COL7160 : Quantum Computing

Lecture 24: Quantum Money

Instructor: Rajendra Kumar

Scribe: Karthik Nambiar

1 Overview

In this lecture, we explore Wiesner's quantum money scheme, from its minting process to its verification during transactions. While the scheme has several limitations and is not fully practical, the underlying idea is both elegant and foundational to quantum cryptography. We examine a particular verification approach that closely resembles the well-known BB84 quantum key distribution protocol, highlighting the role of basis mismatch and measurement disturbance. Finally, we discuss possible attacks on the scheme and its key drawbacks.

2 Wiesner's Quantum Money

Wiesner proposed one of the earliest quantum cryptographic primitives: *quantum money*. The idea is to create coins that cannot be counterfeited due to the no-cloning theorem.

2.1 Construction

Let $n \in \mathbb{N}$. The bank chooses a serial number $s \in \{0,1\}^n$ and a secret string $q \in \{0,1,+,-\}^n$ uniformly at random. Each symbol of q determines a quantum state according to the encoding

$$0 \mapsto |0\rangle\,, \quad 1 \mapsto |1\rangle\,, \quad + \mapsto |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad - \mapsto |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Definition 1. A *quantum coin* is a pair $(s, |\psi\rangle)$ where

$$|\psi\rangle = \bigotimes_{i=1}^{n} |q_i\rangle\,.$$

The bank stores the corresponding classical information (s, q) in its database.

2.2 Verification

Given a coin $(s, |\psi\rangle)$, the bank retrieves the corresponding secret string q from its database.

$$\text{For each } i \in \{1,\dots,n\}: \quad \begin{cases} \text{measure in computational basis}, & q_i \in \{0,1\}, \\ \text{measure in Hadamard basis}, & q_i \in \{+,-\}. \end{cases}$$

That is, the i-th qubit of $|\psi\rangle$ is measured in the basis specified by q_i, ensuring consistency with the original encoding. In other words, the coin is accepted if and only if every measurement outcome agrees with the corresponding entry of the secret string q.

2.3 A Simple Forgery Argument

Consider an adversary who measures each qubit of the coin $|\psi\rangle$ in the computational basis.

$$|\psi\rangle = \bigotimes_{i=1}^{n} |q_i\rangle \quad \longrightarrow \quad x \in \{0,1\}^n$$

The coin with the adversary post computational basis measurement collapses to the Quantum state whose corresponding classical string is x. We can then forge another Quantum coin using x. Thus we get 2 new identical states which are being sent for verification.

$$P(\text{success for one qubit}) = \begin{cases} 1, & q_i \in \{0,1\}, \\ \frac{1}{2}, & q_i \in \{+,-\}. \end{cases}$$

If the measurement is performed in the correct basis, the adversary reproduces the state perfectly. If it is performed in the wrong basis, the outcome is random and matches the correct state with probability $1/2$.

$$P(\text{both coins pass for one qubit}) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \left(\frac{1}{2} \cdot \frac{1}{2}\right) = \frac{5}{8}.$$

$$P(\text{both coins pass}) = \left(\frac{5}{8}\right)^n.$$

3 Limitations of Wiesner's Scheme

1. It is hard for banks to store and for us to carry such quantum states.
2. Verification requires interaction with the bank.
3. Measurement destroys the quantum state, so the coin cannot be reused.

4 Interactive Verification Protocol

To avoid sending the quantum state directly, an interactive protocol can be used.

Algorithm 1 Interactive Verification

```
User sends serial number s to the bank
Bank sends random challenge c ∈ {0,1}^n
for i = 1 to n do
    if c_i = 0 then
        Measure i-th qubit in computational basis
        q'_i = classical string corresponding to the measurement outcome
    else
        Measure i-th qubit in Hadamard basis
        q'_i = classical string corresponding to the measurement outcome
    end if
end for
Send q' to the bank
Bank checks consistency with q
```

For the case where ($c_i = 0$ and $q_i = 0$ or 1) or ($c_i = 1$ and $q_i = 0$ or 1) check if the corresponding $q'_i = q_i$. If true for all such cases, the coin is accepted.
This protocol still destroys the quantum state after verification.

5 BB84 Protocol

Preparation (Alice).

$$\theta = (\theta_1, \theta_2, \ldots, \theta_n), \quad x = (x_1, x_2, \ldots, x_n), \quad \theta_i \in \{0,1\},\ x_i \in \{0,1\}$$

Here $\theta_i = 0$ implies the standard basis and 1 implies the hadamard basis. $x_i = 0$ implies the state being in 0 or + depending on their basis and $x_i = 1$ implies the state being in 1 or -again depending on their basis.
Alice prepares the quantum state

$$|\psi\rangle = |x_1\rangle_{\theta_1} \otimes |x_2\rangle_{\theta_2} \otimes \cdots \otimes |x_n\rangle_{\theta_n},$$

where each x_i is encoded in the basis θ_i, and sends $|\psi\rangle$ to Bob.

Measurement (Bob).

$$\theta' = (\theta'_1, \theta'_2, \ldots, \theta'_n), \quad \theta'_i \in \{0, 1\}$$

Bob independently chooses a random basis θ'_i for each qubit and measures the received state to obtain

$$x' = (x'_1, x'_2, \ldots, x'_n).$$

Basis Comparison.

$$\text{Keep } i \iff \theta_i = \theta'_i$$

Alice and Bob publicly compare their choice of bases and retain only those indices where the bases match.

Key Generation.

$$k = \{\, x_i \mid \theta_i = \theta'_i \,\}$$

The retained bits form the shared secret key, assuming no adversary is present. As you can see the

Error Checking.

$$\text{sample } S \subseteq \{i : \theta_i = \theta'_i\}$$

Alice and Bob reveal a subset of the retained bits and compare them.

$$\text{Abort if error rate} > \varepsilon$$

If the mismatch exceeds a certain threshold, they conclude that an adversary is present; otherwise, the remaining bits constitute the final secret key. As you can see, we have used an idea similar to the interactive verification protocol where we only verified or considered the bits whose basis matched with the basis corresponding to the element of the challenged bit string.

6 A Basis-Testing Attack on Weisner's Money via Repeated Interaction

We describe a procedure to distinguish whether a given qubit is in the Hadamard basis $\{|+\rangle, |-\rangle\}$ or the computational basis $\{|0\rangle, |1\rangle\}$ using an auxiliary control qubit. If this can be done for single qubit coin then it can be easily extend to multiple qubit coin.

Procedure.

$$|0\rangle_c \otimes |\psi\rangle$$

Initialize a control qubit in state $|0\rangle$ and let $|\psi\rangle$ denote the coin qubit. In each round, apply

$$R_\theta \otimes I \quad \longrightarrow \quad \text{CNOT} \quad \longrightarrow \quad \text{verification.}$$

Here R_θ is a small rotation on the control qubit, and CNOT uses the control as control and the coin as target.

Case 1: $|\psi\rangle = |+\rangle$**.**

$$X|+\rangle = |+\rangle$$

After one round, the joint state becomes

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

No entanglement is created, and the state remains unchanged under verification. After N rounds,

$$|c\rangle = \cos(N\theta)\,|0\rangle + \sin(N\theta)\,|1\rangle\,.$$

Thus, choosing $N\theta \approx \frac{\pi}{2}$ yields

$$P(\text{measure } 1) \approx 1.$$

Case 2: $|\psi\rangle = |-\rangle$**.**

$$X\,|-\rangle = -\,|-\rangle$$

Starting with

$$|0\rangle_c \otimes |-\rangle\,,$$

apply the rotation and CNOT:

$$(R_\theta \otimes I)\,|0\rangle\,|-\rangle = (\cos\theta\,|0\rangle + \sin\theta\,|1\rangle) \otimes |-\rangle\,.$$

After applying CNOT:

$$\cos\theta\,|0\rangle\,|-\rangle + \sin\theta\,|1\rangle\,X\,|-\rangle = \cos\theta\,|0\rangle\,|-\rangle - \sin\theta\,|1\rangle\,|-\rangle\,.$$

$$= (\cos\theta\,|0\rangle - \sin\theta\,|1\rangle) \otimes |-\rangle\,.$$

This can be written as

$$(R_{-\theta} \otimes I)\,|0\rangle\,|-\rangle\,.$$

Thus, the effect of the CNOT is to induce a *phase kickback*, changing θ to $-\theta$ on the control qubit.

Since the state remains unentangled, the verification procedure does not disturb either the coin qubit or the control qubit.

Repeating the procedure, we obtain

$$\text{CNOT}\,(R_\theta \otimes I)\,(R_{-\theta} \otimes I)\,|0\rangle\,|-\rangle = \text{CNOT}\,|0\rangle\,|-\rangle = |0\rangle\,|-\rangle\,.$$

Thus, after two iterations, the control qubit returns to $|0\rangle$.

More generally, the control qubit does not accumulate rotation across iterations. At any stage, it is either in the state

$$|0\rangle \quad \text{or} \quad \cos\theta\,|0\rangle - \sin\theta\,|1\rangle\,.$$

Hence,

$$P(\text{measure } 0) = \cos^2\theta \approx 1 \quad \text{for small } \theta.$$

Case 3: $|\psi\rangle \in \{|0\rangle\,, |1\rangle\}$**.**

$$X\,|0\rangle = |1\rangle\,, \qquad X\,|1\rangle = |0\rangle$$

After applying the rotation and CNOT, the joint state becomes

$$\cos\theta\,|0\rangle\,|\psi\rangle + \sin\theta\,|1\rangle\,X\,|\psi\rangle\,.$$

During verification, the bank measures the coin qubit in the computational basis. Since θ is small, the state collapses to the original basis state $|\psi\rangle$ with probability

$$\cos^2\theta \approx 1.$$

Thus, with high probability, the control qubit is reset to $|0\rangle$ after each iteration.

Repeating this process over multiple iterations, the control qubit continues to return to $|0\rangle$ with high probability, and the probability of observing $|1\rangle$ remains very small.

$$P(\text{measure } 1) \ll 1 \quad \text{over } \frac{\pi}{2\theta} \text{ iterations.}$$

Decision Rule.

$$\text{Output} \begin{cases} \{|+\rangle\}, & \text{if control qubit measures } 1, \\ \{|0\rangle, |1\rangle, |-\rangle\}, & \text{if control qubit measures } 0. \end{cases}$$

The same procedure is applied in all cases without adaptation. The distinction arises entirely from how the verification measurement affects the system.

Exercise

$$\{|0\rangle, |1\rangle, |-\rangle\}$$

Figure out how to distinguish amongst these three states for a single qubit coin?