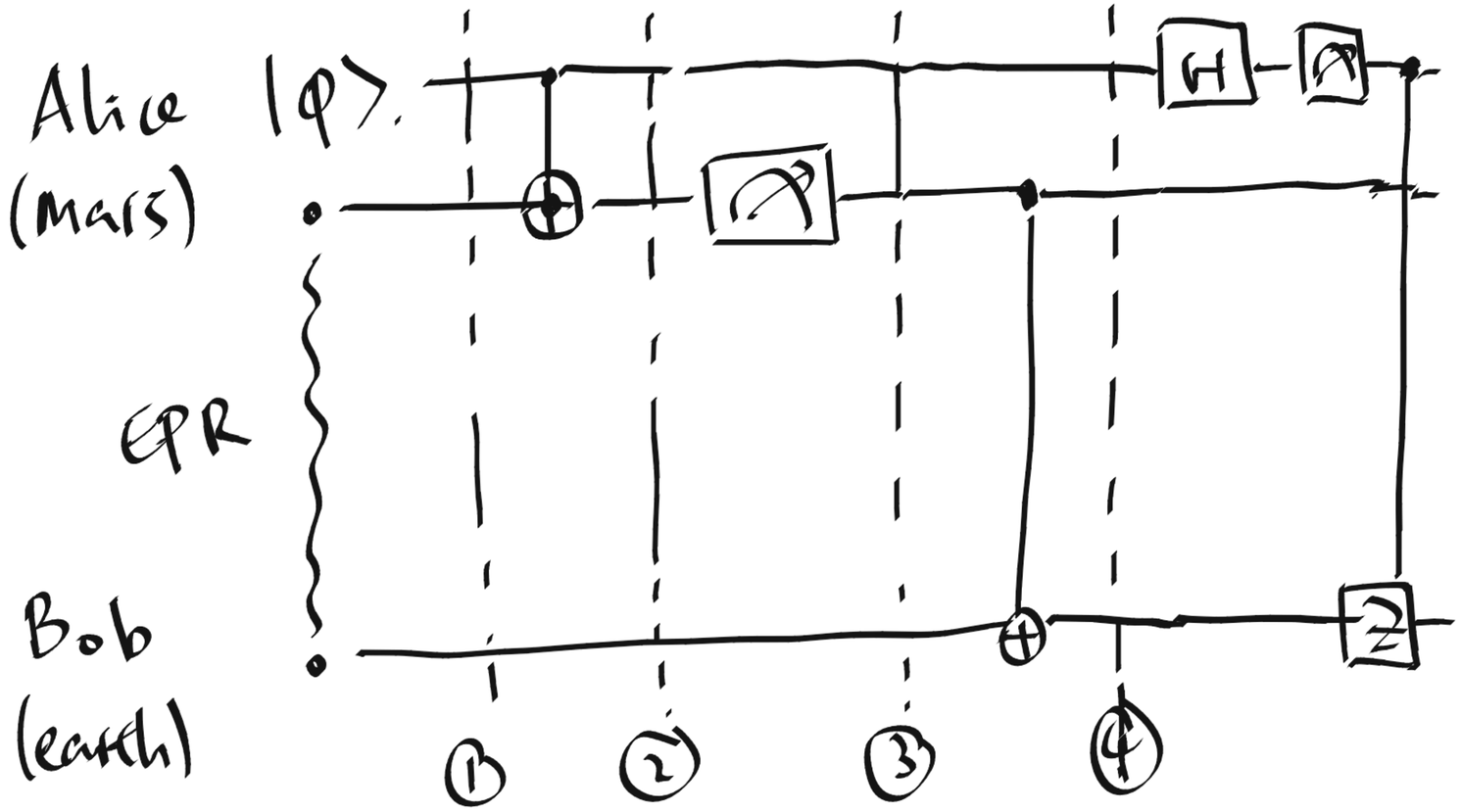
Quantum teleportation

Part II

- Joint state at ① and ②?
- Readout at ③ and joint state collapses to?
- What should Alice right before ④?
- What happens after ④?
- Upshot: “1 ERR + 2 classical bits ≥ 1 qubit”

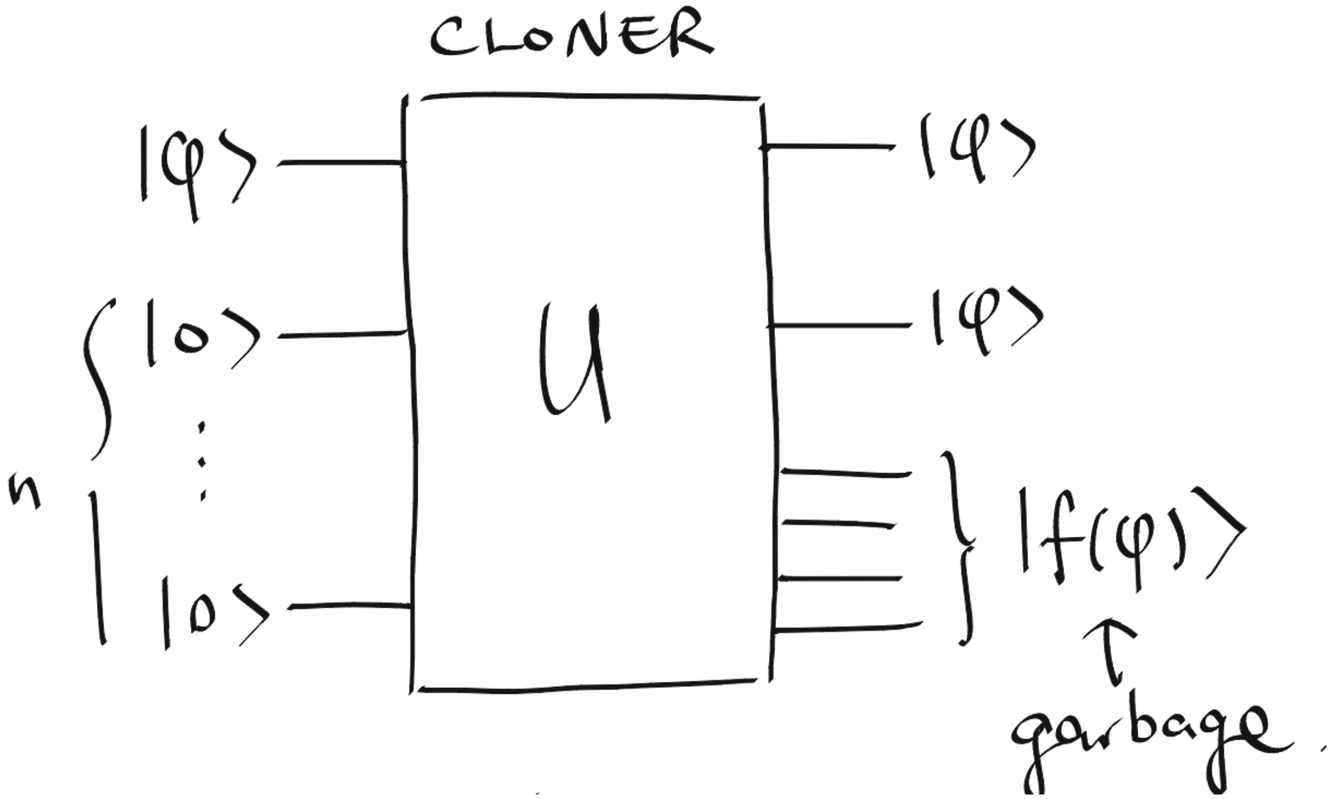


Quantum money

No-cloning theorem

- Bank issues coins and bills
  - Duplication should be impossible
  - Bank should be able to verify validity (Better: everyone can verify validity)
- No-cloning theorem (Wootters, Zurek; Nature 1982): There is no physical device that generates $|\varphi\rangle \otimes |\varphi\rangle$ from $|\varphi\rangle$ for every $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$
- It is possible to have $|0\rangle$-maker, or $|1\rangle$-maker.
- What about CNOT?

Proof of the no-cloning theorem



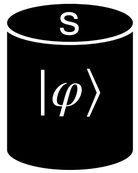
- Consider $|\varphi\rangle = |0\rangle, |1\rangle, |+\rangle$. Then measure the first two qubits.

- There is no cloner that works simultaneously for $|0\rangle, |1\rangle, |+\rangle$
- Remark: The proof does not take into account that “physical device” has internal measurements. Can be dealt with the Deferred Measurement Principle

Wiesner's scheme

Quantum money circa 1983

- "Security parameter" $n = 256$
- Picks "serial number" $s \in \{0,1\}^n$ at random
- Picks $q \in \{0,1,+,-\}^n$
- Creates n-qubit state $|\varphi\rangle = |q_1\rangle \otimes |q_2\rangle \otimes \ldots \otimes |q_n\rangle$
- Manufature quantum coin:
- Store (s, q) in database securely



Verification

Wiesner's scheme

- Bank looks at serial number s, and looks up $q = (q_1, \ldots, q_n)$ from database
- Bank measures i-th qubit of $|\varphi\rangle$ in appropriate basis
  - $|0\rangle, |1\rangle$ if $q_i \in \{0,1\}$
  - $|+\rangle, |-\rangle$ if $q_i \in \{+, -\}$
  - Check whether readout matches q_i
- If all checks pass, gives back the (post-measurement) $|\varphi\rangle$
- If at least 1 check fails, calls police

Non-counterfeitability

Application of the no-cloning theorem

- One shouldn't be able to $(s, |\varphi\rangle) \mapsto (s, |\varphi\rangle), (s, |\varphi\rangle)$
- No-cloning theorem says that doing $|\varphi\rangle \mapsto |\varphi\rangle \otimes |\varphi\rangle$ with 100% probability for all $|\varphi\rangle$ is impossible
- Question: Is it possible to do $|\varphi\rangle \mapsto |\varphi\rangle \otimes |\varphi\rangle$ with 10% probability for all $|\varphi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$? Yes, just randomly guess $|\varphi\rangle$ and create two copies. Success probability is 25%.

Simple attack

What's the success probability?

- Measure each qubit of $|\varphi\rangle$ in the standard basis
- Get some readouts $r \in \{0,1\}^n$
- Make two copies of $(s, |r\rangle)$
- What is the probability that the bank accepts both copies? $(5/8)^n$
- Fact: optimal attack fools bank with probability $(3/4)^n \approx 10^{-32}$ [Molina, Vidick, Watrous 2012]

Wiesner's scheme

Upshot

- Almost impossible to counterfeit? Yes
- Bank can verify validity (private)? Yes
- Everyone can verify validity (public)? No
  - Bank one time generates random: secrete key K_{sec} and public key K_{pub}
  - Users can verify $(s, |\varphi\rangle)$ via some Verif$(s, |\varphi\rangle, K_{\text{pub}})$
  - Open problem: "Public-key Quantum Money"

Policy discussion

- When bank rejects a coin
  - Option 1: Call police
  - Option 2: Return coin if only 1 qubit wrong
- When bank accepts coin
  - Option 1: Give bank the coin
  - Option 2: Destroy the coin, reissue a fresh one
- [Brodutch, Nagaj, Sattath, Unruh 2015] Wiesner's scheme can only be safe if the bank replaces valid notes after validation.

Return coin if only 1 qubit wrong

- How can we learn $|\varphi\rangle$?
  - Say $|\varphi\rangle = |q_1\rangle \otimes |q_2\rangle \otimes \ldots \otimes |q_n\rangle$
  - Trash first qubit $|q_1\rangle$, replace it with your guess (one of $|0\rangle, |1\rangle, |+\rangle, |-\rangle$)
  - Take to bank, ask “Is this good?”
  - Repeat $C \log n$ times for each guess.
- When you guessed right, bank accepts.
- When you guessed wrong, bank rejects it with probability $1 - n^{-C}$.
- You learn $|q_1\rangle$ with probability $1 - n^{-C}$.
- Repeat for all n qubits.