Quantum Money

1 What is Quantum Money?

"Arbitrary quantum states cannot be copied" — so decrees the famous no-cloning theorem in quantum mechanics. While it comes across as an annoyance when one tries to build quantum memory, it turns out to enable a powerful cryptographic task, namely a monetary system whose security relies on the principles of quantum mechanics. Banknotes in this system will be quantum states and uncopyability of banknotes will follow from (quantitative versions of) the no-cloning theorem.

In this lecture, we will describe and analyze a private-key quantum money scheme due to Wiesner, where verification of a banknote can be done only by the bank (or its trusted delegatees).

2 The No-Cloning Theorem

The simplest version of the no-cloning theorem says that there is no unitary map that copies a single (unknown) qubit into two perfect (unentangled) copies.

Theorem 1. *There is no unitary operation that takes* $|\psi\rangle \otimes |0\rangle \in \mathbb{C}^4$ *to* $|\psi\rangle \otimes |\psi\rangle \in \mathbb{C}^4$.

Proof. Assume, for contradiction, that such a unitary operation U exists. Then,

$$U|00\rangle = |00\rangle \qquad \text{and} \qquad U|10\rangle = |11\rangle$$

Therefore, by linearity,

$$U|+\rangle|0\rangle = U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle = U\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

However, if U were to clone the state $|+\rangle$, we would expect

$$U|+\rangle|0\rangle = |+\rangle|+\rangle = \frac{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)}{2} \neq \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Note that this proof tells us not only that general quantum states cannot be cloned, but it gives a specific family of quantum states $\{|0\rangle, |1\rangle, |+\rangle\}$ such that no cloner works on all three states. □

The cloning map can of course be more general than this. It can be an arbitrary quantum channel which, by Stinespring's dilation theorem, can be simulated by a unitary map on a larger Hilbert space. The theorem below shows impossibility of perfect cloning in this more general setting.

Theorem 2. *There is no quantum channel that maps a general quantum state* $\rho \in \mathbb{C}^{d \times d}$ *to* $\rho \otimes \rho$.

Proof. Any channel that maps ρ to $\rho \otimes \rho$ for states ρ corresponds to a unitary acting on 3 registers, that for all pure states $|\psi\rangle$ satisfies

$$U(|\psi\rangle \otimes |0\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \otimes |\mathsf{aux}_\psi\rangle, \tag{1}$$

for some state $|\mathsf{aux}_\psi\rangle$ that depends on $|\psi\rangle$. We will show that no such U exists by considering its action on $|0\rangle, |1\rangle$ and $|+\rangle$. First, from the action of the channel on $|0\rangle$ and $|1\rangle$, together with linearity, we obtain

$$U|000\rangle = |00\rangle|\mathsf{aux}_0\rangle \tag{2}$$

$$U|100\rangle = |11\rangle|\mathsf{aux}_1\rangle \tag{3}$$

$$U|{+}00\rangle = U\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|00\rangle \tag{4}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle|\mathsf{aux}_0\rangle + |11\rangle|\mathsf{aux}_1\rangle). \tag{5}$$

Tracing out the second register in this state yields the mixed state

$$\rho = \frac{1}{2}(|0\rangle\langle 0| \otimes |\mathsf{aux}_0\rangle\langle\mathsf{aux}_0| + |1\rangle\langle 1| \otimes |\mathsf{aux}_1\rangle\langle\mathsf{aux}_1|).$$

However, we also know from eq. 1 that

$$U|{+}00\rangle = |+\rangle|+\rangle|\mathsf{aux}_+\rangle, \tag{6}$$

and tracing out the second register of this state yields the state

$$\rho' = |+\rangle\langle +| \otimes |\mathsf{aux}_+\rangle\langle\mathsf{aux}_+|.$$

It is apparent that $\rho \neq \rho'$; for example, ρ has eigenvalues $(\frac{1}{2}, \frac{1}{2})$, whereas ρ' is a pure state (and has eigenvalues 0 or 1). Hence no U satisfying the desired conditions exists. □

3 Wiesner's Quantum Money Scheme

To generate a banknote with serial number s, the bank picks n random pairs $(x_i, h_i) \in \{0,1\}^2$, and creates n qubits

$$|\psi_i\rangle = H^{h_i}X^{x_i}|0\rangle$$

The bank note is $\otimes_{i=1}^n |\psi_i\rangle$ and the bank stores $\left(s, (x_i, h_i)_{i\in[n]}\right)$ as the (private) verification key.

Note that each qubit is independently one of $|0\rangle, |1\rangle, |+\rangle$ or $|-\rangle$. To verify a banknote with serial number s, the bank looks up the key $\{(x_i, h_i)\}_{i\in[n]}$ corresponding to the serial number, defines a projective measurement $(\Pi, \mathbb{I}-\Pi)$ where

$$\Pi := \bigotimes_{i=1}^{n} H^{h_i}|x_i\rangle\langle x_i|H^{h_i}$$

The outcome corresponding to Π is VALID, i.e. all valid money states live in the Π subspace.

When the bank receives a n-qubit note $|\psi\rangle$, it applies the projector $(\Pi, \mathbb{I}-\Pi)$ to it and reports the outcome to the user. The question is, what to do with the money state. There are three possibilities:

Permissive Testing: The verification algorithm checks if the money state is valid, and returns the state together with the validity bit.

Strict Testing: The verification algorithm checks if the money state is valid. If yes, it returns the state, else, it destroys it.

Super-strict Testing: The verification algorithm checks if the money state is valid. If yes, it creates an entirely new money state (i.e. a new serial number and the corresponding money state), else, it destroys it. That is, in the event that the money state is valid, the bank generates a fresh key $\{(x_i', h_i')\}_{i\in[n]}$ for the same serial number s, records it, generates the corresponding money state $\otimes_{i=1}^{\lambda} |\psi_i'\rangle$ where $|\psi_i'\rangle = H^{h_i'} X^{x_i'} |0\rangle$ and sends it back to the user.

We will prove the security of Wiesner's scheme in due course, but it turns out that the exact implementation of the money verification procedure is a crucial factor that determines whether the scheme is secure or not.

4 Lutomirski's Attack on Permissive Testing

The attacker makes n queries and recovers a classical description of the money state. Once this is done, the attacker can copy the money state at will.
Let the money state be $|\psi_1\rangle \otimes ... \otimes |\psi_i\rangle \otimes ... \otimes |\psi_n\rangle$. The attack works as follows: for each $i \in [n]$, in sequence, the attacker queries the bank with the state

$$|\psi_1\rangle \otimes ... \otimes X |\psi_i\rangle \otimes ... \otimes |\psi_n\rangle$$

If $|\psi_i\rangle$ was either $|+\rangle$ or $|-\rangle$, eigenstates of X, this is exactly the money state and the verification algorithm returns VALID. If it was $|0\rangle$ or $|1\rangle$, the bank returns INVALID (with probability 1) and it also returns the state

$$|\psi_1\rangle \otimes ... \otimes |\psi_i^{\perp}\rangle \otimes ... \otimes |\psi_\lambda\rangle$$

(since this is permissive testing, after all.)

If the bank returns VALID, the attacker knows that $|\psi_i\rangle$ is an eigenstate of X, and can measure it in the X basis (Hadamard basis) to learn if it is $|+\rangle$ or $|-\rangle$. If the bank returns INVALID, the attacker can apply an X unitary to return the state to its original form, and measures it in the Z basis (standard basis) to learn if it was $|0\rangle$ or $|1\rangle$.

Perhaps strict testing might get around this attack? It certainly seems to — it seems the attacker loses the state the moment he tries to run a check on an invalid state. So, he has the option of feeding the verification oracle with a valid state, in which case he doesn't learn anything new, or he can feed the oracle with an invalid state, in which case he loses immediately. Before we see whether strict testing is safe, we take a detour to learn about a very cool quantum effect, namely the Quantum Zeno effect.

5 Detour: Quantum Zeno Effect and the Elitzur-Vaidman Bomb

Quantum Zeno Effect. Suppose you had a qubit that is in the state $|0\rangle$ initially but you wanted to put it into the state $|1\rangle$ with near-certainty. There is a catch, though: all you can do is measure the qubit (many times, perhaps) in a basis of your choice. What would you do?

It turns out, surprisingly enough, that the following strategy works: pick a small enough $\theta \approx 0$. Measure the state successively in the basis defined by $|t\theta\rangle = \cos(t\theta)|0\rangle + \sin(t\theta)|1\rangle$ at time step $t \in [\frac{\pi}{2\theta}]$.

Consider the first step. The probability that the measurement results in $|\frac{\pi}{2} + \theta\rangle$ is $\sin^2\theta \approx \theta^2$. Thus, with probability $\approx 1 - \theta^2$, the post-measurement state is $|\theta\rangle$. By the same argument, conditioned on this event happening, with probability $\approx 1 - \theta^2$, the post-measurement state after the second measurement is $|2\theta\rangle$. After $\frac{\pi}{2\theta}$ measurements, the probability that the state is at $|1\rangle$ is $1 - \frac{1}{\theta} \cdot \theta^2 = 1 - \theta$ which can be made arbitrarily close to 1.

Elitzur-Vaidman Bomb Tester. Let us consider a related problem. This time, you have a box that either contains a bomb or it doesn't. You want to figure out which is the case. There is a catch, though: if you open the box and it has a bomb, the bomb explodes and you die. How do you figure out if the box has bomb ... without dying?

We model the box by a function f_b (where $b \in \{0,1\}$ and $b = 0$ corresponds to a dud and $b = 1$ to a bomb). The input to the functions is a bit c, where $c = 1$ corresponds to opening the box and $c = 0$ corresponds to not opening it.

$$f_0(c) = 0 \quad \text{and} \quad f_1(c) = c$$

Classically, you can "query" the box or not. If you don't, you don't find out the answer. If you do, you find out the answer but also die with probability $\frac{1}{2}$.

Quantumly, you can make a "controlled query" to f_b. So, you start with $|00\rangle$ and apply a rotation map R_θ to the first qubit:

$$R_\delta := \begin{pmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{pmatrix}$$

This gives you

$$\cos\theta\,|00\rangle + \sin\theta\,|10\rangle$$

Feed it to the function which computes

$$\cos\theta\,|0, f_b(0)\rangle + \sin\theta\,|1, f_b(1)\rangle$$

Now, measure the second qubit.

- If $b = 0$ (dud), the second qubit is always zero and the first qubit survives in tact.
- If $b = 1$ (bomb), you get 1 with probability $\sin^2\theta \approx \theta^2$ and you die, or you get 0 with probability $\approx 1 - \theta^2$ and the query qubit is reset to $|0\rangle$.

Continue rotating the query qubit and running this experiment $\approx \frac{\pi}{2\theta}$ times. If $b = 0$, the query qubit rotates to $|1\rangle$. If $b = 1$, the query qubit stays at $|0\rangle$ except with probability $1 - \frac{1}{\theta} \cdot \theta^2 \approx 1 - \theta$. This is also the probability that the bomb does not explode throughout all the $O(1/\theta)$ runs. The Elitzur-Vaidman circuit is as in Figure 1.

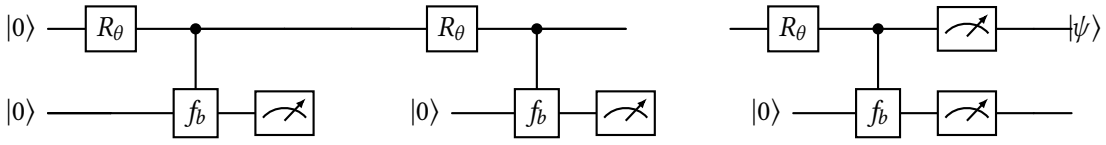

Figure 1: The Elitzur-Vaidman Bomb Tester Circuit. f_b is the box, $b = 0$ corresponding to a box with a dud and $b = 1$ to a box with a bomb. **Vinod**: Need to add a dotted line but how?

6 An Attack on Strict Testing: Lutomirski, Gently

It turns out that strict testing does not work either, as was shown by Nagaj, Sattath, Brodutch and Unruh [NSBU16]. The starting point of their (clever) attack is the observation is that Lutomirski's attack is

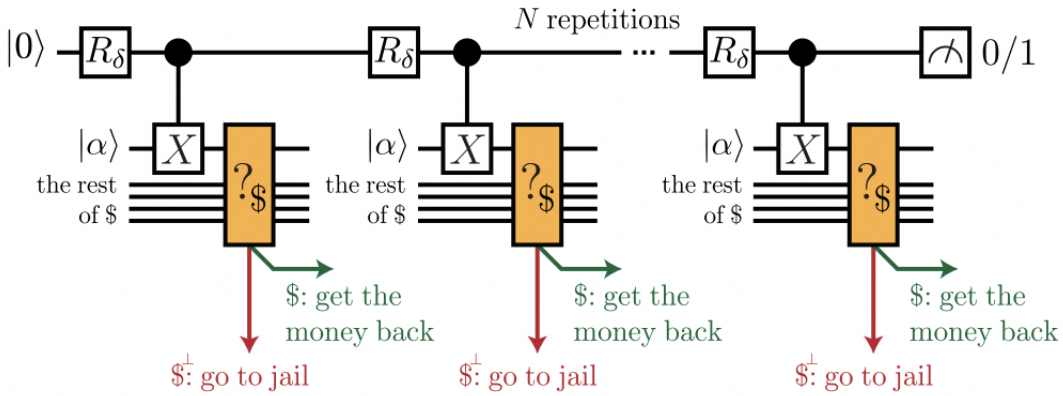

Figure 2: Figure from [NSBU16].

too "harsh". If the attacker's guess was incorrect, the money state is INVALID and the bank promptly destroys it. So, do Lutomirski's attack, just more gently. The underlying idea comes from the Elitzur-Vaidman bomb tester we saw in the last section.

The attack works qubit by qubit, so let us describe what it does on the first qubit. Pick a small number θ, define $N = \frac{\pi}{2\theta}$ and let R_θ be the unitary that rotates a state $|\psi\rangle \in \mathbb{C}^2$ counterclockwise by an angle θ.

- If $|\psi_1\rangle$ is $|+\rangle$, the state remains valid through the N iterations and the first register rotates from $|0\rangle$ to $|1\rangle$.
- If $|\psi_1\rangle$ is $|-\rangle$, still an eigenstate of X, the rotation followed by the controlled-X transforms the input state as follows:

  $$|0\rangle\otimes|-\rangle \xrightarrow{R_\delta\otimes\mathbb{I}} (\cos\delta\,|0\rangle+\sin\delta\,|1\rangle)\otimes|-\rangle \xrightarrow{\text{CNOT}} \cos\delta\,|0\rangle\otimes|-\rangle-\sin\delta\,|1\rangle\otimes|-\rangle = (\cos\delta\,|0\rangle-\sin\delta\,|1\rangle)\otimes|-\rangle$$

  That is, the second register remains a valid money state but the first register rotates by $-\delta$, landing up in the state $\cos\delta\,|0\rangle - \sin\delta\,|1\rangle$. The second iteration rotates this by δ bringing it back to $|0\rangle$, so this iteration does nothing to the money state. The third iteration acts like the first, the fourth like the second, and so on. After an even number of iterations, the first register is in state $|0\rangle$.
- If $|\psi_1\rangle$ is $|0\rangle$ (resp. $|1\rangle$), the tester returns INVALID with probability $\sin^2\delta \approx \delta^2$. In the event that the tester returns VALID, the state is restored to $|0\rangle$ (resp. $|1\rangle$) *and* crucially, the first qubit is also restored to $|0\rangle$ (resp. $|1\rangle$).

  $$|0\rangle\otimes|b\rangle \xrightarrow{R_\delta\otimes\mathbb{I}} (\cos\delta\,|0\rangle+\sin\delta\,|1\rangle)\otimes|b\rangle \xrightarrow{\text{CNOT}} \cos\delta\,|0\rangle\otimes|b\rangle+\sin\delta\,|1\rangle\otimes|1-b\rangle \overset{\text{w.p. }\cos^2\theta}{\rightsquigarrow} |0\rangle\otimes|b\rangle$$

  The probability that all N iterations result in VALID is at least

  $$1 - N\delta^2 = 1 - \frac{\pi^2}{4N}$$

  which can be made arbitrarily small by picking N to be large enough. In this event, the state of the first qubit remains at $|0\rangle$ where it started.

Thus, after N iterations, the state of the first register is $|0\rangle$ if $|\psi_1\rangle = |+\rangle$ and $|1\rangle$ otherwise. We can check if $|\psi_1\rangle = |-\rangle$ by doing the exact same procedure as above except with the controlled-$(-X)$ operation replacing the controlled-X (i.e. CNOT). Once this is done and the state is determined to be either $|0\rangle$ or $|1\rangle$, a Z basis measurement will finish up the job.

The failure probability in the entire experiment is at most

$$\frac{\pi^2}{4N} \cdot 2\lambda = \frac{\pi^2 \lambda}{2N} \leq \varepsilon$$

as long as $N \geq \frac{\pi^2 \lambda}{2\varepsilon}$ is large enough.

7 Security of Wiesner's Scheme

The Trivial Cloner. A trivial cloner for Wiesner's scheme, trying to construct two money states from one, guesses $\widetilde{h}_i \in \{0,1\}^\lambda$. If $\widetilde{h}_i = 0$, measure $|\psi_i\rangle$ in the Z basis (i.e. the standard basis), else measure it in the X basis (i.e. the Hadamard basis). If all guesses are correct, i.e. for all i, $\widetilde{h}_i = h_i$, which happens with probability $\left(\frac{1}{2}\right)^n$, this strategy perfectly recovers the money state. Once this is done, copying is easy. Indeed, this strategy can create as many money states as the cloner wishes, succeeding with the same probability of $(1/2)^n$.

The Projective Single-Qubit Cloner. However, one does not have to recover a classical description of the state in order to clone. Projecting each state onto the $\{|0\rangle, |1\rangle\}$ basis results in a success probability of

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \left(\frac{1}{2}\right)^2 = \frac{5}{8}.$$

Curiously, the strategy of projecting on to any other basis, e.g. $\{|\pi/8\rangle, |5\pi/8\rangle\}$, achieves the same success probability which leads one to wonder if it is indeed optimal.

It turns out the answer is no: one can clone better and achieve a success probability of $\frac{3}{4}$, which is also optimal. What's more, one can show that the optimal cloning probability for an n-qubit money state is $(\frac{3}{4})^n$. To show both statements, one needs to formulate the problem of optimal cloning as that of finding the optimal solution to a semi-definite program.

7.1 The Semidefinite Programming Formulation of Optimal Cloning Attacks.

Let the money state be defined by the ensemble of quantum states $\{(p_k, |\psi_k\rangle)\}_{i=1}^k$ for some $k \in \mathbb{N}$. Consider a cloning channel Φ that maps $\rho \in \mathcal{S}(\mathcal{X})$ to $\Phi(\rho) \in \mathcal{S}(\mathcal{Y} \otimes \mathcal{Z})$, where $\mathcal{Y}$ and $\mathcal{Z}$ are isomorphic to $\mathcal{X}$. In particular, all of them are defined over the same state space Σ.

In order to be physically realizable, the map Φ has to be completely positive and trace-preserving.

Lemma 3. *The success probability of the cloning channel is*

$$\sum_{i=1}^{k} p_k \langle \psi_k \otimes \psi_k | \Phi(|\psi_k\rangle \langle \psi_k|) | \psi_k \otimes \psi_k \rangle \tag{7}$$

Proof. To see this for a fixed k, setting $\rho = \Phi(|\psi_k\rangle\langle\psi_k|)$, observe that the probability of success of the channel Φ is measured by the overlap of $\Phi(\rho)$ with the state $|\psi_k \otimes \psi_k\rangle$. This is a projective measurement with the projector $|\psi_k \otimes \psi_k\rangle\langle\psi_k \otimes \psi_k|$. So, the probability of success can be written as

$$\mathsf{Tr}(|\psi_k \otimes \psi_k\rangle\langle\psi_k \otimes \psi_k| \rho) = \mathsf{Tr}(\langle\psi_k \otimes \psi_k| \rho |\psi_k \otimes \psi_k\rangle) = \langle\psi_k \otimes \psi_k| \rho |\psi_k \otimes \psi_k\rangle$$

where the first equation is by the cyclic property of the trace function and the second since the argument of the trace function is a scalar. □

To reason about the channel Φ, it turns out to be helpful to consider the Choi representation of Φ. Recall from Section **??** the following properties of the Choi representation $J(\Phi) \in \mathcal{L}(\mathcal{Y} \otimes \mathcal{Z} \otimes \mathcal{X})$:

$$J(\Phi) = \sum_{a,b \in \Sigma} \Phi(E_{a,b}) \otimes E_{a,b} \tag{8}$$

- The map that takes Φ to $J(\Phi)$ (given by equation 8) is linear and bijective.
- Φ is completely positive and trace-preserving if and only if $J(\Phi) \in \mathcal{P}(\mathcal{Y} \otimes \mathcal{Z} \otimes \mathcal{X})$ is positive and $\mathsf{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}(J(\Phi)) = \mathsf{Id}_{\mathcal{X}}$.
- The success probability from equation 7 is equal to

$$\sum_{i=1}^{k} p_k \langle\psi_k \otimes \psi_k \otimes \overline{\psi_k}| J(\Phi) |\psi_k \otimes \psi_k \otimes \overline{\psi_k}\rangle = \mathsf{Tr}_{\mathcal{Y}\otimes\mathcal{Z}\otimes\mathcal{X}}\big(J(\Phi)\, Q\big)$$

  where

$$Q = \sum_{i=1}^{k} p_k |\psi_k \otimes \psi_k \otimes \overline{\psi_k}\rangle\langle\psi_k \otimes \psi_k \otimes \overline{\psi_k}|$$

  A proof of this can be derived from Lemma **??**.

The problem of maximizing the success probability of a cloner can be written as the following semi-definite program. The goal is to find a positive matrix X (which is supposedly $J(\Phi)$ for some quantum channel Φ) such that:

$$\begin{array}{ll} \max & \mathsf{Tr}_{\mathcal{Y}\otimes\mathcal{Z}\otimes\mathcal{X}}(QX) \\ \text{s.t.} & \mathsf{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}(X) = \mathsf{Id}_{\mathcal{X}} \\ & X \in \mathcal{P}(\mathcal{Y} \otimes \mathcal{Z} \otimes \mathcal{X}) \end{array}$$

The following two lemmas bound the optimum of this SDP for the Wiesner ensemble.

Lemma 4. *Let*

$$Q = \frac{1}{4}\Big(|000\rangle\langle 000| + |111\rangle\langle 111| + |+++\rangle\langle +++| + |---\rangle\langle ---| \Big)$$

correspond to the Wiesner ensemble

$$\left\{ \left(\frac{1}{4}, |0\rangle\right), \left(\frac{1}{4}, |1\rangle\right), \left(\frac{1}{4}, |+\rangle\right), \left(\frac{1}{4}, |-\rangle\right) \right\}$$

Then, $Q \preceq c \cdot \mathsf{Id}$ for some constant $c < 1/2$.

Proof. It suffices to show that the largest eigenvalue of Q is at most a constant $c < 1/2$. Writing Q in the basis

$$|000\rangle, |111\rangle, |\alpha\rangle := \frac{|011\rangle + |101\rangle + |110\rangle}{\sqrt{3}}, |\beta\rangle := \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}},$$

we write Q as

$$Q = \frac{1}{4} \cdot \begin{pmatrix} \frac{3}{2} & 0 & \frac{1}{2\sqrt{3}} & 0 \\ 0 & \frac{1}{6} & 0 & \frac{1}{2\sqrt{3}} \\ \frac{1}{2\sqrt{3}} & 0 & \frac{1}{6} & 0 \\ 0 & \frac{1}{2\sqrt{3}} & 0 & \frac{3}{2} \end{pmatrix}$$

Using the fact that the largest eigenvalue of Q is bounded by the largest row sum, we get

$$\max_i \lambda_i(Q) \leq \frac{1}{4} \cdot \left(\frac{3}{2} + \frac{1}{2\sqrt{3}} \right) = \frac{3}{8} + \frac{1}{8\sqrt{3}} < \frac{1}{2}$$

□

Lemma 5. *For any X satisfying the conditions of the SDP above,*

$$\mathsf{Tr}(QX) \leq 2c < 1$$

where c is the constant from Lemma 4 For the n-qubit SDP where Q is replaced by $Q^{\otimes n}$, we have

$$\mathsf{Tr}(Q^{\otimes n} X) \leq (2c)^n$$

which decreases exponentially with n.

Proof. Using the fact that X is positive and the fact that $\mathsf{Tr}(X) = 2$, we have

$$\mathsf{Tr}(QX) \leq c \cdot \mathsf{Tr}(X) = 2c$$

The exact same calculations lead to the bound for the n-qubit system. □

Useful Fact: If Q, X are positive semi-definite, $\mathsf{Tr}(QX) \geq 0$.

The Optimal Single-Qubit Cloner. The optimal cloner was discovered by Molina, Vidick and Watrous [MVW12]. is given by the Kraus operators

$$\rho \mapsto A_0 \rho A_0^T + A_1 \rho A_1^T$$

where

$$A_0 = \frac{1}{\sqrt{12}} \begin{pmatrix} 3 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad A_1 = \frac{1}{\sqrt{12}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 3 \end{pmatrix}$$

The Plot Thickens: A Better Quantum Money Scheme. It turns out that the optimal counterfeiting probability for any single-qubit money state is $2/3$, and is given by the ensemble

$$\left\{ \left(\frac{1}{6}, |0\rangle\right), \left(\frac{1}{6}, |1\rangle\right), \left(\frac{1}{6}, |+\rangle\right), \left(\frac{1}{6}, |-\rangle\right), \left(\frac{1}{6}, \frac{|0\rangle + i|1\rangle}{\sqrt{2}}\right), \left(\frac{1}{6}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right) \right\}$$

8 Public-key Quantum Money

The naïve idea of publishing a verification oracle for Wiesner's quantum money scheme, in order to enable public verification, is dangerous as illustrated by Lutomirski's attack. So, we need a better construction, in particular a family of states that remains unclonable even in the presence of a verification oracle. An example is Aaronson and Christiano's subspace state scheme [AC13]. To describe the scheme, we need some setup first.

For a subspace $S \subseteq \mathbb{F}^n$, we will let the subspace state, denoted $|S\rangle$, be defined as

$$|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{s \in S} |s\rangle$$

Analogously, given S and vectors $x, z \in \mathbb{F}^n$, we will let the coset state be

$$|S_{x,z}\rangle := X^x Z^z |S\rangle := \frac{1}{\sqrt{|S|}} \sum_{s \in S} (-1)^{\langle s,z \rangle} |s + x\rangle$$

We will often let the field be $\mathbb{F}_2$.

Lemma 6. *Let $S \subseteq \mathbb{F}_2^n$ be a subspace and let $S^\perp$ be its dual. Then,*

$$H^{\otimes n} |S\rangle = |S^\perp\rangle \ .$$

Analogously, if $S_{x,z}$ is a coset state,

$$H^{\otimes n} |S_{x,z}\rangle = |S^\perp_{z,x}\rangle$$

Proof.

$$H^{\otimes n} |S\rangle = \frac{1}{\sqrt{|S|}} \sum_{s \in S} H^{\otimes n} |s\rangle = \frac{1}{\sqrt{2^n \cdot |S|}} \sum_{s \in S} \sum_{y \in \mathbb{F}_2^n} (-1)^{\langle y,s \rangle} |y\rangle = \frac{1}{\sqrt{2^n \cdot |S|}} \sum_{y \in \mathbb{F}_2^n} \left(\sum_{s \in S} (-1)^{\langle y,s \rangle} \right) |y\rangle$$

For every $y \in S^\perp$, the inner sum is $|S|$, and for every $y \notin S^\perp$, it is 0. Thus,

$$H^{\otimes n} |S\rangle = \sqrt{\frac{|S|}{2^n}} \sum_{y \in S^\perp} |y\rangle = \frac{1}{\sqrt{|S^\perp|}} \sum_{y \in S^\perp} |y\rangle = |S^\perp\rangle$$

Also,

$$H^{\otimes n} |S_{x,z}\rangle = H^{\otimes n} X^x Z^z |S\rangle = Z^x X^z H^{\otimes n} |S\rangle = Z^x X^z |S^\perp\rangle = |S^\perp_{z,x}\rangle$$

□

The money state is a superposition over all vectors in a subspace $S \subseteq \mathbb{F}_2^n$ of rank $n/2$. That is, define

$$|S\rangle := \frac{1}{2^{n/4}} \sum_{s \in S} |s\rangle$$

Note that applying a Hadamard transform $H^{\otimes n}$ results in $|S^\perp\rangle$ as in Lemma 6.

Define the subspace-checker program Π_S to output 1 on input $s \in S$, and 0 otherwise (and similarly $\Pi_{S^\perp}$). Verifying the money state $|\psi\rangle$ works as follows:

1. Run Π_S in superposition over $|\psi\rangle$, and measure the result; and
2. Run $\Pi_{S^\perp} \circ H^{\otimes n}$ on $|\psi\rangle$, and measure the result.
3. Run $H^{\otimes n}$ again to restore the money state.

If both measurements result in a 1, accept; otherwise, reject. If $|\psi\rangle = |S\rangle$, the verification procedure accepts with probability 1.

Aaronson and Christiano showed that given $|S\rangle$, no adversary with a bounded number of queries to the verification oracles Π_S and $\Pi_{S^\perp}$ can produce two copies $|\psi\rangle \otimes |\psi'\rangle$ that both pass the verification test. Zhandry [Zha19] showed how to implement the verification oracle using indistinguishability obfuscation and retain the unclonability guarantee.

There are several other candidate constructions [FGH+12, Kan18, Zha24] of public-key quantum money; however, constructing a public-key quantum money scheme from well-studied cryptographic assumptions is still very much an open problem.

Chapter Notes

The adaptive attack on Wiesner's scheme is due to Nagaj, Sattath, Brodutch and Unruh [NSBU16]. Aaronson [Aar09] came up with a construction of a quantum money scheme in the presence of a quantum oracle. The construction in Section 8 is due to Aaronson and Christiano [AC13], who used a classical oracle and subspace states to construct a public-key quantum money scheme. Zhandry [Zha19] showed how to implement the classical oracle with an (quantum-secure) indistinguishability obfuscation scheme, giving us a construction without oracles.

Exercise

1. Show that the success probability of any projective qubit-by-qubit cloner for the Wiesner scheme has success probability $5/8$.
   The success probability of the projective cloner with basis θ on the state $|0\rangle$ (resp. $|1\rangle$) is given by

$$\begin{aligned}\cos^2\theta \cdot (\cos^2\theta)^2 + \sin\theta \cdot (\sin^2\theta)^2 &= \cos^6\theta + \sin^6\theta \\ &= (\cos^2\theta + \sin^2\theta)^2 - 3\cos^2\theta\sin^2\theta(\cos^2\theta + \sin^2\theta) \\ &= 1 - 3\cos^2\theta\sin^2\theta \\ &= 1 - \frac{3}{4}(2\cos\theta\sin\theta)^2 \\ &= 1 - \frac{3}{4}\sin^2 2\theta\end{aligned}$$

   The success probability of the projective cloner with basis θ on the state $|+\rangle$ (resp. $|-\rangle$) is given by

$$\begin{aligned}\cos^2(\pi/4-\theta) \cdot (\cos^2(\pi/4-\theta))^2 + \sin(\pi/4-\theta) \cdot (\sin^2(\pi/4-\theta))^2 &= 1 - \frac{3}{4}\sin^2 2(\pi/4-\theta) \\ &= 1 - \frac{3}{4}\cos^2 2\theta\end{aligned}$$

The overall success probability is the average, i.e.

$$1 - \frac{3}{8}(\cos^2 2\theta + \sin^2 2\theta) = \frac{5}{8}$$

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 229–242. IEEE Computer Society, 2009.

[AC13] Scott Aaronson and Paul F. Christiano. Quantum money from hidden subspaces. *Theory Comput.*, 9:349–401, 2013.

[FGH+12] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter W. Shor. Quantum money from knots. In Shafi Goldwasser, editor, *Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012*, pages 276–289. ACM, 2012.

[Kan18] Daniel M. Kane. Quantum money from modular forms. *CoRR*, abs/1809.05925, 2018.

[MVW12] Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for wiesner's quantum money. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography, 7th Conference, TQC 2012, Tokyo, Japan, May 17-19, 2012, Revised Selected Papers*, volume 7582 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2012.

[NSBU16] Daniel Nagaj, Or Sattath, Aharon Brodutch, and Dominique Unruh. An adaptive attack on wiesner's quantum money. *Quantum Inf. Comput.*, 16(11&12):1048–1070, 2016.

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 408–438. Springer, 2019.

[Zha24] Mark Zhandry. Quantum money from abelian group actions. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, January 30 to February 2, 2024, Berkeley, CA, USA*, volume 287 of *LIPIcs*, pages 101:1–101:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.