CS 258: Quantum Cryptography

Mark Zhandry

Previously…

Cloner: unitary U such that

$$U|\psi\rangle|0\rangle|0\rangle = |\psi\rangle|\psi\rangle|\tau_\psi\rangle \quad \text{for any} \quad |\psi\rangle$$

$|\tau_\psi\rangle$ is arbitrary state

No-cloning Thm: For dimension >1, there is no cloner

Applying no-cloning to money

Classical “money”

Physical money	Can in principle copy with enough effort Security derives from copying being presumably not cost-effective
Digital money	Trivial to “copy” 0’s and 1’s. Instead, security derives from verification against ledger of past transactions/balances

Promise of Quantum Money

Money made of quantum states that cannot be copied by the no-cloning theorem

Can be made “digital”, while also not needing any transaction ledger

For simplicity, let’s assume just a single banknote in existence. These are called mini-schemes

Def: A quantum money mini-scheme is a pair $(\mathsf{Gen}, \mathsf{Ver})$ of quantum polynomial time* procedures such that:

- $\mathsf{Gen}(1^\lambda)$ samples a classical “serial number” σ and money state $|\$\rangle$
- $\mathsf{Ver}(\sigma, |\$\rangle)$ outputs 1 (for accept) or zero (for reject)
- **Correctness:** for all λ,

$$\Pr[\mathsf{Ver}(\mathsf{Gen}(1^\lambda)) = 1] = 1$$

Defining Security

$\mathsf{Ver}^2(\sigma, |\$\$\rangle_{\mathcal{A}\mathcal{B}})$: apply $\mathsf{Ver}(\sigma, \cdot)$ separately to both $\mathcal{A}$ and $\mathcal{B}$, accept if and only if both runs accept

Def: A quantum money mini-scheme $(\mathsf{Gen}, \mathsf{Ver})$ is *secret key secure* if, for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$\Pr[\mathsf{Ver}^2(\sigma,\ \mathcal{A}(|\$\rangle)\ ) = 1 : (\sigma, |\$\rangle) \leftarrow \mathsf{Gen}(1^\lambda)] \le \epsilon(\lambda)$$

Notes:

The two money states produced by the adversary may be entangled

We allow the copied states to be potentially different from the initial state. The only important thing is that they pass verification

Wiesner's Quantum Money

$\mathsf{Gen}(1^\lambda)$:

$$\left.\begin{array}{l}\mathbf{b} = (b_1, \cdots, b_\lambda) \\ \mathbf{c} = (c_1, \cdots, c_\lambda)\end{array}\right\} \sigma$$

$$|\$\rangle = \ |\psi_{b_1,c_1}\rangle, |\psi_{b_2,c_2}\rangle, \cdots$$

where $|\psi_{b,c}\rangle = \mathbf{H}^b|c\rangle$

Some major limitations of Wiesner's money scheme:

Storing quantum states for long periods of time is hard. Quantum states like to interact with their environment, which irreversibly alters them. This is bad for a money system!

The only way to verify a money state is to talk to the mint

The limitation of secret key quantum money

Verification requires serial number

But adversary can’t know serial number

Def: A quantum money mini-scheme $(\mathsf{Gen}, \mathsf{Ver})$ is *secret key secure* if, for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$\Pr[\mathsf{Ver}^2(\sigma,\ \mathcal{A}(|\$\rangle)\ ) = 1 : (\sigma, |\$\rangle) \leftarrow \mathsf{Gen}(1^\lambda)] \leq \epsilon(\lambda)$$

This means serial number must be kept secret, meaning the general public can’t verify. The only way to verify is to send to the mint

Public key quantum money

Def: A quantum money mini-scheme $(\mathsf{Gen}, \mathsf{Ver})$ is ***public*** *key secure* if, for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$\Pr[\mathsf{Ver}^2(\sigma,\ \mathcal{A}(\sigma, |\$\rangle))\ ) = 1 : (\sigma, |\$\rangle) \leftarrow \mathsf{Gen}(1^\lambda)] \leq \epsilon(\lambda)$$

Now that the adversary can see the serial number, it can be made public, meaning anyone can verify

It turns out that public key quantum money also can resolve the issue of preserving money states. By continuously running the verifier, it is possible to “correct” any alterations that happen to the state as it interacts with the environment.

Unfortunately, Wiesner’s quantum money scheme is not public key secure

The challenge with public key quantum money

It turns out that public key quantum money can be brute forced:

Repeat the following until success:

- Run $(\sigma', |\$'\rangle) \leftarrow \mathsf{Gen}(1^\lambda)$
- If $\sigma = \sigma'$, output $|\$'\rangle$

Note: For sk quantum money, no way to tell if your serial number is same as mint’s without destroying money state

The challenge with public key quantum money

Consequence: for public key quantum money, the no-cloning theorem actually doesn’t apply – states are information-theoretically clonable

Today: Constructing Public Key Quantum Money

Public Key Quantum Money from Abelian Group Actions

Let $(\mathbb{G}, \mathcal{X}, *)$ be a group action where $\mathbb{G} = \mathbb{Z}_q$

(additive)

Everything we say today can be generalized to general abelian groups

Minting

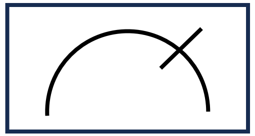
$$\begin{tikzcd}
\frac{1}{\sqrt{q}} \sum_{g \in \mathbb{G}} |g\rangle \arrow[d, "*"] \\
\frac{1}{\sqrt{q}} \sum_{g \in \mathbb{G}} |g, g * x_0\rangle
\end{tikzcd}$$

Minting

$$\begin{tikzcd}
\frac{1}{\sqrt{q}}\sum_{g\in\mathbb{G}}|g\rangle \arrow[d, "*"] \\
\frac{1}{\sqrt{q}}\sum_{g\in\mathbb{G}}|g, g*x_0\rangle \arrow[d, "\text{QFT}"] \\
\frac{1}{q}\sum_{g\in\mathbb{G}} e^{i2\pi gh/q}|h, g*x_0\rangle
\end{tikzcd}$$

Minting

$$\begin{tikzcd}
\frac{1}{\sqrt{q}}\sum_{g\in\mathbb{G}}|g\rangle \arrow[d, "*"] & \\
\frac{1}{\sqrt{q}}\sum_{g\in\mathbb{G}}|g, g*x_0\rangle \arrow[d, "\text{QFT}"] & \\
\frac{1}{q}\sum_{g\in\mathbb{G}} e^{i2\pi gh/q}|h, g*x_0\rangle \arrow[d] \arrow[dr] & \\
\sigma = h & \$ = \frac{1}{\sqrt{q}}\sum_{g\in\mathbb{G}} e^{i2\pi gh/q}|g*x_0\rangle
\end{tikzcd}$$



Verification

First check that support of $\$$ contained in $\mathcal{X}$

Verification

$$\$ = \frac{1}{\sqrt{q}} \sum_g e^{i2\pi gh/q} |g * x_0\rangle$$

$$\Big\downarrow$$

$$\frac{1}{q} \left(\sum_u |u\rangle \right) \left(\sum_g e^{i2\pi gh/q} |g * x_0\rangle \right)$$

Verification

$$\$ = \frac{1}{\sqrt{q}} \sum_{g} e^{i2\pi gh/q} |g * x_0\rangle$$

$$\Big\downarrow$$

$$\frac{1}{q} \left(\sum_{u} |u\rangle \right) \left(\sum_{g} e^{i2\pi gh/q} |g * x_0\rangle \right)$$

$$\Big\downarrow *$$

$$\frac{1}{q} \sum_{u,g} e^{i2\pi gh/q} |u\rangle |u * (g * x_0)\rangle$$

Verification

$$\frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|u*(g*x_0)\rangle$$

$$= \frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|(u+g)*x_0\rangle$$

Verification

$$\frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|u*(g*x_0)\rangle$$

$$= \frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|(u+g)*x_0\rangle$$

$$= \frac{1}{q}\sum_{u,g'} e^{i2\pi (g'-u)h/q}|u\rangle|g'*x_0\rangle$$

Verification

$$\frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|u*(g*x_0)\rangle$$

$$= \frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|(u+g)*x_0\rangle$$

$$= \frac{1}{q}\sum_{u,g'} e^{i2\pi (g'-u)h/q}|u\rangle|g'*x_0\rangle$$

$$= \left(\frac{1}{\sqrt{q}}\sum_{u} e^{-i2\pi uh/q}|u\rangle\right)\otimes \$$$

Verification

$$\frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|u*(g*x_0)\rangle$$

$$= \frac{1}{q}\sum_{u,g} e^{i2\pi gh/q}|u\rangle|(u+g)*x_0\rangle$$

$$= \frac{1}{q}\sum_{u,g'} e^{i2\pi (g'-u)h/q}|u\rangle|g'*x_0\rangle$$

$$= \left(\frac{1}{\sqrt{q}}\sum_{u} e^{-i2\pi uh/q}|u\rangle\right)\otimes \$$$

$$\Big\downarrow \text{QFT}^{-1}$$

$$|h\rangle \otimes \$$$

Verification

With some additional work, can show that the only state that passes verification is the honest banknote

Security

If Dlog is easy, protocol is broken

$$\begin{tikzcd} |h\rangle \arrow[r, "\text{QFT}"] & \frac{1}{\sqrt{q}}\sum_g e^{i2\pi gh/q}|g\rangle \arrow[r, "*"] & \frac{1}{\sqrt{q}}\sum_g e^{i2\pi gh/q}|g, g*x_0\rangle \arrow[dl, "\text{DLog}"] \\ & \frac{1}{\sqrt{q}}\sum_g e^{i2\pi gh/q}|g*x_0\rangle = \$ & \end{tikzcd}$$

If Dlog’s hard, no obvious attack

Unfortunately, no proof of security under “standard” assumptions on group actions

Public Key Quantum Money from Post-quantum insecurity

Def: A hash function H is **collapsing** if, for all QPT adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$|\Pr[W_0(\lambda)] - \Pr[W_1(\lambda)]| \leq \epsilon(\lambda)$$

where $W_b(\lambda)$ is the event that $\mathcal{A}$ outputs 1 in the following:

- $\mathcal{A}$ produces a superposition $\sum_{x,z} \alpha_{x,z} |x, z\rangle$
- If $b = 1$, measure x; if $b = 0$ measure $H(x)$
- Return state of $\mathcal{A}$, which outputs a bit b'

Because hash functions take big inputs to small outputs, measuring $H(x)$ does not fully collapse x. Nevertheless, it “looks like” it does

Theorem: Collision-resistant but not collapsing hash → Public key quantum money

Minting: take $\sum_{x,z} \alpha_{x,z} |x, z\rangle$ produced by collapsing adversary

Measure $H(x)$ → result y is serial number

Leftover state $C \sum_{\substack{x,z \\ H(x)=y}} \alpha_{x,z} |x, z\rangle$ is money state

Theorem: Collision-resistant but not collapsing hash → Public key quantum money

Verification: First check that all x in support satisfy $H(x) = y$

Then run collapsing adversary, reject if it guesses that x was measured

Theorem: Collision-resistant but not collapsing hash → Public key quantum money

Intuition for security:

If adversary can create two states that pass verification, then we know that

1. Both states supported on x such that $H(x) = y$
2. Both states "in superposition"

So measure both states to get x, x'

1. Implies $H(x) = y = H(x')$
2. Implies $x \neq x'$ with noticeable probability

➡ Collision

Constructions of non-collapsing hashes?

Achieving provably *collapsing* is non-trivial, unknown if many natural hashes are collapsing

And yet, only this year was a provably collision-resistant-but-non-collapsing hash demonstrated

A number of other approaches to building public key quantum money

Coset/subspace states

Knots

Other mathematical structures

For almost all of these, security is conjectured. It is considered a major open question to construct quantum money from “standard” cryptographic tools

Next time: More topics in quantum cryptography