Quantum Money

(and what it really captures)

Part I

Omri Shmueli

Warsaw IACR Summer School on Post-quantum Cryptography 2024

Quantum Operations Recap

The quantum gates we are using in this talk:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

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

$$H|0\rangle = |+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

$$H|1\rangle = |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Quantum Operations Recap

A pure quantum state: A quantum state $|\psi\rangle$ consisting of $n \in \mathbb{N}$ qubits:

$$|\psi\rangle \coloneqq \sum_{x \in \{0,1\}^n} \alpha_x \cdot |x\rangle \ ,$$

$$\forall x \in \{0,1\}^n : \alpha_x \in \mathbb{C} \ ,$$

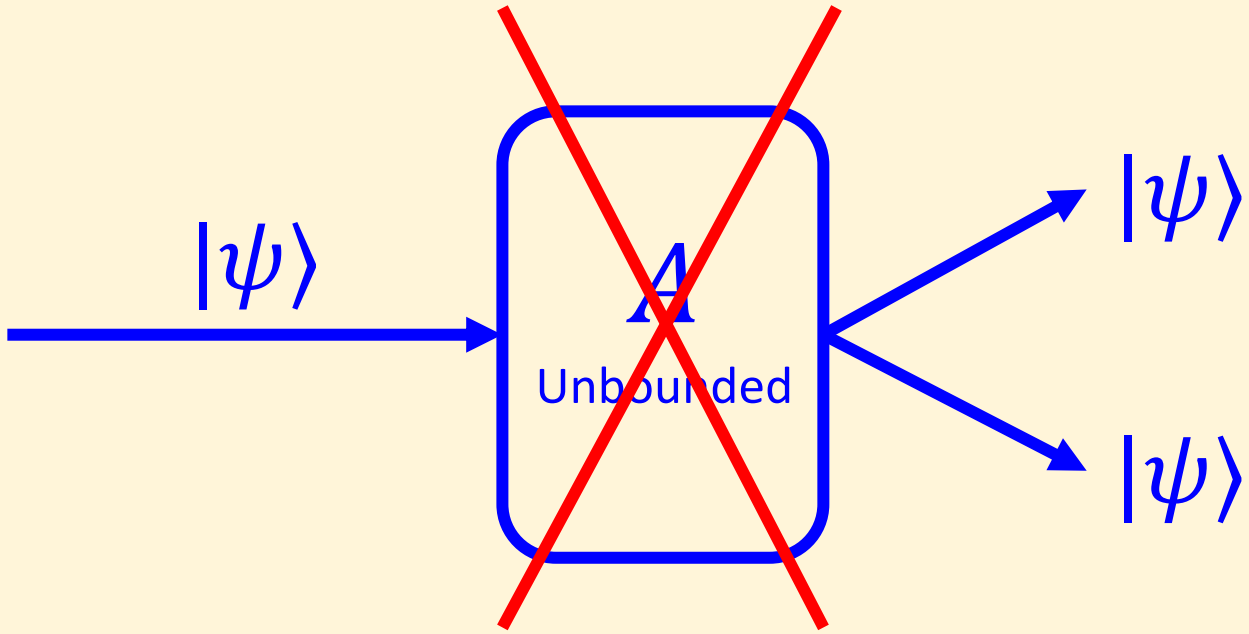
$$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1 \ .$$

A mixed quantum state: Is just a (classical) distribution over quantum states: $|\psi\rangle \leftarrow D$, $D = \{(p_i, |\psi_i\rangle)\}_{i \in M}$.

The No-Cloning Theorem

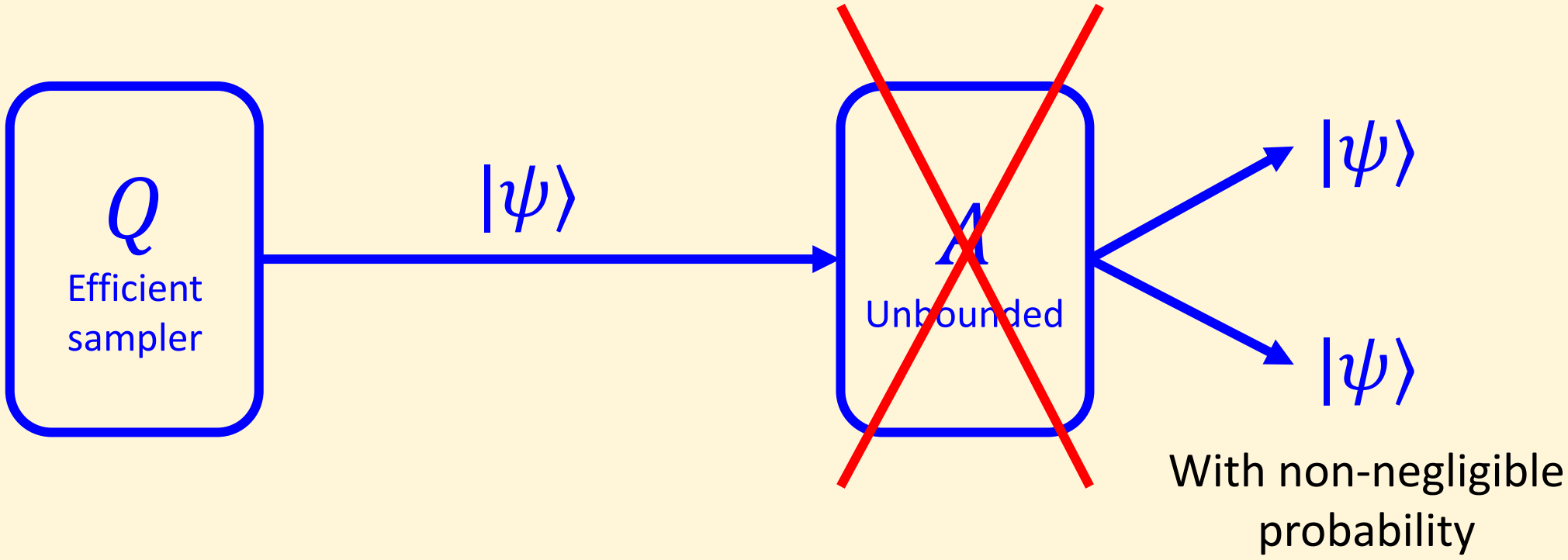
No-Cloning Theorem (informal):

"There is no quantum operation that can copy arbitrary quantum states."



The No-Cloning Theorem

Theorem [No-cloning, cryptographic version]:



The No-Cloning Theorem

Theorem [No-cloning, cryptographic version]:

$\exists$ a quantum polynomial time algorithm Q,

- For input $n \in \mathbb{N}$, $Q(1^n)$ samples an n-qubit state $|\psi\rangle$.
- For every (possibly unbounded) quantum algorithm A,

$$\Pr_{|\psi\rangle \leftarrow Q(1^n)}[A(|\psi\rangle) = |\psi\rangle|\psi\rangle] \leq 2^{-\Omega(n)}.$$

Actually: Many different algorithms for Q!

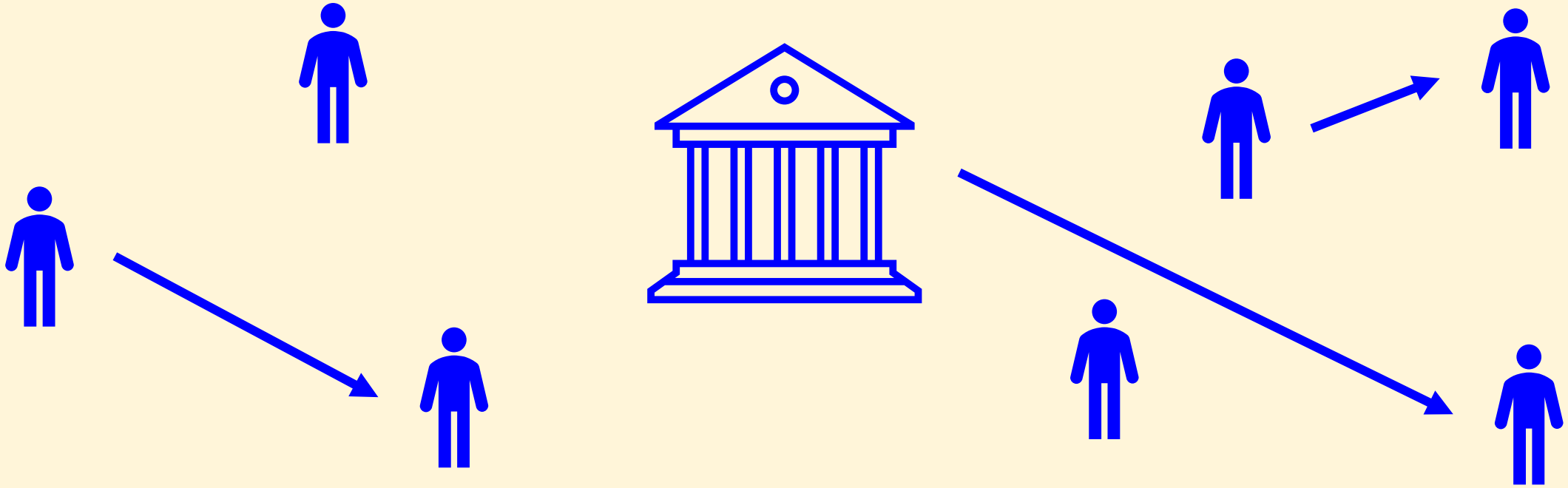
Quantum Money – the vision

- A quantum system can hold an unclonable quantum state $|\psi\rangle$

$\Rightarrow$ Quantum systems can be rare physical objects.

- States take tiny physical space.
- Transferred through communication channels, immediately over large distances.

Quantum Money – the vision



Idealized digital cash:

1. Takes negligible physical space, 2. Locally algorithmically verifiable,
3. Provably unforgeable, 4. Can be sent instantaneously.

Talk Plan – 1st Part

- Quantum money – Definition.
- Quantum money – Why it is about quantum cryptography, and not about money.
- Private-key quantum money.
  - Basic techniques for sampling unclonable states.
- Public-key quantum money.
  - Construction paradigm: Range and quantumness checks.
  - Subspace states and quantum Fourier transform.
- PKQM in the standard model.
  - Subspace-hiding obfuscation.

Quantum Money

Definition [Secret-Key Quantum Money, Wiesner-1969]:

Given by two polynomial-time quantum algorithms,

- $(sk, |\psi\rangle_{sk}) \leftarrow \mathrm{Gen}(1^n)$.
- $(b \in \{0,1\}, |\phi'\rangle) \leftarrow \mathrm{Ver}(sk, |\phi\rangle)$.

Quantum Money

- **Correctness:**

$$\Pr_{(sk,|\psi\rangle_{sk})\leftarrow \mathrm{Gen}(1^n)}[(\qquad\qquad) \leftarrow \mathrm{Ver}(sk, |\psi\rangle_{sk})]$$

Quantum Money

- **Correctness:**

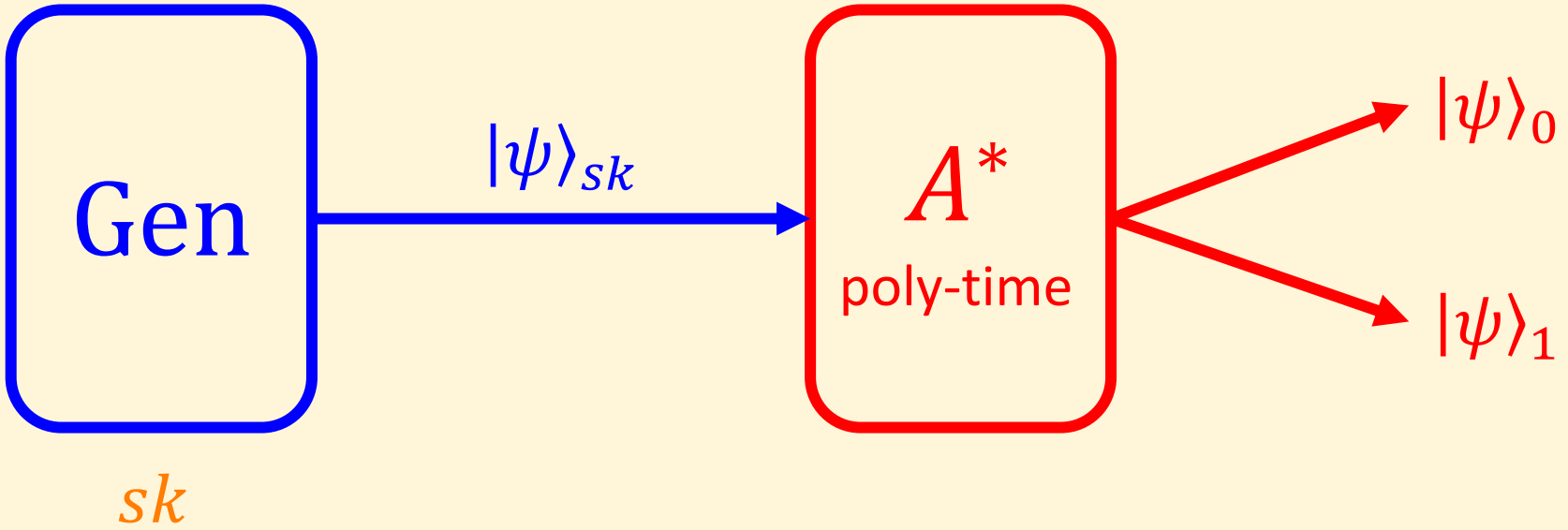
$$\Pr_{(sk,|\psi\rangle_{sk})\leftarrow \mathrm{Gen}(1^n)}[(1,|\psi\rangle_{sk}) \leftarrow \mathrm{Ver}(sk,|\psi\rangle_{sk})] = 1\,.$$

- **Security:**

?

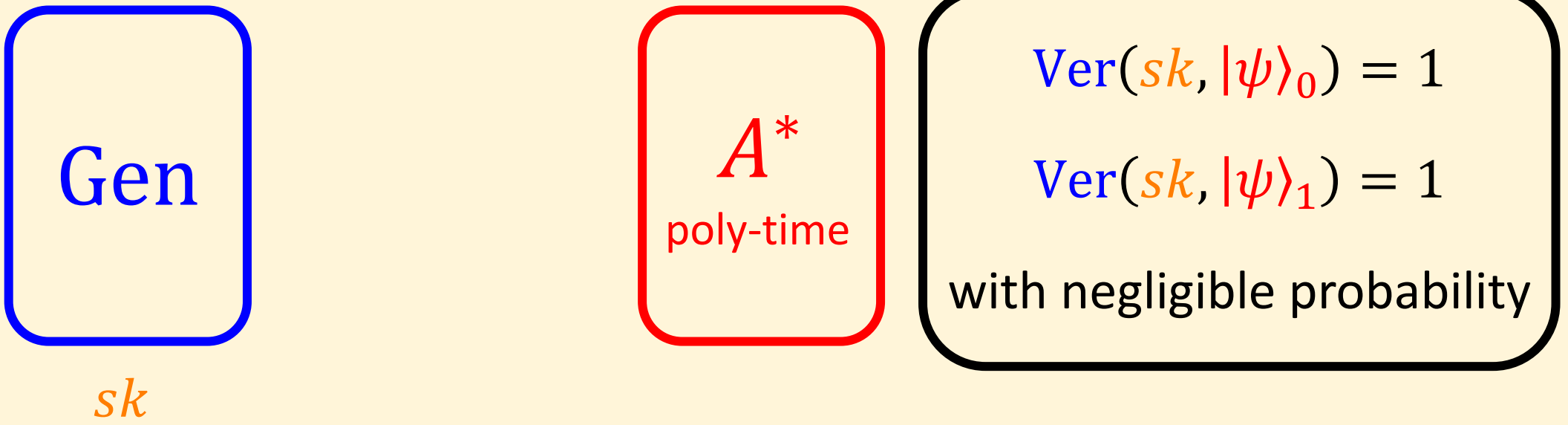
Quantum Money

- **Security:**



Quantum Money

- **Security:**



Quantum Money

- **Correctness:**

$$\Pr_{(sk,|\psi\rangle_{sk})\leftarrow \mathrm{Gen}(1^n)}[(1,|\psi\rangle_{sk}) \leftarrow \mathrm{Ver}(sk,|\psi\rangle_{sk})] = 1\,.$$

- **Security:**

$$\forall \mathrm{poly}-\mathrm{time}\ A^*\colon \Pr_{(sk,|\psi\rangle_{sk})\leftarrow \mathrm{Gen}(1^n)}\begin{bmatrix} A^*(|\psi\rangle_{sk}) = |\psi\rangle_0|\psi\rangle_1, \\ \mathrm{Ver}(sk,|\psi\rangle_0) = 1, \\ \mathrm{Ver}(sk,|\psi\rangle_1) = 1 \end{bmatrix} \leq \mathrm{negl}(n)\,.$$

Quantum Money

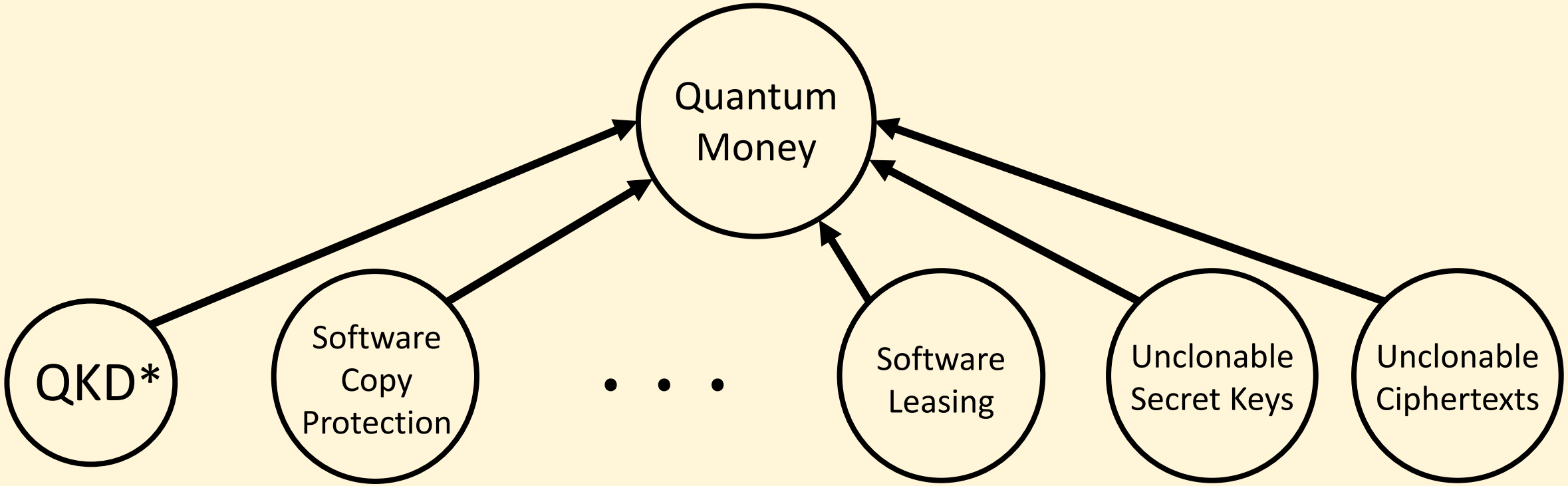
What it really is:

An efficiently samplable distribution over quantum states that is,

(1) Verifiable given a key, (2) Unclonable.

Quantum Money

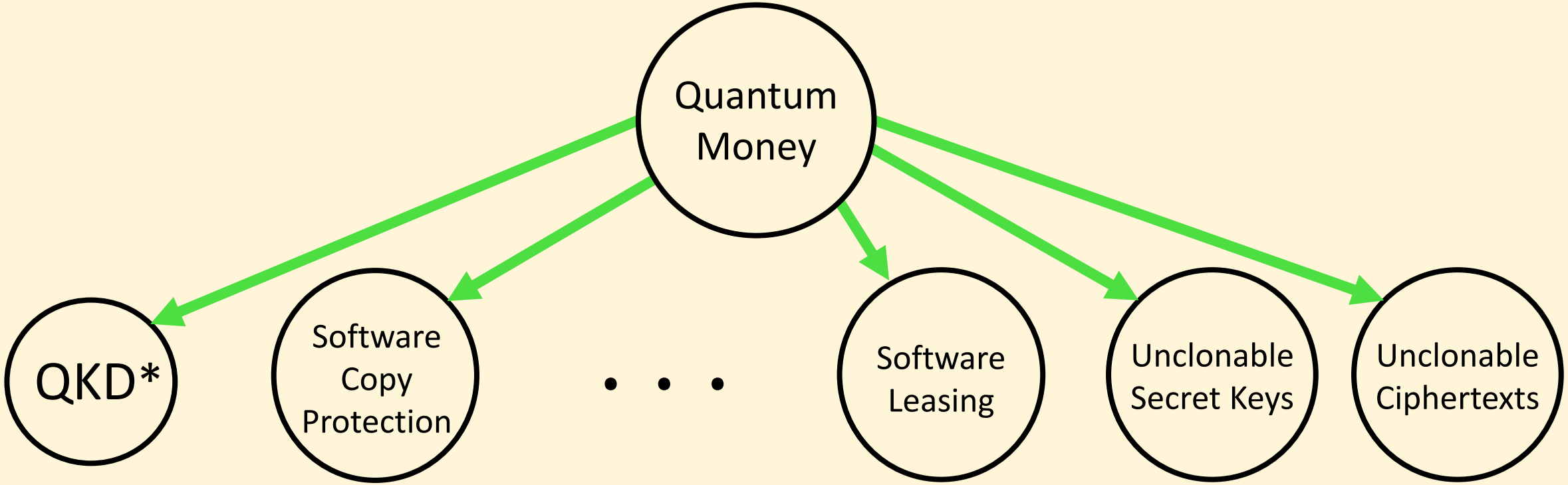
Quantum Money can be viewed as a pre-condition for quantum cryptography.



Quantum Money

Breakthroughs in quantum money techniques

⇒ breakthroughs for a lot of quantum cryptography.



Constructing Private-key Quantum Money

Constructing Quantum Money

Q:

How do we efficiently sample a distribution over quantum states that's both,

(1) verifiable and (2) unclonable?

Constructing Quantum Money

Claim [single-qubit no-cloning, unitary]: Consider the following set of quantum states,

$$S \coloneqq \left\{ \begin{array}{c} |0\rangle, \\ |1\rangle, \\ |+\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} \right\} .$$

Then, there is no unitary transformation U on 2 qubits such that:

$$U(|0\rangle|0\rangle) = |0\rangle|0\rangle, \qquad U(|1\rangle|0\rangle) = |1\rangle|1\rangle,$$
$$U(|+\rangle|0\rangle) = |+\rangle|+\rangle, \qquad U(|-\rangle|0\rangle) = |-\rangle|-\rangle .$$

Constructing Quantum Money

Proof [single-qubit no-cloning, unitary]:

- Assume towards contradiction that there is such cloning $U \in \mathbb{C}^{4\times 4}$.
- U successfully clones $|+\rangle$, thus:

$$U(|+\rangle|0\rangle) = |+\rangle|+\rangle = \frac{1}{2}(1,1,1,1)^T .$$

- However, (1) the state $|+\rangle$ is in the span of $|0\rangle$ and $|1\rangle$, and

(2) U successfully clones both $|0\rangle$ and $|1\rangle$. We get:

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

$$= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) = \frac{1}{\sqrt{2}}(1,0,0,1)^T \neq \frac{1}{2}(1,1,1,1)^T .$$

■

Constructing Quantum Money

Lemma [single-qubit cryptographic no-cloning – no proof]:

Consider the uniform distribution over the same set as before,

$$S \coloneqq \left\{ \begin{array}{c} |0\rangle, \\ |1\rangle, \\ |+\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} \right\} .$$

Then, there is some constant $c \in \mathbb{N}$ s.t. for every quantum algorithm A:

$$\Pr_{|\psi\rangle \leftarrow S}[A(|\psi\rangle) = |\psi\rangle|\psi\rangle] \leq 1/c .$$

Constructing Quantum Money

Construction:

- $(sk, |\psi\rangle_{sk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{sk} = ?$
- $sk = ?$

Constructing Quantum Money

Construction:

- $(sk, |\psi\rangle_{sk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{sk} = n$ i.i.d. samples from S.
- $sk =$ the classical descriptions of the n samples.

Constructing Quantum Money

Construction:

- $(sk, |\psi\rangle_{sk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{sk} = \left(H^{b_1}X^{a_1}|0\rangle, \cdots, H^{b_n}X^{a_n}|0\rangle\right)$
- $sk = (a \in \{0,1\}^n, b \in \{0,1\}^n)$.

Constructing Quantum Money

Construction:

- $(sk, |\psi\rangle_{sk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{sk} = \left(H^{b_1}X^{a_1}|0\rangle, \cdots, H^{b_n}X^{a_n}|0\rangle\right) := H^{\otimes b}X^{\otimes a}|0^n\rangle$.
- $sk = (a \in \{0,1\}^n, b \in \{0,1\}^n)$.
- $\mathrm{Ver}(sk, |\phi\rangle)$: ?

Constructing Quantum Money

Construction:

- $(sk, |\psi\rangle_{sk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{sk} = \left(H^{b_1}X^{a_1}|0\rangle, \cdots, H^{b_n}X^{a_n}|0\rangle\right) := H^{\otimes b}X^{\otimes a}|0^n\rangle$.
- $sk = (a \in \{0,1\}^n, b \in \{0,1\}^n)$.
- $\mathrm{Ver}(sk, |\phi\rangle)$: Accepts iff $|0^n\rangle = \left(X^{\otimes a}\right)^{-1}\left(H^{\otimes b}\right)^{-1}|\phi\rangle$.

Constructing Quantum Money

Claim (Security):

$$\forall A^*: \Pr_{(sk,|\psi\rangle_{sk})\leftarrow \mathrm{Gen}(1^n)}\left[\begin{array}{c} A^*(|\psi\rangle_{sk}) = |\psi\rangle_0|\psi\rangle_1, \\ \mathrm{Ver}(sk,|\psi\rangle_0) = 1, \\ \mathrm{Ver}(sk,|\psi\rangle_1) = 1 \end{array}\right] \leq 2^{-\Omega(n)}.$$

Security proof sketch:

- The verification is projective: The only state that passes with probability 1 is $|\psi\rangle_{sk}$.
- To break security w.p. p, the adversary really needs to clone w.p. p.

Constructing Quantum Money

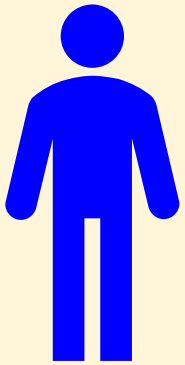
Security proof sketch:

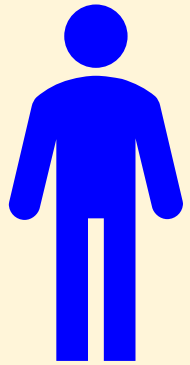
- For the adversary to clone, it needs to clone all n qubits.
- 1-qubit cryptographic no-cloning ⇒ each qubit can be cloned with probability bounded by constant $\frac{1}{c} = \frac{1}{2^{\log(c)}}$.
- Since all qubits are i.i.d., the probability to succeed cloning all n qubits is $\leq 2^{-n \cdot \log(c)} \leq 2^{-\Omega(n)}$.

■

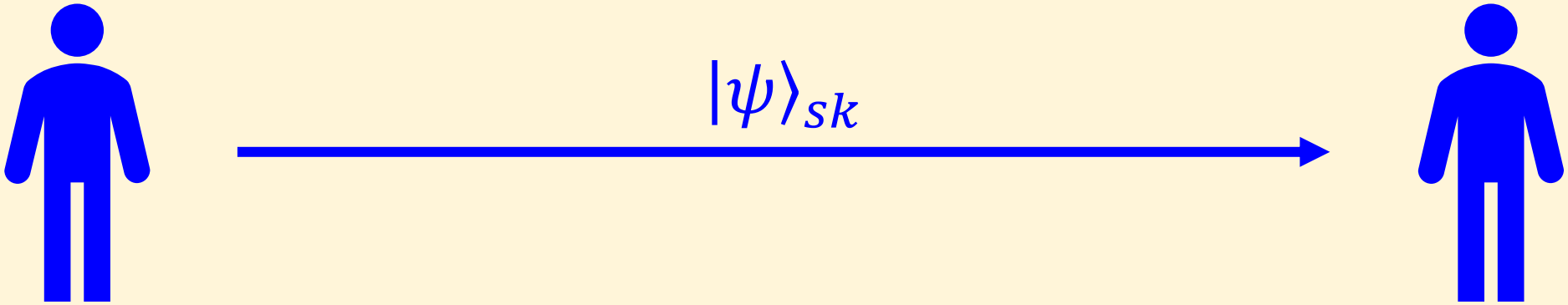
The Public Verification Problem

$|\psi\rangle_{sk}$

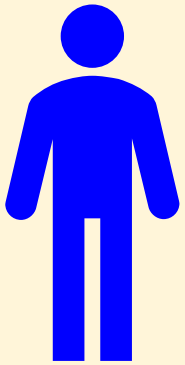




The Public Verification Problem

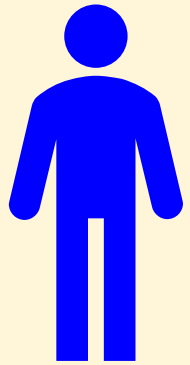


The Public Verification Problem



$|\psi\rangle_{sk}$

? ? ?



Q: Can we publicize sk?

The Public Verification Problem

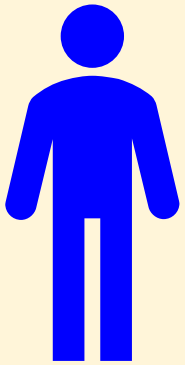
No.

The state $|\psi\rangle_{sk}$ is not only verified, but is <u>generated</u> from the secret key sk:

- $|\psi\rangle_{sk} = \left(H^{b_1}X^{a_1}|0\rangle, \cdots, H^{b_n}X^{a_n}|0\rangle\right) \coloneqq H^{\otimes b}X^{\otimes a}|0^n\rangle$.
- $sk = (a \in \{0,1\}^n, b \in \{0,1\}^n)$.

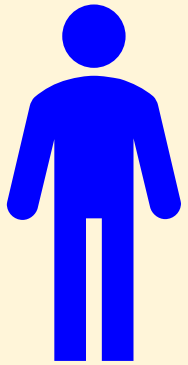
$\Rightarrow$ If you have the key, you can clone.

The Public Verification Problem



$|\psi\rangle_{sk}$

???



Q: Ok, cannot publicize sk. Maybe we can verify without sk?

The Public Verification Problem

No.

Without the key, random quantum information can be indistinguishable from random classical information.

Claim:

$$\{S_1, S_2, \cdots, S_n\} \equiv \{|s\rangle \mid s \leftarrow \{0,1\}^n\}\,.$$

Proof sketch: It is an easy exercise in quantum information theory to prove for a single qubit: $\{S\} \equiv \{|b\rangle \mid b \leftarrow \{0,1\}\}$, that is:

$$\left\{\left(\frac{1}{4}, |0\rangle\right), \left(\frac{1}{4}, |1\rangle\right), \left(\frac{1}{4}, |+\rangle\right), \left(\frac{1}{4}, |-\rangle\right)\right\} \equiv \left\{\left(\frac{1}{2}, |0\rangle\right), \left(\frac{1}{2}, |1\rangle\right)\right\}\,.$$

The Public Verification Problem

- Since the conception of quantum money by Stephen Wiesner (1969), was open.
- First breakthrough by Scott Aaronson and Paul Christiano in 2012 (solution with respect to an oracle).
- Solution in the standard model by Mark Zhandry in 2018.

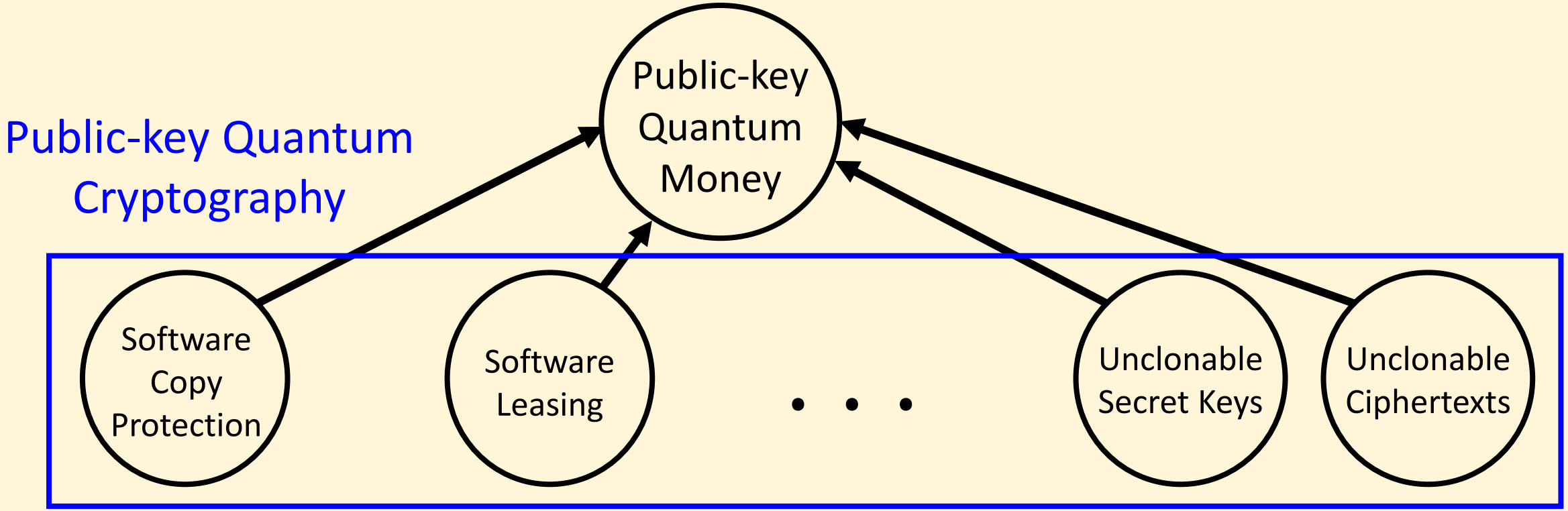
Public-key Quantum Money

An efficiently samplable distribution over quantum states that is,

(1) Publicly verifiable, (2) Unclonable.

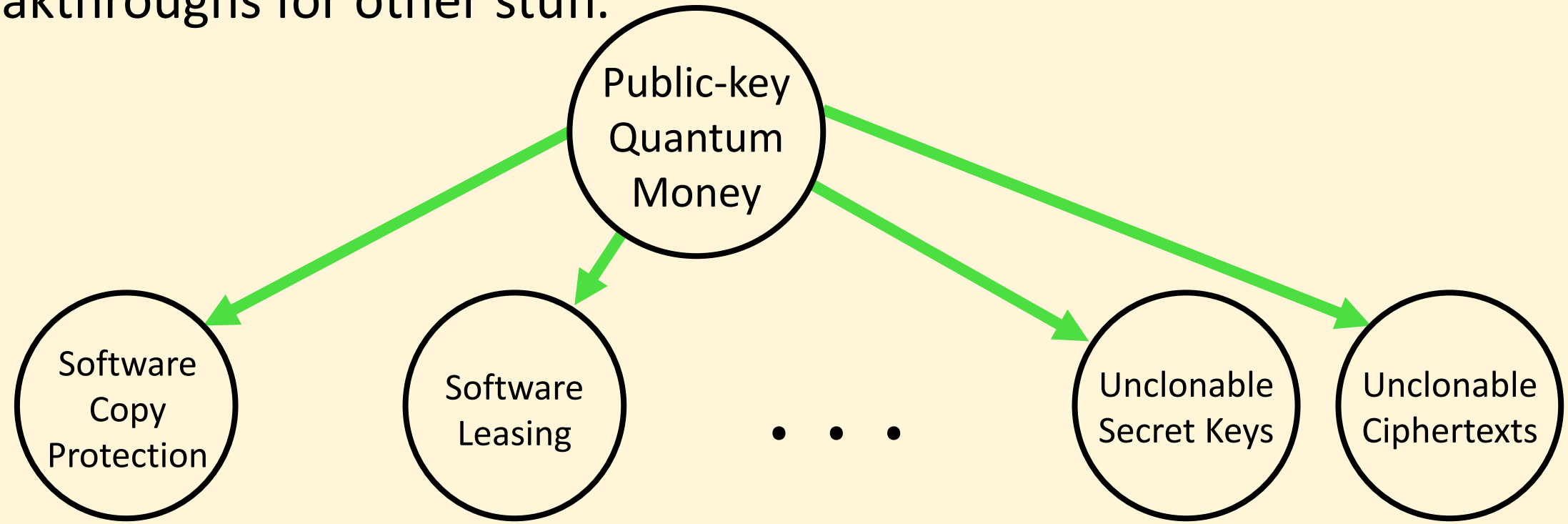
Public-key Quantum Money

A pre-condition for public-key quantum cryptography.



Public-key Quantum Money

As before, technical breakthroughs in PKQM, usually imply breakthroughs for other stuff.



Public-key Quantum Money

Definition:

Given by two polynomial-time quantum algorithms,

- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $(b \in \{0,1\}, |\phi'\rangle) \leftarrow \mathrm{Ver}(pk, |\phi\rangle)$.

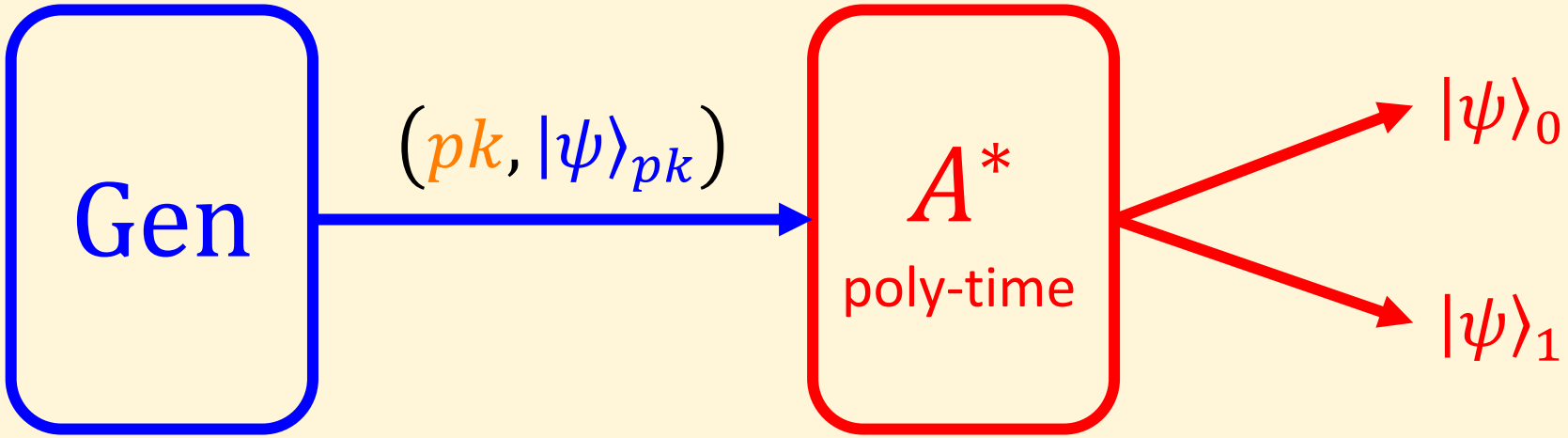
Public-key Quantum Money

- **Correctness:**

$$\Pr_{(pk,|\psi\rangle_{pk})\leftarrow \mathrm{Gen}(1^n)}\left[(1,|\psi\rangle_{pk}) \leftarrow \mathrm{Ver}(pk,|\psi\rangle_{pk})\right] = 1\ .$$

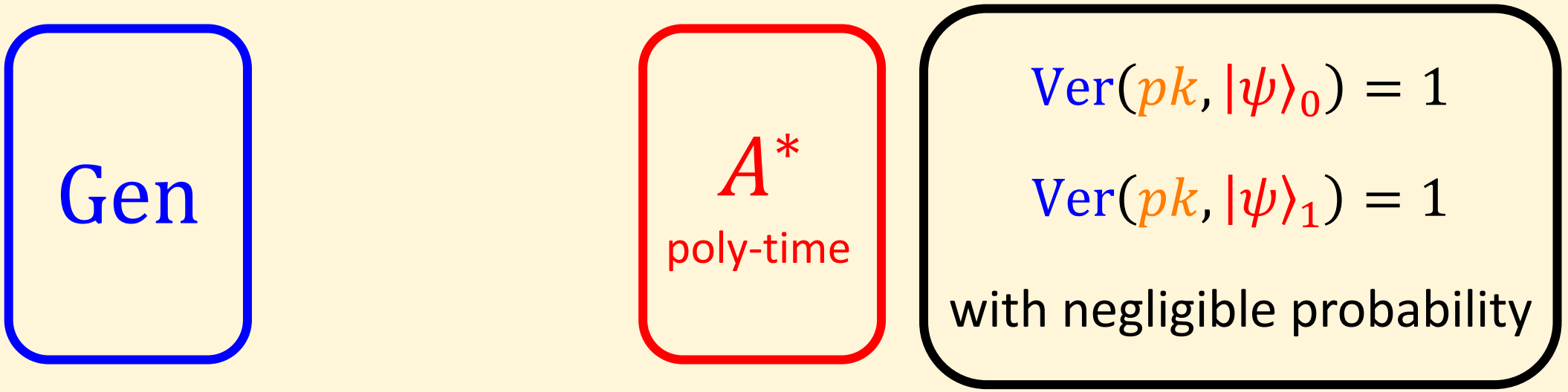
Public-key Quantum Money

- **Security:**



Public-key Quantum Money

- **Security:**



Constructing Public-key Quantum Money

- We will next construct, in steps, the [Aaronson-Christiano-2012] Public-key Quantum Money Scheme.
- The scheme is secure with respect to quantum oracle access to a classical function (to be defined).
- After that, we will see the construction in the plain model by [Zhandry-2018].

Constructing Public-key Quantum Money

Goal: Construct a PKQM scheme.

- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{pk} = ?$
- $pk = ?$
- $\mathrm{Ver}(pk, |\phi\rangle)$: ?

Constructing Public-key Quantum Money

Definition [Quantum-secure Indistinguishability obfuscation]:
A classical probabilistic polynomial-time algorithm iO,

- $\mathrm{Obf}_C \leftarrow \mathrm{iO}\left(1^\lambda, C\right)$, where C, Obf_C are classical circuits, $\lambda \in \mathbb{N}$.
- **Correctness:** The circuits C and Obf_C have the same functionality.
- **Security:** For $\lambda \in \mathbb{N}$, every poly and a pair of functionally-equivalent circuits C_0, C_1 that are both of size $\leq \mathrm{poly}(\lambda)$:

$$\left\{\mathrm{Obf}_{C_0} \leftarrow \mathrm{iO}\left(1^\lambda, C_0\right)\right\} \approx_c \left\{\mathrm{Obf}_{C_1} \leftarrow \mathrm{iO}\left(1^\lambda, C_1\right)\right\}.$$

Constructing Public-key Quantum Money

Quantum-secure iO:

- Hides the inner workings of an algorithm.
- Classically-secure iO is known from well-studied assumptions [Jain-Lin-Sahai-2020].
- Quantum-secure iO is known based on more specific assumptions [Brakerski-Dottling-Garg-Malavolta-2020a + b], [Gay-Pass-2021].
- "Ideal Obfuscation": Obfuscated circuit Obf_C **sometimes** reveals no more than **oracle** access to C.

Constructing Public-key Quantum Money

Classical Computation in Quantum Superposition:

- Let $f:\{0,1\}^n \to \{0,1\}^m$ a classical function. The unitary version of f is given by the $(n+m)$-qubit unitary U_f:

$$\forall x \in \{0,1\}^n : U_f|x,0^m\rangle = |x,f(x)\rangle\,.$$

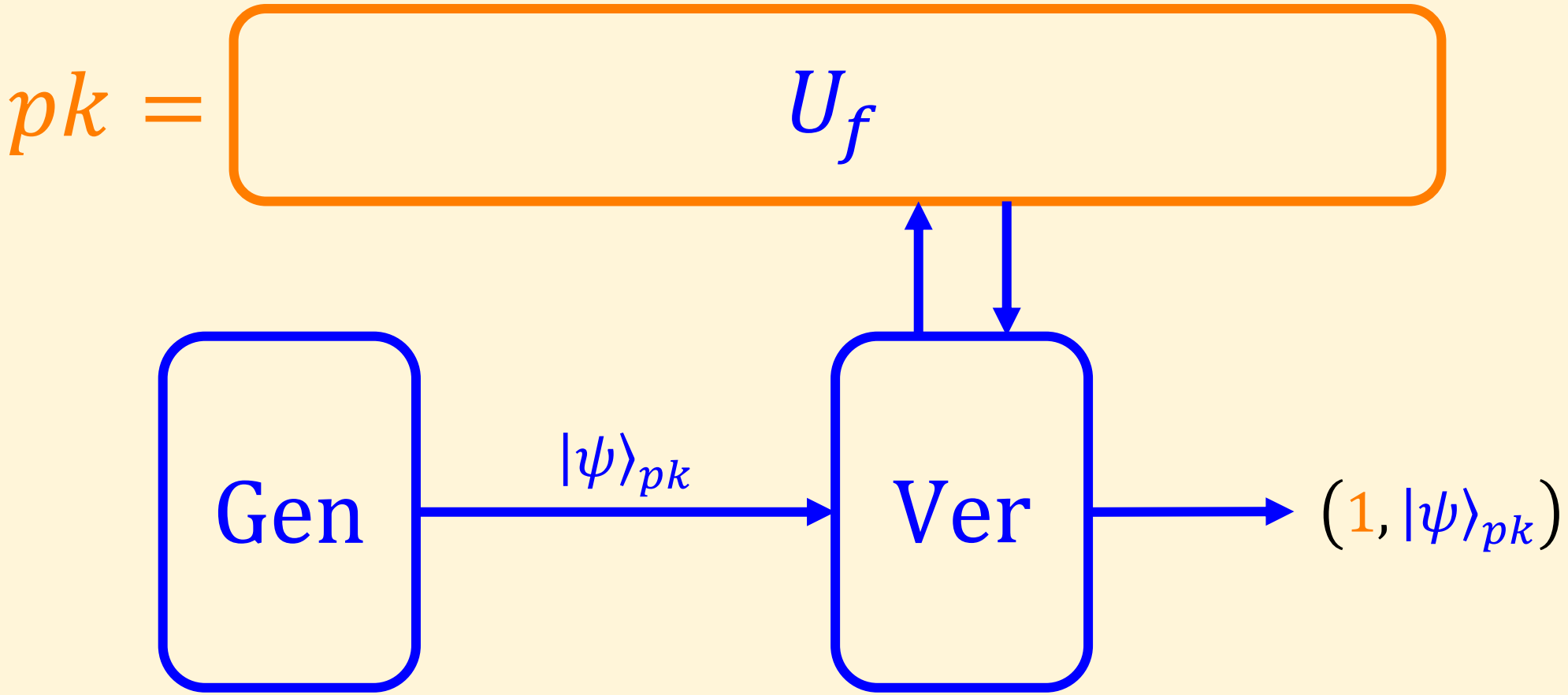
- A quantum oracle access to a classical function $f:\{0,1\}^n \to \{0,1\}^m$, is access to the $(n+m)$-qubit unitary U_f.
- There is an efficient classical algorithm that given a classical circuit C implementing $f:\{0,1\}^n \to \{0,1\}^m$, constructs the (classical description of the) unitary circuit for U_f.

Constructing Public-key Quantum Money

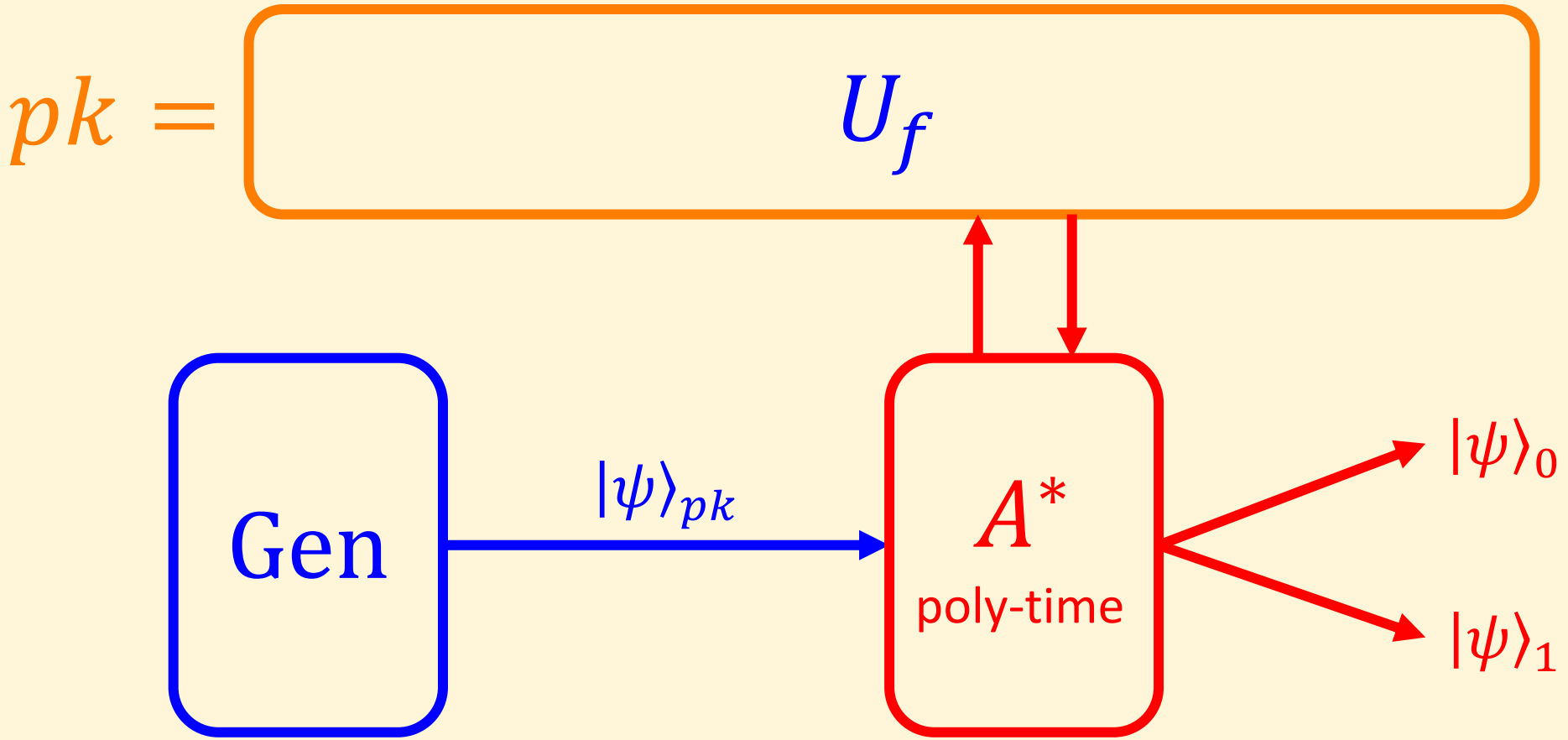
Idea: Think of pk as an ideal obfuscation of some classical $f: \{0,1\}^n \to \{0,1\}^m$.

- We know that Obf_f implies (oracle only) access to U_f.
- $|\psi\rangle_{pk}$ should be verifiable given access to U_f.
- $|\psi\rangle_{pk}$ should remain unclonable given access to U_f.

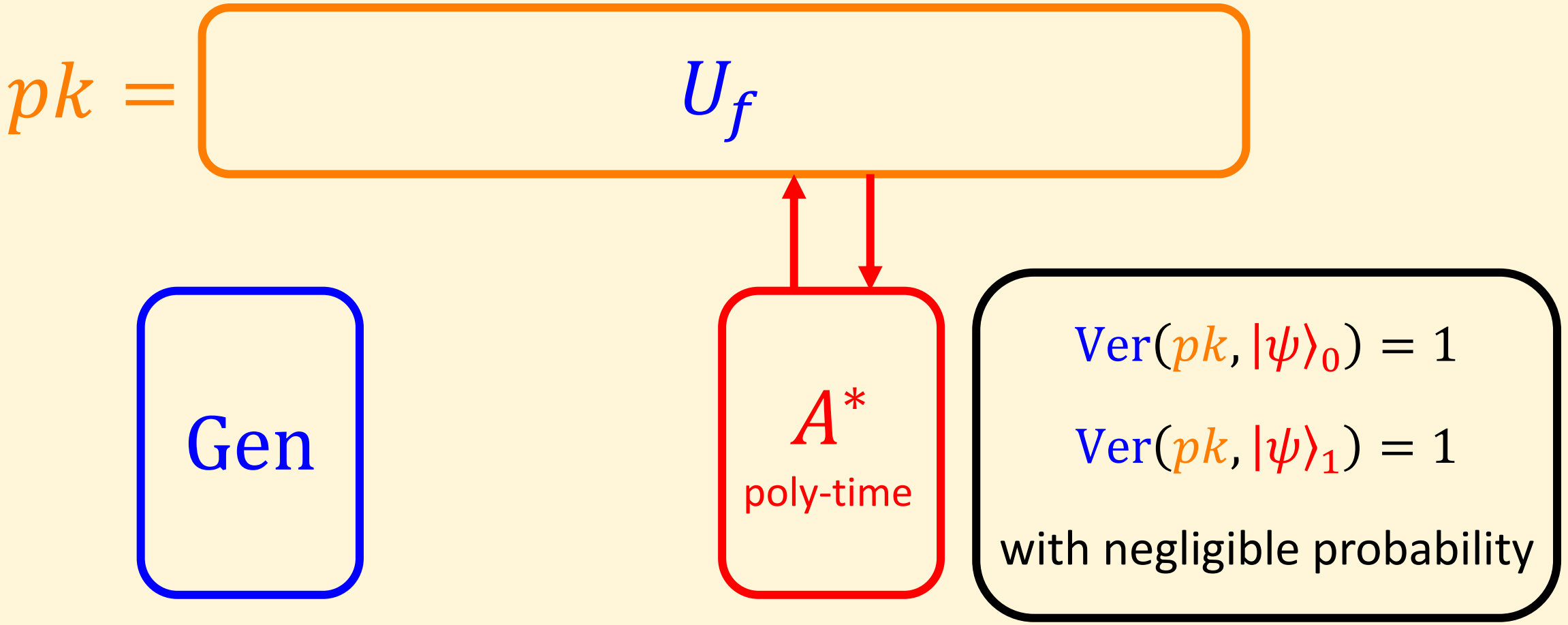
Constructing Public-key Quantum Money



Constructing Public-key Quantum Money



Constructing Public-key Quantum Money



Constructing Public-key Quantum Money

Construction:

- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{pk}$ = Unclonable, even given access to U_f.
- $pk = \mathrm{Obf}_f$ (for now, think of as ideal obfuscation).
- $\mathrm{Ver}(pk, |\phi\rangle)$: $|\psi\rangle_{pk}$ is verifiable given U_f.

Public-key Quantum Money - Intuition

Q: Find $f:\{0,1\}^n \to \{0,1\}$ and $|\psi\rangle_{pk}$ such that: (1) $|\psi\rangle_{pk}$ is verifiable given access to U_f, (2) $|\psi\rangle_{pk}$ stays unclonable given access to U_f.

- Clearly, $|\psi\rangle_{pk}$ cannot be classical (i.e., $|\psi\rangle_{pk} = |x\rangle$ for some specific $x \in \{0,1\}^n$).
- What about very large superpositions?
- Does not necessarily work. For example, Hadamard states $H^{\otimes n} \cdot |x\rangle$, have the largest superposition, but are easily clonable.
- It turns out that if the span of the superposition is both, <u>random</u> and <u>intermediate size</u>, we get an unclonable state.

Public-key Quantum Money - Intuition

Q: Find $f:\{0,1\}^n \to \{0,1\}$ and $|\psi\rangle_{pk}$ such that: (1) $|\psi\rangle_{pk}$ is verifiable given access to U_f, (2) $|\psi\rangle_{pk}$ stays unclonable given access to U_f.

- Pick a random subset $S \subseteq \{0,1\}^n$ of size $2^{\frac{n}{2}}$. Output:

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

- $|S\rangle$ is unclonable.
- Importantly: $|S\rangle$ stays unclonable even given quantum access to membership check in S.

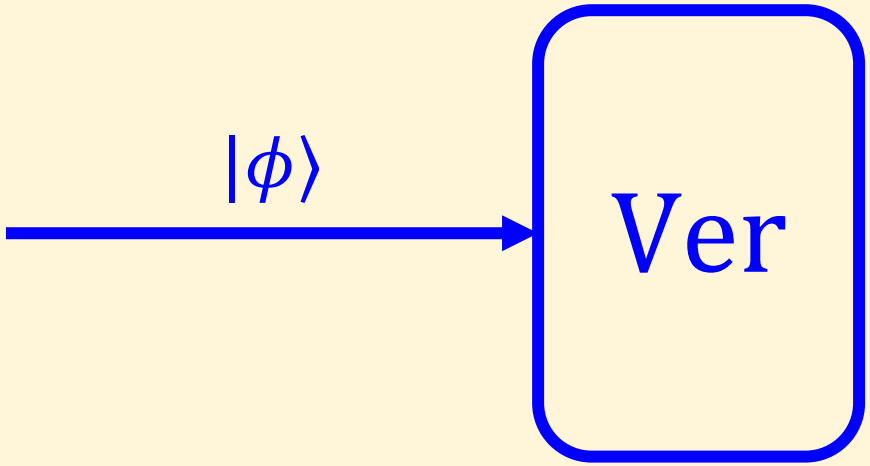
Constructing Public-key Quantum Money

Construction:

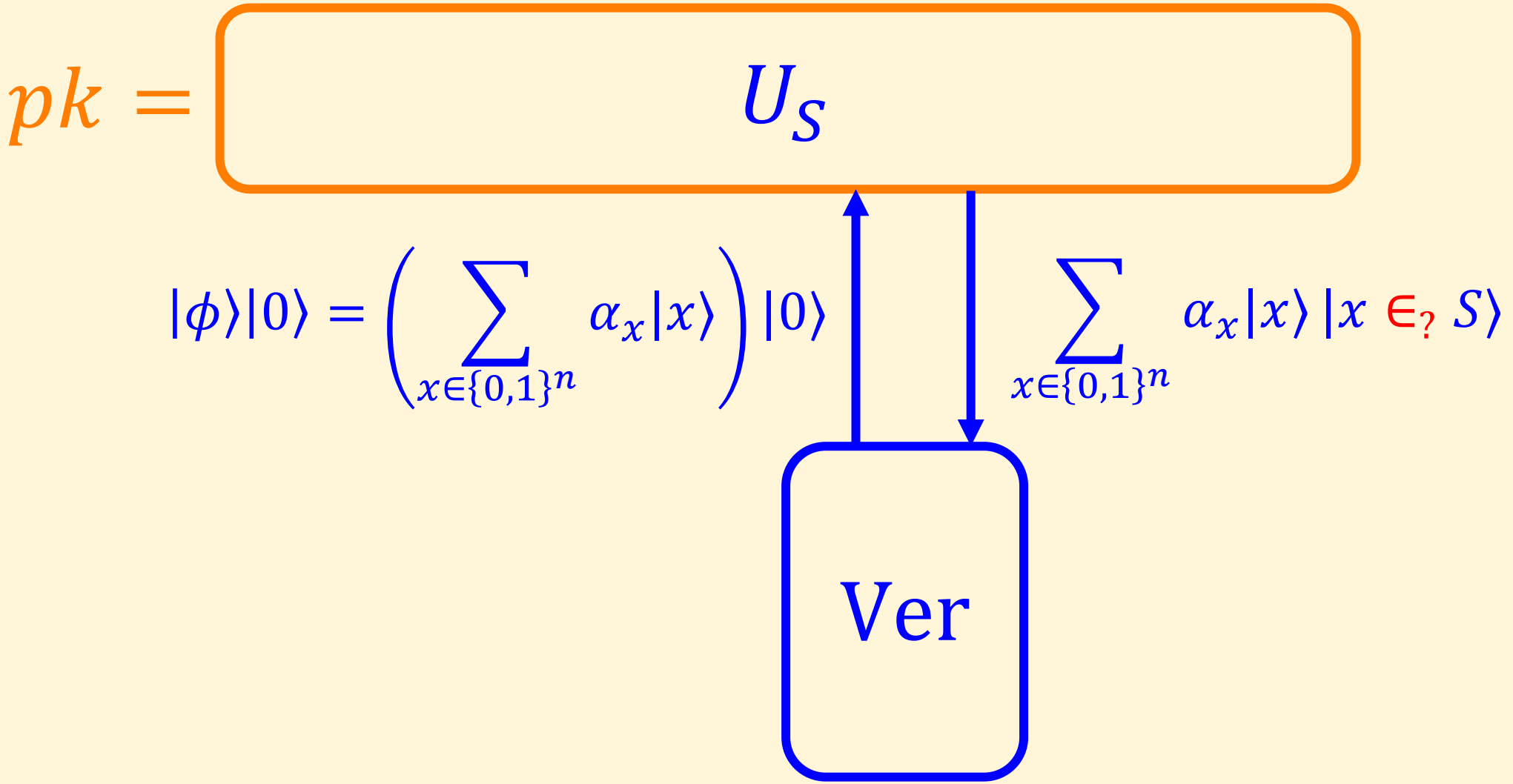
- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{pk} = |S\rangle$, for a random $S \subseteq \{0,1\}^n, |S| = 2^{\frac{n}{2}}$.
- $pk = \mathrm{Obf}_S$ (ideal obfuscation for membership check in S).
- $\mathrm{Ver}(pk, |\phi\rangle)$: ?

Constructing Public-key Quantum Money

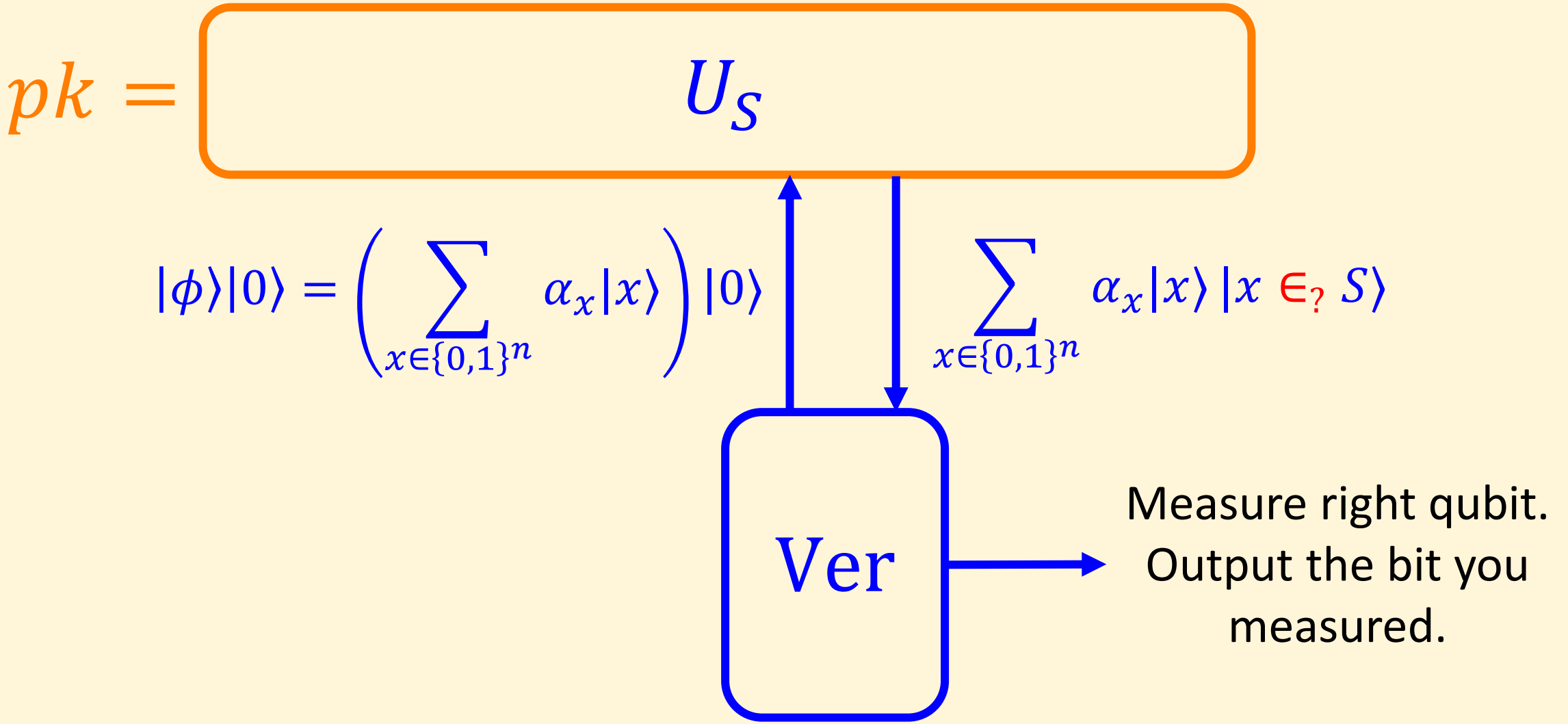
$pk =$ U_S



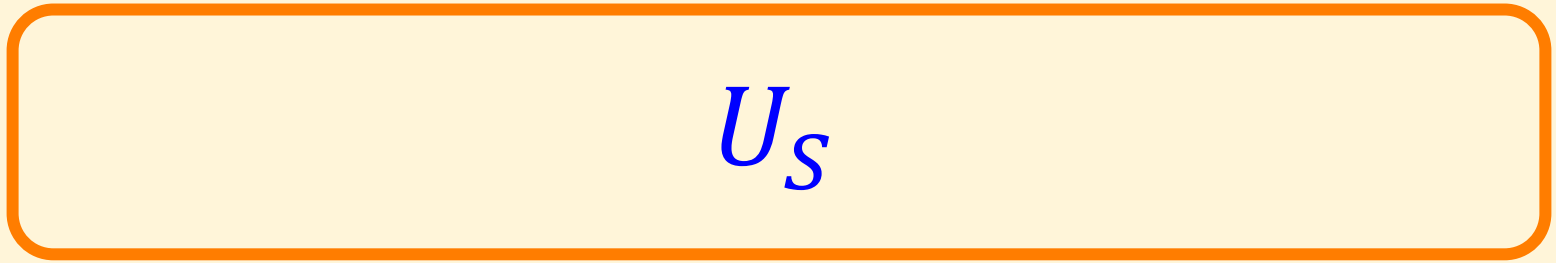
Constructing Public-key Quantum Money

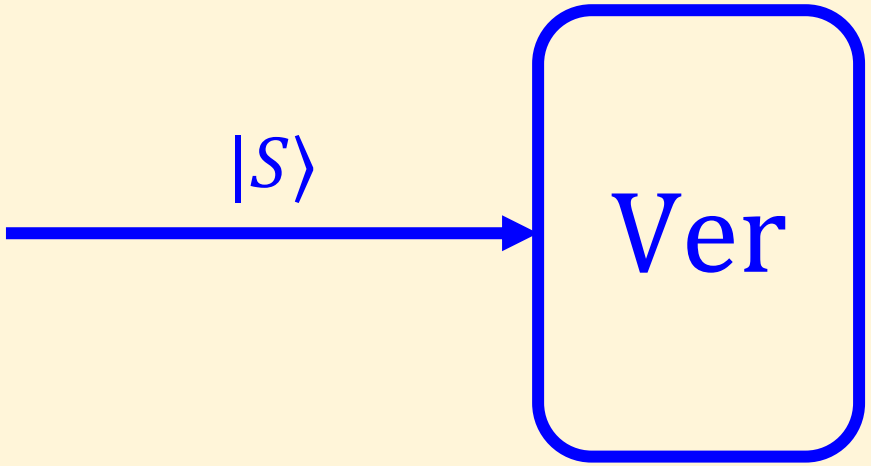


Constructing Public-key Quantum Money

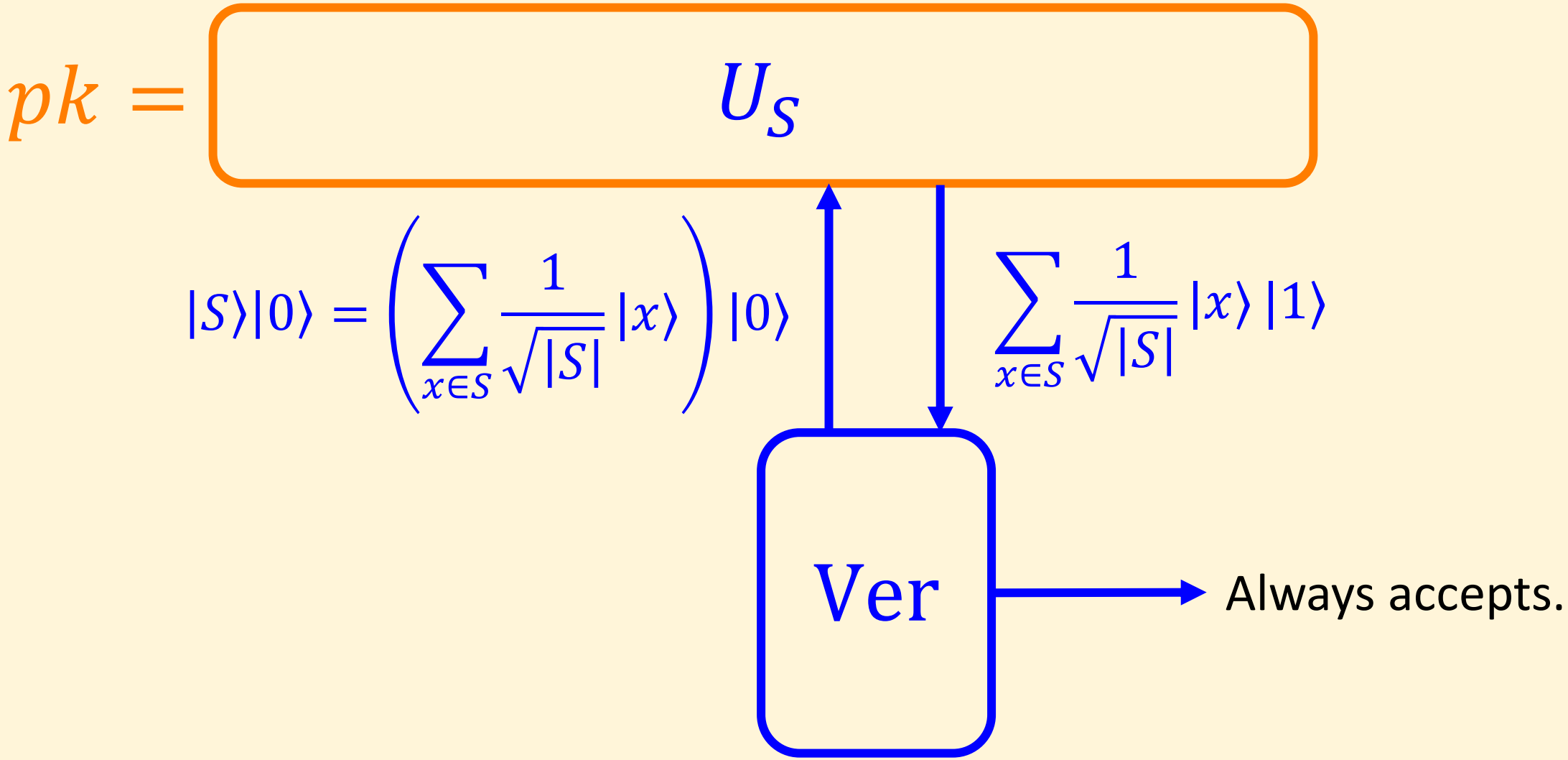


Constructing Public-key Quantum Money

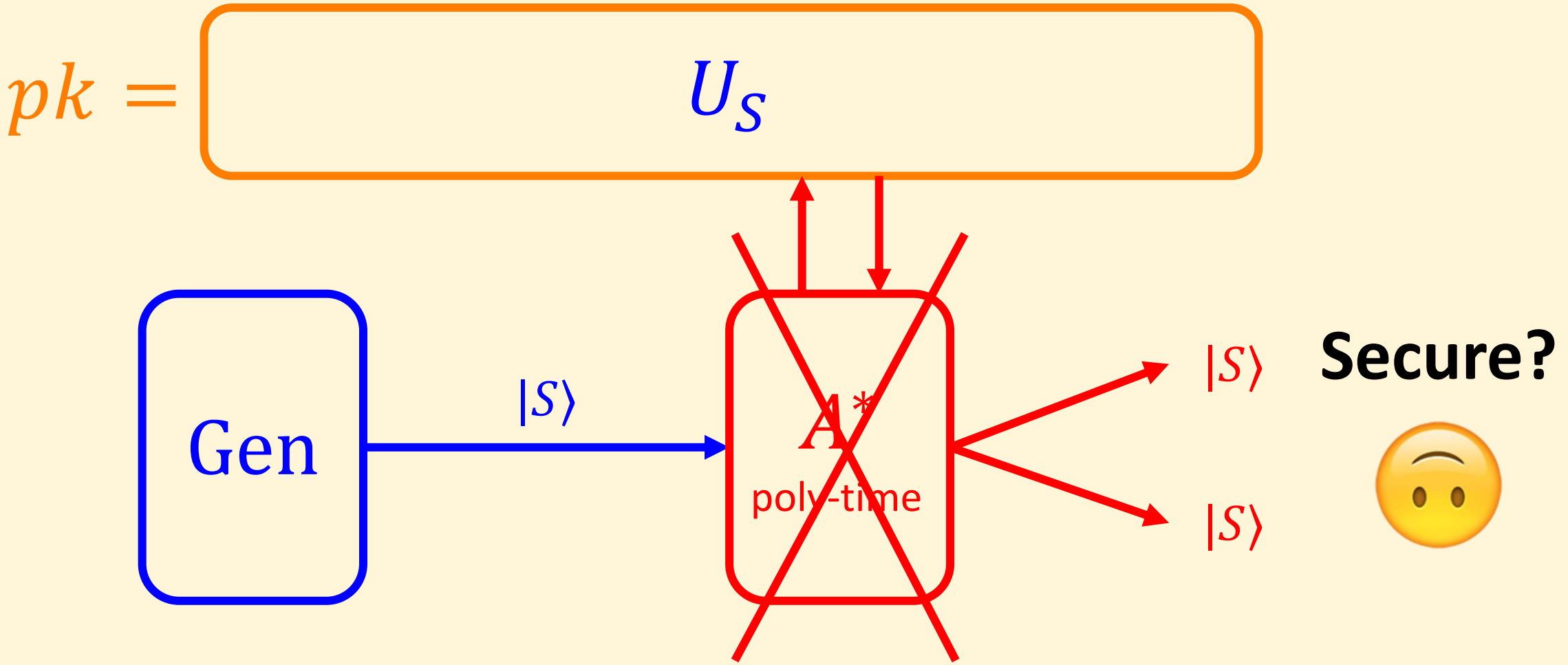
$pk =$ 



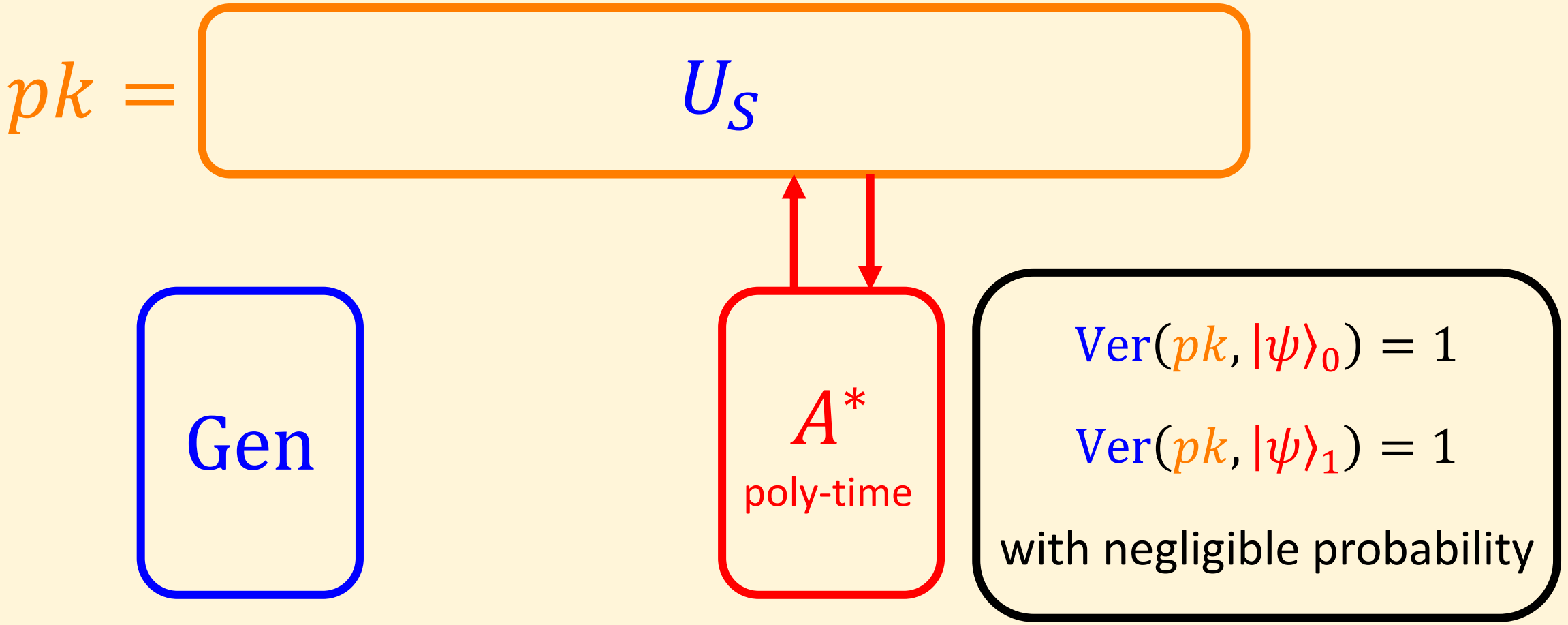
Constructing Public-key Quantum Money



Constructing Public-key Quantum Money



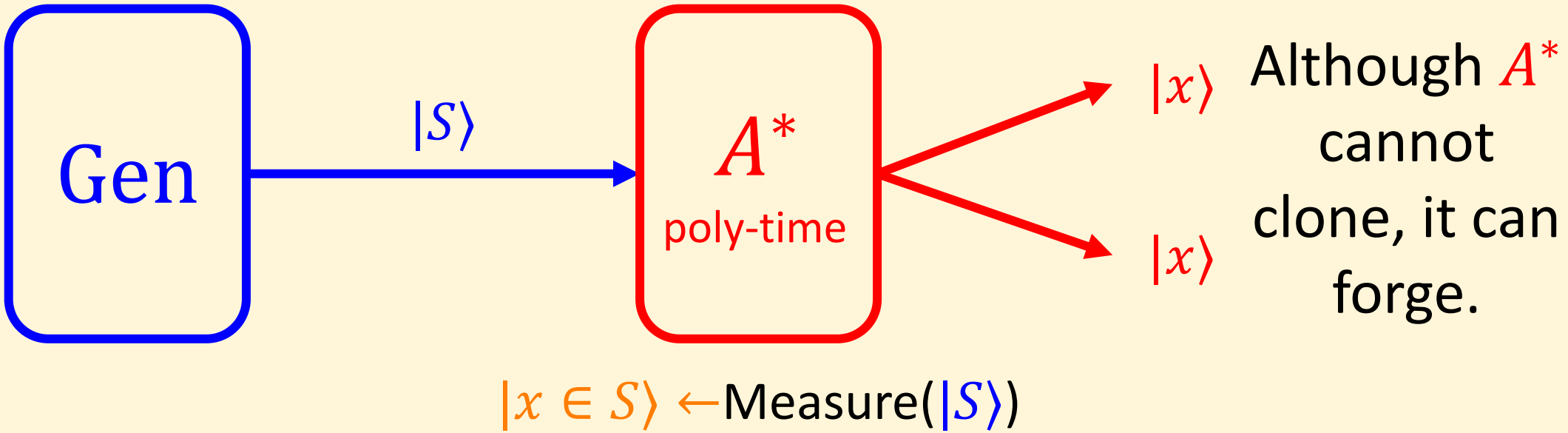
Constructing Public-key Quantum Money



Forging is easier than **Cloning**!

Constructing Public-key Quantum Money

$pk =$ U_S

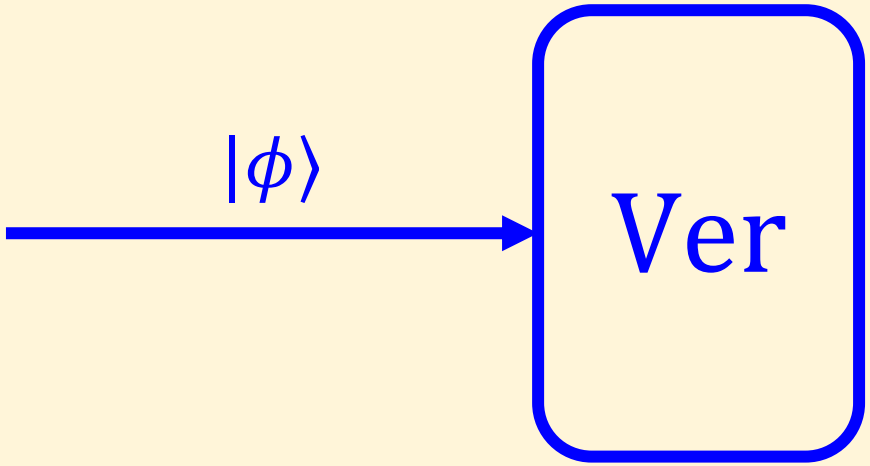


Public-key Quantum Money - Intuition

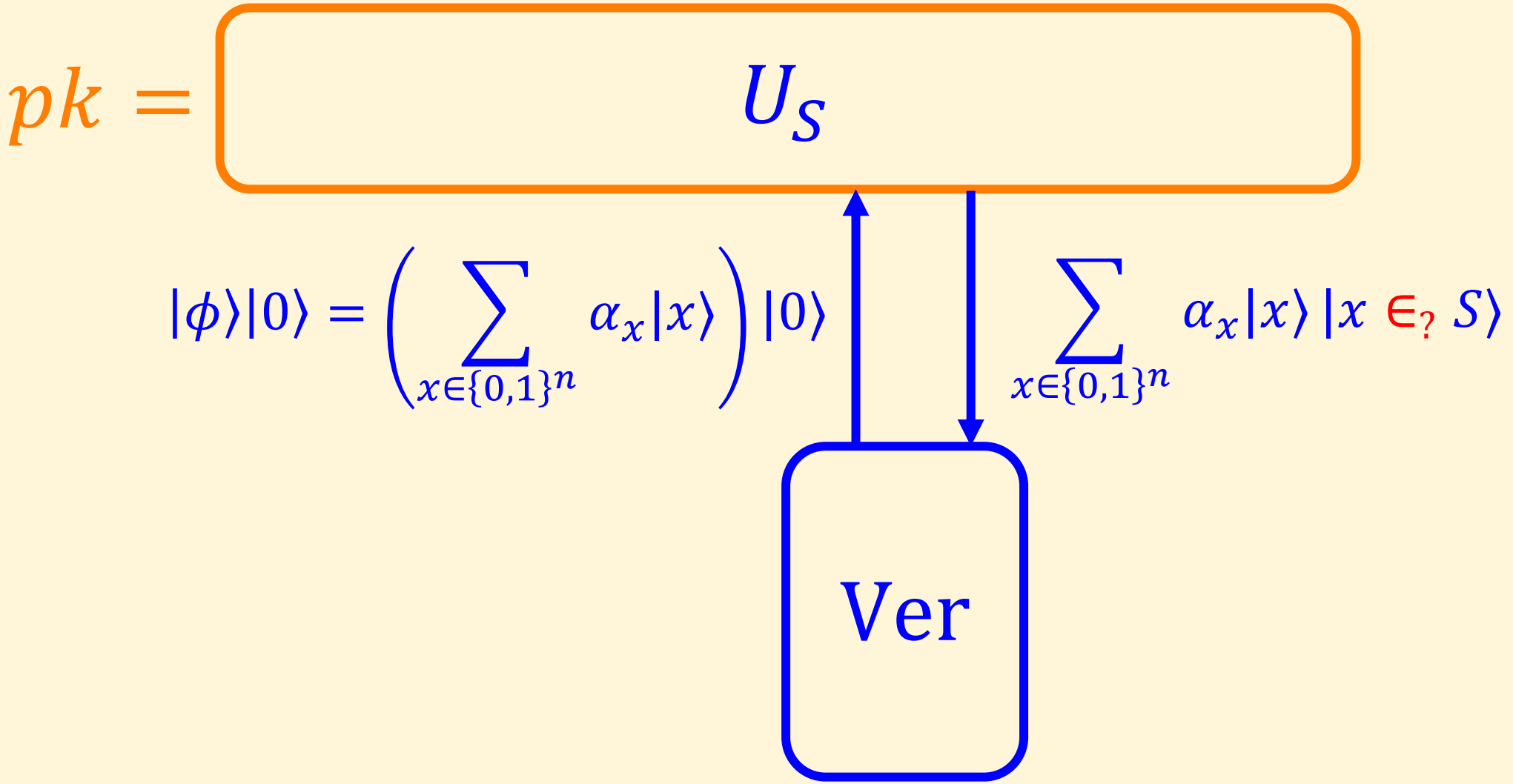
- Although $|\psi\rangle_{pk} = |S\rangle$ was unclonable, the verification could be cheated. Let's focus on improving verification.
- **Q:** What exactly was lacking in Ver?
- **A:** Classical states pass verification. Ver needs to check not only for containment in S, but check for quantumness!
- More concretely, Ver needs to check two things:
  - **Range check:** The superposition $|\phi\rangle$ contains only elements in S.
  - **Quantumness check:** The superposition $|\phi\rangle$ contains many elements in S.
- In the previous scheme, Ver only checked the range.

Public-key Quantum Money - Intuition

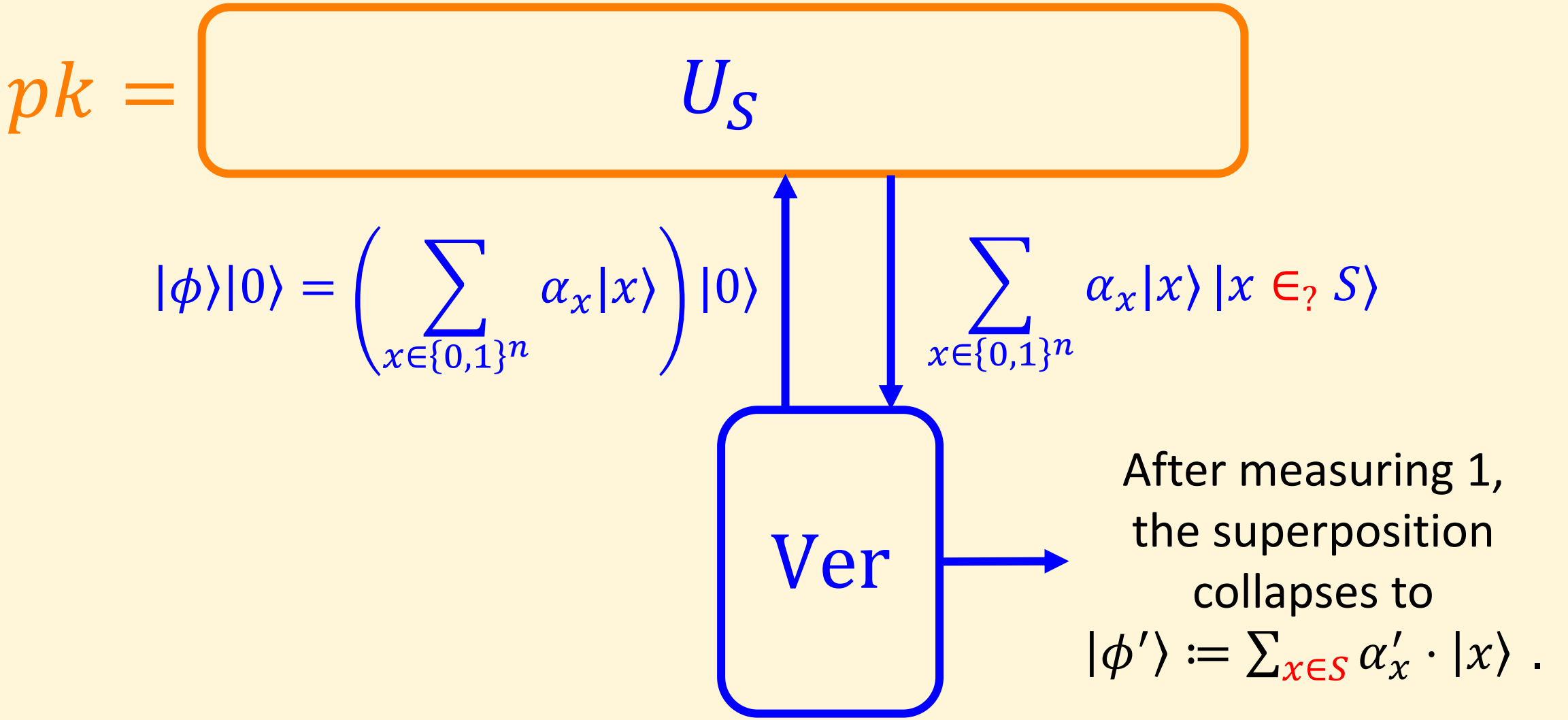
$pk =$ U_S



Public-key Quantum Money - Intuition



Public-key Quantum Money - Intuition



Public-key Quantum Money - Intuition

Q:

Assume you are given a state of the form

$|\phi\rangle := \sum_{x \in S} \alpha_x \cdot |x\rangle$, for some $S \subseteq \{0,1\}^n$.

Can you check, in quantum polynomial-time, that the state is non-classical? (i.e., that it is not the case that $\alpha_x = 1$ for some $x \in S$).

A:

If S is a subspace, then yes!

Constructing Public-key Quantum Money

Definition [Subspace State]:
Let $n \in \mathbb{N}$ and let $S \subseteq \{0,1\}^n$ a subspace of $\{0,1\}^n$. The subspace state of S is defined as

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

Constructing Public-key Quantum Money

Definition [Dual Subspace]:
Let $n \in \mathbb{N}$ and let $S \subseteq \{0,1\}^n$ a subspace of $\{0,1\}^n$. The dual subspace of S, denoted $S^{\perp}$, is defined as the subspace of $\{0,1\}^n$ such that

$$S^{\perp} \coloneqq \{x \in \{0,1\}^n \mid \forall y \in S : \langle x, y \rangle = 0\}.$$

Constructing Public-key Quantum Money

Lemma [Quantum Fourier Transform of a Subspace State]:
Let $n \in \mathbb{N}$ and let $S \subseteq \{0,1\}^n$ a subspace of $\{0,1\}^n$. Then,

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

Proof: By Calculation.

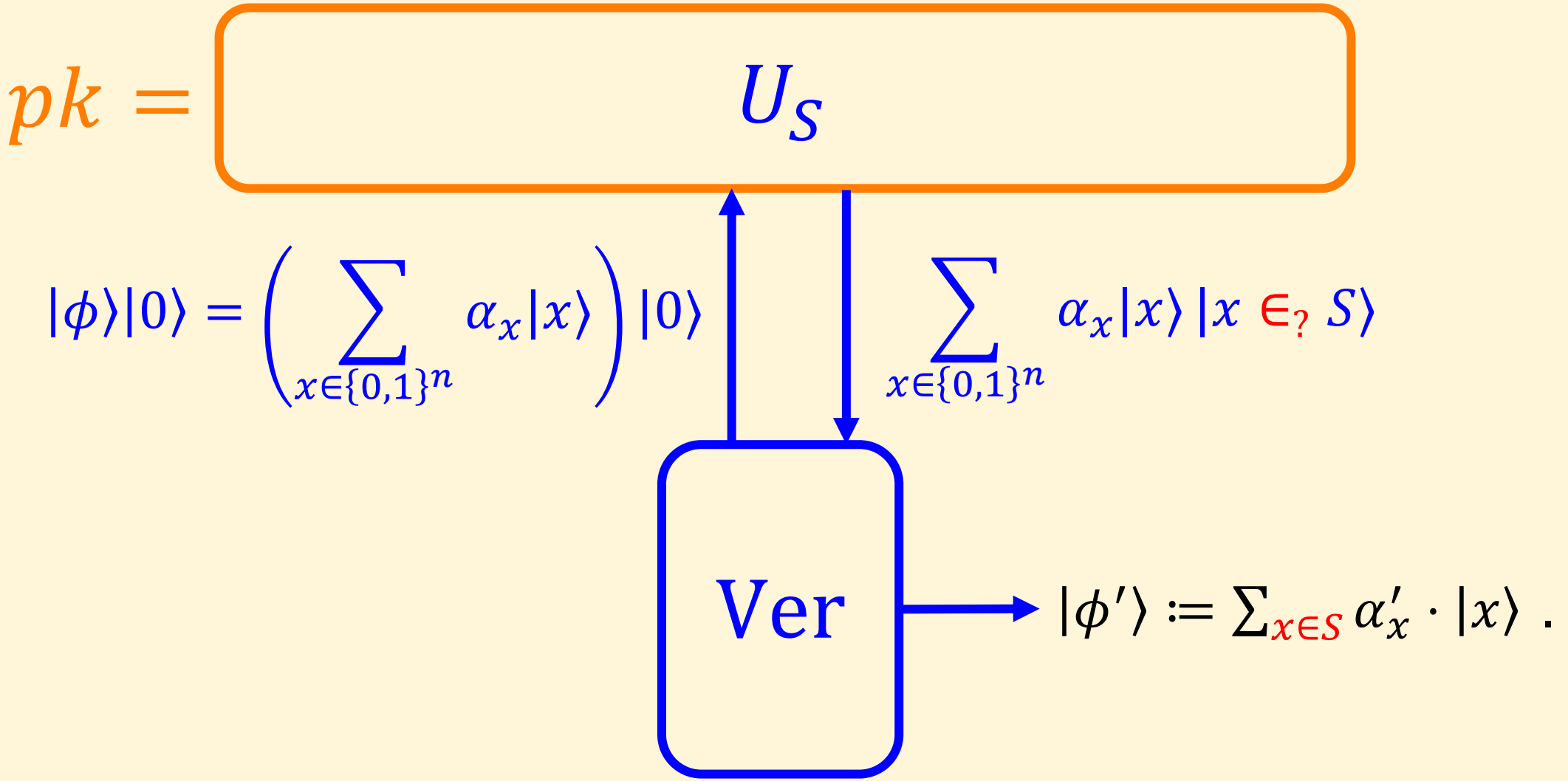
Constructing Public-key Quantum Money

Lemma [Quantum Fourier Transform of a Subspace State]:
Let $n \in \mathbb{N}$ and let $S \subseteq \{0,1\}^n$ a subspace of $\{0,1\}^n$. Then,

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

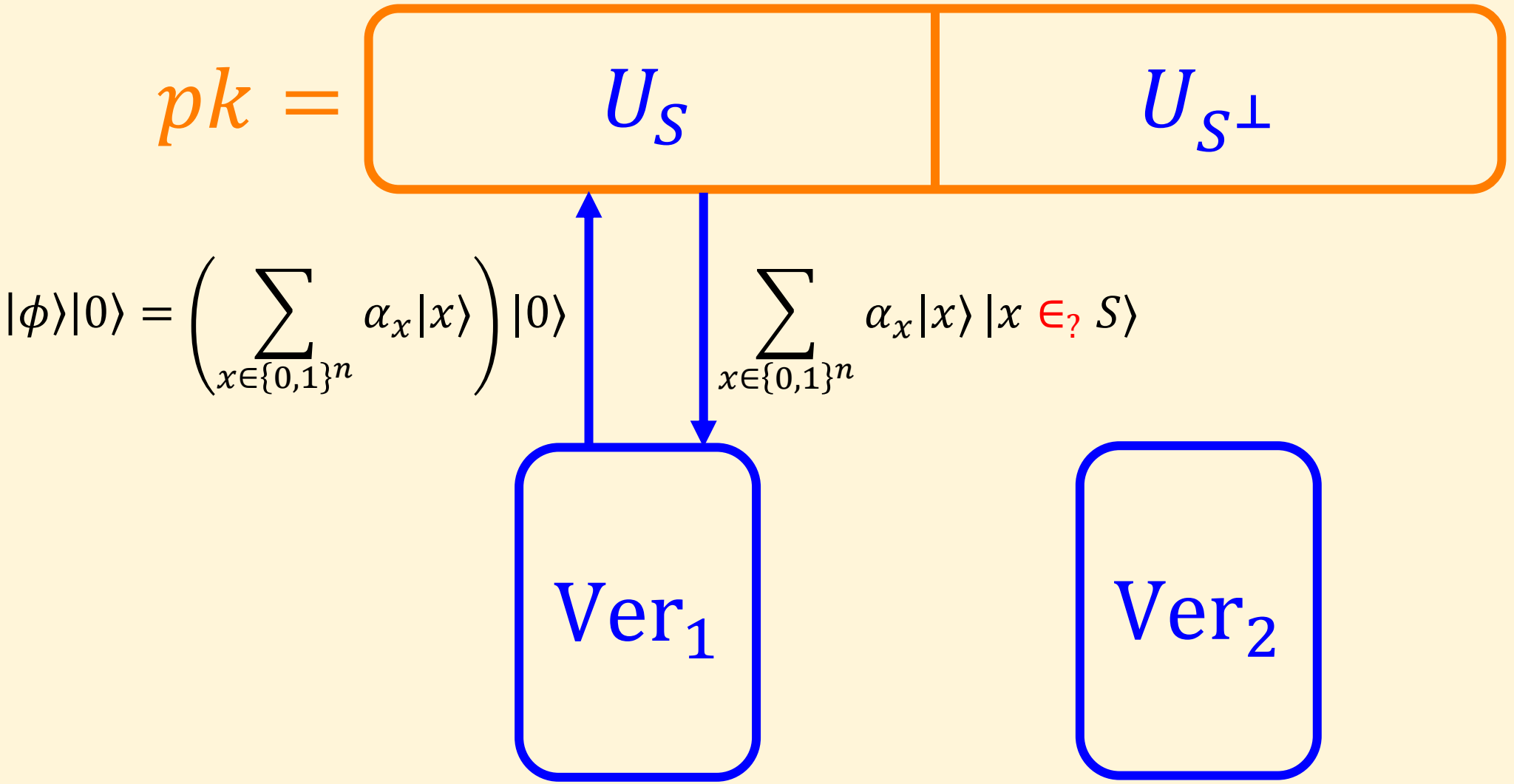
Q: Consider two scenarios, D_0 and D_1. Assume you know S.
D_0: You are given a $|x\rangle$ for $x \in S$.
D_1: You are given $|S\rangle$.
Distinguish between D_0 and D_1. **Hint 1:** What happens after $H^{\otimes n}$?
Hint 2: $H^{\otimes n}|x\rangle$ is a uniform superposition, and from the above we have $H^{\otimes n}|S\rangle = |S^{\perp}\rangle$. Inside a subspace, the <u>wider</u> the superposition, the <u>narrower</u> its $H^{\otimes n}$ transform will be.

Constructing Public-key Quantum Money

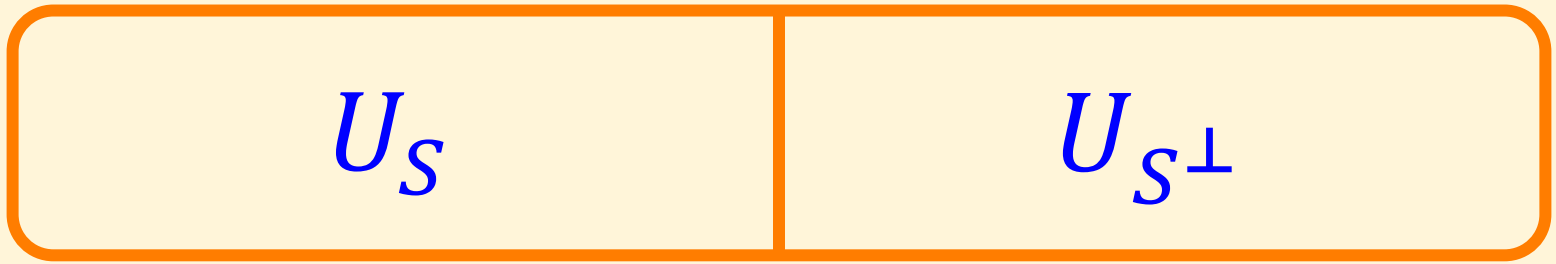


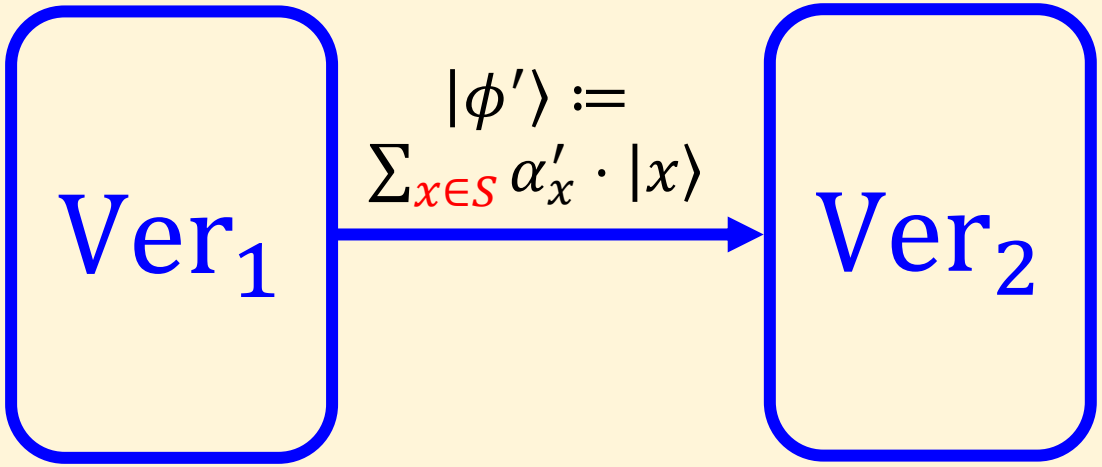
Constructing Public-key Quantum Money

Constructing Public-key Quantum Money



Constructing Public-key Quantum Money

$pk =$ 



Constructing Public-key Quantum Money

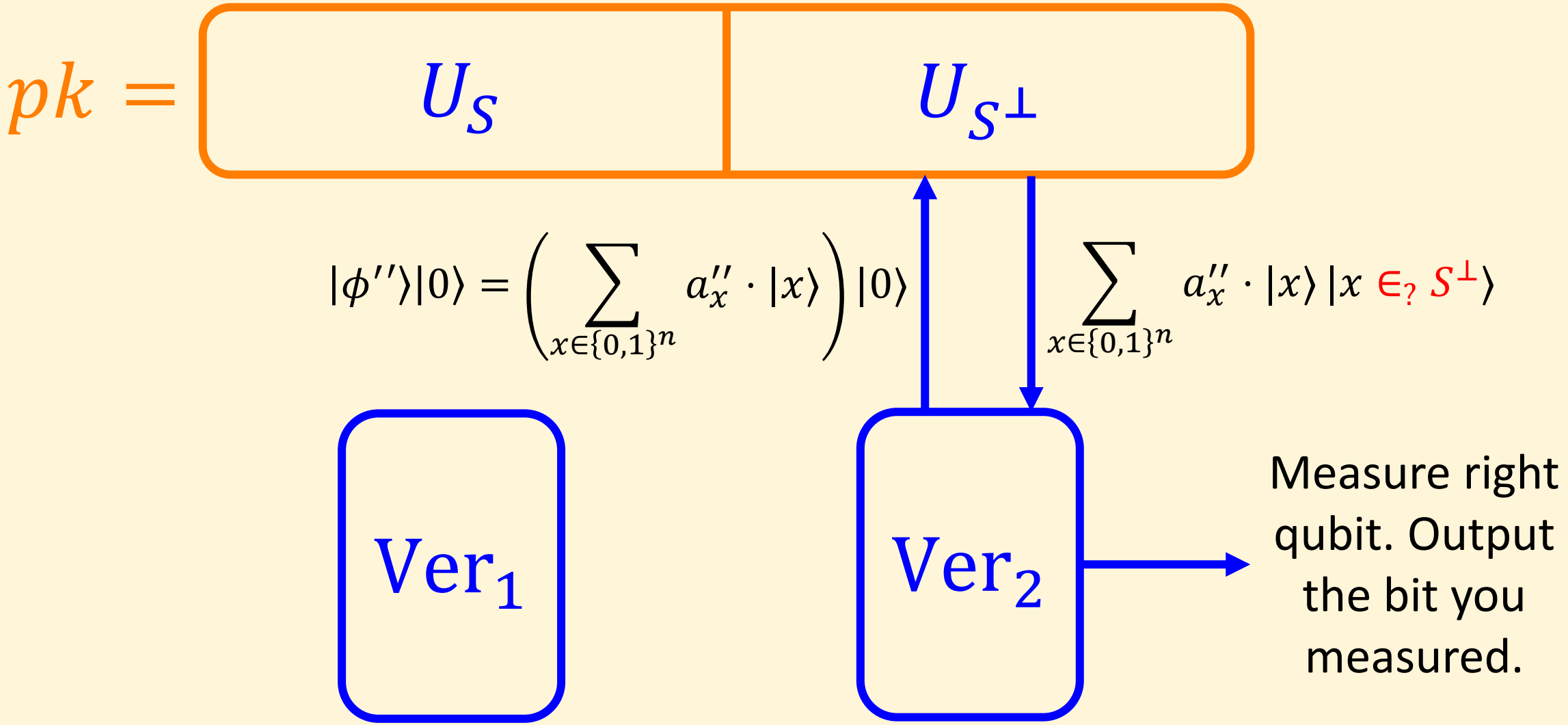
Compute:

$H^{\otimes n}|\phi'\rangle = |\phi''\rangle$

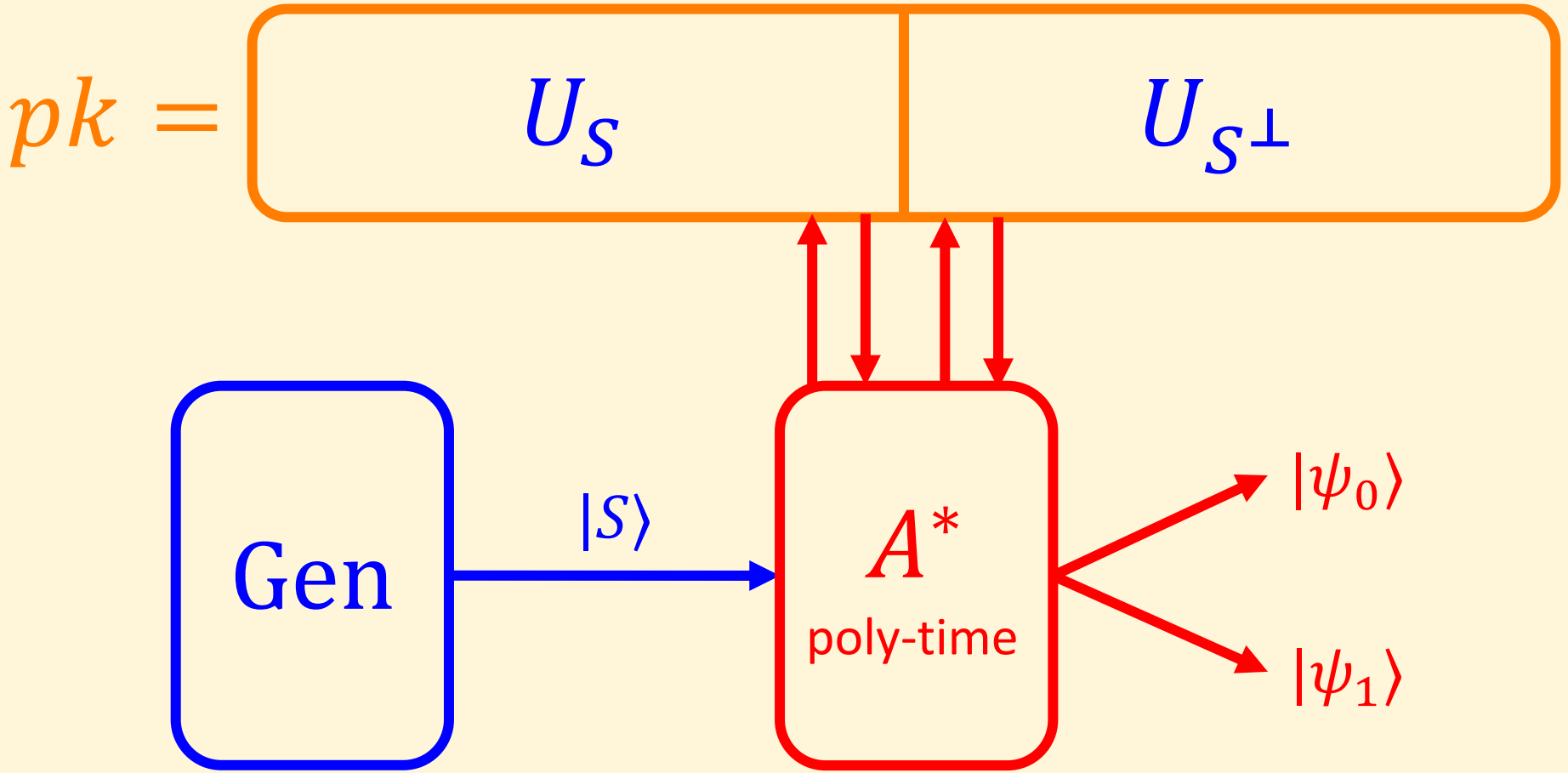
Ver_1

Ver_2

Constructing Public-key Quantum Money

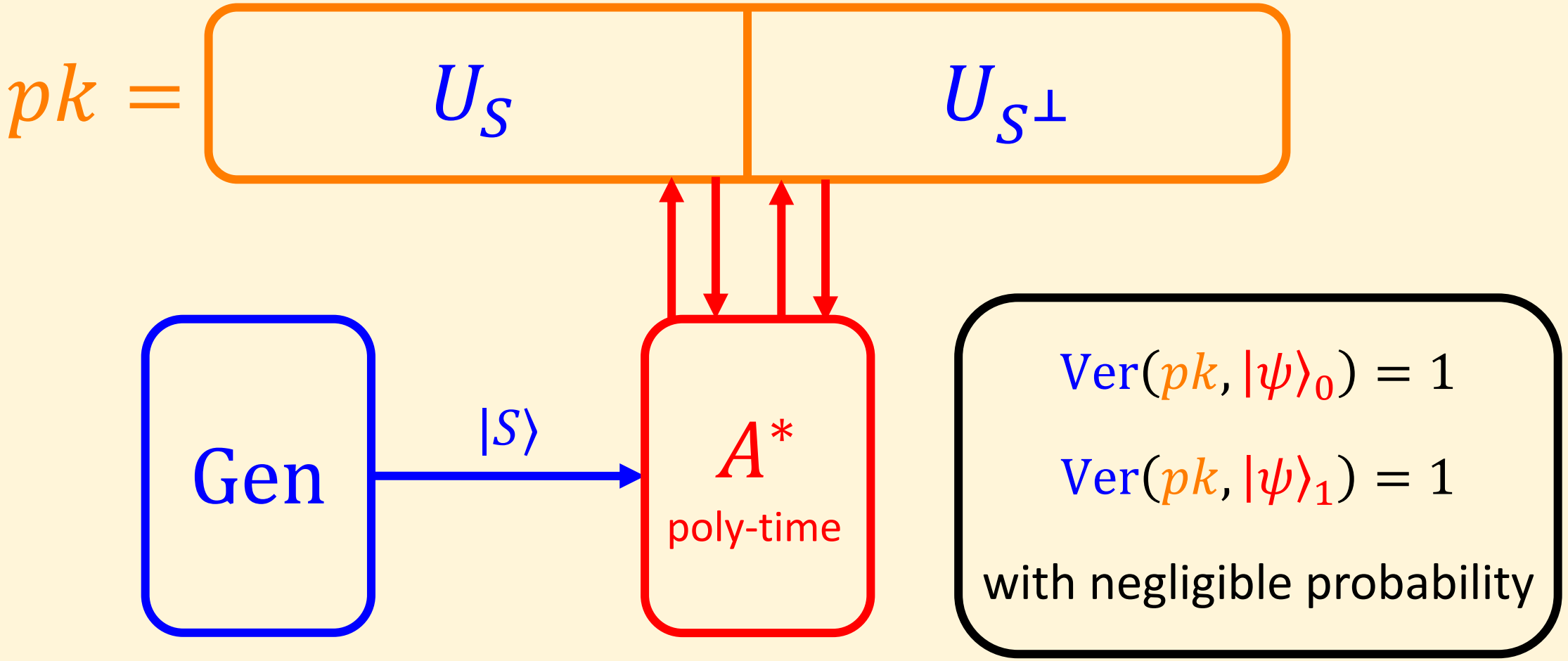


Constructing Public-key Quantum Money



Theorem (Aaronson-Christiano-2012, Theorem 25):

Constructing Public-key Quantum Money



Theorem (Aaronson-Christiano-2012, Theorem 25):

Public-key Quantum Money - Construction

Construction [Aaronson-Christiano-2012]:

- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{pk} = |S\rangle$, for a random subspace $S \subseteq \{0,1\}^n, |S| = 2^{\frac{n}{2}}$.
- $pk = (\mathrm{Obf}_S, \mathrm{Obf}_{S^\perp})$ (Idealized obfuscation).
- $\mathrm{Ver}(pk, |\phi\rangle)$:
  - First, check that the rightmost qubit of $U_S(|\phi\rangle|0\rangle)$ is 1.
  - Now the state is $|\phi'\rangle := \sum_{x\in S} \alpha'_x \cdot |x\rangle$. Apply $H^{\otimes n} \cdot |\phi'\rangle = |\phi''\rangle$.
  - Finally, check that the rightmost qubit of $U_{S^\perp}(|\phi''\rangle|0\rangle)$ is 1.

PKQM in the Standard Model

- The [A-C-2012] construction is secure only with respect to an oracle.
- We want a construction in the plain model, under computational assumptions.
- It was shown by [Zhandry-2018] that the scheme can stay as is, and it is secure in the standard model. Formally:

PKQM in the Standard Model

Construction [Aaronson-Christiano-2012] + [Zhandry-2018]:

- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{pk} = |S\rangle$, for a random subspace $S \subseteq \{0,1\}^n, |S| = 2^{\frac{n}{2}}$.
- $pk = (\mathrm{Obf}_S, \mathrm{Obf}_{S^\perp})$ (Can we obfuscate using iO?).
- $\mathrm{Ver}(pk, |\phi\rangle)$:
  - First, check that the rightmost qubit of $U_S(|\phi\rangle|0\rangle)$ is 1.
  - Now the state is $|\phi'\rangle := \sum_{x\in S} \alpha'_x \cdot |x\rangle$. Apply $H^{\otimes n} \cdot |\phi'\rangle = |\phi''\rangle$.
  - Finally, check that the rightmost qubit of $U_{S^\perp}(|\phi''\rangle|0\rangle)$ is 1.

PKQM in the Standard Model

Theorem (Subspace-hiding Obfuscation) [Zhandry-2018, Theorem 6.3]:

Assume,

- Quantum-secure iO exists (for classical circuits), and
- Quantum-secure injective OWFs exist.

Then, for every subspace $S \subseteq \{0,1\}^n$ with $\dim(S) = \frac{n}{2}$,

the following distributions are indistinguishable:

$$\{\mathrm{O}_S | \mathrm{O}_S \leftarrow \mathrm{iO}(C_S)\} \ ,$$

$$\left\{\mathrm{O}_T \,\middle|\, T \leftarrow \left(S \subseteq T, \dim(T) = \frac{3n}{4}\right) \ , \ \mathrm{O}_T \leftarrow \mathrm{iO}(C_T)\right\} \ .$$

PKQM in the Standard Model

Lemma (Hardness of Cloning Reduced-Entropy Subspace States) [Zhandry-2018, Section 6.2]:

Let $T_0, T_1 \subseteq \{0,1\}^n$ subspaces with $\dim(T_0) = \frac{3n}{4}$, $\dim(T_1) = \frac{n}{4}$, and $T_1 \subseteq T_0$.

Let $T_1 \subseteq S \subseteq T_0$ a uniformly random subspace with $\dim(S) = \frac{n}{2}$.

$$\forall A^*: \Pr_{(|S\rangle)\leftarrow \mathrm{Gen}(1^n)}[A^*(|S\rangle) = |S\rangle|S\rangle] \leq 2^{-\Omega(n)}.$$

PKQM in the Standard Model

Lemma (Dual Check is Projective) [A-C-2012, Lemma 21]:

After a successful state verification in the [A-C-2012] PKQM, the state collapses to the money state $|\psi\rangle_{pk} = |S\rangle$.

PKQM in the Standard Model

Theorem (Security of the [A-C-2012] construction in the standard model) [Zhandry-2018, Corollary 6.6]:

Assume,

- Quantum-secure iO exists (for classical circuits), and
- Quantum-secure injective OWFs exist.

Then, quantum-secure iO can be used to obfuscate the circuits $C_S, C_{S^\perp}$ from the [A-C-2012], and the scheme is secure in the standard model.

PKQM in the Standard Model

Proof sketch:

In each of the following hybrids except the last, we can assume to have $S, S^{\perp}$, so we check at the end whether state passed verification.

- Hyb_0 : The standard security game, the adversary A gets O_S, $\mathrm{O}_{S^{\perp}}$ and $|S\rangle$ and succeeds in forging with noticeable probability.
- Hyb_1 : Use subspace-hiding to move from O_S to O_{T_0} for a random T_0 with dimension $\frac{3n}{4}$.

PKQM in the Standard Model

Proof sketch:

- Hyb_2 : Use subspace-hiding to move from $\mathrm{O}_{S^\perp}$ to $\mathrm{O}_{T_1^\perp}$ for a random $T_1^\perp$ with dimension $\frac{3n}{4}$.
- Note: $T_1 \subseteq S \subseteq T_0$, and $\dim(T_0) = \frac{3n}{4}$, $\dim(T_1) = \dim\left(\left(T_1^\perp\right)^\perp\right) = \frac{n}{4}$.
- Hyb_3 : Swap the order of sampling T_1, S, T_0. First sample T_1, T_0, and then sample S conditioned on $T_1 \subseteq S \subseteq T_0$. Distributes identically to Hyb_2 .

PKQM in the Standard Model

Proof sketch:

Conclude with the following observations.

- The dual check is projective. Until now we can assume access to $S, S^{\perp}$, and we project on $|S\rangle$ after a successful forgery.
- This means that at the end of Hyb_3, the adversary clones $|S\rangle$ with a non-negligible probability.
- We can fix, by an averaging argument the subspaces T_0, T_1 and not S.
- The subspace S is a random subspace of dimension $\frac{n}{2}$, conditioned on $T_1 \subseteq S \subseteq T_0$. According to the hardness of reduced-entropy cloning, it is impossible to clone $|S\rangle$.

■

PKQM in the Standard Model

Construction [Aaronson-Christiano-2012] + [Zhandry-2018]:

- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{pk} = |S\rangle$, for a random subspace $S \subseteq \{0,1\}^n, |S| = 2^{\frac{n}{2}}$.
- $pk = (\mathrm{Obf}_S, \mathrm{Obf}_{S^\perp})$ (Obfuscated using iO).
- $\mathrm{Ver}(pk, |\phi\rangle)$:
  - First, check that the rightmost qubit of $U_S(|\phi\rangle|0\rangle)$ is 1.
  - Now the state is $|\phi'\rangle := \sum_{x\in S} \alpha'_x \cdot |x\rangle$. Apply $H^{\otimes n} \cdot |\phi'\rangle = |\phi''\rangle$.
  - Finally, check that the rightmost qubit of $U_{S^\perp}(|\phi''\rangle|0\rangle)$ is 1.