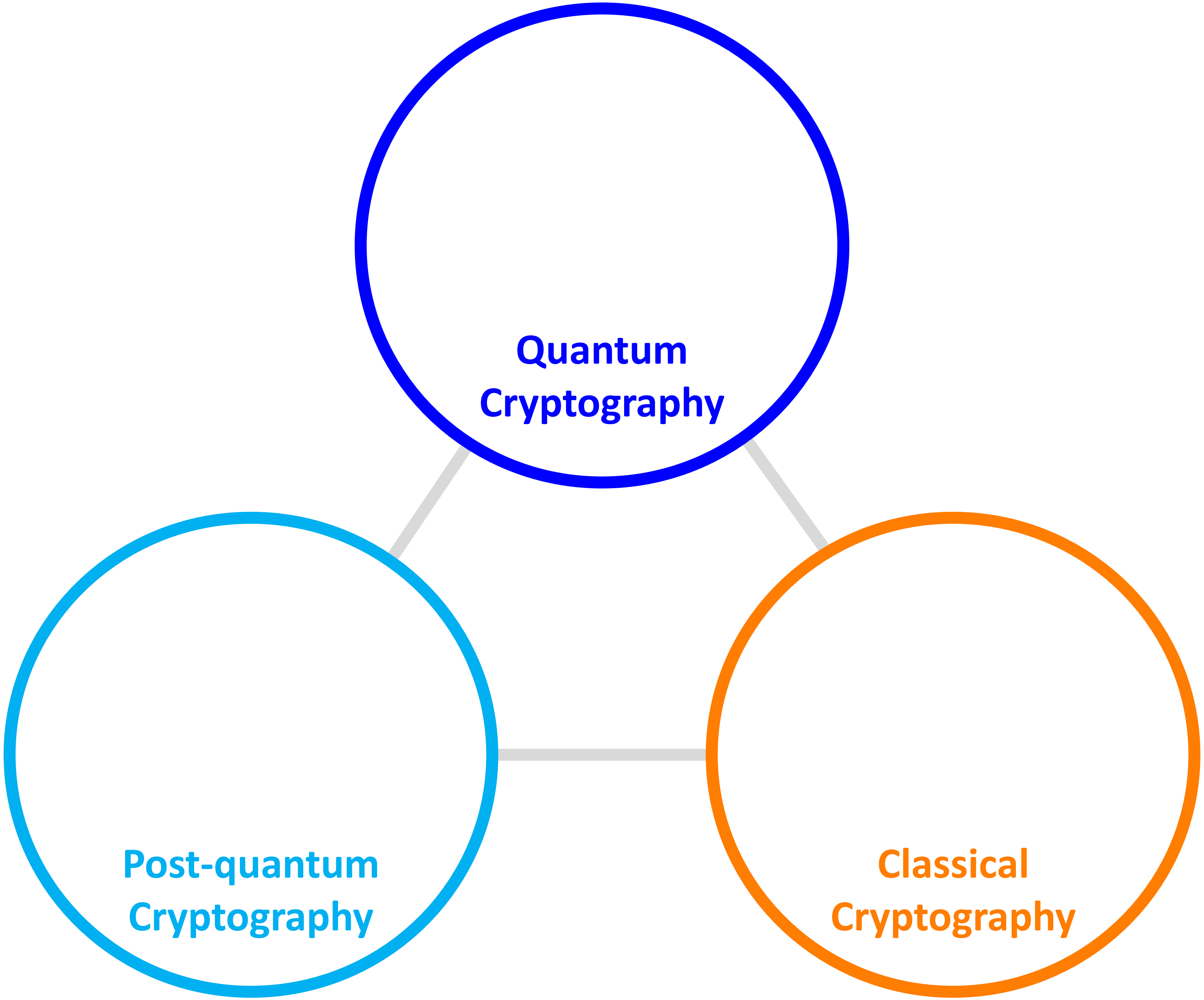
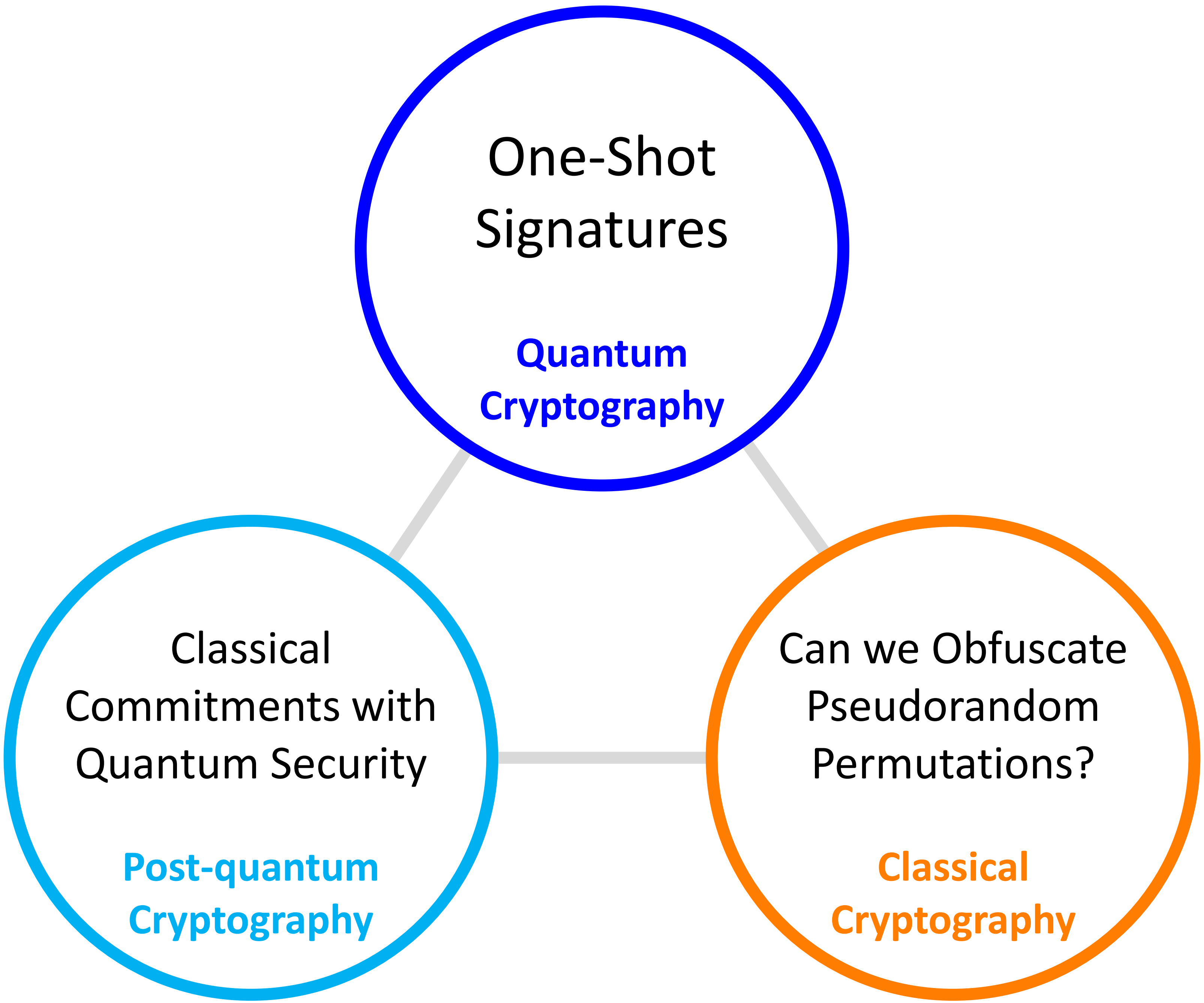
On One-Shot Signatures, Quantum vs Classical Binding, & Obfuscation Permutations

Omri Shmueli
NTT Research

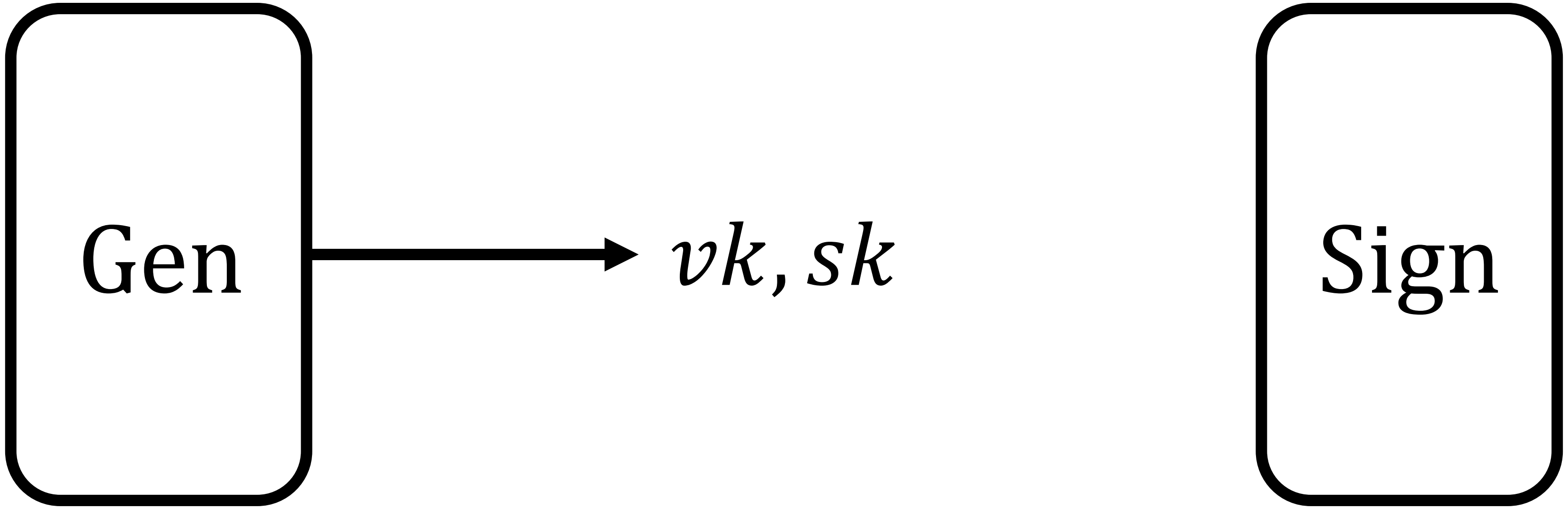
Mark Zhandry
NTT Research
Stanford


Quantum
Cryptography
Post-quantum
Cryptography
Classical
Cryptography


One-Shot Signatures
Quantum Cryptography
Classical Commitments with Quantum Security
Post-quantum Cryptography
Can we Obfuscate Pseudorandom Permutations?
Classical Cryptography

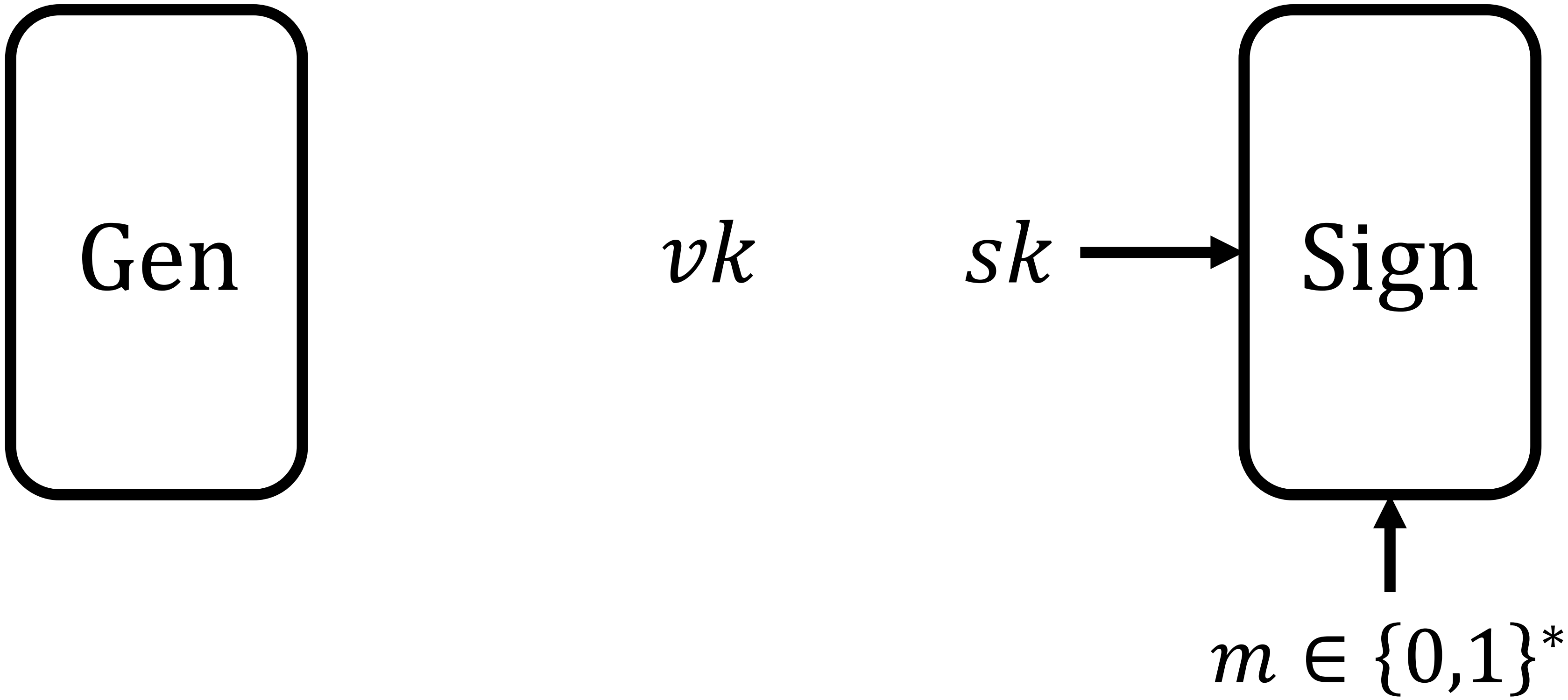
A Question

Is it possible to construct a ***one-time*** signature token?



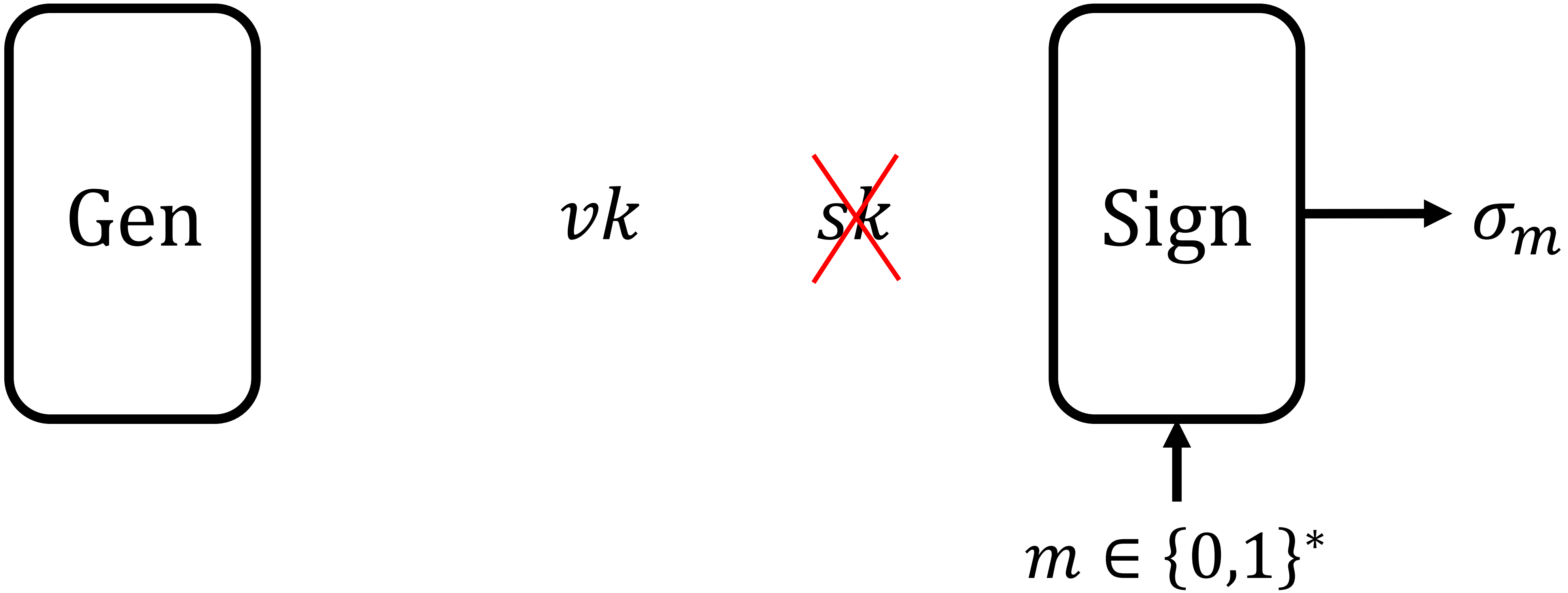
A Question

Is it possible to construct a ***one-time*** signature token?



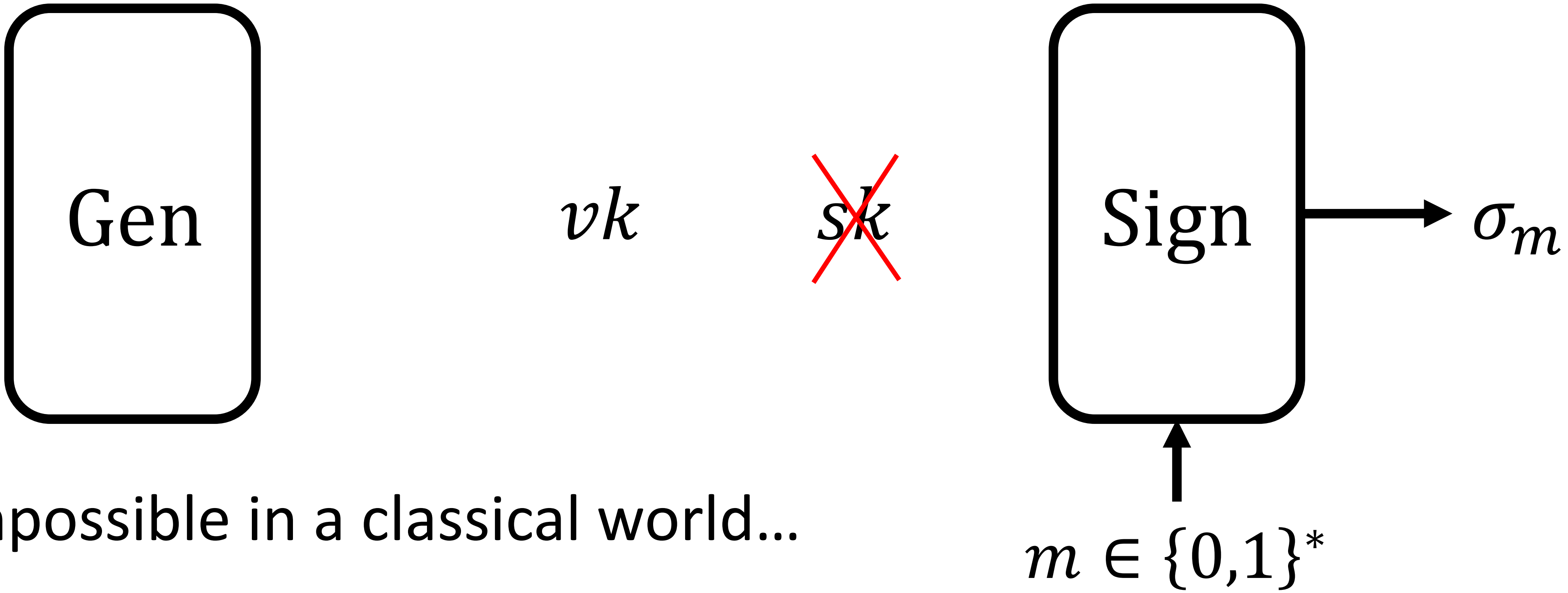
A Question

Is it possible to construct a ***one-time*** signature token?



A Question

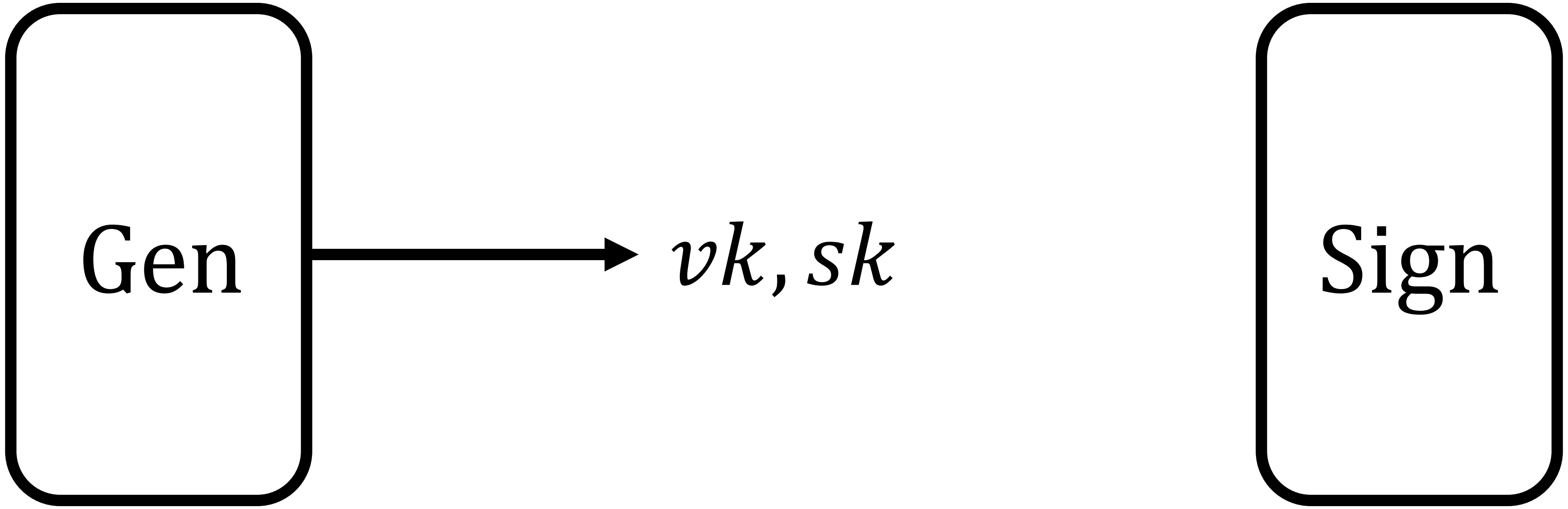
Is it possible to construct a ***one-time*** signature token?



Clearly impossible in a classical world…

A Question

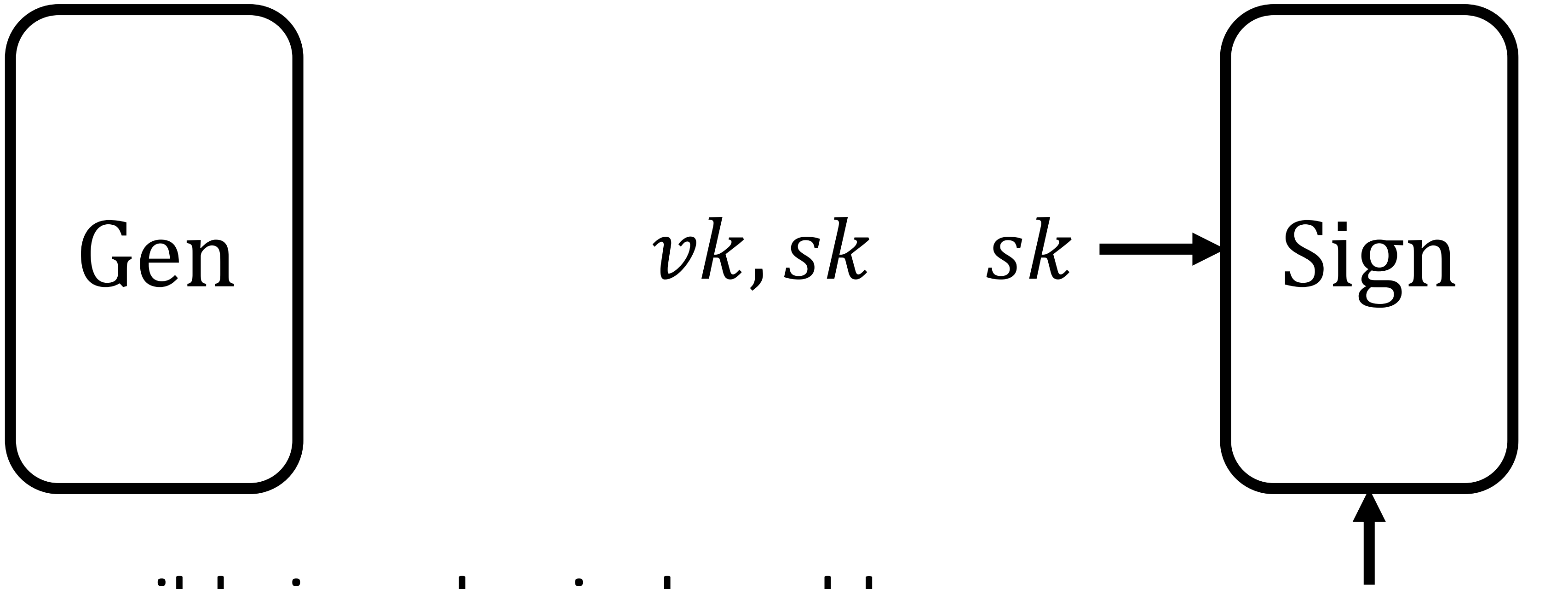
Is it possible to construct a ***one-time*** signature token?



Clearly impossible in a classical world…

A Question

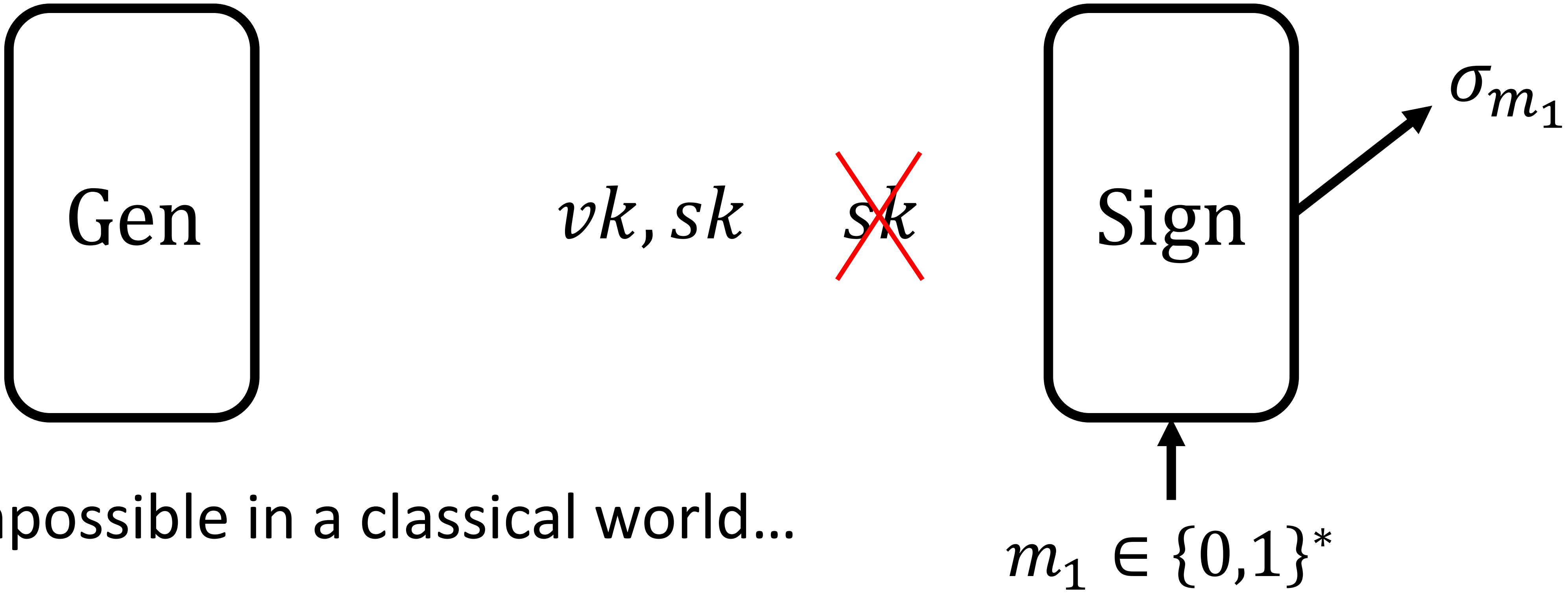
Is it possible to construct a ***one-time*** signature token?



Clearly impossible in a classical world…

A Question

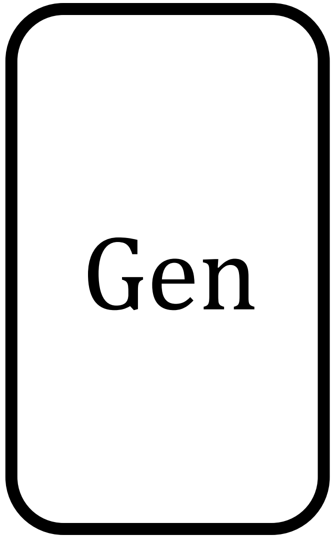
Is it possible to construct a ***one-time*** signature token?



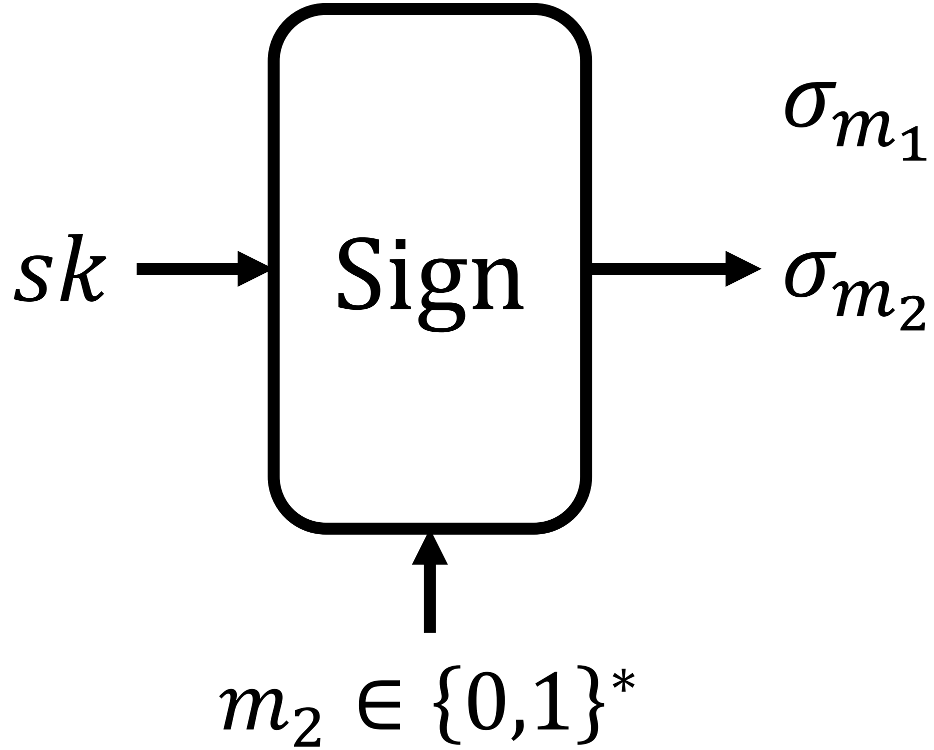
Clearly impossible in a classical world…

A Question

Is it possible to construct a ***one-time*** signature token?



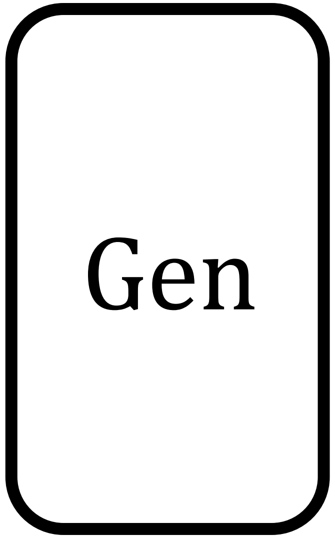
vk, sk



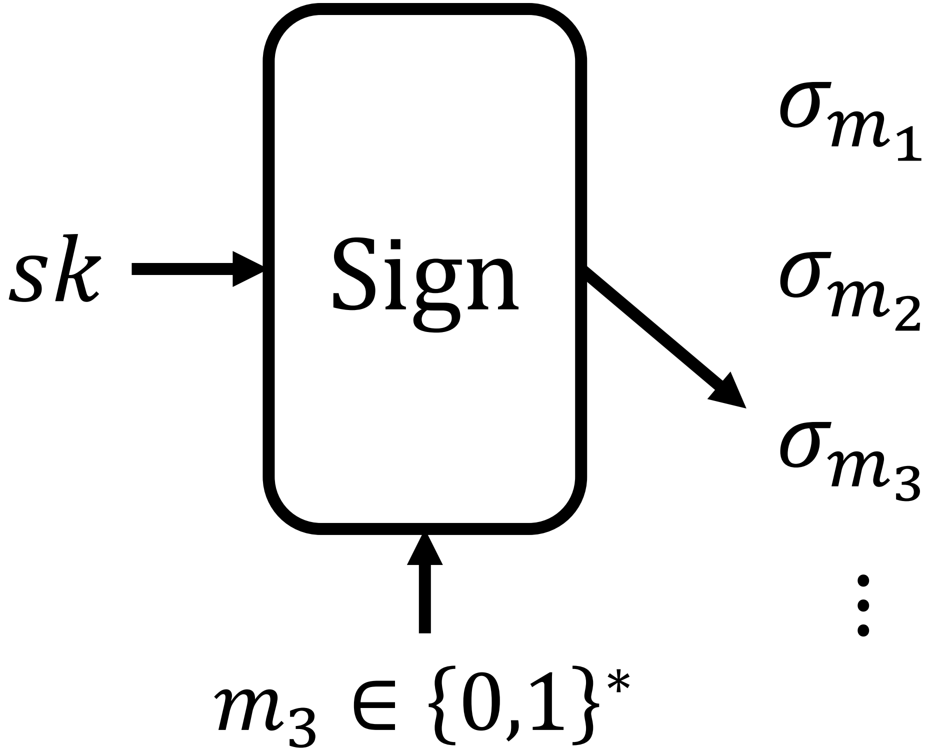
Clearly impossible in a classical world…

A Question

Is it possible to construct a ***one-time*** signature token?



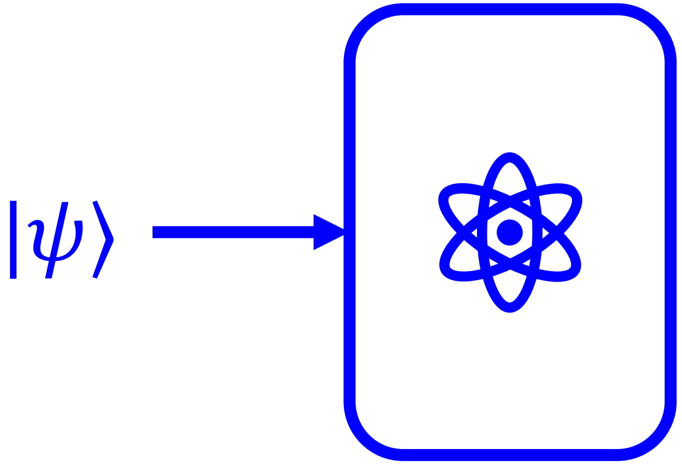
vk, sk



Clearly impossible in a classical world…

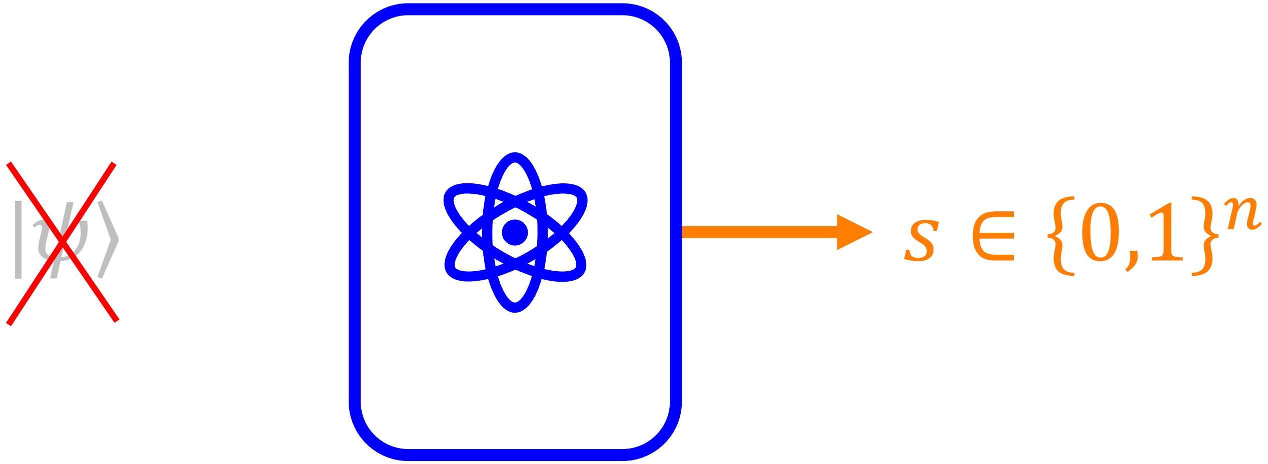
Quantum Information in Cryptography

Extracting classical information from a quantum state can degrade it.



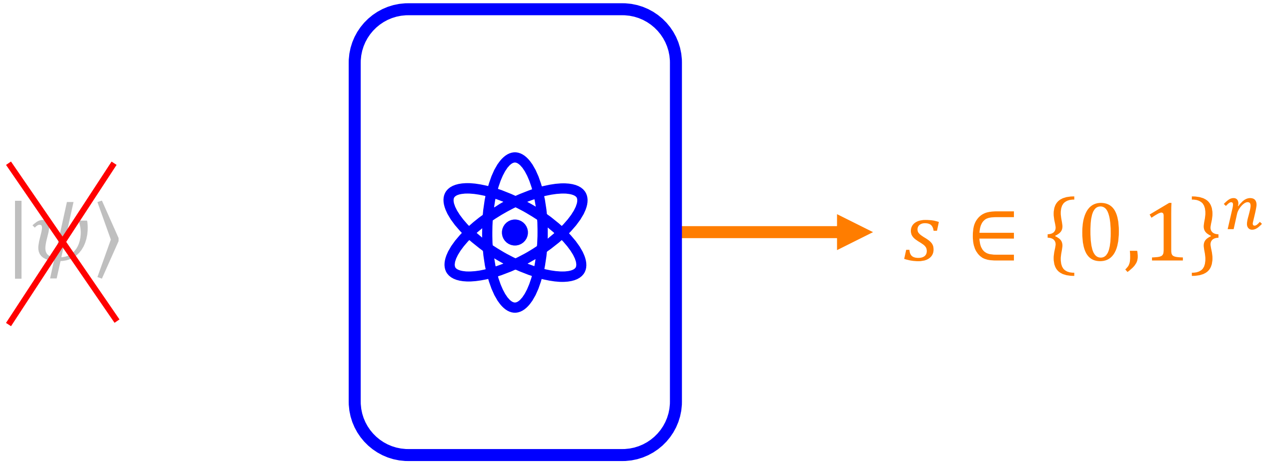
Quantum Information in Cryptography

Extracting classical information from a quantum state can degrade it.



Quantum Information in Cryptography

Extracting classical information from a quantum state can degrade it.



Is it possible to make this degradation ***inherent***, for the ***benefit*** of quantum cryptography?

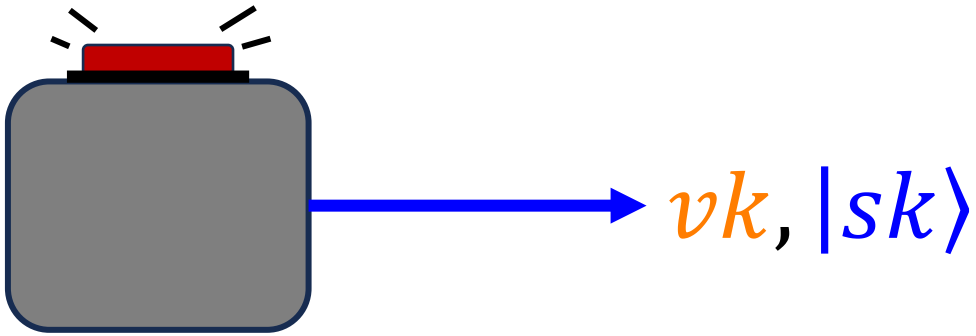
One-Shot Signatures
[Amos-Georgiou-Kiayias-Zhandry-20]

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.

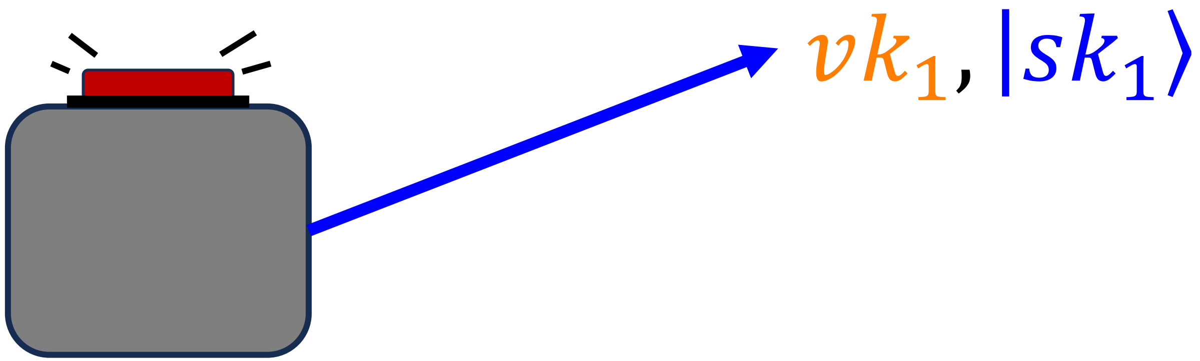


One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.

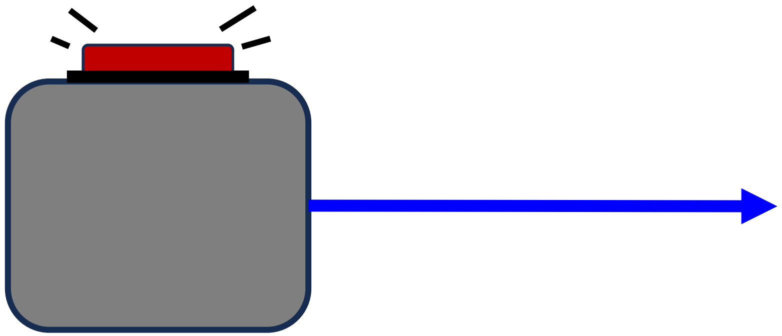


One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.



$vk_1, |sk_1\rangle$

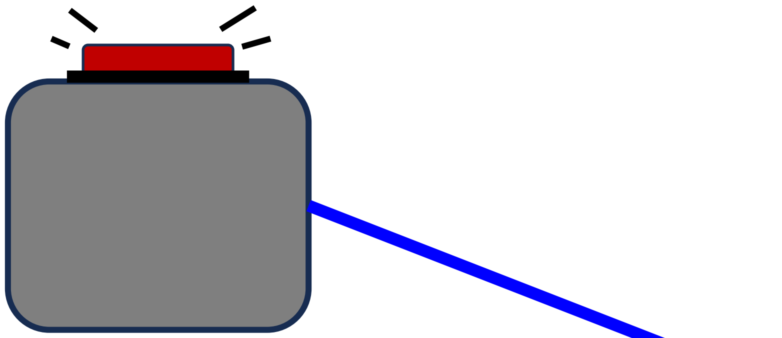
$vk_2, |sk_2\rangle$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.



$vk_1, |sk_1\rangle$

$vk_2, |sk_2\rangle$

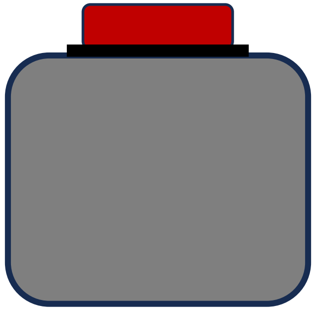
$vk_3, |sk_3\rangle$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.



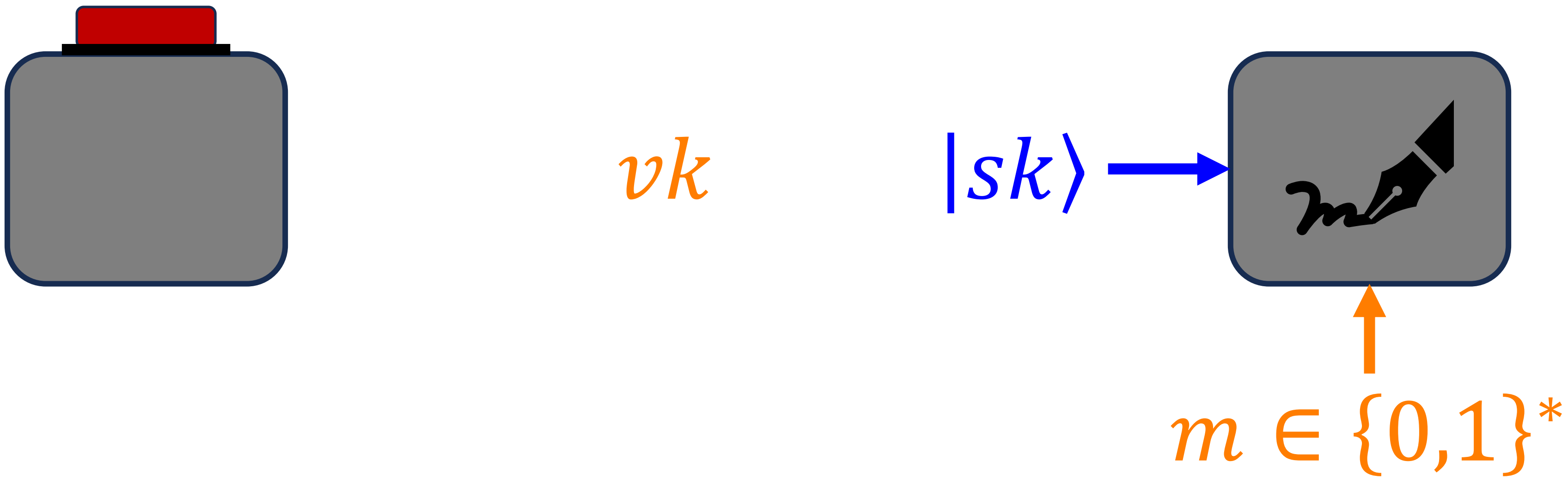
$vk, |sk\rangle$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.

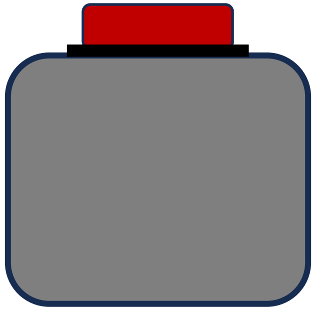


One-Shot Signatures

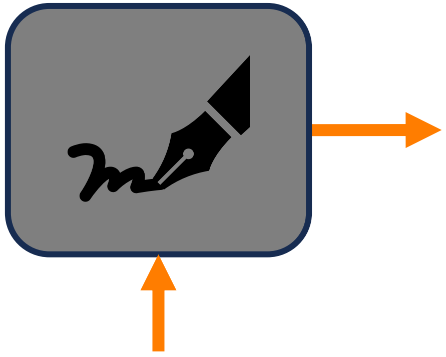
[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.



vk $\quad$ ~~$|sk\rangle$~~



σ_m

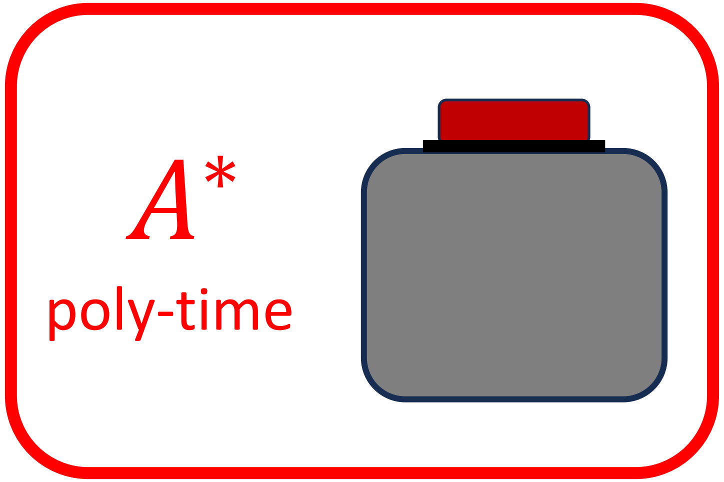
$m \in \{0,1\}^*$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.



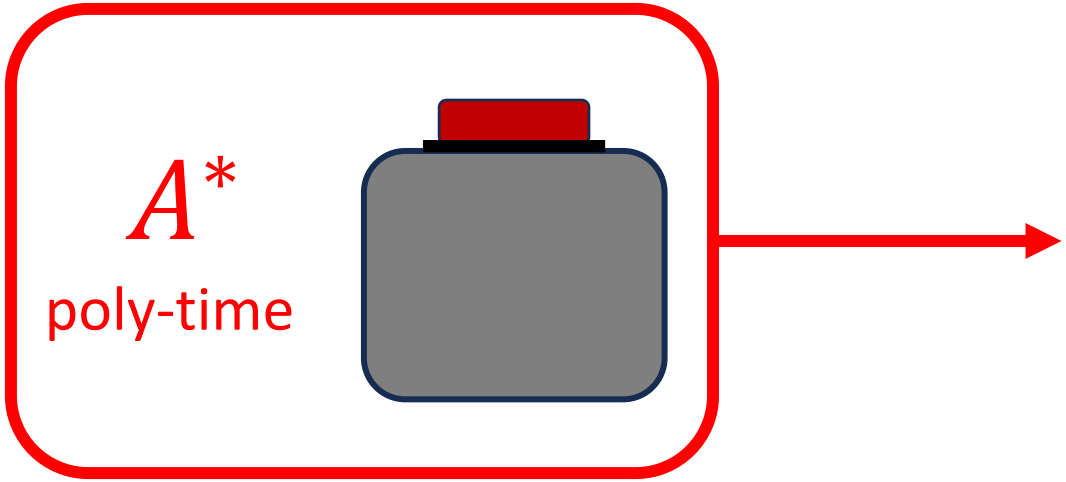
Security: Intractable to sign twice using the same key

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.



$vk_1, |sk_1\rangle$

$vk_2, |sk_2\rangle$

$vk_3, |sk_3\rangle$

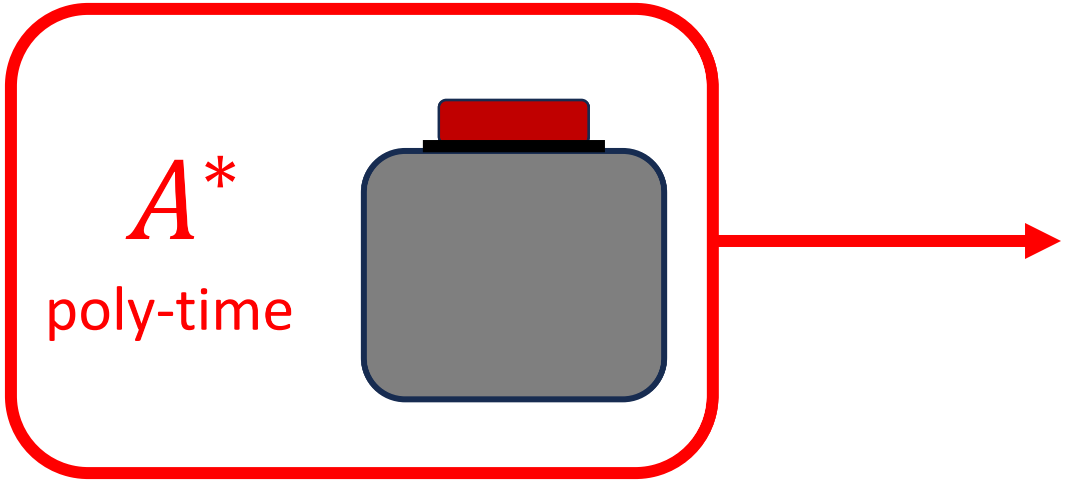
$\vdots$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.



$$(vk_1, m_1, \sigma_{m_1})$$
$$(vk_2, m_2, \sigma_{m_2})$$
$$(vk_3, m_3, \sigma_{m_3})$$
$$\vdots$$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.

$$(vk, m_0, \sigma_{m_0}), (vk, m_1, \sigma_{m_1})$$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.

$$\left(vk, m_0, \sigma_{m_0}\right), \left(vk, m_1, \sigma_{m_1}\right)$$

One-Shot Signatures

[Amos-Georgiou-Kiayias-Zhandry-20]

A box, sampling i.i.d. quantum digital signature tokens, which self-destruct after a single use.

Everyone has access to the box.

$(vk, m_0, \sigma_{m_0}), (vk, m_1, \sigma_{m_1})$

Computationally intractable for $m_0 \neq m_1$

One-Shot Signatures - Applications

One-Shot Signatures - Applications

- **A master primitive in decentralization**
  - Cryptocurrency (based on PoW) without a blockchain [Zha-17].
  - Blockchain-free smart contracts [Sat-22].
  - Solves the Blockchain Scalability Problem [Col-Sat-20].
  - A perfect-finality solution to the double spending problem.
  - A lot more applications for blockchains (see [Drake-23]).

One-Shot Signatures - Applications

- **A master primitive in decentralization**
  - ➢Cryptocurrency (based on PoW) without a blockchain [Zha-17].
  - ➢Blockchain-free smart contracts [Sat-22].
  - ➢Solves the Blockchain Scalability Problem [Col-Sat-20].
  - ➢A perfect-finality solution to the double spending problem.
  - ➢A lot more applications for blockchains (see [Drake-23]).
- **Quantum cryptography with classical communication (!)**

⋮

One-Shot Signatures - Applications

- **A master primitive in decentralization**
  - Cryptocurrency (based on PoW) without a blockchain [Zha-17].
  - Blockchain-free smart contracts [Sat-22].
  - Solves the Blockchain Scalability Problem [Col-Sat-20].
  - A perfect-finality solution to the double spending problem.
  - A lot more applications for blockchains (see [Drake-23]).
- **Quantum cryptography with classical communication (!)**

⋮

We do not know of any other primitive in (quantum) cryptography that solves any of these problems

One-Shot Signatures – Previous Work

One-Shot Signatures – Previous Work

- **Standard model constructions:** No constructions under any (even non-standard) computational assumptions.

One-Shot Signatures – Previous Work

- **Standard model constructions:** No constructions under any (even non-standard) computational assumptions.
- **Oracle model constructions:**
  - [A-G-K-Z-20]: Suggested a construction in a classical oracle model, and a proof.

One-Shot Signatures – Previous Work

- **Standard model constructions:** No constructions under any (even non-standard) computational assumptions.
- **Oracle model constructions:**
  - [A-G-K-Z-20]: Suggested a construction in a classical oracle model, and a proof.
  - The proof was found to contain a fatal bug [Bar-23].

One-Shot Signatures – Previous Work

- **Standard model constructions:** No constructions under any (even non-standard) computational assumptions.
- **Oracle model constructions:**
  - ➢[A-G-K-Z-20]: Suggested a construction in a classical oracle model, and a proof.
  - ➢The proof was found to contain a fatal bug [Bar-23].
  - ➢To date, the security of that construction remains unknown.

A Paradigm for Constructing One-Shot Signatures: Detour into Post-quantum Cryptography

Detour into Post-quantum Cryptography

[Unruh-15]:

Classical **commitments** that are post-quantum computationally binding, may nonetheless be "insecure" against quantum computers.

Detour into Post-quantum Cryptography

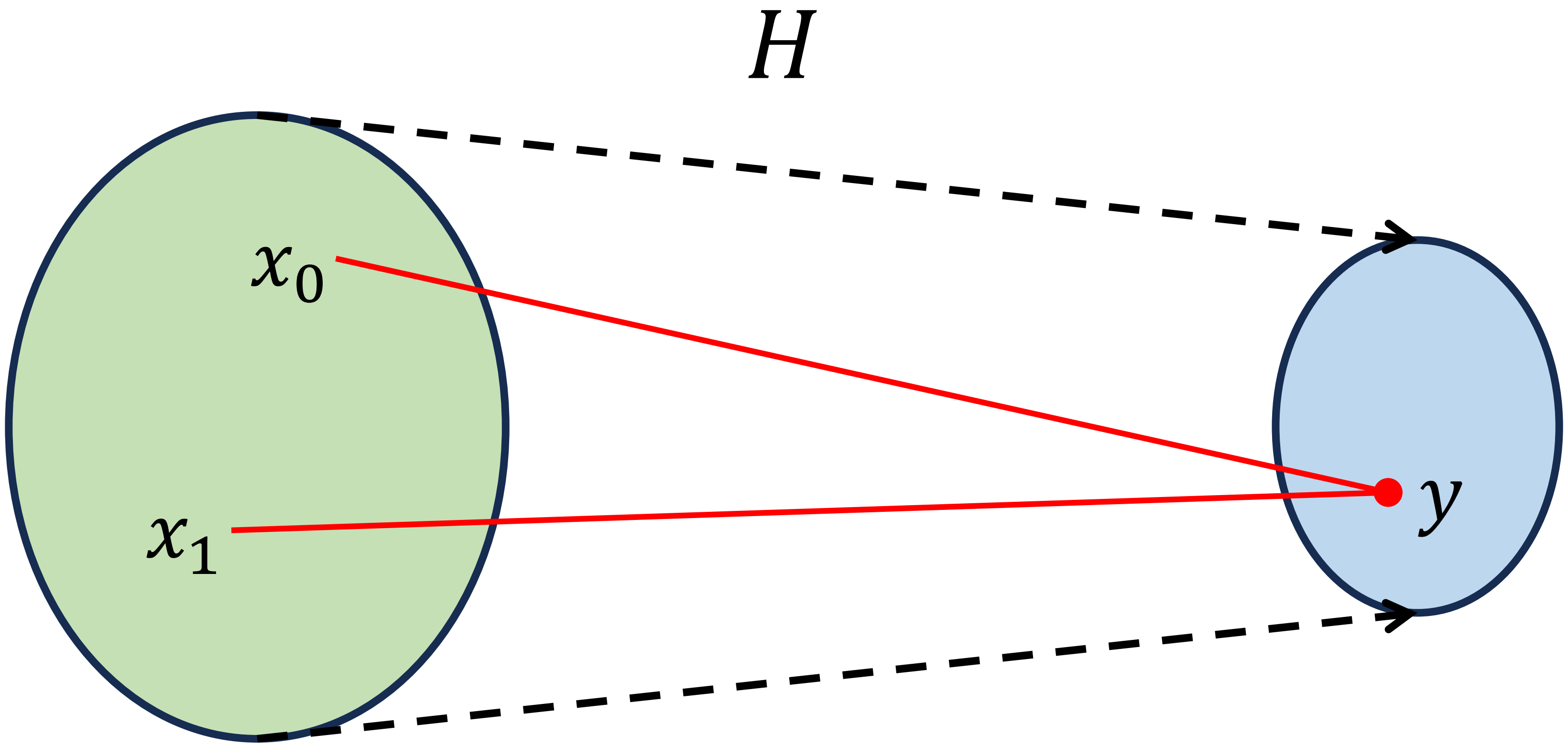
[Unruh-15]:

Classical **commitments** that are post-quantum computationally binding, may nonetheless be “insecure” against quantum computers.

$\Uparrow$

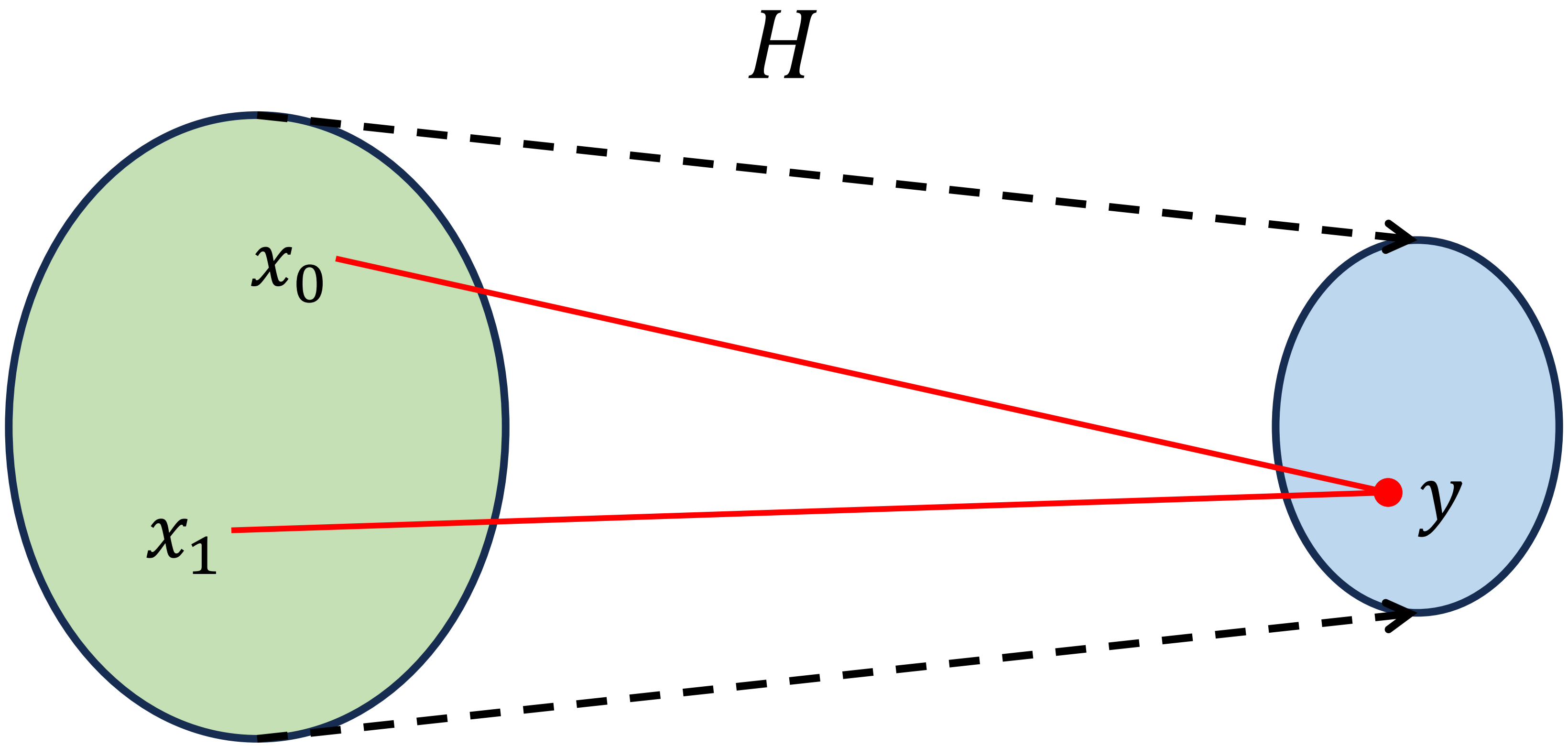
Classical **hash functions** that are post-quantum collision-resistant, may nonetheless be “insecure” against quantum computers.

Post-quantum Collision-Resistant Hash



Computationally intractable to find $x_0 \neq x_1$ s.t. $H(x_0) = H(x_1)$,
even for a quantum computer.

Post-quantum Collision-Resistant Hash

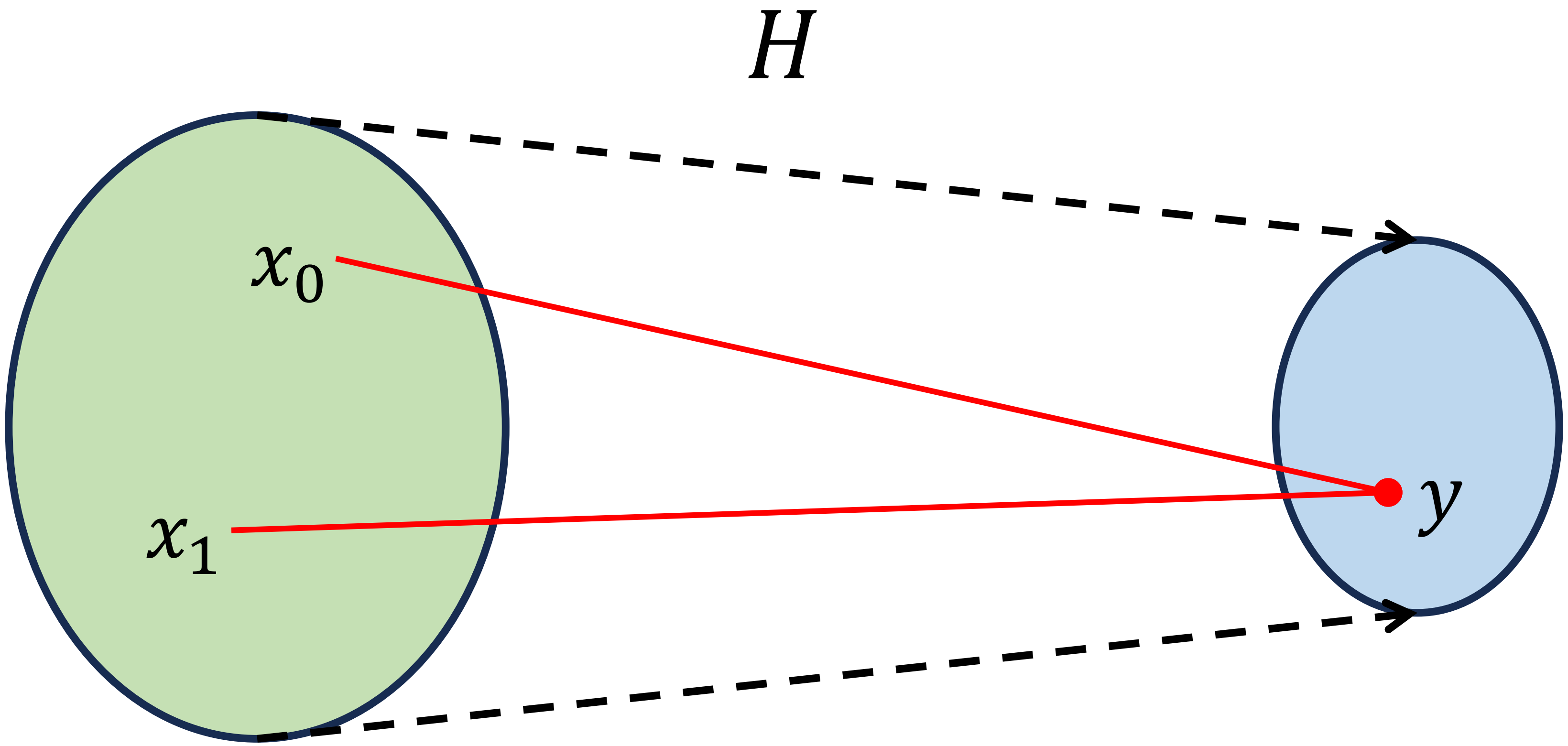


For computationally binding commitments we want:

If the adversary sends y, it is intractable for it choose x_b later.

Post-quantum Collision-Resistant Hash

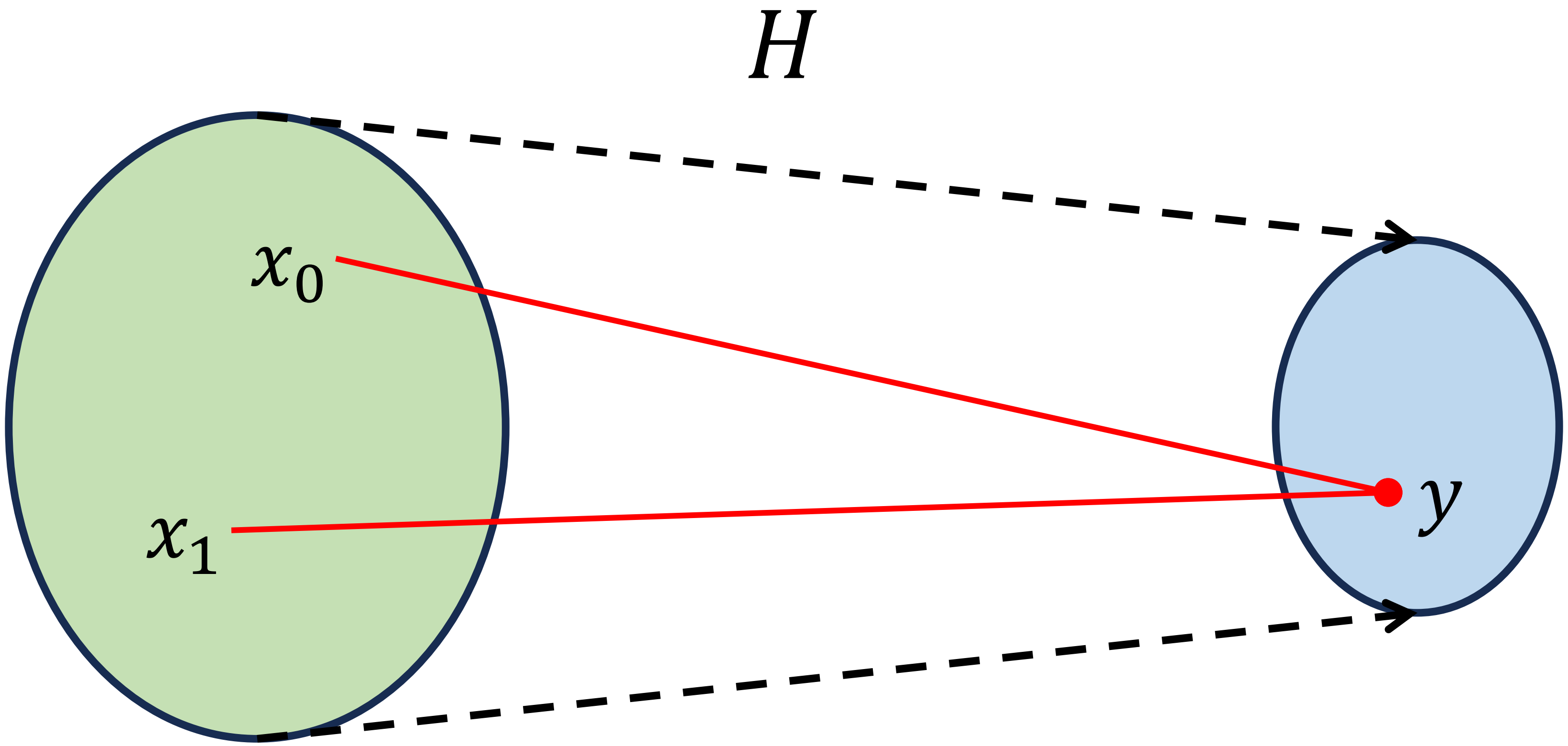
For **classical** **adversaries:** The below is equivalent to collision resistance



For computationally binding commitments we want:
If the adversary sends y, it is intractable for it choose x_b later.

Post-quantum Collision-Resistant Hash

For **classical** **adversaries:**
The below is equivalent to collision resistance

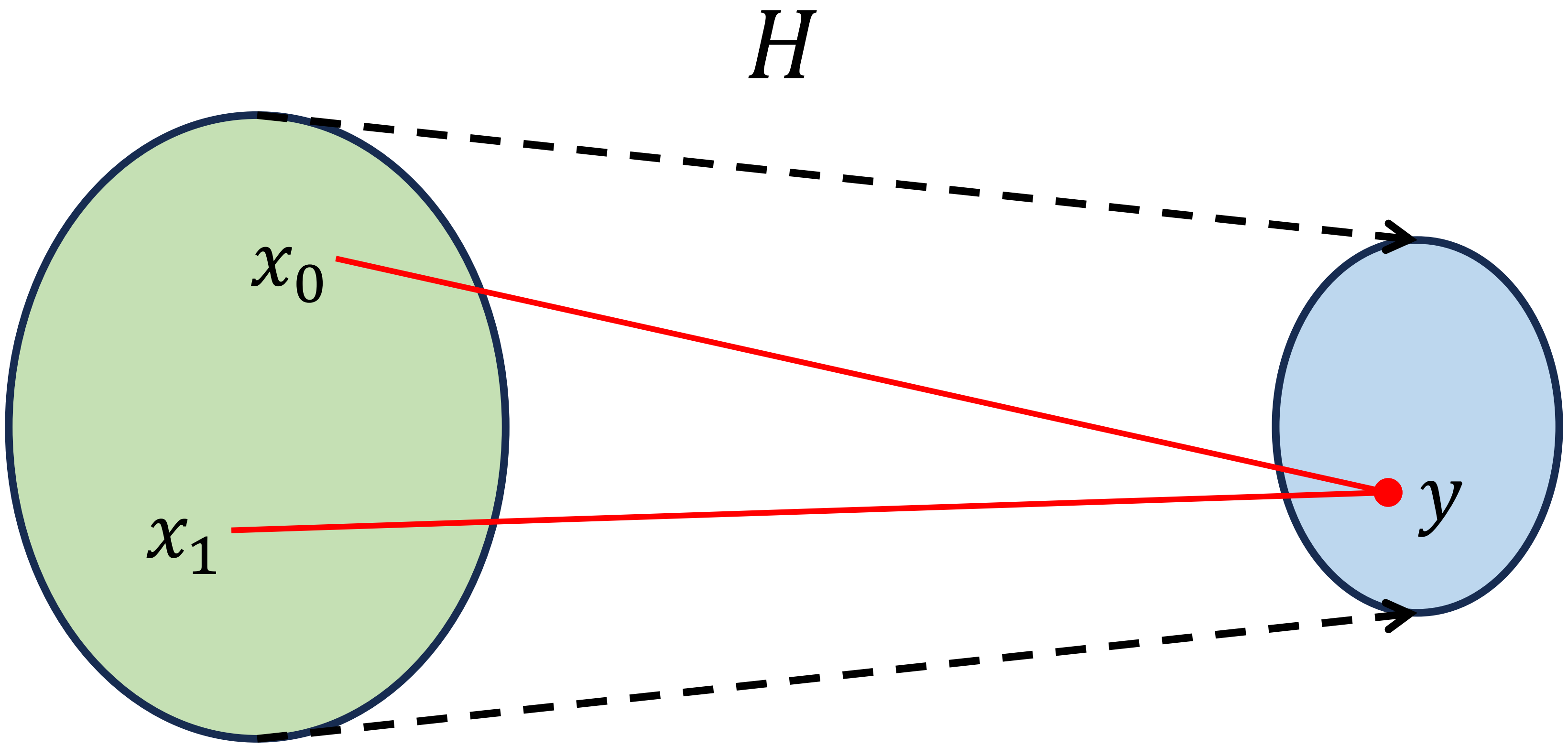


The reason of equivalence:
Rewinding!

For computationally binding commitments we want:
If the adversary sends y, it is intractable for it choose x_b later.

Post-quantum Collision-Resistant Hash

For quantum adversaries:

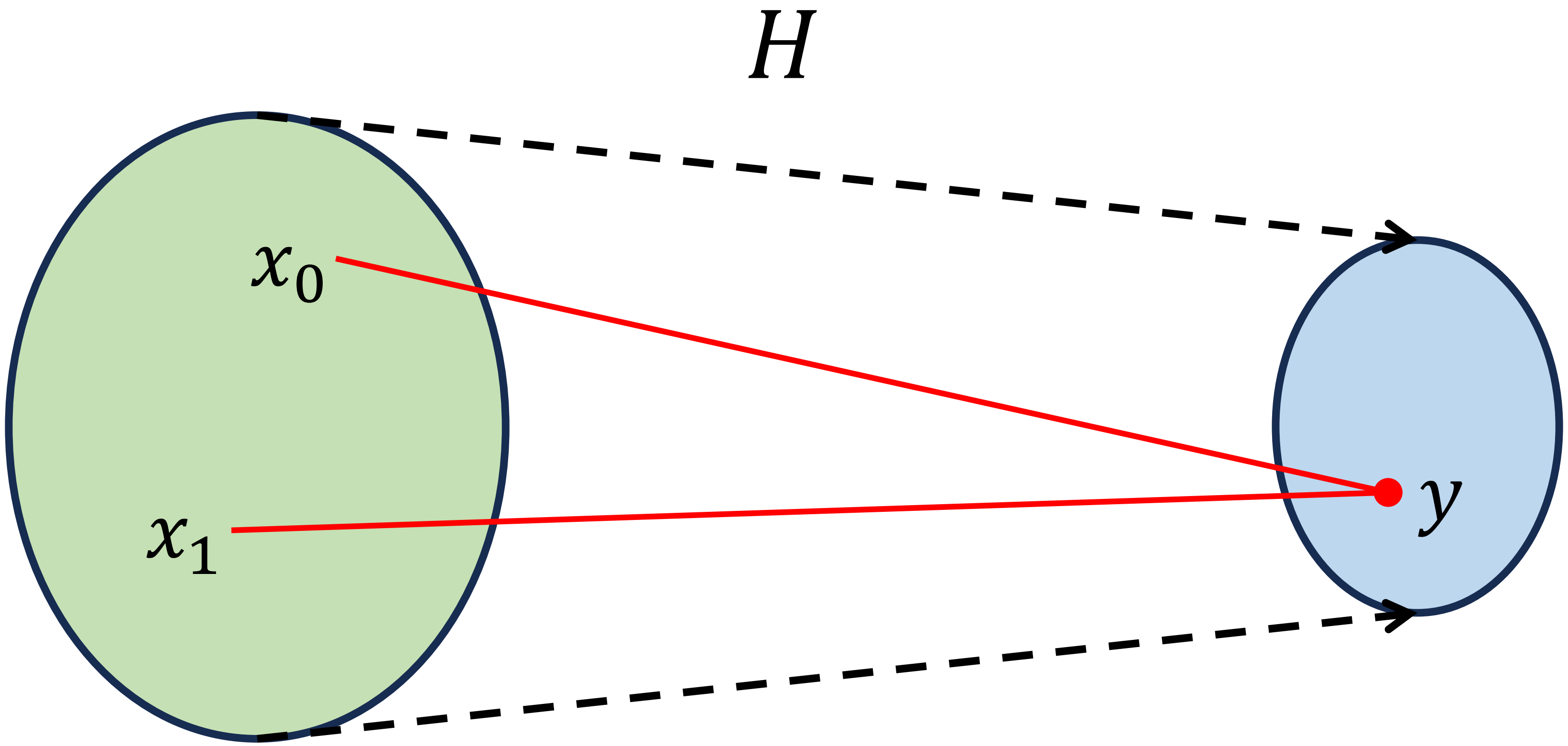


For computationally binding commitments we want:

If the adversary sends y, it is intractable for it choose x_b later.

Post-quantum Collision-Resistant Hash

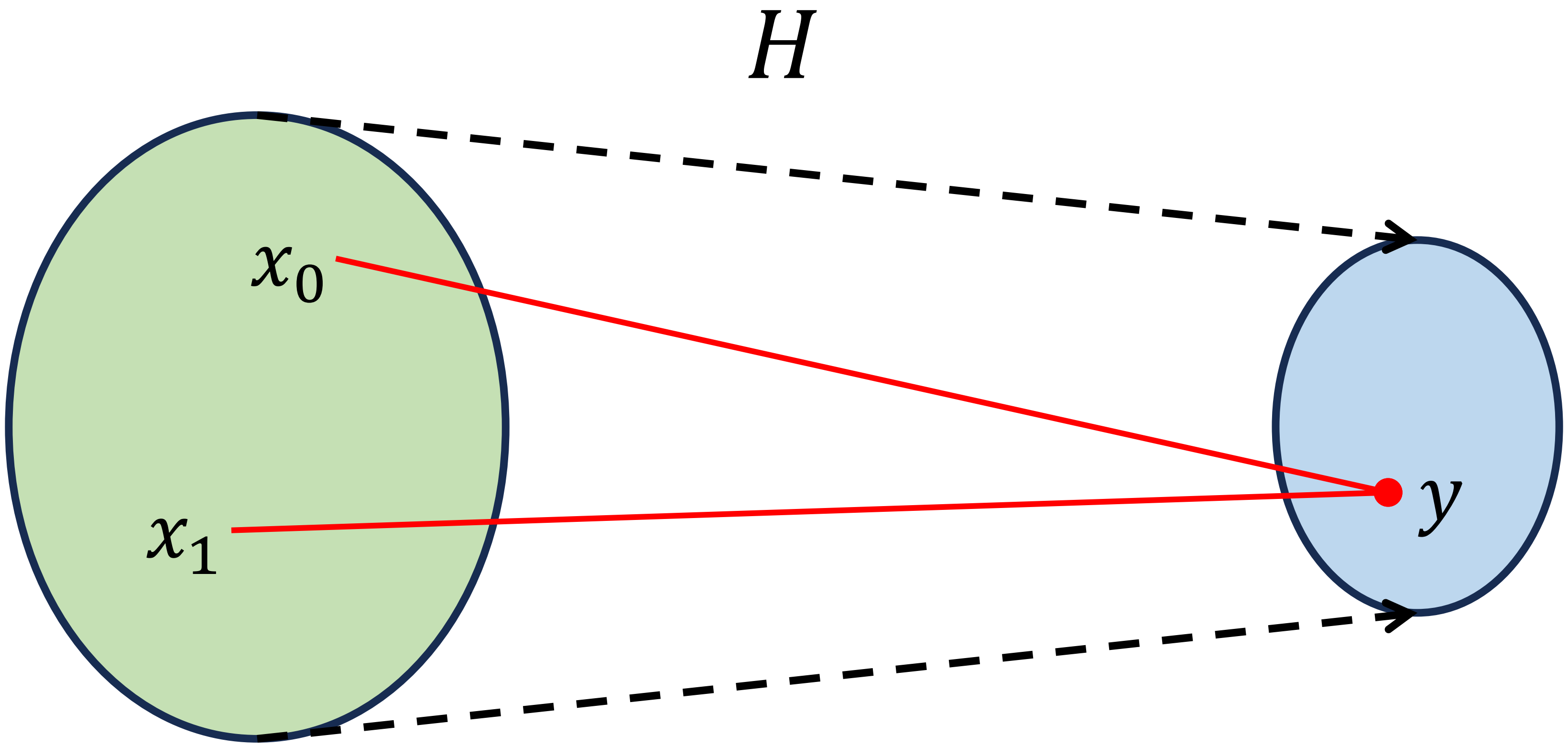
For **quantum** **adversaries:**
The below is <u>not</u> known to be equivalent to collision resistance



For computationally binding commitments we want:
If the adversary sends y, it is intractable for it choose x_b later.

Post-quantum Collision-Resistant Hash

For quantum adversaries: The below is <u>not</u> known to be equivalent to collision resistance



The reason: We generally <u>cannot</u> rewind quantum computers

For computationally binding commitments we want:
If the adversary sends y, it is intractable for it choose x_b later.

Quantum Rewinding is Hard

[VDG-C-97], [Wat-02], [Kob-03], [D-F-S-04], [Wat-09], [Unr-12], [H-S-S-11], [L-N-11], [A-R-U-14], [B-J-S-W-16], [Unr-16a], [Unr-16b], [B-S-20], [C-M-S-Z-21], [L-M-S-22], …

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle$$

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle$$

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \to \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle \,,\, y \,.$$

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \to \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle \, , y \, .$$

- The adversary sends y as the commitment.

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \to \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle, y.$$

- The adversary sends y as the commitment.
- **The issue:** The adversary has $\sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle$. Theoretically, could steer the superposition to a specific preimage x (e.g., that starts with a 0).

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \to \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle\,,\, y\,.$$

- [Unruh-15]: Defined **collapsing** hash functions.

Collapsing Hash Functions

- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \to \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle , y \, .$$

- [Unruh-15]: Defined **collapsing** hash functions.
- For a collapsing H: $\sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle \approx_c \{x : x \leftarrow H^{-1}(y)\}$.

Collapsing Hash Functions

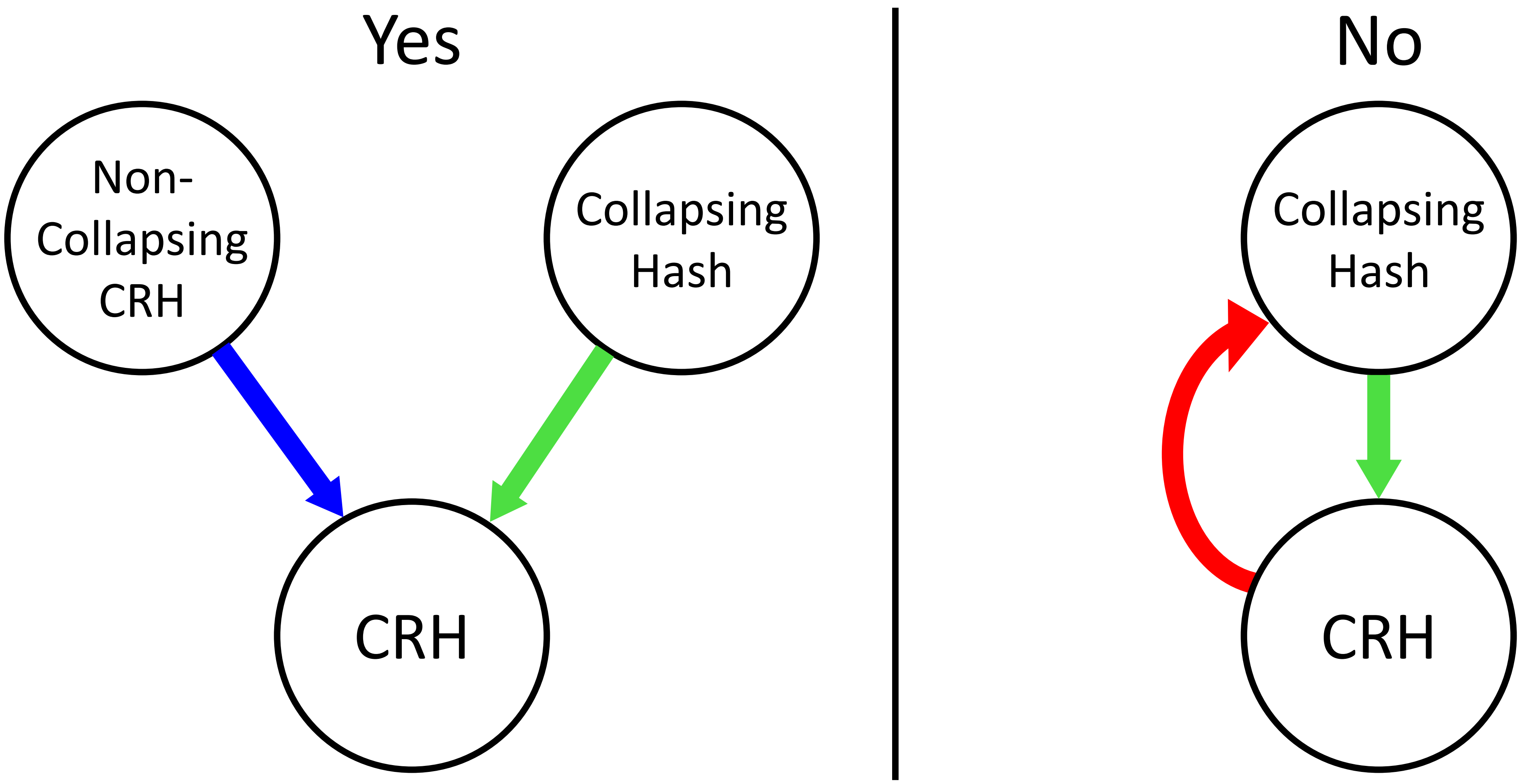
- What can a quantum adversary do with a CRH H?

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \to \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle , y .$$

- [Unruh-15]: Defined **collapsing** hash functions.
- For a collapsing H: $\sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle \approx_c \{x : x \leftarrow H^{-1}(y)\}$.
- Plenty of constructions of **collapsing hash functions** in the standard model ([Unr-16], [L-Z-19], [Zha-22], [L-M-Z-23]).

Does there exist a Non-collapsing CRH?

Does there exist a Non-collapsing CRH?



Does there exist a Non-collapsing CRH?

Definition: An (always) non-collapsing CRH is (H, D) s.t. :

Does there exist a Non-collapsing CRH?

Definition: An (always) non-collapsing CRH is (H, D) s.t. :

- H is a CRH.
- D is a quantum algorithm that can detect superpositions of H:

Does there exist a Non-collapsing CRH?

Definition: An (always) non-collapsing CRH is (H, D) s.t. :

- H is a CRH.
- D is a quantum algorithm that can detect superpositions of H:

$$\sum_{x \in \{0,1\}^n} |x\rangle$$

Does there exist a Non-collapsing CRH?

Definition: An (always) non-collapsing CRH is (H, D) s.t. :

- H is a CRH.
- D is a quantum algorithm that can detect superpositions of H:

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle$$

Does there exist a Non-collapsing CRH?

Definition: An (always) non-collapsing CRH is (H, D) s.t. :

- H is a CRH.
- D is a quantum algorithm that can detect superpositions of H:

$$\sum_{x\in\{0,1\}^n} |x\rangle \rightarrow \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \rightarrow \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle, y,$$

Does there exist a Non-collapsing CRH?

Definition: An (always) non-collapsing CRH is (H, D) s.t. :

- H is a CRH.
- D is a quantum algorithm that can detect superpositions of H:

$$\sum_{x\in\{0,1\}^n} |x\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle \to \sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle , y ,$$

$$\sum_{x\in\{0,1\}^n : H(x)=y} |x\rangle \not\approx \{x : x \leftarrow H^{-1}(y)\}$$

$\uparrow$

D

Does there exist a Non-collapsing CRH?

- Initially, motivation purely came from understanding post-quantum cryptography.

Does there exist a Non-collapsing CRH?

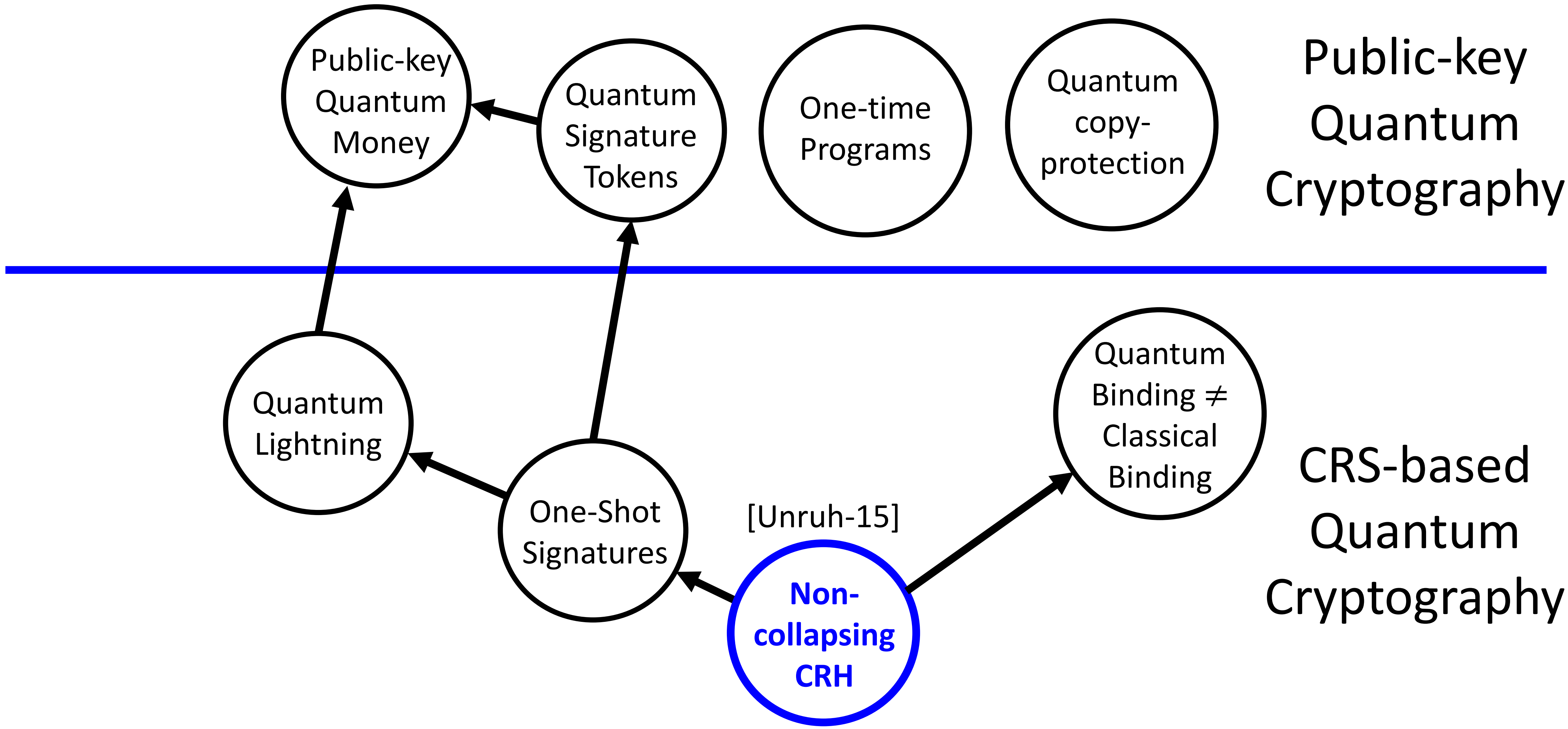
- Initially, motivation purely came from understanding post-quantum cryptography.
- [Zha-17]: A non-collapsing CRH is a powerful primitive for quantum cryptography!
- [Zha-17]: Non-collapsing CRH $\Rightarrow$ Quantum Lightning .

Does there exist a Non-collapsing CRH?

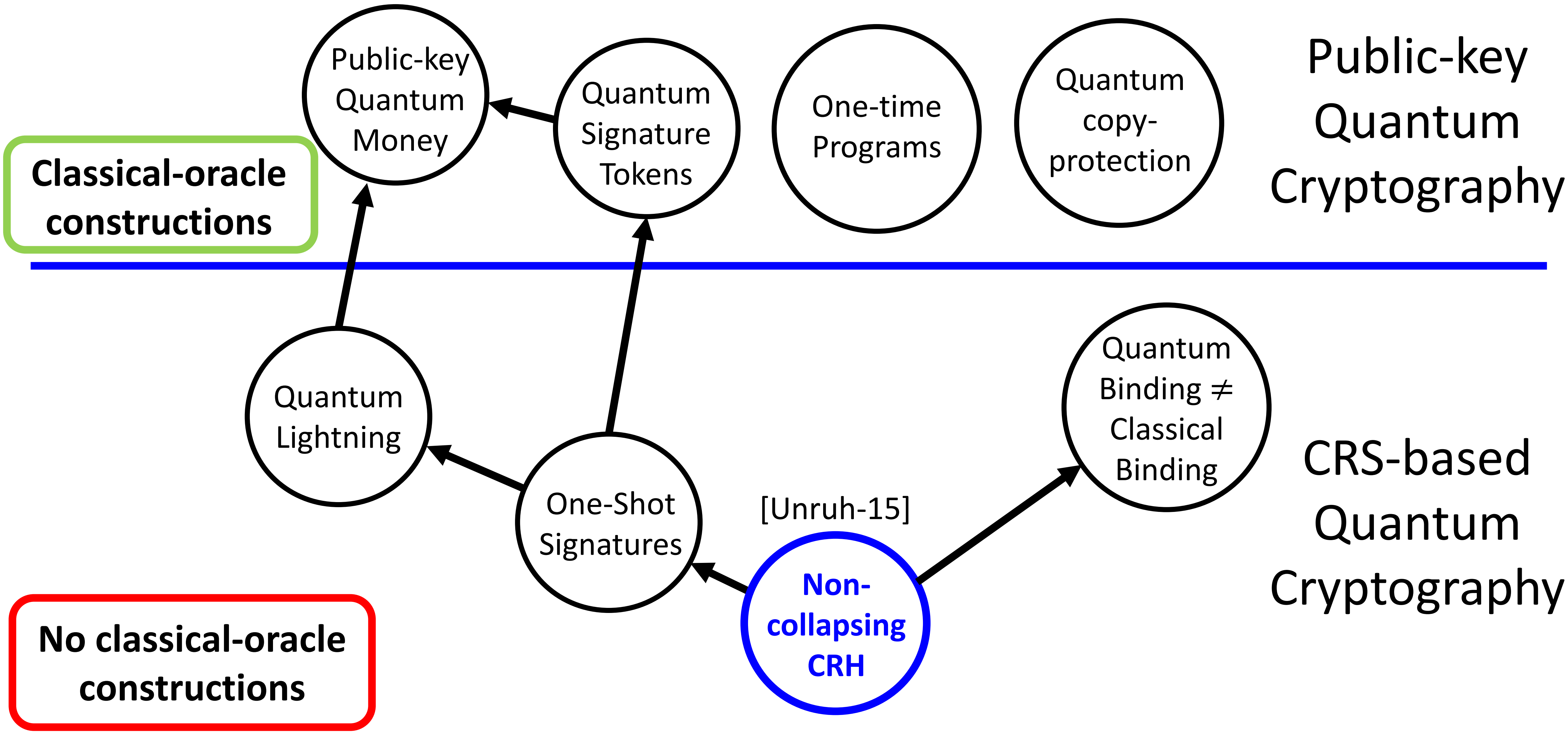
- Initially, motivation purely came from understanding post-quantum cryptography.
- [Zha-17]: A non-collapsing CRH is a powerful primitive for quantum cryptography!
- [Zha-17]: Non-collapsing CRH $\Rightarrow$ Quantum Lightning .
- [Zha-17], [A-G-K-Z-20], [D-S-22]:
  Non-collapsing CRH $\Rightarrow$ One-Shot Signatures .

(+ collapsing is **necessary** for post-quantum binding)

Does there exist a Non-collapsing CRH?



Does there exist a Non-collapsing CRH?



Some of our Results

Theorem 1:

Relative to a classical oracle there exists a non-collapsing CRH unconditionally.

Some of our Results

Theorem 1:

Relative to a classical oracle there exists a non-collapsing CRH unconditionally.

Theorem 2:

Assume,

- Polynomial hardness of **LWE** (with sub-exponential noise-to-modulus ratio), and

Some of our Results

Theorem 1:

Relative to a classical oracle there exists a non-collapsing CRH unconditionally.

Theorem 2:

Assume,

- Polynomial hardness of **LWE** (with sub-exponential noise-to-modulus ratio), and
- Sub-exponentially-secure **One-Way Functions**, and

Some of our Results

Theorem 1:

Relative to a classical oracle there exists a non-collapsing CRH unconditionally.

Theorem 2:

Assume,

- Polynomial hardness of **LWE** (with sub-exponential noise-to-modulus ratio), and
- Sub-exponentially-secure **One-Way Functions**, and
- Sub-exponentially-secure **iO** for classical circuits.

Some of our Results

Theorem 1:

Relative to a classical oracle there exists a non-collapsing CRH unconditionally.

Theorem 2:

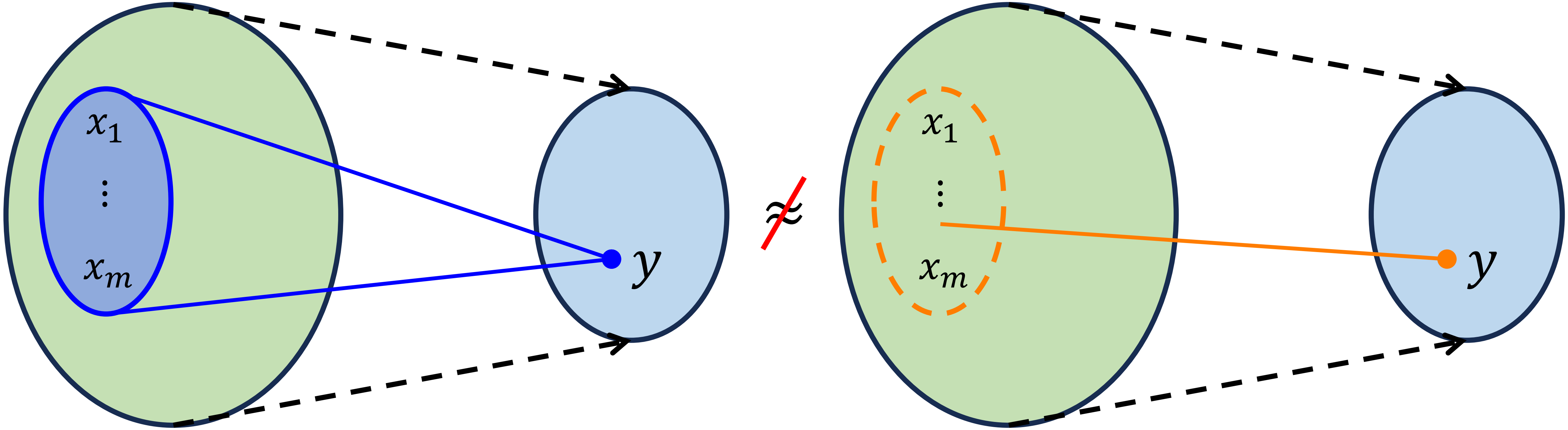
Assume,

- Polynomial hardness of **LWE** (with sub-exponential noise-to-modulus ratio), and
- Sub-exponentially-secure **One-Way Functions**, and
- Sub-exponentially-secure **iO** for classical circuits.

Then, there exists a **non-collapsing CRH** in the standard model.

Intuition for Constructing a Non-collapsing CRH

Intuition for Constructing a Non-collapsing CRH



Construct a CRH where the two cases above are **distinguishable**.

Intuition for Constructing a Non-collapsing CRH

The Challenge (intuitively):

- Non-collapsing:

- Collision resistance:

Intuition for Constructing a Non-collapsing CRH

The Challenge (intuitively):

- Non-collapsing:

Detecting a superposition publicly, without giving a description of the state, needs a highly structured set.

- Collision resistance:

Intuition for Constructing a Non-collapsing CRH

The Challenge (intuitively):

- Non-collapsing:

Detecting a superposition publicly, without giving a description of the state, needs a highly structured set.

- Collision resistance:

However, what makes a hash function collision resistant is the lack of predictable structure of inputs.

Intuition for Constructing a Non-collapsing CRH

Our technique:

A *random permutation* $\Pi: \{0,1\}^n \to \{0,1\}^n$ can be used to mediate between two requirements:

Intuition for Constructing a Non-collapsing CRH

Our technique:

A *random permutation* $\Pi: \{0,1\}^n \to \{0,1\}^n$ can be used to mediate between two requirements:

1. Unstructured, collision-resistant sets, and
2. Structured sets, detectable in quantum superposition.

Intuition for Constructing a Non-collapsing CRH

Our technique:

- Let $\Pi: \{0,1\}^n \to \{0,1\}^n$ a random permutation.

Intuition for Constructing a Non-collapsing CRH

Our technique:

- Let $\Pi: \{0,1\}^n \to \{0,1\}^n$ a random permutation.
- Define two functions $H, J: \{0,1\}^n \to \{0,1\}^{\frac{n}{2}}$:

$$\Pi(x) \coloneqq \Big(\underbrace{H(x)}_{\frac{n}{2}\text{ bits}}, \underbrace{J(x)}_{\frac{n}{2}\text{ bits}}\Big)$$

Intuition for Constructing a Non-collapsing CRH

Our technique:

- Let $\Pi: \{0,1\}^n \to \{0,1\}^n$ a random permutation.
- Define two functions $H, J: \{0,1\}^n \to \{0,1\}^{\frac{n}{2}}$:

$$\Pi(x) \coloneqq \Big(\underbrace{H(x)}_{\frac{n}{2}\text{ bits}}, \underbrace{J(x)}_{\frac{n}{2}\text{ bits}}\Big)$$

- $H: \{0,1\}^n \to \{0,1\}^{\frac{n}{2}}$ is simply a random $2^{n/2}$-to-1 function.
  $\Rightarrow H$ is collision resistant.

Intuition for Constructing a Non-collapsing CRH

Our technique:

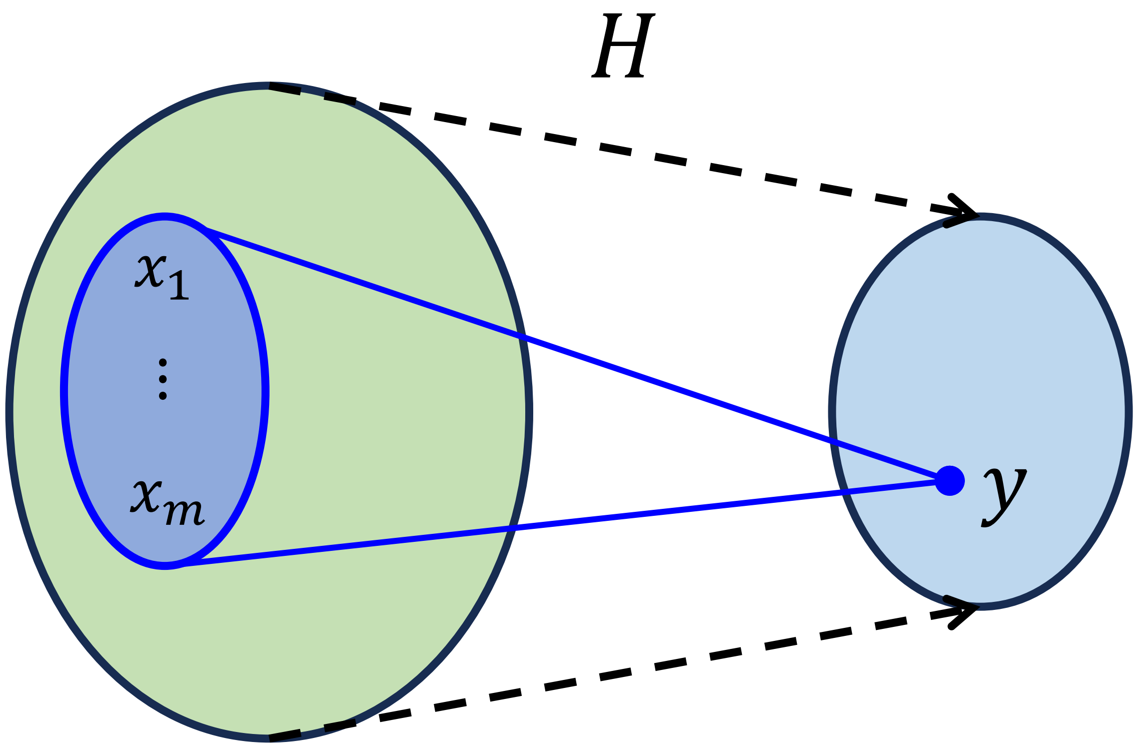
- Let $\Pi: \{0,1\}^n \to \{0,1\}^n$ a random permutation.
- Define two functions $H, J: \{0,1\}^n \to \{0,1\}^{\frac{n}{2}}$:

$$\Pi(x) := \Big(\underbrace{H(x)}_{\frac{n}{2}\text{ bits}}, \underbrace{J(x)}_{\frac{n}{2}\text{ bits}}\Big)$$

- $H: \{0,1\}^n \to \{0,1\}^{\frac{n}{2}}$ is simply a random $2^{n/2}$-to-1 function.
  $\Rightarrow H$ is collision resistant.

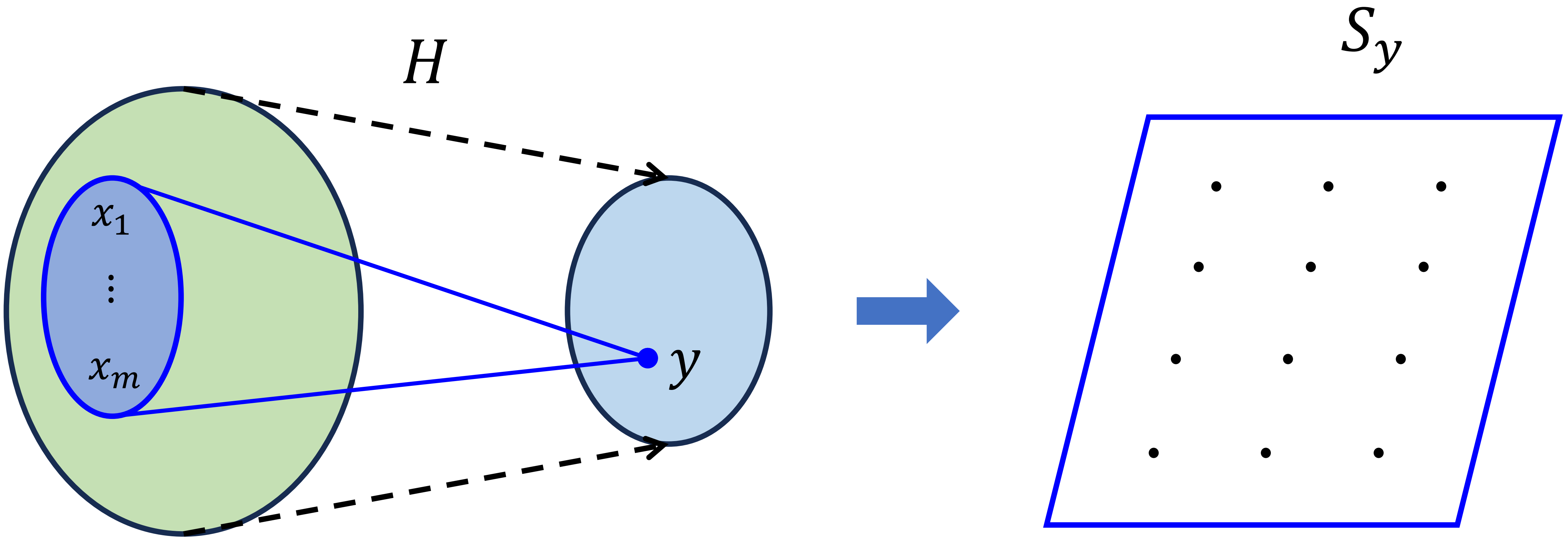
Non-collapsing: How to detect superpositions of preimages of H?

Intuition for Constructing a Non-collapsing CRH



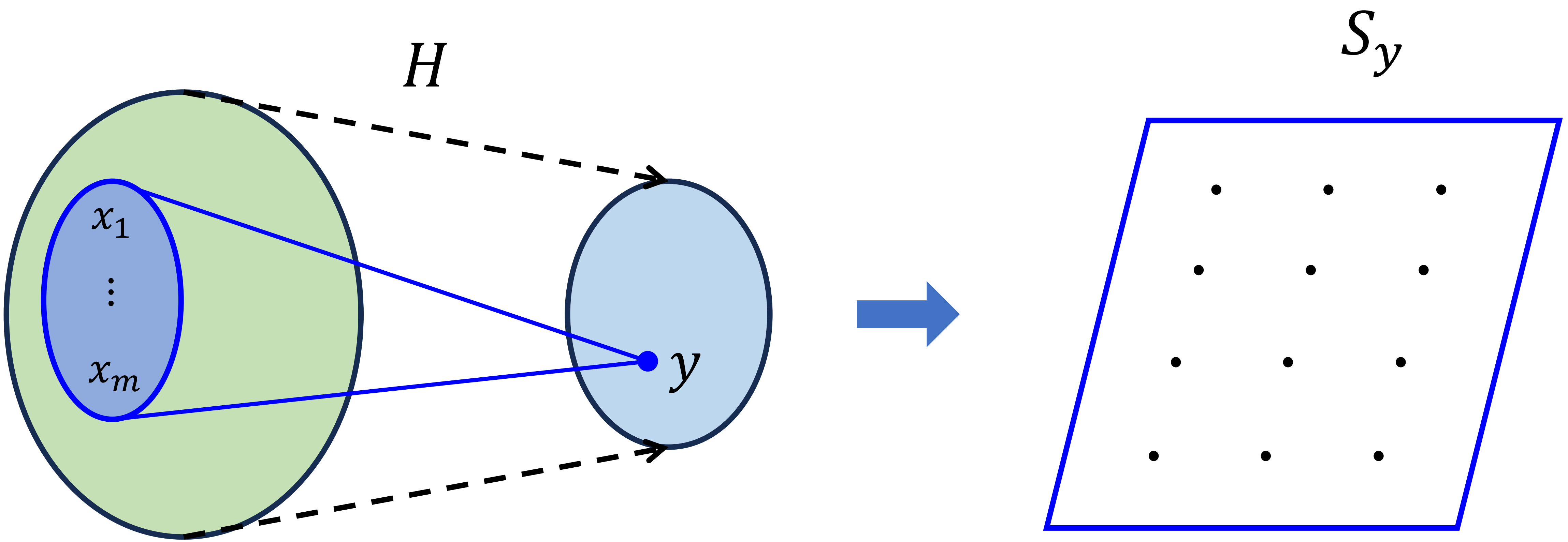
1. Compute H in superposition and measure an output y.

Intuition for Constructing a Non-collapsing CRH



2. Given y, sample a secret sparse subspace $S_y \subseteq \mathbb{Z}_2^k$.

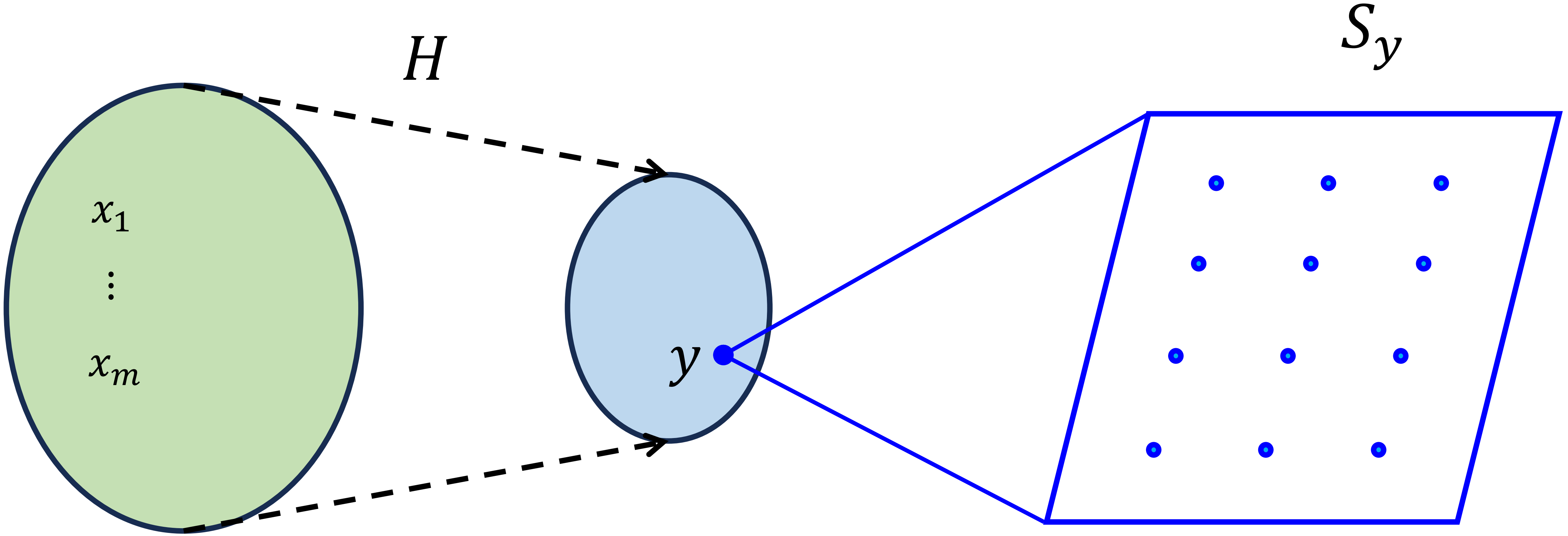
Intuition for Constructing a Non-collapsing CRH



3. Note $\{J(x)\}_{x \in H^{-1}(y)} = \{0,1\}^{n/2}$. We can think of it as $\mathbb{Z}_2^{n/2}$.

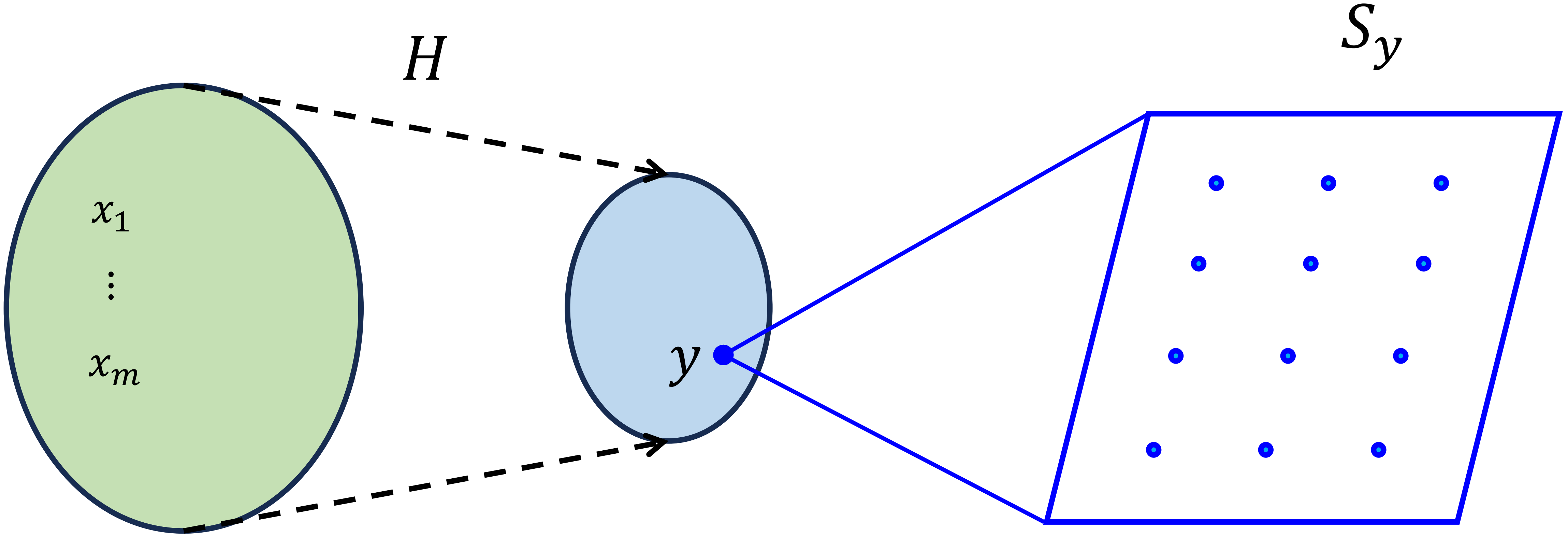
These can be coordinate vectors for S_y .

Intuition for Constructing a Non-collapsing CRH



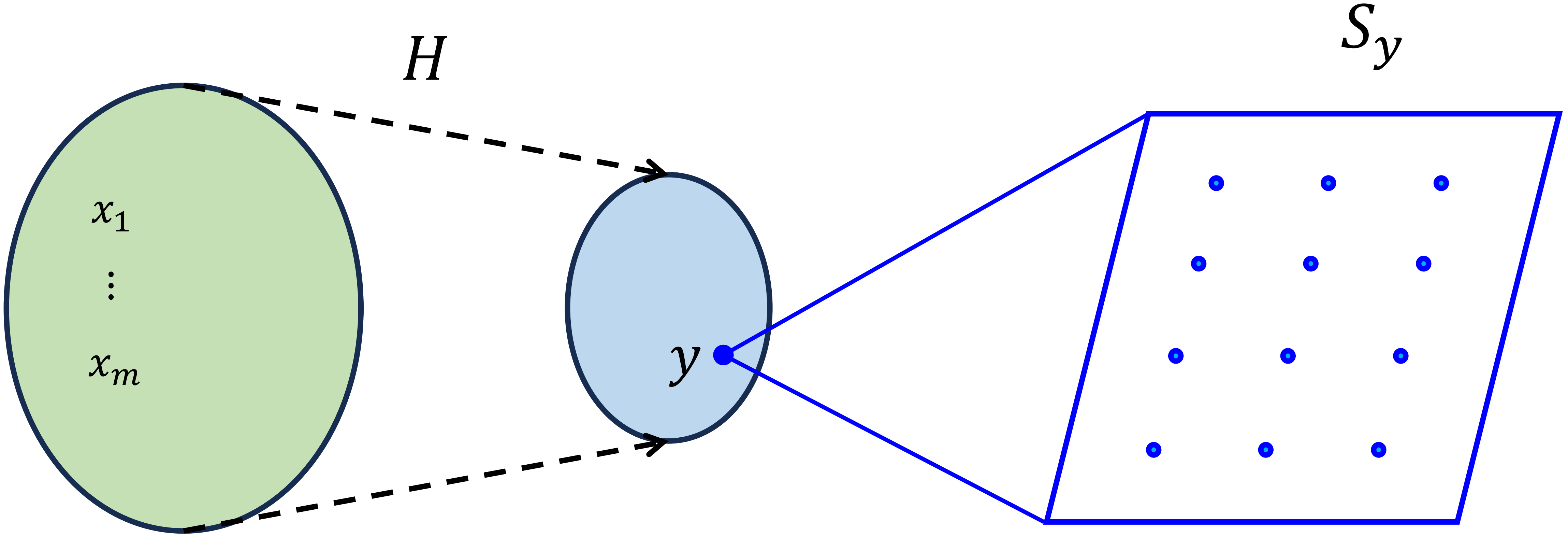
4. We show how to move between $H^{-1}(y)$ and S_y reversibly, while keeping the collision resistance of H.

Intuition for Constructing a Non-collapsing CRH

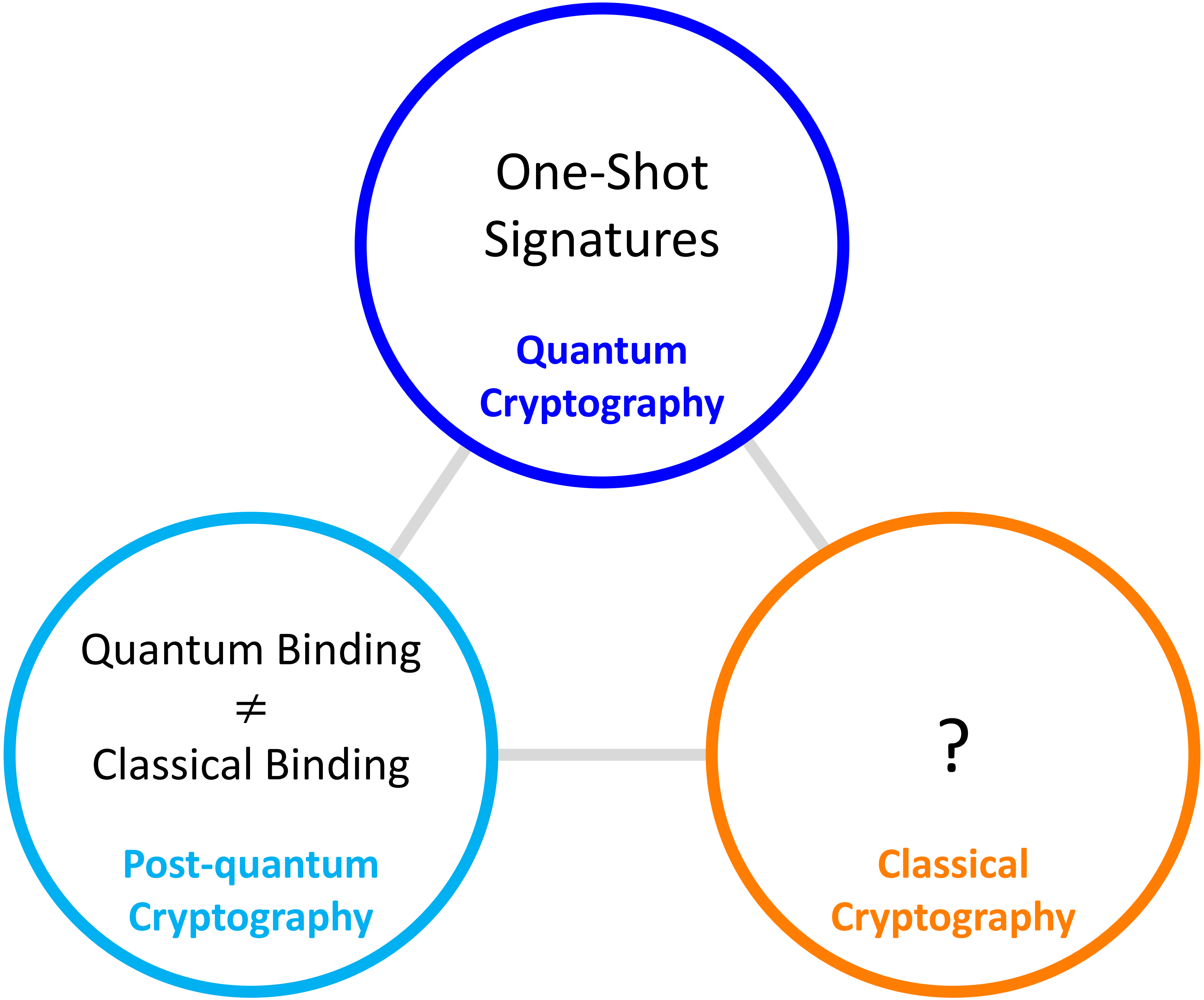


5. By known techniques [A-C-12]: Superposition over S_y can be detected publicly, without revealing it.

Intuition for Constructing a Non-collapsing CRH



In the paper: We show how to formalize these intuitions to get a Non-collapsing CRH in a classical oracle model.


One-Shot Signatures
Quantum Cryptography
Quantum Binding
≠
Classical Binding
Post-quantum Cryptography
?
Classical Cryptography

A word on Standard-Model Security & Obfuscating Pseudorandom Permutations

A word on Standard-Model Security & Obfuscating Pseudorandom Permutations

- In our standard model construction,
  - ➢We use a pseudorandom permutation (PRP) for Π.
  - ➢We use iO to make the scheme public.

A word on Standard-Model Security & Obfuscating Pseudorandom Permutations

- In our standard model construction,
  - ➢We use a pseudorandom permutation (PRP) for Π.
  - ➢We use iO to make the scheme public.
- **The challenge:** We need to obfuscate a PRP (open problem in classical cryptography, for at least a decade).

A word on Standard-Model Security & Obfuscating Pseudorandom Permutations

- In our standard model construction,
  - ➢ We use a pseudorandom permutation (PRP) for Π.
  - ➢ We use iO to make the scheme public.
- **The challenge:** We need to obfuscate a PRP (open problem in classical cryptography, for at least a decade).
- We define a new notion: Permutable PRPs.
- Permutable PRPs allow: $iO(\Pi) \approx_c iO(\Gamma \circ \Pi)$, for a known Γ.

A word on Standard-Model Security & Obfuscating Pseudorandom Permutations

We show how to obfuscate a permutable PRP and make the circuit public, without revealing the PRP.

A word on Standard-Model Security & Obfuscating Pseudorandom Permutations

We show how to obfuscate a permutable PRP and make the circuit public, without revealing the PRP.

Theorem 3:

Assume,

- Sub-exponentially-secure **One-Way Functions**, and
- Sub-exponentially-secure **iO** for classical circuits.

Then, ∃ a **trapdoor one-way permutation** with domain $\{0,1\}^n$.

Two Open Problems

Two Open Problems

1. What classes of permutations Γ can we permute by?

Two Open Problems

1. What classes of permutations Γ can we permute by?

- We have $iO(\Pi) \approx_c iO(\Gamma \circ \Pi)$ only if Γ is "decomposable".

Two Open Problems

1. What classes of permutations Γ can we permute by?

- We have $iO(\Pi) \approx_c iO(\Gamma \circ \Pi)$ only if Γ is "decomposable".
- A purely combinatorial question: What permutations Γ are decomposable?

Two Open Problems

1. What classes of permutations Γ can we permute by?

- We have $iO(\Pi) \approx_c iO(\Gamma \circ \Pi)$ only if Γ is “decomposable”.
- A purely combinatorial question: What permutations Γ are decomposable?

2. Can we construct One-Shot Signatures (or even weaker primitives) **without** indistinguishability obfuscation?

Questions?