Quantum Money

(and what it really captures)

Part II

Omri Shmueli

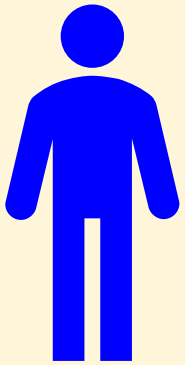
Warsaw IACR Summer School on Post-quantum Cryptography 2024

Talk Plan – 2nd Part

- The quantum delivery verification problem.
- Tokenized signatures.
  - Coset states and classical proofs of quantum information deletion.
- Semi-quantum money.
  - Classical delegation of unclonable state generation (technical).

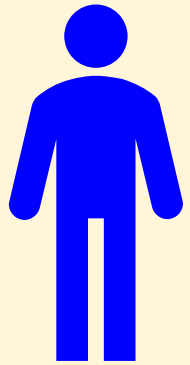
The Quantum Delivery Verification Problem

pk



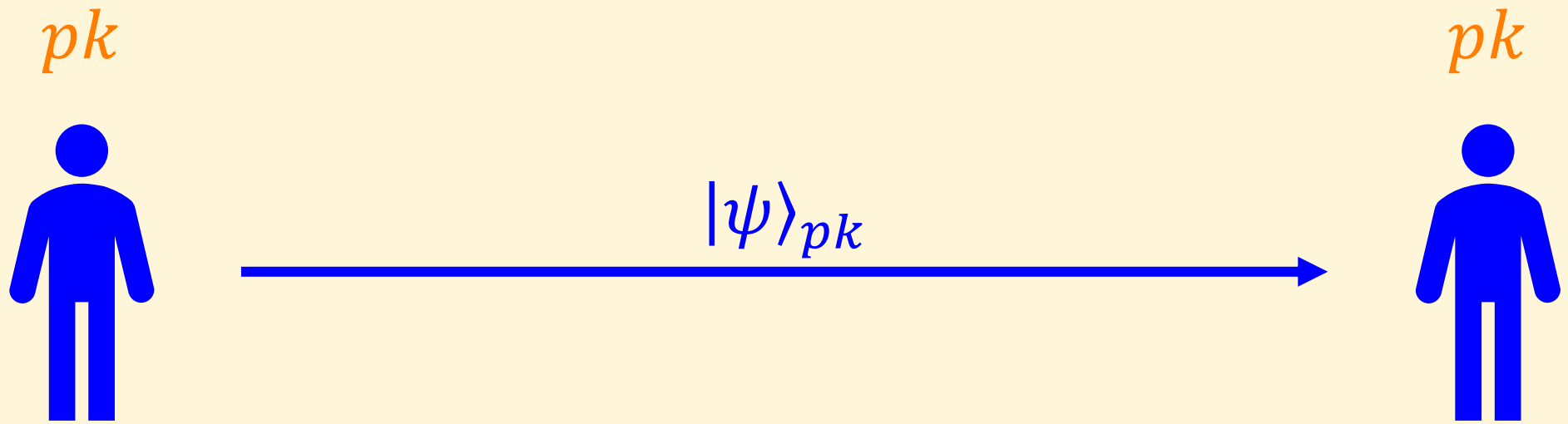
$|\psi\rangle_{pk}$

pk



Scenario I

The Quantum Delivery Verification Problem



Scenario I

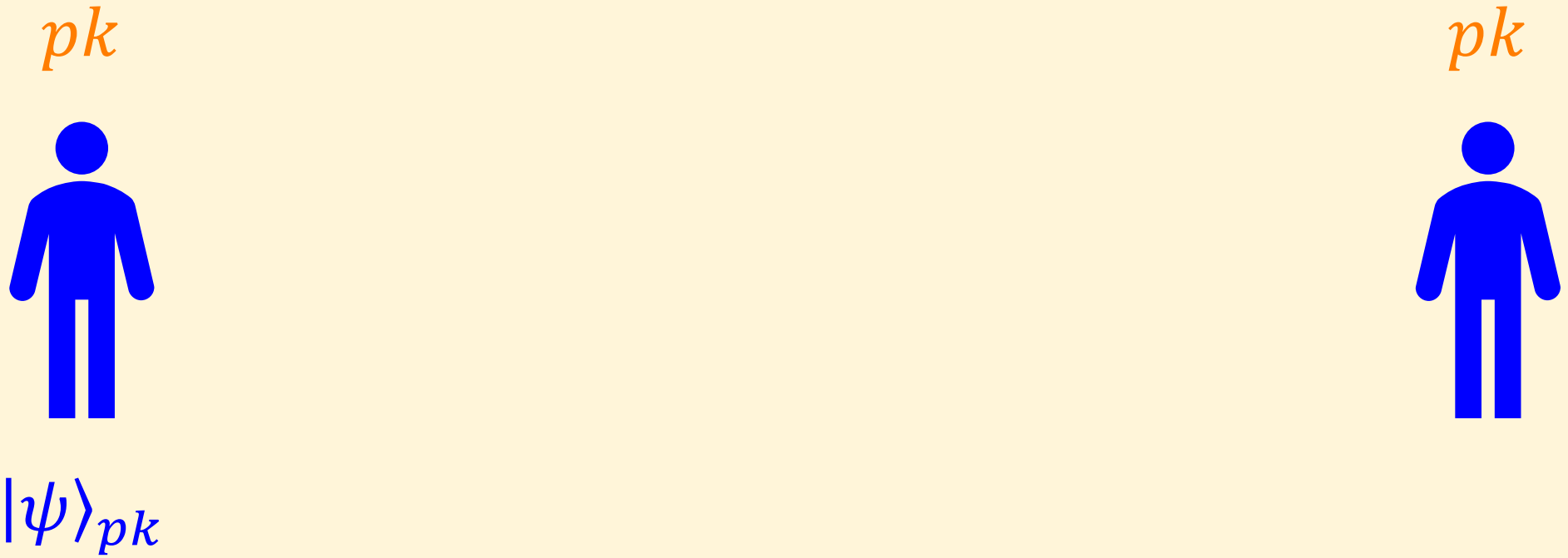
The Quantum Delivery Verification Problem

Scenario I

The Quantum Delivery Verification Problem

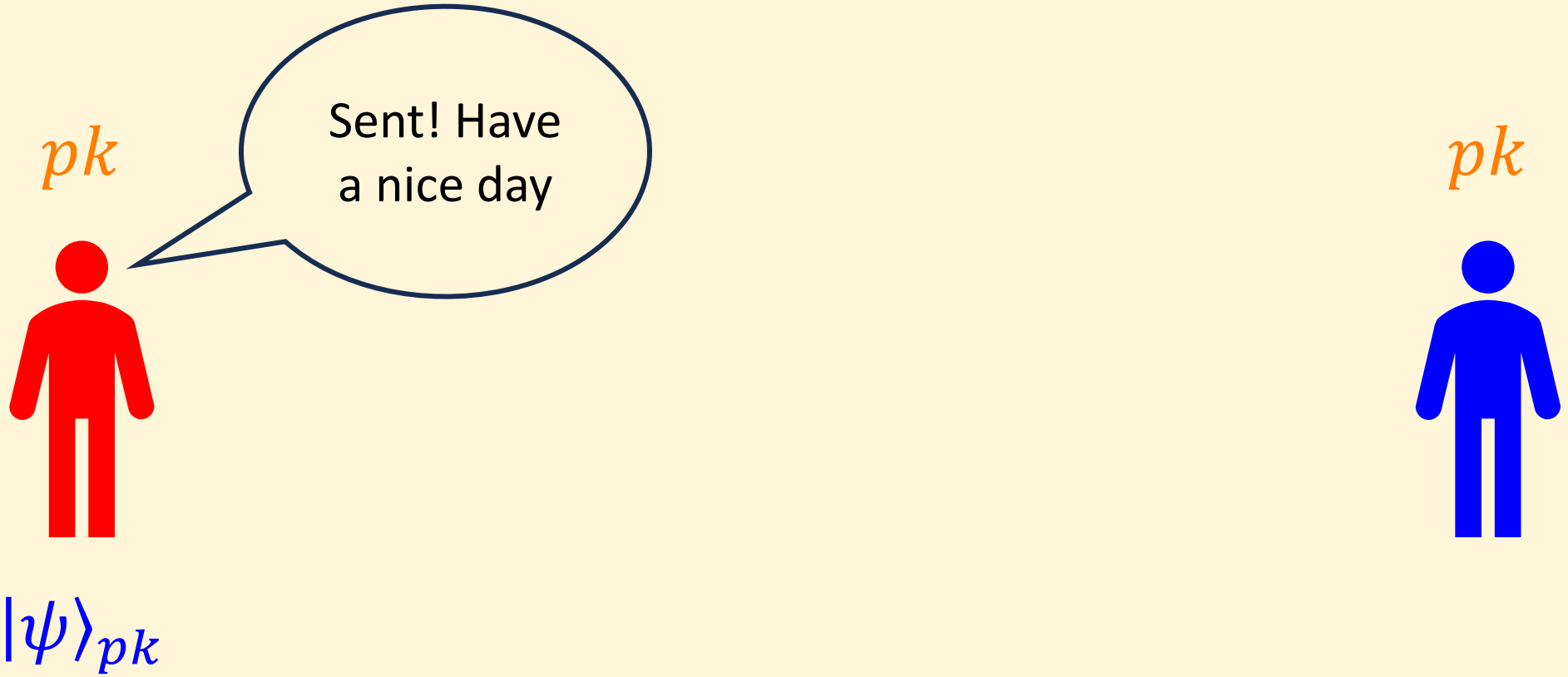
Scenario I

The Quantum Delivery Verification Problem



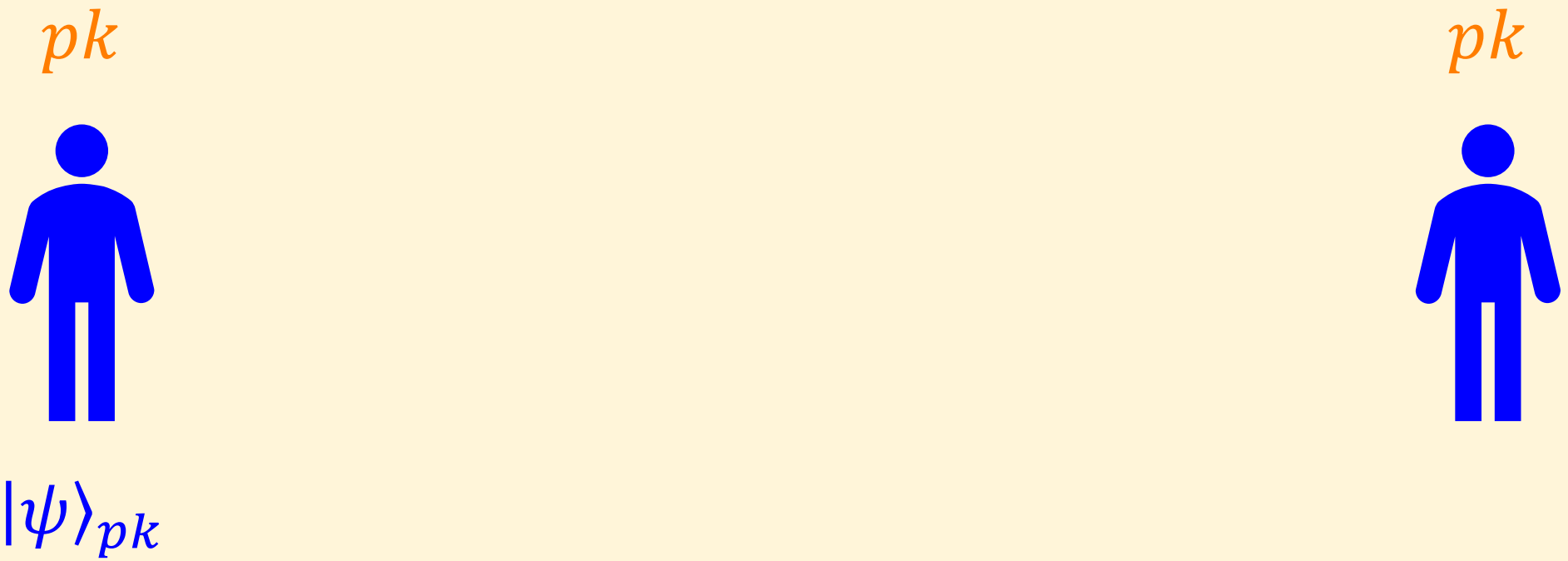
Scenario II

The Quantum Delivery Verification Problem



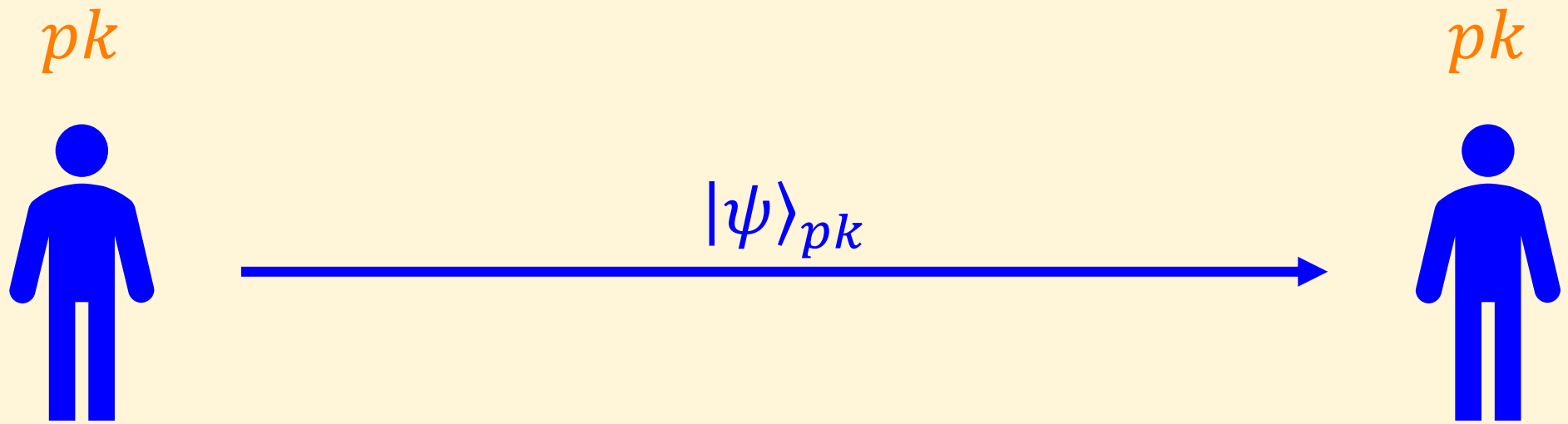
Scenario II

The Quantum Delivery Verification Problem



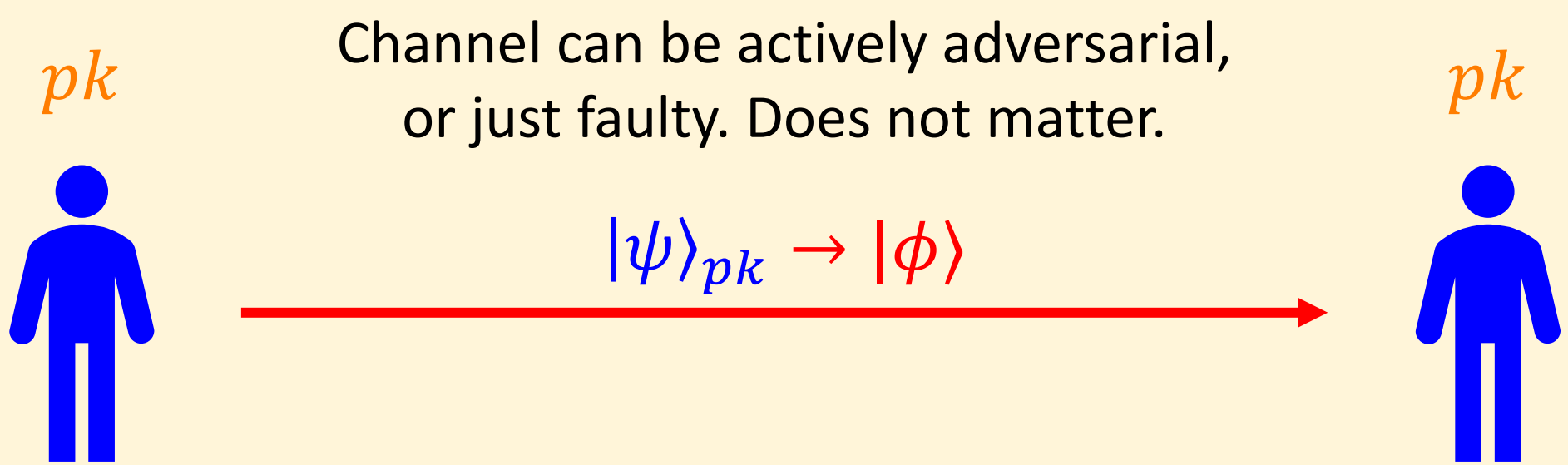
Scenario III

The Quantum Delivery Verification Problem



Scenario III

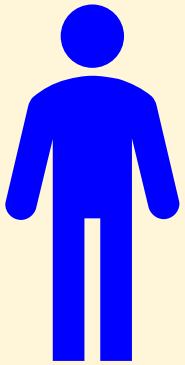
The Quantum Delivery Verification Problem



Scenario III

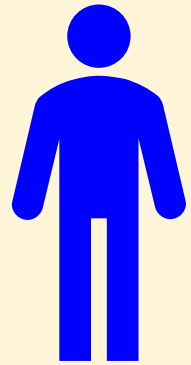
The Quantum Delivery Verification Problem

pk



Quantum state was unclonable and is now destroyed.
We cannot try sending again.

pk



$|\phi\rangle$

Scenario III

The Quantum Delivery Verification Problem

Q:

How can you guarantee & prove that you have sent an unclonable quantum state (to some given destination)?

Tokenized Signatures

Tokenized Signatures

[Ben-David-Sattath-2016]

Definition [Tokenized Signatures Scheme] :

Given by three polynomial-time quantum algorithms, and one classical algorithm,

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

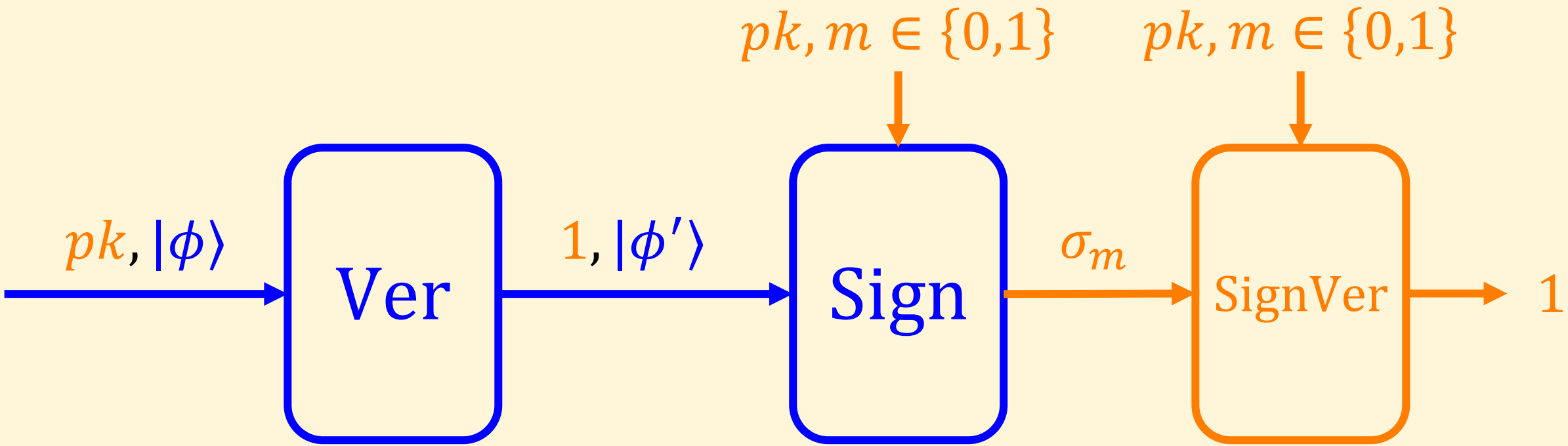
Tokenized Signatures

- **Correctness 1:**

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

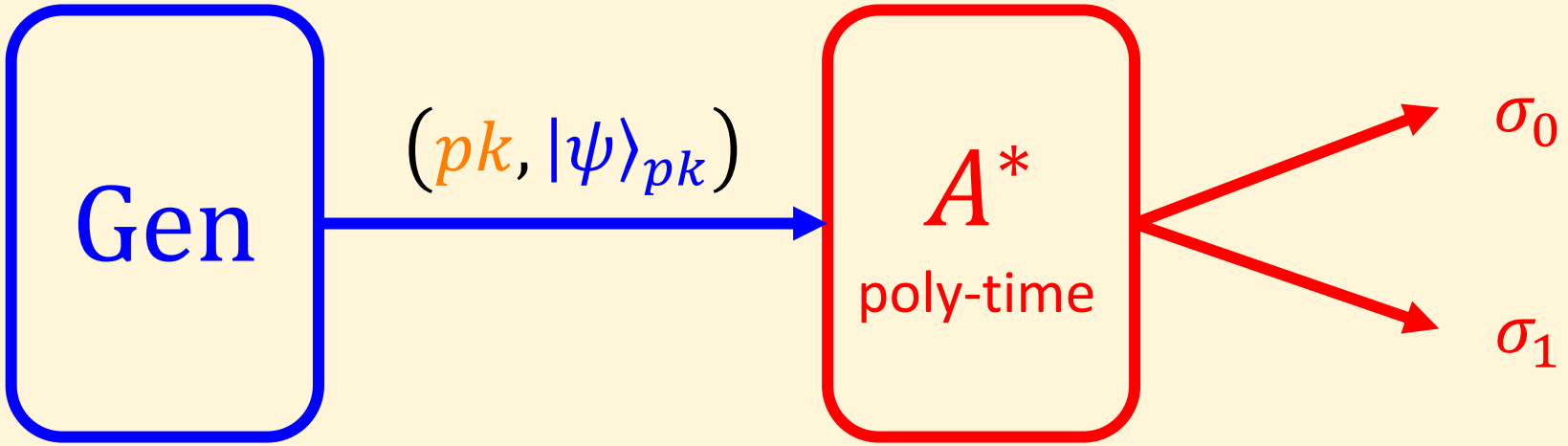
Tokenized Signatures

- **Correctness 2:** If the verifier accepted the state, the state can be used to successfully sign on any bit $m \in \{0,1\}$.



Tokenized Signatures

- **Security:**



Tokenized Signatures

- **Security:**

Gen

A^*
poly-time

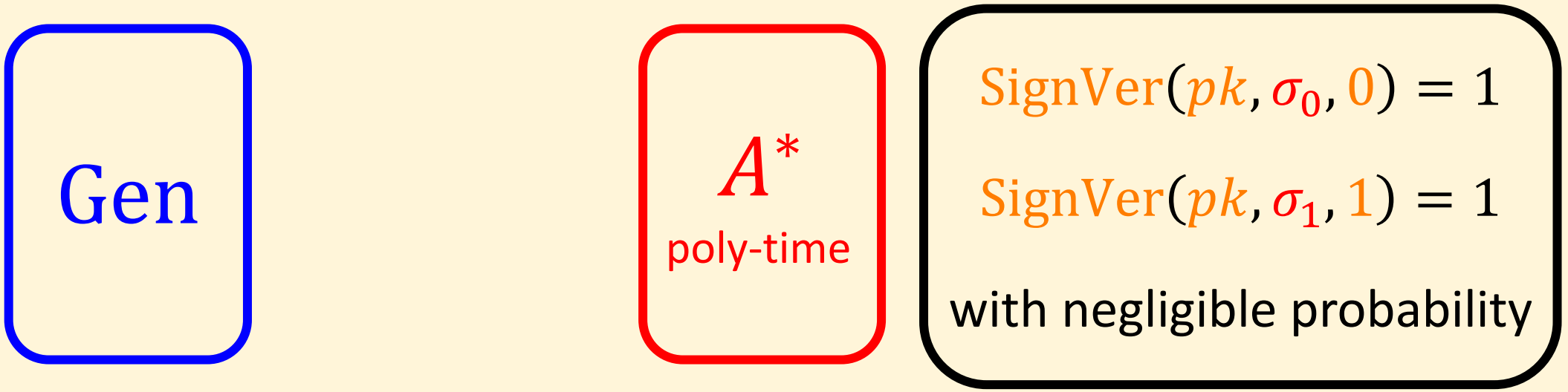
$\mathrm{SignVer}(pk, \sigma_0, 0) = 1$

$\mathrm{SignVer}(pk, \sigma_1, 1) = 1$

with negligible probability

Tokenized Signatures

- **Security:**

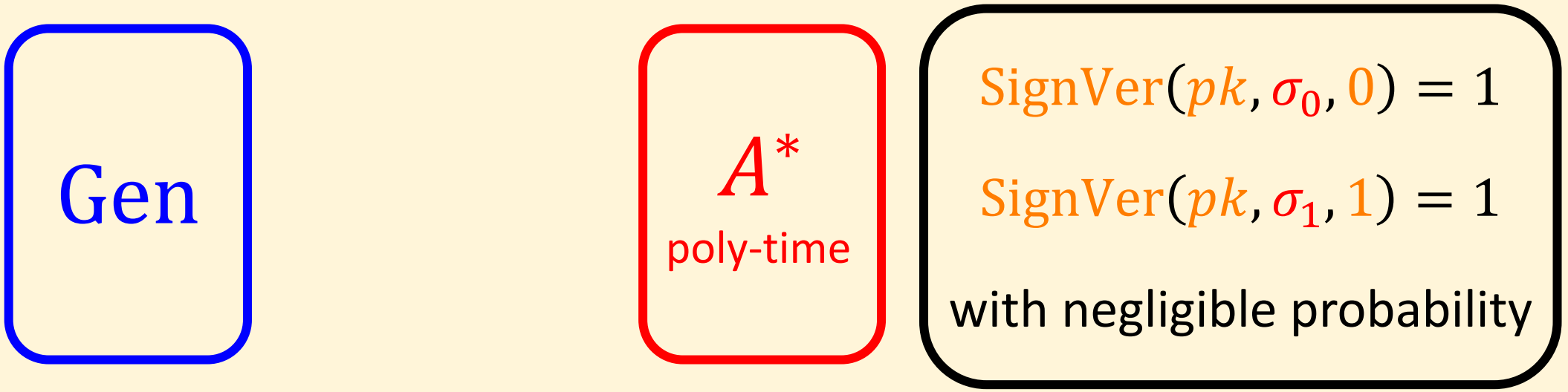


Q:

Tokenized signatures imply PKQM. How?

Tokenized Signatures

- **Security:**

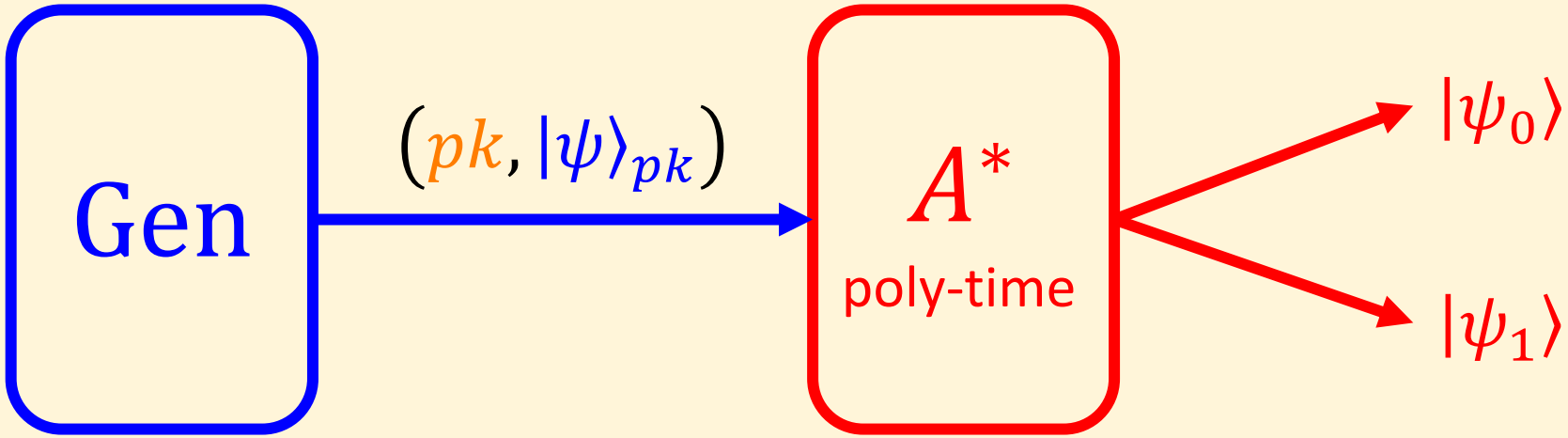


A:

Assume you can cheat the verifier. Then you can sign on both 0 and 1.

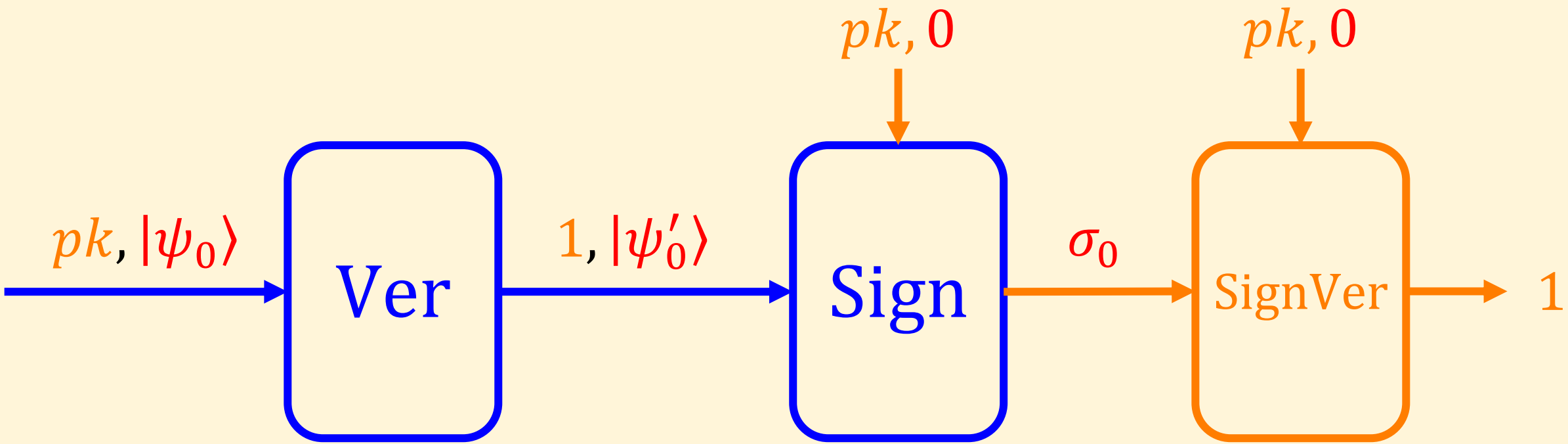
Tokenized Signatures

- **Security:**



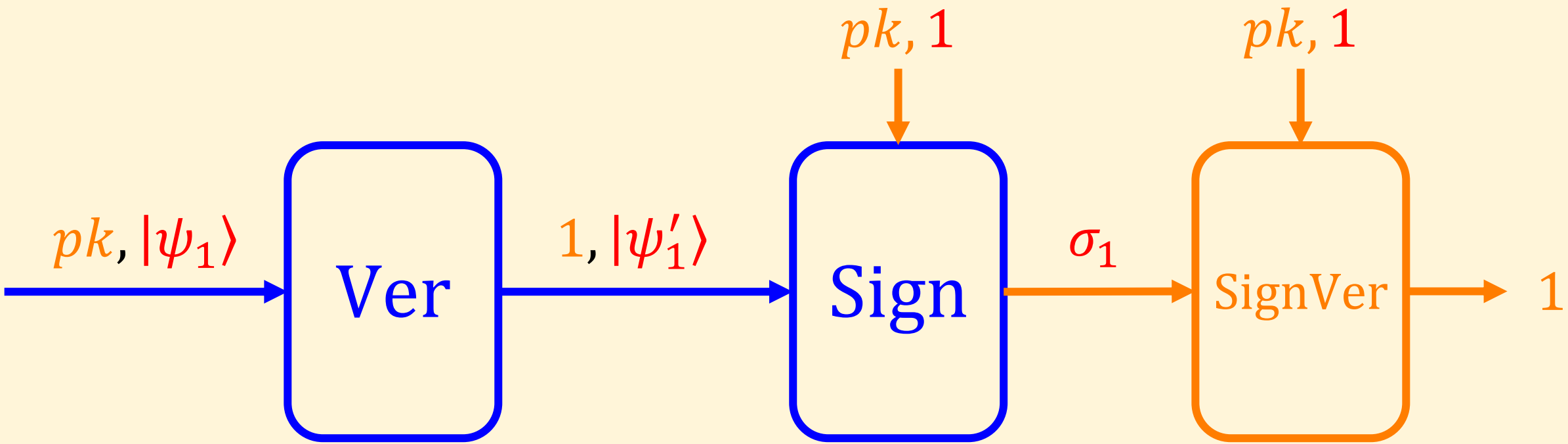
Tokenized Signatures

- **Correctness 2:** If the verifier accepted the state, the state can be used to successfully sign on any bit $m \in \{0,1\}$.



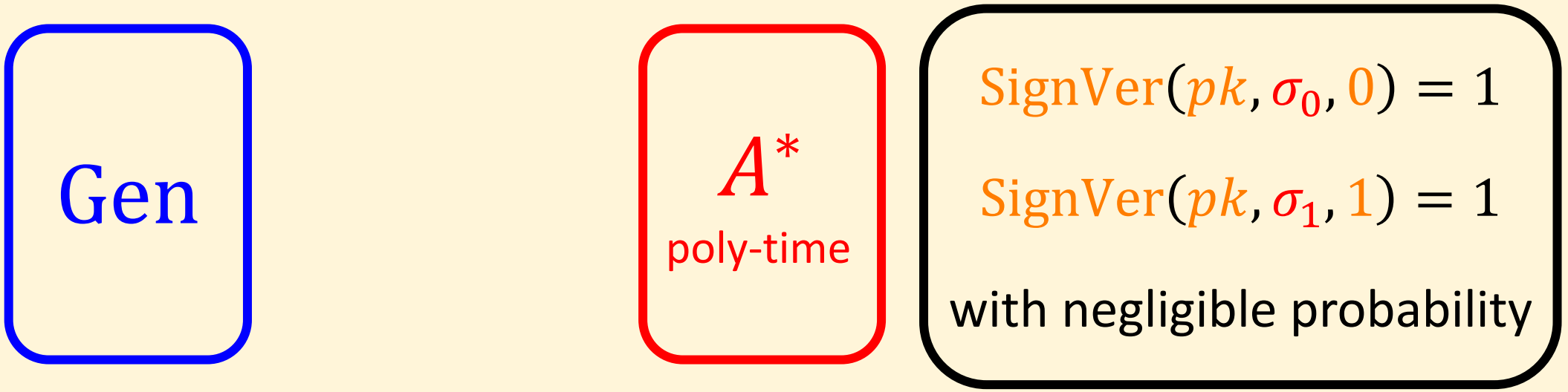
Tokenized Signatures

- **Correctness 2:** If the verifier accepted the state, the state can be used to successfully sign on any bit $m \in \{0,1\}$.



Tokenized Signatures

- **Security:**

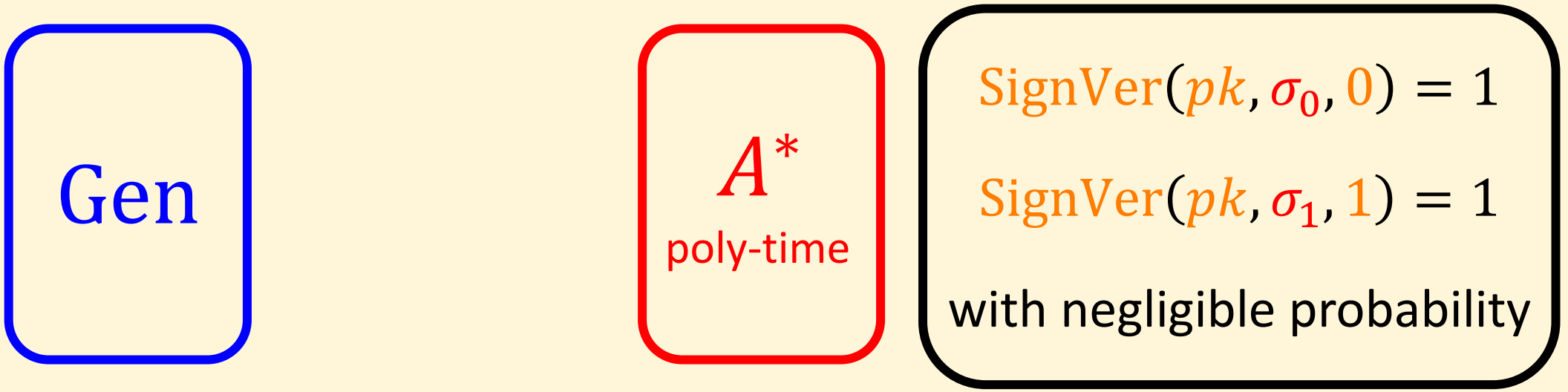


A:

Assume you can cheat the verifier. Then you can sign on both 0 and 1.

Tokenized Signatures

- **Security:**

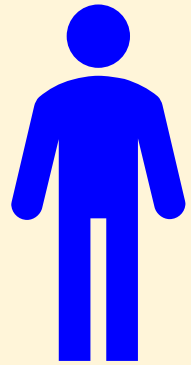


Note: $\sigma_m \in \{0,1\}^n$ serves as a *classical proof of destruction* for the quantum information in $|\psi\rangle_{pk}$.

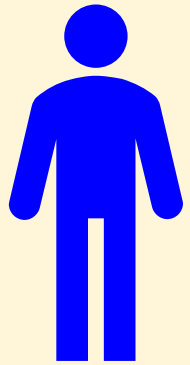
The Quantum Delivery Verification Problem:

Solution using Tokenized Signatures

pk

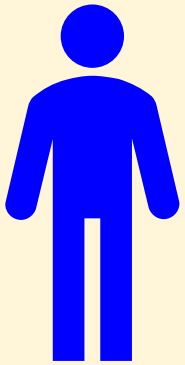


$|\psi\rangle_{pk}$



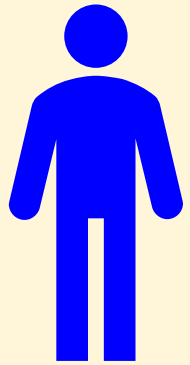
The Quantum Delivery Verification Problem:

Solution using Tokenized Signatures



pk, val_{pk}

$|\psi\rangle_{pk}$



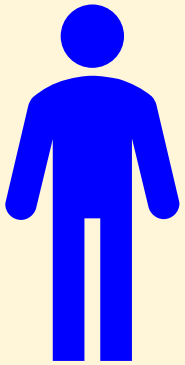
$pk', \mathrm{val}_{pk'}$

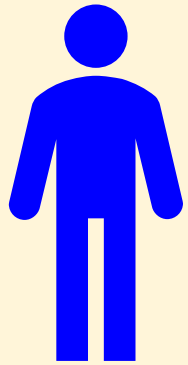
$|\psi\rangle_{pk'}$

The Quantum Delivery Verification Problem:

Solution using Tokenized Signatures

A CRH $H: \{0,1\}^* \to \{0,1\}^\lambda$





$$\overrightarrow{pk} = \left(pk_1, \cdots, pk_\lambda, \mathrm{val}_{\overrightarrow{pk}}\right)$$

$$|\psi\rangle_{\overrightarrow{pk}} = \left(|\psi\rangle_{pk_1}, \cdots, |\psi\rangle_{pk_\lambda}\right)$$

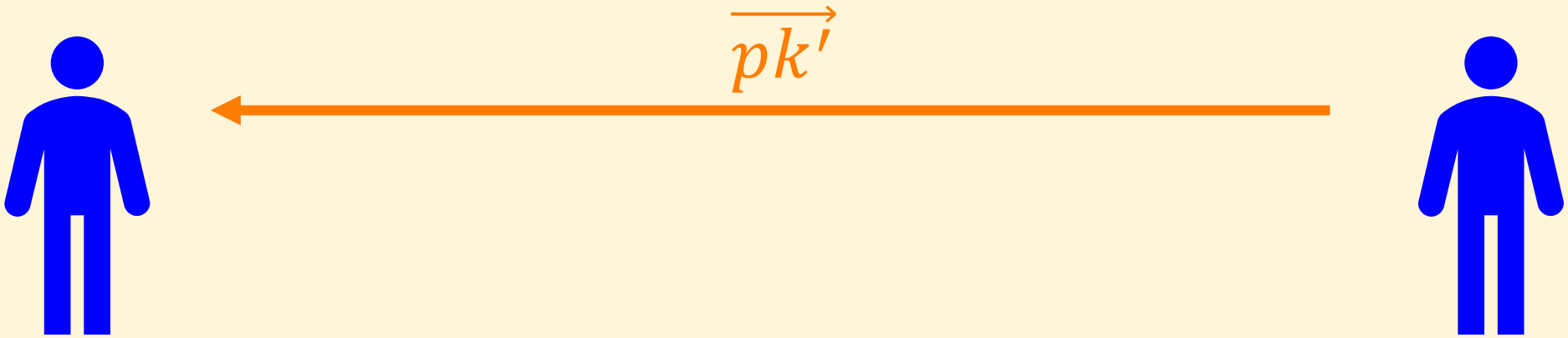
$$\overrightarrow{pk'} = \left(pk'_1, \cdots, pk'_\lambda, \mathrm{val}_{\overrightarrow{pk'}}\right)$$

$$|\psi\rangle_{\overrightarrow{pk'}} = \left(|\psi\rangle_{pk'_1}, \cdots, |\psi\rangle_{pk'_\lambda}\right)$$

The Quantum Delivery Verification Problem:

Solution using Tokenized Signatures

A CRH $H: \{0,1\}^* \to \{0,1\}^\lambda$



$$\overrightarrow{pk} = \left(pk_1, \cdots, pk_\lambda, \mathrm{val}_{\overrightarrow{pk}}\right)$$

$$|\psi\rangle_{\overrightarrow{pk}} = \left(|\psi\rangle_{pk_1}, \cdots, |\psi\rangle_{pk_\lambda}\right)$$

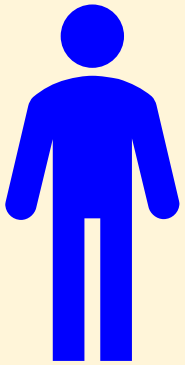
$$\overrightarrow{pk'} = \left(pk'_1, \cdots, pk'_\lambda, \mathrm{val}_{\overrightarrow{pk'}}\right)$$

$$|\psi\rangle_{\overrightarrow{pk'}} = \left(|\psi\rangle_{pk'_1}, \cdots, |\psi\rangle_{pk'_\lambda}\right)$$

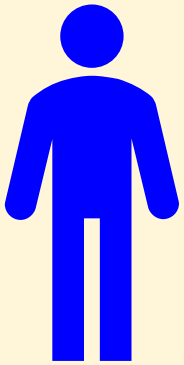
The Quantum Delivery Verification Problem:

Solution using Tokenized Signatures

A CRH $H: \{0,1\}^* \to \{0,1\}^\lambda$



1. $h \leftarrow H\left(\overrightarrow{pk'}\right)$.
2. $\left(\sigma_h \in \{0,1\}^{n\cdot\lambda}\right) \leftarrow \mathrm{Sign}\left(\overrightarrow{pk}, |\psi\rangle_{\overrightarrow{pk}}, h\right)$.



$$\overrightarrow{pk} = \left(pk_1, \cdots, pk_\lambda, \mathrm{val}_{\overrightarrow{pk}}\right)$$

~~$|\psi\rangle_{\overrightarrow{pk}} = \left(|\psi\rangle_{pk_1}, \cdots, |\psi\rangle_{pk_\lambda}\right)$~~

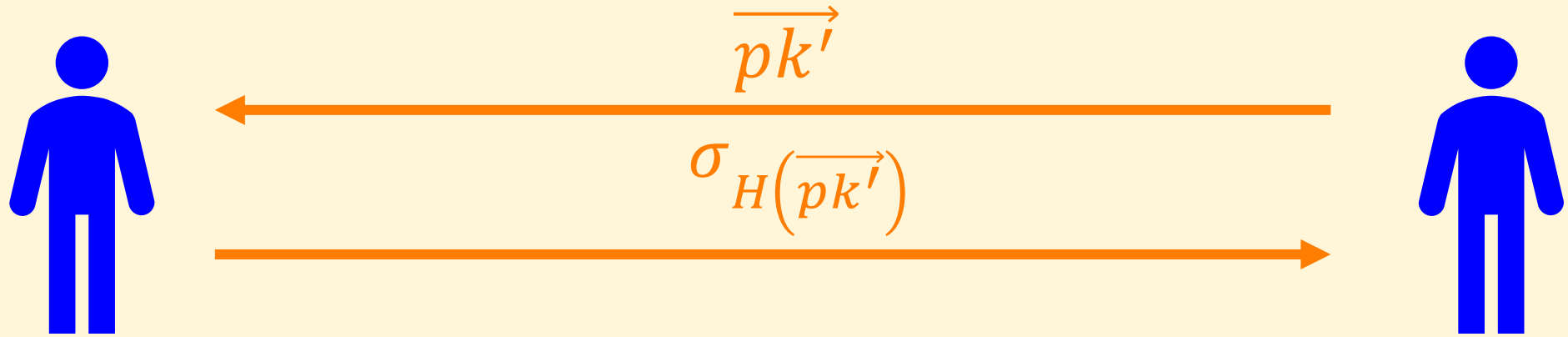
$$\overrightarrow{pk'} = \left(pk'_1, \cdots, pk'_\lambda, \mathrm{val}_{\overrightarrow{pk'}}\right)$$

$$|\psi\rangle_{\overrightarrow{pk'}} = \left(|\psi\rangle_{pk'_1}, \cdots, |\psi\rangle_{pk'_\lambda}\right)$$

The Quantum Delivery Verification Problem:

Solution using Tokenized Signatures

A CRH $H: \{0,1\}^* \to \{0,1\}^\lambda$



$$\overrightarrow{pk} = \left(pk_1, \cdots, pk_\lambda, \mathrm{val}_{\overrightarrow{pk}}\right)$$

$$\overrightarrow{pk'} = \left(pk'_1, \cdots, pk'_\lambda, \mathrm{val}_{\overrightarrow{pk'}}\right)$$

Note: We got classical-only communication for free!

$$|\psi\rangle_{\overrightarrow{pk'}} = \left(|\psi\rangle_{pk'_1}, \cdots, |\psi\rangle_{pk'_\lambda}\right)$$

How to Construct Tokenized Signatures

Definition [Coset State]:

Let $n \in \mathbb{N}$ and let $S \subseteq \{0,1\}^n$ a subspace of $\{0,1\}^n$ and let $x, z \in \{0,1\}^n$.

The coset state of S with string shift x and phase shift z is defined as

$$|S\rangle^{x,z} := \frac{1}{\sqrt{|S|}} \sum_{u \in S} (-1)^{\langle z,u \rangle} \cdot |x + u\rangle \ .$$

How to Construct Tokenized Signatures

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

$$H^{\otimes n} \cdot |S\rangle^{x,z} = |S^{\perp}\rangle^{z,x}.$$

Proof: By calculation.

How to Construct Tokenized Signatures

Theorem [Ben-David-Sattath-2018] + [Coladangelo-Liu-Liu-Zhandry-2021]:

Assume the existence of a quantum-secure iO and injective OWFs.

Let S a random subspace $S \subseteq \{0,1\}^n$ of dimension $\frac{n}{2}$, and let $x, z \in \{0,1\}^n$ random strings.

For every quantum polynomial-time algorithm A^*, the following probability is negligible:

$$\Pr_{(\mathrm{O}_{S+x}, \mathrm{O}_{S^\perp+z}, |S\rangle^{x,z}) \leftarrow \mathrm{Gen}(1^n)} \left[\begin{array}{c} A^*\left(\mathrm{O}_{S+x}, \mathrm{O}_{S^\perp+z}, |S\rangle^{x,z}\right) = (u, v), \\ u \in S + x, \\ v \in S^\perp + z \end{array} \right].$$

How to Construct Tokenized Signatures

Construction [Ben-David-Sattath-2018] + [Coladangelo-Liu-Liu-Zhandry-2021]:

- $(pk, |\psi\rangle_{pk}) \leftarrow \mathrm{Gen}(1^n)$.
- $|\psi\rangle_{pk} = |S\rangle^{x,z}$.
- $pk = (\mathrm{Obf}_{S+x}, \mathrm{Obf}_{S^\perp+z})$.
- $\mathrm{Ver}(pk, |\phi\rangle)$:
  - First, check that the rightmost qubit of $U_{S+x}(|\phi\rangle|0\rangle)$ is 1.
  - Now the state is $|\phi'\rangle := \sum_{u\in S} \alpha'_u \cdot |x+u\rangle$. Apply $H^{\otimes n} \cdot |\phi'\rangle = |\phi''\rangle$.
  - Finally, check that the rightmost qubit of $U_{S^\perp+z}(|\phi''\rangle|0\rangle)$ is 1.

How to Construct Tokenized Signatures

Construction [Ben-David-Sattath-2018] + [Coladangelo-Liu-Liu-Zhandry-2021]:

- $\mathrm{Sign}(pk, |S\rangle^{x,z}, m \in \{0,1\})$: ?
- $\mathrm{SignVer}(pk, \sigma_m, m \in \{0,1\})$: ?

How to Construct Tokenized Signatures

Construction [Ben-David-Sattath-2018] + [Coladangelo-Liu-Liu-Zhandry-2021]:

- $\mathrm{Sign}(pk, |S\rangle^{x,z}, m \in \{0,1\})$: Execute $\left(H^{\otimes n}\right)^{m} \cdot |S\rangle^{x,z}$, and measure.
- $\mathrm{SignVer}(pk, \sigma_m, m \in \{0,1\})$:

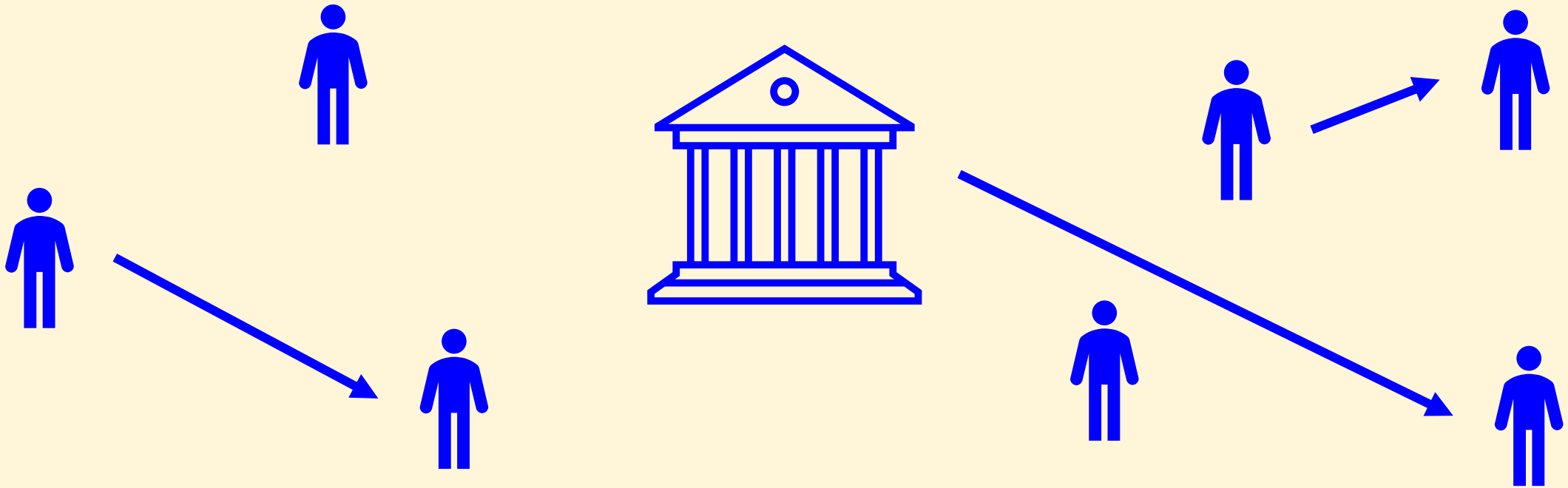
How to Construct Tokenized Signatures

Construction [Ben-David-Sattath-2018] + [Coladangelo-Liu-Liu-Zhandry-2021]:

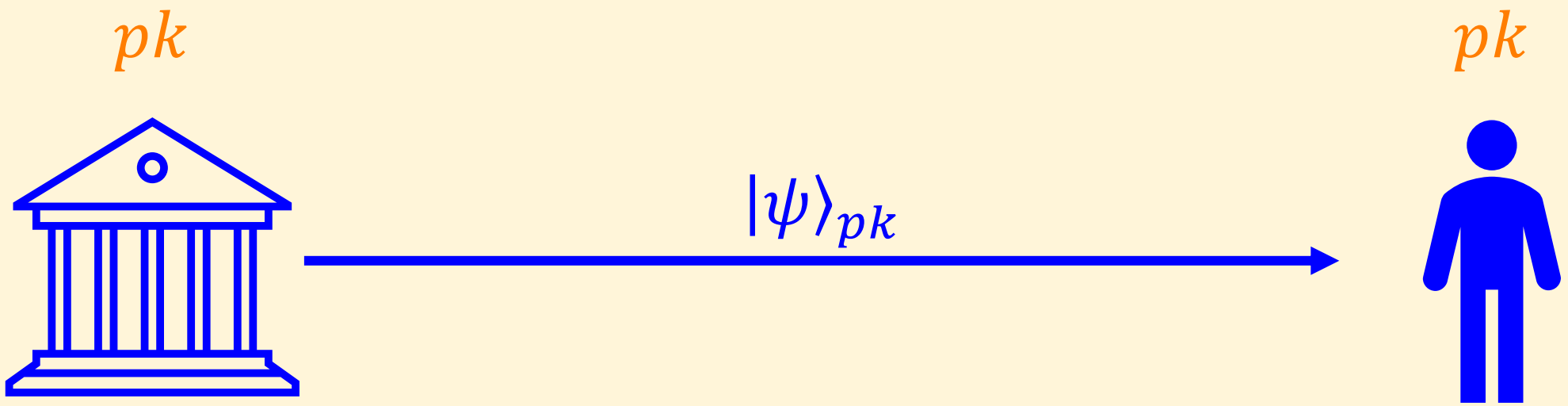
- $\mathrm{Sign}(pk, |S\rangle^{x,z}, m \in \{0,1\})$: Execute $\left(H^{\otimes n}\right)^{m} \cdot |S\rangle^{x,z}$, and measure.
- $\mathrm{SignVer}(pk, \sigma_m, m \in \{0,1\})$: If $m = 0$ then check $\sigma_m \in S + x$, otherwise, check $\sigma_m \in S^{\perp} + z$.

The Quantum Delivery Verification Problem
(Strikes Again)

The Quantum Delivery Verification Problem
(Strikes Again)

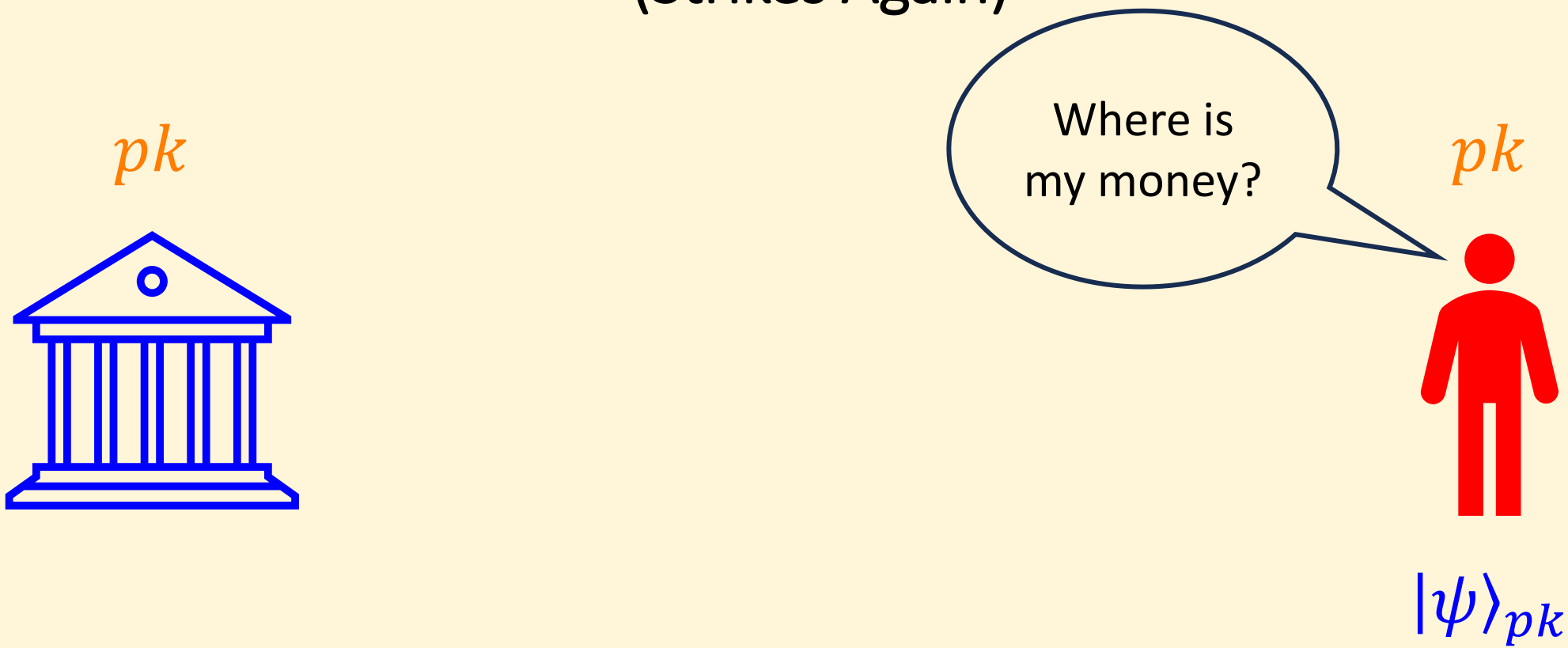


The Quantum Delivery Verification Problem
(Strikes Again)



Scenario I

The Quantum Delivery Verification Problem
(Strikes Again)



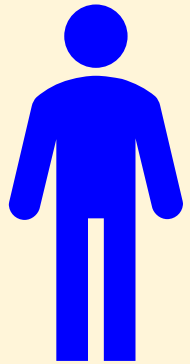
Scenario I

The Quantum Delivery Verification Problem
(Strikes Again)

pk

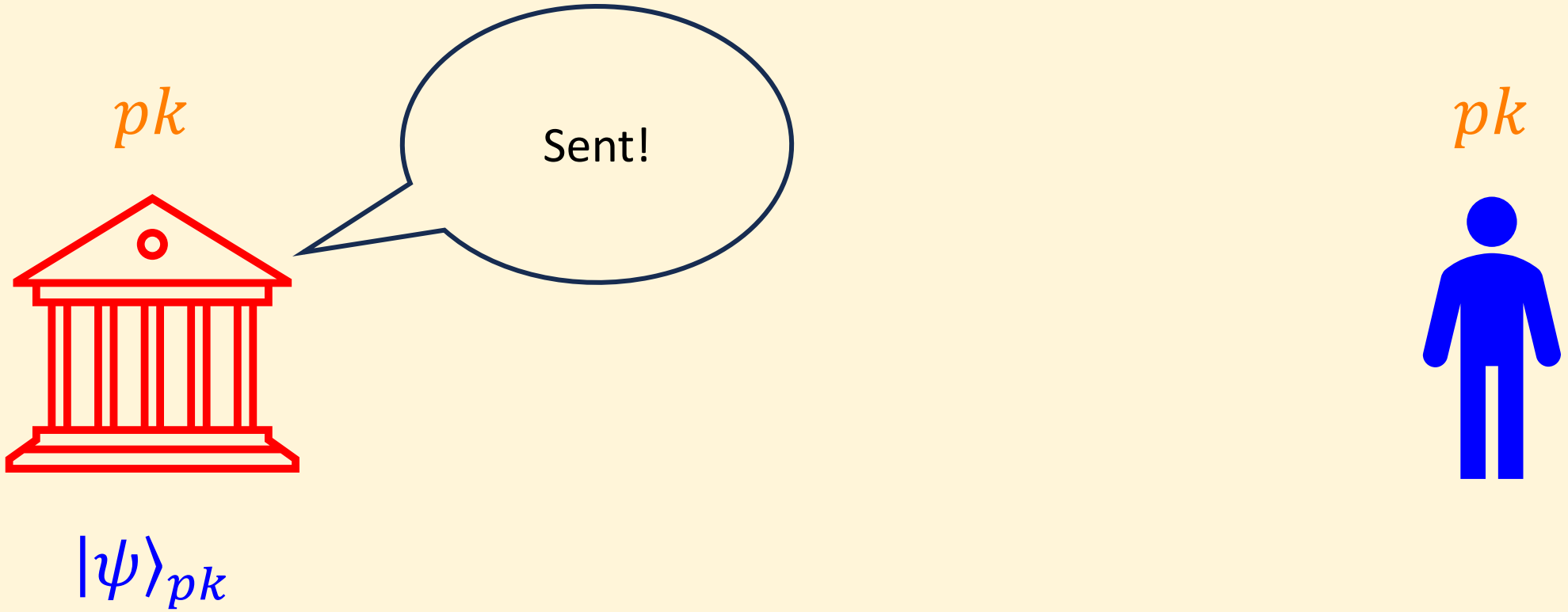
$|\psi\rangle_{pk}$

pk



Scenario II

The Quantum Delivery Verification Problem
(Strikes Again)



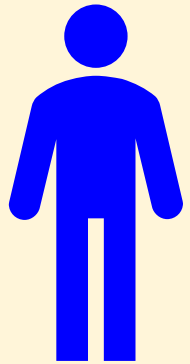
Scenario II

The Quantum Delivery Verification Problem
(Strikes Again)

pk

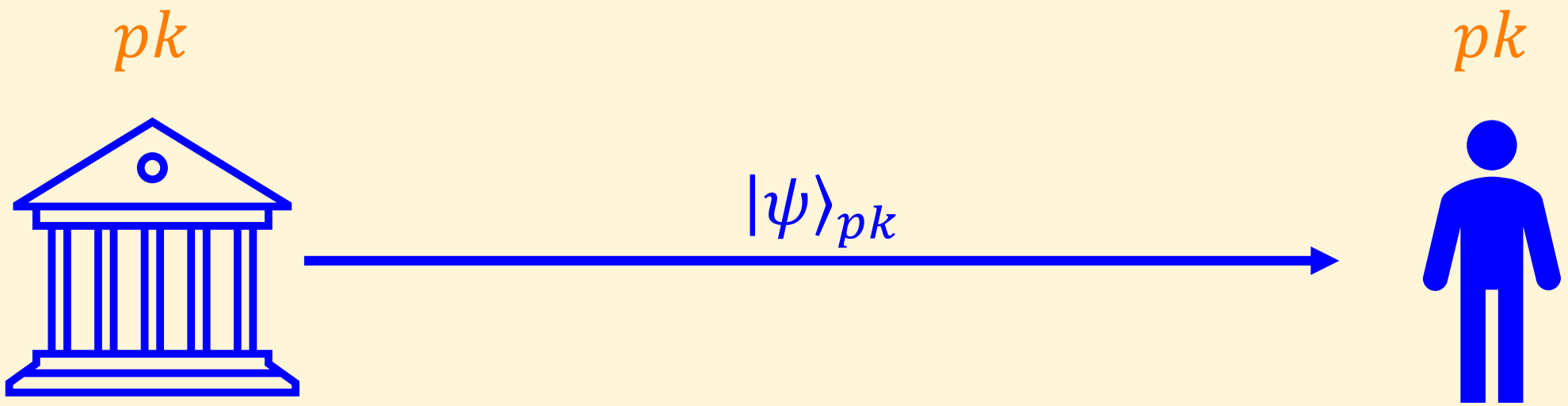
$|\psi\rangle_{pk}$

pk



Scenario III

The Quantum Delivery Verification Problem
(Strikes Again)



Scenario III

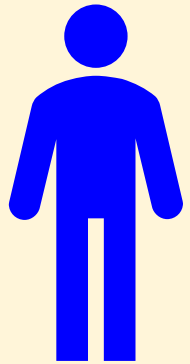
The Quantum Delivery Verification Problem
(Strikes Again)

Channel can be actively adversarial,
or just faulty. Does not matter.

pk

$|\psi\rangle_{pk} \rightarrow |\phi\rangle$

pk



Scenario III

The Quantum Delivery Verification Problem
(Strikes Again)

Q:

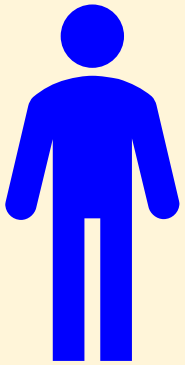
Why doesn’t the solution from before work?

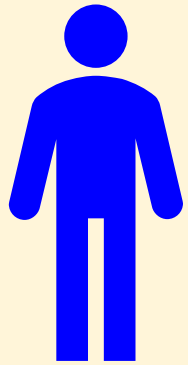
That is, why doesn’t tokenized signatures solve the problem?

The Quantum Delivery Verification Problem:

Solution using Tokenized Signatures

A CRH $H: \{0,1\}^* \to \{0,1\}^\lambda$





$$\overrightarrow{pk} = \left(pk_1, \cdots, pk_\lambda, \mathrm{val}_{\overrightarrow{pk}}\right)$$

$$|\psi\rangle_{\overrightarrow{pk}} = \left(|\psi\rangle_{pk_1}, \cdots, |\psi\rangle_{pk_\lambda}\right)$$

$$\overrightarrow{pk'} = \left(pk'_1, \cdots, pk'_\lambda, \mathrm{val}_{\overrightarrow{pk'}}\right)$$

$$|\psi\rangle_{\overrightarrow{pk'}} = \left(|\psi\rangle_{pk'_1}, \cdots, |\psi\rangle_{pk'_\lambda}\right)$$

The Quantum Delivery Verification Problem
(Strikes Again)

Q:

Why doesn’t the solution from before work?

That is, why doesn’t tokenized signatures solve the problem?

A:

The previous solution assumed the two parties already have money states! For this, the bank needs to distribute states in the first place.

Public-key Semi-quantum Money

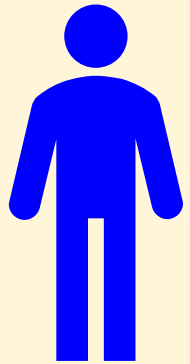
The Quantum Delivery Verification Problem

When $|\psi\rangle_{pk}$ is already generated,
it is unknown how to send it.

pk

$|\psi\rangle_{pk}$

pk



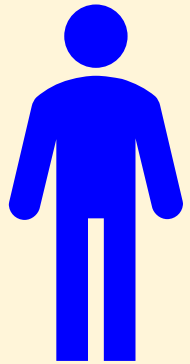
The Quantum Delivery Verification Problem

pk

$|\psi\rangle_{pk}$

We need to somehow let the receiver generate it by itself.

pk



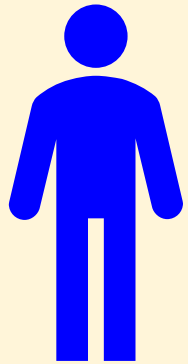
The Quantum Delivery Verification Problem

pk

$|\psi\rangle_{pk}$

Idea: If you can classically delegate the generation of the state, then you can prove in ZK that the (classical) instructions yield a valid state.

pk



The Quantum Delivery Verification Problem

Definition [Tokenized Signatures Scheme] :

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

Semi-quantum Tokenized Signatures

[S-2021], [S-2022]

Definition [Semi-quantum Tokenized Signatures]:

- $\left(pk, \text{Rec: } |\psi\rangle_{pk}\right) \leftarrow \langle\, \text{Sen}, \text{Rec} \,\rangle(1^n)$.
- $(b \in \{0,1\}, |\phi'\rangle) \leftarrow \text{Ver}(pk, |\phi\rangle)$.
- $(\sigma_m \in \{0,1\}^n) \leftarrow \text{Sign}\left(pk, |\psi\rangle_{pk}, m \in \{0,1\}\right)$.
- $(b \in \{0,1\}) \leftarrow \text{SignVer}(pk, \sigma_m, m \in \{0,1\})$.

Semi-quantum Tokenized Signatures

[S-2021], [S-2022]

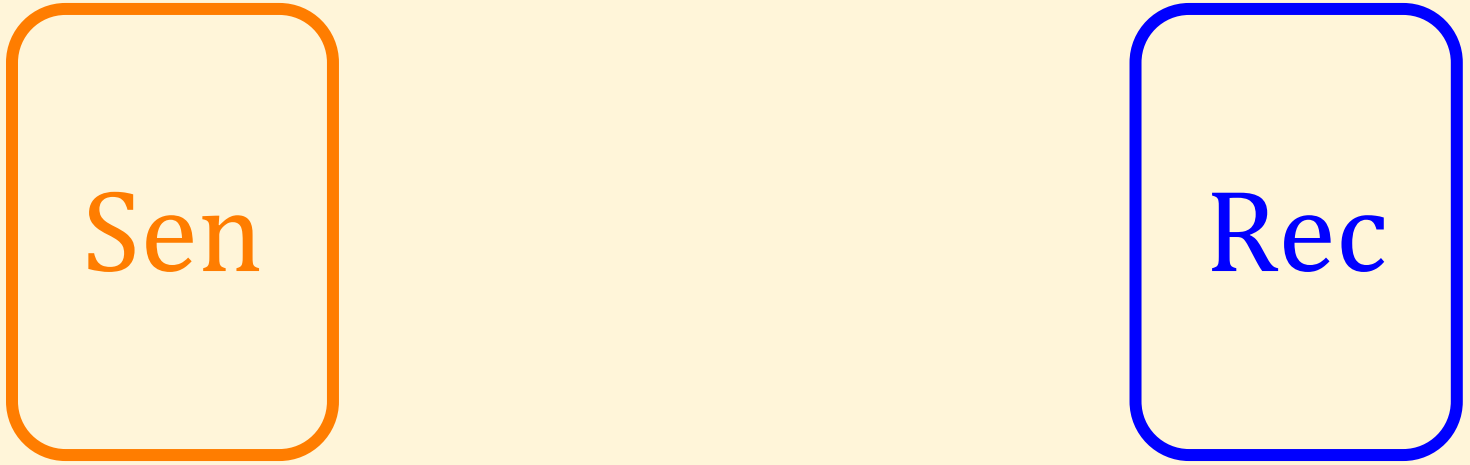
Step 1 [S-2021]:

Classical delegation of unclonable state generation.

Step 2 [S-2022]:

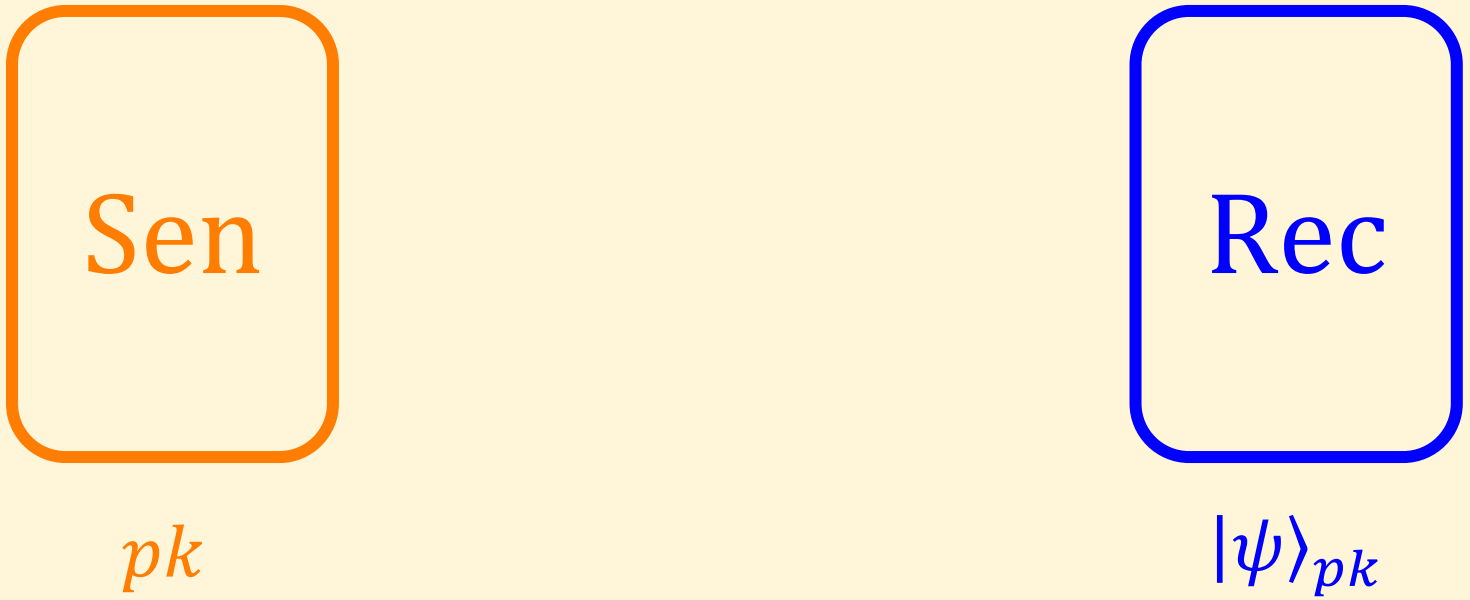
A different technique for signing quantum money states, tailored for states that resulted from delegation.

Classical delegation of state generation:

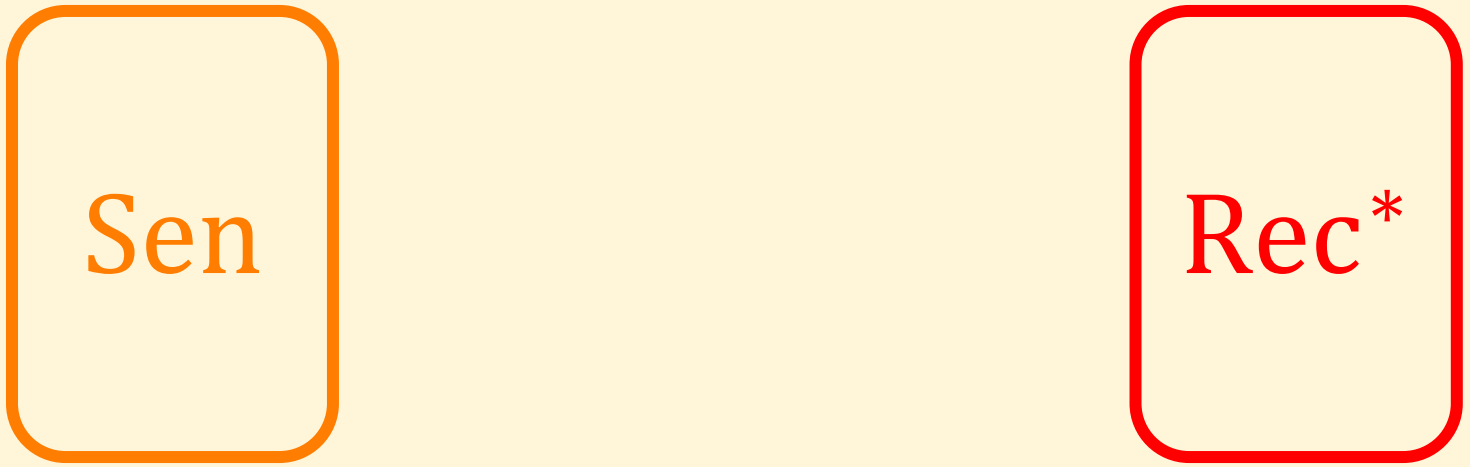


Classical delegation of state generation:

Classical delegation of state generation:

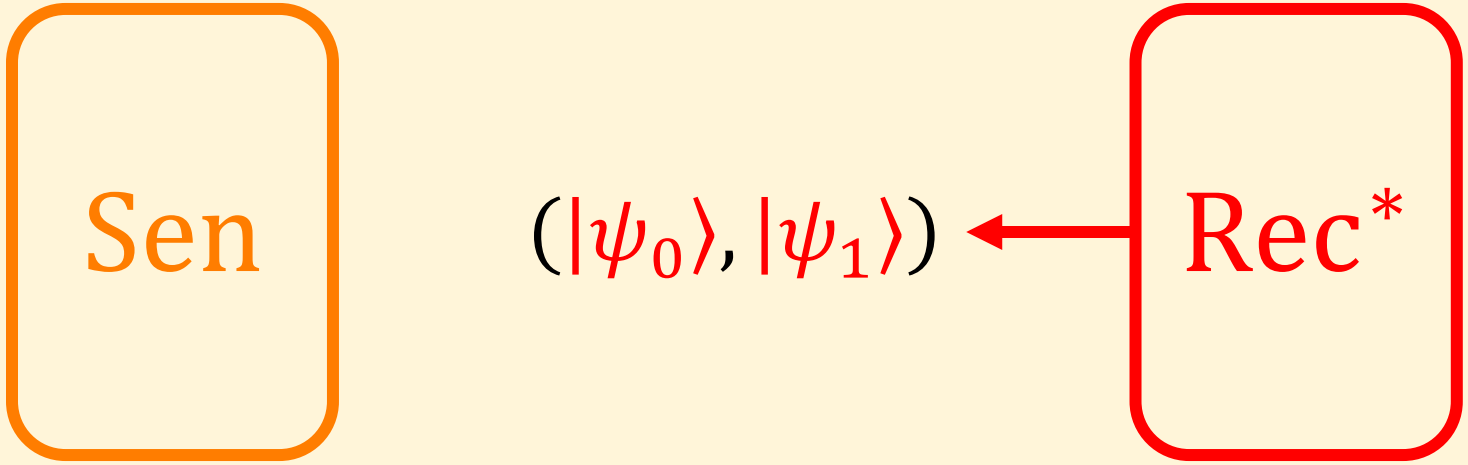


Security - Remote No Cloning



Security - Remote No Cloning

Security - Remote No Cloning



Security - Remote No Cloning

Main difference: $|\psi\rangle_{pk}$ is unclonable for the <u>generating computer</u>.

Sen

Rec^*

$\mathrm{Ver}(pk, |\psi\rangle_0) = 1$

$\mathrm{Ver}(pk, |\psi\rangle_1) = 1$

with negligible probability

Public-key Semi-quantum Money

Introduced in [Radian-Sattath-2019]

Definition [Public-key Semi-quantum Money]:

- $\left(pk, \text{Rec: } |\psi\rangle_{pk}\right) \leftarrow \langle\, \text{Sen}, \text{Rec} \,\rangle(1^n)$.
- $(b \in \{0,1\}, |\phi'\rangle) \leftarrow \text{Ver}(pk, |\phi\rangle)$.

Public-key Semi-quantum Money

Theorem [S-2021]:

Assume,

- Quantum sub-exponential hardness of LWE, and
- Quantum-secure indistinguishability obfuscation for classical circuits.

Then, there exists a Public-Key Semi-Quantum Money Scheme.

Public-key Semi-quantum Money - Intuition

Construct a protocol:

- Sen : A classical sender, wants to delegate the state generation.
- Rec : A quantum receiver, generates the state. Possibly malicious.

At the end of interaction: Sen outputs pk, Rec outputs $|\psi\rangle_{pk}$.

Public-key Semi-quantum Money - Intuition

- $(gk) \leftarrow \chi$: Classically efficiently samplable distribution.
- $\left(|\psi\rangle_\beta, \beta\right) \leftarrow G(gk)$: A quantum polynomial-time algorithm, outputs classical $\beta \in \{0,1\}^n$ and a quantum $|\psi\rangle_\beta$.

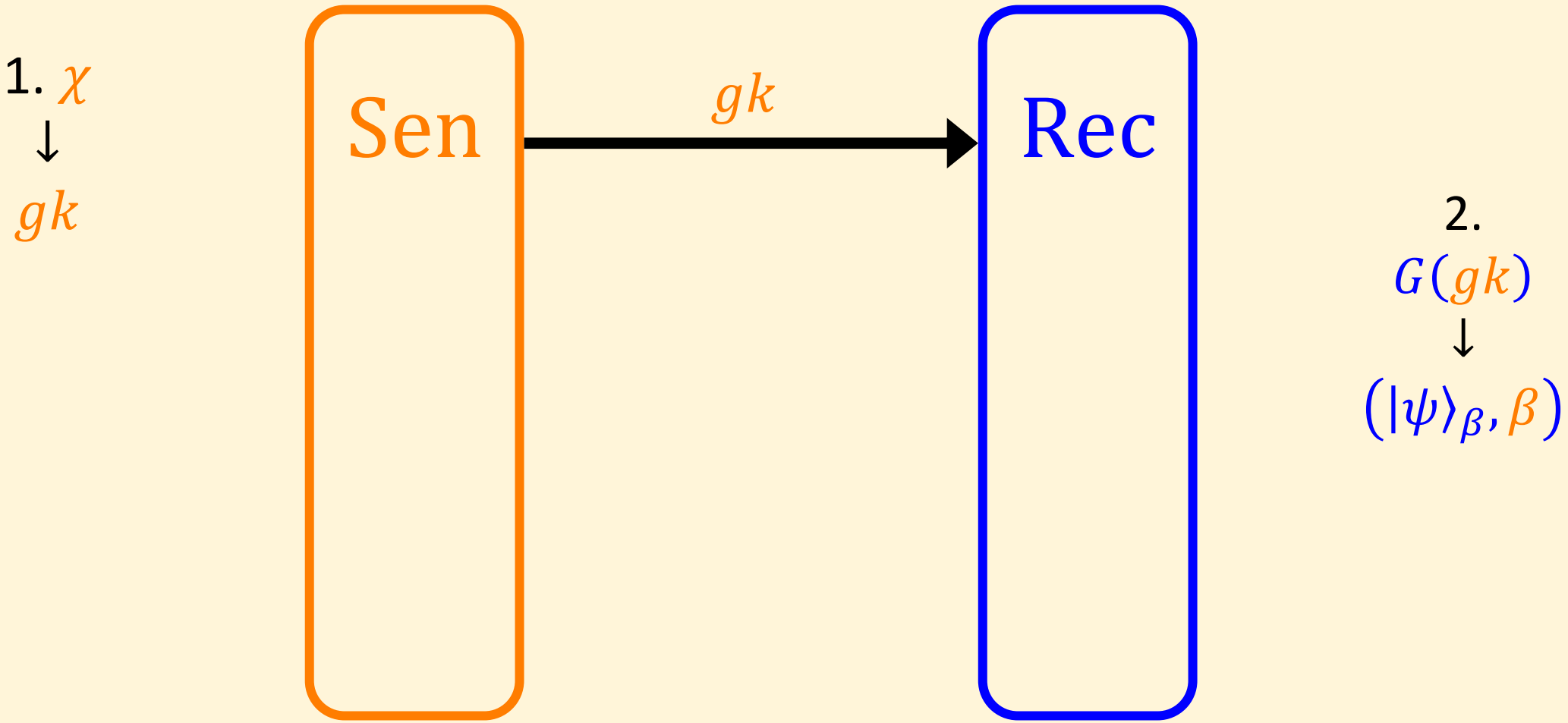
Public-key Semi-quantum Money - Intuition

- $(gk) \leftarrow \chi$: Classically efficiently samplable distribution.
- $\left(|\psi\rangle_\beta, \beta\right) \leftarrow G(gk)$: A quantum polynomial-time algorithm, outputs classical $\beta \in \{0,1\}^n$ and a quantum $|\psi\rangle_\beta$.

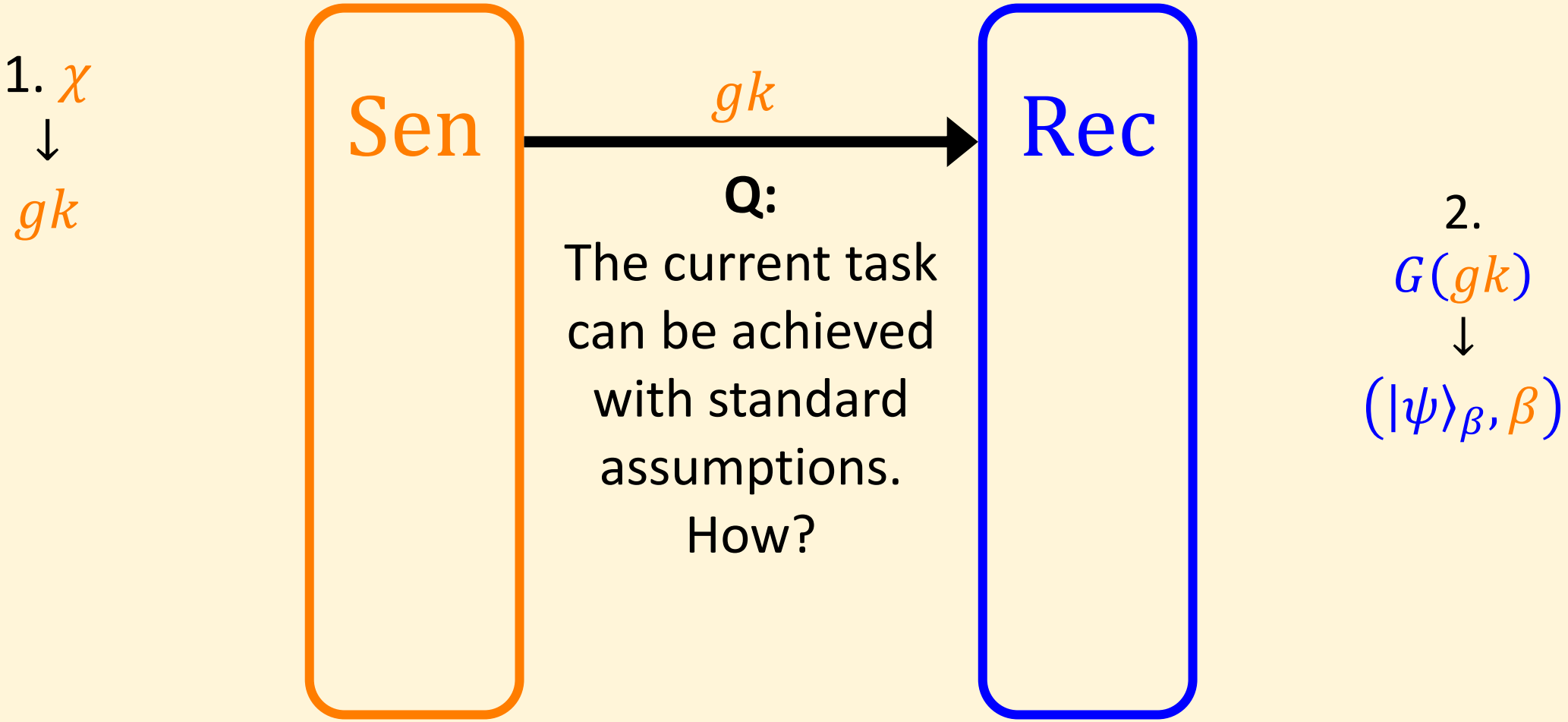
Unclonability: Given a sampled gk, it is computationally impossible to compute

$$\left(|\psi\rangle_\beta, |\psi\rangle_\beta, \beta\right)$$

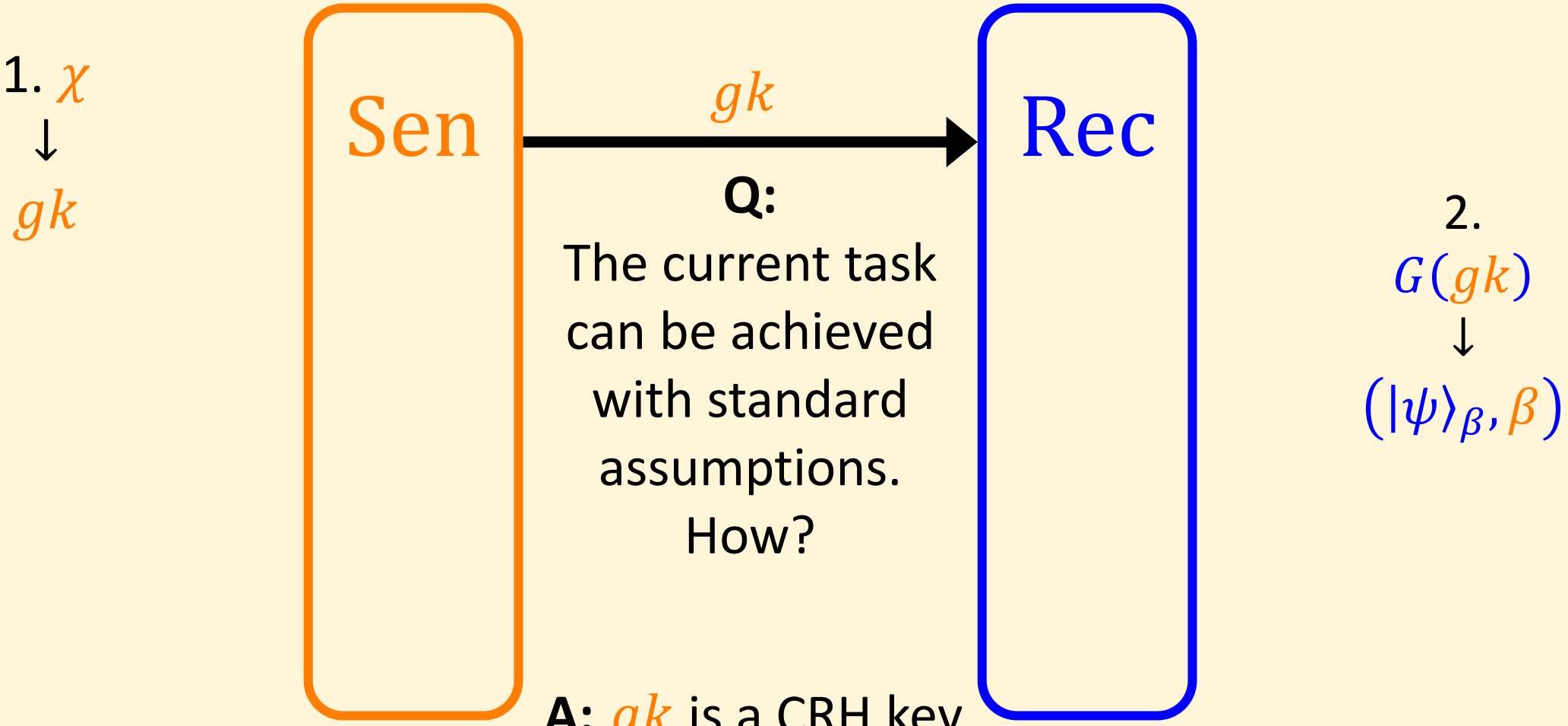
A General Template



A General Template



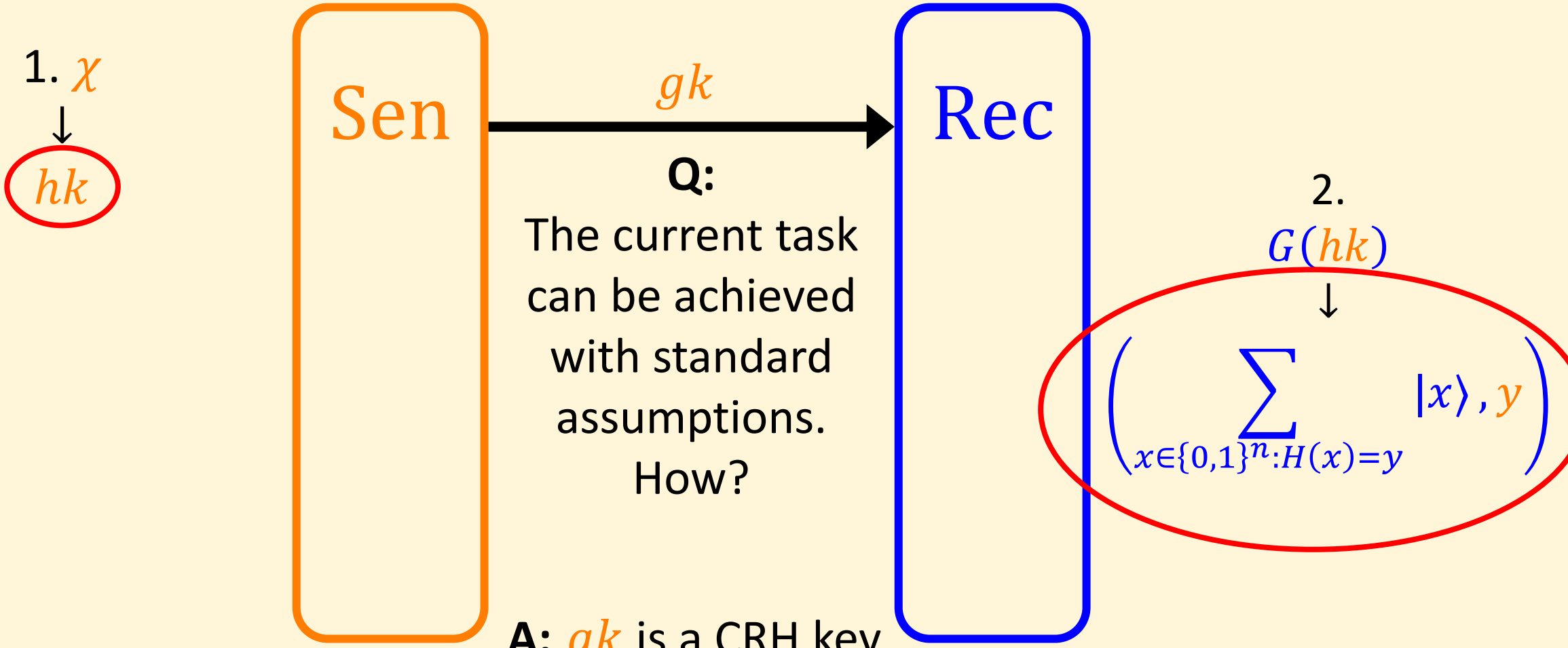
A General Template



A: gk is a CRH key.

$G(gk)$ computes in superposition and measures the output of the CRH H.

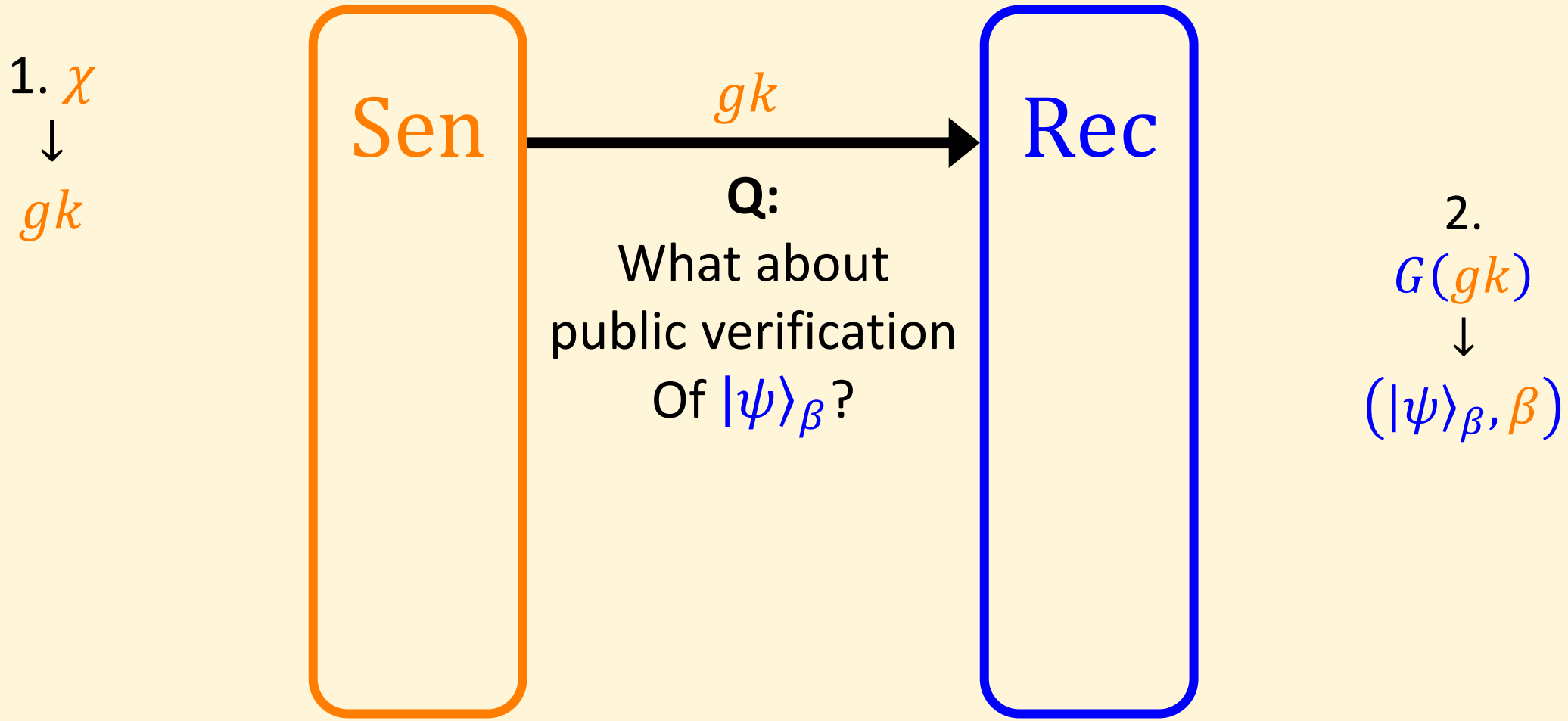
A General Template



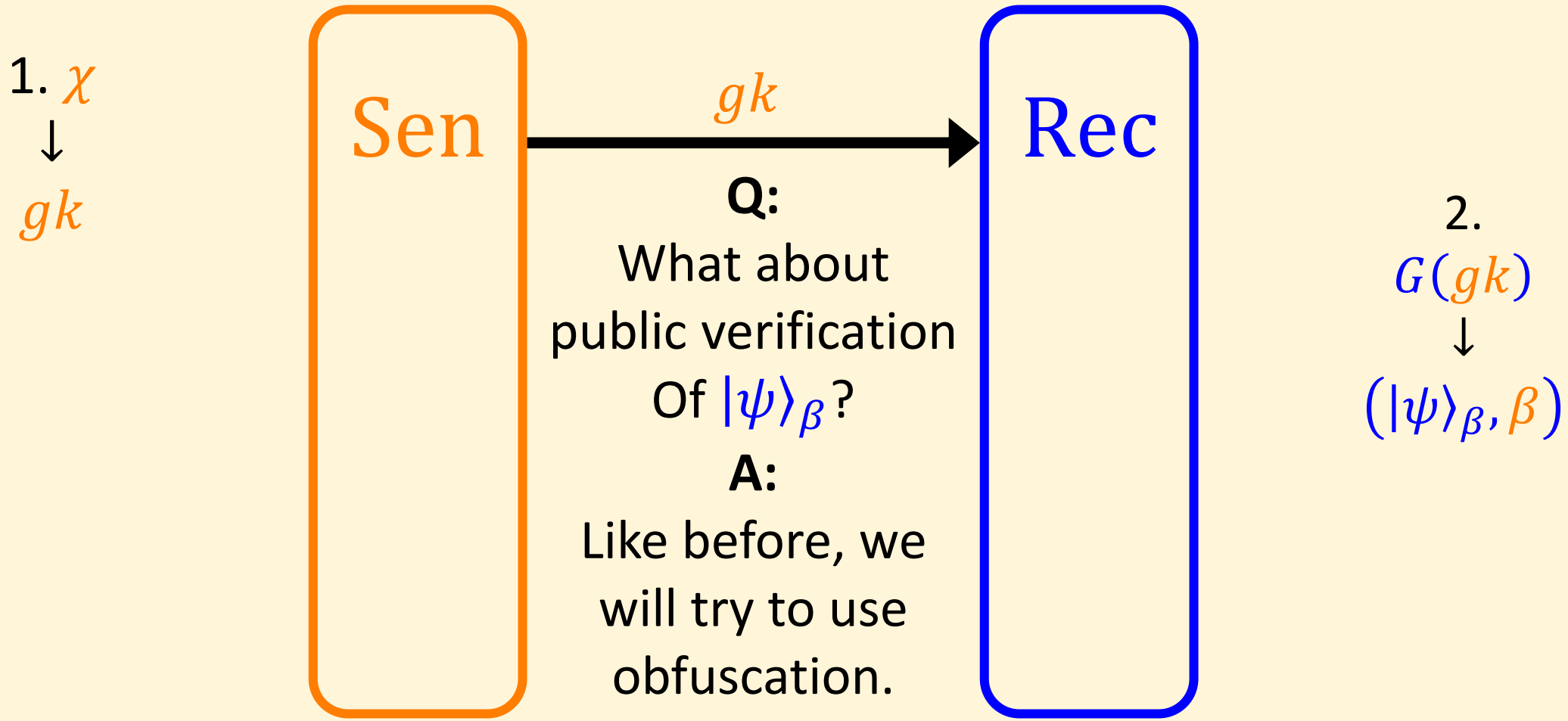
A: gk is a CRH key.

$G(gk)$ computes in superposition and measures the output of the CRH H.

A General Template



A General Template



A General Template

- $(gk, sk) \leftarrow \chi$: Classically efficiently samplable distribution.
- $\left(|\psi\rangle_\beta, \beta\right) \leftarrow G(gk)$: A quantum polynomial-time algorithm, outputs classical $\beta \in \{0,1\}^n$ and a quantum $|\psi\rangle_\beta$.

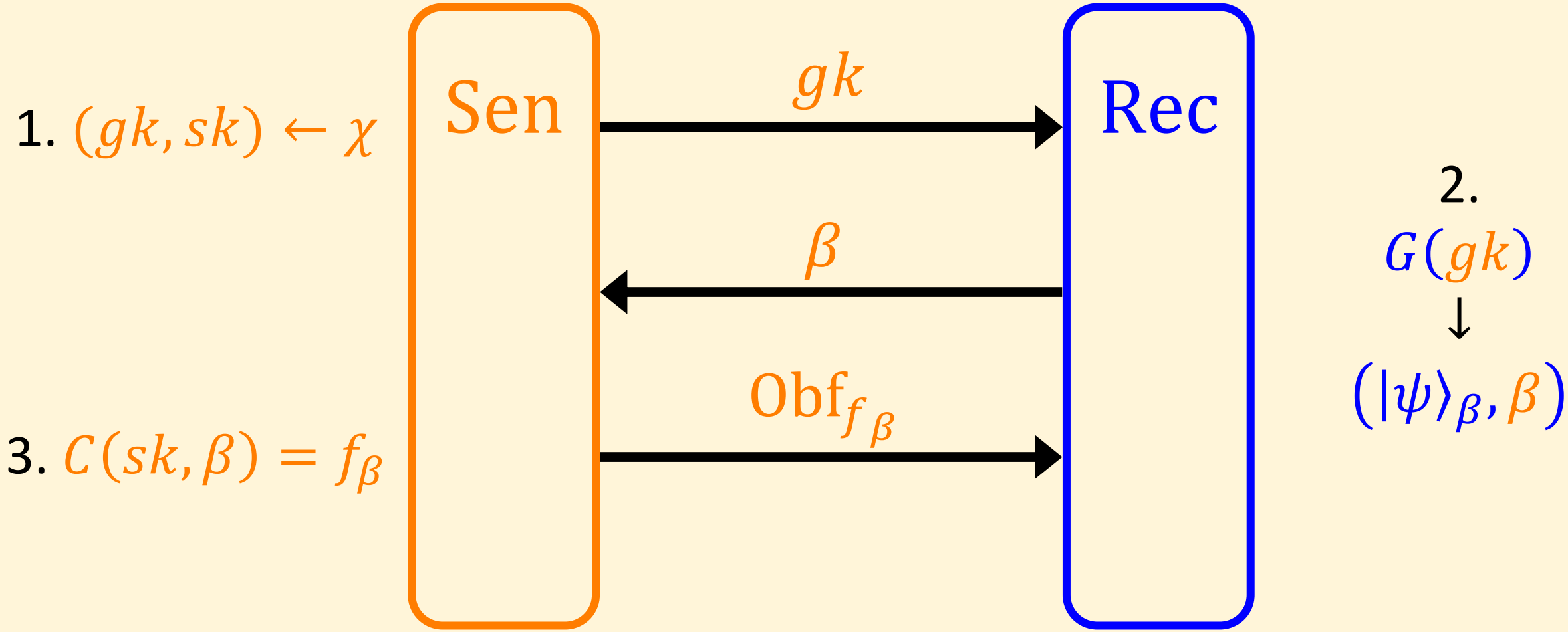
A General Template

Verification:

1. There is an efficient classical computation C: $\forall\beta$: $C(sk,\beta) = f_\beta$. f_β is a classical circuit.
2. $|\psi\rangle_\beta$ can be verified, having quantum oracle access to f_β.

Unclonability: For every β, the state $|\psi\rangle_\beta$ is unclonable, even given gk AND oracle access to f_β.

A General Template



Public-key Semi-quantum Money - Intuition

- We want to implement the template.
- $(gk, sk) \leftarrow \chi$.
- $\left(|\psi\rangle_\beta, \beta\right) \leftarrow G(gk)$.
- $C(sk, \beta) = f_\beta$.

Public-key Semi-quantum Money - Intuition

- We want to implement the template.
- $(gk, sk) \leftarrow \chi$.
- $(|\psi\rangle_\beta, \beta) \leftarrow G(gk)$.
- $C(sk, \beta) = f_\beta$.

Q: What is a <u>minimal but expressive</u> property we need from these?

Public-key Semi-quantum Money - Intuition

- We want to implement the template.
- $(gk, sk) \leftarrow \chi$.
- $\left(|\psi\rangle_\beta, \beta\right) \leftarrow G(gk)$.
- $C(sk, \beta) = f_\beta$.

Q: What is a <u>minimal but expressive</u> property we need from these?

A: Measurement result β <u>must</u> contain entropy.

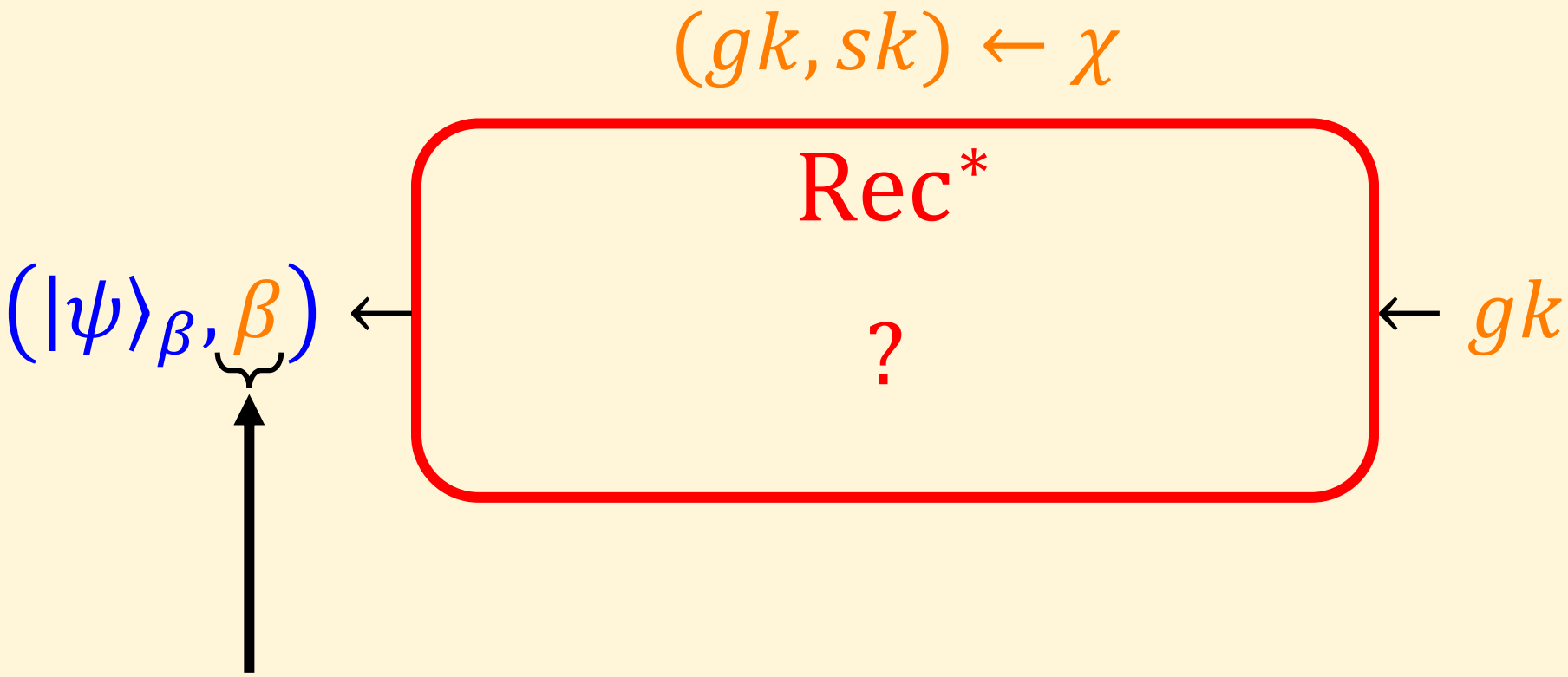
Public-key Semi-quantum Money - Intuition

$$(gk, sk) \leftarrow \chi$$

$$(|\psi\rangle_\beta, \underbrace{\beta}) \leftarrow G(gk)$$

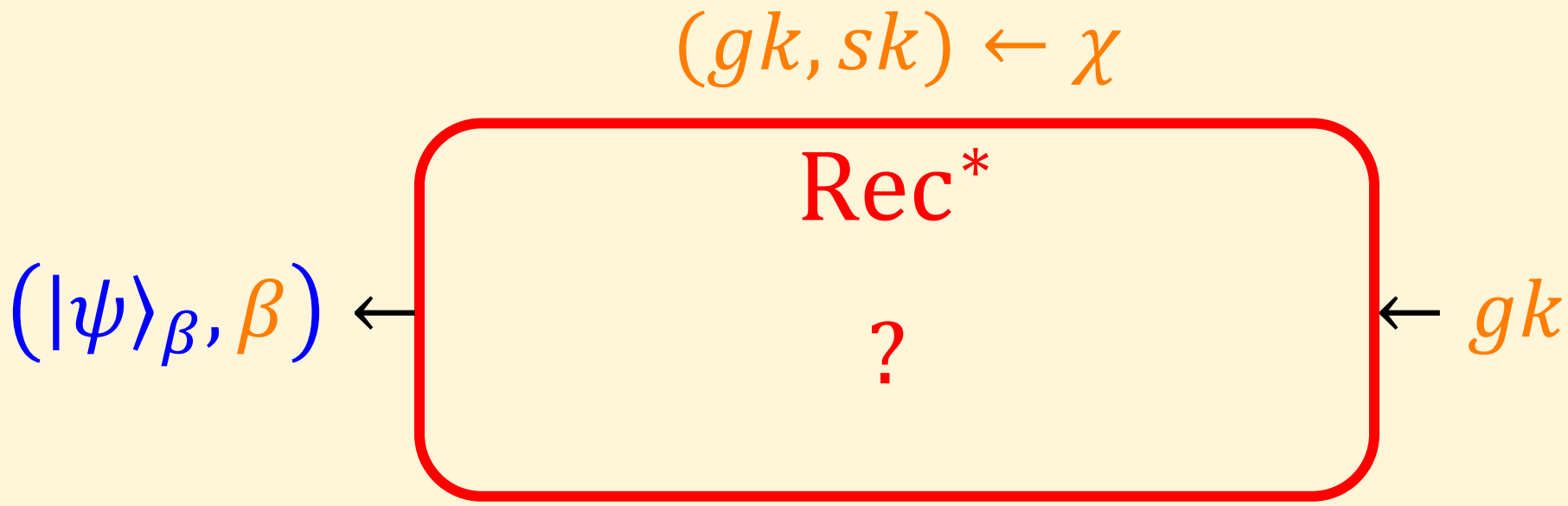
Easy to generate entropy honestly

Public-key Semi-quantum Money - Intuition



Still high-entropy!

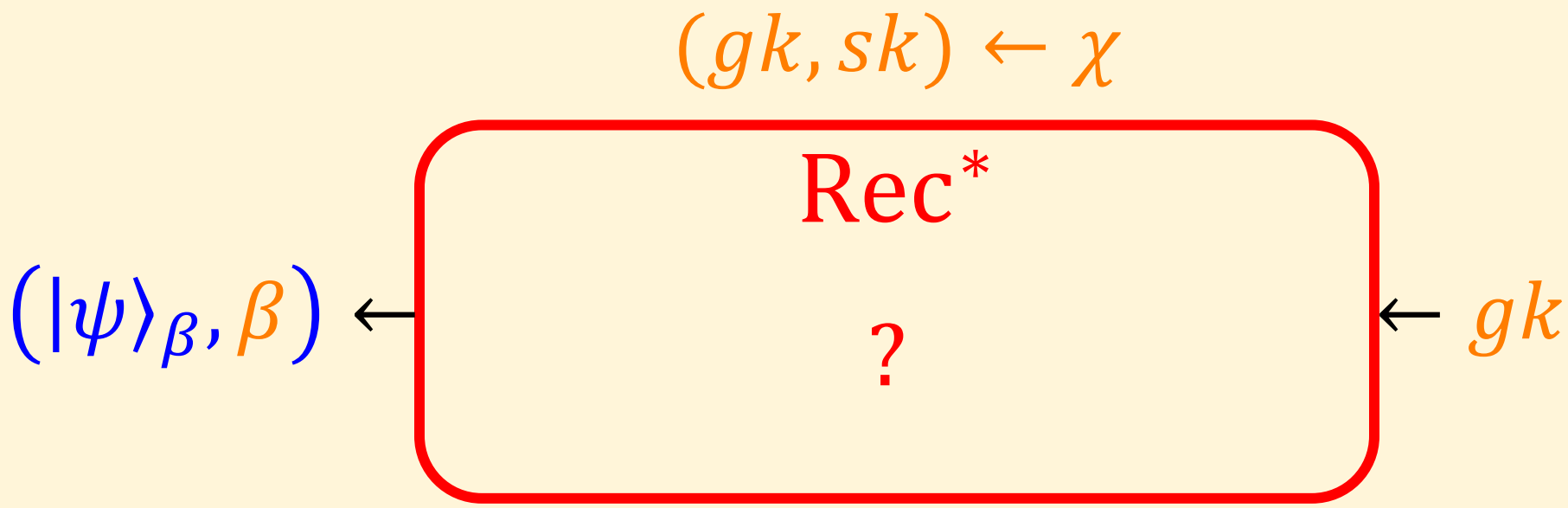
Public-key Semi-quantum Money - Intuition



Q:

We claim that for $|\psi\rangle_\beta$ to be unclonable, the classical part β must have a non-trivial amount of entropy. Why?

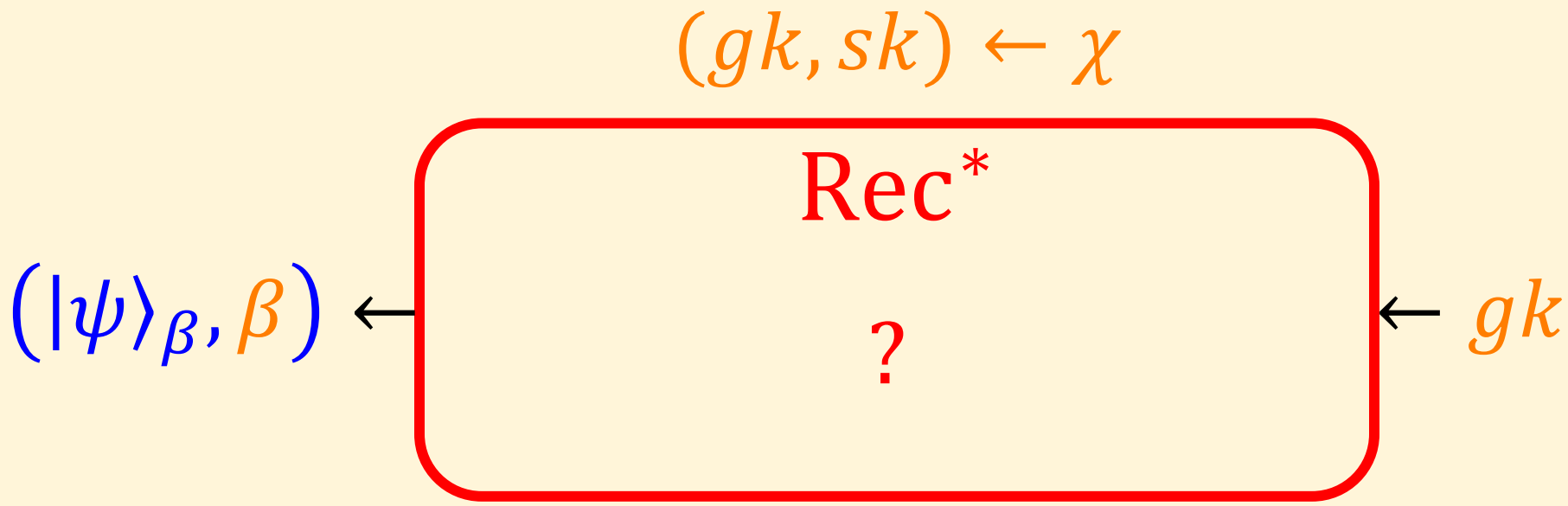
Public-key Semi-quantum Money - Intuition



A:

If some <u>specific</u> β can be sampled with $|\psi\rangle_\beta$, with good probability, then this can be done twice, and we cloned $|\psi\rangle_\beta$ with good probability.

Public-key Semi-quantum Money - Intuition



Meaning:

$|\psi\rangle_\beta$ is a quantum proof for the entropy of β.

Hybrid Quantum Fully-Homomorphic Encryption

[Broadbent-Jeffrey-2015], [Dulek-Schaffner-Speelman-2016], [Mahadev-2018]

Hybrid Quantum Fully-Homomorphic Encryption

[Broadbent-Jeffrey-2015], [Dulek-Schaffner-Speelman-2016], [Mahadev-2018]

- Quantum Fully-Homomorphic Encryption (QFHE):
  - Encryption scheme $(\mathrm{Enc}, \mathrm{Dec}, \mathrm{Eval})$.
  - $\mathrm{Enc}\big(Q(y)\big) \leftarrow \mathrm{Eval}(\mathrm{Enc}(y), Q)$.

- Hybrid QFHE:
  - For every $|\psi\rangle$, $\mathrm{Enc}(|\psi\rangle) := \left(|\psi\rangle^{x,z}, \mathrm{ct}_{x,z}\right)$.
  - $|\psi\rangle^{x,z}$ is the quantum one-time pad encryption of $|\psi\rangle$,

$$|\psi\rangle := \sum_{y\in\{0,1\}^n} \alpha_y \cdot |y\rangle \ ,$$

$$|\psi\rangle^{x,z} := \sum_{y\in\{0,1\}^n} \alpha_y \cdot (-1)^{\langle z,y\rangle} \cdot |x+y\rangle \ .$$

Hybrid Quantum Fully-Homomorphic Encryption

[Broadbent-Jeffrey-2015], [Dulek-Schaffner-Speelman-2016], [Mahadev-2018]

$$\left((y \oplus r, \mathrm{ct}_r), sk\right) \leftarrow \mathrm{Enc}(y)$$

$$\left(Q(y)^{x,z}, \mathrm{ct}_{x,z}\right) \leftarrow \mathrm{Eval}\left((y \oplus r, \mathrm{ct}_r), Q\right)$$

$$(x, z) = \mathrm{Dec}_{sk}(\mathrm{ct}_{x,z})$$

Public-key Semi-quantum Money - Intuition

Observation:

In all Hybrid QFHE constructions we know, the pad-transition $(x, z) \leftarrow r$ is **sometimes randomized**.

Public-key Semi-quantum Money - Intuition

Observation:

In all Hybrid QFHE constructions we know, the pad-transition $(x, z) \leftarrow r$ is **sometimes randomized**.

More precisely: When,

$$\left(Q(y)^{x,z}, \mathrm{ct}_{x,z}\right) \leftarrow \mathrm{Eval}\left((y \oplus r, \mathrm{ct}_r), Q\right)$$

Is executed honestly, the mapping $(x, z) \leftarrow r$ is random for some circuits Q.

Public-key Semi-quantum Money - Intuition

Observation:

In all Hybrid QFHE constructions we know, the pad-transition $(x, z) \leftarrow r$ is **sometimes randomized**.

For example:

- If Q is a Clifford circuit , the mapping is deterministic.
- If Q contains Toffoli gates, the mapping is randomized.

∃ Hybrid QFHE scheme with deterministic pad-transition?

OR,

∃ Q^* where the pad-transition uncontrollably random?

Public-key Semi-quantum Money - Intuition

Why should we care?

∃ Hybrid QFHE scheme with deterministic pad-transition?

OR,

∃ Q^* where the pad-transition uncontrollably random?

Public-key Semi-quantum Money - Intuition

Why should we care? Assume we found such Q^*.

∃ Hybrid QFHE scheme with <u>deterministic</u> pad-transition?

OR,

∃ Q^* where the pad-transition <u>uncontrollably random</u>?

Public-key Semi-quantum Money - Intuition

Why should we care? Assume we found such Q^*.

Public-key Semi-quantum Money - Intuition

Why should we care? Assume we found such Q^*.

We wanted

$$(gk, sk) \leftarrow \chi$$

$$(|\psi\rangle_\beta, \underbrace{\beta}) \leftarrow G(gk)$$

forced entropy

Public-key Semi-quantum Money - Intuition

Why should we care? Assume we found such Q^*.

$$\left((y \oplus r, \mathrm{ct}_r), sk\right) \leftarrow \chi_{QFHE}$$

$$\left(Q^*(y)^{x,z}, \mathrm{ct}_{x,z}\right) \leftarrow \mathrm{Eval}\left((y \oplus r, \mathrm{ct}_r), Q^*\right)$$

Public-key Semi-quantum Money - Intuition

Why should we care? Assume we found such Q^*.

$$\left((y \oplus r, \mathrm{ct}_r), sk\right) \leftarrow \chi_{QFHE}$$

$$(\quad gk \quad , sk) \leftarrow \chi$$

$$\left(Q^*(y)^{x,z}, \mathrm{ct}_{x,z}\right) \leftarrow \mathrm{Eval}\left((y \oplus r, \mathrm{ct}_r), Q^*\right)$$

$$(\quad |\psi\rangle_\beta \quad , \quad \beta \quad) \leftarrow \quad G(\quad gk \quad)$$

Public-key Semi-quantum Money - Intuition

Why should we care? Assume we found such Q^*.

$$\left((y \oplus r, \mathrm{ct}_r), sk\right) \leftarrow \chi_{QFHE}$$

$$(\quad gk \quad , sk) \leftarrow \chi$$

$$\left(Q^*(y)^{x,z}, \mathrm{ct}_{x,z}\right) \leftarrow \mathrm{Eval}\left((y \oplus r, \mathrm{ct}_r), Q^*\right)$$

$$(\quad |\psi\rangle_\beta \quad , \quad \beta \quad) \leftarrow \quad G(\quad gk \quad)$$

If the pad (x, z) must be randomized, so is $\mathrm{ct}_{x,z} = \beta$!

Public-key Semi-quantum Money - Intuition

Why should we care? Assume we found such Q^*.

$$\left((y \oplus r, \mathrm{ct}_r), sk\right) \leftarrow \chi_{QFHE}$$

$$\left(Q^*(y)^{x,z}, \mathrm{ct}_{x,z}\right) \leftarrow \mathrm{Eval}\left((y \oplus r, \mathrm{ct}_r), Q^*\right)$$

If the pad (x, z) must be randomized, so is $\mathrm{ct}_{x,z} = \beta$!

Public-key Semi-quantum Money - Intuition

We define a quantum **Subspace-Generating Circuit (SGC)** to be a circuit Q_{SG} that maps:

$$\forall \text{ subspace } S \subseteq \{0,1\}^n \text{ and basis } M_S \text{ ,}$$
$$Q_{SG}(M_S) = |S\rangle \text{ .}$$

Public-key Semi-quantum Money - Intuition

Hybrid QFHE and **Subspace-Generating Circuits (SGC)** are synergetic in two ways:

1. When a SGC is homomorphically evaluated, the resulting state is unclonable (the pad x', z' must contain entropy).
2. Subspace states were known to be publicly verifiable. However, due to the structure of Hybrid QFHE, even an encrypted subspace state is publicly verifiable.

Homomorphic Evaluation of SGC Generates Unclonable States

Homomorphic Evaluation of SGC Generates Unclonable States

$$M_S \leftarrow \text{random subspace } S \subseteq \{0,1\}^n$$

$$(M_S \oplus r, \mathrm{ct}_r) \leftarrow \mathrm{Enc}(M_S)$$

Homomorphic Evaluation of SGC Generates Unclonable States

$$M_S \leftarrow \text{random subspace } S \subseteq \{0,1\}^n$$

$$(M_S \oplus r, \mathrm{ct}_r) \leftarrow \mathrm{Enc}(M_S)$$

$$\mathrm{A}^*$$

$$\left(|S\rangle^{x,z}, \mathrm{ct}_{x,z}\right) \leftarrow \mathrm{Eval}\left((M_S \oplus r, \mathrm{ct}_r), Q_{SG}\right)$$

Homomorphic Evaluation of SGC Generates Unclonable States

$$M_S \leftarrow \text{random subspace } S \subseteq \{0,1\}^n$$

$$(M_S \oplus r, \mathrm{ct}_r) \leftarrow \mathrm{Enc}(M_S)$$

$$\mathrm{A}^*$$

$$\underbrace{(|S\rangle^{x,z}}, \mathrm{ct}_{x,z}) \leftarrow \mathrm{Eval}\big((M_S \oplus r, \mathrm{ct}_r), Q_{SG}\big)$$

Unclonable!

Homomorphic Evaluation of SGC Generates Unclonable States

Lemma (informal):

Let S a random subspace $S \subseteq \{0,1\}^n$ of dimension $\frac{n}{2}$.

Let $M_S \in \{0,1\}^{\left(\frac{n}{2}\times n\right)}$ a basis for S.

Then, no quantum polynomial-time A^* can get $(M_S \oplus r, \mathrm{ct}_r)$ an encryption by $\mathrm{Enc}(M_S)$, and output,

$$\left(|S\rangle^{x,z}, |S\rangle^{x,z}, \mathrm{ct}_{x,z}\right),$$

For some x, z.

Homomorphic Evaluation of SGC Generates Unclonable States

Proof:

- Let $M_S \in \{0,1\}^{\left(\frac{n}{2}\times n\right)}$ a basis for a random subspace $S \subseteq \{0,1\}^n$, $\dim(S) = \frac{n}{2}$.
- Assume a quantum poly-time A^*, gets an encryption $(M_S \oplus r, \mathrm{ct}_r)$ and outputs,

$$\left(|S\rangle^{x,z}, |S\rangle^{x,z}, \mathrm{ct}_{x,z}\right).$$

- Observe: S takes negligible fraction $\frac{2^{\frac{n}{2}}}{2^n} = 2^{-\frac{n}{2}}$ from $\{0,1\}^n$. By security of QFHE, computationally hard to find $s \in (S \setminus \{0\})$.

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

- How can the reduction use $\left(|S\rangle^{x,z}, |S\rangle^{x,z}, \mathrm{ct}_{x,z}\right)$ to find a vector $s \in (S \setminus \{0\})$?

1. Measure one copy: get $v + x \leftarrow |S\rangle^{x,z}$, for $v \in S$.
2. Add $v + x$ to the other superposition:

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

2. Add $v + x$ to the other superposition:

$$C_{v+x}(|S\rangle^{x,z})$$

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

2. Add $v + x$ to the other superposition:

$$C_{v+x}(|S\rangle^{x,z})$$

$$= C_{v+x}\left(\sum_{u\in S}(-1)^{\langle z,u\rangle}|x+u\rangle\right)$$

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

2. Add $v + x$ to the other superposition:

$$C_{v+x}(|S\rangle^{x,z})$$

$$= C_{v+x}\left(\sum_{u\in S}(-1)^{\langle z,u\rangle}|x+u\rangle\right)$$

$$= \sum_{u\in S}(-1)^{\langle z,u\rangle}|x+x+v+u\rangle$$

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

2. Add $v + x$ to the other superposition:

$$= \sum_{u \in S} (-1)^{\langle z,u \rangle} |x + x + v + u\rangle$$

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

2. Add $v + x$ to the other superposition:

$$= \sum_{u \in S} (-1)^{\langle z,u \rangle} |x + x + v + u\rangle$$

On one hand, string shift cancels

$$= \sum_{u \in S} (-1)^{\langle z,u \rangle} |v + u\rangle$$

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

2. Add $v + x$ to the other superposition:

$$= \sum_{u \in S} (-1)^{\langle z,u \rangle} |x + x + v + u\rangle$$

On one hand, string shift cancels

$$= \sum_{u \in S} (-1)^{\langle z,u \rangle} |v + u\rangle$$

$$= \sum_{u \in S} (-1)^{\langle z,u \rangle} |u\rangle$$

On the other hand, Subspace undisturbed!

Homomorphic Evaluation of SGC Generates Unclonable States

Proof (continued):

- Finally, measuring $\sum_{u \in S}(-1)^{\langle z,u \rangle}|u\rangle$ yields $s \in (S \setminus \{0\})$ with high probability.
- This in contradiction to the security of the hybrid QFHE.

■

Public-key Semi-quantum Money - Intuition

Hybrid QFHE and **Subspace-Generating Circuits (SGC)** are synergetic in two ways:

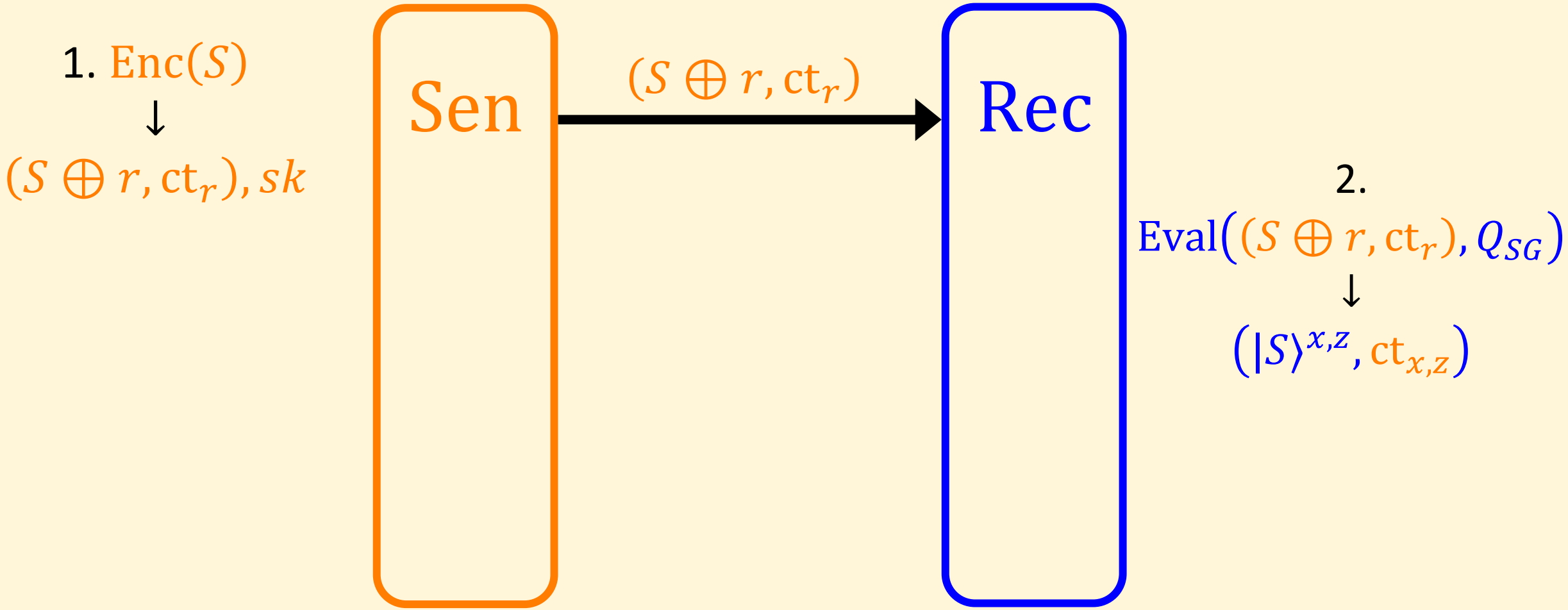
1. When a SGC is homomorphically evaluated, the resulting state is unclonable (the pad x', z' must contain entropy).
2. Subspace states were known to be publicly verifiable. However, due to the structure of Hybrid QFHE, even an encrypted subspace state is publicly verifiable.

Public-key Semi-quantum Money - Intuition

Hybrid QFHE and **Subspace-Generating Circuits (SGC)** are synergetic in two ways:

1. When a SGC is homomorphically evaluated, the resulting state is unclonable (the pad x', z' must contain entropy).
2. Subspace states were known to be publicly verifiable. However, due to the structure of Hybrid QFHE, even an encrypted subspace state is publicly verifiable.

Encrypted Subspace State Verification



How to verify $|S\rangle^{x,z}$?

Encrypted Subspace State Verification

[Aaronson-Christiano-2012]:

Given quantum oracle access to membership for S and $S^{\perp}$, the state $|S\rangle$ can be verified.

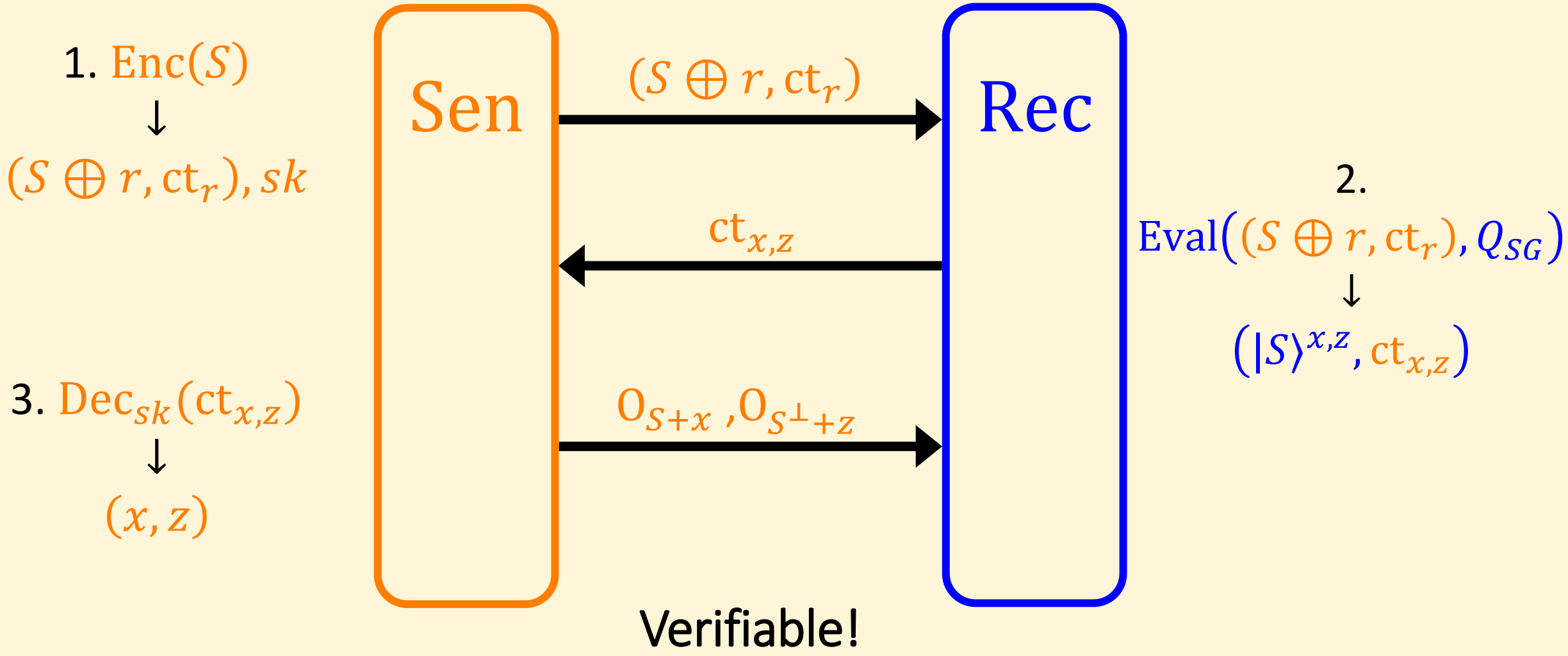
- We want to verify the encrypted $|S\rangle^{x,z}$.

Encrypted Subspace State Verification

Hybrid QFHE is useful in two ways for our verification:

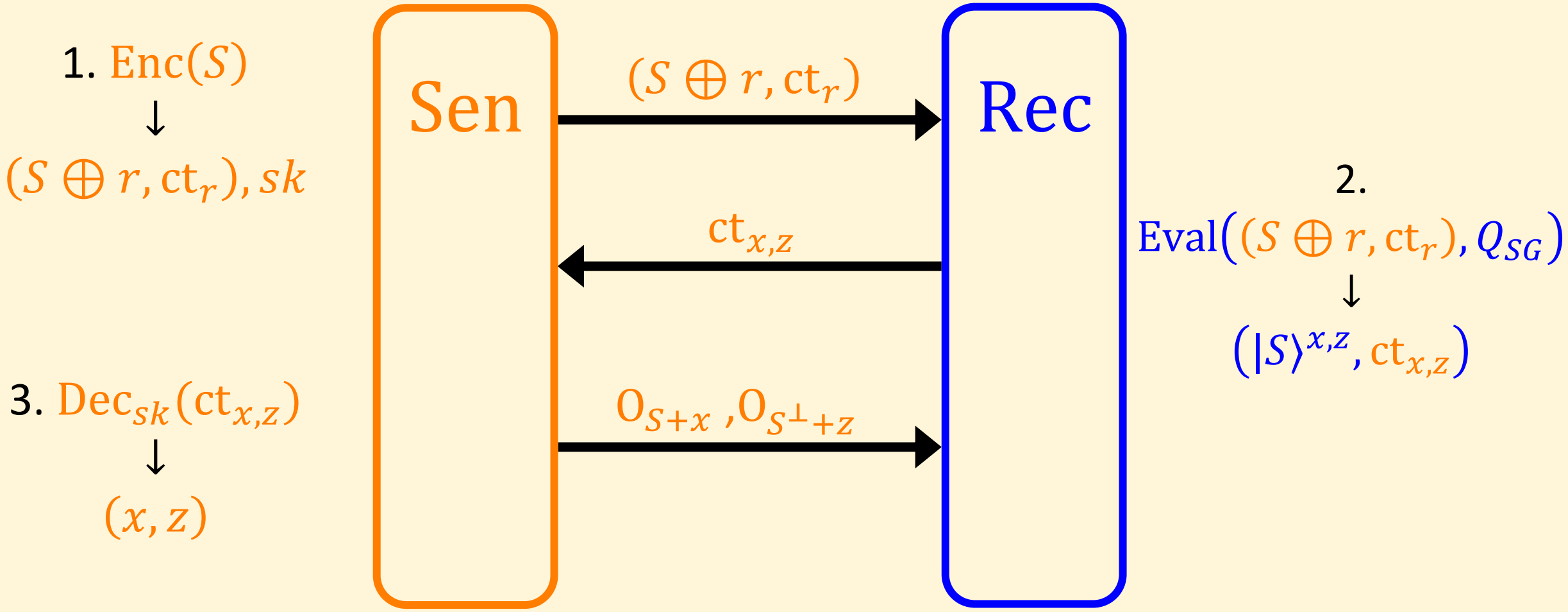
1. By the exact same techniques from [AC-12], the state $|S\rangle^{x,z}$ can be verified with quantum oracle access to membership in $S + x$ and $S^{\perp} + z$.
2. Even though x, z randomly distribute, the sender can know the pads by decrypting the message of the receiver.

Encrypted Subspace State Verification



Verifiable!

Encrypted Subspace State Verification



Additional hurdles – in [S-2021]

Two Open Problems

1. **Reduce assumptions:** Can we construct PKQM from non-iO assumptions? Possibly lattice-based?
2. **Increase functionality:** Can we make semi-quantum schemes non-interactive? This will imply *Quantum Lightning* [Zhandry-2018] or even *One-Shot Signatures* [Amos-Georgiou-Kiayias-Zhandry-2020].