University of Waterloo

IQC Institute for Quantum Computing

Uncloneable Quantum Money

Douglas Stebila[1]

Institute for Quantum Computing
University of Waterloo

Joint work with Michele Mosca

CQISC 2006

[1] Supported by NSERC, Sun Microsystems, CIAR, CFI, CSE, MITACS, ORDCF.

Outline

Motivation for quantum money

- One of the main challenges for digital money is ensuring that it cannot be counterfeited.
- If we use quantum states to represent money, the no-cloning theorem might help us prevent it from being copied.
- Quantum money was one of the earliest applications of quantum information theory.
- We present a new model for quantum money based on the difficulty of counterfeiting in the black box model.

Requirements of money

- Non-counterfeitable
  - Given 0 or more pieces of money and a method for verifying money, it should be difficult to create more money than you started with.
- Efficiently offline verifiable
  - Money should be verifiable by anyone with a verification device, preferably without having to use online communication to a bank.
- Anonymous
  - When money is used in a purchase or redeemed at a bank, it should be difficult to determine who originally withdrew the money.

Requirements of money

- Transferable
  - Money should be able to be transferred from one party to another.
  - For example, a store should be able to give out tokens it has received as change to other customers.
- Robust
  - Money should last a sufficiently long time and not be able to be inadvertently destroyed.

Classical digital cash

- Classical digital cash was first proposed by Chaum [Cha85, Cha88] and Chaum, Fiat, and Naor [CFN88].
- The security of classical digital cash is based on various classical (public key) cryptography problems.
- Since the tokens are classical data, they can be copied as many times as desired.
- Thus, the main problem in designing classical digital cash schemes is detecting and preventing multiple spending.

Multiple spending vs. anonymity

- The obvious method for detecting multiple spending is to verify a token when it is presented at purchase time.
- However, this requires an online verification which can be inconvenient or expensive.
- Instead, we could want an offline way to verify the validity of the token at purchase time and then at a later time redeem them with the bank to see if they've been spent multiple times.
- Some schemes encode information in the tokens so that if they are redeemed once, the spender remains anonymous, but if they are redeemed twice the bank has enough information to recover the identity of the spender.

Drawbacks of classical digital cash

- Non-transferable
  - Can't give reuse previous tokens in new transactions.
- Either not offline verifiable or not anonymous
  - Requires online verification or requires embedding of identity inside tokens to be used in the case of multiple spending.
- All schemes are based on computational assumptions.

[BBBW82]: "unforgeable subway tokens"

- A computational number theory problem (factoring) is embedded in a quantum state.
- Let $n = pq$, $\gcd(a, n) = 1$, $x^2 \equiv y^2 \equiv a \mod n$.
- x and y are encoded ("multiplexed") in a single $\log_n$-bit quantum string so that at most one of x, y can be obtained using individual measurements.
- If the obtained string is a square root of $a \mod n$, then accept the token.
- Pros: Tokens can be efficiently verified offline with only knowledge of n.
- Cons: Tokens are non-transferable, not necessarily anonymous, and non-counterfeitable only if factoring is hard and an adversary is allowed only individual, not coherent, attacks.

Wiesner: conjugate bases

- Wiesner [Wie83] proposed a quantum money scheme based on encoding in conjugate bases (e.g., the BB84 bases).
- A secret binary string B is used to choose the bases in which another secret binary string S is encoded.
- The choice of B and S must be different for each token to prevent quantum state tomography, so each token must also have a serial number.
- Tokens can only be verified by parties that know both B and S for every serial number: only the bank, or a party trusted by the bank, can verify a token.
- Pros: Tokens cannot be counterfeited except with exponentially-small probability in the number of qubits.
- Cons: Tokens are non-transferable, not offline verifiable, and not necessarily anonymous.

[TOI03]: Anonymous quantum cash

- Tokunaga, Okamoto, and Imoto [TOI03] created a scheme similar to Wiesner's scheme but which allows anonymity.
- As before, a random binary string is encoded in a fixed secret set of bases, with the condition that some of the bits that are encoded are parity check bits.
- A user masks the token by applying a randomly chosen unitary of a certain form that randomizes the binary string encoded but preserves the parity check conditions.

[TOI03]: Anonymous quantum cash

- Tokens are verified by sending them to the bank; the bank checks the parity check bits. Because of the random unitary applied, no information other than the validity of the token can be obtained.
- Anonymous only if bank issues tokens of the specified form; no method for a user to verify this.
- Only proven secure against attacks against individual tokens, not against all issued tokens.
- Pros: Tokens cannot be counterfeited except with exponentially-small probability in the number of qubits and are anonymous.
- Cons: Tokens are non-transferable and not offline verifiable.

Quantum coins

- Tokens are n-qubit pure states in an 2^n-dimensional Hilbert space $\mathcal{H}$.
- A valid money state is a single pure state $|\psi\rangle$; all tokens for the same denomination are the same state.
- Alternatively, an entire 2^d-dimensional subspace $\mathcal{L}$ of $\mathcal{H}$ could represent valid money states; tokens for the same denomination could be chosen from this subspace.
- To prevent a counterfeiter from performing quantum state tomography, an issuer should not issue more than $\mathrm{poly}(n)$ states.

Verification

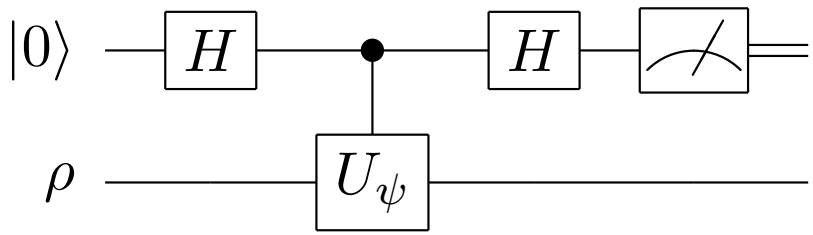
- The issuer provides an offline verification circuit that recognizes valid money states.
- The circuit is implemented using an oracle which flips the sign on the phase of valid money tokens and does nothing to states that are orthogonal to valid money tokens.
- The circuit is treated as a black box: given the decomposition of the circuit, one shouldn't be able to do much more than just given an oracle.
- Let $|\psi\rangle$ be the single valid money state. Let U_ψ be an oracle such that

$$U_\psi |\psi\rangle = -|\psi\rangle, \qquad U_\psi |\varphi\rangle = |\varphi\rangle,$$

for all $|\varphi\rangle$ orthogonal to $|\psi\rangle$ (i.e., $\langle\varphi|\psi\rangle = 0$).

Verification

- Let $\mathcal{C}_{U_\psi}$ be the following circuit:



- If ρ is a valid money state $|\psi\rangle$, then the result of the measurement is 1.
- When the input is orthogonal to a valid money state, the result of the measurement is 0.

Transferability

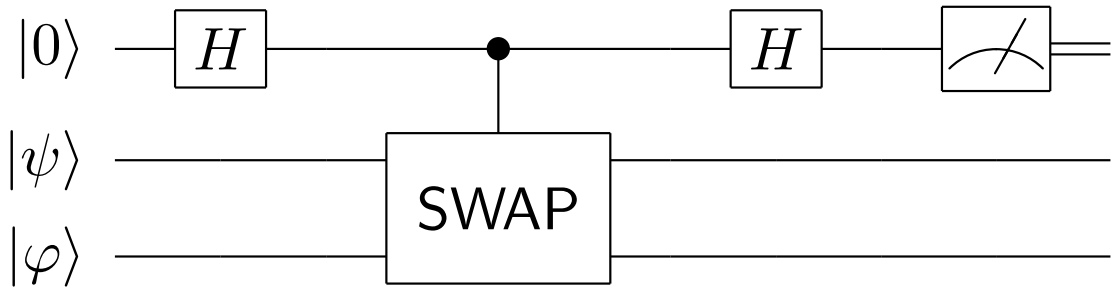
- When a valid token is input and the measurement result is 1, then the state is unchanged by verification.
- Thus the state can be reused by the person who received the state in another transaction.
- This also improves the robustness of the state. Suppose the state has decohered a little, but not so much that it is unlikely to pass verification.
- If it passes verification, then it is projected into a valid money state and is now a perfect version of a valid money state.

Anonymity

- An issuer could create money states that are not all identical states $|\psi\rangle$.
- For example, an issuer could create up to 2^d different money states from a 2^d-dimensional subspace $\mathcal{L}$. The issuer can distinguish among these states and may be able to trace the use of a coin.
- Our main tool for detecting dishonest issuers is the swap test.

The swap test

- The circuit for the swap test [BCWW01] is:



- The probability of measuring 1 in the first register is

$$\frac{1}{2}\left(1 - |\langle\varphi|\psi\rangle|\right).$$

- If the two input states $|\psi\rangle$ and $|\varphi\rangle$ are the same, then the probability of measuring a 1 in the first register is 0.

Anonymity using the swap test

- A user can check the anonymity of a given token ρ by obtaining a k randomly-chosen other money states $\sigma_1, \ldots, \sigma_k$ and running the swap test for ρ with each σ_i, $i = 1, \ldots, k$.
- Note there is no value in running the swap test again with the same σ_i: once a pair of states passes a swap test, they are projected into a subspace which will always pass subsequent swap tests.
- If any of the swap tests fail, then there is a non-negligible probability that an issuer can distinguish ρ from other valid money states.
- If none of the swap tests fail, then with high probability the amount of information the issuer can obtain to distinguish ρ from other states is negligible.

Model for black box counterfeiting

- A counterfeiter has k copies of a valid money state $|\psi\rangle$.
- Additionally, the counterfeiter has access to a verification circuit $\mathcal{C}_{U_\psi}$ as a black box oracle.
- Goal: Produce $k+1$ states that are likely to pass the verification process.
- Construct ρ such that

$$\langle\psi|^{\otimes k+1} \rho |\psi\rangle^{\otimes k+1} \geq p.$$

Modelling security against counterfeiting

- Want to obtain a lower bound on the amount of work needed to obtain a state ρ such that

$$\langle\psi|^{\otimes k+1} \rho |\psi\rangle^{\otimes k+1} \geq p.$$

- Can we use the no-cloning theorem?
  - No, because in addition to being given k copies of $|\psi\rangle$, a counterfeiter is also given an oracle recognizing $|\psi\rangle$.
- Can we use search lower bounds?
  - No, because in addition to being given an oracle recognizing $|\psi\rangle$, a counterfeiter is also given k copies of $|\psi\rangle$.
- We need to merge these two techniques.

A hybrid no-cloning theorem

- Aaronson [Aar06] gives a complexity-theoretic version of the no-cloning theorem that combines
  - the lower bound for quantum search and
  - the no-cloning theorem.
- **Theorem.** Given k copies of an n-qubit pure state $|\psi\rangle$ and an oracle U_ψ recognizing a state $|\psi\rangle$. To prepare a state ρ such that $\langle\psi|^{\otimes k+1} \rho |\psi\rangle^{\otimes k+1} \geq p$ requires

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

queries to U_ψ.

A hybrid no-cloning theorem

- If a counterfeiter is given k copies of a valid money state $|\psi\rangle$, this reduces the number of queries required to make more money by only a polynomial amount in k.
- If an issuer only issues $\mathrm{poly}(n)$ money states, then a counterfeiter cannot clone quantum coins in polynomial time with non-negligible probability.

A generalized hybrid no-cloning theorem

- Suppose valid money states are not just a single state $|\psi\rangle$ but any state in a 2^d-dimensional subspace $\mathcal{L}$.
- The hybrid no-cloning theorem can be generalized for subspaces.
- **Theorem.** Given n-qubit pure states $|\psi_1\rangle, \ldots, |\psi_k\rangle$ in a 2^d-dimensional subspace $\mathcal{L}$ and an oracle $U_{\mathcal{L}}$ recognizing a states in $\mathcal{L}$. To prepare a state ρ such that $|\mathrm{Tr}\left(P_{\mathcal{L}^{\otimes k+1}}\rho\right)| \geq p$ requires

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

queries to $U_{\mathcal{L}}$.

Interpolating quantum search and quantum cloning

- Both of these hybrid no-cloning theorems provide an interpolation between the quantum search lower bound and the fidelity of approximate quantum cloning.
- If a constant (or zero) number of copies of valid states are given, then the lower bound corresponds to the number of queries needed for quantum search:
  - $\Omega(\sqrt{2^n})$ when there is one valid state, or
  - $\Omega(\sqrt{2^{n-d}})$ where there are 2^d valid states.
- If a constant (or zero) number of queries are allowed, then the lower bound corresponds to the fidelity of approximate quantum cloning.

Summary

- We have an introduced a new model for quantum money which is anonymous, transferable, and efficiently offline verifiable.
- We can prove lower bounds on the amount of work needed to counterfeit in the black box query model.
- Black box counterfeiting uses new results on combining quantum search lower bounds and the no-cloning theorem.
- We have several candidate quantum money schemes and are working on more.
- Announcement: effective 2038, grad students will be paid only using quantum money.

References I

[Aar06] S. Aaronson.
Quantum copy-protection, June 2006.
In preparation.

[BBBW82] C. H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner.
Quantum cryptography, or unforgeable subway tokens.
In D. Chaum, R. Rivest, and A. T. Sherman, eds., *Advances in Cryptology – Proc. CRYPTO '82*. Plenum Press, 1982.

[BCWW01] H. Burham, R. Cleve, J. Watrous, and R. de Wolf.
Quantum fingerprinting.
Phys. Rev. Lett., 87(16):167902, October 2001.
quant-ph/0102001.

[CFN88] D. Chaum, A. Fiat, and M. Naor.
Untraceable electronic cash (extended abstract).
In S. Goldwasser, ed., *Advances in Cryptology – Proc. CRYPTO '88*, volume 403 of *LNCS*, pp. 319–327. Springer, 1988.

[Cha85] D. Chaum.
Security without identification: transaction systems to make big brother obsolete.
Communications of the ACM, 28(10):1030–1044, October 1985.

[Cha88] D. Chaum.
Privacy protected payments: Unconditional payer and/or payee untracability.
In *Smartcard 2000*. North Holland, 1988.

References II

[TOI03] Y. Tokunaga, T. Okamoto, and N. Imoto.
Anonymous quantum cash.
In *ERATO Conference on Quantum Information Science (EQIS) 2003*. September 2003.

[Wie83] S. Wiesner.
Conjugate coding.
ACM SIGACT News, 15(1):78–88, 1983.