Uncloneable Quantum Money

Michele Mosca and Douglas Stebila

Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada. *Supported by Canada's NSERC, Sun Microsystems, CIAR, CFI, CSE, MITACS, and ORDCF.*

Abstract

One of the earliest cryptographic applications of the quantum no-cloning theorem was to create quantum digital cash that could not be counterfeited. In this poster, we develop two notions of quantum money, namely quantum coins and quantum bills, which have many of the desirable properties of digital cash, such as non-counterfeitability and transferability. Quantum coins can be non-destructively verified but cannot be efficiently cloned in the black box model. Quantum bills have greater resistance to counterfeiting outside the black box model at the expense of anonymity.

Security goals

- **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.
- **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.

The following table summarizes the security properties of various money systems. The use of a ○ denotes a property that is partially supported while ● denotes a fully-supported property.

Security goal	**Physical coins**	**Physical bills**	**Classical cash**	**Quantum coins**	**Quantum bills**
non-counterfeitable	○	○		●	●
offline verifiable	○	○	○	●	●
anonymous	●	○	○	●	○
transferable	●	●		●	●
robust	●	●	●	(not yet)	(not yet)

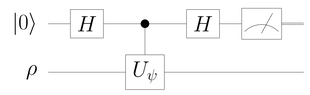
Quantum coins

Quantum coins are n-qubit pure quantum states where the same quantum state $|\psi\rangle$ is used for every token of a certain denomination. 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 $U_\psi|\psi\rangle = -|\psi\rangle$ and $U_\psi|\varphi\rangle = |\varphi\rangle$, for all $|\varphi\rangle$ orthogonal to $|\psi\rangle$ (i.e., $\langle\varphi||\psi\rangle = 0$). 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.

Black box counterfeiting

Model: 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. We want to obtain a lower bound on the amount of work needed to obtain a state ρ such that

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

Theorem [Aar07]. 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.

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. We can detect dishonest issuers through a distributed swap test.

Quantum bills

Quantum bills are classical-quantum states where many different states $(x, |\psi_x\rangle)$ are used for each denomination. Some schemes may need to authenticate x using digital signatures.

The classical string x can be thought of as a serial number or can play a role in the verification process. For example, the verification process could consist of eigenvalue estimation, and x should be the desired result.

Ongoing work

For **quantum coins**, we are investigating the role of obfuscation in realizing black box oracles.

For **quantum bills**, we are investigating a variety of candidate schemes based on black-box groups and lattice problems (the latter in collaboration with John Watrous). This may lead to interesting developments in "computationally-secure quantum cryptography", where security is based on the hardness of various computational problems such as the lattice gap-closest-vector problem (GapCVP). While this may seem undesirable compared to the information-theoretic security offered by quantum key distribution, it could allow for a greater variety of cryptographic tasks to be addressed in a quantum setting.

References

[Aar07] S. Aaronson. Quantum copy-protection. In preparation, 2007.

[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.

[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.