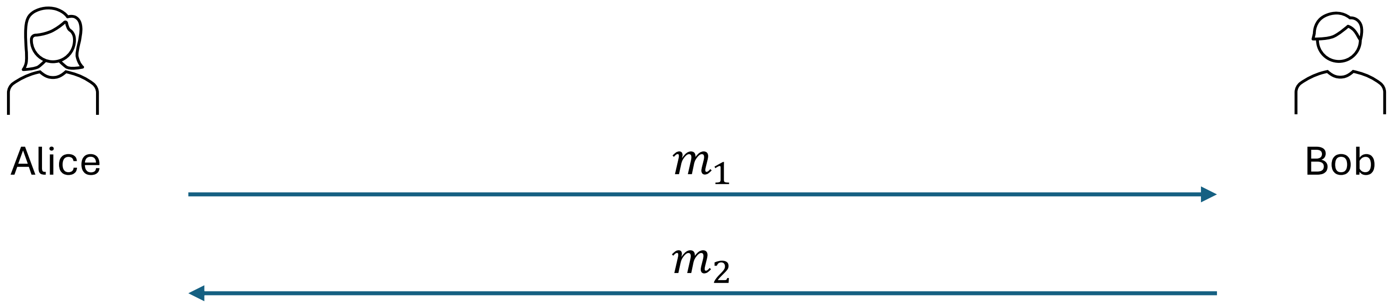
Quantum Computing

- Week 14 (July 23-24, 2025)

- Topics:
  - Quantum key distribution
  - Quantum money
  - Summary of this course

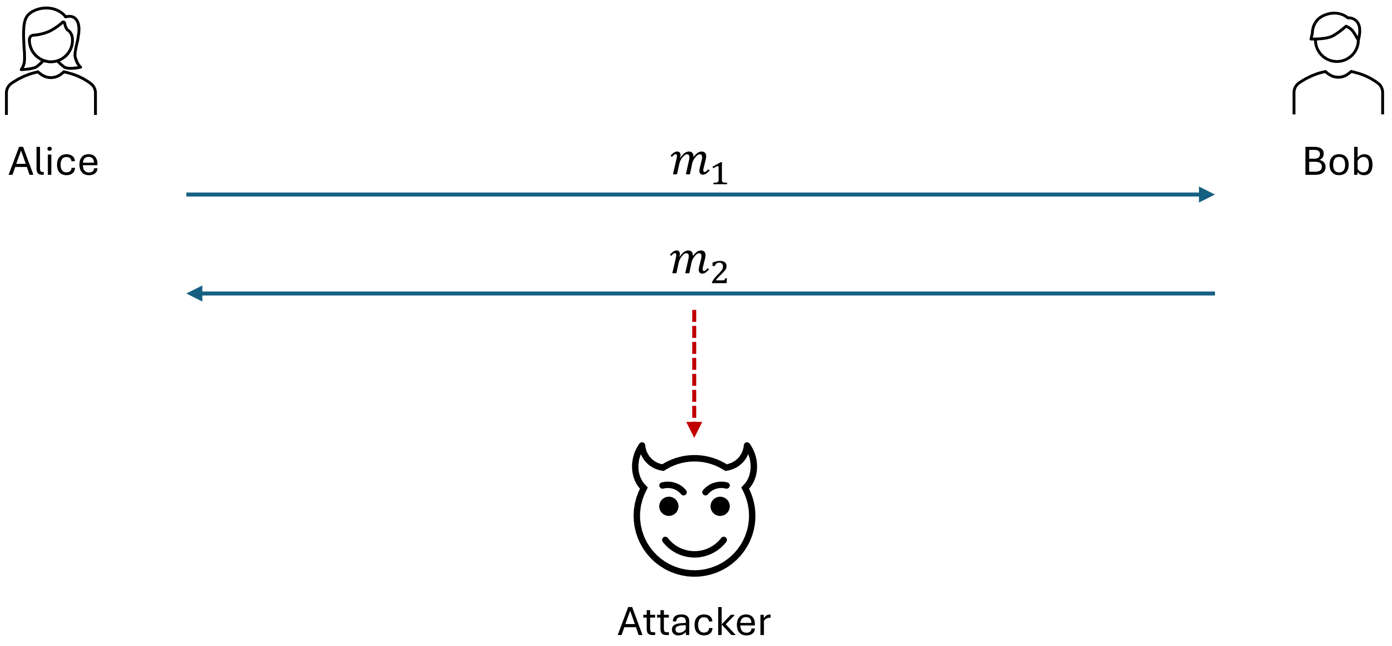
Key Distribution

- Application scenario:



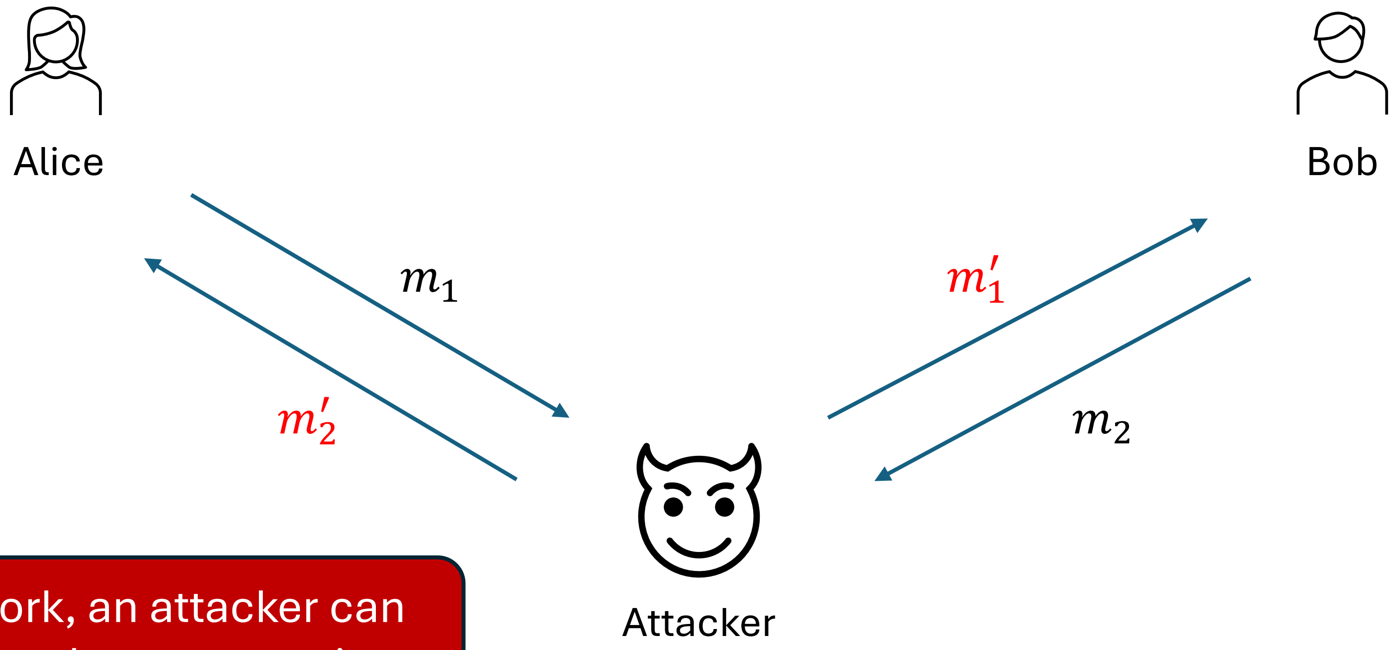
Key Distribution

- Application scenario:



Key Distribution

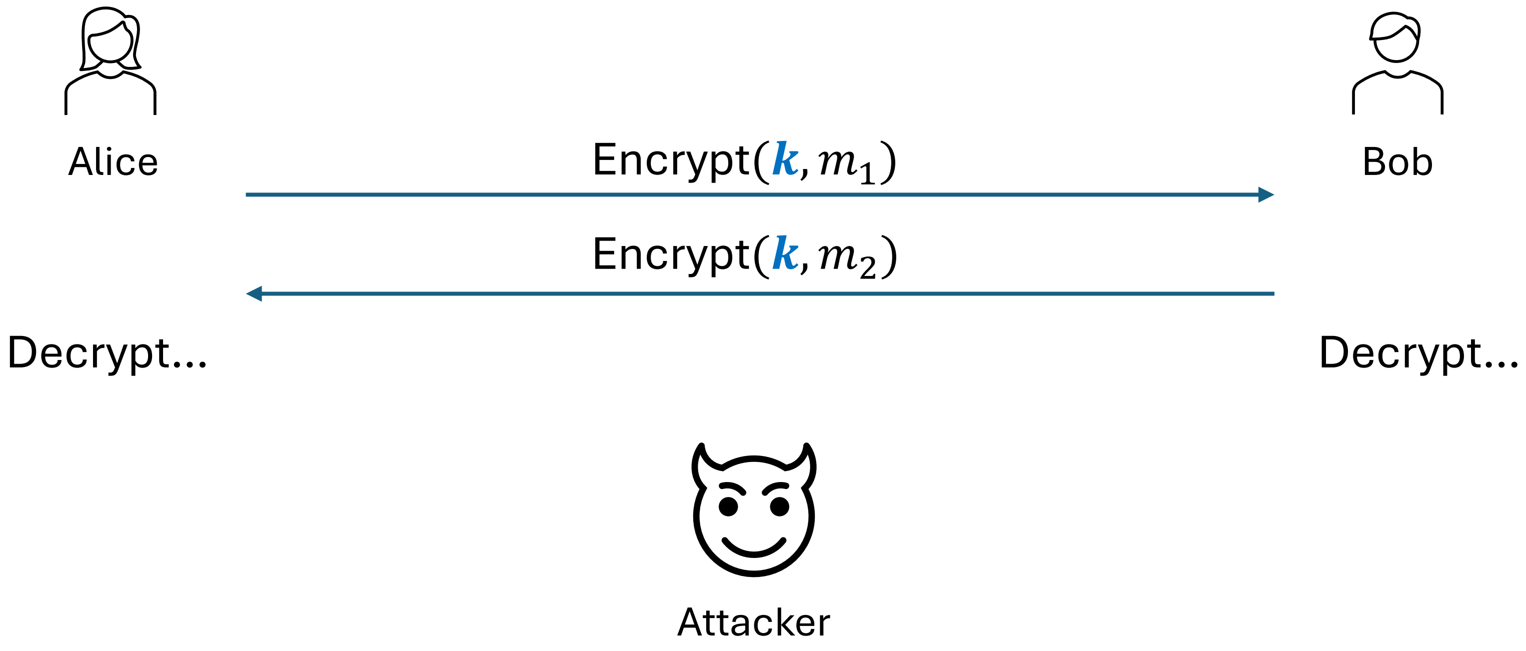
- Application scenario:



- Over a public network, an attacker can eavesdrop or tamper the conversation..

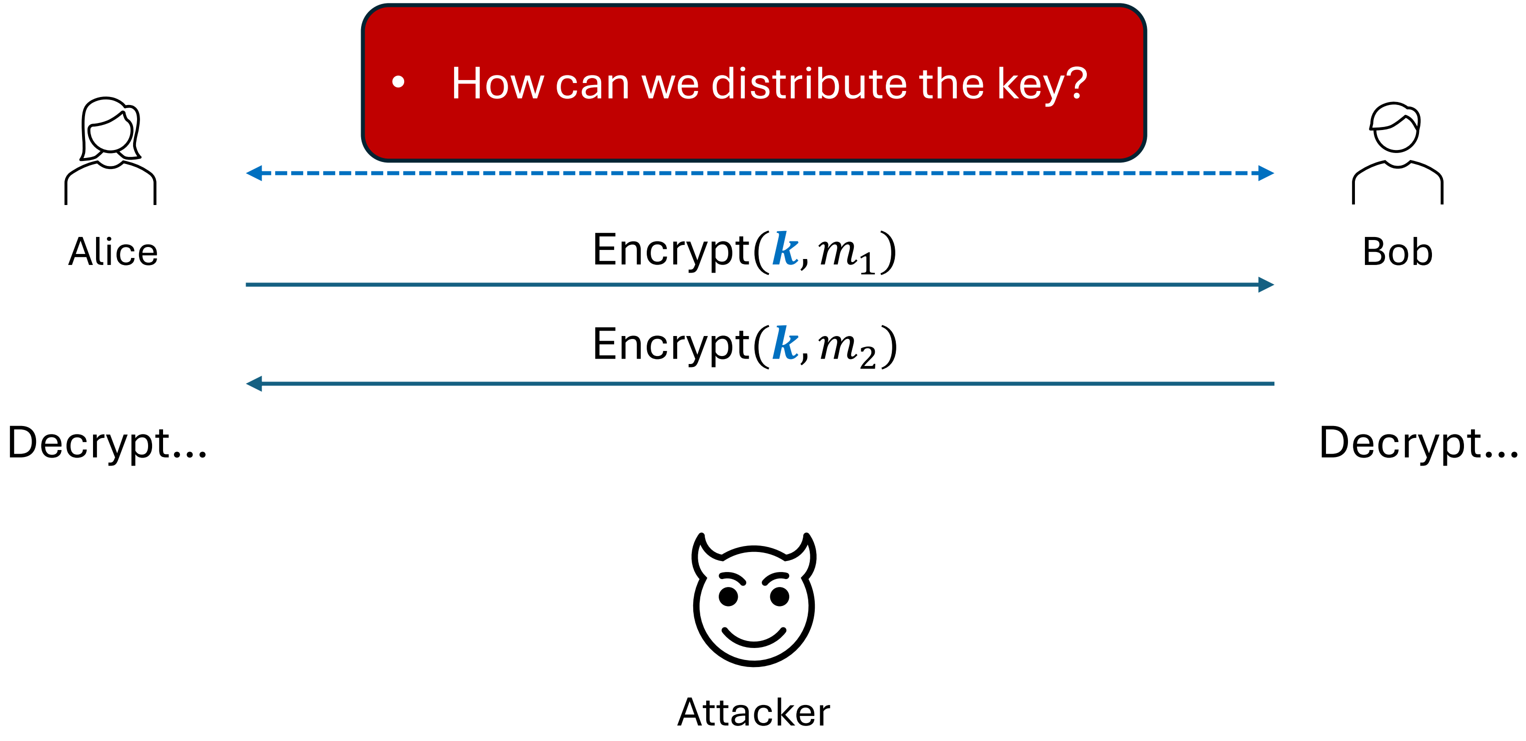
Key Distribution

- Application scenario: Encrypt your conversation using a secret key $\boldsymbol{k}$



Key Distribution

- Application scenario: Encrypt your conversation using a secret key $\boldsymbol{k}$



Key Distribution

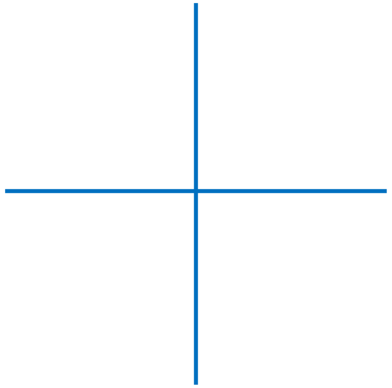
- Application scenario: Encrypt your conversation using a secret key $\boldsymbol{k}$

- But we first need to share the key $\boldsymbol{k}$ in some secure ways:
  - Typical example: TLS 1.3 handshake in HTTPS, X3DH in WhatsApp/Signal…
  - Security relies on the hardness of Discrete Logarithm (DL)
  - DL could be efficiently solved by quantum algorithms (QFT)

- Two ways to fix it:
  - Find new intractable problems
  - Utilize **quantum technique (QKD [BB84])**

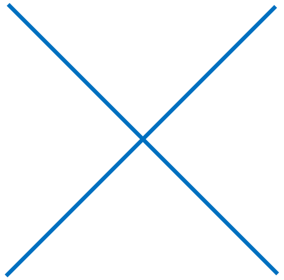
Quantum Key Distribution

- Consider two bases



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

"+"
(Rectilinear)

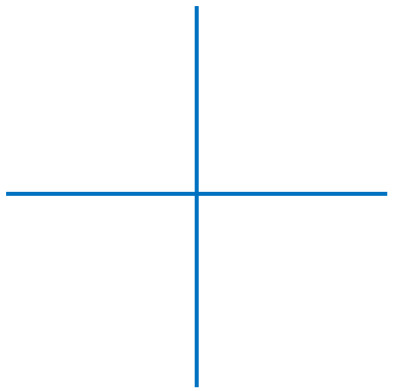


$\{|+\rangle, |-\rangle\}$ $(= \{H|0\rangle, H|1\rangle\})$

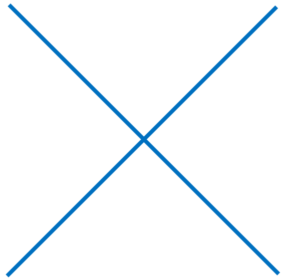
"×"
(Diagonal)

Quantum Key Distribution

- Consider two bases

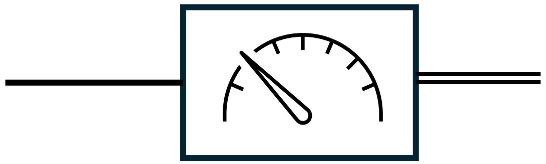


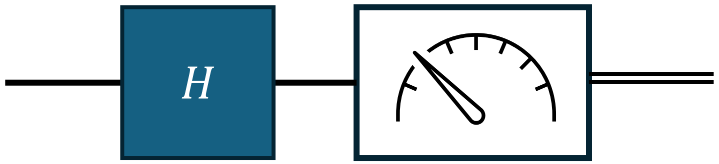
$\{|0\rangle, |1\rangle\}$



$\{|+\rangle, |-\rangle\}$

We encode the measurement result $+$ as 0 and $-$ as 1





Quantum Key Distribution

- The sender (Alice) prepares the following classical random bits

Data bits: $b_1, b_2, b_3, b_4, \ldots, b_m$ Encode bits: $\theta_1, \theta_2, \theta_3, \theta_4, \ldots, \theta_m$

- Encode the data bits via (Weisner Coding):

$$|e_i\rangle \coloneqq H^{\theta_i}|b_i\rangle$$

Namely, if $\theta_i = 0$, then encode b_i as $|b_i\rangle$ (using the "+" basis);
Otherwise, encode b_i as $H|b_i\rangle$ (using the "×" basis).

- Send $|e_1 e_2 \ldots e_m\rangle$ to Bob (via some quantum channels)

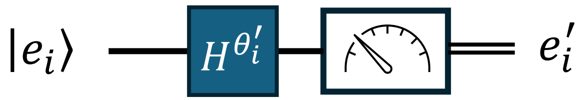
Quantum Key Distribution

- Upon receiving $|e_1 e_2 \dots e_m\rangle$, Bob chooses the following bits uniformly at random

$$\text{Measure bits: } \theta_1', \theta_2', \theta_3', \theta_4', \dots, \theta_m'$$

- Measure $|e_i\rangle$ on the "+" basis if $\theta_i' = 0$ or on the "×" basis if $\theta_i' = 1$:

$$|e_i'\rangle \coloneqq H^{\theta_i'}|e_i\rangle = H^{\theta_i'} H^{\theta_i}|b_i\rangle$$



- Now the "data bits" that Bob possesses are b_i'
- Bob tells Alice that he has received and measured $|e_i\rangle$
- Then, Alice and Bob announce $\theta_1, \theta_2, \dots, \theta_m$ and $\theta_1', \theta_2', \dots, \theta_m'$, and discard b_i and b_i' if $\theta_i \neq \theta_i'$

Quantum Key Distribution

- Example: $m = 4$

b (Alice's data bits)	θ (Alice's encode bits)	$\lvert e_i \rangle$ (The states Alice sent)	θ_i' (Bob's measure bits)	b_i' (The bits Bob measures)
1	1	$\lvert - \rangle$	0	~~0 or 1 (with prob. $\frac{1}{2}$)~~
0	0	$\lvert 0 \rangle$	0	0
1	0	$\lvert 1 \rangle$	1	~~0 or 1 (with prob. $\frac{1}{2}$)~~
0	1	$\lvert + \rangle$	1	0

Quantum Key Distribution

- Upon receiving $|e_1 e_2 \dots e_m\rangle$, Bob chooses the following bits uniformly at random

Measure bits: $\theta'_1, \theta'_2, \theta'_3, \theta'_4, \dots, \theta'_m$

- Measure $|e_i\rangle$ on the "+" basis if $\theta'_i = 0$ or on the "×" basis if $\theta'_i = 1$:

$$|e'_i\rangle \coloneqq H^{\theta'_i}|e_i\rangle = H^{\theta'_i} H^{\theta_i} |b_i\rangle$$

- Now the "data bits" that Bob possesses are b'_i
- Bob tells Alice that he has received and measured $|e_i\rangle$
- Then, Alice and Bob **announce** $\theta_1, \theta_2, \dots, \theta_m$ and $\theta'_1, \theta'_2, \dots, \theta'_m$, and discard b_i and b'_i if $\theta_i \neq \theta'_i$

Does announcing $\theta_1, \theta_2, \dots, \theta_m, \theta'_1, \theta'_2, \dots, \theta'_m$ reveal the bits they shared?

Disturbance Check in QKD

- $b_i = b'_i$ if $\theta_i = \theta'_i$ (Namely, the encode basis of Alice = the measure basis of Bob)

- The attacker may disturb the protocol so that $b_i \neq b'_i$ even if $\theta_i = \theta'_i$. How can we detect this?

Disturbance Check in QKD

- After sharing $n \approx \frac{m}{2}$ bits $b_1 \dots b_n$, Alice and Bob want to check how many (qu)bits are disturbed (eavesdropped or modified) by an attacker…
- Let $m = 4k$ for some integer k. Then $n \approx 2k$

- Alice first picks k bits from $b_1 \dots b_n$ uniformly at random: $b_{i_1} \dots b_{i_k}$.
- Then, Alice sends $i_1, \dots, i_k$ and $b_{i_1} \dots b_{i_k}$ to Bob.
- Bob compares $b_{i_1} \dots b_{i_k}$ with $b'_{i_1} \dots b'_{i_k}$ and discuss with Alice.

- If **too many bits differ**, then they abort the protocol
- Otherwise, keep the remaining k bits and use some standard cryptographic algorithms to derive a key.

Quantum Money

- An important property of money (or currency):
  - Hard to be copied

- Somehow relevant to some properties of quantum states:
  - No-cloning theorem
  - Collapse after measurement

Quantum Money

- **Weisner Coding:** Encode two random bits b and θ as

$$|e\rangle \coloneqq H^{\theta}|b\rangle$$

- If we know θ, then we can perfectly copy the state
  - Knowing θ allows us to perform measurement on the correct basis (“+” or “x”)
  - Measurement gives us b, so we can create $H^{\theta}|b\rangle$ again.

- What if θ is unknown?

Quantum Money

- **Weisner Coding:** Encode two random bits b and θ as

$$|e\rangle \coloneqq H^{\theta}|b\rangle$$

- If we know θ, then we can perfectly copy the state
  - Knowing θ allows us to perform measurement on the correct basis ("+" or "x")
  - Measurement gives us b, so we can create $H^{\theta}|b\rangle$ again.

- What if θ is unknown?
  - Lemma: **The best strategy** for cloning such a $|e\rangle$ has **winning probability** $\frac{3}{4}$
  - Implication: If we have n (b_i, θ_i) pairs, then cloning $|e_1 e_2 \ldots e_n\rangle$ has winning probability at most $\left(\frac{3}{4}\right)^n$

Quantum Money

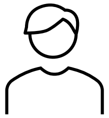
- A simple but impractical quantum money using Weisner Coding:

- Algorithm for issuing money:

$$b_1 b_2 b_3 \dots b_n \leftarrow_{\$} \{0,1\}^n$$
$$\theta_1 \theta_2 \theta_3 \dots \theta_n \leftarrow_{\$} \{0,1\}^n$$
$$|€\rangle \coloneqq |e_1 e_2 e_3 \dots e_n\rangle$$
where $|e_i\rangle \coloneqq H^{\theta_i}|b_i\rangle$

The bank keeps the serial number:
$$\boldsymbol{s} \coloneqq (b_1 \dots b_n, \theta_1 \dots \theta_n)$$

Banknote: $|€\rangle$ →



$|€\rangle$

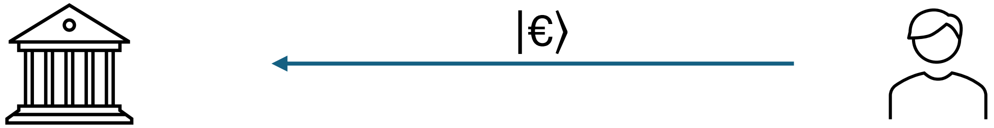
Quantum Money

- A simple but impractical quantum money using Weisner Coding:

- Algorithm for issuing money:

$\boldsymbol{s} \coloneqq (b_1 \ldots b_n, \theta_1 \ldots \theta_n)$ $|€\rangle$

- Algorithm for verifying money:

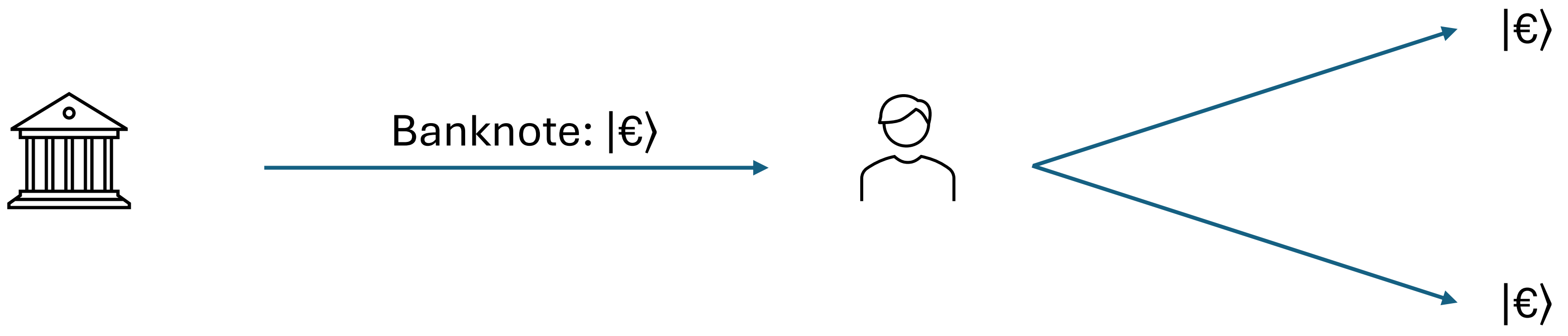


$\boldsymbol{s} \coloneqq (b_1 \ldots b_n, \theta_1 \ldots \theta_n)$

Measure each qubit in |€⟩ (according to $\theta_1 \ldots \theta_n$)
and check if the outcome is $b_1 \ldots b_n$

Quantum Money

- Security (if the serial number is unknown)



...with success probability at most $\left(\frac{3}{4}\right)^n$

- **Drawback:**
  - To verify the money, the merchant (not the bank!) needs to know the serial number

Reference

- **[NC00]:** Section 12.6.3
- Qipeng Liu's lecture note on quantum money: https://drive.google.com/file/d/1bVW-g8Kv6NDkS1vWd3wX2lgSyRmPQZGm/view