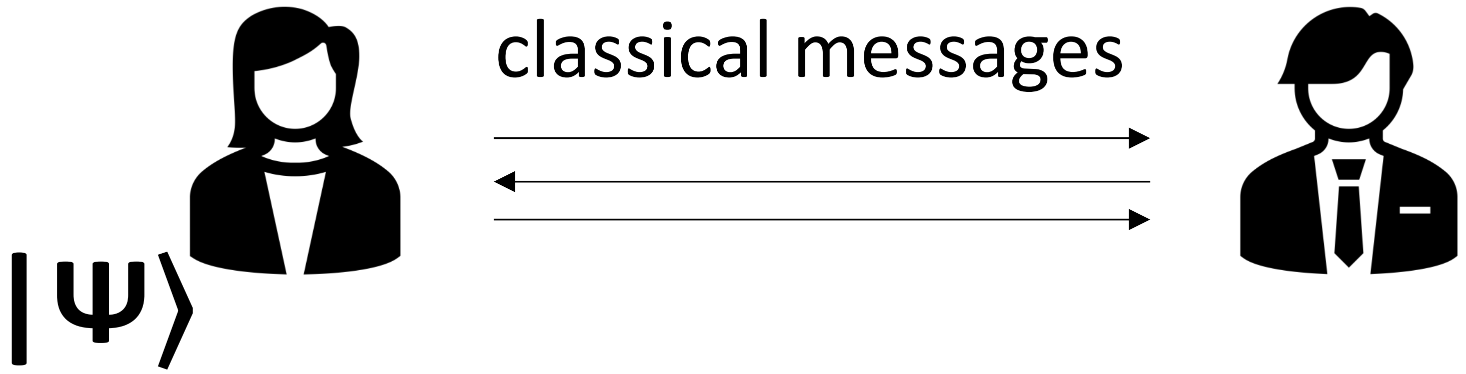
One-Shot Signatures

Mark Zhandry (NTT Research & Stanford University)

Based on joint works with Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Omri Shmueli

Question 1

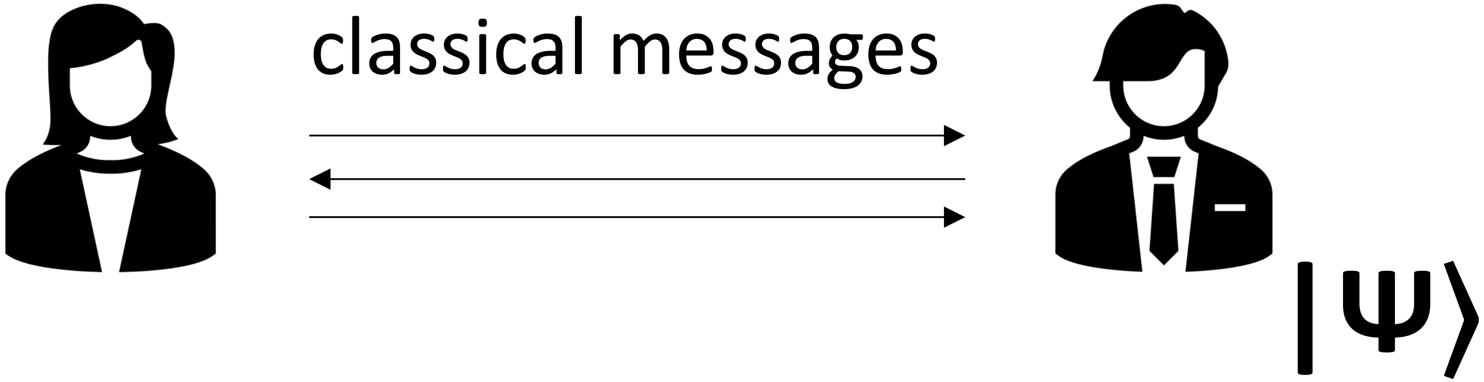
Can you send “inherently quantum” states with classical communication?



No pre-shared entanglement!!!

Question 1

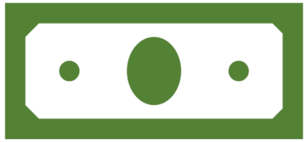
Can you send “inherently quantum” states with classical communication?



No pre-shared entanglement!!!

Question 1

Example: quantum money [Wiesner'70]

 $= \quad |\Psi\rangle$

Unforgeability derives from unclonability of quantum states

Can you send quantum money with classical communication?

Question 1

Information theory: *impossible!*

Family of states $\{|\Psi_i\rangle\}_i$ can be "telegraphed" if and only if orthogonal

+

Can rotate orthogonal states $\{|\Psi_i\rangle\}_i$ into computational basis states $\{|i\rangle\}_i$

⬇

Corollary: cannot telegraph "inherently quantum" states

Question 1

Complexity theory: all bets are off

Orthogonality does not imply *efficient* telegraphing

Orthogonality dos not imply *efficient* transformation into classical states

Still some barriers, e.g. cannot be used to establish entanglement

Question 1

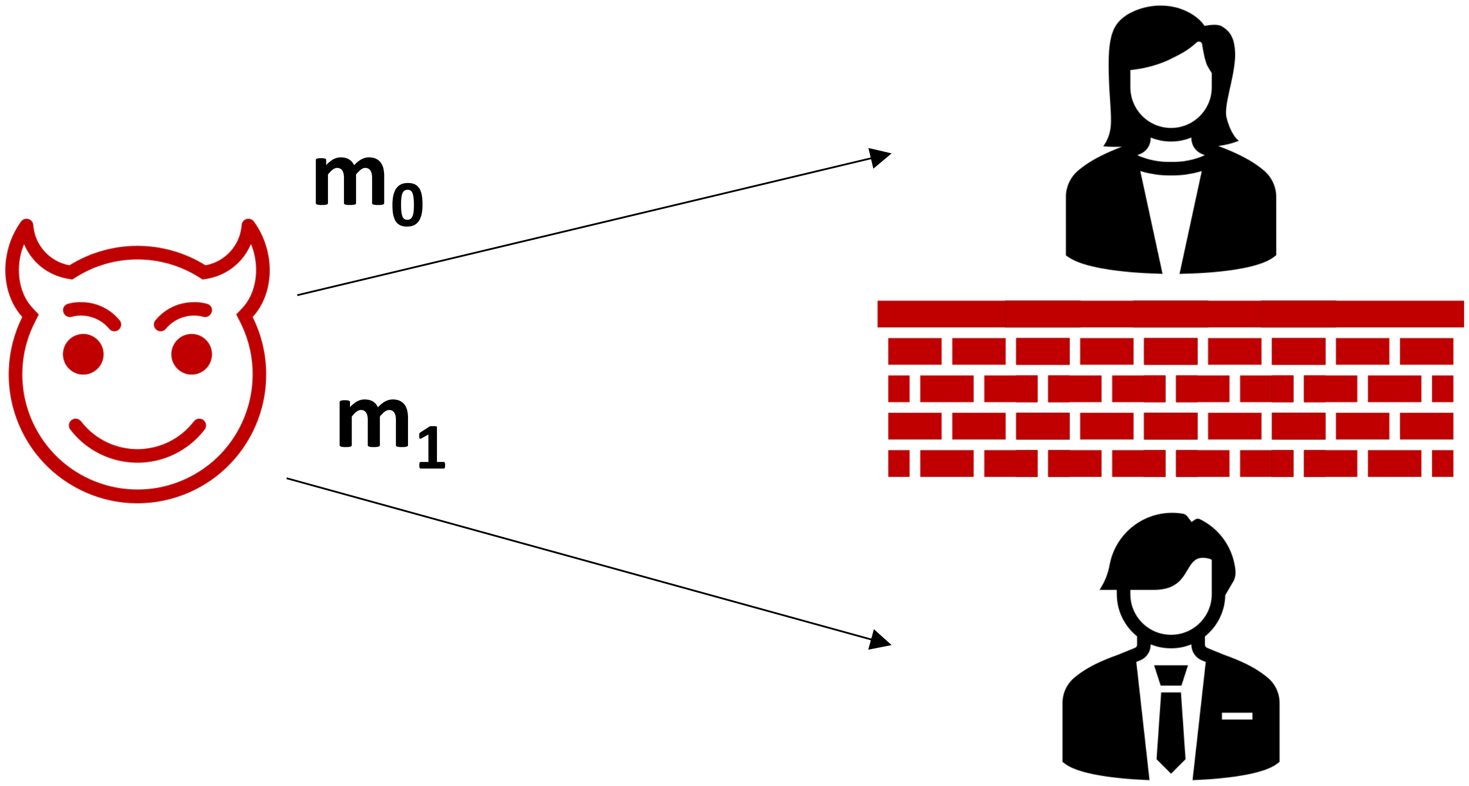
Many prior works on LOCC model, but
none directly address this question

Quantum teleportation + friends: *Needs pre-shared entanglement*

Complexity-theoretic remote state preparation: *Alice knows state*

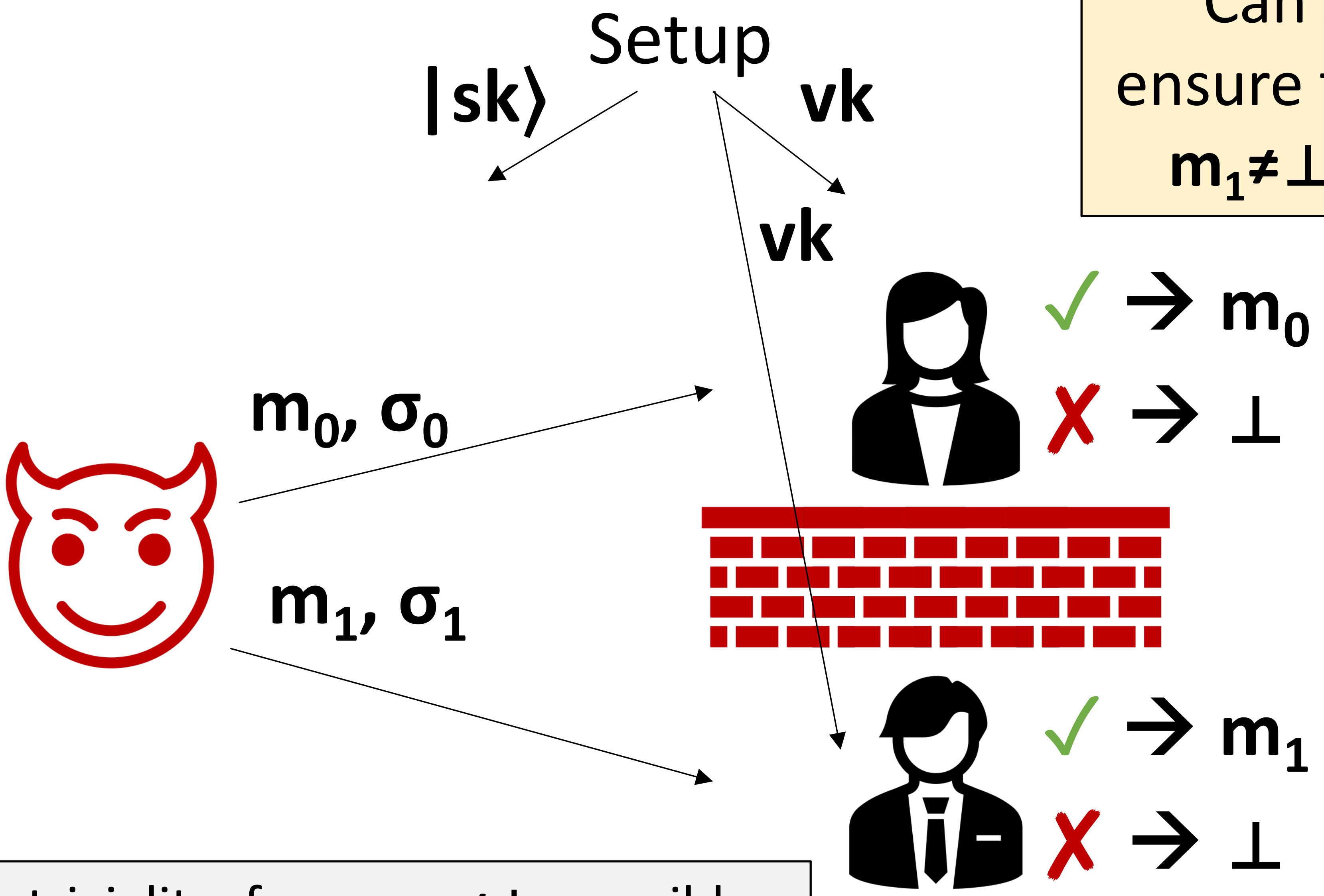
Question 2

Can Alice and Bob ensure that $\mathbf{m_0} = \mathbf{m_1}$ without any communication



Question 2

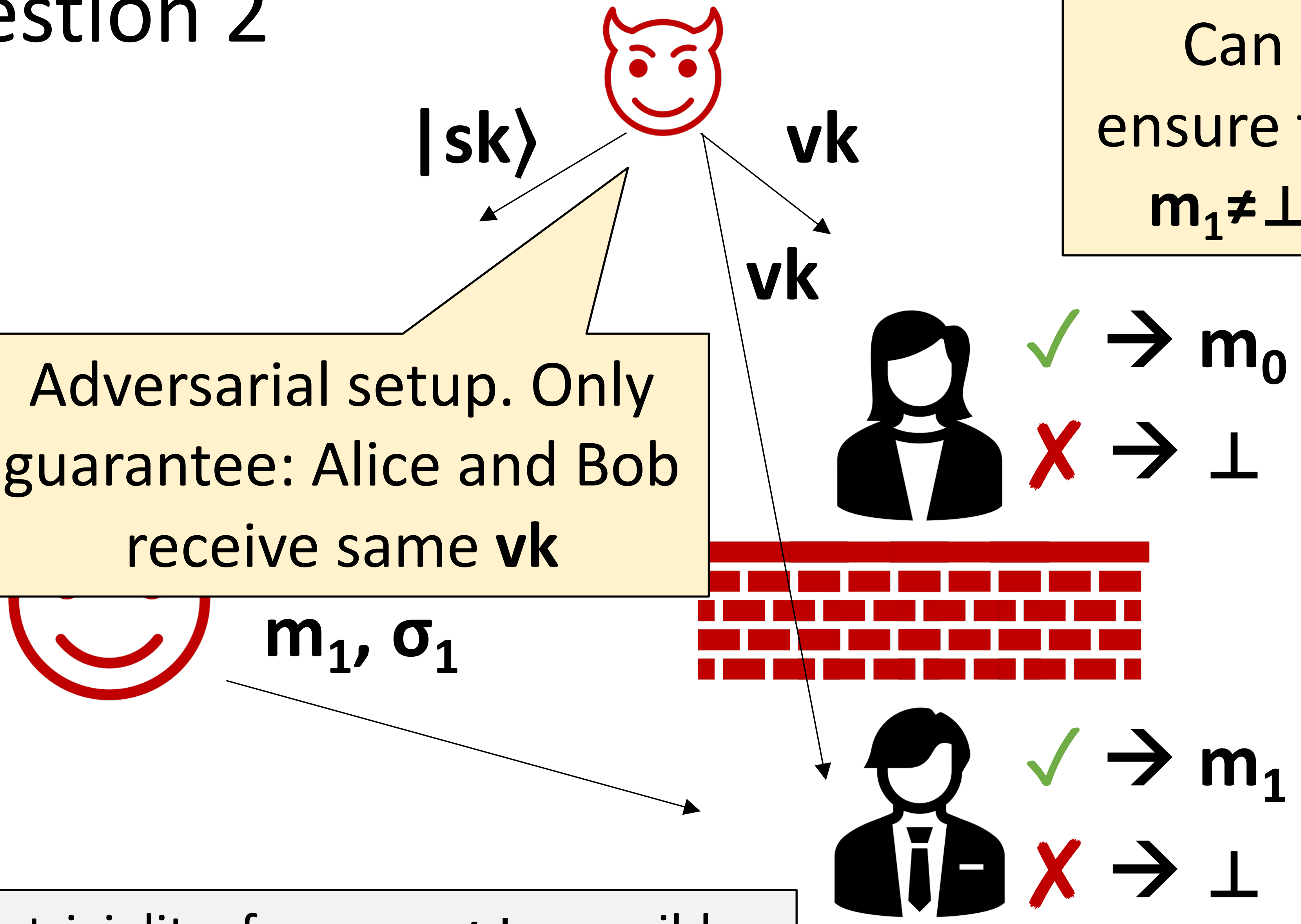
Can Alice and Bob ensure that if $\mathbf{m_0} \neq \perp$ and $\mathbf{m_1} \neq \perp$, then $\mathbf{m_0} = \mathbf{m_1}$



Non-triviality: for any $\mathbf{m} \neq \perp$, possible adversary to send $\mathbf{m_0} = \mathbf{m_1} = \mathbf{m}$

Question 2

Can Alice and Bob ensure that if $\mathbf{m_0} \neq \perp$ and $\mathbf{m_1} \neq \perp$, then $\mathbf{m_0} = \mathbf{m_1}$



Adversarial setup. Only guarantee: Alice and Bob receive same **vk**

Non-triviality: for any $\mathbf{m} \neq \perp$, possible adversary to send $\mathbf{m_0} = \mathbf{m_1} = \mathbf{m}$

Question 2

Information theory: *impossible!*

Non-triviality ➡ $\forall \mathbf{m}, \exists$ valid $\boldsymbol{\sigma}$

An inefficient adversary can choose arbitrary $\mathbf{m_0 \neq m_1}$, brute-force the appropriate $\boldsymbol{\sigma_0}$, $\boldsymbol{\sigma_1}$, and send $\mathbf{(m_0, \sigma_0)}$, $\mathbf{(m_1, \sigma_1)}$ to Alice and Bob, resp.

Question 2

Classical complexity theory: *impossible!*

Non-triviality ➡ $\boldsymbol{\sigma}$ efficiently computable from **sk,m**

An efficient adversary can choose arbitrary $\mathbf{m_0 \neq m_1}$, compute $\boldsymbol{\sigma_0}$, $\boldsymbol{\sigma_1}$ using **sk**, and send $\mathbf{(m_0, \sigma_0)}$, $\mathbf{(m_1, \sigma_1)}$ to Alice and Bob, resp.

Question 2

Quantum complexity theory: all bets are off

Non-triviality ➡ **σ** efficiently computable from **$|sk\rangle$,m**

But, computing **σ_0, σ_1** from **$|sk\rangle$** involves measurements that may not commute. Computing **σ_0** may destroy **$|sk\rangle$**, preventing computing **σ_1**

Question 2

Solution = "One-shot Signature"
[Amos-Georgiou-Kiayias-**Z**'20]

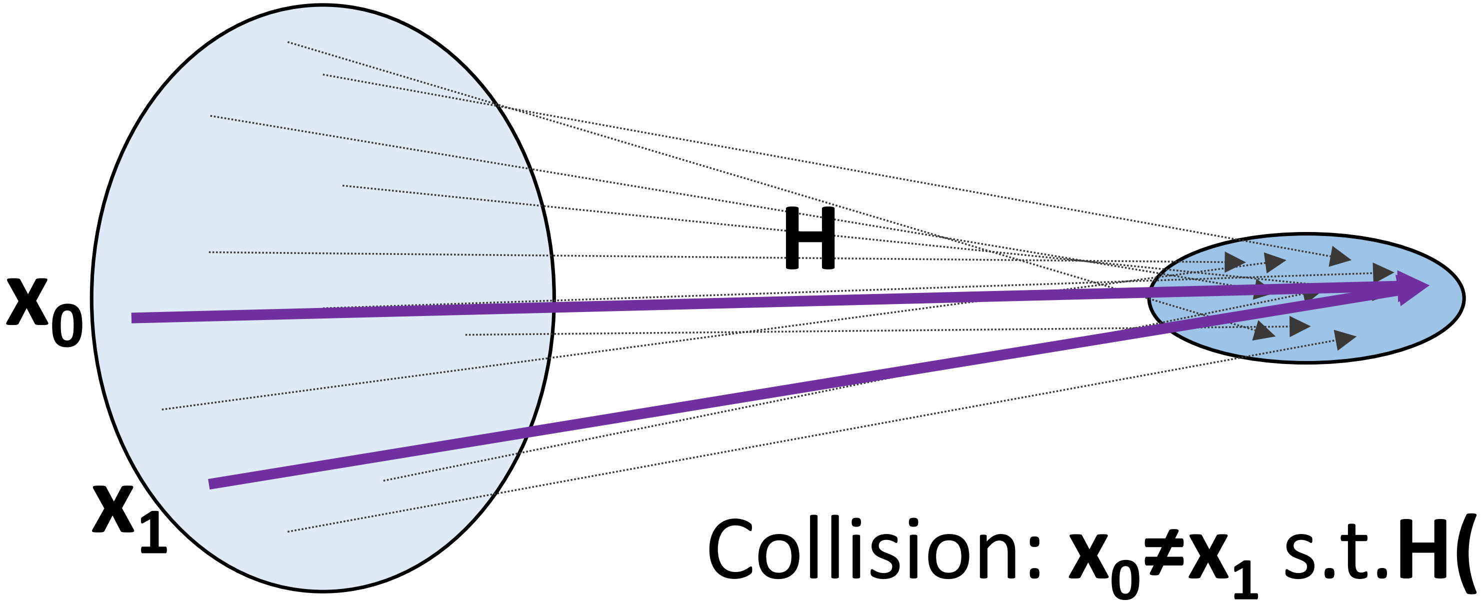
Numerous applications:

- Smart contracts without blockchain [Sattath'22]
- Overcoming lower-bounds in consensus protocols [Drake'24]
- *Sending quantum money with classical communication*
- …

However, unclear a priori if OSS could even exist

Question 3

Cryptographic hash functions



Collision: $\mathbf{x_0 \neq x_1}$ s.t. $\mathbf{H(x_0)=H(x_1)}$

Pigeonhole principle: ∃ many collisions

Collision resistance: computationally infeasible to find them

Question 3

Coin tossing from hash functions

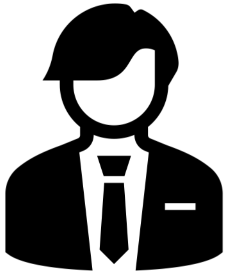
$b_A \leftarrow \{0,1\}$

$r \leftarrow \$$

$h = H(b_A, r)$ $\longrightarrow$

$\longleftarrow$ b_B

b_A, r $\longrightarrow$



$b_B \leftarrow \{0,1\}$

Verify $h == H(b_A, r)$

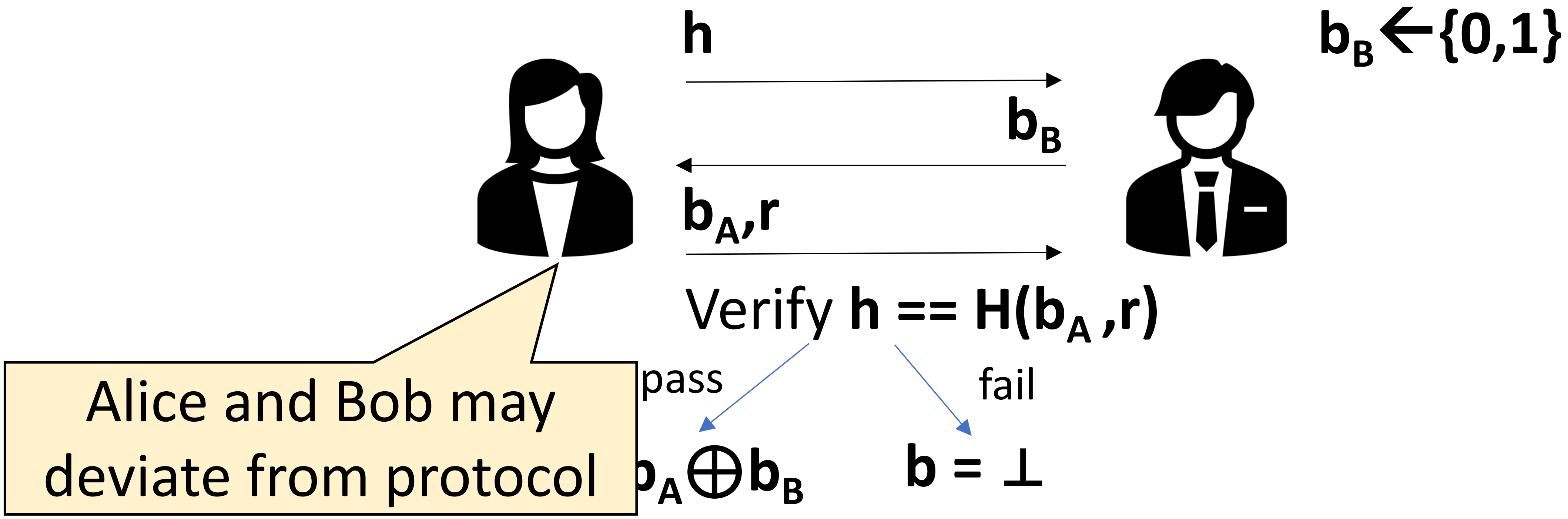
pass: $b = b_A \oplus b_B$

fail: $b = \perp$

Alice wants $\mathbf{Pr[b=0] > ½+ε}$ Bob wants $\mathbf{Pr[b=1] > ½-ε}$

Question 3

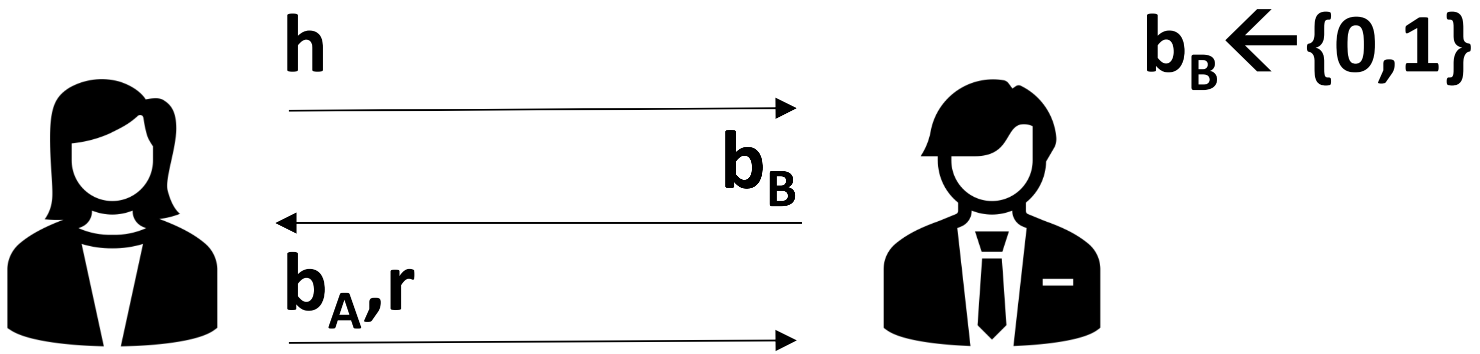
Coin tossing from hash functions



Alice wants **Pr[b=0] > ½+ε** Bob wants **Pr[b=1] > ½-ε**

Question 3

Coin tossing from hash functions



Crucially uses that **H** is many-to-1

Thm: can assume that **h** is (statistically close to) independent of $\mathbf{b_A}$

→ If Alice honest, no matter what Bob does, $\mathbf{Pr[b=1]} \lesssim$ ½

Question 3

Breaks security against Bob

Thm: if **H** injective, then no matter what Alice does, **Pr[b=0] ≤ ½**

Proof: **h** perfectly commits Alice to $\mathbf{b_A}$, which is chosen independently of $\mathbf{b_B}$ → $\mathbf{b = b_A \oplus b_B}$ is uniform

Thm: if **H** is collision-resistant against *classical* adversaries, then no matter what a *classical* Alice does, **Pr[b=0]** $\lesssim$ **½**

Proof: **Pr[b=0] > ½+ε**, Alice must be able "open" **c** to both $\mathbf{b_A = 0}$ and $\mathbf{b_A = 1}$ → Opening **c** both ways gives a collision → intractable!

Question 3

What about quantum?

Producing **$(0,r_0)$** and **$(1,r_1)$** may involve non-commuting measurements of Alice's state

Alice may be able to "open" to both **0** and **1**, but be unable to do both *simultaneously*

[van de Graaf'97,Ambainis-Rosmanis-Unruh'14,Unruh'16]

Does collision-resistance nevertheless justify coin tossing quantumly?

Question 3

Importance: similar arguments used extensively in e.g. signature schemes, a crucial part of a secure internet

When transitioning to a quantum world, we will upgrade building blocks (e.g. hash functions) with post-quantum version. Will the resulting schemes then be post-quantum secure?

Let’s answer the questions in reverse order…

Equivocal hash functions

Thm [Ambainis-Rosmanis-Unruh’14,Unruh’16]:
∃ (quantum) collision-resistant **H** s.t. Alice has a near-perfect strategy (aka **H** is equivocal) ***relative to a quantum oracle***

Proof idea: start with random compressing function **H**

[Aaronson-Shi’04, Yuen’13, **Z**’15]: **H** is collision-resistant

[Unruh’16]: but **H** is also secure in coin-tossing!

Thm [Ambainis-Rosmanis-Unruh'14,Unruh'16]:
∃ (quantum) collision-resistant **H** s.t. Alice has a near-perfect strategy (aka **H** is equivocal) ***relative to a quantum oracle***

Proof idea: start with random compressing function **H**

Additionally supply, for each image **h**, the oracle $\mathbf{U_h}$ which reflects about

$$|\Psi_h\rangle = \sum_{b,r:H(b,r)=h} |b,r\rangle$$

Thm [Ambainis-Rosmanis-Unruh'14,Unruh'16]:
∃ (quantum) collision-resistant **H** s.t. Alice has a near-perfect strategy (aka **H** is equivocal) ***relative to a quantum oracle***

Proof idea: Breaking coin tossing (equivocating):

Initialize $|\boldsymbol{\Psi}\rangle = \sum_{\mathbf{b,r}} |\mathbf{b,r}\rangle$

Measure $\mathbf{H(b,r)} \rightarrow \mathbf{h}$

Keep collapsed state $|\boldsymbol{\Psi}_{\mathbf{h}}\rangle$

$\xrightarrow{\mathbf{h}}$

Thm [Ambainis-Rosmanis-Unruh'14,Unruh'16]:
∃ (quantum) collision-resistant **H** s.t. Alice has a near-perfect strategy (aka **H** is equivocal) ***relative to a quantum oracle***

Uses $\mathbf{U_h}$

Proof idea: B n tossing (equivocating):

Amplitude amplification

$$|\Psi_h\rangle \Rightarrow |\Psi_{h,b}\rangle = \sum_{r:H(b,r)=h} |b,r\rangle$$

Measure → **b,r**

$\xleftarrow{\mathbf{b}}$

$\xrightarrow{\mathbf{b,r}}$

Thm [Ambainis-Rosmanis-Unruh'14,Unruh'16]:
∃ (quantum) collision-resistant **H** s.t. Alice has a near-perfect strategy (aka **H** is equivocal) ***relative to a quantum oracle***

Proof idea:

Possible to show that $\mathbf{U_h}$ doesn't break collision-resistance of **H**

Intuition: $\mathbf{U_h}$ enables amplitude amplification, but doesn't give any obvious way to actually construct a second pre-image

Is there a *classical* oracle “separation”?

Is there an *oracle-free* separation?

(using computational assumptions)

Thm [Amos-Georgiou-Kiayias-Z'20]:
∃ (quantum) collision-resistant **H** s.t. Alice has a near-perfect strategy (aka **H** is equivocal) *relative to a classical oracle*

Fatal bug in the proof [Bartusek]

Note: no attack on construction

Thm [Shmueli-**Z**'25]: ∃ (quantum) collision-resistant **H** s.t. Alice has a near-perfect strategy (aka **H** is equivocal) ***relative to a classical oracle***, or ***without oracles assuming*** (somewhat accepted post-quantum) ***cryptographic assumptions***

Proof idea from [AGKZ'20]: Simulate $\mathbf{U_h}$ with classical oracle

Set **H** to be *coset partition function:* pre-image set of each image **h** is large-ish affine subspace $\mathbf{S_h}$

Provide additional oracle **Q(h,y):** test for membership in $\mathbf{S_h}^\perp$

Proof idea from [AGKZ'20]: Simulate $\mathbf{U_h}$ with classical oracle

Can project onto $$|\boldsymbol{\Psi_h}\rangle = \sum_{\mathbf{b,r:H(b,r)=h}} |\mathbf{b,r}\rangle$$ (equivalent to reflection)

- Use **H** to test that support is on preimages of **h**
- Apply **QFT**
- Use **Q** to test for membership in $\mathbf{S_h}^\perp$
- [Aaronson-Christiano'12]: $|\boldsymbol{\Psi_h}\rangle$ is the only state passing verification

Problem with [AGKZ'20] construction:

- Extra structure due to **H** being coset partition function
- Oracle **Q** potentially provides more information than $\mathbf{U_h}$

⬇

Need new arguments to prove collision resistance of **H**

Unfortunately, our proof was fatally flawed,
though I still think the construction works

A slightly different construction (based on idea of James Bartusek):

Leave **H** unstructured, though assume all pre-image sets have size $\mathbf{2^r}$

For each **h**, choose random affine subspace $\mathbf{S_h}$ such that $|\mathbf{S_h}|$ = #(preimages of **h**)

In completely different universe

Provide 2 additional oracles:

- **P(b,r):** random bijection with $\mathbf{S_h}$ where **h=H(b,r)**
- **Q(h,y):** test for membership in $\mathbf{S_h}^\perp$

A slightly different construction (based on idea of James Bartusek):

- **P(b,r):** random bijection with $\mathbf{S_h}$ where $\mathbf{h=H(b,r)}$
- **Q(h,y):** test for membership in $\mathbf{S_h}^{\perp}$

⬇

Can still project onto $|\Psi_h\rangle$ by using **P** to map to $\mathbf{S_h}$

Now **H** has less structure, so maybe easier.
Though still a priori not obvious how to prove

Proof idea (oracle setting): Need to prove that **P,Q** don't break collision-resistance

Use *random self-reduction*

Overly simplified view of proof:

Step 1: Reduce to case without **Q**

Step 2: Reduce to *worst-case* collision-resistance of many-to-1 coset partition function (CPFs)

Step 3: Worst-case CPFs are collision-resistant

2-to-1 funcs are automatically CPFs
→ Parallel repetition to get many-to-1

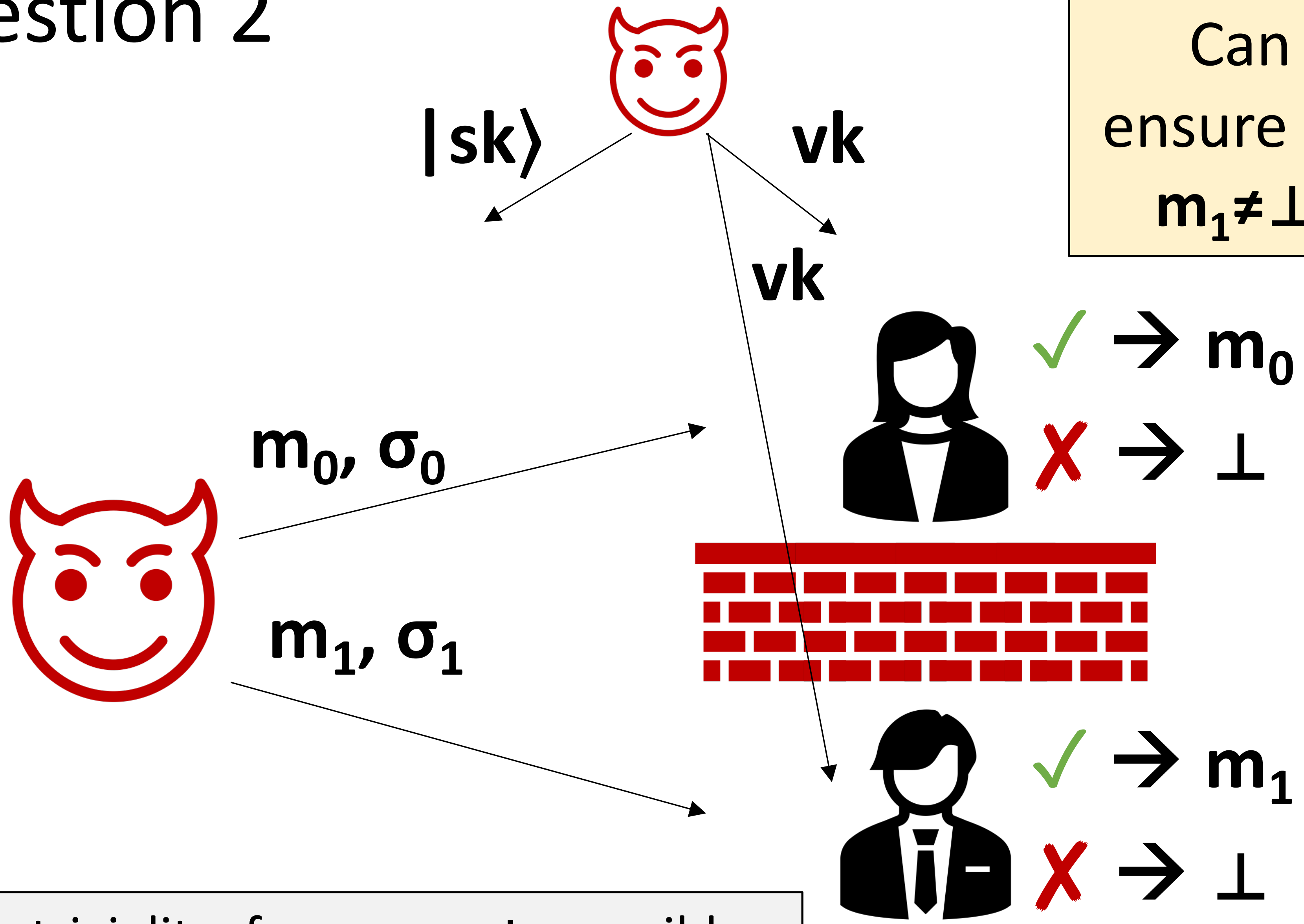
Proof idea (oracle-free setting):

- Instantiate random choices with pseudorandom functions / permutations
- Instantiate oracles **P,Q** with *indistinguishability obfuscation* (iO)
- Replace each step in proof with cryptographic step

Requires interesting new techniques for obfuscating pseudorandom permutations

Equivocal hash functions → OSS

Question 2



Can Alice and Bob ensure that if $\mathbf{m_0} \neq \perp$ and $\mathbf{m_1} \neq \perp$, then $\mathbf{m_0} = \mathbf{m_1}$

Non-triviality: for any $\mathbf{m} \neq \perp$, possible adversary to send $\mathbf{m_0} = \mathbf{m_1} = \mathbf{m}$

Thm [Z’19, Amos-Georgiou-Kiayias-Z’20, Dall’Agnol-Spooner’23]:
Equivocal hash function → OSS

Proof idea: (Honest) setup samples **h**, $|\Psi_h\rangle$ ➡ **vk = h**, $|\mathbf{sk}\rangle = |\Psi_h\rangle$

Sign($|$sk$\rangle$, b): equivocate to **(b,r)** s.t. **H(b,r) = h** ➡ **σ = r**

Ver(vk, b, σ): check that **H(b, σ) =h**

Can extend to multi-bit messages by parallel repetition

OSS → Quantum Money w/ Classical Communication

Thm [Amos-Georgiou-Kiayias-Z'20]: OSS → Publicly-verifiable quantum Money with classical communication

Proof: Mint publishes verification key **vk*** for *plain* signature scheme, keeps plain signing key **sk*** secret

$$|\$\rangle = |sk\rangle, vk, \sigma_{vk^* \to vk}$$

$$\sigma_{vk^* \to vk} = \text{Sign}^*(sk^*, vk)$$

Verification: Check that $\sigma_{vk^* \to vk}$ is valid signature on **vk** (relative to **vk***), and that $|sk\rangle$ can sign messages relative to **vk**

Thm [Amos-Georgiou-Kiayias-Z'20]: OSS → Publicly-verifiable quantum Money with classical communication

Proof: Sending money

$|\$\rangle = |sk\rangle, vk, \sigma_{vk^* \to vk}$

Thm [Amos-Georgiou-Kiayias-Z'20]: OSS → Publicly-verifiable quantum Money with classical communication

Proof: Sending money

$|sk'\rangle$, vk' ← Setup

$|\$\rangle = |sk\rangle, vk, \sigma_{vk^* \to vk}$

Thm [Amos-Georgiou-Kiayias-Z'20]: OSS → Publicly-verifiable quantum Money with classical communication

Proof: Sending money

$|sk'\rangle, vk' \leftarrow$ **Setup**

vk'

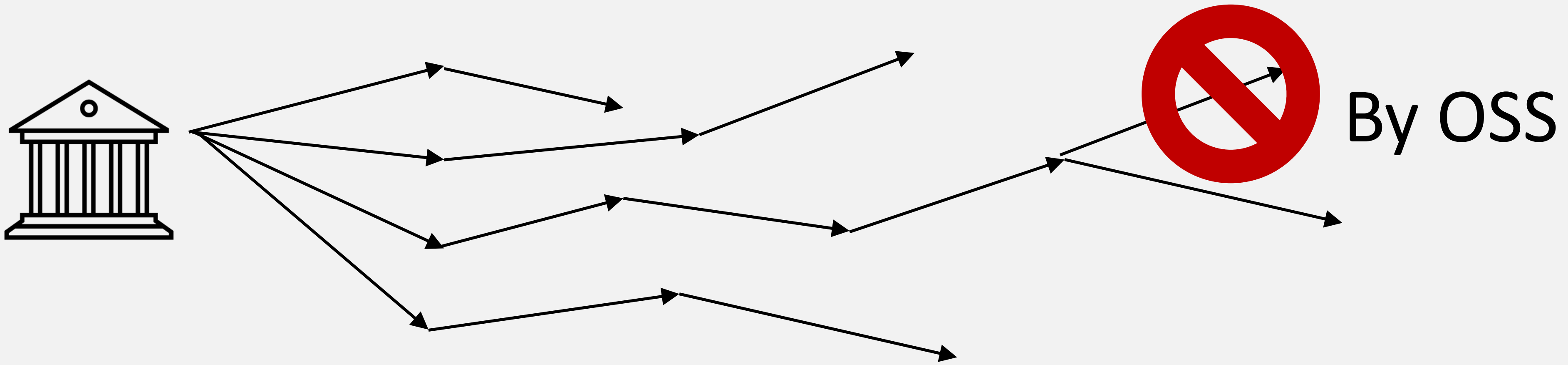
$\sigma_{vk \to vk'} \leftarrow \mathbf{Sign}(|sk\rangle, vk')$

$\cancel{|\$\rangle = |sk\rangle, vk, \sigma_{vk^* \to vk}}$ $|\$'\rangle = |sk'\rangle, vk', \sigma_{vk^* \to vk}, \sigma_{vk \to vk'}$

Thm [Amos-Georgiou-Kiayias-**Z**'20]: OSS → Publicly-verifiable quantum Money with classical communication

Proof:

In general, **|$⟩** = **|sk⟩ + vk +** chain of signatures from **vk*** to **vk**



?