Contemporary Mathematics
Volume **523**, 2010

Quantum Coins

Michele Mosca and Douglas Stebila

Abstract. One of the earliest cryptographic applications of quantum information was to create quantum digital cash that could not be counterfeited. In this paper, we describe a new type of quantum money: **quantum coins**, where all coins of the same denomination are represented by identical quantum states. We state desirable security properties such as anonymity and unforgeability and propose two candidate quantum coin schemes: one using black box operations, and another using blind quantum computation.

1. Introduction

The uncertainty principle and no-cloning theorem of quantum mechanics made quantum money one of the original interests of quantum information theory. The ability to create digital money which cannot be counterfeited because of the laws of physics is a compelling idea. Classical digital cash has been researched extensively, with ongoing improvements to its security tradeoffs, but remains fundamentally subject to the constraint that classical bits can be easily copied. With quantum money, we hope to use the inability to perfectly clone quantum states to prevent counterfeiting. Besides being non-counterfeitable, an effective digital cash scheme should also be efficiently verifiable, anonymous, transferable, and robust.

In this paper, we describe a new form of quantum money called *quantum coins*, where all coins of the same denomination are represented by identical quantum states. We state formally what it means for them to be unforgeable and describe how to implement quantum coin schemes using black box operations and using blind quantum computing. We also describe *quantum bills* which capture a wide range of notions of quantum money.

Contributions. In this paper, we present a new type of quantum money, which we call *quantum coins*: coins are transferable, locally verifiable, and unforgeable, and have some anonymity properties. Each coin generated by the bank should be a

2000 *Mathematics Subject Classification.* Primary 81P68; Secondary 94A60.

Key words and phrases. Quantum money, digital cash, quantum cryptography.

The first author was supported by Canada's NSERC, QuantumWorks, MITACS, CIFAR, CRC, ORF, the Government of Canada, and Ontario-MRI.

The second author was supported by a Canada NSERC Postgraduate Scholarship and Sun Microsystems Laboratories. Research performed while the second author was at the University of Waterloo.

copy of the same quantum state, and hence coins should be indistinguishable from one another. Additionally, a circuit is provided to allow the coins to be verified locally and then transferred for later use.

We describe how to achieve quantum coins with black box quantum circuits and with blind quantum computation. The unforgeability of coins in our scheme comes from complexity theoretic assumptions on the adversary's running time.

Our work contrasts with previous quantum money schemes, which we call *quantum bills*: in a quantum bill scheme, the bank generates tokens that are classical/quantum pairs, which in general are distinct. The classical string may serve as a serial number or as some input value to be used in the verification procedure.

Future directions. Our quantum coin construction of Section 4 requires the use of a black-box oracle in the verification circuit, but it is not yet known how these can be implemented. An open question is to find a way to obfuscate the verification circuit so that it is effectively a black box, and in general to find a model for obfuscation of quantum circuits, possibly using computational assumptions. We describe how blind quantum computation could be used in the context of quantum coin verification and note the limitations, in particular the online quantum communication required. Reducing the communication and computational requirements of blind quantum computing is a problem that merits further study.

Although our coins are inherently anonymous if the bank issues coins correctly, we do not yet have a mechanism to allow users of the system to verify that the coins are indeed issued correctly, so this remains an open question.

In Section 3.2, we briefly discuss a model for quantum bills. An open question related to quantum bills is to find an offline-verifiable quantum bill scheme; this may require using computational hardness assumptions.

Outline. The remainder of the paper is organized as follows. In Section 2, we describe the goals for a quantum money scheme and analyze existing quantum money schemes, as well as our own, in relation to these goals. Section 3 introduces the two main types of quantum money, quantum coins and quantum bills, and describes their precise security properties. In Section 4, we describe how to implement quantum coins in the black box model and give bounds on unforgeability. In Section 5, we discuss implementing quantum coins using blind quantum computation.

1.1. Related work.

Digital cash. Digital cash has been well-explored in classical cryptographic contexts, with the first schemes being proposed by Chaum [**Cha85, Cha88**] and Chaum, Fiat, and Naor [**CFN88**]. For classical digital cash schemes, one of the main problems to solve is the *multiple-spending problem*: since classical digital cash can easily be duplicated, there must be a way to prevent the same tokens from being redeemed more than once. An online scheme, in which each token is verified with the bank at the time it is meant to be spent, solves this problem immediately, but online verification requires an online communications channel between merchant and bank. The other general solution for preventing multiple spending is to embed some identity information in the money tokens such that, if the token is spent only once, the transaction remains anonymous, but if the token is spent multiple times, then the bank can combine these multiple transactions to recover the identity of the multiple spender. Moreover, classical digital cash is not transferable unless we allow the size of the token to grow linearly in the number of transfers [**CP92**].

Quantum money. Quantum money was one of the earliest applications of quantum information theory, and was introduced in the early papers of Wiesner [**Wie83**] and Bennett, Brassard, Breidbard, and Wiesner [**BBBW82**]. In both schemes, a bank constructs distinct quantum tokens and corresponding classical serial numbers. The tokens are the encoding of a random string in randomly chosen basis states of two non-orthogonal bases; the no-cloning theorem prevents perfect cloning of individual tokens. However, the tokens can only be verified by the bank: verification requires knowledge of the bases chosen for each token and the classical string that should be obtained upon measurement in the appropriate bases. This means that an online quantum channel is required between merchants and the bank. The tokens are non-transferable and are not anonymous.

Tokunaga, Okamoto, and Imoto [**TOI03**] give a scheme for non-transferable anonymous quantum cash with online verification. In their scheme, a user obtains a distinct token from the bank; tokens are generated using private parameters and random values stored by the bank. The user then alters the token with an appropriate randomly chosen unitary transformation to obtain anonymity. At payment time, the user presents the token to the merchant who transmits it (over a quantum channel) to the bank for verification. The scheme is secure against an attacker who can examine a single token, but has not been proven secure against an attacker who can obtain and examine all the quantum tokens.

Our work on quantum coins makes use of work by Aaronson [**Aar05a**] that introduced a complexity-theoretic no-cloning theorem that allows us to argue for the unforgeability of quantum coins. Our work was first presented in [**MS06**], [**MS07**], and [**Ste09**]. Subsequently Aarsonson expanded his work based on discussions with us to also include a presentation of quantum money [**Aar09**] similar to ours; we have noted in footnotes throughout this paper where that he presents similar concepts.

2. Security goals

We now describe, informally, the properties that a good money scheme should have.

- G1. *Anonymous*: it should be difficult for any party to trace the use of a token to determine who spent it or where they spent it.
- G2. *Unforgeable*: given zero or more tokens and the verification circuit, it should be difficult for a forger to produce another token that passes the verification procedure with non-negligible probability.
- G3. *Efficiently locally verifiable*: there should be an efficient algorithm that can determine with high accuracy whether a token is valid or not, without communicating with the bank.
- G4. *Transferable*: a valid token should be unchanged by the verification procedure, and thus can be transferred and reused in a subsequent verification procedure.

We will formally define unforgeability for quantum coin schemes in Section 3.1.2.

Figure 1 shows which of the above goals are satisfied by various existing money schemes. The "type" column indicates whether the tokens for a given denomination are all identical ("coin") or different ("bill"). For classical digital cash schemes, we

note that while unforgeability is impossible, it is possible to detect double spending of a token and trace it back to the offending party; such schemes, however, offer anonymity and offline double-spending detection only with computational assumptions. Our quantum coin schemes offer "partial" anonymity as we describe in Section 3.1.3. Additionally, the size of transferable digital cash must grow linearly in the number of transfers [**CP92**].

Scheme	**Type**	**Anonymous**	**Unforgeable**	**Locally verifiable**	**Transferable**
Physical coins	coin	yes	physically	yes	yes
Physical bills	bill	no	physically	yes	yes
Classical digital cash	bill	yes	double-spending detection	yes	grows in size
[**Wie83**]	q. bill	no	yes	no	no
[**BBBW82**]	q. bill	no	yes	no	no
[**TOI03**]	q. bill	yes	yes	no	no
This work: black box	q. coin	partial	yes	yes	yes
This work: blind comp.	q. coin	partial	yes	no	yes

FIGURE 1. Summary of money schemes and their properties

3. Types of quantum money

3.1. Quantum coins. In one type of quantum money, *quantum coins*, a bank issues many tokens for a particular denomination, and all these tokens are (supposed to be) copies of the same quantum state. The state for a 5-cent coin, for example, might be the pure state $|\psi_5\rangle$ and the bank produces many copies $|\psi_5\rangle^{\otimes 1000000}$, issuing one copy to each person who withdraws 5 cents from the bank. We use the term *quantum coin* because physical coins in the real world have the same property: there should be no discernible difference between different coins of the same denomination. The specification of a quantum coin scheme consists of the specification of the money state and the verification circuit.

DEFINITION 3.1. A *quantum coin scheme* is a pair $(V, |\psi\rangle)$, where $|\psi\rangle$ is an n-qubit pure state in a 2^n-dimensional Hilbert space $\mathcal{H}^{2^n}$, and V is a quantum circuit with a quantum n-qubit input register (denoted ρ), plus optional ancilla quantum registers, a classical output bit, and a quantum output register of n qubits.

The basic scenario of how a quantum coin scheme would operate is as follows. A bank generates a large number of quantum coins and stores them. A user withdraws coins from the bank via a private quantum channel and stores the coins. When the user wishes to spend the coins, it transfers the coins to the merchant using a quantum channel. The merchant uses a quantum circuit to verify the coins; this procedure may or may not involve classical or quantum communication with the bank. Finally, the merchant stores the coins until redeeming them with the bank or issuing them as change to subsequent users.

3.1.1. *Verification.* In the most general setting, the verification circuit V operates on three registers: a 1-qubit data readout register, an n-qubit input register, and an arbitrary m-qubit ancilla. After applying V, the first register is measured, and the output is the decision on whether to accept the token as valid or not. If the input is a valid quantum coin $|\psi\rangle$, then, after the application of V and the measurement, the classical output should be 0 and the partial trace over the first and third registers should leave the second register in the same state $|\psi\rangle$. The circuit diagram is given in Figure 2.

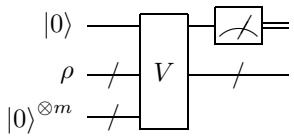

FIGURE 2. Generic verification circuit for a quantum coin scheme $(V, |\psi\rangle)$.

We cannot simply provide this circuit in an unprotected form to the public: it may be possible to decompose the circuit into component gates and find a way to forge money. In Section 4 we describe two techniques for implementing this circuit in a safe way: (1) black box verification, in which we assume the circuit is a black box and security rests on complexity-theoretic assumptions, and (2) blind quantum computation, which allows one party to implement an operation without gaining any information about the operation being performed, and security is information-theoretic. It could be possible to construct a scheme based on computational assumptions.

3.1.2. *Unforgeability.* We assume that a forger has the verification circuit V and many (or all) tokens issued, say k of them. The goal of a forger is to produce a state that passes more than k verification tests with good probability. Since the verification circuit projects the state into the subspace spanned by $|\psi\rangle$, this is equivalent to creating a state that has good overlap with the state $|\psi\rangle^{\otimes k+1}$.

DEFINITION 3.2. A quantum coin scheme $(V, |\psi\rangle)$, where $|\psi\rangle$ is an n-qubit state, is *unforgeable* if, given the verification circuit V and k copies of the state $|\psi\rangle$, for any $k \geq 0$, $k \in \text{poly}(n)$, it is not possible for a quantum adversary running in time $\text{poly}(n)$ to produce a state ρ such that $\langle\psi|^{\otimes k+1} \rho |\psi\rangle^{\otimes k+1}$ is non-negligible (in n).[1]

In order to prevent a counterfeiter from performing quantum state tomography [**AJK04**] and precisely determining the state $|\psi\rangle$, the bank should avoid issuing more than a polynomial number (in n) of coins.

Information theoretically, no offline quantum coin scheme can be perfectly unforgeable (that is, with $\langle\psi|^{\otimes k+1} \rho |\psi\rangle^{\otimes k+1} = 0$ and no running time restriction in Definition 3.2). If a forger has a verification circuit and unbounded quantum computational resources, the forger can repeatedly generate test states until one such state passes; after verification, this state is projected into a valid money state and

[1] In the language of Aaronson [**Aar09**], this is a single key public key quantum money scheme with completeness error 0 and soundness error negligible in n.

can subsequently be used as a money token. Thus, we must introduce computational assumptions on a forger and attempt to lower bound the amount of work required to forge.

Without any further specification of the quantum coin scheme and the verification circuit, we cannot say anything more about the unforgeability of such schemes. In Section 4.2, we show that a black box quantum coin scheme is unforgeable.

3.1.3. *Anonymity.* In our ideal formulation, all quantum coins (for a particular denomination) are minted as the same quantum state $|\psi\rangle$. However, the bank could create quantum coins from different quantum states, all of which can be verified by a particular verification circuit. Although we have no procedure for users to test the anonymity of the system, it would be possible for a regulator to regularly review the procedures of the bank and ensure that it is issuing identical tokens as the coins. If indeed all the coins issued are identical, then it is impossible for the use of a coin to be tracked. If quantum circuits can be obfuscated, then the verification circuit could be provided in an obfuscated form as a fixed public classical string which merchants then implement; since the circuit is fixed for all merchants, this would give anonymity to merchants as well. If an interactive protocol is required for verification (as in our use of blind quantum computing in Section 5), then anonymous classical [**BT07**] and quantum [**BBF$^+$07**] communication can be used to improve the anonymity of merchants.

3.2. Quantum bills. Whereas all quantum coins of the same denomination are identical states, with *quantum bills* we allow tokens of the same denomination to be different quantum states and additionally allow some classical information associated with each quantum state. So a bank might issue a set of states $\{(s_i, |\psi_i\rangle) : i \in \Gamma\}$ as the valid \$20 bills. This corresponds to physical bills which have a distinct serial number on each bill.

An example of an approach one might take to making quantum bills would be the following. Let a be an element of order m of some group G and let r be a function that encrypts elements of G. Suppose there were a way to publish a circuit C that implements, for any group element b and integer $y \in \{0, 1, \ldots, m-1\}$, the mapping $|y\rangle |r(b)\rangle \to |y\rangle |r(ba^y)\rangle$ but from which one cannot (among other things) determine x given $|r(a^x)\rangle$. (Note that the standard quantum discrete logarithm algorithm for computing x would require a means for computing $r(a^{zx+y})$ for arbitrary integers z and y.) Then a possible way to generate quantum money is for a bank to perform eigenvalue estimation (starting from a state $|r(b)\rangle$) in order to generate a random eigenstate of the operation induced by C, of the form

$$|\psi_k\rangle = \sum_{x=0}^{m-1} e^{-2\pi i k x/m} |r(ba^x)\rangle \quad ,$$

together with the eigenvalue parameter k. The bank would publish an authentic list of valid parameters k. The bill would consist of the state $|\psi_k\rangle$ and the classical value k, which any verifier could check by performing eigenvalue estimation on the bill and confirming the eigenvalue parameter is k (and that k is on the authentic list of valid serial numbers). There are many variations of this approach that one might try, and many open questions. We will focus on quantum coins in this paper.

Definition 3.3. A *quantum bill scheme* is a pair $(V, \{(s_i, |\psi_i\rangle) : i \in \Gamma\})$, where Γ is a finite set, and for each $i \in \Gamma$, s_i is a label in a set $\mathcal{S}$, $|\psi_i\rangle$ is an n-qubit pure

state in a 2^n-dimensional Hilbert space $\mathcal{H}^{2^n}$. Moreover, V is a quantum circuit with a quantum input register (denoted $|s\rangle$), a quantum n-qubit input register (denoted ρ), plus optional ancilla quantum registers, a classical output bit, and a quantum output register of n qubits.[2]

3.2.1. *Verification.* A generic verification circuit for a quantum bill scheme is given in Figure 3.

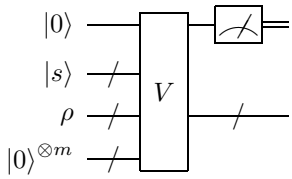

FIGURE 3. Generic verification circuit for a quantum bill scheme $(V, \{(s_i, |\psi_i\rangle) : i \in \Gamma\})$.

The use of the classical label s_i may vary according to the scheme. For example, in the schemes of Wiesner [**Wie83**] and Bennett *et al.* [**BBBW82**], s_i is a serial number that allows the issuer to retrieve the verification details, while in the scheme of Tokunga *et al.* [**TOI03**], s_i is effectively unused; in their scheme it is used to represent the denomination of the bill (e.g., \$5), but in our formulation the denomination is fixed for a particular scheme so the label is effectively the empty string for all $i \in \Gamma$. Schemes where s_i is non-trivial and unchanged by verification inherently limit the anonymity of the scheme, just as the serial number on physical bills places some limits on anonymity.

While all previous quantum money schemes discussed in Section 1 are classified as quantum bill schemes based on the above definition, none of them satisfy all of the security properties described in Section 2. In particular, no previous quantum money scheme is offline verifiable: all previous schemes require that the issuer verify a token via quantum communication, a requirement which we aim to remove for quantum coins. In the rest of this paper, we are only concerned with quantum coin schemes, not quantum bill schemes.

4. Black box quantum coins

Our first implementation for quantum coins works in the black box circuit model. We assume the verification circuit provided to the public is a black box: "anything one can compute from it one could also compute from the input-output behavior of the program" [**BGI+01a**, p. 2]. With this assumption, we present a scheme in which coins are unforgeable. The scheme allows coins to be transferred an arbitrary number of times. The use of a black box circuit means that coins can be verified locally without any communication, classical or quantum, with the bank.

We note that it is not known at present whether a quantum circuit can be implemented as a true black box. There are pessimistic results about the ability to obfuscate classical circuits [**BGI+01b**], although loopholes do exist: for example,

[2]In the language of Aaronson [**Aar09**], this is a public key quantum money scheme.

point functions can be obfuscated [**Wee05**]. However, no results are known about quantum circuits. Another classical technique for black box computation is physically tamper-proof hardware, but again the parallel in quantum computation is not clear.

In our black box construction, a coin is a randomly chosen secret state, and the verification circuit recognizes precisely that state using an oracle like the iterate in amplitude amplification [**BBHT98**].

Let $|\psi\rangle$ a pure state chosen randomly (according to the Haar measure) from among the pure states in $\mathcal{H}^{2^n}$. The verification oracle is $U_\psi = I - 2|\psi\rangle\langle\psi|$. Since this is a black-box oracle scheme, the unforgeability proof of Section 4.2 applies and the scheme is unforgeable in the black-box oracle model.

In practice, however, choosing a pure state $|\psi\rangle$ randomly according to the Haar measure with the additional constraints that we must be able to compute $I - 2|\psi\rangle\langle\psi|$ and that we must be able to produce many copies of $|\psi\rangle$ is problematic and it is not known how to do so in polynomial time. Recent work has focused on developing *approximate quantum t-designs* [**AE07**] where, roughly speaking, t copies of a state can be efficiently constructed such that tensor product state is sufficiently close to t copies of a state selected uniformly at random according to the Haar measure. Aaronson [**Aar09**, Theorem 8] gives a technique for constructing $t \in \text{poly}(n)$ copies of a pseudorandom state that are nearly indistinguishable (that is, negligibly different) from t copies of a truly random state by any measurement, even allowing the measurement procedure to make $\text{poly}(n)$ calls to an oracle U_ψ recognizing the state. Aaronson's technique allows us to use pseudorandom states instead of truly random states with a negligible loss in security.

We note that, for quantum coins, it is not sufficient to choose a random binary string encoded randomly in a pair of non-orthogonal bases, such as the so-called "BB84" bases. An adversary with a small number of quantum coins, say $O(\log n)$, can measure each qubit of the $O(\log n)$ tokens in both bases, and will with good probability find the correct basis choices and thus the random binary string, allowing her to then create arbitrarily many forged coins.

4.1. Verification. Let U_ψ be an oracle that recognizes the state $|\psi\rangle$ by flipping the sign of the phase of the state $|\psi\rangle$. That is, $U_\psi|\psi\rangle = -|\psi\rangle$ and $U_\psi|\phi\rangle = |\phi\rangle$ for all $|\phi\rangle$ orthogonal to $|\psi\rangle$; in other words, $U_\psi = I - 2|\psi\rangle\langle\psi|$.

We can construct a verification circuit V from the oracle U_ψ as follows. On the data readout register, input the state $|0\rangle$, then perform a Hadamard transformation on the ancilla. Use the ancilla as the control bit of a controlled-U_ψ applied to the input state ρ. Then perform a Hadamard transformation again on the ancilla and measure it in the computational basis. The circuit diagram is given in Figure 4.

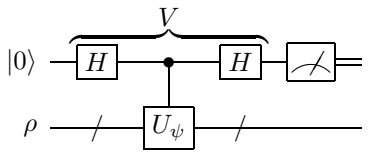

FIGURE 4. Verification circuit for quantum coins $|\psi\rangle$ recognized using the oracle U_ψ.

When a measurement in the computational basis is performed on the ancilla register, the result will be $|1\rangle$ when the input state ρ is $|\psi\rangle$ and $|0\rangle$ when the input state is $|\phi\rangle$ for $\langle\phi|\psi\rangle = 0$. Moreover, the state on the second register remains unchanged when its input is $|\psi\rangle$.

The fact that a valid token is unchanged by the verification process allows transferability of quantum coins. When a customer spends a quantum coin at a store, the merchant, after verifying and accepting the coin, can retain the coin until the merchant needs to make change. At that time, the merchant can give the coin to another user who, after optionally verifying the coin, can use that coin in another transaction. (In fact, the verification process not only enables transferability but also enhances the robustness of the quantum coins. Although over time a quantum state may decohere, at verification time the token may still be sufficiently close to the expected state $|\psi\rangle$ to pass the verification process with high probability. If it does pass, then the measurement process will project the coin back into the original state $|\psi\rangle$.)

Security. The verification procedure described in the previous section yields a correct quantum money scheme: valid money tokens are recognized. We now discuss the security of such a scheme. For unforgeability, we want that invalid tokens are recognized as being invalid and that it is difficult to forge new money.

4.2. Black-box unforgeability. To analyze the forgeability of the quantum coin scheme given in Figure 4, we suppose that the circuit for the unitary U_ψ is a black box, meaning that no information can be obtained from observing its inner workings; equivalently, we assume that U_ψ is given as an oracle. Having made this assumption, we proceed to obtain a lower bound on the number of queries to the oracle that must be made in order to produce a state that has a particular overlap p with $|\psi\rangle^{\otimes k+1}$, when the adversary is only given k coins. We show this result in the next section.

Definition 4.1. A quantum coin scheme $(V, |\psi\rangle)$, where $|\psi\rangle$ is an n-qubit state, is *black-box unforgeable* if, given an oracle U_ψ recognizing the state $|\psi\rangle$ and k copies of the state $|\psi\rangle$, for any $k \geq 0$, $k \in \text{poly}(n)$, it is not possible for a quantum adversary using $\text{poly}(n)$ queries to U_ψ to produce a state ρ such that $\langle\psi|^{\otimes k+1} \rho |\psi\rangle^{\otimes k+1}$ is non-negligible.[3]

We note that our definition of unforgeability has the adversary producing a $(k+1)$-register state, each register of which should overlap well with $|\psi\rangle$. An alternative formulation could be that the adversary needs to produce a multi-register state such that some $k+1$ of its registers, but not necessarily all of its registers, overlap well with $|\psi\rangle$. These definitions are equivalent. The adversary has access to a verification oracle and, for each of the many registers it constructs, could simply apply the verification oracle to each register and then trace out any registers that do not pass verification. This requires additional calls to the verification oracle, but still only $\text{poly}(n)$ calls to the oracle (since a polynomial-time adversary can only construct $\text{poly}(n)$ registers), and hence remains within the constraints of the security argument above.

[3]In the language of Aaronson [**Aar09**], this is a single key private key quantum money scheme with completeness error 0 and soundness error negligible in n.

We note as well that it is not necessary to extend this definition to $k+\ell$ copies of $|\psi\rangle$: any adversary who can construct $k+\ell$ copies of $|\psi\rangle$ with non-negligible probability can in particular construct $k+1$ copies of $|\psi\rangle$ with non-negligible probability. In other words, there are no "long shots" that pay off in expected value: the definition precludes being able to generate a very large number of coins with a very small probability but with non-negligible expected number of coins.

We now aim to show that a generic quantum coin scheme implemented with black-box oracles as in Figure 4 is black-box unforgeable. However, we cannot use the basic no-cloning theorem [**WZ82, Die82**] or the result on approximate cloning [**BM07**] because not only does a forger have copies of the state $|\psi\rangle$, the forger also has an oracle U_ψ that will indicate whether the attempted cloning was successful. Similarly, we cannot directly apply the $\Omega(\sqrt{N})$ lower bound on quantum search [**BBBV97**] because the forger has not only an oracle U_ψ recognizing the desired state but also some copies of the state itself. Rather, we need a hybrid of these two results.

Aaronson [**Aar05a**] gives the following complexity-theoretic version of the no-cloning theorem that combines the lower bound for quantum search with the no-cloning theorem.

THEOREM 4.2 (Theorem 5, [**Aar05a**]). *Let $|\psi\rangle$ be an n-qubit pure state. Suppose we are given the initial state $|\psi\rangle^{\otimes k}$ for some $k \geq 1$ as well as an oracle U_ψ such that $U_\psi|\psi\rangle = -|\psi\rangle$ and $U_\psi|\phi\rangle = |\phi\rangle$ whenever $\langle\phi|\psi\rangle = 0$. Then to prepare a state ρ such that*

$$\langle\psi|^{k+1} \rho |\psi\rangle^{k+1} \geq p \tag{4.1}$$

we need

$$\Omega\left(\frac{\sqrt{2^n p}}{k \log k} - k\right) \tag{4.2}$$

queries to U_ψ.

This allows us to show that a quantum coin scheme is unforgeable in the black-box oracle model.

THEOREM 4.3. *Let $(V, |\psi\rangle)$ be a quantum coin scheme, where V is as in Figure 4 with U_ψ given as a black-box oracle, and $|\psi\rangle$ is an n-qubit pure state. If not more than $\mathrm{poly}(n)$ coins are issued, then $(V, |\psi\rangle)$ is black-box unforgeable.*

PROOF. Suppose otherwise. Then there exists an adversary who, upon receiving k copies of $|\psi\rangle$ and using $q = \mathrm{poly}(n)$ queries to U_ψ, can produce a state ρ such that $\langle\psi|^{\otimes k+1} \rho |\psi\rangle^{\otimes k+1} = p \in 1/\mathrm{poly}(n)$. By Theorem 4.2, we need

$$q = \Omega\left(\frac{\sqrt{2^n p}}{k \log k} - k\right) = \Omega\left(\frac{\sqrt{2^n/\mathrm{poly}(n)}}{\mathrm{poly}(n)\log \mathrm{poly}(n)} - \mathrm{poly}(n)\right) = \Omega\left(\frac{\sqrt{2^n}}{\mathrm{poly}(n)}\right) \tag{4.3}$$

queries to U_ψ. But since the adversary is allowed only a polynomial number q of queries to U_ψ, we have that $q \in \mathrm{poly}(n)$ and hence $\mathrm{poly}(n) = \Omega\left(\frac{\sqrt{2^n}}{\mathrm{poly}(n)}\right)$, which is a contradiction. Thus the quantum coin scheme must be black-box unforgeable. □

5. Quantum coins using blind quantum computation

Blind quantum computation allows one party, Alice, to have another party, Bob, perform computations on her behalf without Bob learning any information about the input state, output state, or the operation performed.

Blind quantum computation was first introduced by Childs [**Chi05**] under the name "secure assisted quantum communication". The basic idea is that Alice, who has limited quantum computational abilities (quantum communication, quantum storage, and controlled-X and controlled-Z gates) can have Bob securely perform arbitrary quantum computation, with quantum input and quantum output. In Childs' protocol, Alice and Bob must perform large amounts of quantum communication, though this could be replaced by quantum teleportation (shared entanglement with Bell measurements and classical communication).

Broadbent, Fitzsimons, and Kashefi [**BFK09**] present a protocol for blind quantum computation with quantum input and output using measurement-based quantum computation that needs only two rounds of quantum communication: one at the beginning and one at the end.

Blind quantum computation could be used as follows for verifying quantum coins as follows. The merchant, playing the role of Bob, implements the verification circuit blindly for the bank, playing the role of Alice. The merchant receives the coin as the input to the circuit, and interacts with the bank who helps it implement the circuit. In the [**BFK09**] scheme, this requires mostly classical interaction, with a round of quantum interaction at the end for the final output correction. In the end, the output state along with the accept/reject information is with the merchant. Since the bank is actively involved in the verification procedure, the merchant must trust that the bank is not colluding with the customer.

Although the quantum communication requirements for verifying quantum coins using blind quantum computation are no better than simply teleporting the coin to the bank for verification, the quantum computation requirement for the bank is markedly reduced: instead of having to implement the full quantum circuit for coin verification for the thousands of coins being verified each second, it only has to perform step 5 of Protocol 3 of [**BFK09**], which consists of at most one X gate and one Z gate per coin qubit.

Obviously, it would be preferable to reduce this quantum communication requirement even further, for example by only requiring quantum communication at the beginning of the protocol and only classical communication for the remainder of the protocol, and without using shared entanglement for teleportation. A protocol for doing so would be an interactive protocol for quantum circuit obfuscation, and quantum obfuscation is a long standing open problem (cf. [**Aar05b**]).

Acknowledgements. The authors gratefully acknowledge helpful discussions with Scott Aaronson, Anne Broadbent, Joseph Fitzsimons, Miklos Santha, and John Watrous.

References

[Aar05a] Scott Aaronson, *Quantum copy-protection*, Private correspondence, 2005.

[Aar05b] ———, *Ten semi-grand challenges for quantum computing theory*, July 2005.

[Aar09] ———, *Quantum copy-protection and quantum money*, IEEE 24th Conference on Computational Complexity (CCC) 2009, IEEE, 2009, To appear.

[AE07] Andris Ambainis and Joseph Emerson, *Quantum t-designs: t-wise independence in the quantum world*, Proc. 22nd Ann. IEEE Conference on Computational Complexity (CCC) 2007, IEEE, June 2007, pp. 129–140.

[AJK04] Joseph B. Altepeter, Daniel F. V. James, and Paul G. Kwiat, *4 qubit quantum state tomography*, Quantum State Estimation (Matteo Paris and Jaroslav Řeháček, eds.), Lecture Notes in Physics, vol. 649, Springer, 2004, pp. 113–145.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani, *Strengths and weaknesses of quantum computing*, SIAM Journal on Computing **26** (1997), no. 5, 1510–1523.

[BBBW82] Charles H. Bennett, Gilles Brassard, Seth Breidbard, and Stephen Wiesner, *Quantum cryptography, or unforgeable subway tokens*, Advances in Cryptology – Proc. CRYPTO '82 (David Chaum, Ronald L. Rivest, and Alan T. Sherman, eds.), Plenum Press, 1982.

[BBF+07] Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp, *Anonymous quantum communication*, in Kurosawa [**Kur07**], pp. 460–473.

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp, *Tight bounds on quantum searching*, Fortschritte der Physik **46** (1998), no. 4–5, 493–505.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi, *Universal blind quantum computation*, Proc. 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2009, IEEE Press, 2009, To appear.

[BGI+01a] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang, *On the (im)possibility of obfuscating programs*, 2001, Published as [**BGI+01b**].

[BGI+01b] ———, *On the (im)possibility of obfuscating programs*, Advances in Cryptology – Proc. CRYPTO 2001 (Joe Kilian, ed.), LNCS, vol. 2139, Springer, 2001, Full version available as [**BGI+01a**], pp. 1–18.

[BM07] Dagmar Bruß and Chiara Macchiavello, *Approximate quantum cloning*, Lectures on Quantum Information (Dagmar Bruß and Gerd Leuchs, eds.), Wiley-VCH, 2007.

[BT07] Anne Broadbent and Alain Tapp, *Information-theoretic security without an honest majority*, in Kurosawa [**Kur07**], pp. 410–426.

[CFN88] David Chaum, Amos Fiat, and Moni Naor, *Untraceable electronic cash (extended abstract)*, Advances in Cryptology – Proc. CRYPTO '88 (Shafi Goldwasser, ed.), LNCS, vol. 403, Springer, 1988, pp. 319–327.

[Cha85] David Chaum, *Security without identification: transaction systems to make big brother obsolete*, Communications of the ACM **28** (1985), no. 10, 1030–1044.

[Cha88] ———, *Privacy protected payments: Unconditional payer and/or payee untraceability*, Smartcard 2000 (David Chaum and I. Schaumuller-Bichl, eds.), North Holland, 1988, pp. 69–93.

[Chi05] Andrew Childs, *Secure assisted quantum computation*, Quantum Information and Computation **5** (2005), no. 6, 456–466.

[CP92] David Chaum and Torben Pryds Pedersen, *Transferred cash grows in size*, Advances in Cryptology – Proc. EUROCRYPT '92 (Rainer A. Rueppel, ed.), LNCS, vol. 658, Springer-Verlag, 1992, pp. 390–407.

[Die82] D. Dieks, *Communication by EPR devices*, Physics Letters A **92** (1982), no. 6, 271–272.

[Kur07] Kaoru Kurosawa (ed.), *Advances in cryptology – proc. ASIACRYPT 2007*, LNCS, vol. 4833, Springer, 2007.

[MS06] Michele Mosca and Douglas Stebila, *Uncloneable quantum money*, Canadian Quantum Information Students' Conference (CQISC) 2006 (Calgary, Alberta), August 2006.

[MS07] ———, *A framework for quantum money*, Quantum Information Processing (QIP) 2007 (Brisbane, Australia), January 2007.

[Ste09] Douglas Stebila, *Classical authenticated key exchange and quantum cryptography*, Ph.D. thesis, University of Waterloo, 2009.

[TOI03] Yuuki Tokunaga, Taisuaki Okamoto, and Nobuyuki Imoto, *Anonymous quantum cash*, ERATO Conference on Quantum Information Science (EQIS) 2003, September 2003.

[Wee05] Hoeteck Wee, *On obfuscating point functions*, Proc. 37th Annual ACM Symposium on the Theory of Computing (STOC), ACM Press, 2005, pp. 523–532.

[Wie83] Stephen Wiesner, *Conjugate coding*, ACM SIGACT News **15** (1983), no. 1, 78–88.

[WZ82] William K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802–803.

Institute for Quantum Computing and Department of Combinatorics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada; Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON, N2L 2Y5, Canada
E-mail address: mmosca@iqc.ca

Information Security Institute, Queensland University of Technology, Brisbane, Queensland 4001, Australia
E-mail address: douglas@stebila.ca