COL7160 : Quantum Computing

Lecture 24: Quantum Money

Instructor: Rajendra Kumar

Scribe: Zainab Aziz

1 Introduction

Classical information can be copied without restriction. While this property enables the modern digital economy, it also makes purely digital money inherently insecure: any classical encoding of value can be duplicated perfectly. Consequently, all electronic payment systems today depend on trusted intermediaries (such as banks or credit card companies) to prevent double-spending.

Quantum information, however, behaves fundamentally differently. Quantum states cannot be copied arbitrarily. In particular, the *no-cloning theorem* asserts that an unknown quantum state cannot be perfectly replicated. Any attempt to duplicate such a state inevitably disturbs it, allowing forgery attempts to be detected.

This naturally leads to the question: can these physical limitations be harnessed to construct forms of money that are impossible to counterfeit?

The concept was first introduced by Stephen Wiesner in the late 1960s. In his proposal, each banknote contains qubits prepared in secret bases known only to the issuing authority. More broadly, quantum money refers to a cryptographic paradigm that uses the laws of quantum mechanics to achieve security guarantees unattainable in classical systems.

Key motivations:

- Classical cryptographic security relies on computational assumptions and is not provably absolute.
- Physical currency can be forged given sufficient resources and sophistication.
- The objective is to design currency whose security is enforced by fundamental physical principles, such as the no-cloning theorem, rather than computational hardness.

2 Wiesner's Scheme

2.1 Setup

Definition 1 (Quantum Coin)**.** A *quantum coin* is a pair $(s, |\Psi\rangle)$ where:

- $s \in \{0,1\}^n$ is a classical *serial number*, chosen uniformly at random.
- $|\Psi\rangle$ is an n-qubit quantum state encoding a randomly chosen basis string.

2.2 Coin Creation

To create a quantum coin, the bank proceeds as follows:

Algorithm 1 Wiesner Coin Creation

Input: Security parameter n.
Output: A coin $(s, |\Psi\rangle)$ and a database entry (s, q).
Pick $s \in \{0,1\}^n$ uniformly at random. ▷ serial number
Pick $q \in \{0, 1, +, -\}^n$ uniformly at random. ▷ $2n$ random bits
Prepare the n-qubit state

$$|\Psi\rangle \;=\; \bigotimes_{i=1}^{n} |q_i\rangle\,,$$

where $|0\rangle, |1\rangle$ are the standard basis states and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are the Hadamard basis states.
Output the coin $(s, |\Psi\rangle)$ and store (s, q) in the bank's database.

Example 1. For $n = 11$, a sample basis string might be $q = (0, 1, +, +, 1, -, +, 0, 1, 0, 0)$, giving

$$|\Psi\rangle = |0\rangle \otimes |1\rangle \otimes |+\rangle \otimes |+\rangle \otimes |1\rangle \otimes |-\rangle \otimes |+\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle\,.$$

2.3 Verification

Algorithm 2 Wiesner Coin Verification

Input: Coin $(s, |\Psi\rangle)$.
Output: ACCEPT or REJECT.
Look up (s, q) in the bank's database.
for $i = 1$ to n **do**
    if $q_i \in \{0, 1\}$ **then**
        Measure the i-th qubit in the standard basis $\{|0\rangle, |1\rangle\}$.
    else $(q_i \in \{+, -\})$
        Measure the i-th qubit in the Hadamard basis $\{|+\rangle, |-\rangle\}$.
    end if
    if outcome $\neq q_i$ **then return** REJECT.
    end if
end for
return ACCEPT and give back the post-measurement state.

2.4 Storing the Coin: Private-Key Scheme

A major limitation of Wiesner's original scheme is that the bank must store all (s, q) pairs, resulting in an exponentially large database. To address this, a later proposal by Bennett, Brassard, Breidbart, and Wiesner replaces the database with a pseudorandom function.
Specifically, the bank selects a secret key $k \in \{0,1\}^n$ and defines

$$q := f_k(s),$$

where f_k is a pseudorandom function. The quantum state is then prepared according to q, just as in Wiesner's original scheme. During verification, the bank recomputes q from s using the secret key k, eliminating the need to store all (s, q) pairs.

3 Security Against Attacks

3.1 The Attack Problem

The goal of the adversary is to produce two valid coins from one:

$$(s, |\Psi\rangle) \;\to (s, |\Psi\rangle),\ (s, |\Psi\rangle).$$

By the *no-cloning theorem*, perfectly cloning an unknown quantum state is impossible. However, this does not immediately rule out approximate or probabilistic attacks that succeed with high probability. Therefore, the central question is to bound the success probability of any such attack strategy that attempts to produce multiple valid copies of a given quantum coin.

3.2 A Simple Attack

The most straightforward attack proceeds as follows:

1. Measure each qubit of $|\Psi\rangle$ in the standard basis, obtaining outcomes $r = r_1 r_2 \cdots r_n \in \{0,1\}^n$.
2. Prepare two (or more) copies of $(s, |r_1 r_2 \cdots r_n\rangle)$.

Proposition 1. *The simple attack succeeds (both copies pass verification) with probability*

$$\Pr[\textit{success}] = \left(\frac{5}{8}\right)^n.$$

Proof. For each qubit i, there is a $\frac{1}{2}$ chance that $q_i \in \{0,1\}$ (standard basis) and a $\frac{1}{2}$ chance that $q_i \in \{+,-\}$ (Hadamard basis).

- If $q_i \in \{0,1\}$: the measurement outcome $r_i = q_i$ exactly, so $\Pr[\text{Verified}] = 1$.
- If $q_i \in \{+,-\}$: the outcome r_i is equally likely 0 or 1, so $\Pr[\text{Verifier accepts } |r_i\rangle \text{ as } |q_i\rangle] = \frac{1}{2}$. Thus $\Pr[\text{both copies pass on qubit } i] = \frac{1}{4}$.

Combining:

$$\Pr[\text{success per qubit}] = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{4} = \frac{5}{8}.$$

Since qubits are independent, $\Pr[\text{both copies pass}] = (5/8)^n$.

□

3.3 Optimal Attack

The optimal attack i.e., the strategy that maximises the probability of producing two valid coins from a single input, succeeds with probability at most

$$\left(\frac{3}{4}\right)^n.$$

Remark 1. This bound was originally claimed by Wiesner, but with entirely flawed reasoning that went unquestioned for many years. A rigorous proof was established later, confirming that no attack can achieve a higher success probability.

4 Defects and Extensions

4.1 Defect 1: Quantum Storage Required

The primary practical limitation of Wiesner's scheme is the requirement of reliable quantum memory. A quantum state cannot be stored and carried around like classical information, and maintaining coherence over extended periods remains experimentally challenging, even in advanced laboratories. This makes the scheme difficult to implement with current technology. For the purposes of analysis, we assume that future technological advances will enable the construction of robust quantum storage devices.

4.2 Defect 2: Verification Requires Sending the State to the Bank

The second major defect: to verify a coin, you must send the quantum state to the bank over a quantum channel, or physically walk it to the bank. This is very inconvenient.

We describe a simple protocol, discovered around 15 years ago, that allows verification using only classical communication with the bank. This protocol is directly related to BB84 Quantum Key Distribution.

Fix: A way to verify using only classical communication with the bank (which is eavesdroppable):

Algorithm 3 Classical-Communication Verification

1: User sends serial number s to bank (classically, over an authenticated channel).
2: Bank sends back a uniformly random *challenge string* $c \in \{0,1\}^n$.
3: For each $i \in [n]$: user measures $|\Psi_i\rangle$ in the standard basis if $c_i = 0$, or in the Hadamard basis if $c_i = 1$. User sends all measurement outcomes back to the bank.
4: Bank checks the $\approx 50\%$ of positions i where c_i matches the basis of q_i. Declares VERIFIED if all outcomes on these positions are correct; otherwise REJECTED.

This works because a valid coin, measured in the correct basis, always gives the right outcome. An invalid coin will fail on the checked positions with high probability.

Security note: Knowing the challenge string c tells an adversary which basis was used for each qubit, but not the value of q_i. Whether $q_i \in \{0,1\}$ (standard basis) or $q_i \in \{+,-\}$ (Hadamard basis) are independent of c. The only secret is which of the four values q_i actually takes — so the protocol remains secure even though c is sent in the clear.

Remark 2 (Connection to BB84). This protocol is closely related to Bennett & Brassard's *Quantum Key Distribution* protocol "BB84." In BB84, one party samples random bit values x and random bases θ, creates the corresponding quantum states, and sends them over a quantum channel. The other party samples random bases θ' and measures. After measurement, both parties publicly announce θ and θ'. For the $\approx 50\%$ of positions where $\theta_i = \theta'_i$, the measurement outcomes agree, and those shared uniformly random bits become the secret key.

The security argument: if an adversary intercepts and measures the quantum channel, the state collapses to a basis state corresponding to the adversary's measurement. When the two parties later compare a random subset of their outcomes publicly, any adversarial disturbance causes detectable mismatches — so eavesdropping is always detectable.

5 The Elitzur–Vaidman Bomb Attack

5.1 Setup

We wish to learn an unknown qubit $|X\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ by submitting it for verification, while minimising the probability that the bank detects the attack.
Let $C = \frac{\pi}{2\theta}$.
Attach a *control qubit* in state $|0\rangle$, giving the joint state $|0\rangle \otimes |X\rangle$.

Repeat C times:

1. **Rotate** the control qubit by angle θ (a single-qubit unitary).
2. **CNOT** (control qubit onto target $|X\rangle$).
3. **Submit** the second qubit to the bank for verification. Receive back the post-measurement state.

The control qubit becomes entangled with the coin state without the verification authority noticing.

5.2 Case Analysis

After $C = \frac{\pi}{2\theta}$ repetitions, the following hold in each case.
Case 1: $|X\rangle = |+\rangle$ **(bank measures in Hadamard basis).**

$$|0\rangle \otimes |+\rangle \xrightarrow{\text{rotate}} (\cos\theta\ |0\rangle + \sin\theta\ |1\rangle) \otimes |+\rangle \xrightarrow{\text{CNOT}} (\cos\theta\ |0\rangle + \sin\theta\ |1\rangle) \otimes |+\rangle\,.$$

Since $|+\rangle$ is an eigenstate of the NOT operation, the CNOT gate has no effect on the joint state.
The bank measures the second qubit in the Hadamard basis $\{|+\rangle, |-\rangle\}$:

- $|+\rangle$ is obtained with probability 1,

so the state is always accepted and returned unchanged.
After each iteration, only the control qubit is rotated further. Repeating this process $C = \frac{\pi}{2\theta}$ times accumulates the rotation:

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

Thus,

$$\Pr[\text{detected}] = 0, \qquad \text{final state} = |1\rangle \otimes |+\rangle\,.$$

Case 2: $|X\rangle = |-\rangle$ **(bank measures in Hadamard basis).**

$$|0\rangle \otimes |-\rangle \xrightarrow{\text{rotate}} (\cos\theta\ |0\rangle + \sin\theta\ |1\rangle) \otimes |-\rangle \xrightarrow{\text{CNOT}} \cos\theta\ |0,-\rangle - \sin\theta\ |1,-\rangle = (\cos\theta\ |0\rangle - \sin\theta\ |1\rangle) \otimes |-\rangle\,.$$

(Because $\text{NOT}\,|-\rangle = -\,|-\rangle$.) Bank gets $|-\rangle$ and passes it back with probability 1. The control qubit moves to angle $-\theta$. On the next repetition it is rotated back to 0, and the cycle repeats. Thus $\Pr[\text{undetected}] = 1$ with final state $|0\rangle \otimes |-\rangle$ (assuming C even).

Case 3: $|X\rangle = |0\rangle$ **(bank measures in standard basis).**

$$|0\rangle \otimes |0\rangle \xrightarrow{\text{rotate}} (\cos\theta\ |0\rangle + \sin\theta\ |1\rangle) \otimes |0\rangle \xrightarrow{\text{CNOT}} \cos\theta\ |00\rangle + \sin\theta\ |11\rangle\,.$$

Bank measures the second qubit:

- $|00\rangle$ with probability $\cos^2\theta$,
- $|11\rangle$ (fraud detected) with probability $\sin^2\theta \le \theta^2$.

After $C = \frac{\pi}{2\theta}$ repetitions:

$$\Pr[\text{detected}] \ \le\ \frac{\pi}{2}\,\theta, \qquad \text{final state} = |00\rangle\,.$$

Case 4: $|X\rangle = |1\rangle$ **(bank measures in standard basis).**

$$|0\rangle \otimes |1\rangle \xrightarrow{\text{rotate}} (\cos\theta\ |0\rangle + \sin\theta\ |1\rangle) \otimes |1\rangle \xrightarrow{\text{CNOT}} \cos\theta\ |01\rangle + \sin\theta\ |10\rangle\,.$$

Bank measures the second qubit:

- $|01\rangle$ with probability $\cos^2\theta$,
- $|10\rangle$ (fraud detected) with probability $\sin^2\theta \le \theta^2$.

After $C = \frac{\pi}{2\theta}$ repetitions:

$$\Pr[\text{detected}] \ \le\ \frac{\pi}{2}\,\theta, \qquad \text{final state} = |01\rangle\,.$$

5.3 Summary and Conclusion

Measuring the control qubit in the standard basis at the end reveals whether $|X\rangle = |+\rangle$:

- If $|X\rangle = |+\rangle$: control qubit ends at $|1\rangle$.
- If $|X\rangle \neq |+\rangle$: control qubit ends at $|0\rangle$.

By appropriate rotations, the same scheme can determine whether $|X\rangle = |p\rangle$ for any $p \in \{0, 1, -, +\}$, each with $\Pr[\text{detected}] \leq \frac{\pi}{2}\theta$.

Exercise 1. By applying appropriate basis rotations before and after the procedure described above, show that one can similarly test whether $|X\rangle = |-\rangle$.

References