Franchised Quantum Money

Bhaskar Roberts[1] and Mark Zhandry[2]

[1]UC Berkeley and Princeton University [2]Princeton University
bhaskarr@berkeley.edu

Abstract

Classical bits can be copied, but quantum bits, in general, cannot. As a result, there is interest in creating uncounterfeitable quantum money, in which a set of qubits can be spent as money but cannot be duplicated. However existing constructions of quantum money are limited: the verification key, which is used to verify that a banknote was honestly generated, can also be used to create counterfeit banknotes. Recent attempts have tried to allow public key verification, where any untrusted user, even a would-be counterfeiter, can verify the banknotes. However, despite many attempts, a secure construction of public-key quantum money has remained elusive.

Here we introduce franchised quantum money (FQM), a new notion that is weaker than public key quantum money but brings us closer to realizing it. Franchised quantum money allows any untrusted user to verify the banknotes, and every user gets a unique secret verification key. Furthermore, we give a construction of franchised quantum money and prove security assuming the quantum hardness of the short-integer solution problem (SIS). This is the first construction of quantum money that allows an untrusted user to verify the banknotes, and which has a proof of security based on widespread assumptions. It is therefore a useful step toward public key quantum money.

Public Key Quantum Money

Generation: A trusted party called the mint generates the banknotes, and may use a secret key to do so.

Verification: Any untrusted user, with only a public key, can verify that a banknote was honestly generated by the mint.

Security: The scheme is secure if it is hard for an adversary with access to the public key and several honestly generated banknotes to generate an additional banknote that passes verification.

Franchised Quantum Money

Generation: Same as for public key quantum money.

Registration: The mint also distributes to each user a unique secret verification key.

Verification: With their unique key, an untrusted user can verify any banknote, but they cannot create counterfeit money that would fool another user. This is different from public key quantum money because the verification key may actually enable the user to create counterfeit banknotes, but the only person that the counterfeiter can fool is themselves.

Collusion bound: A small number of users may collude: pool their verification keys to increase their chance of successfully counterfeiting. As long as the number of colluding users is smaller than a fixed collusion bound, the scheme remains secure. In our construction, we can increase the collusion bound by increasing the size of the banknotes.

Relevance

For illustration, consider a group of large corporations, mutually distrustful, that nevertheless want to make transactions with each other. The mint gives each corporation a unique secret verification key that allows them to verify banknotes from another corporation. Now what if one corporation uses its key to create counterfeit banknotes? Then the counterfeit banknotes will fail to verify when a different corporation's key is used. So the dishonest corporation will not be able to fool anyone but themselves.

Franchised quantum money is the first form of quantum money that allows an untrusted user to verify banknotes without the mint involved, so franchised quantum money may serve as a stepping stone to constructing public key quantum money.

Construction of FQM

Banknote: The banknote is composed of independent components called mini-states. Each mini-state is a superposition over short colliding inputs to a SIS hash function. Then, the banknote is a concatenation of independent mini-states, each with a different hash function.

Verification key: For each mini-state, the verification key a short vector in the kernel of the hash function. However, the vector does not span the entire kernel. For the overall banknote, the verification key comprises the keys for a random subset of the mini-states.

Security: An adversary who knows a small number of verification keys has no information about some of the mini-states, and for the rest of the mini-states, they are not likely to know the entire kernel. Moreover, the verifier is likely to check a mini-state or a dimension of the kernel that the adversary knows nothing about. Therefore, the adversary's counterfeit banknote will fail verification with overwhelming probability.

Future Work

1. Adapt franchised quantum money to construct public key quantum money. Franchised quantum money is the first scheme to allow an untrusted user to verify a banknote without the mint involved, so it may be a stepping stone to public key quantum money.

2. Remove the collusion bound. Create a scheme that remains secure when the number of colluding users is any polynomial function of the security parameter.

Selected Bibliography

- [BF10] Dan Boneh and David Freeman. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. IACR Cryptology ePrint Archive, 2010:453, 01 2010.
- [GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. volume 14, pages 197-206, 05 2008.
- [Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, Advances in Cryptology - EURO-CRYPT 2019, pages 408-438, Cham, 2019. Springer International Publishing.