# Franchised Quantum Money

**Bhaskar Roberts**[1] and Mark Zhandry[2,3]

[1] UC Berkeley, [2] Princeton University, [3] NTT Research

Asiacrypt 2021

# Quantum Money

- Cash (physical money) should be:
  - Unclonable
  - Locally verifiable - no communication with the bank during verification
- Classical digital currency cannot be unclonable
- No-cloning theorem suggests unclonability may be possible
- *Public key quantum money* (PKQM)
  - Unclonable quantum banknotes
  - Can be verified locally with a public key

# Other Unclonable Primitives

- Other unclonable primitives include:
  - Copy protection
  - Copy detection and secure software leasing
  - Unclonable signature tokens
- The proposed constructions of these primitives are often based on proposals for quantum money [BS17; Aar+20; KNY21]

# Approaches to PK Quantum Money

- There are many proposals for quantum money
- [AC12; Zha19] uses quantum-secure iO

# Franchised Quantum Money

- *Public key quantum money* (PKQM) - Banknotes are verified with a single public key.
- *Franchised quantum money* (FQM) - Each verifier gets a unique secret key.
  - The adversary doesn't know the verifier's key, so it's harder to trick the verifier

# Applications

- Money
- Secure software leasing
- Other unclonable primitives in the franchised model?

# Public Key Quantum Money

Syntax

- $Setup(1^\lambda) \to pk, sk$
- $Mint(sk) \to |\$\rangle$
- $Ver(pk, |\$\rangle) \to b, |\$'\rangle$

# PKQM from iO

- Computations are done over $\mathbb{Z}_2^n$, an $n$-dimensional finite vector space.
- Secret key: $sk$ is a random subspace $A$ such that $dim(A) = dim(A^\perp) = n/2$
- Banknote: $|\$\rangle \propto \sum_{x \in A} |x\rangle$
- Public key: $pk = (O_A, O_{A^\perp})$, a pair of oracles deciding membership in $A$ and $A^\perp$.
  - The oracles are obfuscated using quantum-secure iO.

# PKQM from iO

*Ver*:

1. Check that $O_A(|\$\rangle)$ passes.
2. Take the quantum Fourier transform: $|\$\rangle \to |\tilde{\$}\rangle$
   - A valid banknote becomes $|\tilde{\$}\rangle \propto \sum_{y \in A^\perp} |y\rangle$
3. Check that $O_{A^\perp}(|\tilde{\$}\rangle)$ passes.

# FQM Construction (simplified)

- Master secret key: a random subspace $A$
- Banknote: $|\$\rangle \propto \sum_{x \in A} |x\rangle$
- Verification key:
  - Let $V \leq A$ be a random subspace of dimension $\Theta(\sqrt{n})$.
  - Let $W \leq A^{\perp}$ be a random subspace of dimension $\Theta(\sqrt{n})$.
  - $vk = (O_{W^{\perp}}, O_{V^{\perp}})$
  - $O_{W^{\perp}}$ and $O_{V^{\perp}}$ do not need to be obfuscated

# FQM Construction (simplified)

*Ver*:

1. Check that $O_{W^\perp}(|\$\rangle)$ passes.
2. Take the quantum Fourier transform of the banknote.
3. Check that $O_{V^\perp}(|\tilde{\$}\rangle)$ passes.

# Collusion Bound

- If $\omega(\sqrt{n})$ verifiers collude, they can learn the entire subspace, with high probability.
- Then they can create counterfeit banknotes.
- We require a collusion bound: no more than $C = O(\sqrt{n})$ verifiers can collude.
- Future work aims to improve or eliminate the collusion bound.

# Security

We prove security against two kinds of attacks:

1. *Counterfeiting*: The adversary gets $n$ banknotes and produces $n+1$ states that pass verification
2. *Sabotage*: adversary introduces error into a banknote so that one user accepts it but another user rejects it
   - Does not require that the adversary can counterfeit

# Security Proof

- *Full verifier*: the verification key is $(O_A, O_{A^\perp})$
  - Equivalent to [AC12]'s construction of PKQM
- *Franchised verifier*: the verification key is $(O_{W^\perp}, O_{V^\perp})$, for random subspaces $V \leq A$ and $W \leq A^\perp$

# Security Proof

- Main Lemma: the adversary can't distinguish whether they're interacting with full or franchised verifiers
  - Proof based on the adversary method
  - $O_{W^\perp}$ and $O_{V^\perp}$ each accept a negligible fraction of $\mathbb{Z}_2^n$

# Security Proof

[AC12]'s construction is secure against counterfeiting and sabotage, so our FQM construction is as well

# Future Work

- Improve the collusion bound.
  - For any $poly(\lambda)$ collusion bound $C$, there should be an efficient FQM scheme (polynomial size and runtime) that is secure against $C$ colluding adversaries.
  - Perhaps techniques from traitor tracing will help [GKW18]

# References I


[Aar+20] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. *New Approaches for Quantum Copy-Protection*. 2020. arXiv: 2004.09674 [cs.CR].

[AC12] Scott Aaronson and Paul Christiano. "Quantum Money from Hidden Subspaces". In: *Proceedings of the Annual ACM Symposium on Theory of Computing* (Mar. 2012). DOI: 10.1145/2213977.2213983.

[BS17] Shalev Ben-David and Or Sattath. *Quantum Tokens for Digital Signatures*. 2017. arXiv: 1609.09047 [quant-ph].

[GKW18] Rishab Goyal, Venkata Koppula, and Brent Waters. "Collusion Resistant Traitor Tracing from Learning with Errors". In: *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2018. Los Angeles, CA, USA: Association for Computing Machinery, 2018, pp. 660–670.

# References II


[KNY21] Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. *Secure Software Leasing from Standard Assumptions*. 2021. arXiv: 2010.11186 [quant-ph].

[Zha19] Mark Zhandry. "Quantum Lightning Never Strikes the Same State Twice". In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Yuval Ishai and Vincent Rijmen. Cham: Springer International Publishing, 2019, pp. 408–438. ISBN: 978-3-030-17659-4.