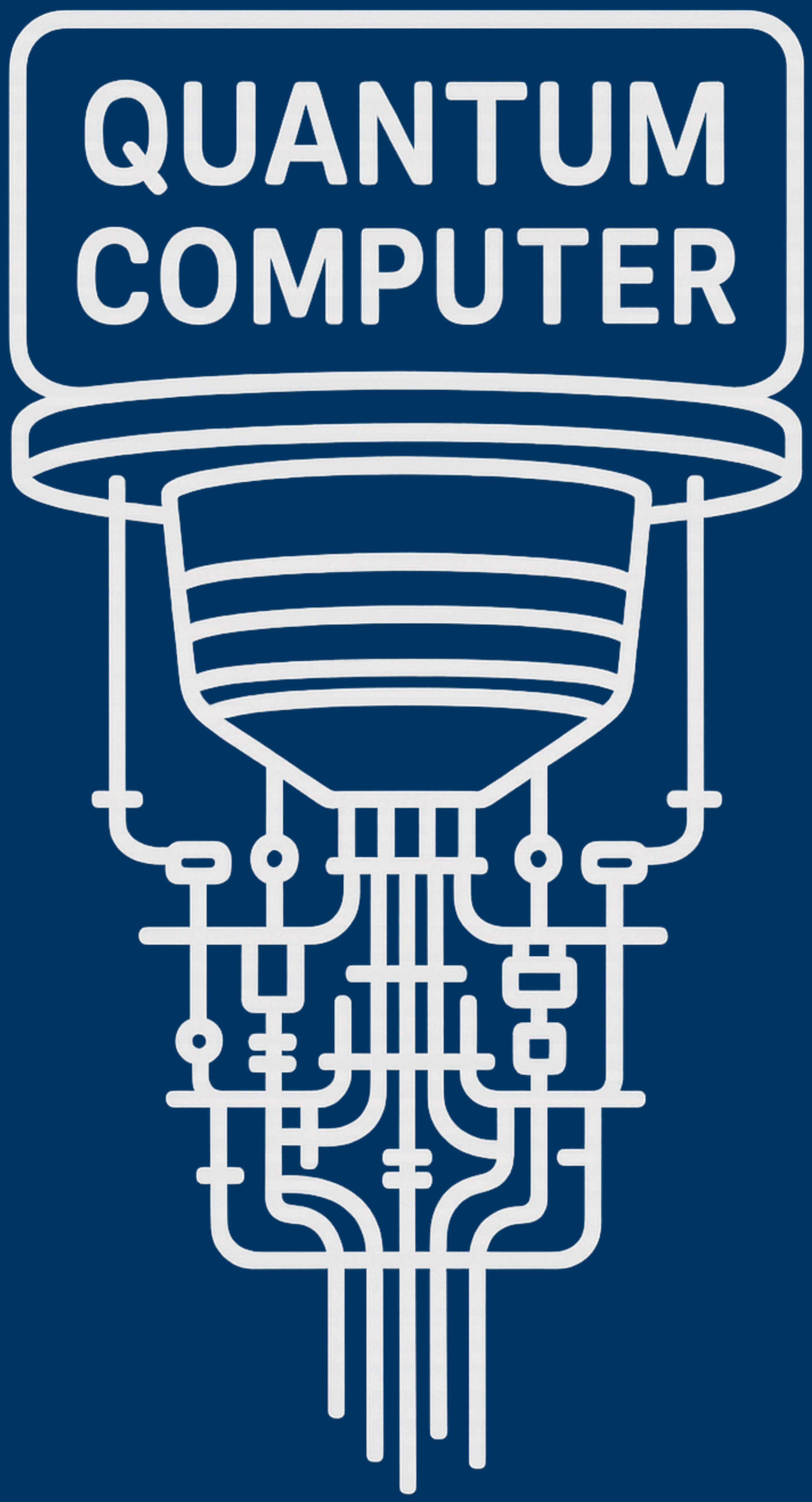
How to Verify that a Small Device is Quantum, Unconditionally

Giulio Malavolta

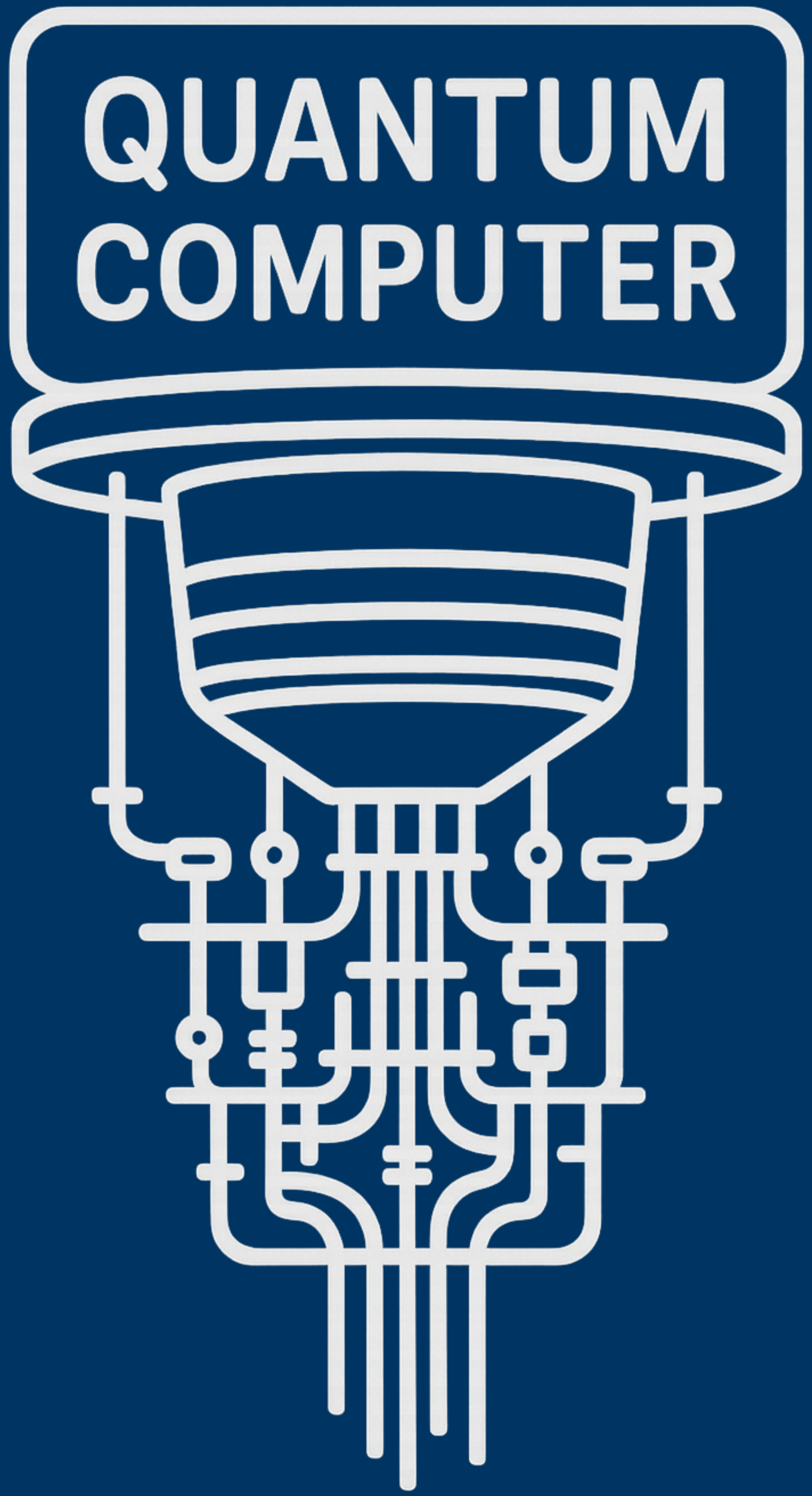
Bocconi University

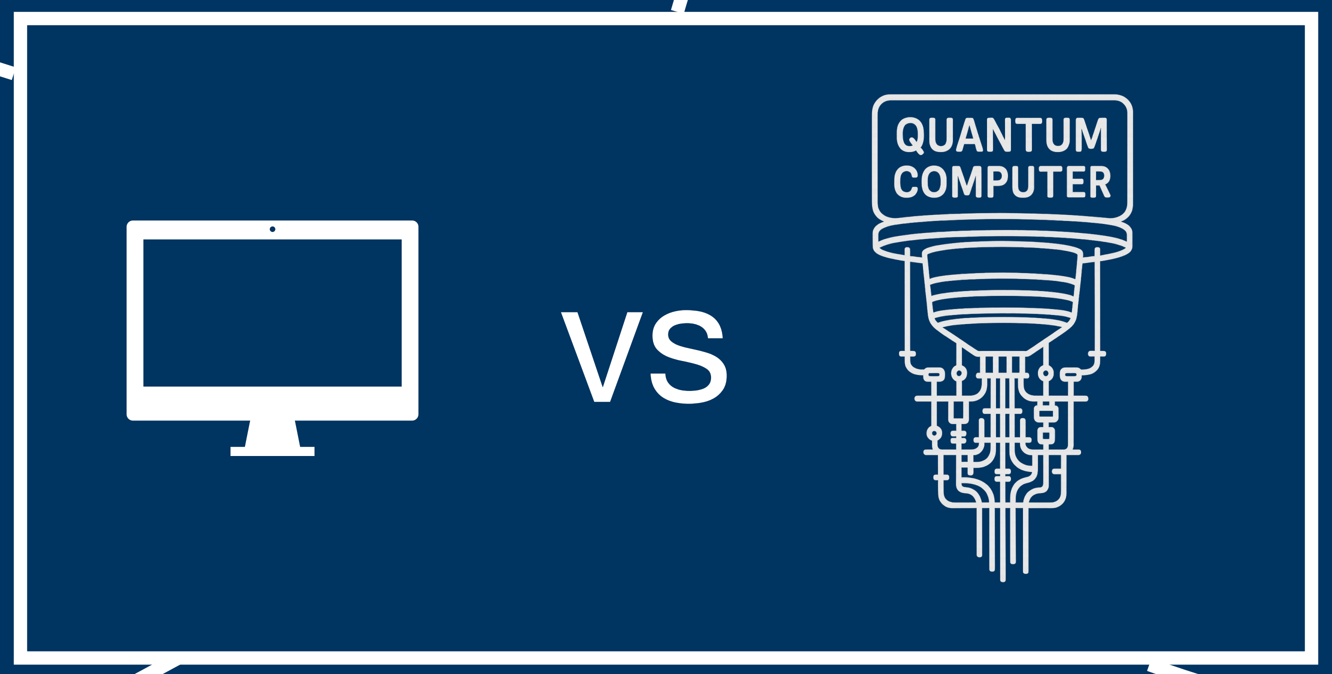
Based on joint work with Tamer Mour


QUANTUM
COMPUTER

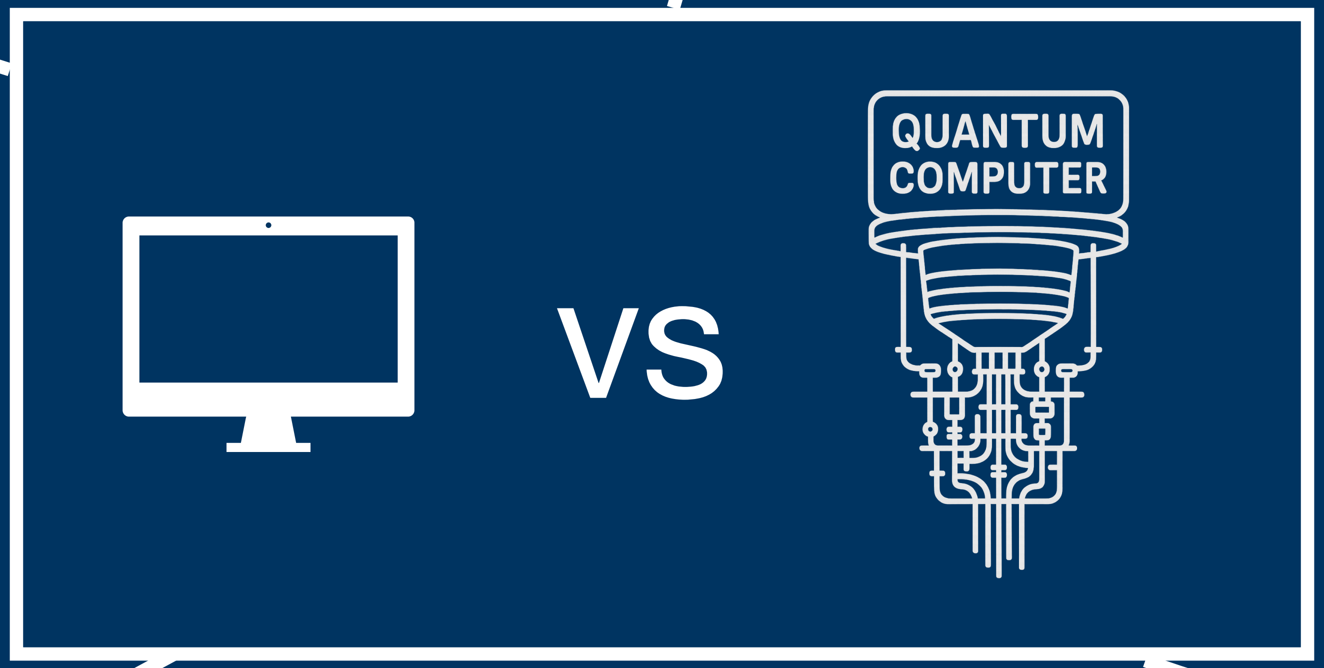
Is my computer **really** quantum?

Can my quantum computer calculate something that classical computers cannot?

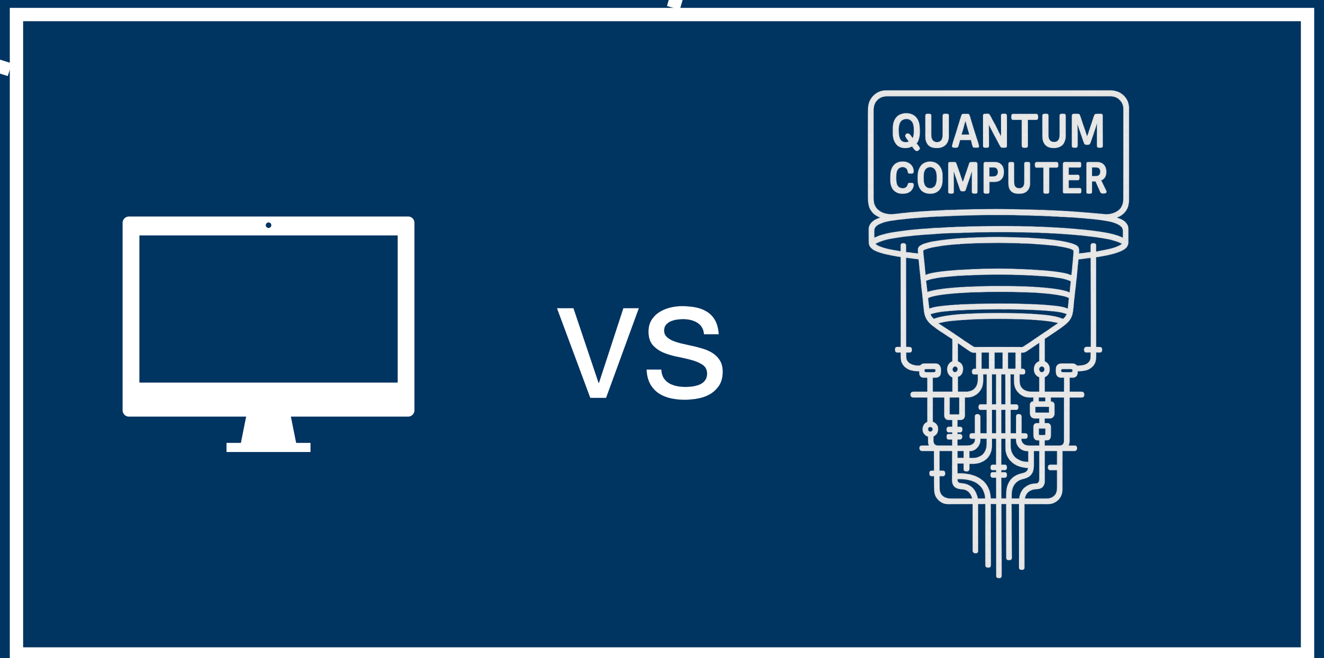



VS
QUANTUM
COMPUTER

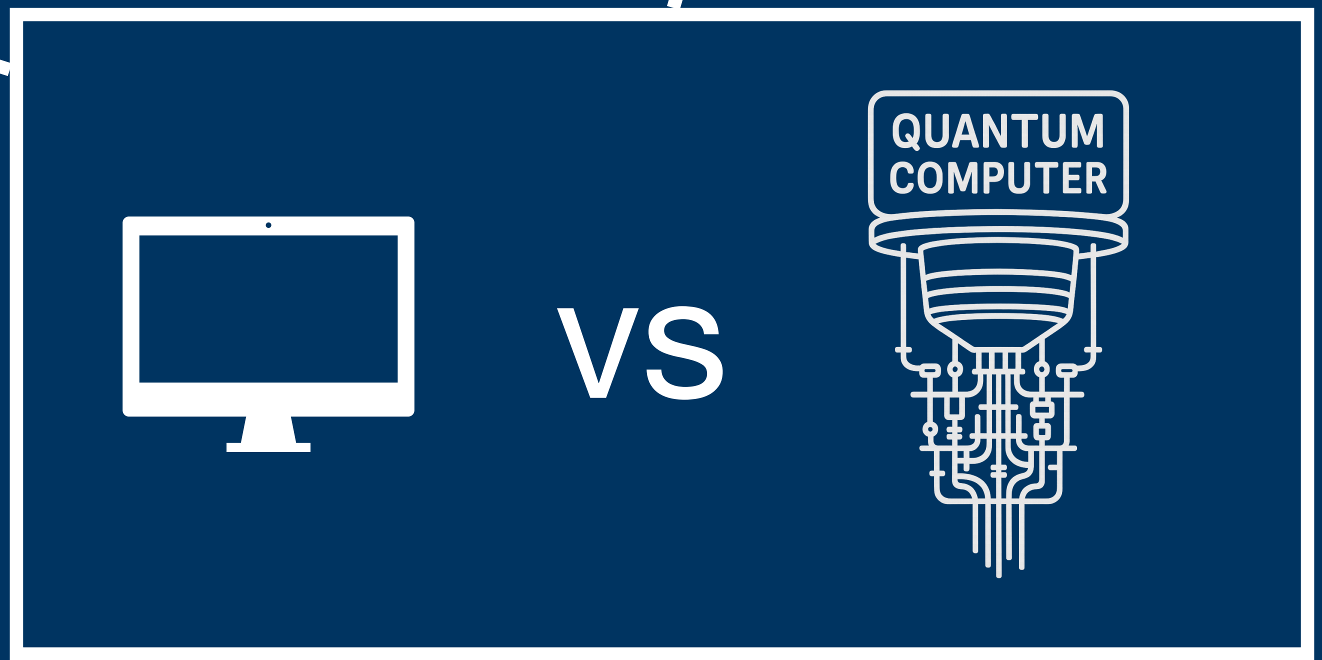
Bell inequalities / Nonlocal games



~~Bell inequalities / Nonlocal games~~



~~Bell inequalities / Nonlocal games~~



Factoring

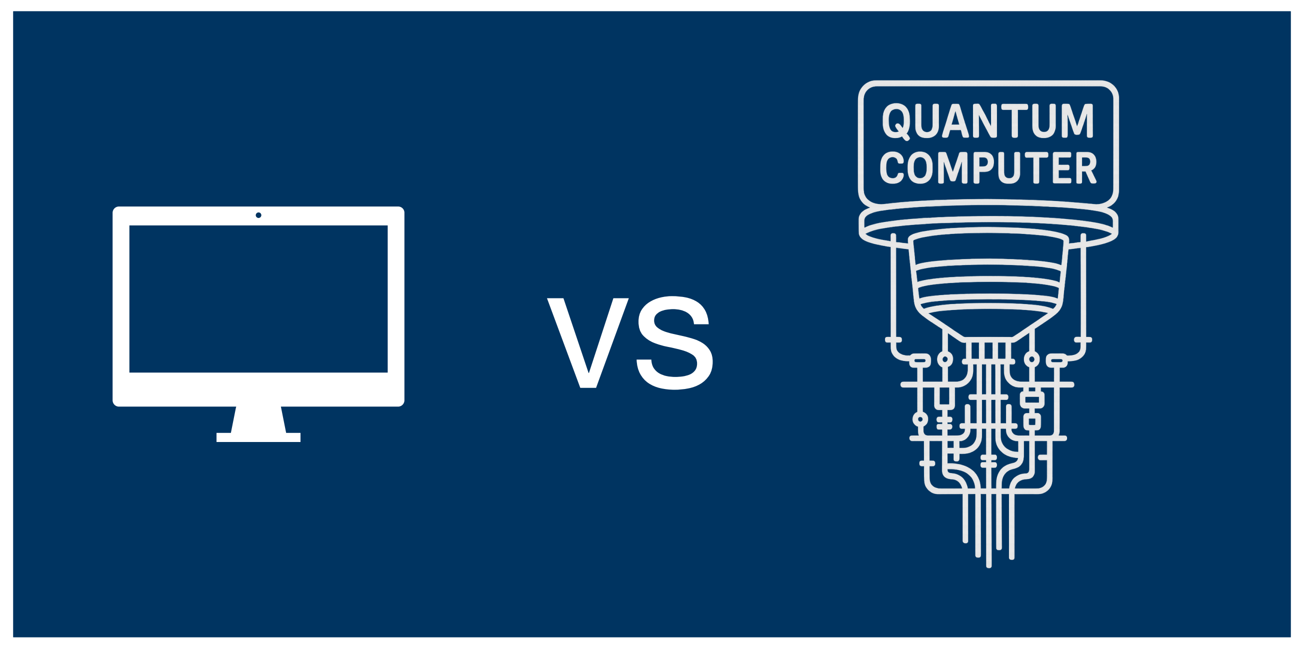
Yamakawa-Zhandry

Compiled nonlocal games

Cryptographic test of quantumness

~~Bell inequalities / Nonlocal games~~

Circuit / Boson Sampling



Factoring

Yamakawa-Zhandry

Compiled nonlocal games

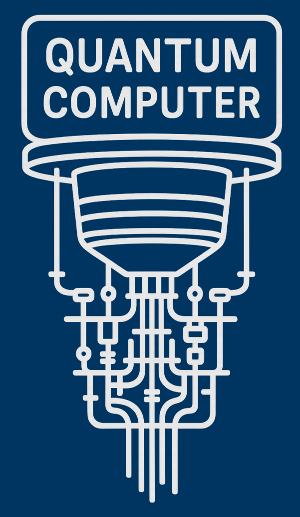
Cryptographic test of quantumness

~~Bell inequalities / Nonlocal games~~

Circuit / Boson Sampling

QAOA / Quantum ML

vs



Factoring

Yamakawa-Zhandry

Compiled nonlocal games

Cryptographic test of quantumness

~~Bell inequalities / Nonlocal games~~

Circuit / Boson Sampling

QAOA / Quantum ML

vs

BQP ≠ BPP

Factoring

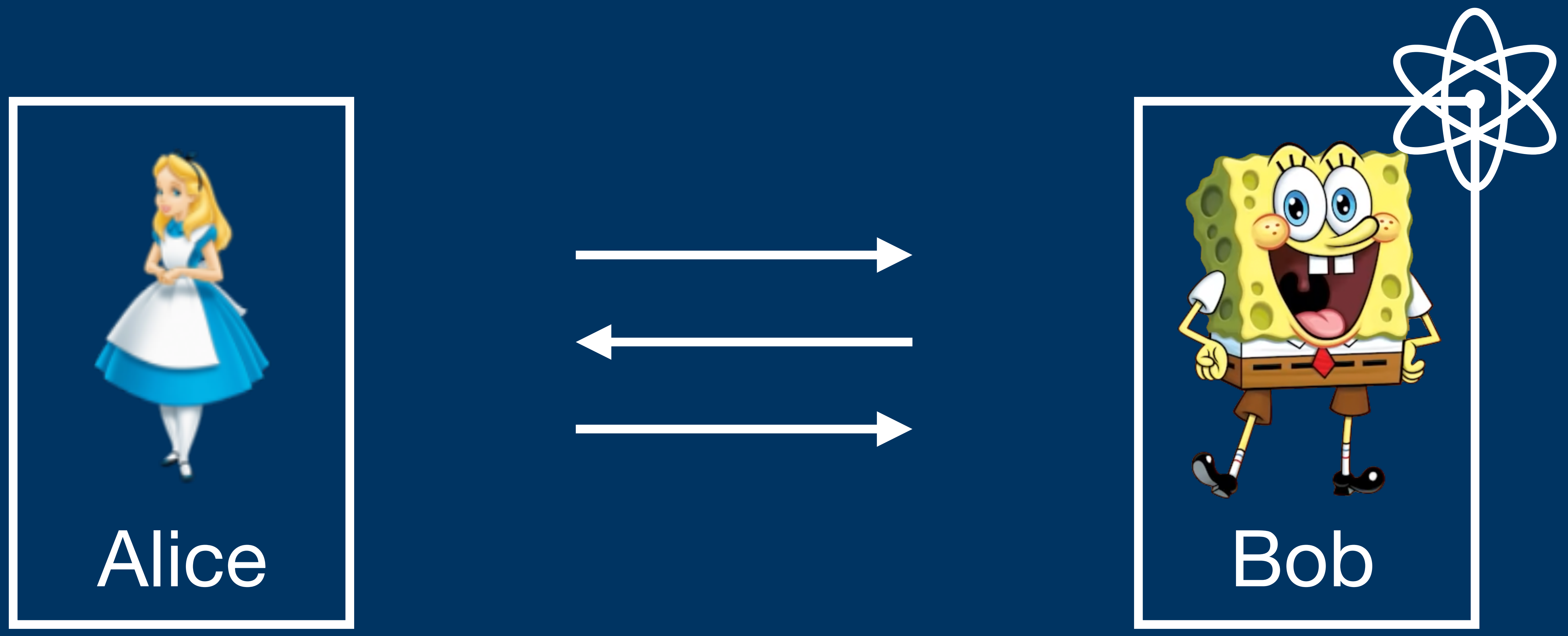
Yamakawa-Zhandry

Compiled nonlocal games

Cryptographic test of quantumness

IDEA: CONSTRAIN SPACE INSTEAD OF TIME

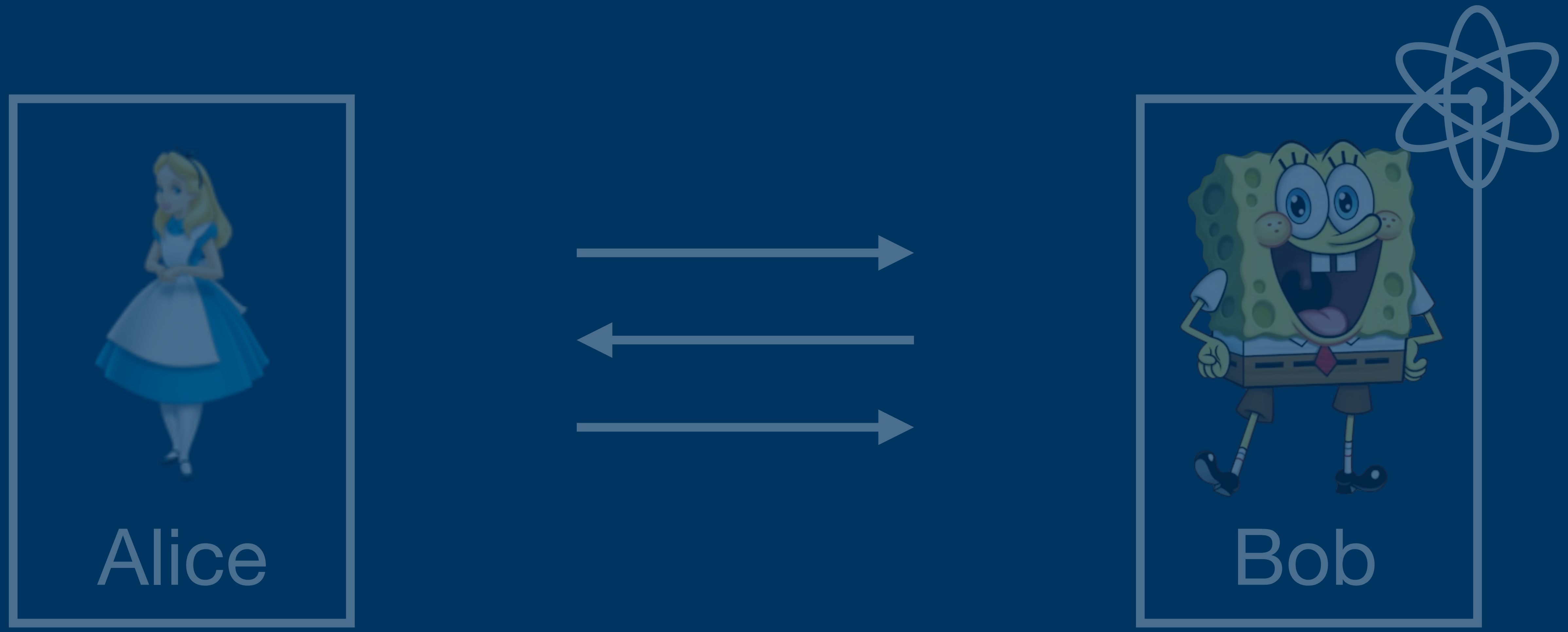
QUANTUM EASY



YES!

Efficiency: Memory of Alice and Bob $o(N)$
Runtime of Alice and Bob $O(N)$

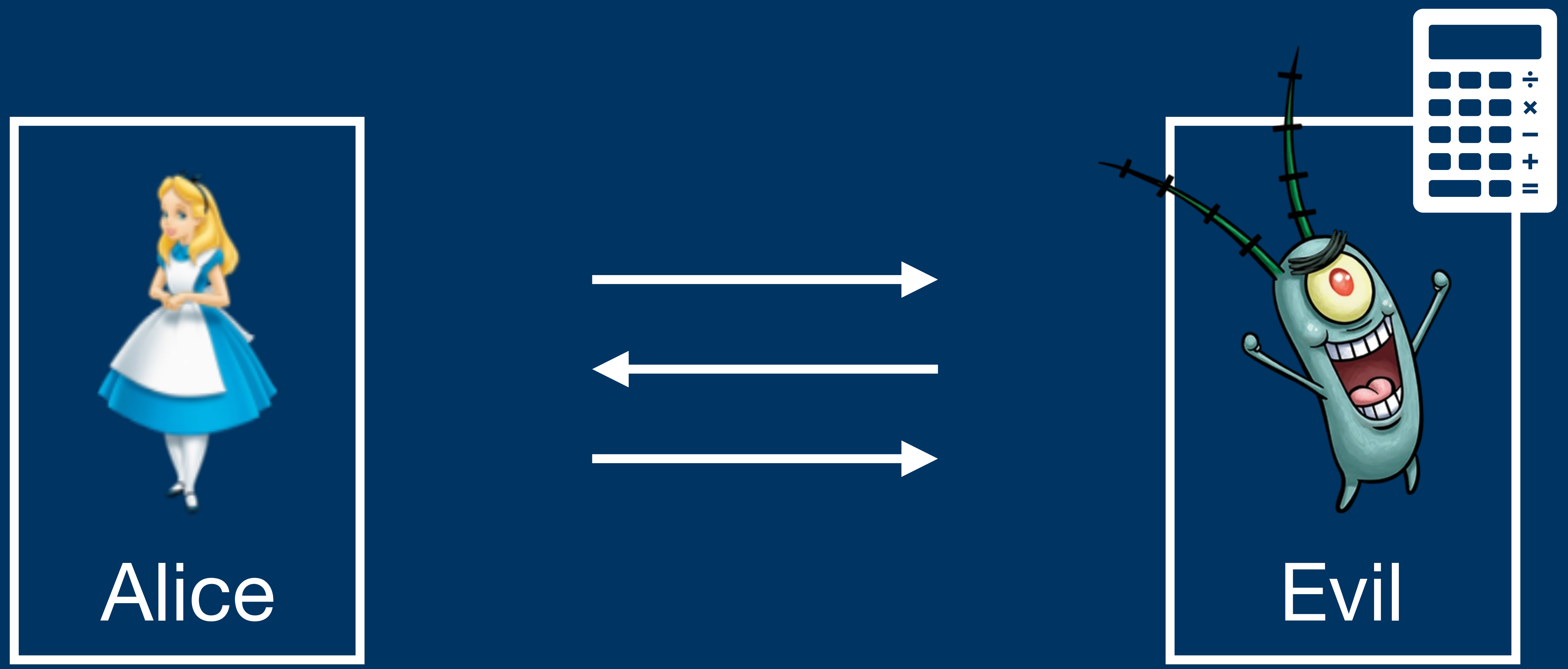
QUANTUM EASY



YES!

Efficiency: Memory of Alice and Bob $o(N)$
Runtime of Alice and Bob $O(N)$

CLASSICAL HARD



NO!

Soundness: Unconditional against *classical* attackers with $o(N)$-bits of memory

THEOREM 1:

Proof of quantumness (PoQ) complete with $O(n)$ memory and sound against classical attackers with $o(n^2)$ memory

THEOREM 1:

Proof of quantumness (PoQ) complete with $O(n)$ memory and sound against classical attackers with $o(n^2)$ memory

THEOREM 2:

PoQ complete with $O(\text{poly} \log n)$ memory and sound against classical attackers with $o(n)$ memory

THEOREM 1:

Proof of quantumness (PoQ) complete with $O(n)$ memory and sound against classical attackers with $o(n^2)$ memory

THEOREM 2:

PoQ complete with $O(\text{poly} \log n)$ memory and sound against classical attackers with $o(n)$ memory

THEOREM 3:

BQP verification against memory-bounded *quantum* attackers

THEOREM 1:

Proof of quantumness (PoQ) complete with $O(n)$ memory and sound against classical attackers with $o(n^2)$ memory

THEOREM 2:

PoQ complete with $O(\text{poly}\log n)$ memory and sound against classical attackers with $o(n)$ memory

THEOREM 3:

BQP verification against memory-bounded *quantum* attackers

$s \sim \mathbb{F}_2^n$

$s \sim \mathbb{F}_2^n$

$a_1 \sim \mathbb{F}_2^n$

$$a_1, \langle a_1, s \rangle \longrightarrow$$

$s \sim \mathbb{F}_2^n$

$a_1 \sim \mathbb{F}_2^n$

$\vdots$

$$\xrightarrow{a_1, \langle a_1, s \rangle}$$

$s \sim \mathbb{F}_2^n$

$a_1 \sim \mathbb{F}_2^n$

$$a_1, \langle a_1, s \rangle \longrightarrow$$

$\vdots$

$a_i \sim \mathbb{F}_2^n$

$$a_i, \langle a_i, s \rangle \longrightarrow$$

$s \sim \mathbb{F}_2^n$

$a_1 \sim \mathbb{F}_2^n$ $\xrightarrow{a_1, \langle a_1, s \rangle}$

$\vdots$

$a_i \sim \mathbb{F}_2^n$ $\xrightarrow{a_i, \langle a_i, s \rangle}$

Objective: Find s

Classical Hardness: [Raz'18]

$s \sim \mathbb{F}_2^n$

$a_1 \sim \mathbb{F}_2^n$ $\xrightarrow{a_1, \langle a_1, s \rangle}$

$\vdots$

$a_i \sim \mathbb{F}_2^n$ $\xrightarrow{a_i, \langle a_i, s \rangle}$

Objective: Find s

Classical Hardness: [Raz'18]

Quantum Easy: ???

$s \sim \mathbb{F}_2^n$

$a_1 \sim \mathbb{F}_2^n$ $\quad a_1, \langle a_1, s \rangle \longrightarrow$

$\vdots$

$a_i \sim \mathbb{F}_2^n$ $\quad a_i, \langle a_i, s \rangle \longrightarrow$

Objective: Find s

Claw-State Generation

Claw-State Generation

$$\left\{ \frac{|x_0\rangle + |x_1\rangle}{\sqrt{2}} \right\}_{x_0,x_1}$$

Claw-State Generation

$$\left\{ \frac{|x_0\rangle + |x_1\rangle}{\sqrt{2}} \right\}_{x_0,x_1}$$

Completeness: It is easy to obtain a copy of such state

Claw-State Generation

$$\left\{ \frac{|x_0\rangle + |x_1\rangle}{\sqrt{2}} \right\}_{x_0,x_1}$$

Completeness: It is easy to obtain a copy of such state

Claw-Freeness: It is hard to output both x_0 and x_1

$|x_0\rangle + |x_1\rangle$

[KMCVY22,BGK+23]

$r \sim \mathscr{U}$

$|x_0\rangle + |x_1\rangle$

r

$\longrightarrow$

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r

$\longrightarrow$

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

$\xrightarrow{\quad r \quad}$

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r

$\longrightarrow$

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

d

$\longleftarrow$

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

d

CHSH Test

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

d

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r →

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

← d

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

θ →

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r →

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

← d

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

θ →

measure in the basis

$\{\cos\theta|0\rangle + \sin\theta|1\rangle, \cos\theta|0\rangle - \sin\theta|1\rangle\}$

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

d

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

θ

measure in the basis

$\{\cos\theta|0\rangle + \sin\theta|1\rangle, \cos\theta|0\rangle - \sin\theta|1\rangle\}$

b

[KMCVY22,BGK+23]

$r \sim \mathcal{U}$

$|x_0\rangle + |x_1\rangle$

r

$|x_0, \langle x_0, r\rangle\rangle + |x_1, \langle x_1, r\rangle\rangle$

measure 1st register in Hadamard basis

d

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

θ

measure in the basis

$\{\cos\theta|0\rangle + \sin\theta|1\rangle, \cos\theta|0\rangle - \sin\theta|1\rangle\}$

b

Accept if the most likely outcome

[KMCVY22,BGK+23]

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

θ →

measure in the basis

$\{\cos\theta|0\rangle + \sin\theta|1\rangle, \cos\theta|0\rangle - \sin\theta|1\rangle\}$

b ←

Accept if the most likely outcome

[KMCVY22,BGK+23]

A **quantum** prover succeeds with probability $\cos^2 \pi/8 \approx 0.853$

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

θ →

measure in the basis

$\{\cos\theta|0\rangle + \sin\theta|1\rangle, \cos\theta|0\rangle - \sin\theta|1\rangle\}$

← b

Accept if the most likely outcome

[KMCVY22,BGK+23]

A **quantum** prover succeeds with probability $\cos^2 \pi/8 \approx 0.853$

A **classical** prover can be used to extract a **claw**

CHSH Test

$\theta \sim \{-\pi/8, +\pi/8\}$

θ →

measure in the basis

$\{\cos\theta|0\rangle + \sin\theta|1\rangle, \cos\theta|0\rangle - \sin\theta|1\rangle\}$

← b

Accept if the most likely outcome

[KMCVY22,BGK+23]

NEXT: UNCONDITIONAL CLAW GENERATION

$$\vdots$$

$$v_i = (a_i, \langle a_i, s \rangle)$$

$$\vdots$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s\rangle)$$

$$\longrightarrow$$

$$\vdots$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s\rangle)$$

$$\longrightarrow$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1\rangle, \ldots, \langle x, v_i\rangle\rangle$$

$$\vdots$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s \rangle)$$

$$\longrightarrow$$

$$\vdots$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1 \rangle, \ldots, \langle x, v_i \rangle\rangle$$

$$\vdots$$

$$\sum_x |x, xV\rangle$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s \rangle)$$

$$\longrightarrow$$

$$\vdots$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1 \rangle, \ldots, \langle x, v_i \rangle\rangle$$

$$\vdots$$

$$\sum_x |x, xV\rangle \qquad V \in \mathbb{F}_2^{n+1 \times n+1}$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s \rangle) \longrightarrow$$

$$\vdots$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1 \rangle, \ldots, \langle x, v_i \rangle\rangle$$

$$\vdots$$

$$\sum_x |x, xV\rangle \qquad V \in \mathbb{F}_2^{n+1 \times n+1}$$

$$\mathrm{rank}(V) = n$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s\rangle)$$

$$\longrightarrow$$

$$\vdots$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1\rangle, \ldots, \langle x, v_i\rangle\rangle$$

$$\vdots$$

$$\sum_x |x, xV\rangle \qquad V \in \mathbb{F}_2^{n+1 \times n+1}$$

$$\mathrm{rank}(V) = n$$

$$\ker(V) = \{0,(s, -1)\}$$

$\vdots$

$v_i = (a_i, \langle a_i, s \rangle)$

$\longrightarrow$

$\vdots$

$$\sum_x |x\rangle$$

$\vdots$

$$\sum_x |x, \langle x, v_1 \rangle, \ldots, \langle x, v_i \rangle\rangle$$

$\vdots$

$$\sum_x |x, xV\rangle \qquad V \in \mathbb{F}_2^{n+1 \times n+1}$$

$$\text{rank}(V) = n$$

$$\ker(V) = \{0, (s, -1)\}$$

$$\sum_{x : xV = y} |x, y\rangle = |x_0, y\rangle + |x_1, y\rangle$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s \rangle)$$

$$\longrightarrow$$

$$\vdots$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1 \rangle, \ldots, \langle x, v_i \rangle\rangle$$

$$\vdots$$

$$\sum_x |x, xV\rangle \qquad V \in \mathbb{F}_2^{n+1 \times n+1}$$

$$\mathrm{rank}(V) = n$$

$$\ker(V) = \{0, (s, -1)\}$$

$$\sum_{x : xV = y} |x, y\rangle = |x_0, y\rangle + |x_1, y\rangle$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s \rangle)$$

$$\longrightarrow$$

$$\vdots$$

Requires only $O(n)$ qubits

$$\sum_x |x\rangle$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1 \rangle, \ldots, \langle x, v_i \rangle\rangle$$

$$\vdots$$

$$\sum_x |x, xV\rangle \qquad V \in \mathbb{F}_2^{n+1 \times n+1}$$

$$\mathrm{rank}(V) = n$$

$$\ker(V) = \{0, (s, -1)\}$$

$$\sum_{x : xV = y} |x, y\rangle = |x_0, y\rangle + |x_1, y\rangle$$

$$\sum_x |x\rangle$$

$$\vdots$$

$$v_i = (a_i, \langle a_i, s\rangle)$$

$$\vdots$$

$$\sum_x |x, \langle x, v_1\rangle, \ldots, \langle x, v_i\rangle\rangle$$

$$\vdots$$

$$\sum_x |x, xV\rangle \quad V \in \mathbb{F}_2^{n+1\times n+1}$$

$$\mathrm{rank}(V) = n$$

$$\ker(V) = \{0,(s,-1)\}$$

Requires only $O(n)$ qubits

Finding a claw implies learning s

$$x_0 = x_1 + (s,-1)$$

$$\sum_{x:xV=y} |x, y\rangle = |x_0, y\rangle + |x_1, y\rangle$$

OPEN PROBLEMS

OPEN PROBLEMS

1. Learning Parities with Quantum Memory

OPEN PROBLEMS

1. Learning Parities with Quantum Memory

    Possible to get a Grover-like advantage

OPEN PROBLEMS

1. Learning Parities with Quantum Memory

    Possible to get a Grover-like advantage

2. Communication Complexity

OPEN PROBLEMS

1. Learning Parities with Quantum Memory

   Possible to get a Grover-like advantage

2. Communication Complexity

OPEN PROBLEMS

1. Learning Parities with Quantum Memory

   Possible to get a Grover-like advantage

2. Communication Complexity

3. Experiments!

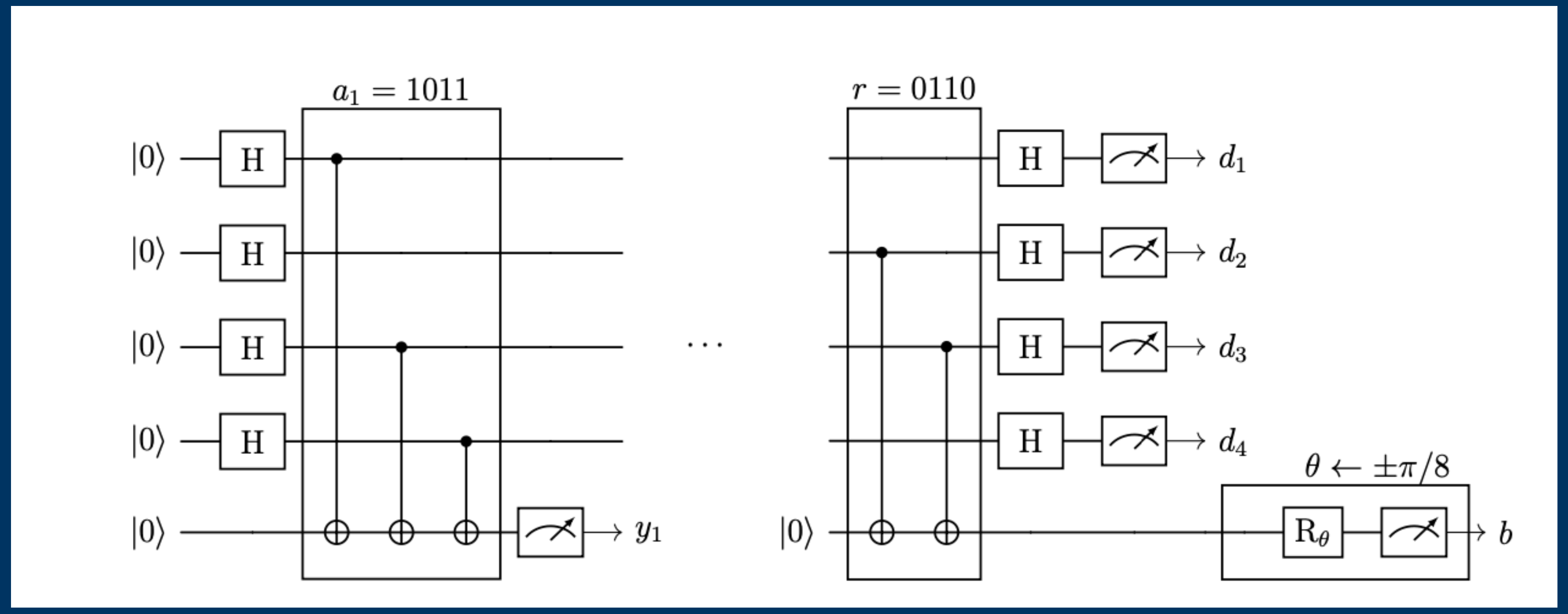
OPEN PROBLEMS

1. Learning Parities with Quantum Memory

   Possible to get a Grover-like advantage

2. Communication Complexity

3. Experiments!



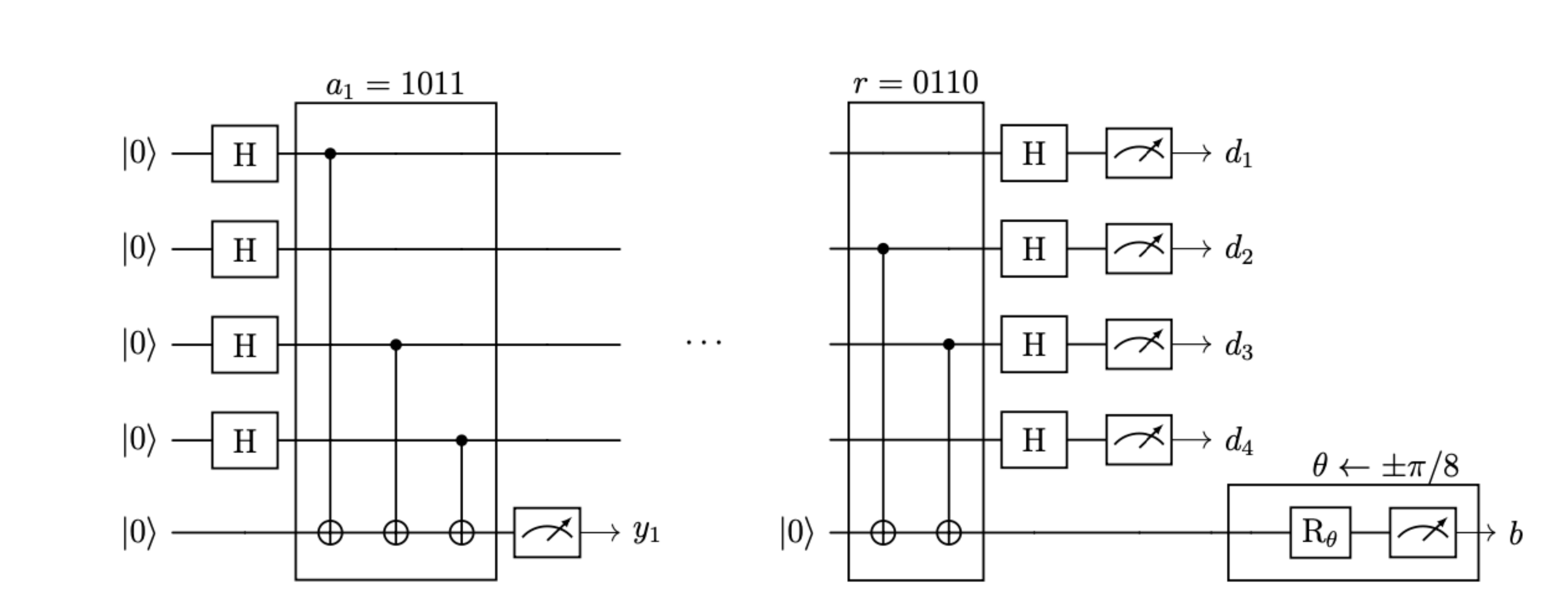
OPEN PROBLEMS

1. Learning Parities with Quantum Memory

   Possible to get a Grover-like advantage

2. Communication Complexity

3. Experiments!



THANK YOU!

https://arxiv.org/abs/2505.23978

THEOREM 1:

Proof of quantumness (PoQ) complete with $O(n)$ memory and sound against classical attackers with $o(n^2)$ memory

THEOREM 2:

PoQ complete with $O(\text{poly}\log n)$ memory and sound against classical attackers with $o(n)$ memory

THEOREM 3:

BQP verification against memory-bounded *quantum* attackers

$\vdots$

$u_i \sim \mathbb{F}_2$ $\xrightarrow{\quad u_i \quad}$

$\vdots$

$u_i \sim \mathbb{F}_2$ $\xrightarrow{u_i}$

$\vdots$

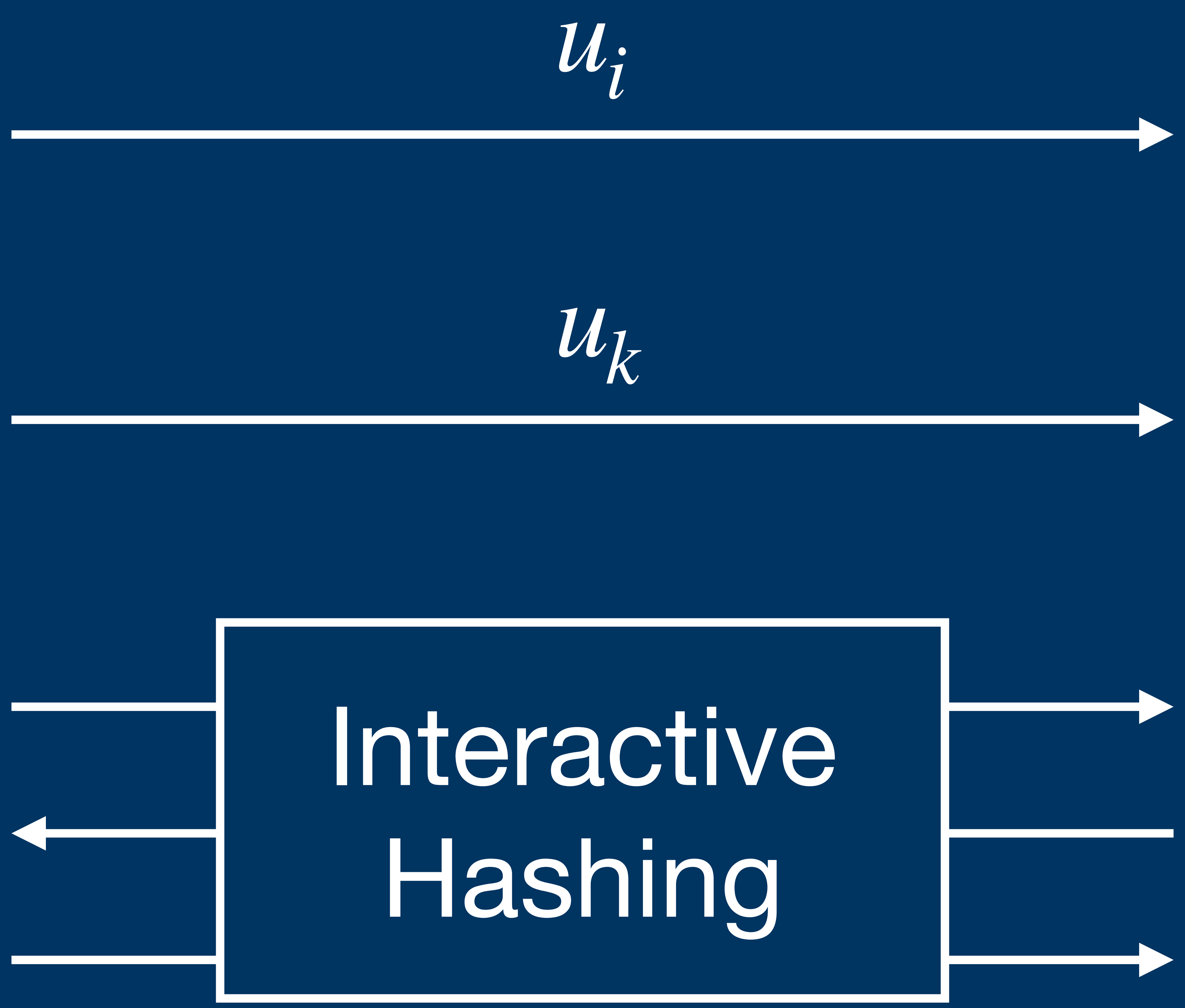
$u_k \sim \mathbb{F}_2$ $\xrightarrow{u_k}$

$\vdots$

$u_i \sim \mathbb{F}_2$

$\vdots$

$u_k \sim \mathbb{F}_2$

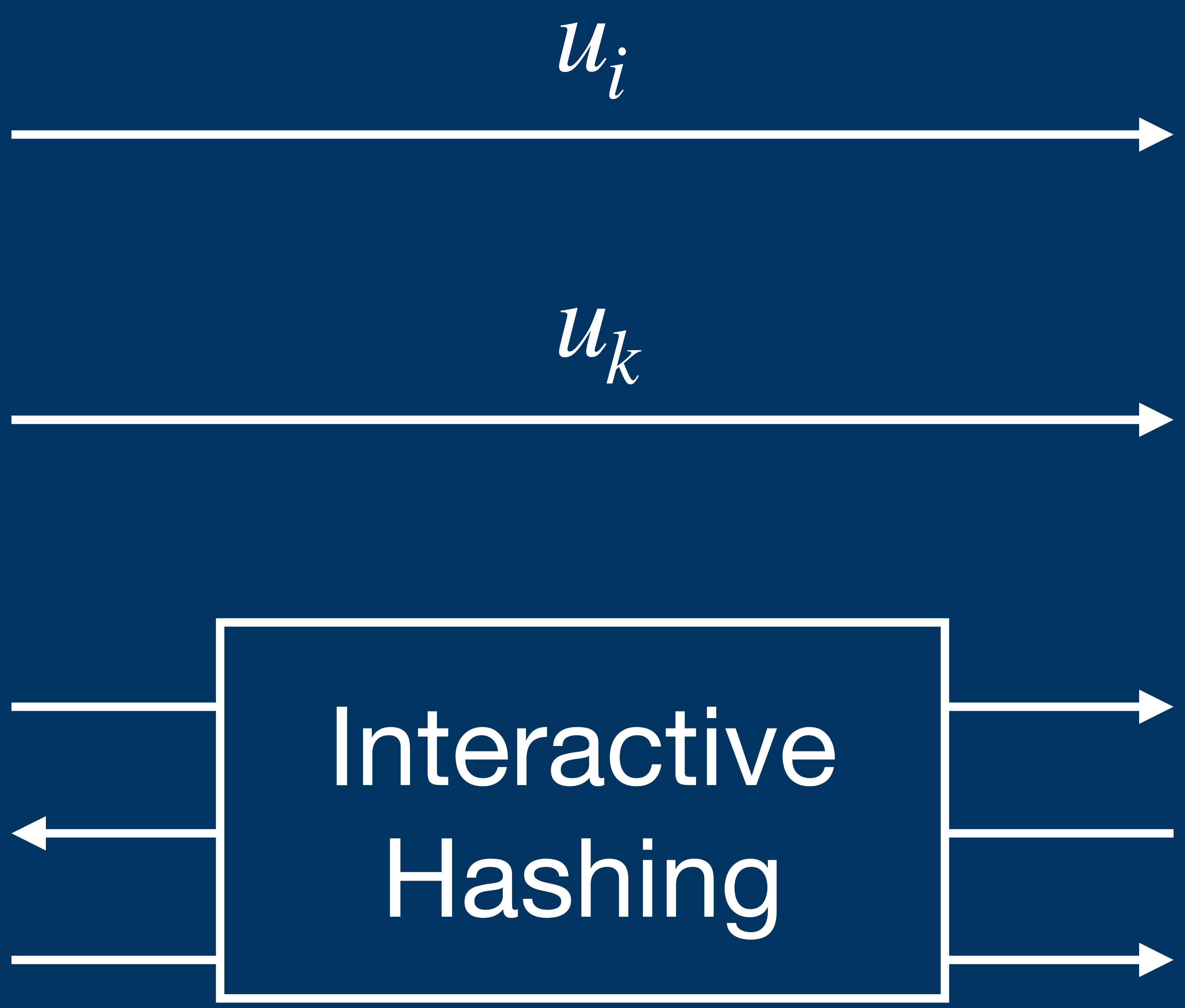


$$\vdots$$

$$u_i \sim \mathbb{F}_2$$

$$\vdots$$

$$u_k \sim \mathbb{F}_2$$



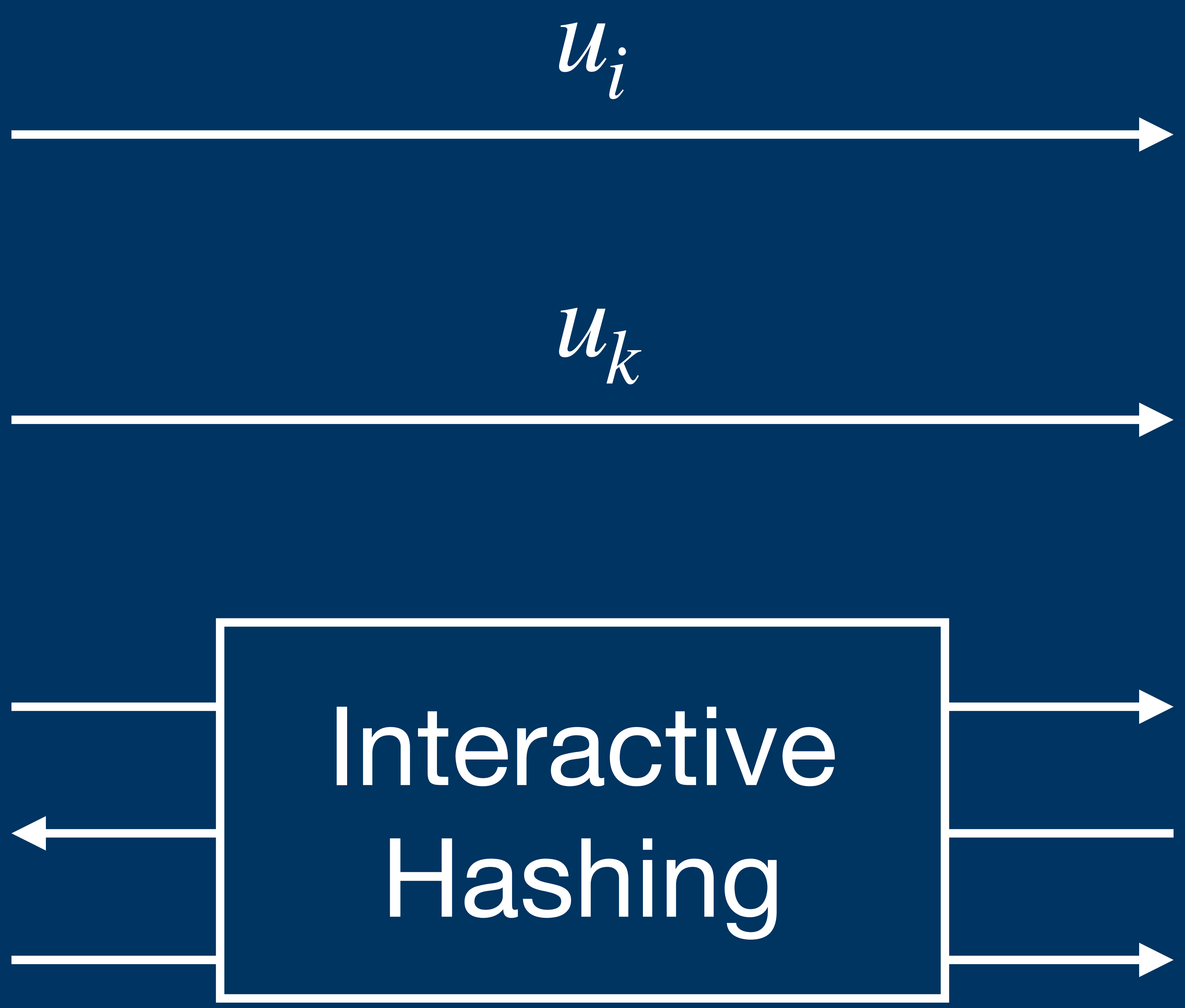
$$y : h^{-1}(y) = \{v_0, v_1\} \in [k]$$

$\vdots$

$u_i \sim \mathbb{F}_2$

$\vdots$

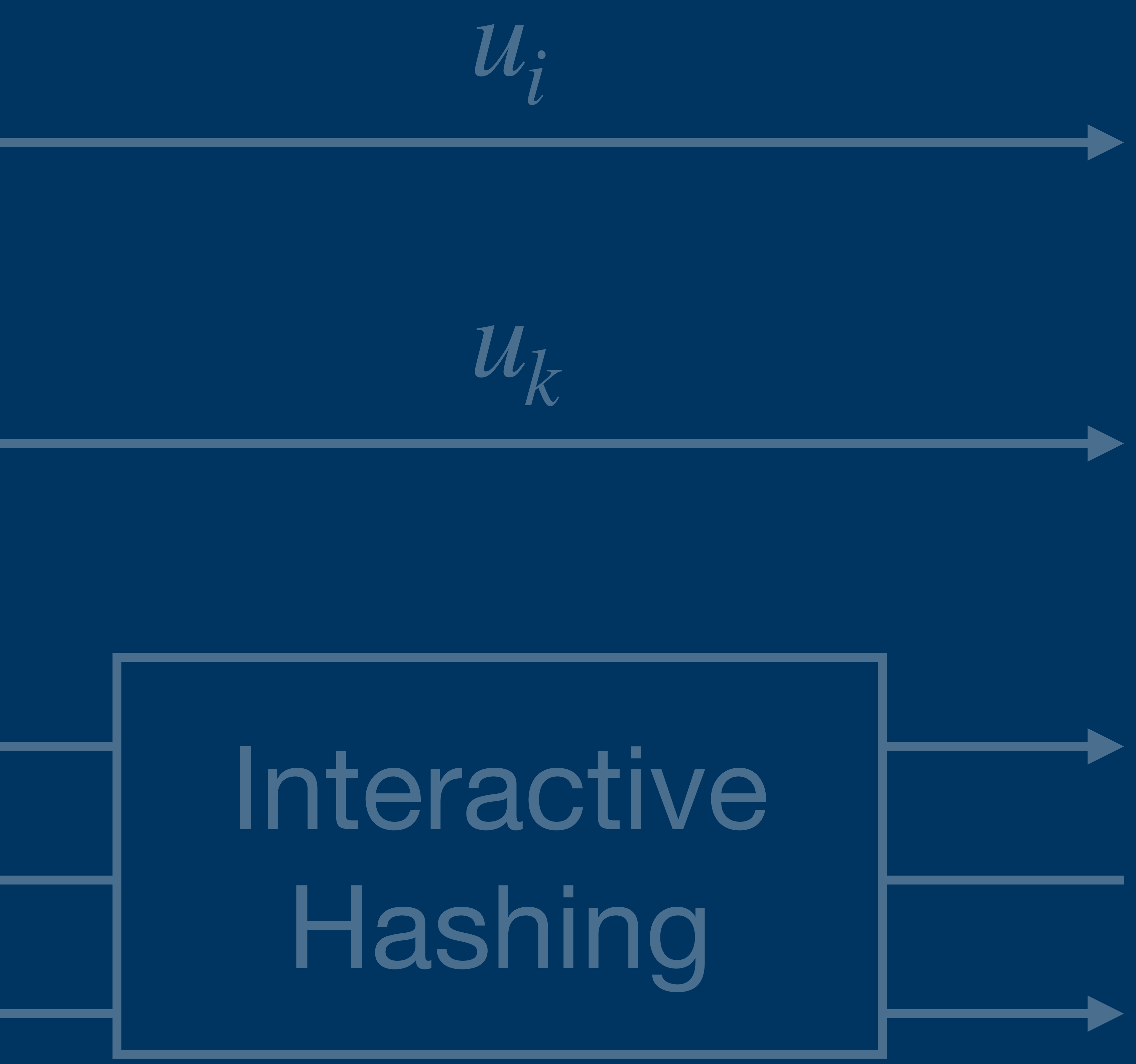
$u_k \sim \mathbb{F}_2$



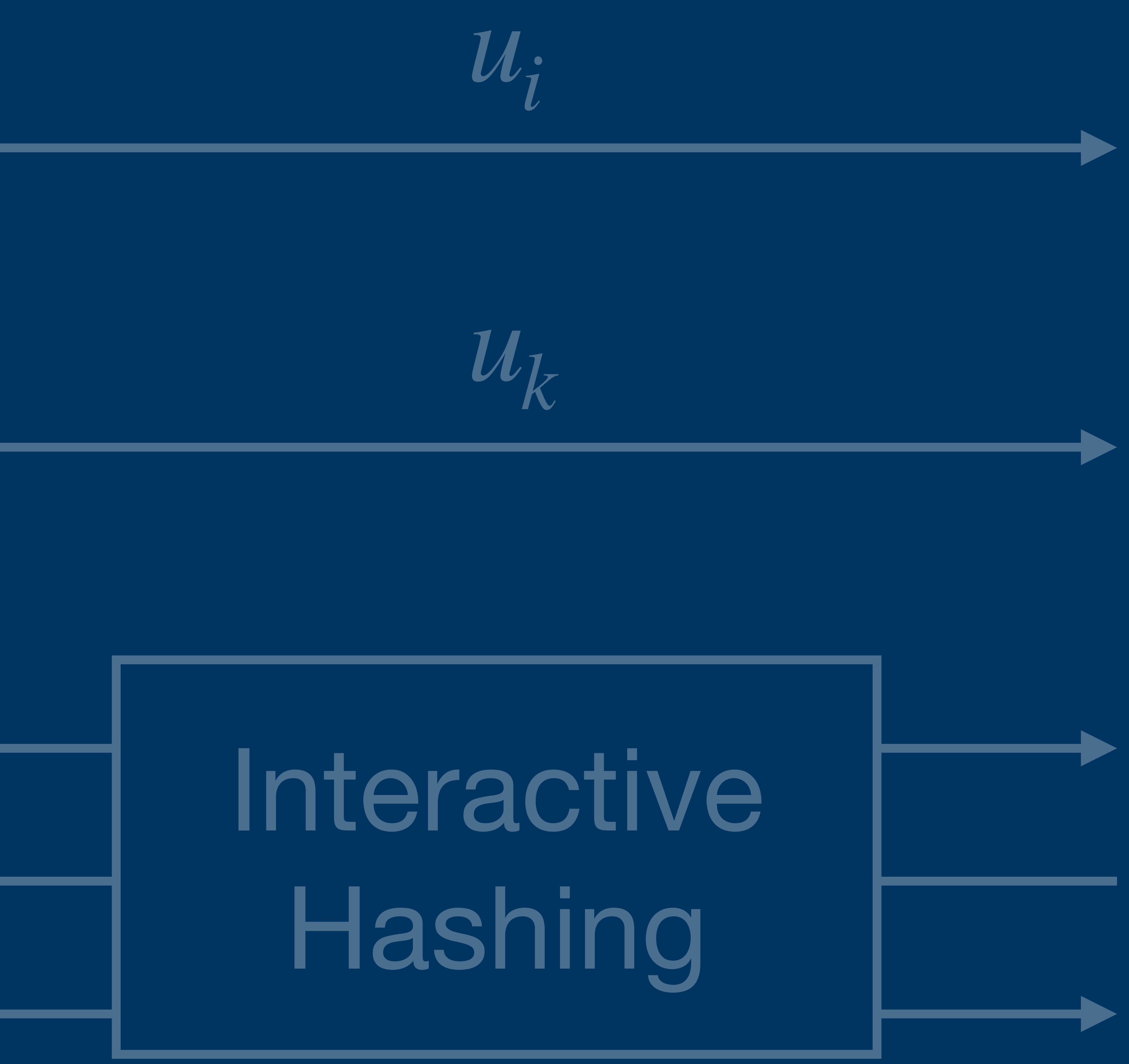
$$y : h^{-1}(y) = \{v_0, v_1\} \in [k]$$

Abort if $\{v_0, v_1\} \neq \{v_0^*, v_1^*\}$

PROVER'S COMPUTATION

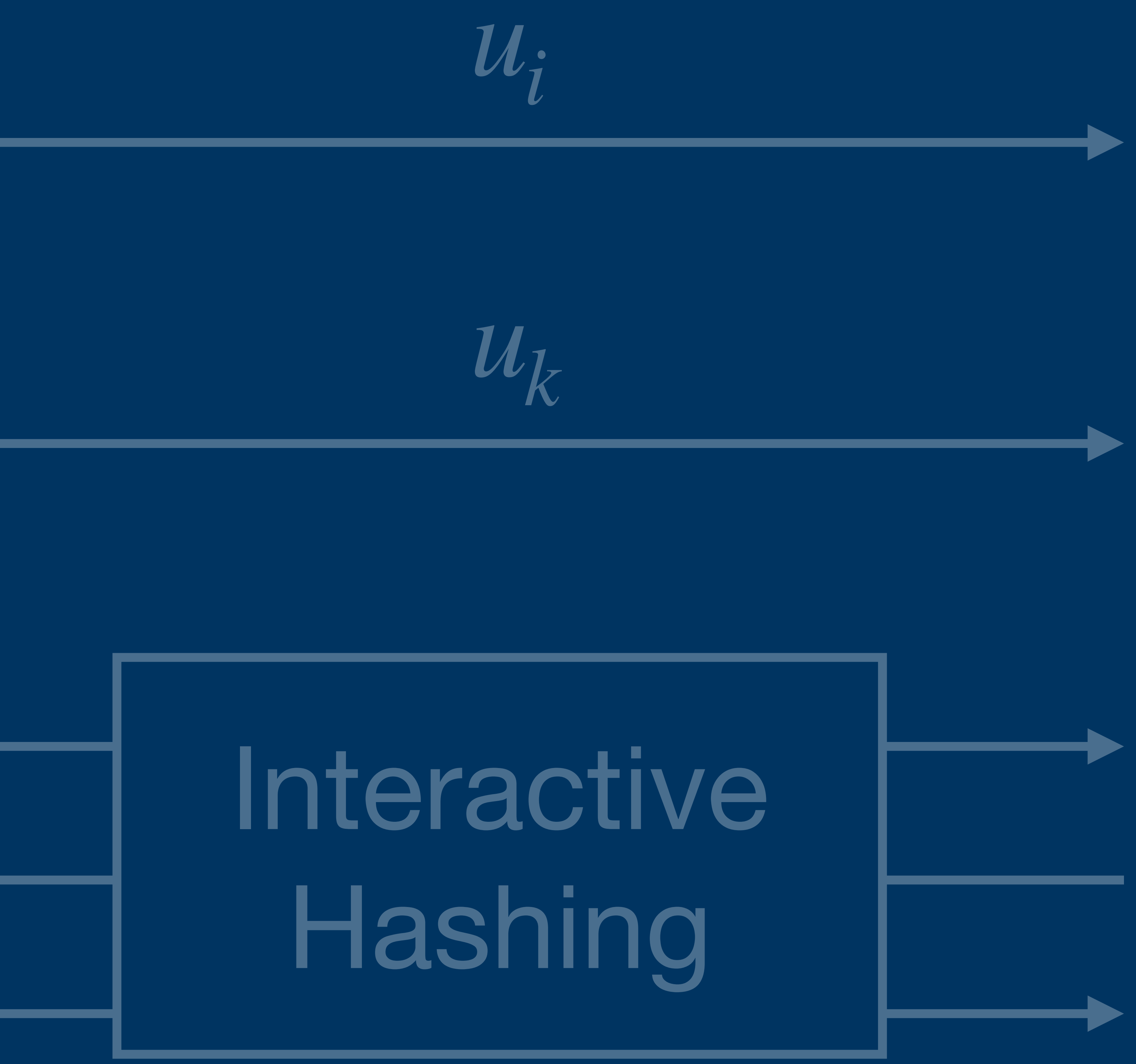


PROVER’S COMPUTATION



$$\sum_v |v\rangle$$

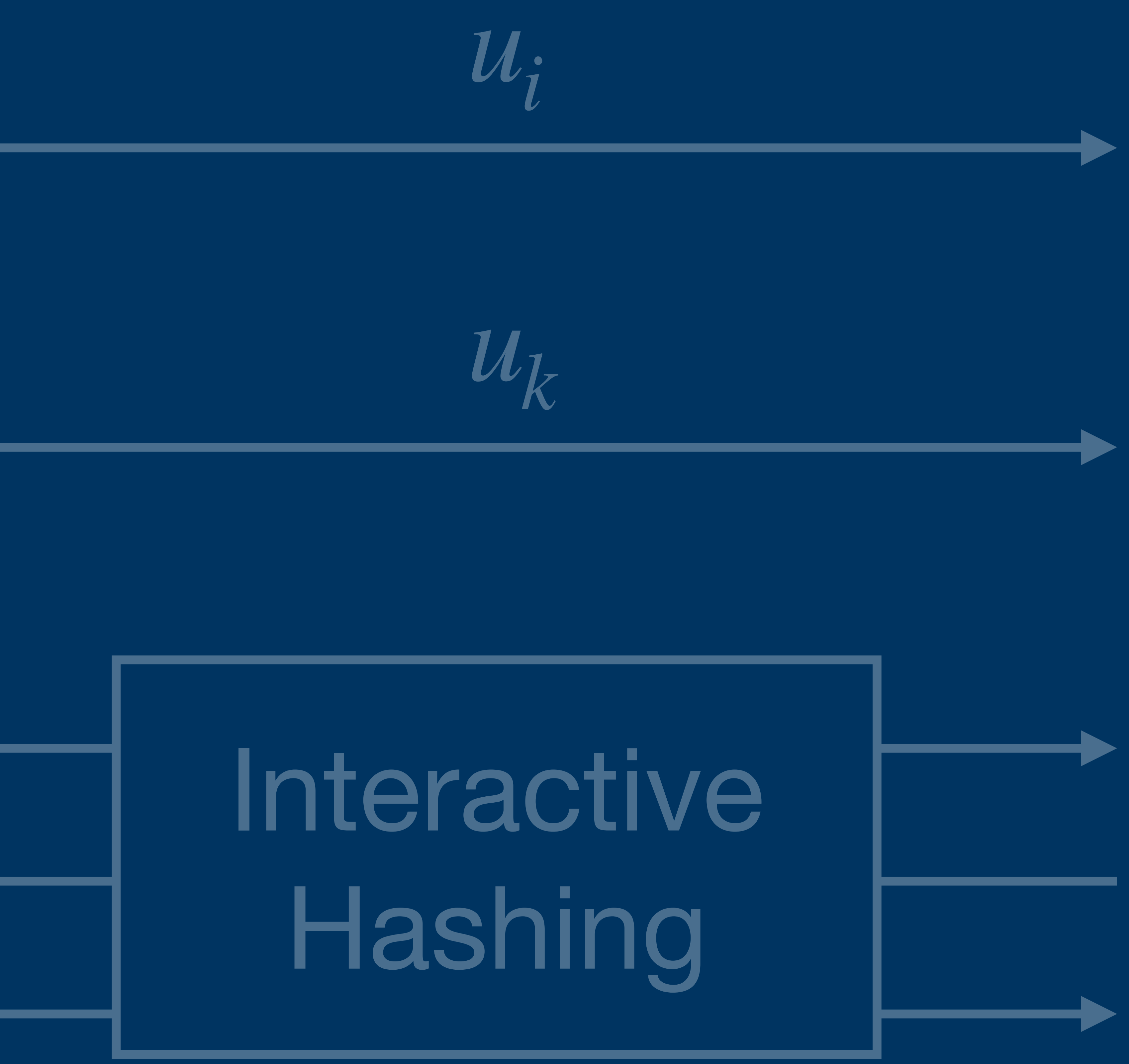
PROVER'S COMPUTATION



$$\sum_v |v\rangle$$

$$\sum_v |v, u_v\rangle$$

PROVER'S COMPUTATION

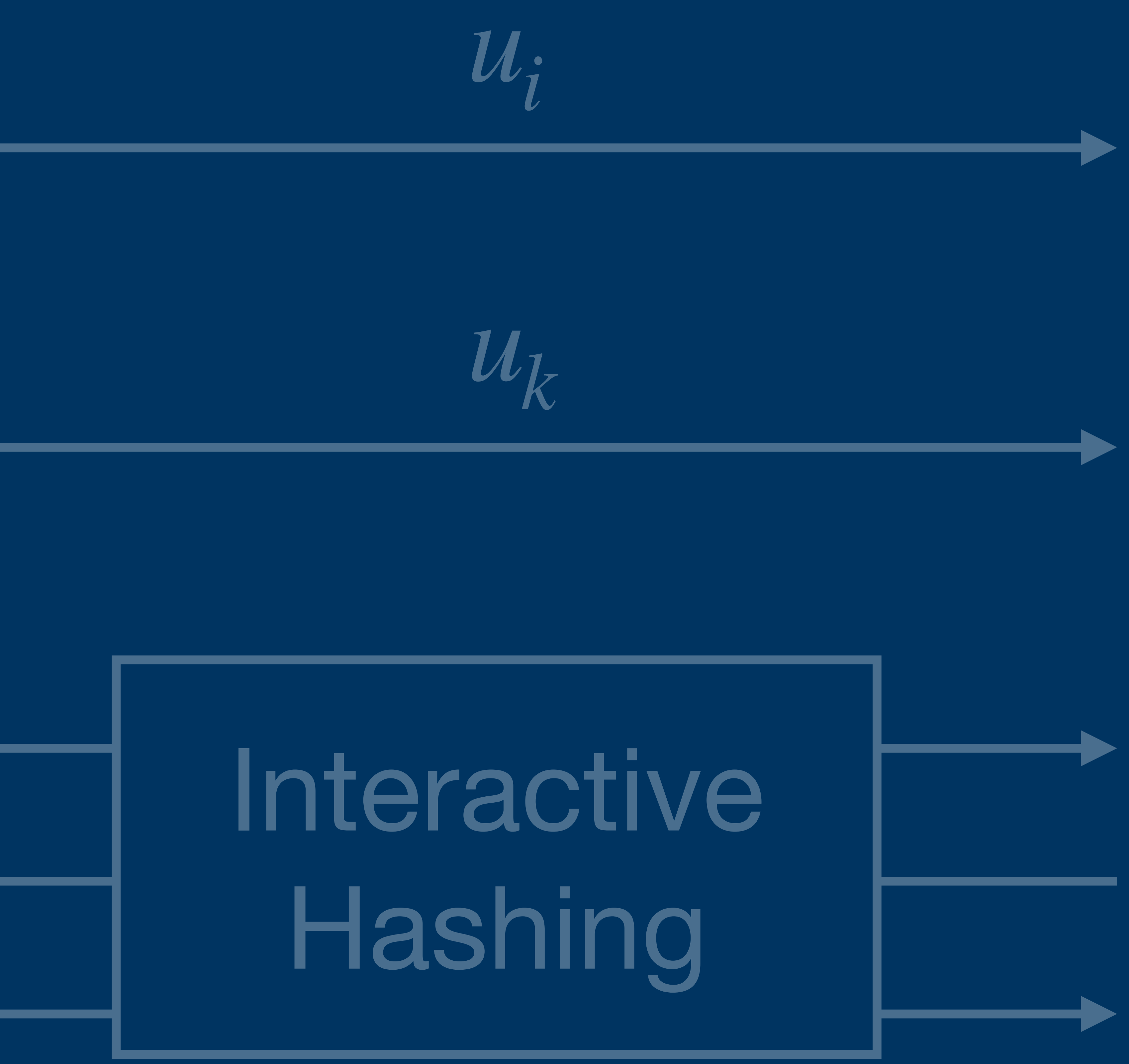


$$\sum_v |v\rangle$$

$$\sum_v |v, u_v\rangle$$

$$|v_0, u_{v_0}\rangle + |v_1, u_{v_1}\rangle$$

PROVER'S COMPUTATION



$$\sum_v |v\rangle$$

$$\sum_v |v, u_v\rangle$$

$$|v_0, u_{v_0}\rangle + |v_1, u_{v_1}\rangle$$

The bits u_{v_0} and u_{v_1} are hard to guess!

CLAW-STITCHING

$$\Big(|v_0, u_{v_0}\rangle + |v_1, u_{v_1}\rangle \Big) \otimes \Big(|w_0, u_{w_0}\rangle + |w_1, u_{w_1}\rangle \Big)$$

$$\neq$$

$$|v_0, u_{v_0}, w_0, u_{w_0}\rangle + |v_1, u_{v_1}, w_1, u_{w_1}\rangle$$

CLAW-STITCHING

$$\Big(|v_0, u_{v_0}\rangle + |v_1, u_{v_1}\rangle \Big) \otimes \Big(|w_0, u_{w_0}\rangle + |w_1, u_{w_1}\rangle \Big)$$

$$\neq$$

$$|v_0, u_{v_0}, w_0, u_{w_0}\rangle + |v_1, u_{v_1}, w_1, u_{w_1}\rangle$$

Solution: Entangle by measuring the XOR of the bits