq \sqrt{\varepsilon}\,.\end{aligned}$$

Hence

$$\mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\left|\left\langle \eta_{t,i}^{U} | \psi_{t,i}^{V} \right\rangle\right|\right] \leq \sqrt{\varepsilon}$$

as well, and likewise

$$\mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\left|\left\langle \psi_{t,i}^{U} | \eta_{t,i}^{V} \right\rangle\right|\right] \leq \sqrt{\varepsilon}$$

by symmetry. Putting everything together,

$$\begin{aligned}
p_{t-1} - p_t &= \mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\left|\left\langle \Phi_t^U | \Phi_t^V \right\rangle\right| - \left|\left\langle \Psi_t^U | \Psi_t^V \right\rangle\right|\right] \\
&\leq 2 \mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\max_{i\in[B]} \left|\left\langle \eta_{t,i}^{U} | \psi_{t,i}^{V} \right\rangle\right|\right] + 2 \mathop{\mathrm{E}}_{U,V\,:\,(U,V)\in R}\left[\max_{i\in[B]} \left|\left\langle \psi_{t,i}^{U} | \eta_{t,i}^{V} \right\rangle\right|\right] \\
&\leq 4\sqrt{\varepsilon}\,.
\end{aligned}$$

This proves inequality (*) and hence the lemma. □

From Lemma 4.1 we immediately deduce the following.

Theorem 4.2 (Inner-Product Adversary Method)**.** *Suppose that initially* $\left|\left\langle \Psi_0^U | \Psi_0^V \right\rangle\right| \geq c$ *for all* $(U,V) \in R$*, whereas by the end we need* $\left|\left\langle \Psi_T^U | \Psi_T^V \right\rangle\right| \leq d$ *for all* $(U,V) \in R$*. Then* Q *must make* $T = \Omega((c-d)/\sqrt{\varepsilon})$ *oracle queries.*

5 Classical oracle scheme

In this section, we construct a mini-scheme, called the *Hidden Subspace Mini-Scheme*, that requires only a classical oracle. We then use the inner-product adversary method from Section 4 to show that our mini-scheme is secure—indeed, that any counterfeiter must make $\Omega\left(2^{n/4}\right)$ queries to copy a banknote. By the results of Sections 3.3 and 2.1, our mini-scheme will automatically imply a full-blown public-key quantum money scheme, which requires only a classical oracle and is unconditionally secure.

5.1 The hidden subspace mini-scheme

We identify n-bit strings $x \in \{0,1\}^n$ with elements of the vector space $\mathbb{F}_2^n$ in the standard way. Then in our mini-scheme, each n-qubit money state will have the form

$$|A\rangle := \frac{1}{\sqrt{|A|}} \sum_{x\in A} |x\rangle\,,$$

where A is some randomly-chosen subspace of $\mathbb{F}_2^n$ (i.e., a set of codewords of a linear code), with $\dim A = n/2$. Let $A^{\perp}$ be the orthogonal complement of A, so that $\dim A^{\perp} = n/2$ as well. Notice that we can transform $|A\rangle$ to $\left|A^{\perp}\right\rangle$ and vice versa by simply applying $H_2^{\otimes n}$: a Hadamard gate on each of the n qubits, or equivalently a quantum Fourier transform over $\mathbb{F}_2^n$.

The basic idea of the mini-scheme is as follows: the bank can easily prepare the quantum money state $|A\rangle$, starting from a classical description $\langle A\rangle$ of A (e. g., a list of $n/2$ generators). The bank distributes the state $|A\rangle$, but keeps the classical description $\langle A\rangle$ secret. Along with $|A\rangle$ itself, the bank also publishes details of how to *verify* $|A\rangle$ by querying two classical oracles, U_A and $U_{A^\perp}$. The first oracle, U_A, decides membership in A: for all n-qubit basis states $|x\rangle$,

$$U_A|x\rangle = \begin{cases} -|x\rangle & \text{if } x \in A, \\ |x\rangle & \text{otherwise.} \end{cases}$$

The second oracle, $U_{A^\perp}$, decides membership in $A^\perp$ in the same way.

Using U_A, it is easy to implement a projector $\mathbb{P}_A$ onto the set of basis states in A. To do so, simply initialize a control qubit to

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$

then apply U_A conditioned on the control qubit being in state $|1\rangle$, then measure the control qubit in the $\{|+\rangle, |-\rangle\}$ basis, and postselect on getting the outcome $|-\rangle$. Likewise, using $U_{A^\perp}$, it is easy to implement a projector $\mathbb{P}_{A^\perp}$ onto the set of basis states in $A^\perp$. Then V_A, the public verification algorithm for the money state $|A\rangle$, will simply consist of $\mathbb{P}_A$, then a Fourier transform, then $\mathbb{P}_{A^\perp}$, and finally a second Fourier transform to return the legitimate money state back to $|A\rangle$:

$$V_A := H_2^{\otimes n}\mathbb{P}_{A^\perp}H_2^{\otimes n}\mathbb{P}_A.$$

We show in Lemma 5.1 that V_A is just a projector onto $|A\rangle$. This means, in particular, that $V_A|A\rangle = |A\rangle$, and that V_A accepts an arbitrary state $|\psi\rangle$ with probability $|\langle\psi|A\rangle|^2$. Thus, our mini-scheme is *projective* and has *perfect completeness*.

But what about security? Intuitively, a counterfeiter could query U_A or $U_{A^\perp}$ to find a generating set for A or $A^\perp$—but that would require an exponentially-long Grover search, since $|A| = |A^\perp| = 2^{n/2} \ll 2^n$. Alternatively, the counterfeiter could measure $|A\rangle$ in the standard or Hadamard bases—but that would reveal just *one* random element of A or $A^\perp$. Neither ability seems useful for *copying* $|A\rangle$, let alone recovering a full classical description of A.[17]

And indeed, using the inner-product adversary method plus some other tools, we will prove the following tight lower bound (Theorem 5.5): even if given a single copy of $|A\rangle$, as well as oracle access to U_A and $U_{A^\perp}$, a counterfeiter still needs $\Omega\left(\varepsilon 2^{n/4}\right)$ queries to prepare a state that has fidelity ε with $|A\rangle^{\otimes 2}$. This will imply that our mini-scheme has $1/\exp(n)$ soundness error.

5.2 Formal specification

We are not quite done, since we never explained how the bank provides access to U_A and $U_{A^\perp}$. Thus, in our "final" mini-scheme $\mathcal{M} = (\mathsf{Bank}_{\mathcal{M}}, \mathsf{Ver}_{\mathcal{M}})$, the bank, verifier, and counterfeiter will all have access to a *single* classical oracle U, which consists of four components:

[17] Obviously, if the counterfeiter had $\Omega(n)$ copies of $|A\rangle$, then it *could* recover a generating set for A, by simply measuring each copy independently in the standard basis. That is why, in our full quantum money scheme, the counterfeiter will *not* have $\Omega(n)$ copies of $|A\rangle$. Instead, each banknote will involve a completely different subspace $A_s \leq \mathbb{F}_2^n$ (parameterized by its unique serial number s), so that measuring one banknote reveals nothing about the others.

- A **banknote generator** $\mathcal{G}(r)$, which takes as input a random string $r \in \{0,1\}^n$, and outputs a set of linearly independent generators $\langle A_r \rangle = \{x_1, \ldots, x_{n/2}\}$ for a subspace $A_r \leq \mathbb{F}_2^n$, as well as a unique $3n$-bit *serial number* $s_r \in \{0,1\}^{3n}$. The function $\mathcal{G}$ is chosen uniformly at random, subject to the constraint that the serial numbers are all distinct.[18]

- A **serial number checker** $\mathcal{H}(s)$, which outputs 1 if $s = s_r$ is a valid serial number for some $\langle A_r \rangle$, and 0 otherwise.

- A **primal subspace tester** $\mathcal{T}_{\text{primal}}$, which takes an input of the form $|s\rangle |x\rangle$, applies U_{A_r} to $|x\rangle$ if $s = s_r$ is a valid serial number for some $\langle A_r \rangle$, and does nothing otherwise.

- A **dual subspace tester** $\mathcal{T}_{\text{dual}}$, identical to $\mathcal{T}_{\text{primal}}$ except that it applies $U_{A_r^\perp}$ instead of U_{A_r}.

Then $\mathcal{M} = (\mathsf{Bank}_\mathcal{M}, \mathsf{Ver}_\mathcal{M})$ is defined as follows:

- $\mathsf{Bank}_\mathcal{M}(0^n)$ chooses $r \in \{0,1\}^n$ uniformly at random. It then looks up $\mathcal{G}(r) = (s_r, \langle A_r \rangle)$, and outputs the banknote $|\$_r\rangle = |s_r\rangle |A_r\rangle$.

- $\mathsf{Ver}_\mathcal{M}(\cent)$ first uses $\mathcal{H}$ to check that $\cent$ has the form (s, ρ), where $s = s_r$ is a valid serial number. If so, then it uses $\mathcal{T}_{\text{primal}}$ and $\mathcal{T}_{\text{dual}}$ to apply $V_{A_r} = H_2^{\otimes n} \mathbb{P}_{A_r^\perp} H_2^{\otimes n} \mathbb{P}_{A_r}$, and accepts if and only if $V_{A_r}(\rho)$ accepts.

5.3 Analysis

We now analyze the mini-scheme defined in Sections 5.1 and 5.2. For convenience, we assume for most of the proof that the subspace $A \leq \mathbb{F}_2^n$ is *fixed*, and that the counterfeiter (who does not know A) only has access to the oracles U_A and $U_{A^\perp}$. Then, at the end, we will explain how to generalize the conclusions to the "final" mini-scheme $\mathcal{M}$.

It will be convenient to consider the subset $A^* \subset \{0,1\}^{n+1}$, defined by

$$A^* := (0, A) \cup (1, A^\perp).$$

Let S_{A^*} be the subspace of $\mathbb{C}^{2^{n+1}}$ that is spanned by basis states $|x\rangle$ such that $x \in A^*$. Then we can think of the pair of oracles $(U_A, U_{A^\perp})$ as being a *single* oracle U_{A^*}, which satisfies $U_{A^*}|\psi\rangle = -|\psi\rangle$ for all $|\psi\rangle \in S_{A^*}$, and $U_{A^*}|\eta\rangle = |\eta\rangle$ for all $|\eta\rangle \in S_{A^*}^\perp$ (where here $\perp$ means the orthogonal complement in $\mathbb{C}^{2^{n+1}}$, *not* the orthogonal complement in $\mathbb{F}_2^n$!).

Recall the definition of the verifier V_A:

$$V_A := H_2^{\otimes n} \mathbb{P}_{A^\perp} H_2^{\otimes n} \mathbb{P}_A,$$

where $\mathbb{P}_A$ and $\mathbb{P}_{A^\perp}$ denote projective measurements that accept a basis state $|x\rangle$ if and only if x belongs to A or $A^\perp$ respectively. The following lemma shows that V_A "works," and indeed that it gives us a projective mini-scheme.

[18]Note that one can implement $\mathcal{G}$ using an ordinary random oracle. In that case, the requirement that the serial numbers are distinct will be satisfied with probability $1 - O(2^{-n})$.

Lemma 5.1. *$V_A = |A\rangle \langle A|$ is simply a projector onto $|A\rangle$. So in particular,*

$$\Pr[V_A(|\psi\rangle) \text{ accepts}] = |\langle\psi|A\rangle|^2 .$$

Proof. It suffices to show that $V_A|A\rangle = |A\rangle$ and that $V_A|\psi\rangle = 0$ for all $|\psi\rangle$ orthogonal to $|A\rangle$. First,

$$\begin{aligned} V_A|A\rangle &= H_2^{\otimes n}\mathbb{P}_{A^\perp}H_2^{\otimes n}\mathbb{P}_A|A\rangle \\ &= H_2^{\otimes n}\mathbb{P}_{A^\perp}H_2^{\otimes n}|A\rangle \\ &= H_2^{\otimes n}\mathbb{P}_{A^\perp}|A^\perp\rangle \\ &= H_2^{\otimes n}|A^\perp\rangle \\ &= |A\rangle . \end{aligned}$$

Second, if $\langle\psi|A\rangle = 0$ then we can write

$$|\psi\rangle = \sum_{x\in 2^n} c_x|x\rangle$$

where $\sum_{x\in A} c_x = 0$. Then

$$\begin{aligned} V_A|\psi\rangle &= H_2^{\otimes n}\mathbb{P}_{A^\perp}H_2^{\otimes n}\mathbb{P}_A\sum_{x\in 2^n} c_x|x\rangle \\ &= H_2^{\otimes n}\mathbb{P}_{A^\perp}H_2^{\otimes n}\sum_{x\in A} c_x|x\rangle \\ &= \frac{1}{\sqrt{2^n}}H_2^{\otimes n}\mathbb{P}_{A^\perp}\sum_{x\in A} c_x\sum_{y\perp x}|y\rangle \\ &= \frac{1}{\sqrt{2^n}}H_2^{\otimes n}\sum_{y\in A^\perp}|y\rangle\sum_{x\in A} c_x \\ &= 0 . \end{aligned}$$

□

We now show that perfect counterfeiting requires exponentially many queries to U_{A^*}.

Theorem 5.2 (Lower Bound for Perfect Counterfeiting)**.** *Given one copy of $|A\rangle$, as well as oracle access to U_{A^*}, a counterfeiter needs $\Omega(2^{n/4})$ queries to prepare $|A\rangle^{\otimes 2}$ with certainty (for a worst-case $|A\rangle$).*

Proof. We will apply Theorem 4.2. Let the set $\mathcal{O}$ contain U_{A^*} for every possible subspace $A \leq \mathbb{F}_2^n$ with $\dim A = n/2$. Also, put $(U_{A^*}, U_{B^*}) \in R$ if and only if $\dim(A\cap B) = n/2-1$. Then given $U_{A^*} \in \mathcal{O}$ and $|\eta\rangle \in S_{A^*}^{\perp}$, let

$$|\eta\rangle = \sum_{x\in\{0,1\}^{n+1}\setminus A^*} \alpha_x|x\rangle .$$

We have

$$
\begin{aligned}
\mathop{\mathrm{E}}_{U_{B^*}\,:\,(U_{A^*},U_{B^*})\in R}\left[F\left(|\eta\rangle, S_{B^*}\right)^2\right] &= \mathop{\mathrm{E}}_{B\,:\,\dim(B)=n/2,\dim(A\cap B)=n/2-1}\left[\sum_{x\in B^*\setminus A^*}|\alpha_x|^2\right] \\
&\le \max_{x\in\{0,1\}^{n+1}\setminus A^*}\left(\Pr_{B\,:\,\dim(B)=n/2,\dim(A\cap B)=n/2-1}[x\in B^*]\right) \\
&= \max_{x\in\{0,1\}^{n}\setminus A}\left(\Pr_{B\,:\,\dim(B)=n/2,\dim(A\cap B)=n/2-1}[x\in B]\right) \\
&= \frac{|B\setminus A|}{|\{0,1\}^n\setminus A|}\quad(\text{for } \dim(B)=n/2,\ \dim(A\cap B)=n/2-1) \\
&= \frac{2^{n/2-1}}{2^n-2^{n/2}} \\
&\le \frac{1}{2^{n/2}}\,.
\end{aligned}
$$

Here the first line uses the definition of fidelity, the second line uses the easy direction of the minimax theorem, the third line uses the symmetry between A and $A^{\perp}$, and the fourth line uses the symmetry among all $2^n-2^{n/2}$ strings $x\in\{0,1\}^n\setminus A$. The conclusion is that we can set $\varepsilon := 2^{-n/2}$.

Fix $(U_{A^*},U_{B^*})\in R$. Then $|\langle A|B\rangle| = 1/2$. On the other hand, if the counterfeiter succeeds, it must map $|A\rangle$ to some state $|f_A\rangle := |A\rangle|A\rangle|\mathrm{garbage}_A\rangle$, and $|B\rangle$ to some state $|f_B\rangle := |B\rangle|B\rangle|\mathrm{garbage}_B\rangle$. Therefore $|\langle f_A|f_B\rangle|\le 1/4$. So setting $c=1/2$ and $d=1/4$, Theorem 4.2 tells us that the counterfeiter must make

$$
\Omega\left(\frac{c-d}{\sqrt{\varepsilon}}\right) = \Omega\left(2^{n/4}\right)
$$

queries to U_{A^*}. □

A simple modification to the proof of Theorem 5.2 shows that even to counterfeit money *almost* perfectly, one still needs exponentially many queries to U_{A^*}.

Corollary 5.3 (Lower Bound for Small-Error Counterfeiting)**.** *Given one copy of $|A\rangle$, as well as oracle access to U_{A^*}, a counterfeiter needs $\Omega(2^{n/4})$ queries to prepare a state ρ such that $\langle A|^{\otimes 2}\rho\,|A\rangle^{\otimes 2}\ge 0.9999$ (for a worst-case $|A\rangle$).*

Proof. Let $|\langle A|B\rangle| = c$, and let $\varepsilon = 0.0001$. If the counterfeiter succeeds, it must map $|A\rangle$ to some state ρ_A, and $|B\rangle$ to some state ρ_B, such that $\langle A|^{\otimes 2}\rho_A\,|A\rangle^{\otimes 2}$ and $\langle B|^{\otimes 2}\rho_B\,|B\rangle^{\otimes 2}$ are both at least $1-\varepsilon$. So letting $|f_A\rangle$ and $|f_B\rangle$ be purifications of ρ_A and ρ_B respectively, we have

$$
\begin{aligned}
|\langle f_A|f_B\rangle| &\le F\left(\rho_A,\rho_B\right) \\
&\le \left|\langle A|^{\otimes 2}|B\rangle^{\otimes 2}\right| + 2\varepsilon^{1/4} \\
&= c^2 + 2\varepsilon^{1/4}
\end{aligned}
$$

where the second line follows from Lemma 2.5. So setting $d := c^2 + 2\varepsilon^{1/4}$, Theorem 4.2 tells us that the counterfeiter must make

$$\Omega\left(\frac{c - c^2 - 2\varepsilon^{1/4}}{\sqrt{2^{-n/2}}}\right)$$

queries to U_{A^*}. Fixing $c := 1/2$, the above is $\Omega\left(2^{n/4}\right)$. □

Since the verifier V_A is projective, we can now combine Corollary 5.3 with Theorem 3.5 to obtain the following "amplified" lower bound.

Corollary 5.4 (Lower Bound for High-Error Counterfeiting)**.** *Let $1/\varepsilon = o\left(2^{n/2}\right)$. Given one copy of $|A\rangle$, as well as oracle access to U_{A^*}, a counterfeiter needs $\Omega\left(\sqrt{\varepsilon}2^{n/4}\right)$ queries to prepare a state ρ such that $\langle A|^{\otimes 2}\rho\,|A\rangle^{\otimes 2} \geq \varepsilon$ (for a worst-case $|A\rangle$).*

Proof. Suppose we have a counterfeiter C that makes $o\left(\sqrt{\varepsilon}2^{n/4}\right)$ queries to U_{A^*}, and prepares a state σ such that $\langle A|^{\otimes 2}\sigma\,|A\rangle^{\otimes 2} \geq \varepsilon$. Let $\delta := 0.00001$. Then by Theorem 3.5, there exists an amplified counterfeiter C' that makes

$$O\left(\frac{\log 1/\delta}{\sqrt{\varepsilon}\left(\sqrt{\varepsilon}+\delta^2\right)}\right) = O\left(\frac{1}{\sqrt{\varepsilon}}\right)$$

calls to C and V_A, and that prepares a state ρ such that $\langle A|^{\otimes 2}\rho\,|A\rangle^{\otimes 2} \geq 1-\delta$. Now, counting the $o\left(\sqrt{\varepsilon}2^{n/4}\right)$ queries from each C invocation and $O(1)$ queries from each V_A invocation, the total number of queries that C' makes to U_{A^*} is

$$\left[o\left(\sqrt{\varepsilon}2^{n/4}\right) + O(1)\right]\cdot O\left(\frac{1}{\sqrt{\varepsilon}}\right) = o\left(2^{n/4}\right).$$

But this contradicts Corollary 5.3. □

So far, we have only made statements about the *worst* case for a would-be counterfeiter. But such guarantees are clearly not enough: it could be that *most* money states $|A\rangle$ are easy to duplicate, without contradicting any of the results we have seen so far.

We will show that the problem faced by a counterfeiter is *random self-reducible*: if a counterfeiter could duplicate a uniformly-random money state $|A\rangle$, then it could duplicate *any* $|A\rangle$. Thus the bank can ensure security by creating uniformly-random money states.

In what follows, let $\mathcal{S}$ be the set of all subspaces $A \leq \mathbb{F}_2^n$ such that $\dim A = n/2$. Also, let $V_A^{\otimes 2} = (|A\rangle\langle A|)^{\otimes 2}$ be the projector onto $|A\rangle^{\otimes 2}$.

Theorem 5.5 (Lower Bound for Average-Case Counterfeiting)**.** *Let $A \leq \mathbb{F}_2^n$ be a uniformly-random element of $\mathcal{S}$. Then given one copy of $|A\rangle$, as well as oracle access to U_{A^*}, a counterfeiter C needs $\Omega\left(\sqrt{\varepsilon}2^{n/4}\right)$ queries to prepare a $2n$-qubit state ρ that $V_A^{\otimes 2}$ accepts with probability at least ε, for all $1/\varepsilon = o\left(2^{n/2}\right)$. Here the probability is taken over the choice of $A \in \mathcal{S}$, as well as the behavior of C and $V_A^{\otimes 2}$.*

Proof. Suppose we had a counterfeiter C that violated the above. Using C as a black box, we will show how to construct a new counterfeiter C' that violates Corollary 5.4.

Given a (deterministically-chosen) money state $|A\rangle$ and oracle access to U_{A^*}, first choose an invertible linear map $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ uniformly at random. Then $f(A)$, the image of A under f, is a uniformly-random element of $\mathcal{S}$. Furthermore, the state $|A\rangle$ can be transformed into $|f(A)\rangle$ straightforwardly, the oracle $U_{f(A)}$ can be simulated by composing f with U_A, and the oracle $U_{f(A)^\perp}$ can likewise be simulated by composing f^{-T} with U_A (where f^{-T} denotes the inverse transpose of f). So by using the counterfeiter C for uniformly-random states, we can produce a state ρ_f that $V_{f(A)}^{\otimes 2}$ accepts with probability at least ε. By applying f^{-1} to both registers of ρ_f, we can then obtain a state ρ that $V_A^{\otimes 2}$ accepts with probability at least ε, thereby contradicting Corollary 5.4. □

We are now ready to prove security for the "final" mini-scheme $\mathcal{M}$ defined in Section 5.2.

Theorem 5.6 (Security of Mini-Scheme). *The mini-scheme $\mathcal{M} = (\mathsf{Bank}_{\mathcal{M}}, \mathsf{Ver}_{\mathcal{M}})$, which is defined relative to the classical oracle U, has perfect completeness and $1/\exp(n)$ soundness error.*

Proof. That $\mathcal{M}$ has perfect completeness follows from its definition and from Lemma 5.1. That $\mathcal{M}$ has $1/\exp(n)$ soundness error *essentially* follows from Theorem 5.5. We only need to show that, given a banknote of the form $|\$_r\rangle = |s_r\rangle|A_r\rangle$, a polynomial-time counterfeiter C can gain no additional advantage by querying the "full" oracles $\mathcal{G}, \mathcal{H}, \mathcal{T}_{\text{primal}}, \mathcal{T}_{\text{dual}}$, beyond what it gains from querying $U_{A_r^*} = (U_{A_r}, U_{A_r^\perp})$.

Let $r \in \{0,1\}^n$ be the random string chosen by the bank, so that $\mathcal{G}(r) = (s_r, \langle A_r\rangle)$. Then observe that, even conditioned on s_r and A_r, as well as complete descriptions of $\mathcal{T}_{\text{primal}}, \mathcal{T}_{\text{dual}}$, and $\mathcal{H}$, the string r remains uniformly random. Nor can querying $\mathcal{G}(r')$ for $r' \neq r$ reveal any information about r, since the values of $\mathcal{G}$ are generated independently. So suppose we *modify* $\mathcal{G}$ by setting $\mathcal{G}(r) := (s', \langle A'\rangle)$, for some new $3n$-bit serial number s' and list of generators $\langle A'\rangle$ chosen uniformly at random. Then the BBBV hybrid argument [13] tells us that, in expectation over r, this can alter the final state output by the counterfeiter $C(|\$_r\rangle)$ by at most $\operatorname{poly}(n)/2^{n/2}$ in trace distance. So in particular, if C succeeded with non-negligible probability before, then C must *still* succeed with non-negligible probability after we set $\mathcal{G}(r) := (s', \langle A'\rangle)$.

However, once we make this modification, an adversary trying to counterfeit $|A\rangle$ given U_A and $U_{A^\perp}$ can easily "mock up" a serial number s, as well as the oracles$\mathcal{G}, \mathcal{H}, \mathcal{T}_{\text{primal}}$ and $\mathcal{T}_{\text{dual}}$, for itself. For s, $\mathcal{G}$, and $\mathcal{H}$ are now drawn from a distribution completely independent of A. The oracles $\mathcal{T}_{\text{primal}}$ and $\mathcal{T}_{\text{dual}}$ are likewise independent of A, *except* that $\mathcal{T}_{\text{primal}}|s\rangle|v\rangle = |s\rangle U_A|v\rangle$ and $\mathcal{T}_{\text{dual}}|s\rangle|v\rangle = |s\rangle U_{A^\perp}|v\rangle$—behaviors that an adversary can easily simulate using U_A and $U_{A^\perp}$, together with its knowledge of s. Just like in Corollary 3.8, since our security guarantees are query complexity bounds, we do not care about the *computational* complexity of creating the mock-ups.

By using the mock-ups, one can convert any successful attack on $\mathcal{M}$ into successful counterfeiting of $|A\rangle$, given oracle access to U_A and $U_{A^\perp}$ only. But the latter contradicts Theorem 5.5. □

Finally, using Theorem 5.6 together with Corollary 3.8, we can obtain a secure public-key quantum money scheme, relative to a classical oracle.

Theorem 5.7 (Security of Hidden Subspace Money)**.** *By combining the mini-scheme* $\mathcal{M}$ *with a digital signature scheme, it is possible to construct a public-key quantum money scheme*

$$\mathcal{S} = (\mathsf{KeyGen}_{\mathcal{S}}, \mathsf{Bank}_{\mathcal{S}}, \mathsf{Ver}_{\mathcal{S}}) ,$$

defined relative to some classical oracle U'*, which has perfect completeness and* $1/\exp(n)$ *soundness error.*

6 Explicit quantum money scheme

We have shown how to construct a provably-secure public-key quantum money scheme, when an appropriate classical oracle is available. In this section, we propose a way to obtain the same functionality without an oracle. The key challenge is this:

> *Given a subspace* $A \le \mathbb{F}_2^n$*, how can a bank distribute an "obfuscated program"* P_A*, which legitimate buyers and sellers can use to decide membership in both* A *and* $A^\perp$*, but which does not reveal anything else about* A *that might facilitate counterfeiting?*

Note that, aside from the detail that we need security against quantum adversaries, the above challenge is purely "classical"; it and its variants seem interesting even apart from our quantum money application.

We will suggest a candidate protocol to achieve the challenge, based on *multivariate polynomial cryptography*. Given a collection $p_1, \ldots, p_m : \mathbb{F}_2^n \to \mathbb{F}_2$ of multivariate polynomials over $\mathbb{F}_2$, it is generally hard to find a point $v \in \mathbb{F}_2^n$ on which all of vanish. On the other hand, it is easy to check whether a *particular* point v has that property. To "hide" a subspace A, we will provide uniformly-random low-degree polynomials $p_1, \ldots, p_m$ that vanish on each point of A. This information is sufficient to decide membership in A. On the other hand, there is no known efficient algorithm to *find* A given the polynomials, and current techniques seem unlikely to yield even a quantum algorithm.

We can also introduce a constant fraction of *noise* into our scheme without interfering with its completeness. In other words, if only $(1-\varepsilon)\,m$ of the polynomials $p_1, \ldots, p_m$ are chosen to vanish on A, and the remaining εm are random, then counting the p_i that vanish at a point v still suffices to determine whether $v \in A$. Although we know of no attack even against our noise-free scheme, adding noise in this way might improve security.

Crucially, we will state a "classical" conjecture about the security of multivariate polynomial cryptography, and show that the conjecture *implies* the security of our explicit money scheme. For the benefit of cryptographers, let us now state an "abstract" version of our conjecture, which implies what we need, and which might hold even if our concrete conjecture about multivariate polynomials fails.

Conjecture 6.1 (Subspace-Hiding Conjecture, Sufficient for Quantum Money)**.** *There exists a polynomial-time algorithm that takes as input a description of a uniformly-random subspace* $A \le \mathbb{F}_2^n$ *with* $\dim(A) = n/2$*, and that outputs circuits* C_A *and* $C_{A^\perp}$*, such that the following holds.*

(i) $C_A(v)$ *decides whether* $v \in A$*, and* $C_{A^\perp}(v)$ *decides whether* $v \in A^\perp$*, for all* $v \in \mathbb{F}_2^n$*.*

(ii) Given descriptions of C_A *and* $C_{A^\perp}$*, no polynomial-time quantum algorithm can find a generating set for* A *with success probability* $\Omega\left(2^{-n/2}\right)$*.*

Later, Conjecture 6.7 will specialize Conjecture 6.1 to the setting of multivariate polynomials.

6.1 Useful facts about polynomials

By viewing elements of $\mathbb{F}_2^n$ as n-tuples $(x_1,\ldots,x_n)$, we can evaluate a polynomial $p(x_1,\ldots,x_n)$ on points of $\mathbb{F}_2^n$.

Given a subspace $A \le \mathbb{F}_2^n$ and a positive integer d, let $\mathcal{I}_{d,A}$ be the set of degree-d polynomials (not necessarily homogeneous) that vanish on A. Since we are working over $\mathbb{F}_2$, note that $x_i^2 = x_i$, so it suffices to consider *multilinear* polynomials (in which no x_i is ever raised to a higher power than 1).

Before presenting our scheme, we need to establish some basic properties of polynomials over $\mathbb{F}_2^n$. First, we observe that the set of polynomials does not depend on the choice of basis.

Proposition 6.2. *Let L be any invertible linear transformation on $\mathbb{F}_2^n$. Then the map $p(v) \mapsto p(Lv)$ defines a permutation on the set of degree-d polynomials, which maps $\mathcal{I}_{d,A}$ to $\mathcal{I}_{d,L^{-1}A}$.*

Implementing our scheme will require sampling uniformly from $\mathcal{I}_{d,A}$, which the next lemma shows is possible.

Lemma 6.3. *It is possible to sample a uniformly-random element of $\mathcal{I}_{d,A}$ in time $O(n^d)$.*

Proof. By Proposition 6.2, we can instead sample from the space of polynomials which vanish on span$\left(x_1,\ldots,x_{n/2}\right)$, and then apply an appropriate change of basis to obtain a sample from $\mathcal{I}_{d,A}$. So assume without loss of generality that $A = \operatorname{span}(x_1,\ldots,x_{n/2})$.

We claim that a polynomial p vanishes on A if and only if every monomial of p intersects the set $\{x_{n/2+1},\ldots,x_n\}$. This will immediately give an $O\left(n^d\right)$-time sampling algorithm, because we can consider each of the $O\left(n^d\right)$ degree-d monomials in turn, and include each one independently with probability $1/2$ if it intersects $\{x_{n/2+1},\ldots,x_n\}$.

To prove the claim: first, if every monomial intersects $\{x_{n/2+1},\ldots,x_n\}$, then clearly p vanishes on A. Otherwise, let m be a minimal monomial that does *not* intersect $\{x_{n/2+1},\ldots,x_n\}$. Consider the vector $v = (v_1,\ldots,v_n)$ with $v_i = 1$ if and only if $x_i \in m$. Since m does not intersect $\{x_{n/2+1},\ldots,x_n\}$, clearly $v \in A$. Also, since m is minimal, every other monomial must evaluate to 0 on v. Thus $p(v) = m(v) = 1$, so p is not identically zero on A. □

In addition to sampling polynomials that vanish on A, we would like to guarantee that a sufficiently large system of such polynomials uniquely determines the space A, so that such a system can be effectively used as a membership oracle.

Lemma 6.4. *Fix $A \le \mathbb{F}_2^n$ and $\beta > 1$, and choose βn polynomials $p_1,\ldots,p_{\beta n}$ uniformly and independently from $\mathcal{I}_{d,A}$. Let Z be the set of $v \in \mathbb{F}_2^n$ such that $p_i(v) = 0$ for all $i \in [\beta n]$. Then $A \subseteq Z$, and* $\Pr[Z = A] = 1 - 2^{-\Omega(n)}$.

Proof. $A \subseteq Z$ is clear. For the probabilistic part, fix a point $v \notin A$. Then by the union bound, it suffices to show that $\Pr[v \in Z] < c^{-n}$ for some $c > 2$.

There must be some $w \in A^{\perp}$ such that $w \cdot v = 1$. Then the map $p(v) \mapsto p(v) + w \cdot v$ defines an involution of $\mathcal{I}_{d,A}$, such that exactly one of $p(v)$ and $p(v) + w \cdot v$ is zero. This means that exactly half of the polynomials in $\mathcal{I}_{d,A}$ vanish at v. Hence

$$\Pr\left[p_1(v) = \cdots = p_{\beta n}(v) = 0\right] = 2^{-\beta n}$$

and we are done. □

As mentioned earlier, we would also like to allow sampling from *noisy* systems of equations, defined as follows: let $\mathcal{R}_{d,A,m,\varepsilon}$ be the probability distribution over m-tuples $(p_1,\ldots,p_m)$ that sets exactly $(1-\varepsilon)m$ of the polynomials p_i (chosen uniformly at random) to be uniformly-random samples from $\mathcal{I}_{d,A}$, and that sets the remaining εm of the polynomials p_i to be uniformly-random samples from $\mathcal{I}_{d,A'}$, for a uniformly-random subspace $A' \leq \mathbb{F}_2^n$ of dimension $\dim(A)$. (Note that a *different* A' is chosen for every such p_i.) Then using a Chernoff bound, it is not hard to show that, provided m is large enough compared to n, a sample from $\mathcal{R}_{d,A,m,\varepsilon}$ *also* uniquely defines the subspace A with overwhelming probability.

Lemma 6.5. *Fix $A \leq \mathbb{F}_2^n$ and $\varepsilon < 1/2$, let $\beta \geq 3/(1-2\varepsilon)^2$, and choose polynomials $p_1,\ldots,p_{\beta n}$ from $\mathcal{R}_{d,A,\beta n,\varepsilon}$. Let $w(v) := \sum_{i=1}^{\beta n} p_i(v)$, and let Z be the set of $v \in \mathbb{F}_2^n$ such that $w(v) \leq \varepsilon\beta n$. Then $A \subseteq Z$, and* $\Pr[Z = A] = 1 - 2^{-\Omega(n)}$.

Proof. Again, $A \subseteq Z$ is clear. For the probabilistic part, fix $v \notin A$. Then by the union bound, it suffices to show that $\Pr[v \in Z] < \alpha^{-n}$ for some $\alpha < 1/2$.

Observe that v is a zero of little more than half the polynomials $p_1,\ldots,p_{\beta n}$. If p_i was chosen to vanish on A, then $\mathrm{E}[p_i(v)] = 1/2$, by the argument of Lemma 6.4. If p_i was chosen to vanish on a uniformly-random A', then

$$\begin{aligned}\mathrm{E}[p_i(v)] &\geq \frac{1}{2} - \Pr[v \in A'] \\ &= \frac{1}{2} - \frac{1}{2^{n/2}}.\end{aligned}$$

Hence

$$\mathrm{E}\left[p_1(v) + \cdots + p_{\beta n}(v)\right] \geq \beta n \left(\frac{1}{2} - \frac{1}{2^{n/2}}\right).$$

Furthermore, the p_i are chosen independently, up to an irrelevant ordering. Choose $\delta = 1 - 2\varepsilon$ to satisfy $(1-\delta)/2 = \varepsilon$. Then by a Chernoff bound,

$$\begin{aligned}\Pr[v \in Z] &= \Pr\left[p_1(v) + \cdots + p_{\beta n}(v) \leq \varepsilon\beta n\right] \\ &\leq \exp\left(-\frac{1}{2}\frac{\beta n}{2}\left(1 - \frac{2}{2^{n/2}}\right)\delta^2\right) \\ &\leq \exp\left(-\frac{3n}{4}\left(1 - \frac{2}{2^{n/2}}\right)\right) \\ &< 0.48^n\end{aligned}$$

for large enough n, and we are done. □

6.2 Explicit hidden-subspace mini-scheme

In our explicit mini-scheme, the bank chooses a subspace A randomly and publishes sets of polynomials drawn from $\mathcal{R}_{d,A,\beta n,\varepsilon}$ and $\mathcal{R}_{d,A^{\perp},\beta n,\varepsilon}$, along with the quantum money state $|A\rangle$. By Lemma 6.5, a user can use these polynomials to test membership in A and $A^{\perp}$, and can therefore implement the oracle mini-scheme in Section 5.1.

Formally, the mini-scheme $\mathcal{E}$ is defined as follows. Parameters $\varepsilon \in [0,1/2)$, $\beta \geq 3/(1-2\varepsilon)^2$, and $d \geq 4$ are fixed. The complexity of the verification procedure will grow like $O\left(\beta n^{d+1}\right)$, but security might also improve for larger ε and d. Then:

- $\mathsf{Bank}(0^n)$ selects an $n/2$-dimensional subspace $A \leq \mathbb{F}_2^n$ uniformly at random, say by selecting $n/2$ random linearly-independent generators. It then sets $s := (s_A, s_{A^\perp})$, where s_A and $s_{A^\perp}$ are lists of polynomials drawn from $\mathcal{R}_{d,A,\beta n,\varepsilon}$ and $\mathcal{R}_{d,A^\perp,\beta n,\varepsilon}$ respectively. It prepares the money state $|A\rangle$ and outputs the banknote $|\$_s\rangle := |s\rangle\,|A\rangle$.
- $\mathsf{Ver}(\cent)$ first checks that $\cent$ has the form $(s_A, s_{A^\perp}, \rho)$ where $s_A = \left(p_1,\ldots,p_{\beta n}\right)$ and $s_{A^\perp} = \left(q_1,\ldots,q_{\beta n}\right)$ are lists of βn polynomials over $\mathbb{F}_2^n$. If not, it rejects. If so, then it defines Z and $Z^\perp$ to be the sets of points $v \in \mathbb{F}_2^n$ such that
$$\sum_{i=1}^{\beta n} p_i(v) \leq \varepsilon\beta n \quad \text{and} \quad \sum_{i=1}^{\beta n} q_i(v) \leq \varepsilon\beta n$$
respectively. (Recall that with overwhelming probability, $Z = A$ and $Z^\perp = A^\perp$. Also, while Ver will not have explicit listings of the exponentially-large sets Z and $Z^\perp$, all that matters for us is that it can efficiently apply the projections $\mathbb{P}_Z$ and $\mathbb{P}_{Z^\perp}$.) It then applies the operation $V_Z := H_2^{\otimes n}\mathbb{P}_{Z^\perp}H_2^{\otimes n}\mathbb{P}_Z$ to ρ, and accepts $\cent$ if and only if $V_Z(\rho)$ accepts.

6.3 Analysis

We first observe that the mini-scheme $\mathcal{E}$ has perfect completeness.

Theorem 6.6. *$\mathcal{E}$ has perfect completeness.*

Proof. This follows from Lemmas 6.4 and 6.5, and particularly from the fact that $A \subseteq Z$ and $A^\perp \subseteq Z^\perp$ with certainty. From this it follows that $V_Z := H_2^{\otimes n}\mathbb{P}_{Z^\perp}H_2^{\otimes n}\mathbb{P}_Z$ accepts the state $|A\rangle$ with probability 1. □

Let us remark that, if we want the fraction ε of "decoy" polynomials to be even greater than $1/2$, then we can define a variant of our scheme that works for all $\varepsilon < 1$. In this variant scheme, Ver will guess that $v \in A$ (i.e., put $v \in Z$) if
$$p_1(v) + \cdots + p_{\beta n}(v) \leq \frac{(1+\varepsilon)\beta n}{4},$$
and will guess that $v \notin A$ (i.e., put $v \notin Z$) otherwise. By direct analogy with Lemma 6.5, one can prove using a Chernoff bound that this rule will guarantee $\Pr[Z = A] = 1 - 2^{-\Omega(n)}$, and likewise $\Pr\left[Z^\perp = A^\perp\right] = 1 - 2^{-\Omega(n)}$, provided we set $\beta \geq 12/(1-\varepsilon)^2$. However, the disadvantage is that if $\varepsilon \geq 1/3$, then we lose the property that $A \subseteq Z$ and $A^\perp \subseteq Z^\perp$ with probability 1, since $\varepsilon \geq (1+\varepsilon)/4$. This means, in particular, that we lose perfect completeness, and can only ensure a completeness error of $2^{-\Omega(n)}$.

We now wish to argue about $\mathcal{E}$'s soundness. Naturally, we can only hope to prove soundness assuming some computational hardness conjecture. What is nice, though, is that we can base $\mathcal{E}$'s soundness on a conjecture that talks only about the hardness of a "classical" cryptographic problem (i.e., a problem with classical inputs and outputs). Let us now state that conjecture, which is simply the abstract Conjecture 6.1 specialized to the setting of multivariate polynomials.

Conjecture 6.7 (Direct Product for Finding Subspace Elements)**.** *Let $\varepsilon < 1/2$ and $\beta := 3/(1-2\varepsilon)^2$. Given samples from $\mathcal{R}_{d,A,\beta n,\varepsilon}$ and $\mathcal{R}_{d,A^\perp,\beta n,\varepsilon}$, no polynomial-time quantum algorithm can find a complete list of generators for A with success probability $\Omega(2^{-n/2})$.*

Note that it is easy to find *one* nonzero element of A with success probability $2^{-n/2}$, by choosing $x \in \mathbb{F}_2^n$ randomly. Conjecture 6.7 asserts both that it is impossible to do too much better using $\mathcal{R}_{d,A,\beta n,\varepsilon}$ and $\mathcal{R}_{d,A^\perp,\beta n,\varepsilon}$, and that finding multiple elements of A is significantly harder than finding one element.

The security of mini-scheme $\mathcal{E}$ follows easily from Conjecture 6.7, *despite* the fact that a would-be counterfeiter has access to a valid quantum banknote, whereas Conjecture 6.7 involves no such assumption.

Theorem 6.8 (Security Reduction for Explicit Mini-Scheme)**.** *If Conjecture 6.7 holds, then $\mathcal{E}$ is secure.*

Proof. Let $C_{\mathcal{E}}$ be a counterfeiter against $\mathcal{E}$. Then we need to show that, using $C_{\mathcal{E}}$, we can find a complete list of generators for A with $\Omega\left(2^{-n/2}\right)$ success probability.

Given $A \le \mathbb{F}_2^n$ with $\dim(A) = n/2$, let $s := (s_A, s_{A^\perp})$ where s_A and $s_{A^\perp}$ are samples from $\mathcal{R}_{d,A,\beta n,\varepsilon}$ and $\mathcal{R}_{d,A^\perp,\beta n,\varepsilon}$ respectively. Recall from Lemma 6.5 that $\Pr[A = Z] = 1 - 2^{-\Omega(n)}$ and $\Pr\left[A^\perp = Z^\perp\right] = 1 - 2^{-\Omega(n)}$. Provided both of these events occur, we can use s to decide membership in A, and can therefore apply the projective measurement $\mathbb{P}_A$. So let us prepare the uniform superposition over all 2^n elements of $\mathbb{F}_2^n$, and then apply $\mathbb{P}_A$ to it. With probability $2^{-n/2}$, this produces the state $|A\rangle$.

Once we have s and $|A\rangle$, we can then form the banknote $|\$\rangle := |s\rangle\,|A\rangle$, and provide this banknote to the counterfeiter $C_{\mathcal{E}}$. By hypothesis, $C_{\mathcal{E}}$ outputs a (possibly-entangled) state ρ on two registers, such that $\langle A|^{\otimes 2}\rho\,|A\rangle^{\otimes 2} \ge \Delta$ for some $\Delta = \Omega(1/\operatorname{poly}(n))$. But now, because the mini-scheme $\mathcal{E}$ is projective, Theorem 3.5 applies, and we can *amplify* ρ to increase its fidelity with $|A\rangle^{\otimes 2}$. After $O(\log(n)/\Delta^2)$ calls to $C_{\mathcal{E}}$, this gives us a state σ such that

$$\langle A|^{\otimes 2}\,\sigma\,|A\rangle^{\otimes 2} \ge 1 - \frac{1}{n^2}\,.$$

More generally, by alternating counterfeiting steps and amplification steps, we can produce as many registers as we like that each have large overlap with $|A\rangle$. In particular, we can produce a state ξ such that

$$\langle A|^{\otimes n}\,\xi\,|A\rangle^{\otimes n} \ge 1 - o(1)\,.$$

If we now run Ver on each of the registers of ξ, the probability that every invocation accepts is $1 - o(1)$. Furthermore, supposing that happens, the state we are left with is simply $|A\rangle^{\otimes n}$.

Finally, we measure each register of $|A\rangle^{\otimes n}$ in the standard basis. This gives us n elements $x_1,\ldots,x_n \in A$, which are independent and uniformly random. So by standard estimates, the probability that $x_1,\ldots,x_n$ do *not* contain a complete generating set for A is $1/\exp(n)$.

Overall, the procedure above succeeded with probability $2^{-n/2}(1 - o(1))$, thereby giving us the desired contradiction with Conjecture 6.7. □

Using the standard construction of quantum money schemes, we can now produce a complete explicit money scheme, whose security follows from Conjecture 6.7.

Theorem 6.9 (Security Reduction for Explicit Scheme)**.** *Assuming Conjecture 6.7, there exists a public-key quantum money scheme with perfect completeness and soundness error* $2^{-\Omega(n)}$.

Proof. We apply the standard construction of Theorem 3.6 with the mini-scheme $\mathcal{E}$, whose completeness and soundness follow from Theorems 6.6 and 6.8 respectively, assuming Conjecture 6.7. □

6.4 Justifying our hardness assumption

Though our hardness assumption is new, it is closely related to standard assumptions in *multivariate polynomial cryptography*. Given a system of multivariate quadratics over $\mathbb{F}_2$, finding a common zero is known to be NP-hard; moreover, it is strongly believed that the problem remains hard even for *random* systems of multivariate polynomials, and cryptosystems based on this hardness assumption are considered promising candidates for post-quantum cryptography [22]. Therefore, if Conjecture 6.7 fails, it will almost certainly be because some additional structure in this problem facilitates a new attack.

There are several ways in which Conjecture 6.7 is stronger than the assumption that solving random systems of multivariate polynomials is hard. First, our systems have large, well-structured solution spaces A and $A^{\perp}$. Systems with many solutions are not normally considered in the literature, and while there seem to be no known attacks that exploit this structure, the possibility is not ruled out. Second, we provide two related systems, one with zeroes in A and one with zeroes in $A^{\perp}$. Again, this is a very specific structural property which has not been considered, and there might be unexpected attacks exploiting it. Third, Conjecture 6.7 asserts that no adversary can succeed with probability $2^{-n/2}$, which seems significantly easier than succeeding with non-negligible probability.

On the other hand, Conjecture 6.7 is *weaker* than typical assumptions in multivariate polynomial cryptography in at least one respect: a would-be counterfeiter needs to solve a system of polynomial equations with a constant fraction of noise. Solving noisy systems of *linear* equations over $\mathbb{F}_2$ is called the *learning parity with noise* problem, and is generally believed to be hard even for quantum computers [39]. If true, this suggests that Gaussian elimination is fundamentally hard to adapt to the presence of noise. But computing a Gröbner basis is a strict generalization of Gaussian elimination to higher degree, and involves a nearly identical process of elimination. It therefore seems unlikely that these approaches can be efficiently adapted to the setting with noise. The problem of solving polynomials with noise has been studied recently, and the best-known approaches involve performing an exponential time search to determine which equations are noisy [7].

But if solving linear systems with noise is already hard, why do we even use higher-degree polynomials in our scheme? The reason is that, alas, the "dual" structure of our money scheme facilitates a simple attack in the case $d = 1$.

Claim 6.10. *For all* $\varepsilon < 1/2$*, there exists a* β *such that one can recover A efficiently given samples from* $\mathcal{R}_{d,A,\beta n,\varepsilon}$ *and* $\mathcal{R}_{d,A^{\perp},\beta n,\varepsilon}$.[19]

Proof. Let $p_1, \ldots, p_m$ and $q_1, \ldots, q_m$ be homogeneous linear polynomials, of which a $1-\varepsilon$ fraction vanish on A and $A^{\perp}$ respectively. Then the key observation is that each p_i vanishes on A if and only if it has the form $p_i(v) = u_i \cdot v$ for some $u_i \in A^{\perp}$, while each q_i vanishes on $A^{\perp}$ if and only if it has the

[19] This claim also goes through, with no essential changes, for the variant of our scheme discussed earlier with $\varepsilon \in [1/2, 1)$ (i.e., the variant without perfect completeness).

form $q_i(v) = w_i \cdot v$ for some $w_i \in A$. But by Lemma 6.5, if $\beta > 3/(1-2\varepsilon)^2$, then for each $i \in [m]$, we can efficiently *decide* whether $u_i \in A^\perp$ by counting those values j for which $q_j(u_i) = 0$, and can likewise decide whether $w_i \in A$ by counting those values j for which $p_j(w_i) = 0$. Thus we can learn $\Theta(n)$ random elements of A or $A^\perp$, and thereby recover a basis for A. □

There *might* be a more sophisticated attack for higher degrees, but this is suggested only weakly by the existence of an attack in the linear case. Indeed, the relation between the complementary linear subspaces A and $A^\perp$ is precisely the sort of structure that should be preserved by linear maps, but *not* by higher-degree polynomials!

For degree-2 polynomials, it is possible to obtain a similar attack which recovers A from only a *single* sample. This attack relies on the observation that quadratics have an easily-computed canonical form [18], from which a basis for A can be extracted in polynomial time. The essential problem is that quadratic polynomials are very closely related to bilinear forms, and that powerful methods from linear algebra can therefore be applied to them.

Fortunately, the linear structure seems to be computationally obscured when $d \geq 3$. This phenomenon is related to the sharp discontinuity in the difficulty of tensor problems with order 3 and higher. More concretely, the coefficients of a degree-d polynomial can be viewed as the entries of an order-d tensor, and the existence of an attack in the degree $d = 2$ case corresponds to the possibility of efficient operations on order-2 tensors. Basic operations on order-3 tensors are NP-hard [28], however, and this suggests that analogous attacks might not exist against degree-3 polynomials.

This state of affairs is reflected in existing attacks on a standard cryptographic assumption called *polynomial isomorphism with one secret*. Here we are given two polynomials p, q which are related by an unknown linear change of coordinates L, and the task is to find such an L. For degree-2 polynomials, this problem can be easily solved in polynomial time [18], but already for degree-3 polynomials the best known attacks take exponential time [38, 26, 18]. However, if an attacker is given n bits of partial information about the linear transformation, then even in the $d = 3$ case, it becomes possible to find the linear transformation that relates the polynomials [18]. This does *not* directly facilitate an attack on our assumption, but it suggests that a similar attack *might* be possible when $d = 3$, since an attacker is only required to succeed with $2^{-n/2}$ probability. Fortunately, this attack seems to rely on the particular structure of degree 2 and 3 polynomials. Of course it is possible that similar algorithms may be discovered for higher-degree polynomials, but this would represent an advance in algebraic cryptanalysis.

7 Private-key quantum money

Recall that a *private-key* quantum money scheme is one where only the bank itself is able to verify banknotes, using an n-bit key $k = k_{\text{private}} = k_{\text{public}}$ that it keeps a closely-guarded secret. Compensating for this disadvantage, private-key schemes are known with much stronger security guarantees than seem possible for public-key schemes.

In particular, as mentioned in Section 1.1, already forty years ago Wiesner [42] described how to create private-key quantum money that is *information-theoretically secure*. In Wiesner's scheme, each banknote consists of n unentangled qubits together with a classical serial number s. Wiesner's scheme also requires a giant database of serial numbers maintained by the bank, or in our setting, access to a random oracle R. But in followup work, BBBW [15] pointed out that we can replace R by any *pseudorandom function family* $\{f_k\}_k$, to obtain a private-key quantum money scheme that is computationally secure, *unless* a polynomial-time algorithm can distinguish the f_k from random functions.

Strangely, we are unaware of any rigorous proof of the security of Wiesner's scheme until recently. However, answering a question by one of us,[20] Molina, Vidick and Watrous [33] have now supplied the key ingredient for a security proof. Specifically they show that, if a counterfeiter tries to copy an n-qubit banknote $|\$\rangle$ in Wiesner's scheme, then the output can have squared fidelity at most $(3/4)^n$ with $|\$\rangle^{\otimes 2}$. (They also show that this is tight: there *exists* a non-obvious counterfeiting strategy that succeeds with $(3/4)^n$ probability.)

To complete the security proof, one needs to show that, even given q banknotes $|\$_1\rangle, \ldots, |\$_q\rangle$, a counterfeiter cannot prepare an additional banknote with non-negligible probability (even with a new serial number). In a forthcoming paper [4], we will show how to adapt the methods of Section 3 to prove that claim. Briefly, one can first define a notion of *private-key mini-schemes*, in close analogy to public-key mini-schemes. The work of Molina et al. [33] then directly implies the security of what we call the "Wiesner mini-scheme." Next, one can give a general reduction, showing how to construct a full-blown private-key quantum money scheme $\mathcal{S}$ starting from

(1) any private-key *mini*-scheme $\mathcal{M}$, and

(2) any random or pseudorandom function family R.

Though the details turn out to be more complicated in the private-key case, the proof of correctness for this reduction is conceptually similar to the proof of Theorem 3.6. Namely, one shows that any counterfeiter would yield *either* a break of the underlying mini-scheme $\mathcal{M}$, or *else* a way to distinguish R from a random function. Notice that the analysis is completely unified: if R is a "true" random oracle, then we get information-theoretic security (as in Wiesner's scheme), while if R is pseudorandom, then we get computational security (as in the BBBW scheme).

Unfortunately, as pointed out by Lutomirski [30] and Aaronson [3], the Wiesner and BBBW schemes both have a serious security hole. Namely, suppose a counterfeiter C can repeatedly submit alleged banknotes to a "naïve and trusting bank" for verification. Given a quantum state σ, such a bank not only tells C whether the verification procedure accepted or rejected, but also, in either case, *gives the post-measurement state* $\widetilde{\sigma}$ *back to* C. Then starting from a single valid banknote $|\$\rangle$, we claim that C can recover a complete classical description of $|\$\rangle$, using $O(n \log n)$ queries to the bank. Once it has such a description, C can of course prepare as many copies of $|\$\rangle$ as it likes.

The attack is simple: let $|\$\rangle = |\theta_1\rangle \cdots |\theta_n\rangle$ (we omit the classical serial number s, since it plays no role here). Then for each $i \in [n]$, the counterfeiter tries "swapping out" the i^{th} qubit $|\theta_i\rangle$ and replacing it with $|b\rangle$, for each of the four possibilities $|b\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. It then uses $O(\log n)$ queries to the bank, to estimate the probability that the state $|\theta_1\rangle \cdots |\theta_{i-1}\rangle |b\rangle |\theta_{i+1}\rangle \cdots |\theta_n\rangle$ passes the verification test. By doing so, C can learn a correct value of $|\theta_i\rangle$ with success probability $1 - o(1/n)$. The crucial point is that none of these queries damage the qubits *not* being investigated ($|\theta_j\rangle$ for $j \neq i$), since the bank measures those qubits in the correct bases. Therefore C can reuse the same banknote for each query.

[20]See http://theoreticalphysics.stackexchange.com/questions/370/rigorous-security-proof-for-wiesners-quantum-money

More generally, recall from Section 3.1 that we call a private-key quantum money scheme *query-secure*, if it remains secure even assuming the counterfeiter C can make adaptive queries to $\mathsf{Ver}(k,\cdot)$. Then we saw that the Wiesner and BBBW schemes are *not* query-secure. Recently, Farhi et al. [23] proved a much more general "no-go" theorem—which says intuitively that, if we want query-secure quantum money, then the banknotes *must* hide information in the "global correlations" between large numbers of qubits.

Theorem 7.1 (Adaptive Attack on Wiesner-Like Schemes [23])**.** *No quantum money scheme can be query-secure, if*

(i) the banknotes have the form $|\$_s\rangle = |s\rangle |\psi_s\rangle$,

(ii) verification of (s,ρ) *consists of projecting* ρ *onto* $|\psi_s\rangle\langle\psi_s|$, *and*

(iii) $|\psi_s\rangle$ *can be reconstructed uniquely from the statistics of* $T = \mathrm{poly}(n)$ *efficiently-implementable measurements* $M_1,\ldots,M_T$, *each of which has at most* $\mathrm{poly}(n)$ *possible outcomes.*

On the positive side, any *public-key* quantum money scheme—for example, our multivariate polynomial scheme from Section 6—immediately yields a query-secure scheme with the same security guarantee. This is because a counterfeiter who knows the code of Ver can easily simulate oracle access to Ver. But can we do any better than that, and construct a query-secure money scheme whose security is *unconditional* (as in Wiesner's scheme), or else based on a pseudorandom function (as in the BBBW scheme)?

In the forthcoming paper [4], we will answer this question in the affirmative, by *directly* adapting the hidden subspace scheme from Section 5 (i.e., the scheme based on a classical oracle). Since the idea is an extremely simple one, let us sketch it here.

Theorem 7.2 (Query-Secure Variant of Wiesner's Scheme)**.** *Relative to a random oracle R,*[21] *there exists a private-key quantum money scheme, with perfect completeness and* $2^{-\Omega(n)}$ *soundness error, that is information-theoretically query-secure. One can also replace the random oracle R by a pseudorandom function family* $\{f_k\}_k$*, to obtain a private-key quantum money scheme, with no oracle, that is query-secure assuming that the* f_k *cannot be distinguished from random in quantum polynomial time.*

Proof sketch. For each key k and a serial number s, we will think of the random oracle R as encoding a classical description $R(k,s)$ of a subspace $A_{k,s} \leq \mathbb{F}_2^n$, which is uniformly random subject to $\dim(A_{k,s}) = n/2$. Let $|A_{k,s}\rangle$ be a uniform superposition over $A_{k,s}$. Then the private-key money scheme $\mathcal{S} = (\mathsf{KeyGen},\mathsf{Bank},\mathsf{Ver})$ is defined as follows:

- $\mathsf{KeyGen}(0^n)$ generates an n-bit key k uniformly at random.
- $\mathsf{Bank}(k)$ outputs a banknote $|\$_s\rangle := |s\rangle |A_{k,s}\rangle$, for a random serial number $s \in \{0,1\}^n$.
- $\mathsf{Ver}(k,(s,\rho))$ applies a projective measurement that accepts ρ with probability $\langle A_{k,s}|\rho|A_{k,s}\rangle$.

[21] Or alternatively, assuming the bank has access to a giant random number table, as in Wiesner's original setup [42].

Now, suppose it were possible to break $\mathcal{S}$ (i.e., to counterfeit $|A_{k,s}\rangle$), using $\mathrm{poly}(n)$ adaptive queries to $\mathsf{Ver}(k,\cdot)$. Then we claim that it would *also* be possible to break our *public-key* scheme from Section 5, and thereby contradict the unconditional security proof for the latter! The reason is simply that any query to Ver, of the form $\mathsf{Ver}(k,(s,\rho))$, can easily be simulated using queries to $U_{A_{k,s}}$ and $U_{A_{k,s}^{\perp}}$, the membership oracles for $A_{k,s}$ and $A_{k,s}^{\perp}$ respectively that are available to a counterfeiter against the public-key scheme.

Finally, suppose we replace $R(k,s)$ by a pseudorandom function $f_k(s)$. Then just like with the original BBBW scheme [15], we can argue as follows. Since we already showed that $\mathcal{S}$ is information-theoretically secure when instantiated with a "true" random function, any break of $\mathcal{S}$ in the pseudorandom case would thereby distinguish the function f_k from random. □

8 Open problems

The "obvious" problem is to better understand the security of our explicit scheme based on polynomials. Are there nontrivial attacks, for example using Gröbner-basis algorithms? Can we base the security of our scheme—or a related scheme—on some cryptographic assumption that does *not* involve exponentially-small success probabilities? What happens as we change the field size or polynomial degree? Does "hiding" a subspace $A \leq \mathbb{F}_2^n$ in the way we suggest, as the set of common zeroes of multivariate polynomials $p_1,\ldots,p_m : \mathbb{F}_2^n \to \mathbb{F}_2$, have other cryptographic applications, for example to *program obfuscation* [11]?

Of course, there is also tremendous scope for inventing new schemes, which might be based on different assumptions and have different strengths and weaknesses.

Let us move on to some general questions about public-key quantum money. First, is there an unconditionally-secure public-key quantum money scheme relative to a *random* oracle R? (Recall that Wiesner's original scheme [42] was unconditionally-secure and used only a random oracle, but was private-key. Meanwhile, our scheme from Section 5 is unconditionally-secure and public-key, but requires a non-random oracle.) Second, is there a public-key quantum money scheme where the banknotes consist of *single, unentangled qubits*, as in Wiesner's scheme? Note that the results of Farhi et al. [23] imply that, if such a scheme exists, then it cannot be projective. Third, is there a general way to amplify soundness error in quantum money schemes?[22] (We show how to amplify *completeness* error in Appendix A.)

8.1 Quantum copy-protection and more

Quantum money is just *one* novel cryptographic use for the No-Cloning Theorem. Given essentially *any* object of cryptographic interest, one can ask whether quantum mechanics lets us make the object uncloneable. Section 1.4 already discussed one example—*uncloneable signatures*—but there are many others, such as commitments and proofs.[23]

Along those lines, Aaronson [3] proposed a task that, if achievable, would arguably be an even more dramatic application of the No-Cloning Theorem than quantum money: namely, *quantum software copy-protection*. He gave explicit schemes—which have not yet been broken—for copy-protecting a

[22] Theorem 3.5 gives *some* soundness amplification for projective schemes: namely, from constant to $1/\mathrm{poly}(n)$. Here we are asking whether one can do anything better.

[23] Even within complexity theory, it would be interesting to study the class QMA (Quantum Merlin-Arthur) subject to the constraint that witnesses must be hard to clone—or alternatively, that witnesses must be *easy* to clone!

restricted class of functions, namely the *point functions*. In these schemes, given a "password" $s \in \{0,1\}^n$, a software vendor can prepare a quantum state $|\psi_s\rangle$, which allows its holder to *recognize* s: in other words, to decide whether $x = s$ given $x \in \{0,1\}^n$ as input. On the other hand, given $|\psi_s\rangle$, it seems intractable not only to *find* s for oneself, but even to prepare a *second* quantum state with which s can be recognized.

Admittedly, recognizing passwords is an extremely restricted functionality. However, relative to a quantum oracle, Aaronson [3] also described a scheme to quantumly copy-protect *arbitrary* programs, just as well as if the software vendor were able to hand out uncloneable black boxes.[24] In the spirit of this paper, we can now ask: is there likewise a way to quantumly copy-protect arbitrary programs relative to a *classical* oracle? We conjecture that the answer is yes, and in fact we have plausible candidate constructions, which are directly related to the hidden-subspace money scheme of Section 5. However, the security of those constructions seems to hinge on the following conjecture.

Conjecture 8.1 (Direct Product for Finding Black-Box Subspace Elements)**.** *Let A be a uniformly-random subspace of $\mathbb{F}_2^n$ satisfying $\dim(A) = n/2$. Then given membership oracles for both A and $A^{\perp}$, any quantum algorithm needs $2^{\Omega(n)}$ queries to find two distinct nonzero elements $x, y \in A$, with success probability $\Omega\left(2^{-n/2}\right)$.*

Besides its applications for copy-protection, a proof of Conjecture 8.1 would be an important piece of formal evidence for Conjecture 6.7, on which we based the security of our explicit money scheme.

Appendix A Reducing completeness error

When we defined quantum money schemes and mini-schemes in Section 3, we allowed the verifier to reject a *legitimate* money state with probability up to $1/3$. But of course, a money scheme with completeness error $\varepsilon = 1/3$ is not very useful in practice! So in this appendix, we prove that the completeness error ε can be made exponentially small in n, at the cost of only a modest increase in the soundness error δ (i.e., the probability of successful counterfeiting).

Theorem A.1 (Completeness Amplification for Mini-Schemes)**.** *Let $\mathcal{M} = (\mathsf{Bank}, \mathsf{Ver})$ be a quantum money mini-scheme with completeness error $\varepsilon < 1/2$ and soundness error $\delta < 1 - 2\varepsilon$. Then for all polynomials p and all $\delta' > \delta/(1-2\varepsilon)$, we can construct an amplified mini-scheme $\mathcal{M}' = \left(\mathsf{Bank}', \mathsf{Ver}'\right)$ with completeness error $1/2^{p(n)}$ and soundness error δ'.*

Proof. Let $k = \operatorname{poly}(n)$ and $\eta > 0$ be parameters to be determined later. Our construction of $\mathcal{M}'$ is the "obvious" one based on repetition:

- $\mathsf{Bank}'(0^n)$ outputs a composite banknote $\$' := (s_1 \ldots s_k, \rho_{s_1} \ldots \rho_{s_k})$, where $(s_1, \rho_{s_1}), \ldots, (s_k, \rho_{s_k})$ are banknotes output independently by $\mathsf{Bank}(0^n)$.
- $\mathsf{Ver}'(\cancel{\$})$ runs $\mathsf{Ver}(\cancel{\$}_1), \ldots, \mathsf{Ver}(\cancel{\$}_k)$, where $\cancel{\$}_1, \ldots, \cancel{\$}_k$ are the (s, ρ_s) pairs in the alleged composite banknote $\cancel{\$}$, and accepts if and only if at least $(1 - \varepsilon - \eta)k$ invocations accept.

[24] As usual, full details have not yet appeared yet.

Note that Ver_2', the amplified double verifier, then takes as input a state of the form

$$(s_1 \dots s_k, \sigma_1 \dots \sigma_k, \xi_1 \dots \xi_k),$$

and accepts if and only if $\mathsf{Ver}'(s_1 \dots s_k, \sigma_1 \dots \sigma_k)$ and $\mathsf{Ver}'(s_1 \dots s_k, \xi_1 \dots \xi_k)$ both accept. By choosing k sufficiently large and applying a Chernoff bound, it is clear that we can make the completeness error $1/2^{p(n)}$ for any polynomial p.

Meanwhile, suppose $\mathcal{M}'$ has soundness error δ': in other words, there exists a counterfeiter C' such that $\mathsf{Ver}_2'(s_1 \dots s_k, C'(\$'))$ accepts with probability δ', given a valid composite banknote $\$'$. Then to prove the theorem, it suffices to construct a counterfeiter C for the original mini-scheme $\mathcal{M}$, such that $\mathsf{Ver}_2(s, C(\$))$ accepts with probability $\delta \geq (1 - 2\varepsilon - \eta)\delta'$, given a valid banknote $\$ = (s, \rho_s)$.

This C works as follows:

(1) By calling $\mathsf{Bank}'(0^n)$, generate a new composite banknote $\$' = (\$_1, \dots, \$_k)$.

(2) Let $\$'_{\text{new}}$ be the result of starting with $\$'$, then swapping out $\$_i$ for the banknote $\$$ to be copied, for some $i \in [k]$ chosen uniformly at random.

(3) Let $(s_1 \dots s_k, \sigma_1 \dots \sigma_k, \xi_1 \dots \xi_k) := C'(\$'_{\text{new}})$.

(4) Output (s_i, σ_i, ξ_i).

By assumption,

$$\Pr\left[\mathsf{Ver}_2'(s_1 \dots s_k, \sigma_1 \dots \sigma_k, \xi_1 \dots \xi_k) \text{ accepts}\right] \geq \delta'.$$

Now, suppose Ver_2' does accept. Then by the definition of Ver_2', at least $(1 - \varepsilon - \eta)k$ of

$$\mathsf{Ver}(s_1, \sigma_1), \dots, \mathsf{Ver}(s_k, \sigma_k)$$

must have accepted, along with at least $(1 - \varepsilon - \eta)k$ of

$$\mathsf{Ver}(s_1, \xi_1), \dots, \mathsf{Ver}(s_k, \xi_k).$$

So there must be at least $(1 - 2\varepsilon - 2\eta)k$ indices $j \in [k]$ such that $\mathsf{Ver}(s_j, \sigma_j)$ and $\mathsf{Ver}(s_j, \xi_j)$ *both* accepted. Therefore

$$\begin{aligned} \Pr[\mathsf{Ver}_2(s_i, \sigma_i, \xi_i) \text{ accepts}] &= \Pr[\mathsf{Ver}(s_i, \sigma_i) \text{ and } \mathsf{Ver}(s_i, \xi_i) \text{ accept}] \\ &\geq (1 - 2\varepsilon - 2\eta)\delta'. \end{aligned}$$

Taking $\eta > 0$ sufficiently small now yields the theorem. □

A direct counterpart of Theorem A.1, with exactly the same parameters, can be proved for public-key quantum money schemes. Once again, the main idea is to consider "composite banknotes" $\$' = (\$_1, \dots, \$_k)$—and this time, to associate with each $\$_i$ a *different*, independently-chosen public/private key pair. Another counterpart of Theorem A.1 can be proved for digital signature schemes, indeed with slightly better parameters ($\delta' > \delta/(1 - \varepsilon)$ instead of $\delta' > \delta/(1 - 2\varepsilon)$). We omit the details.

Appendix B Complexity-theoretic no-cloning theorem

In Section 5, we applied the inner-product adversary method to show that a uniform superposition $|A\rangle$ over a random subspace $A \leq \mathbb{F}_2^n$ requires $\Omega(2^{n/4})$ quantum queries to duplicate, even if we are given access to an oracle that decides membership in both A and $A^{\perp}$. For completeness, in this appendix we present a simpler application of the inner-product adversary method: namely, we show that a Haar-random n-qubit state $|\psi\rangle$ requires $\Omega(2^{n/2})$ queries to duplicate, if we are given access to an oracle U_ψ that accepts $|\psi\rangle$ and that rejects every state orthogonal to $|\psi\rangle$. The latter is the original result that Aaronson [3] called the "Complexity-Theoretic No-Cloning Theorem," though a proof has not appeared until now.

In Section 5, we used the lower bound for copying subspace states to construct a quantum money mini-scheme that was provably secure relative to a classical oracle. In the same way, one can use the Complexity-Theoretic No-Cloning Theorem to construct a mini-scheme that is provably secure relative to a *quantum* oracle. We omit the details of that construction, not only because it is superseded by the classical oracle construction in Section 5, but because the two constructions are essentially the same. The one real difference is that the quantum oracle construction benefits from a quadratically better lower bound on the number of queries needed to counterfeit: $\Omega(2^{n/2})$ rather than $\Omega(2^{n/4})$.

Choose an n-qubit pure state $|\psi\rangle$ uniformly from the Haar measure, and fix $|\psi\rangle$ in what follows. Let U_ψ be a unitary transformation such that $U_\psi|\psi\rangle = -|\psi\rangle$ and $U_\psi|\eta\rangle = |\eta\rangle$ for all $|\eta\rangle$ orthogonal to $|\psi\rangle$. The following is the direct analogue of Theorem 5.2.

Theorem B.1 (Complexity-Theoretic No-Cloning)**.** *Given one copy of $|\psi\rangle$, as well as oracle access to U_ψ, a counterfeiter needs $\Omega(2^{n/2})$ queries to prepare $|\psi\rangle^{\otimes 2}$ with certainty (for a worst-case $|\psi\rangle$).*

Proof. We will apply Theorem 4.2. Let the set $\mathcal{O}$ contain U_ψ for every possible n-qubit state $|\psi\rangle$. Then S_{U_ψ} is just the 1-dimensional subspace corresponding to $|\psi\rangle$. Also, put $\left(U_\psi, U_\varphi\right) \in R$ if and only if $|\langle\psi|\varphi\rangle| = c$, for some $0 < c < 1$ to be specified later. Then for all $U_\psi \in \mathcal{O}$ and $|\eta\rangle \in S_{U_\psi}^{\perp}$, we have

$$\begin{aligned}
\mathop{\mathrm{E}}_{U_\varphi\,:\,\left(U_\psi,U_\varphi\right)\in R}\left[|\langle\eta|\varphi\rangle|^2\right] &= \mathop{\mathrm{E}}_{|\varphi\rangle\,:\,|\langle\psi|\varphi\rangle|=c}\left[|\langle\eta|\varphi\rangle|^2\right] \\
&= \mathop{\mathrm{E}}_{|v\rangle\in S_{U_\psi}^{\perp}}\left[\left|\langle\eta|\left(c|\psi\rangle+\sqrt{1-c^2}\,|v\rangle\right)\right|^2\right] \\
&= \left(1-c^2\right)\mathop{\mathrm{E}}_{|v\rangle\in S_{U_\psi}^{\perp}}\left[|\langle\eta|v\rangle|^2\right] \\
&= \frac{1-c^2}{2^n-1}\,.
\end{aligned}$$

So set $\varepsilon := (1-c^2)/(2^n-1)$. If the counterfeiter succeeds, it must map

$$|\psi\rangle \quad \text{to some state} \quad \left|f_\psi\right\rangle := |\psi\rangle|\psi\rangle\left|\mathrm{garbage}_\psi\right\rangle,$$

and

$$|\varphi\rangle \quad \text{to some state} \quad \left|f_\varphi\right\rangle := |\varphi\rangle|\varphi\rangle\left|\mathrm{garbage}_\varphi\right\rangle.$$

Note that $|\langle f_\psi | f_\varphi \rangle| \leq c^2$. So setting $d := c^2$, Theorem 4.2 tells us that the counterfeiter must make

$$\Omega\left(\left(c-c^2\right)\sqrt{\frac{2^n-1}{1-c^2}}\right)$$

queries to U_ψ. Fixing (say) $c = 1/2$, this is $\Omega\left(2^{n/2}\right)$. □

Like Theorem 5.2, Theorem B.1 is easily seen to be tight, since one can use the amplitude amplification algorithm (Lemma 2.7) to find $|\psi\rangle$, and thereby prepare $|\psi\rangle^{\otimes 2}$, using $O\left(2^{n/2}\right)$ queries to U_ψ.

For completeness, we observe the following generalization of Theorem B.1.

Theorem B.2. *Given k copies of $|\psi\rangle$, as well as oracle access to U_ψ, a counterfeiter needs $\Omega(2^{n/2}/\sqrt{k})$ queries to prepare $|\psi\rangle^{\otimes k+1}$ with certainty (for a worst-case $|\psi\rangle$).*

Proof. If the counterfeiter succeeds, it must map

$$|\psi\rangle^{\otimes k} \quad \text{to some state} \quad |f_\psi\rangle := |\psi\rangle^{\otimes k+1} \left|\text{garbage}_\psi\right\rangle,$$

and

$$|\varphi\rangle^{\otimes k} \quad \text{to some state} \quad |f_\varphi\rangle := |\varphi\rangle^{\otimes k+1} \left|\text{garbage}_\varphi\right\rangle.$$

Note that $\left|\langle f_\psi | f_\varphi \rangle\right| \leq c^{k+1}$. So setting $d := c^{k+1}$, Theorem 4.2 tells us that the counterfeiter must make

$$\Omega\left(\left(c^k - c^{k+1}\right)\sqrt{\frac{2^n-1}{1-c^2}}\right)$$

queries to U_ψ. Fixing $c := 1 - 1/k$, the above is $\Omega(2^{n/2}/\sqrt{k})$. □

We end this appendix by stating, without proof, three stronger lower bounds that are the direct analogues of Corollary 5.3, Corollary 5.4, and Theorem 5.5 respectively.

Corollary B.3. *Given one copy of $|\psi\rangle$, as well as oracle access to U_ψ, a counterfeiter needs $\Omega\left(2^{n/2}\right)$ queries to prepare a state ρ such that $\langle\psi|^{\otimes 2}\rho\,|\psi\rangle^{\otimes 2} \geq 0.9999$ (for a worst-case $|\psi\rangle$).*

Corollary B.4. *Let $1/\varepsilon = o\left(2^n\right)$. Given one copy of $|\psi\rangle$, as well as oracle access to U_ψ, a counterfeiter needs $\Omega\left(\sqrt{\varepsilon}2^{n/2}\right)$ queries to prepare a state ρ such that $\langle\psi|^{\otimes 2}\rho\,|\psi\rangle^{\otimes 2} \geq \varepsilon$ (for a worst-case $|\psi\rangle$).*

Theorem B.5. *Let $|\psi\rangle$ be an n-qubit pure state chosen uniformly from the Haar measure. Given one copy of $|\psi\rangle$, as well as oracle access to U_ψ, a counterfeiter C needs $\Omega\left(\sqrt{\varepsilon}2^{n/2}\right)$ queries to prepare a $2n$-qubit state ρ that a projector $V_\psi^{\otimes 2}$ onto $|\psi\rangle^{\otimes 2}$ accepts with probability at least ε, for all $1/\varepsilon = o\left(2^n\right)$. Here the probability is taken over the choice of $|\psi\rangle$, as well as the behavior of C and $V_\psi^{\otimes 2}$.*

Acknowledgments

We thank Andris Ambainis, Boaz Barak, Dmitry Gavinsky, Daniel Gottesman, Aram Harrow, Yuval Ishai, Shelby Kimmel, Shaunak Kishore, Greg Kuperberg, Andy Lutomirski, Abel Molina, Rafi Ostrovsky, Amit Sahai, Peter Shor, and John Watrous for helpful discussions and correspondence; and the anonymous reviewers and ToC editors for their comments.

References

[1] SCOTT AARONSON: Quantum lower bound for the collision problem. In *Proc. 34th STOC*, pp. 635–642. ACM Press, 2002. Preprint at arXiv. [doi:10.1145/509907.509999] 354

[2] SCOTT AARONSON: Limitations of quantum advice and one-way communication. *Theory of Computing*, 1(1):1–28, 2005. Preliminary version in CCC'04. Preprint at arXiv. [doi:10.4086/toc.2005.v001a001] 363

[3] SCOTT AARONSON: Quantum copy-protection and quantum money. In *Proc. 24th IEEE Conf. on Computational Complexity (CCC'09)*, pp. 229–242. IEEE Comp. Soc. Press, 2009. [doi:10.1109/CCC.2009.42] 353, 355, 356, 357, 366, 373, 390, 392, 393, 395

[4] SCOTT AARONSON: On the security of private-key quantum money, 2013. In preparation. 390, 391

[5] SCOTT AARONSON AND GREG KUPERBERG: Quantum versus classical proofs and advice. *Theory of Computing*, 3(7):129–157, 2007. Preliminary version in CCC'07. Preprint at arXiv. [doi:10.4086/toc.2007.v003a007] 360

[6] SCOTT AARONSON AND YAOYUN SHI: Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, 2004. [doi:10.1145/1008731.1008735] 354

[7] MARTIN R. ALBRECHT AND CARLOS CID: Cold boot key recovery by solving polynomial systems with noise. In *Proc. 9th Internat. Conf. on Applied Cryptography and Network Security (ACNS'11)*, pp. 57–72. Springer, 2011. Available in preprint. [doi:10.1007/978-3-642-21554-4_4] 388

[8] NOGA ALON, MICHAEL KRIVELEVICH, AND BENNY SUDAKOV: Finding a large hidden clique in a random graph. *Random Structures & Algorithms*, 13(3-4):457–466, 1998. Preliminary version in SODA'98. [doi:10.1002/(SICI)1098-2418(199810/12)13:3/4<457::AID-RSA14>3.0.CO;2-W] 353

[9] ANDRIS AMBAINIS: Quantum lower bounds by quantum arguments. *J. Comput. System Sci.*, 64(4):750–767, 2002. Preliminary version in STOC'00. Preprint at arXiv. [doi:10.1006/jcss.2002.1826] 354, 355, 361, 372, 373

[10] ANDRIS AMBAINIS, LOÏCK MAGNIN, MARTIN ROETTELER, AND JÉRÉMIE ROLAND: Symmetry-assisted adversaries for quantum state generation. In *Proc. 26th IEEE Conf. on Computational Complexity (CCC'11)*, pp. 167–177. IEEE Comp. Soc. Press, 2011. Preprint at arXiv. [doi:10.1109/CCC.2011.24] 354, 374

[11] BOAZ BARAK, ODED GOLDREICH, RUSSELL IMPAGLIAZZO, STEVEN RUDICH, AMIT SAHAI, SALIL P. VADHAN, AND KE YANG: On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6, 2012. Preliminary versions in CRYPTO'01 and ECCC. [doi:10.1145/2160158.2160159] 392

[12] ROBERT BEALS, HARRY BUHRMAN, RICHARD CLEVE, MICHELE MOSCA, AND RONALD DE WOLF: Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. Preliminary version in FOCS'98. Preprint at arXiv. [doi:10.1145/502090.502097] 354

[13] CHARLES H. BENNETT, ETHAN BERNSTEIN, GILLES BRASSARD, AND UMESH V. VAZIRANI: Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997. Preprint at arXiv. [doi:10.1137/S0097539796300933] 361, 373, 382

[14] CHARLES H. BENNETT AND GILLES BRASSARD: Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE Internat. Conf. on Computers, Systems and Signal Processing*, pp. 175–179, 1984. 353, 358

[15] CHARLES H. BENNETT, GILLES BRASSARD, SETH BREIDBART, AND STEPHEN WIESNER: Quantum cryptography, or unforgeable subway tokens. In *Proceedings of CRYPTO*, pp. 267–275. Plenum Press, 1982. 353, 356, 367, 390, 392

[16] NIELS BOHR: *Atomic Physics and Human Knowledge*. Dover, 2010. First published 1961. 359

[17] DAN BONEH, ÖZGÜR DAGDELEN, MARC FISCHLIN, ANJA LEHMANN, CHRISTIAN SCHAFFNER, AND MARK ZHANDRY: Random oracles in a quantum world. In *17th Internat. Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT'11)*, pp. 41–69, 2011. Preprint at arXiv. [doi:10.1007/978-3-642-25385-0_3] 361

[18] CHARLES BOUILLAGUET, JEAN-CHARLES FAUGÈRE, PIERRE-ALAIN FOUQUE, AND LUDOVIC PERRET: Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In *14th Internat. Conf. on Practice and Theory in Public Key Cryptography (PKC'11)*, pp. 473–493. Springer, 2011. [doi:10.1007/978-3-642-19379-8_29] 358, 389

[19] GILLES BRASSARD, PETER HØYER, MICHELE MOSCA, AND ALAIN TAPP: Quantum amplitude amplification and estimation. In JR. SAMUEL J. LOMONACO AND HOWARD E. BRANDT, editors, *Quantum Computation and Information*, Contemporary Mathematics Series. AMS, 2002. Preprint at arXiv. 363

[20] DAVID CASH, DENNIS HOFHEINZ, EIKE KILTZ, AND CHRIS PEIKERT: Bonsai trees, or how to delegate a lattice basis. *J. Cryptology*, 25(4):601–639, 2012. Preliminary version in EUROCRYPT'10. [doi:10.1007/s00145-011-9105-2] 360

[21] SOURAV CHAKRABORTY, JAIKUMAR RADHAKRISHNAN, AND NANDAKUMAR RAGHUNATHAN: Bounds for error reduction with few quantum queries. In *Proc. 9th Internat. Workshop on Randomization and Computation (RANDOM'05)*, pp. 245–256. Springer, 2005. [doi:10.1007/11538462_21] 364

[22] JINTAI DING AND BO-YIN YANG: Multivariate public key cryptography. In DANIEL J. BERNSTEIN, JOHANNES BUCHMANN, AND ERIK DAHMEN, editors, *Post-Quantum Cryptography*, pp. 193–241. Springer, 2009. [doi:10.1007/978-3-540-88702-7_6] 388

[23] 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(19):190503, 2010. Preprint at arXiv. [doi:10.1103/PhysRevLett.105.190503] 354, 355, 391, 392

[24] EDWARD FARHI, DAVID GOSSET, AVINATAN HASSIDIM, ANDREW LUTOMIRSKI, AND PETER W. SHOR: Quantum money from knots. In *Proc. 3rd Innovations in Theoretical Comput. Sci. (ITCS'12)*, pp. 276–289. ACM Press, 2012. Preprint at arXiv. [doi:10.1145/2090236.2090260] 353, 354, 355, 356, 357, 366, 367, 369, 370

[25] DMITRY GAVINSKY: Quantum money with classical verification. In *Proc. 27th IEEE Conf. on Computational Complexity (CCC'12)*, pp. 42–52. IEEE Comp. Soc. Press, 2012. Preprint at arXiv. [doi:10.1109/CCC.2012.10] 353

[26] WILLI GEISELMANN, WILLI MEIER, AND RAINER STEINWANDT: An attack on the isomorphisms of polynomials problem with one secret. *Int. J. Inf. Sec.*, 2(1):59–64, 2003. [doi:10.1007/s10207-003-0025-5] 358, 389

[27] LOV K. GROVER: A fast quantum mechanical algorithm for database search. In *Proc. 28th STOC*, pp. 212–219. ACM Press, 1996. Preprint at arXiv. [doi:10.1145/237814.237866] 363

[28] CHRISTOPHER J. HILLAR AND LEK-HENG LIM: Most tensor problems are NP-hard. Technical report, 2009. [arXiv:0911.1393] 389

[29] TROY LEE, RAJAT MITTAL, BEN W. REICHARDT, ROBERT SPALEK, AND MARIO SZEGEDY: Quantum query complexity of state conversion. In *Proc. 52nd FOCS*, pp. 344–353. IEEE Comp. Soc. Press, 2011. Preprint at arXiv. [doi:10.1109/FOCS.2011.75] 374

[30] ANDREW LUTOMIRSKI: An online attack against Wiesner's quantum money. Technical report, 2010. [arXiv:1010.0256] 353, 354, 356, 357, 390

[31] ANDREW LUTOMIRSKI: Component mixers and a hardness result for counterfeiting quantum money. Technical report, 2011. [arXiv:1107.0321] 354

[32] ANDREW LUTOMIRSKI, SCOTT AARONSON, EDWARD FARHI, DAVID GOSSET, JONATHAN A. KELNER, AVINATAN HASSIDIM, AND PETER W. SHOR: Breaking and making quantum money: Toward a new quantum cryptographic protocol. In *Proc. Innovations in Comput. Sci. (ICS'10)*, pp. 20–31. Tsinghua University Press, 2010. ICS'10. Preprint at arXiv. 353, 354, 355, 356, 357, 366, 367, 369, 370

[33] ABEL MOLINA, THOMAS VIDICK, AND JOHN WATROUS: Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In *Proc. 7th Conf. Theory of Quantum Computation,*

Communication, and Cryptography (TQC'12), pp. 45–64, 2012. Preprint at arXiv. [doi:10.1007/978-3-642-35656-8_4] 352, 353, 390

[34] MICHELE MOSCA AND DOUGLAS STEBILA: Quantum coins. In *Error-Correcting Codes, Finite Geometries and Cryptography*, volume 523, pp. 35–47. Amer. Math. Soc., 2010. Preprint at arXiv. 353

[35] MONI NAOR AND MOTI YUNG: Universal one-way hash functions and their cryptographic applications. In *Proc. 21st STOC*, pp. 33–43. ACM Press, 1989. [doi:10.1145/73007.73011] 361

[36] MICHAEL NIELSEN AND ISAAC CHUANG: *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. [ACM:544199] 361, 362

[37] FERNANDO PASTAWSKI, NORMAN Y. YAO, LIANG JIANG, MIKHAIL D. LUKIN, AND J. IGNACIO CIRAC: Unforgeable noise-tolerant quantum tokens. Technical report, 2011. [arXiv:1112.5456] 353

[38] JACQUES PATARIN, LOUIS GOUBIN, AND NICOLAS COURTOIS: Improved algorithms for isomorphisms of polynomials. In *Proc. Internat. Conf. on the Theory and Application of Cryptographic Techniques (EUROCRYPT'98)*, pp. 184–200. Springer, 1998. [doi:10.1007/BFb0054126] 358, 389

[39] ODED REGEV: On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34, 2009. Preliminary version in STOC'05. [doi:10.1145/1568318.1568324] 388

[40] JOHN ROMPEL: One-way functions are necessary and sufficient for secure signatures. In *Proc. 22nd STOC*, pp. 387–394. ACM Press, 1990. [doi:10.1145/100216.100269] 361

[41] TATHAGAT TULSI, LOV K. GROVER, AND APOORVA PATEL: A new algorithm for fixed point quantum search. *Quantum Inf. Comput.*, 6(6):483–494, 2006. QIC. [ACM:2011693] 356, 364

[42] STEPHEN WIESNER: Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Original manuscript written circa 1970. [doi:10.1145/1008908.1008920] 352, 356, 389, 391, 392

AUTHORS

Scott Aaronson
associate professor
Massachusetts Institute of Technology, Cambridge, MA
aaronson@csail.mit.edu
`http://www.scottaaronson.com`

Paul Christiano
Ph. D. student
University of California, Berkeley
paulfchristiano@gmail.com

ABOUT THE AUTHORS

SCOTT AARONSON received his bachelor's degree from Cornell University and his Ph. D. from UC Berkeley. He is known for his blog and for founding the Complexity Zoo. He publishes often in Theory of Computing.

PAUL CHRISTIANO is a Ph. D. student at UC Berkeley. He obtained a bachelor's in mathematics from MIT in 2012. As an undergraduate his research was scattered between combinatorial optimization, data structures, and quantum cryptography.