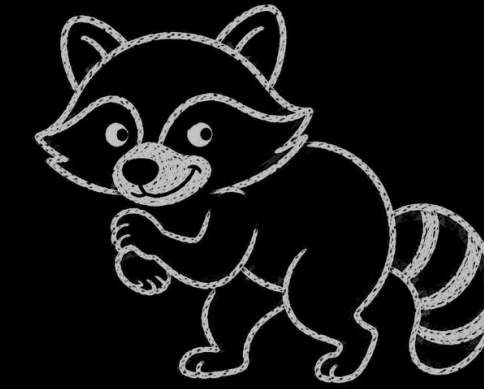




SELF-TESTING IN QUANTUM CRYPTOGRAPHY TUTORIAL



IVAN ŠUPIĆ



CNRS, LIQ
QCRYPT, OTTAWA, 24.08.2026





ALICE



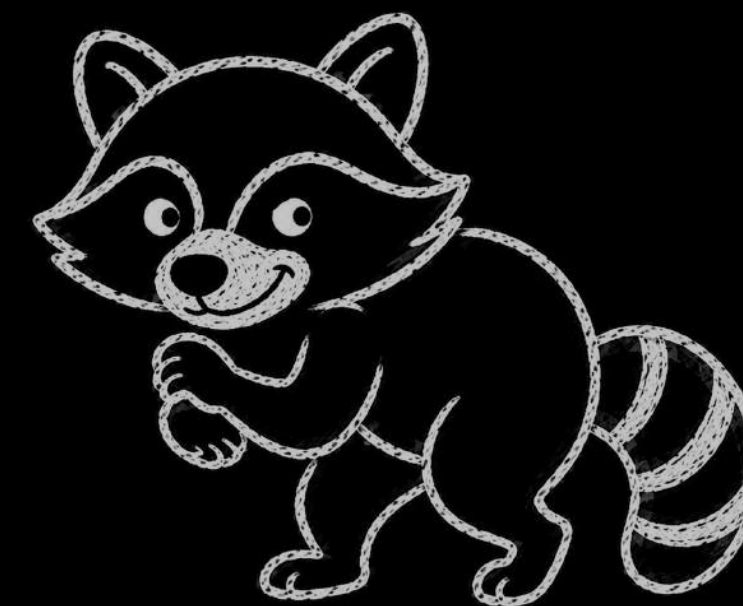
BOB



ALICE



BOB



EVE

STRUCTURE

★ ACT I : THE CONCEPT OF SELF-TESTING

★ ACT II : SOME APPLICATIONS

★ ACT III : MAIN TECHNIQUES

★ACT 1 : THE CONCEPT OF SELF-TESTING

TERMINOLOGY : SELF-TESTING

JOURNAL OF COMPUTER AND SYSTEM SCIENCES 47, 549–595 (1993)

Self-Testing/Correcting with Applications to Numerical Problems

MANUEL BLUM*

Computer Science Division, U.C. Berkeley, Berkeley, California 94720

MICHAEL LUBY†

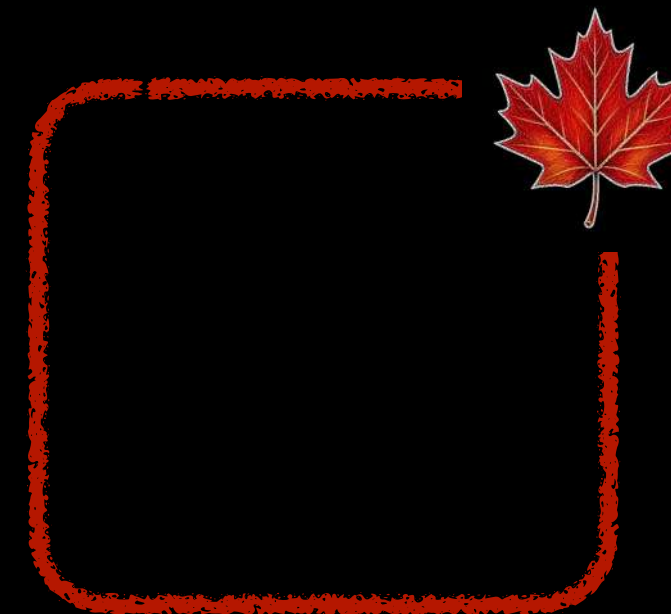
*International Computer Science Institute, Berkeley, California 94704;
and Computer Science Division, U.C. Berkeley, Berkeley, California 94720*

AND

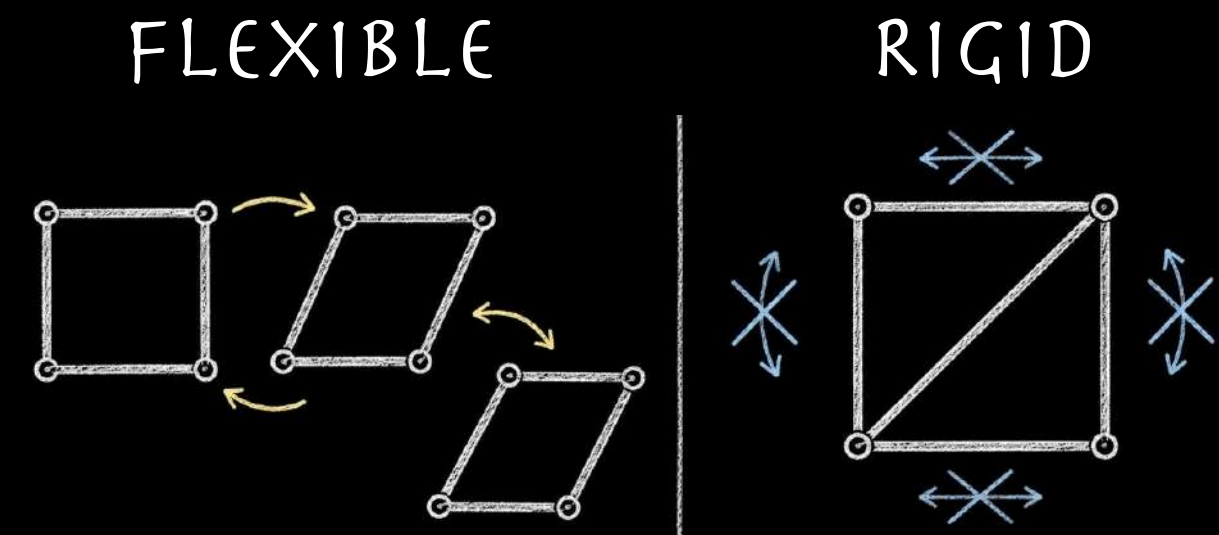
RONITT RUBINFELD‡

Department of Computer Science, Cornell University, Ithaca, New York 14853

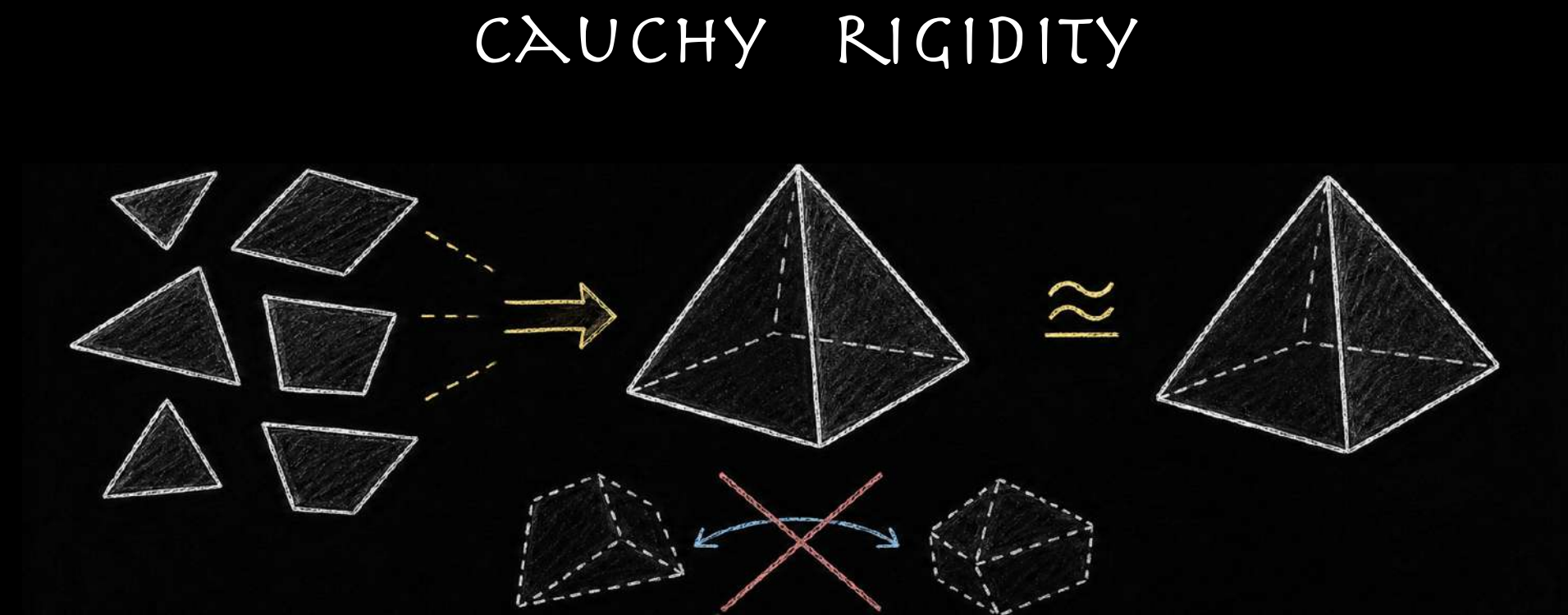
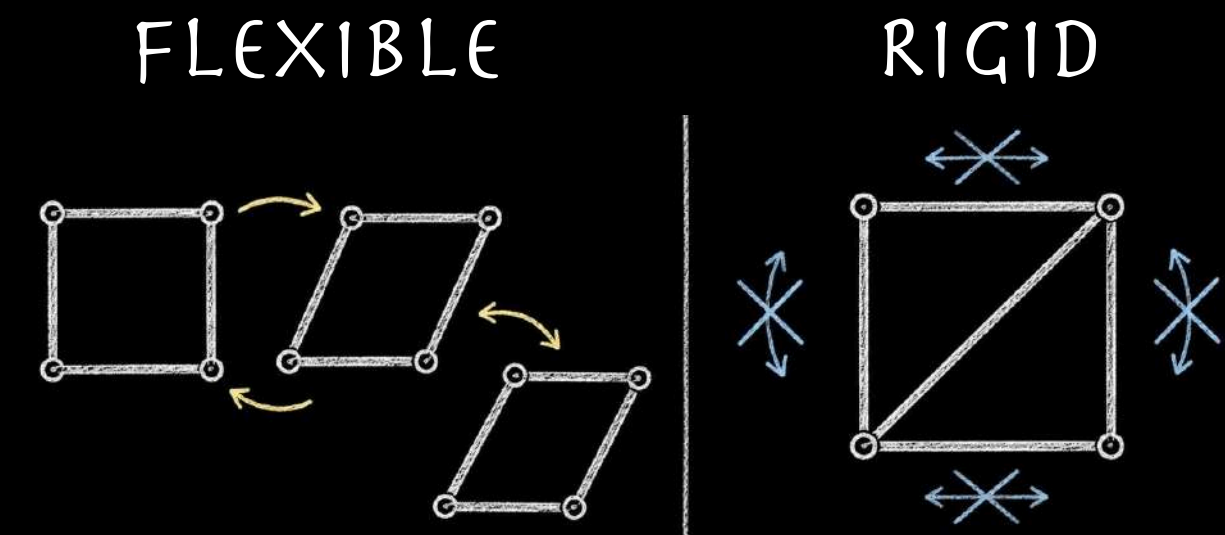
Received August 14, 1990; revised November 19, 1991



TERMINOLOGY : RIGIDITY



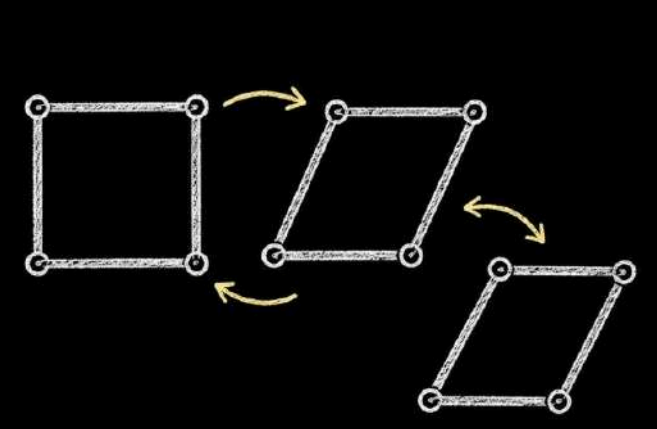
TERMINOLOGY : RIGIDITY



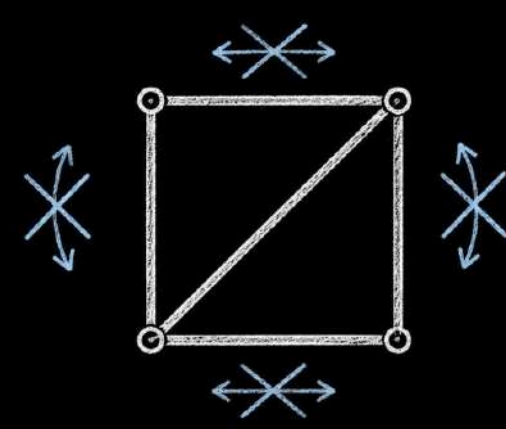
A CONVEX POLYHEDRON IS DETERMINED
BY ITS FACES, UP TO CONGRUENCE

TERMINOLOGY : RIGIDITY

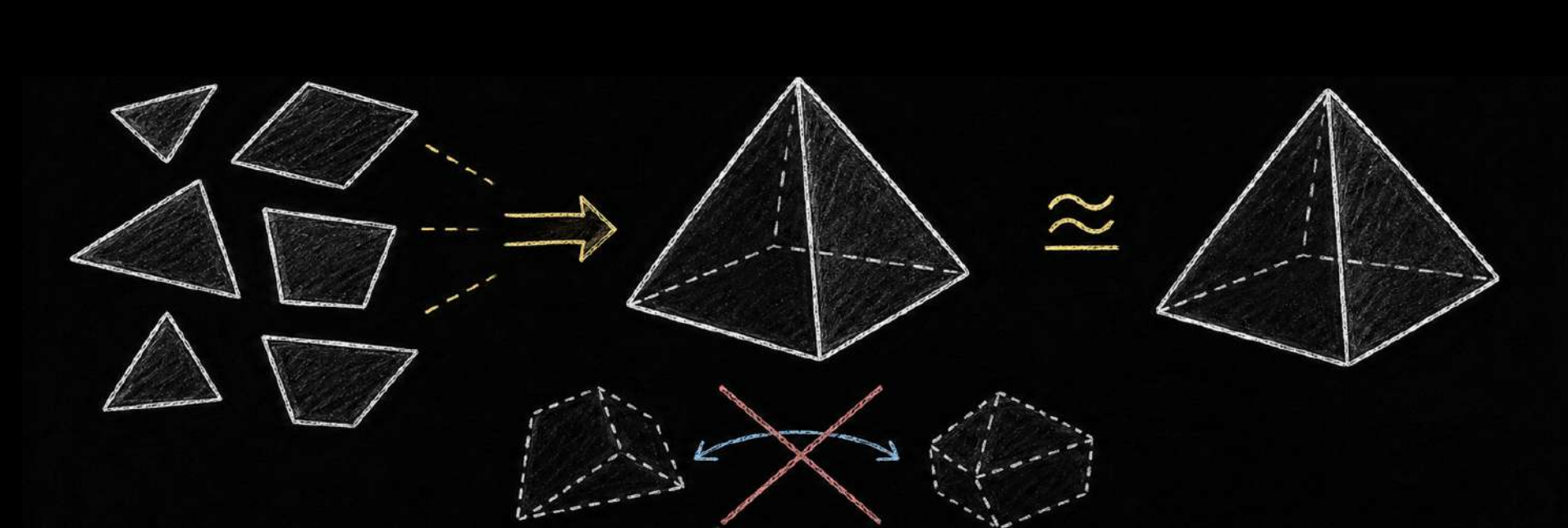
FLEXIBLE



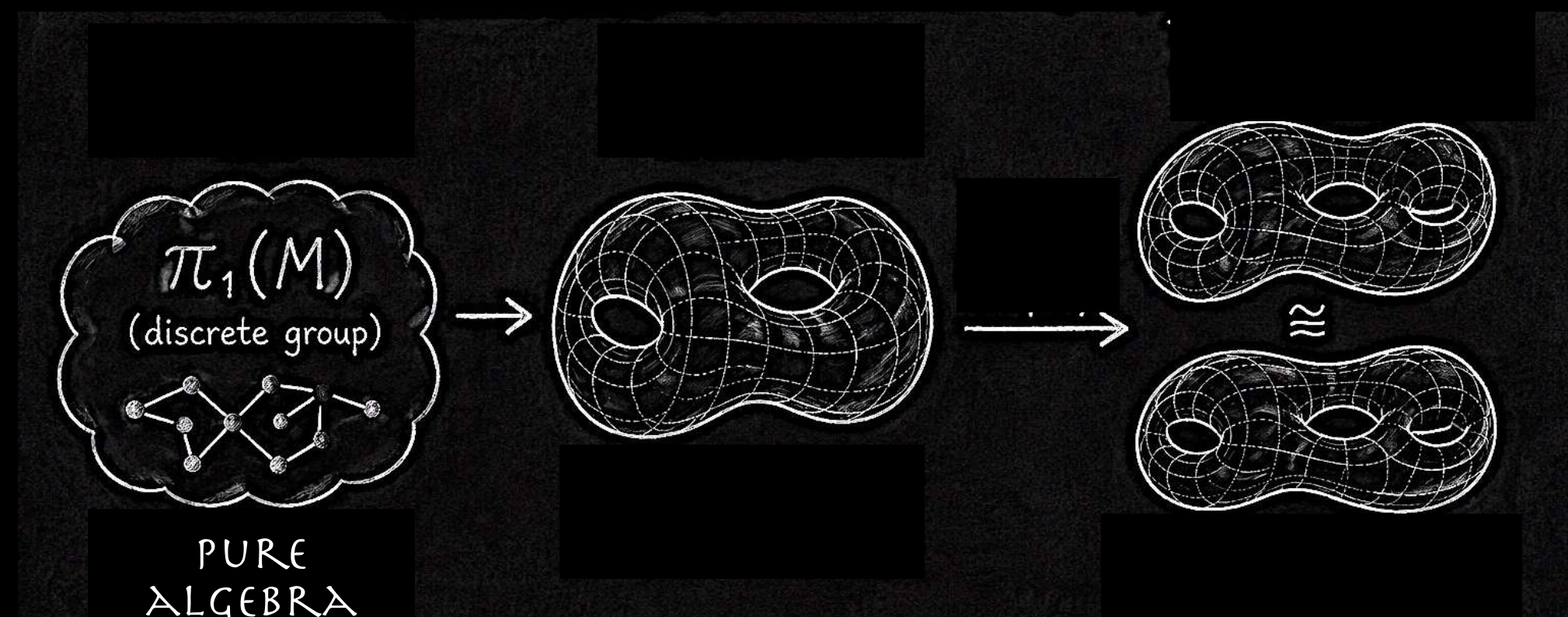
RIGID



CAUCHY RIGIDITY



MOSTOW RIGIDITY

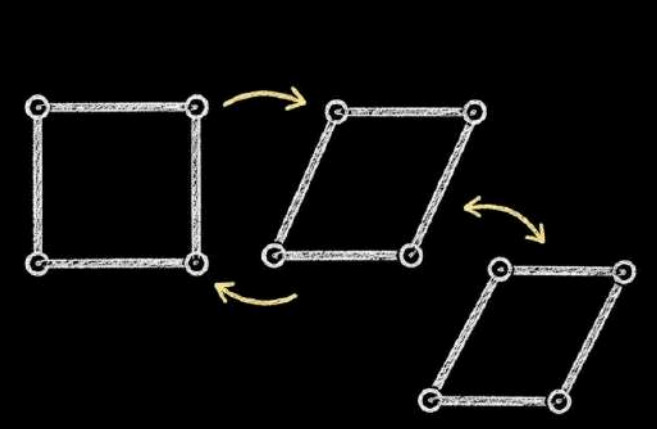


A CLOSED HYPERBOLIC MANIFOLD OF DIMENSION
LARGER THAN 3 IS DETERMINED UP TO ISOMETRY BY ITS
FUNDAMENTAL GROUP

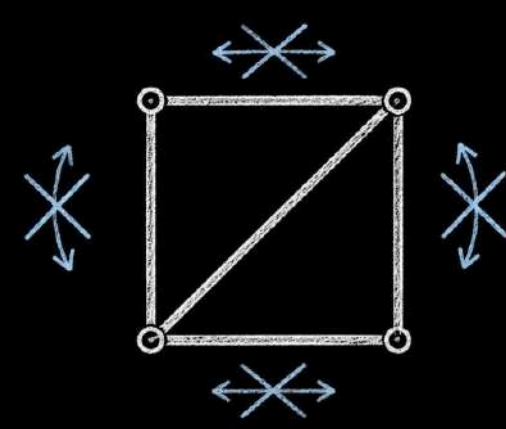
A CONVEX POLYHEDRON IS DETERMINED
BY ITS FACES, UP TO CONGRUENCE

TERMINOLOGY : RIGIDITY

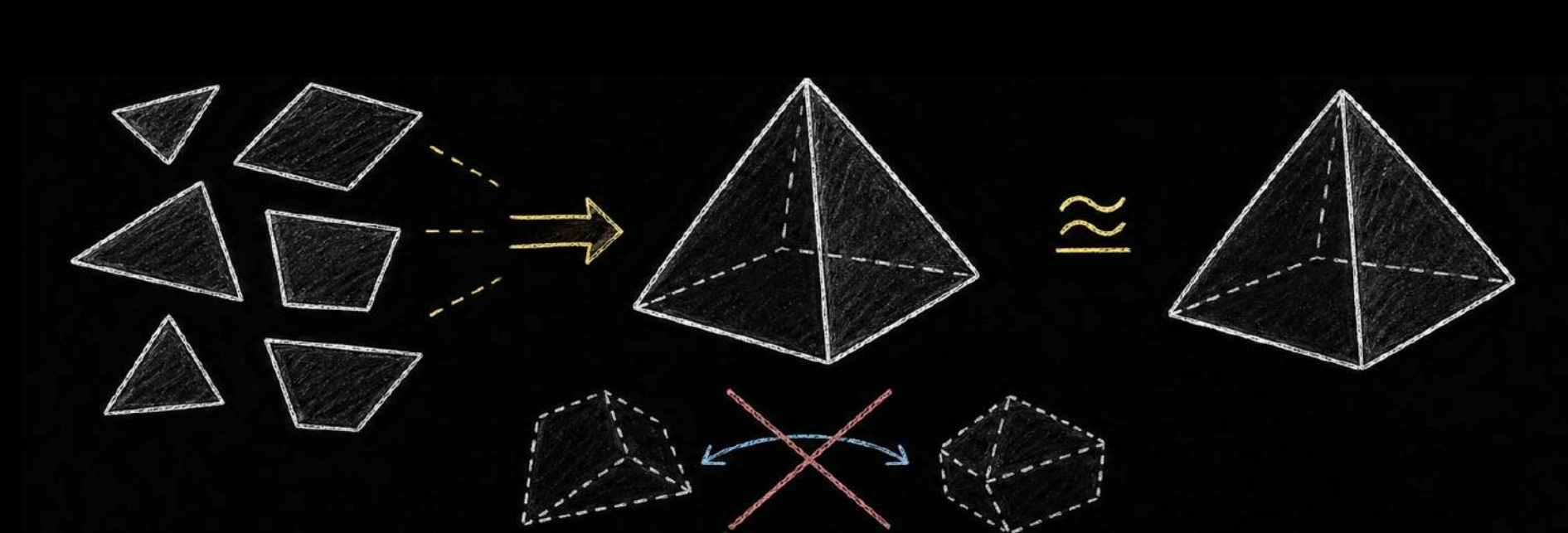
FLEXIBLE



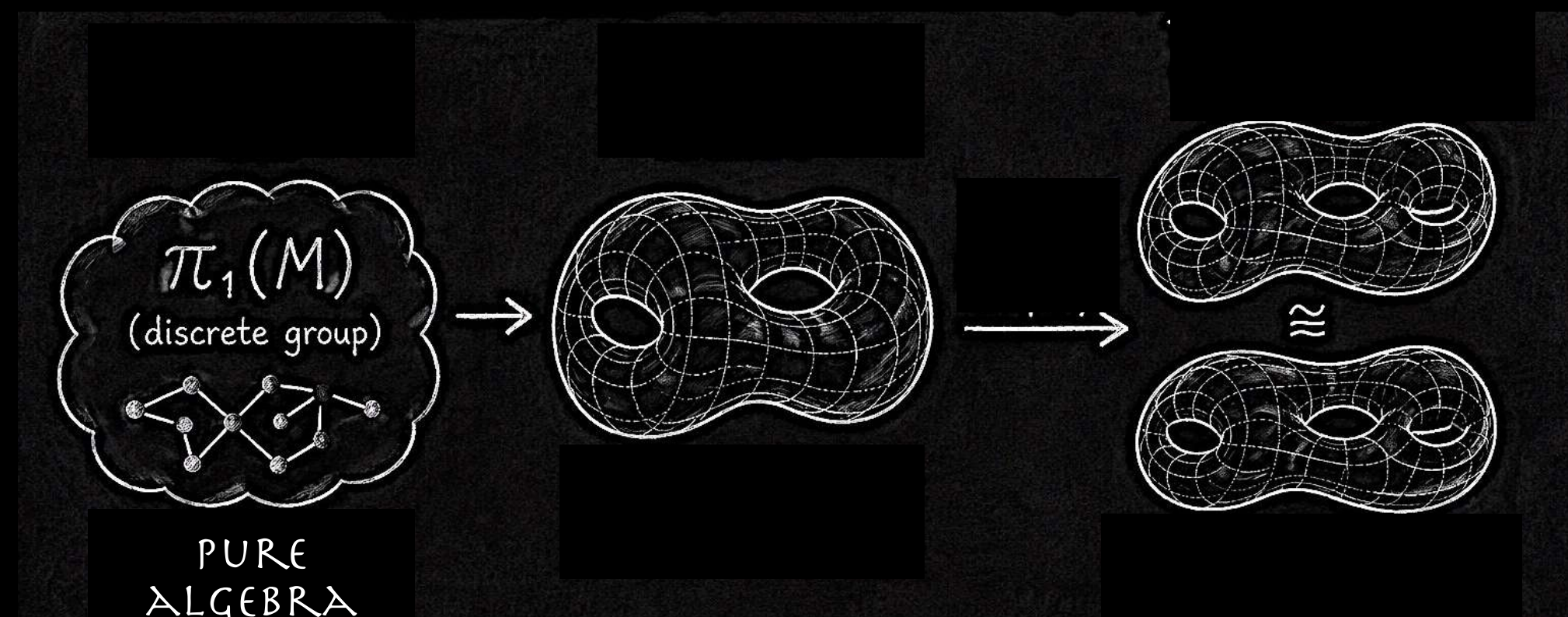
RIGID



CAUCHY RIGIDITY



MOSTOW RIGIDITY

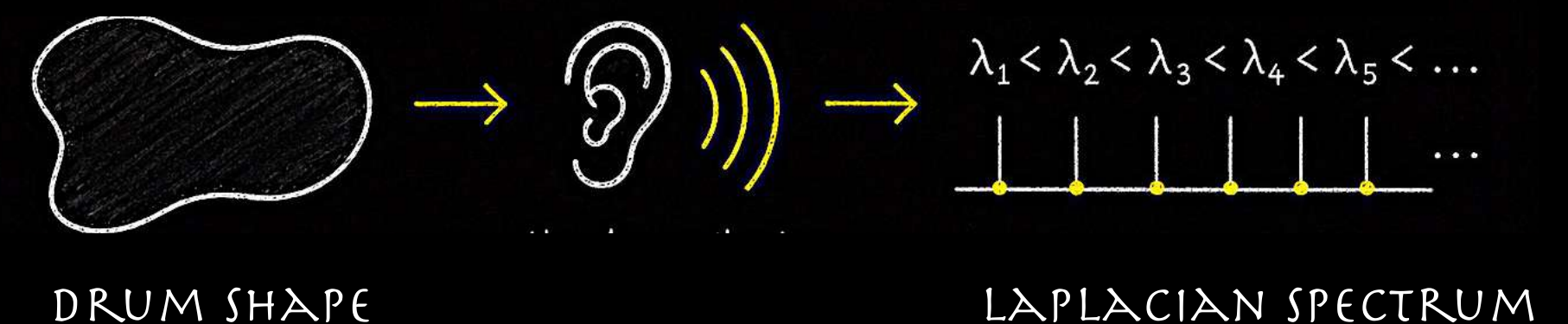


A CLOSED HYPERBOLIC MANIFOLD OF DIMENSION LARGER THAN 3 IS DETERMINES UP TO ISOMETRY BY ITS FUNDAMENTAL GROUP

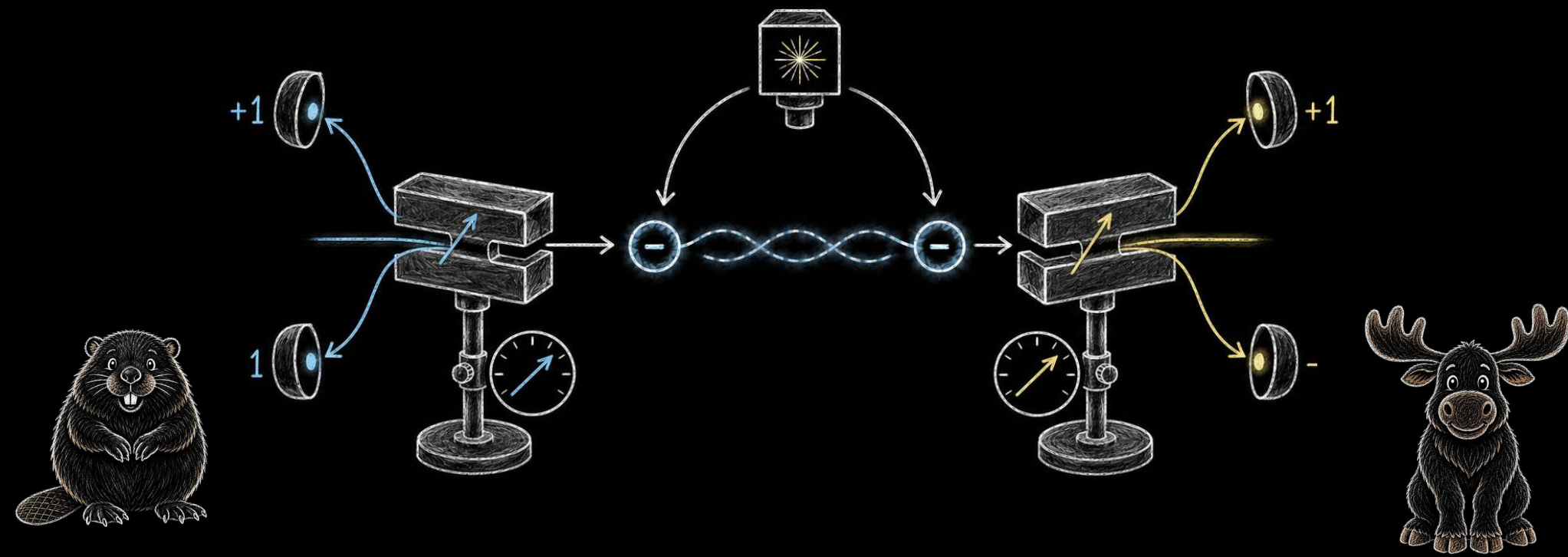
A CONVEX POLYHEDRON IS DETERMINED BY ITS FACES, UP TO CONGRUENCE

SPECTRAL RIGIDITY

KAC: CAN ONE HEAR THE SHAPE OF A DRUM?



CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?

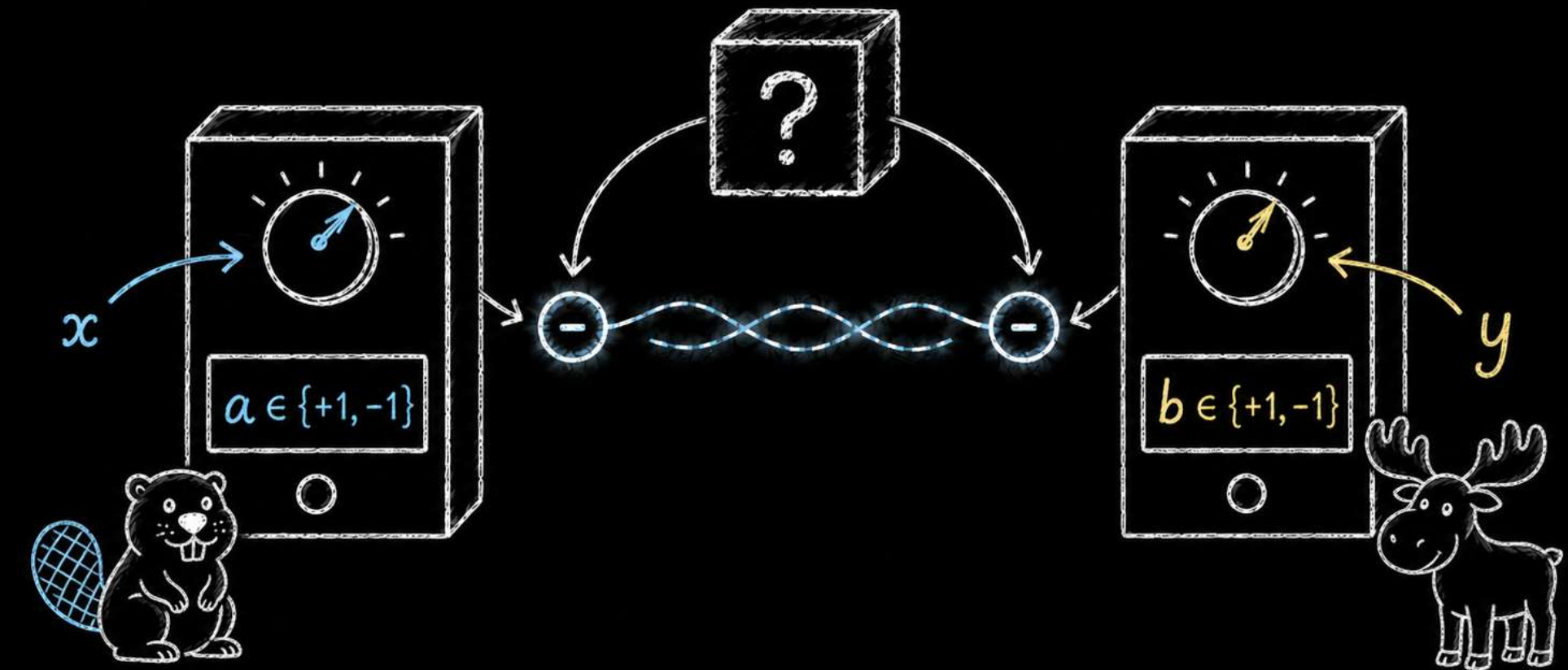
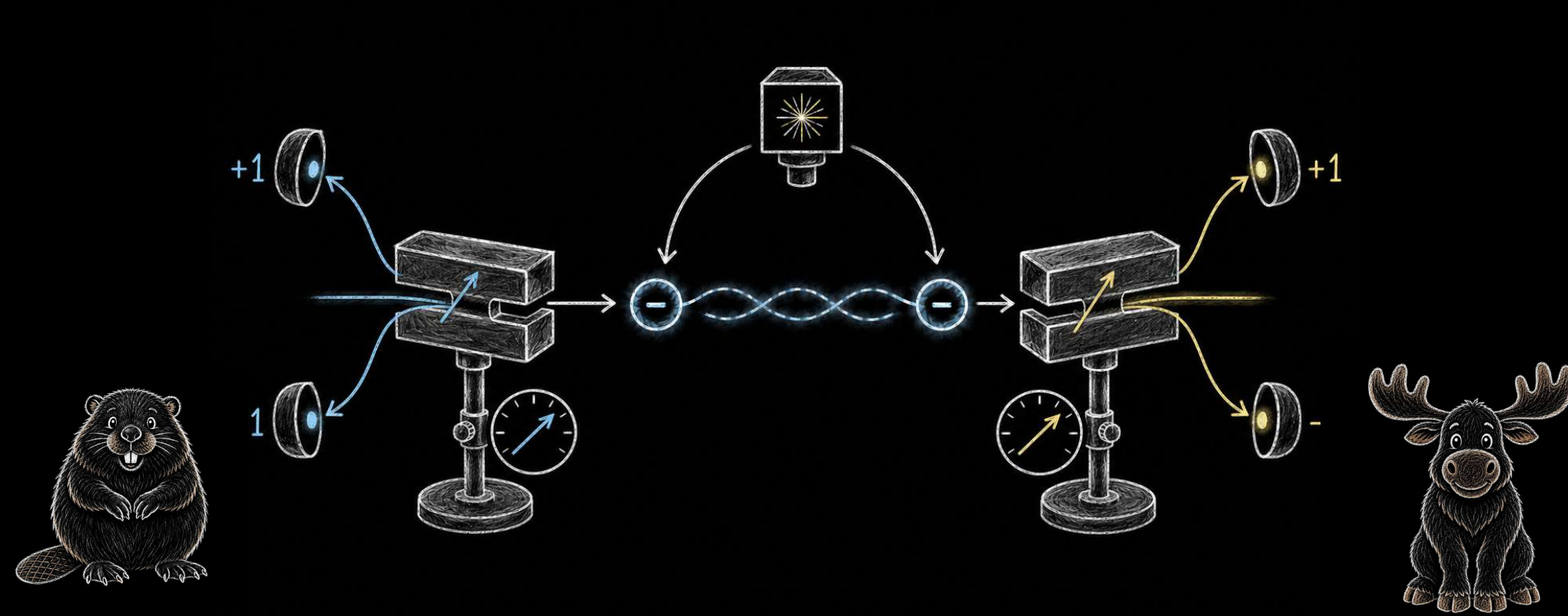


$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$A_0 = \sigma_z \quad B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}$$

$$A_1 = \sigma_x \quad B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}$$

CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?

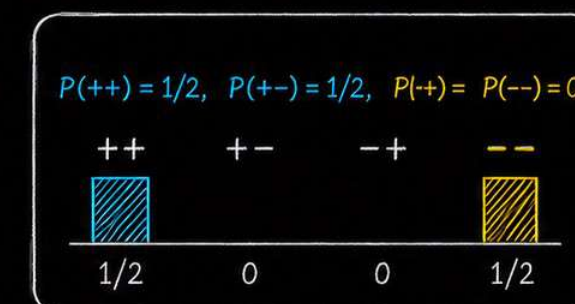


$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

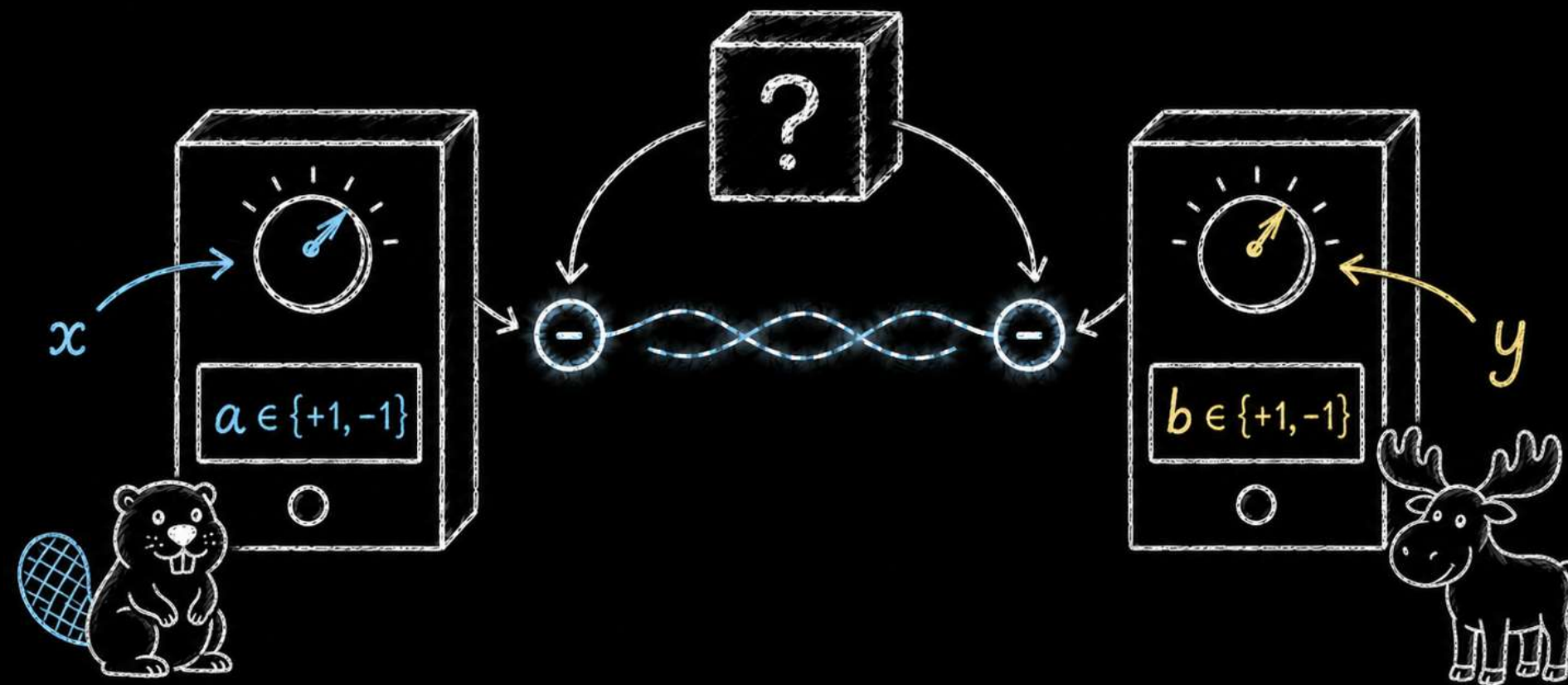
$$A_0 = \sigma_z \quad B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}$$

$$A_1 = \sigma_x \quad B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}$$

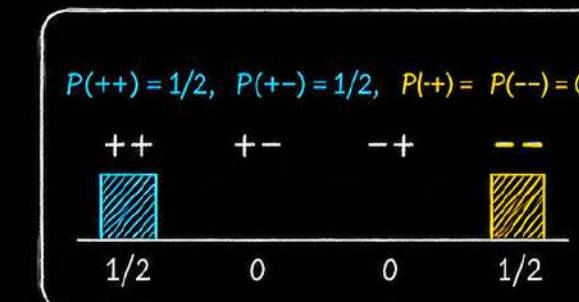
$$p(a, b | x, y)$$



NONLOCAL GAMES / BELL INEQUALITIES



$$p(a, b | x, y)$$



BELL VALUE

$$\omega = \sum_{x,y} \pi(x, y) \sum_{a,b} V(a, b | x, y) p(a, b | x, y)$$

$$\beta = \sum_{x,y,a,b} b_{a,b|x,y} p(a, b | x, y)$$

$$\omega = \sum_{x,y,a,b} \pi(x, y) V(a, b | x, y) \langle \psi | M_a^x \otimes N_b^y | \psi \rangle .$$

BELL OPERATOR

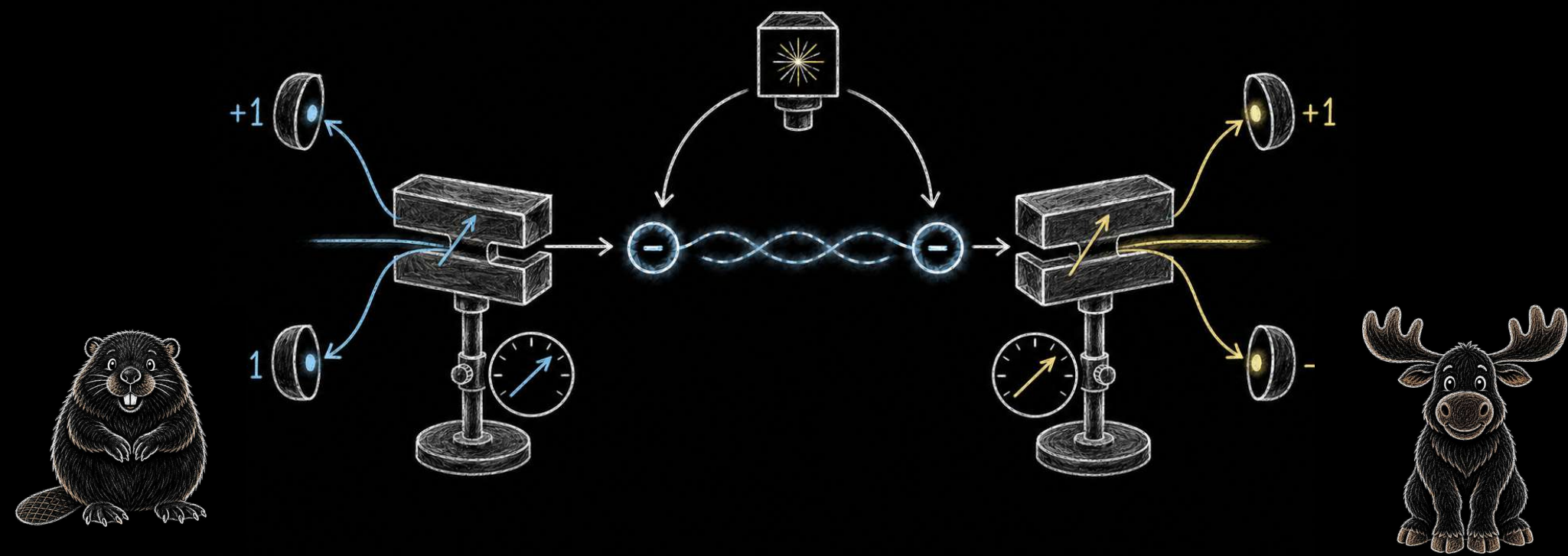
$$\mathcal{B} = \sum_{x,y,a,b} b_{a,b|x,y} M_a^x \otimes N_b^y$$

ω_c CLASSICAL VALUE

ω_q QUANTUM VALUE

$$\beta = \langle \psi | \mathcal{B} | \psi \rangle$$

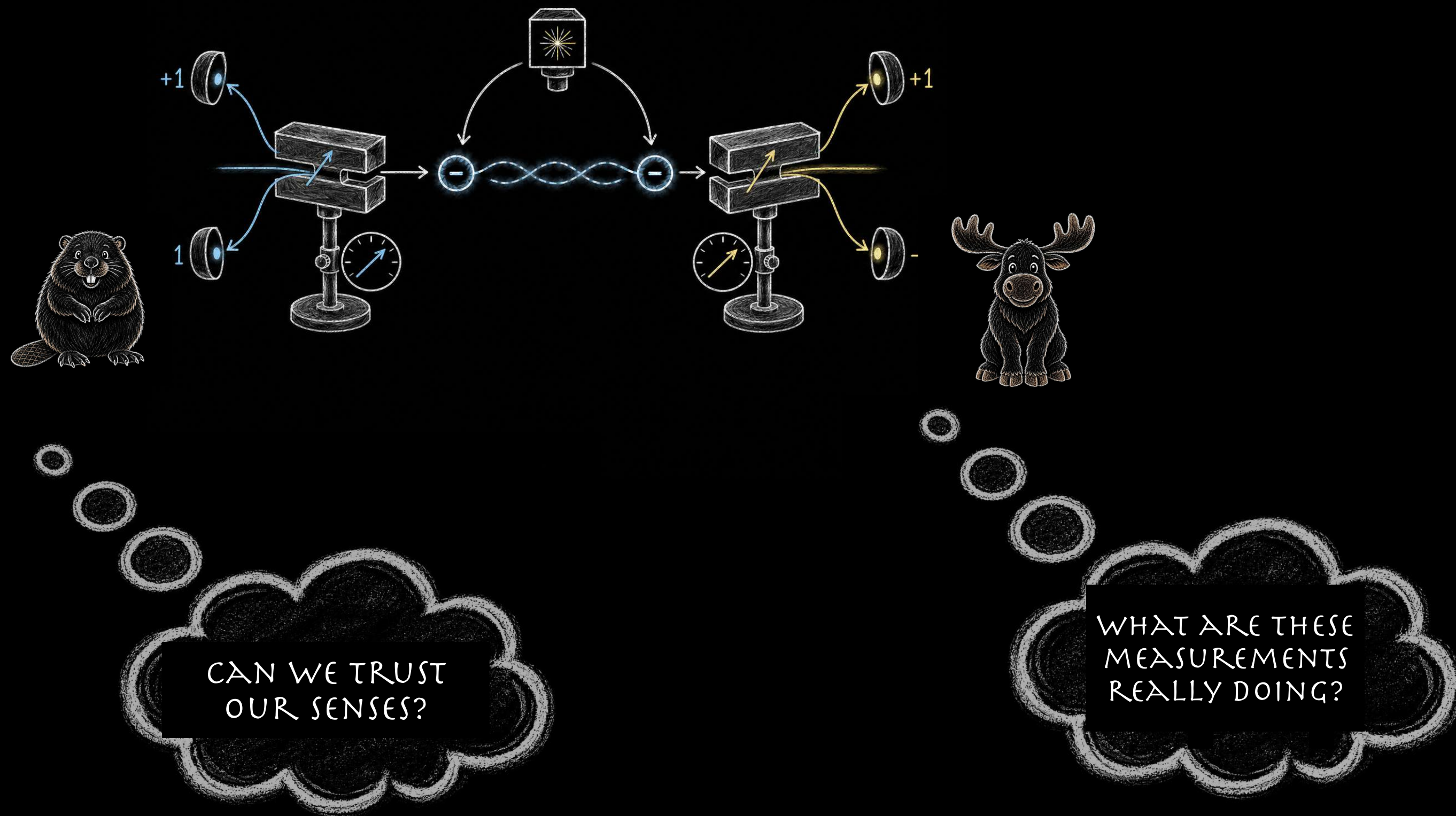
CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?



CAN WE TRUST
OUR SENSES?

WHAT ARE THESE
MEASUREMENTS
REALLY DOING?

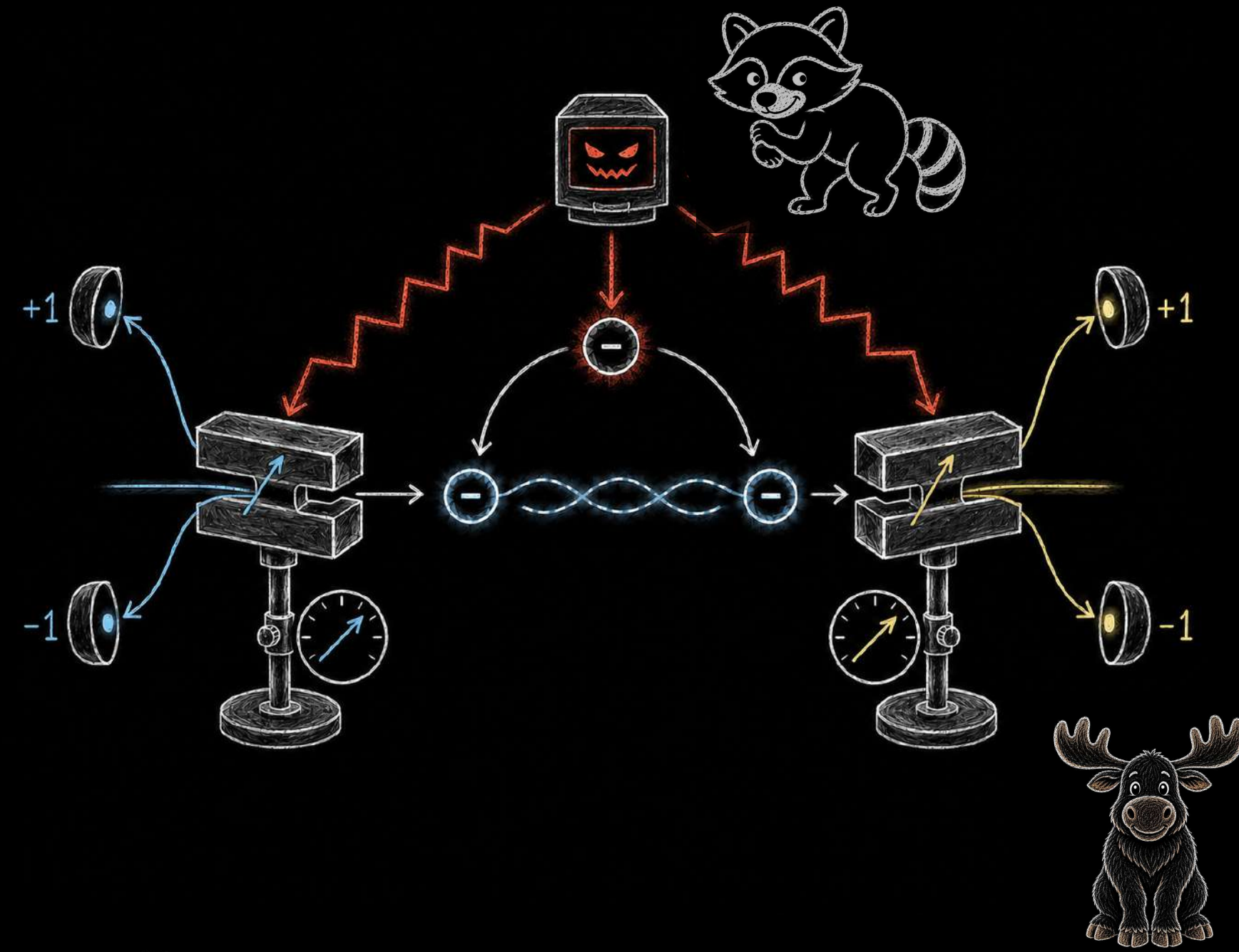
CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?



CAN QUANTUM THEORY
PASS THE TEST OF CARTESIAN
METHODOLOGICAL DOUBT?

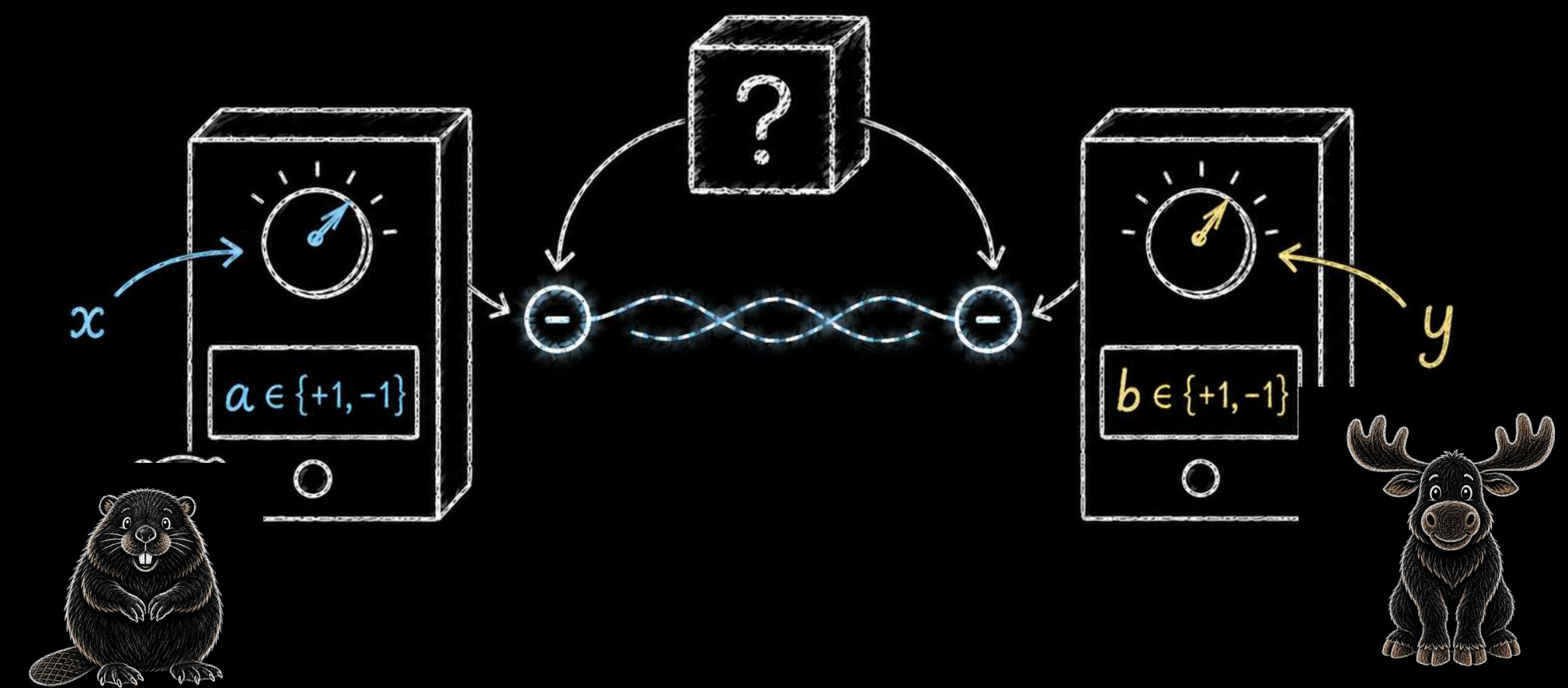
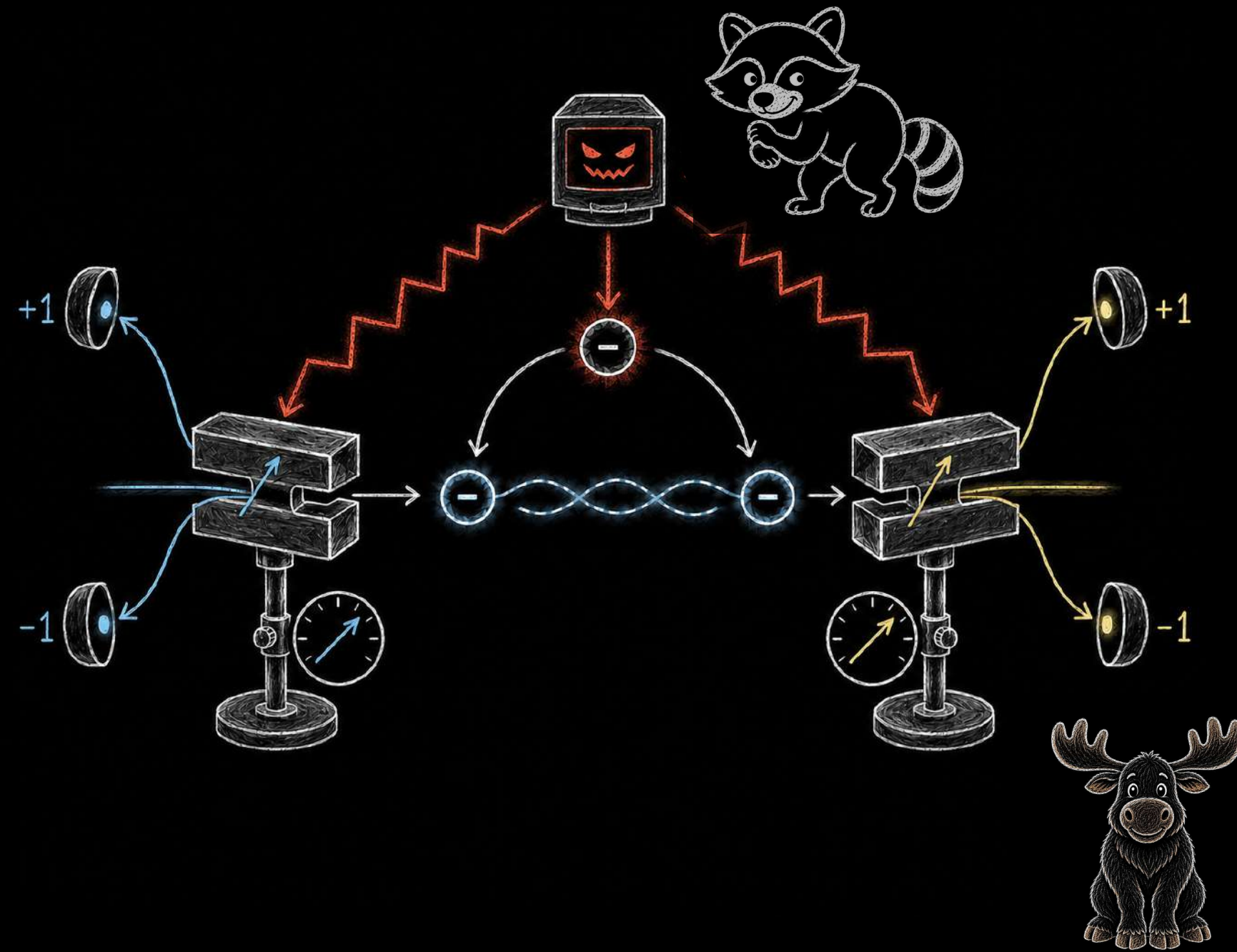


CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?



WHAT IS THERE IS AN
ADVERSARY?

CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?

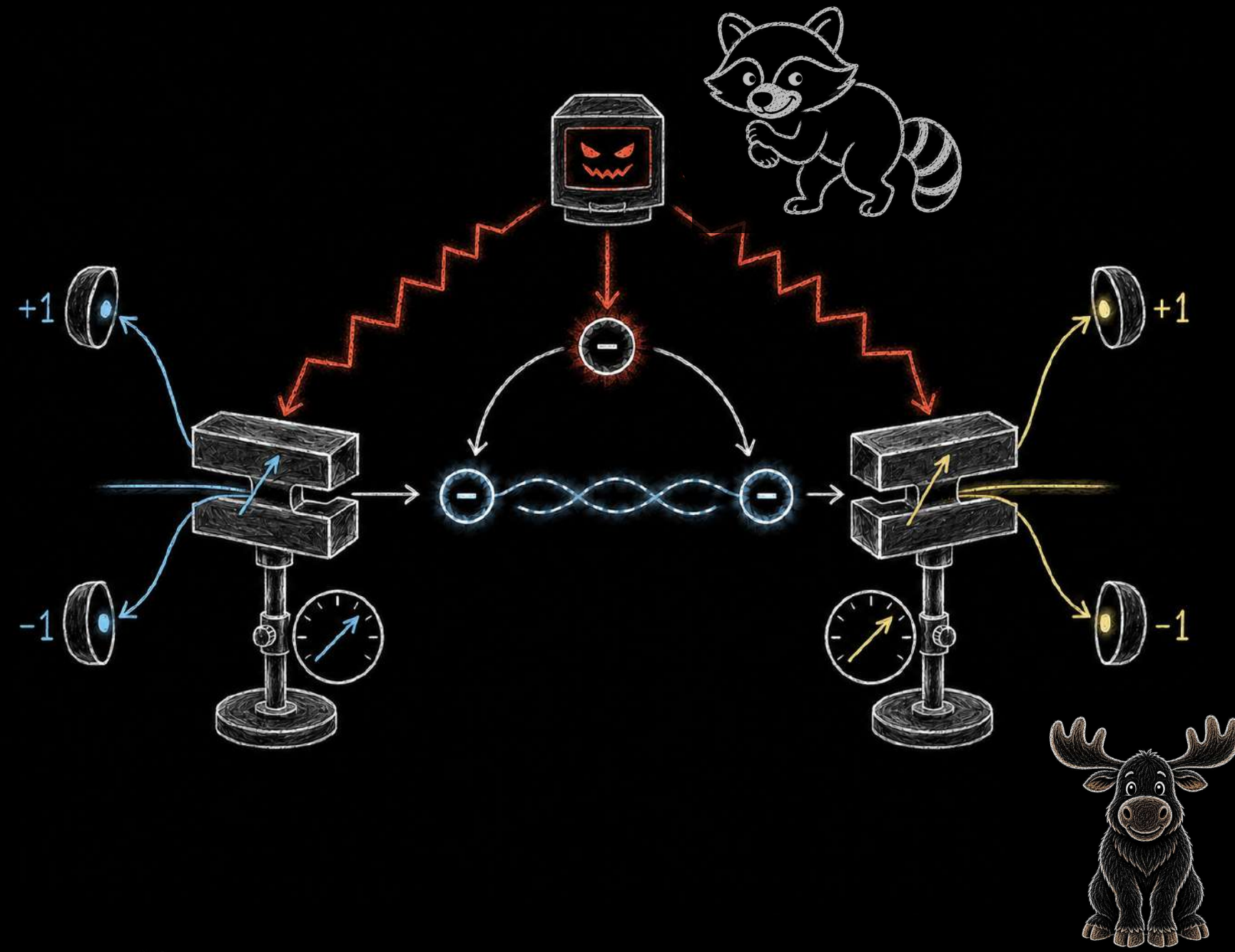


DEVICE-INDEPENDENCE!!!

WHAT IS THERE IS AN
ADVERSARY?

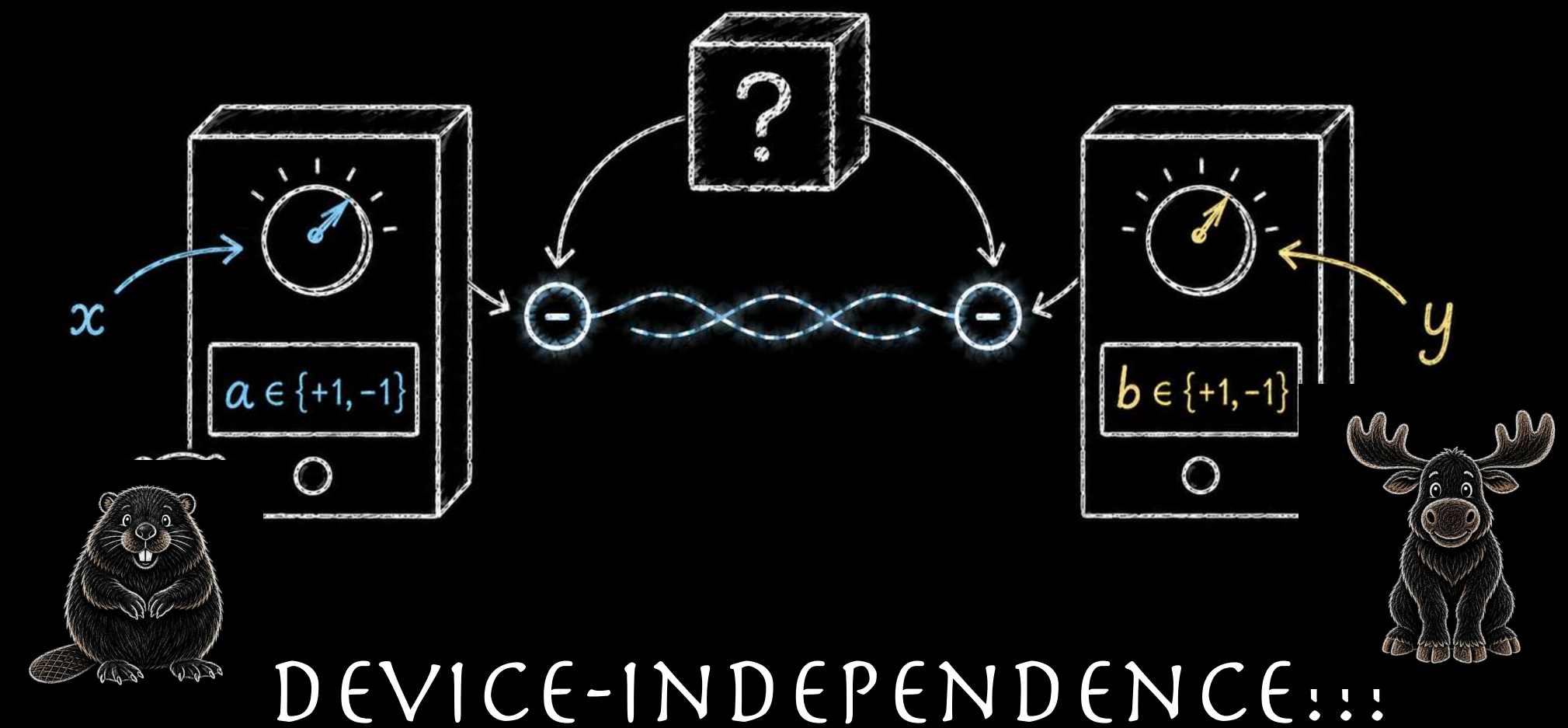
Mayers, Yao
FOCS [1998]

CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?



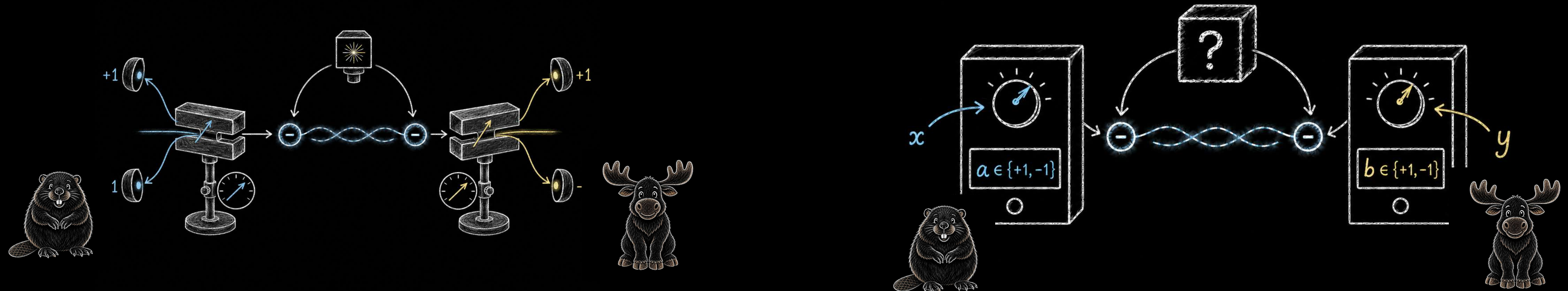
WHAT IS THERE IS AN
ADVERSARY?

Mayers, Yao
FOCS [1998]



SELF-TESTING WAS NOT
INVENTED TO STUDY
FOUNDATIONS. IT WAS
INVENTED BECAUSE SOMEONE
ASKED WHETHER YOU CAN
TRUST A DEVICE YOU DIDN'T
BUILD.

CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?



$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$A_0 = \sigma_z \quad B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}$$

$$A_1 = \sigma_x \quad B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}$$

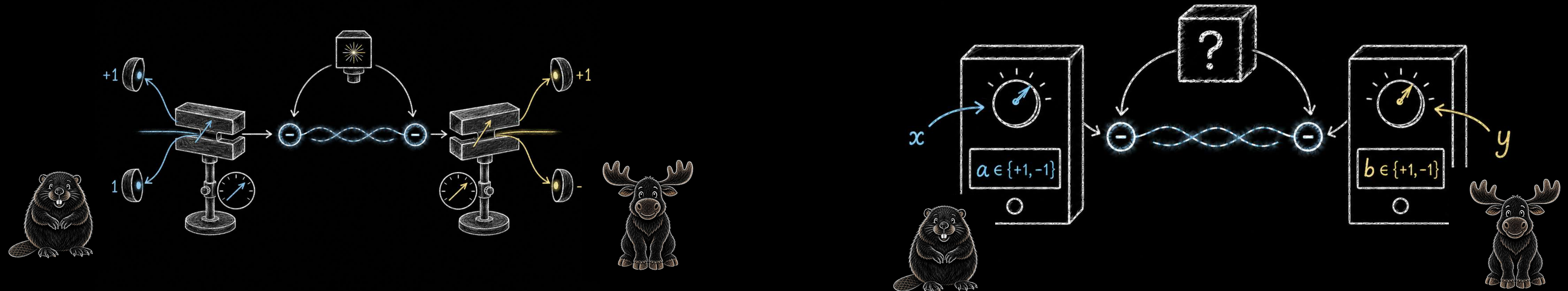
$$\langle EPR | A_x \otimes B_y | EPR \rangle$$

$$p(a, b | x, y)$$

$P(++)=1/2, P(+-)=1/2, P(-+)=0, P(--)=0$

++	+-	-+	--
1/2	0	0	1/2

CAN WE HEAR THE SOUND OF QUANTUM STATES FROM CORRELATIONS?



$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$A_0 = \sigma_z \quad B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}$$

$$A_1 = \sigma_x \quad B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}$$

$$\langle EPR | A_x \otimes B_y | EPR \rangle$$

$$p(a, b | x, y)$$

$P(++)=1/2, P(+-)=1/2, P(-+)=0, P(--)=0$

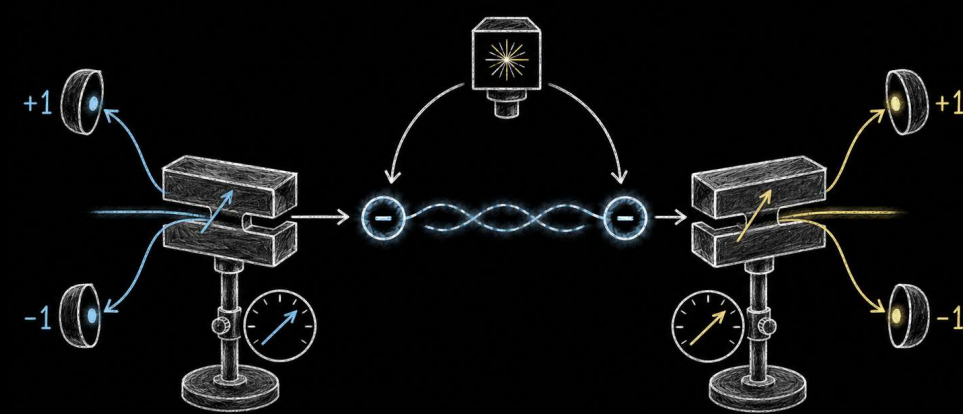
++	+-	-+	--
1/2	0	0	1/2

Mayers, Yao
QIC 4,4 [2004]

WHAT CAN WE HEAR?

LOCAL UNITARIES

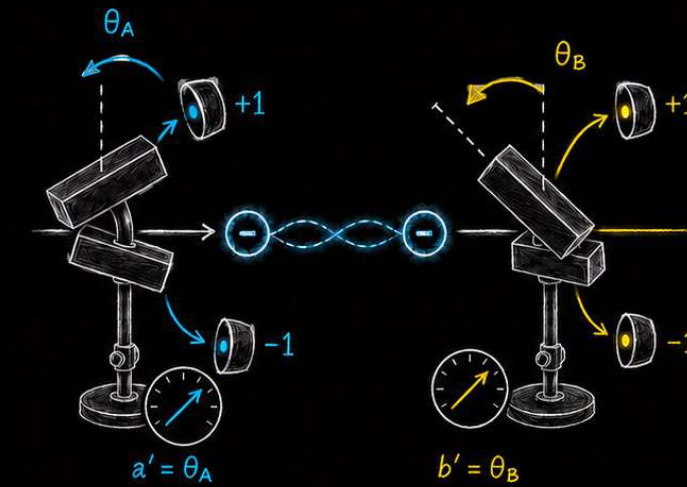
$$S = \left\{ |\psi\rangle, M_{a|x}, N_{b|y} \right\}$$



$$P(++)=1/2, P(+)=1/2, P(-)=0$$

++	+-	-+	--
1/2	0	0	1/2

$$\tilde{S} = \left\{ U \otimes V |\psi\rangle, UM_{a|x}U^\dagger, VN_{b|y}V^\dagger \right\}$$



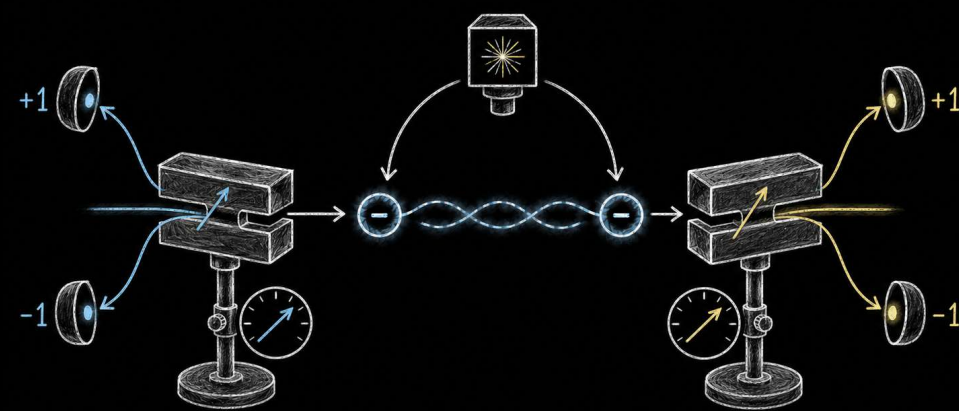
$$P(++)=1/2, P(+)=1/2, P(-)=0$$

++	+-	-+	--
1/2	0	0	1/2

WHAT CAN WE HEAR?

LOCAL UNITARIES

$$S = \{ |\psi\rangle, M_{a|x}, N_{b|y} \}$$

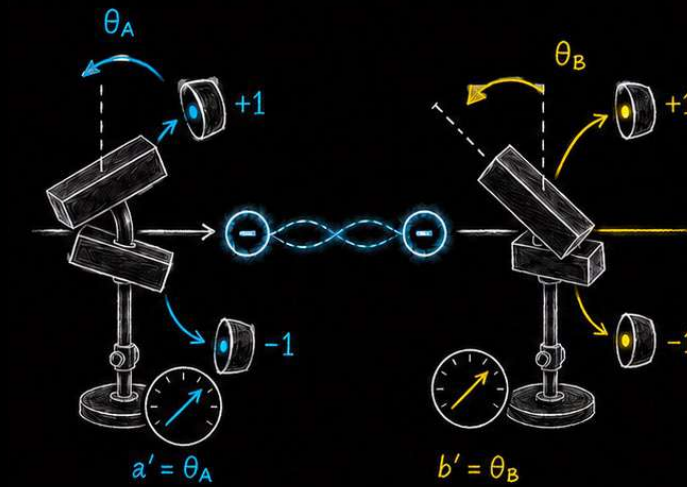


$$P(++)=1/2, P(+)=1/2, P(-)=0$$

++	+-	-+	--
1/2	0	0	1/2

ADDITIONAL DEGREES OF FREEDOM

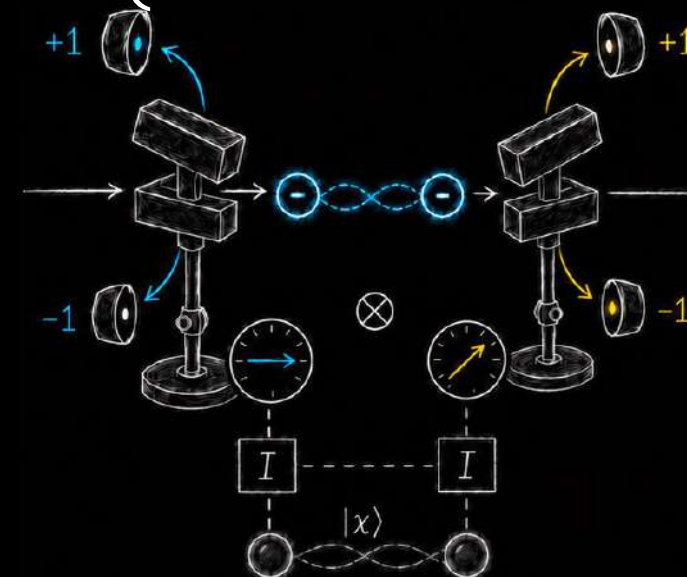
$$\tilde{S} = \{ U \otimes V |\psi\rangle, U M_{a|x} U^\dagger, V N_{b|y} V^\dagger \}$$



$$P(++)=1/2, P(+)=1/2, P(-)=0$$

++	+-	-+	--
1/2	0	0	1/2

$$\bar{S} = \{ |\psi\rangle \otimes |\xi\rangle, M_{a|x} \otimes \mathbb{I}, N_{b|y} \otimes \mathbb{I} \}$$



$$P(++)=1/2, P(+)=1/2, P(-)=0$$

++	+-	-+	--
1/2	0	0	1/2

WHAT CAN WE HEAR?

$$p(a, b | x, y)$$

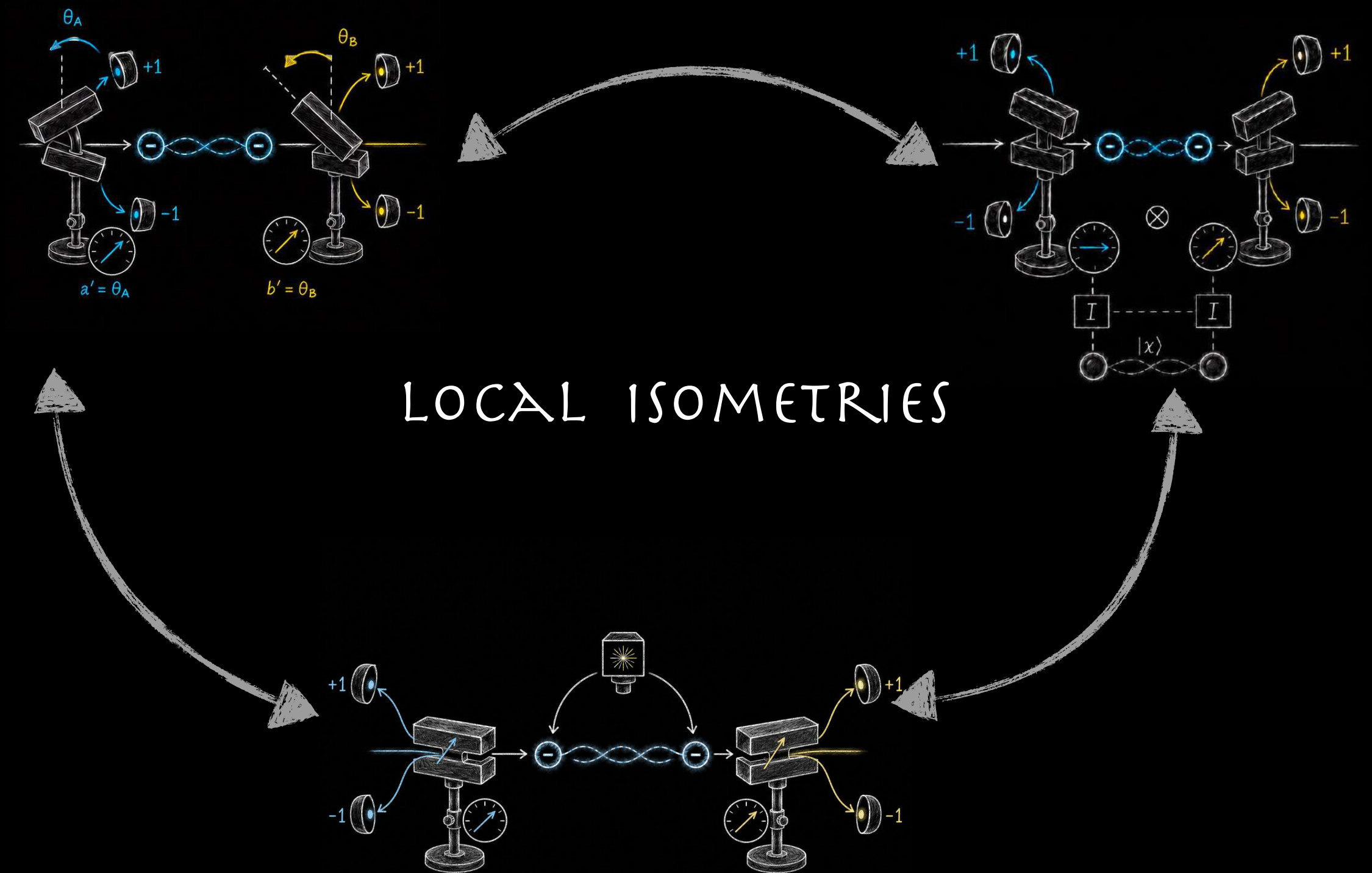
$$P(++)=1/2, P(+-)=1/2, P(-+)=0, P(--)=0$$

++	+-	-+	--
1/2	0	0	1/2

SELF-TESTING

EQUIVALENCE CLASS

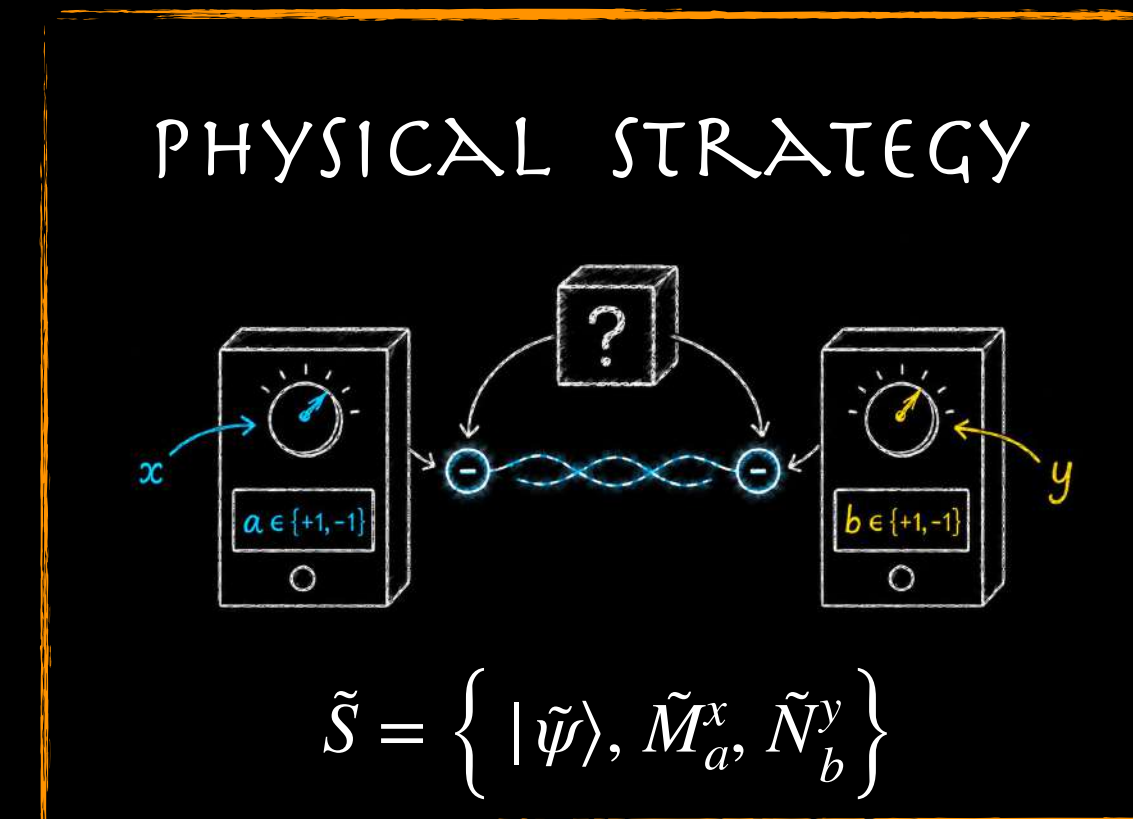
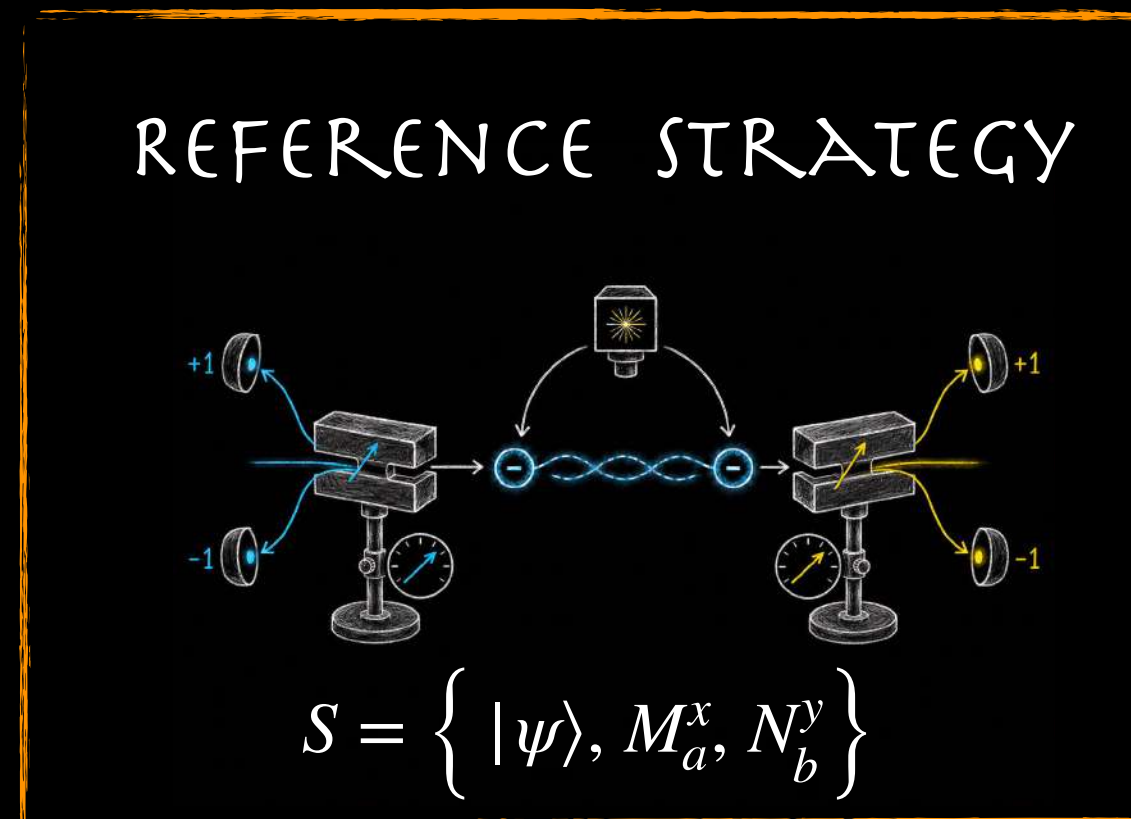
LOCAL ISOMETRIES



EXACT SELF-TESTING : DEFINITION

BLUEPRINT

WHAT IS ACCESSIBLE



ACCESS ONLY TO AN EVENT
THE STRATEGY PRODUCES!

EVENT:
FULL BEHAVIOUR $\{p(a, b | x, y)\}$
SCORE IN A NONLOCAL GAME ω

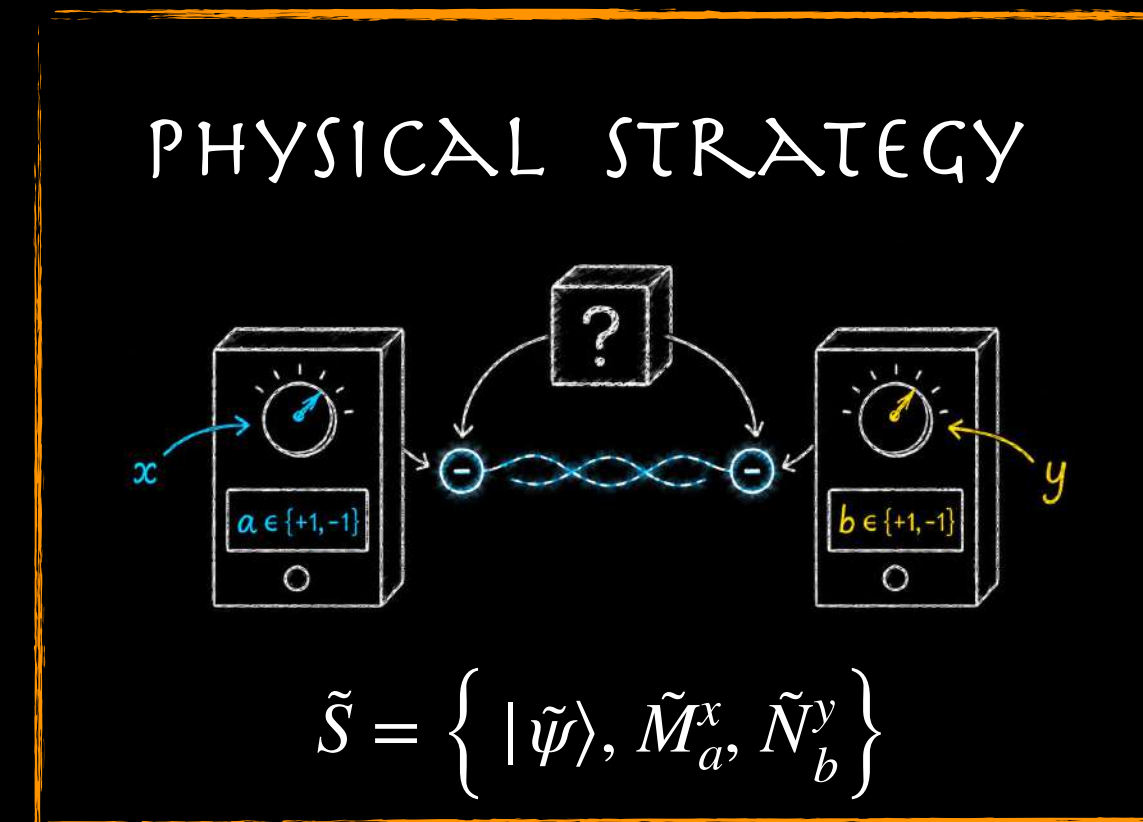
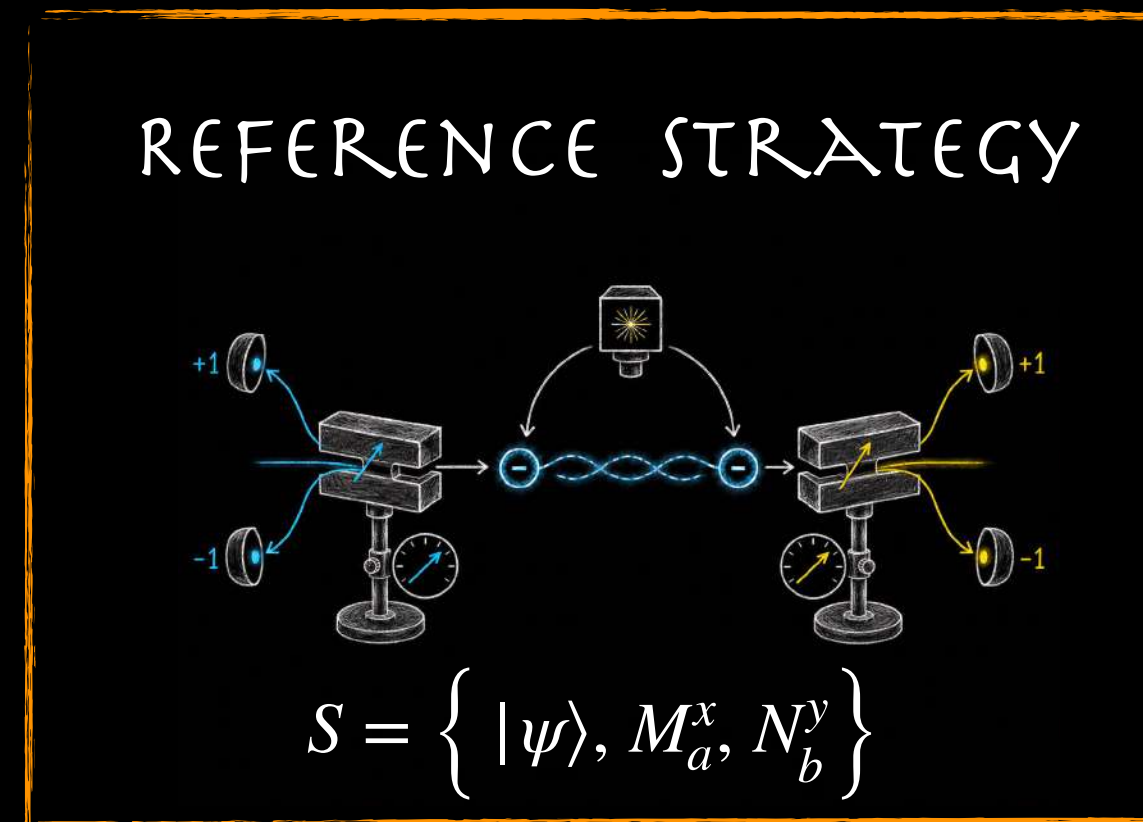
$$\Phi_A \otimes \Phi_B$$

$$\Phi_A \otimes \Phi_B [|\tilde{\psi}\rangle] = |\psi\rangle \otimes |\text{junk}\rangle$$

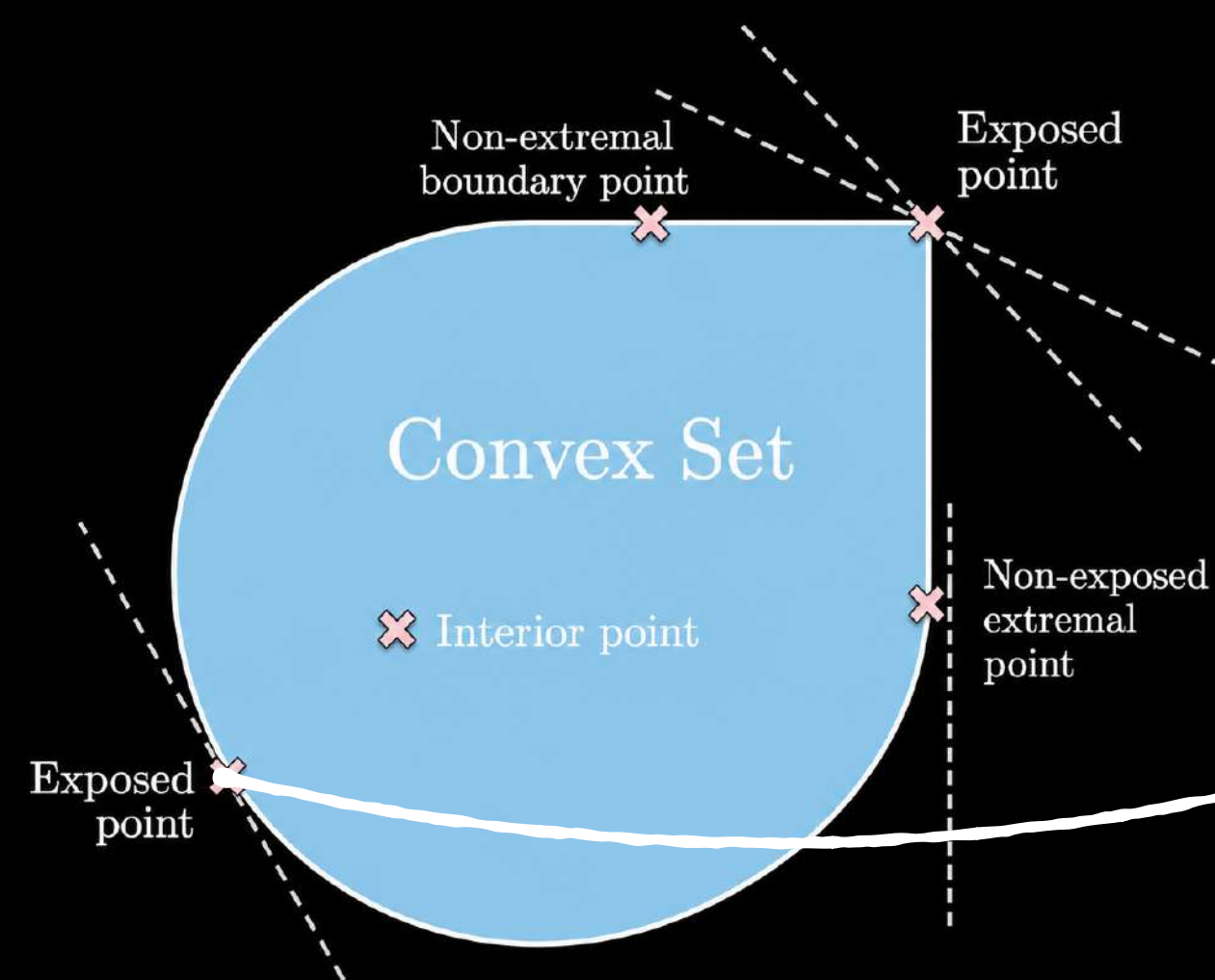
$$\Phi_A \otimes \Phi_B [\tilde{M}_a^x \otimes \tilde{N}_b^y |\tilde{\psi}\rangle] = (M_a^x \otimes N_b^y |\psi\rangle) \otimes |\text{junk}\rangle$$

AN EVENT SELF-TESTS THE REFERENCE STRATEGY S IF EVERY PHYSICAL STRATEGY $\tilde{S}$ REPRODUCING THE EVENT MUST BE RELATED TO THE REFERENCE STRATEGY S THROUGH A LOCAL ISOMETRY.

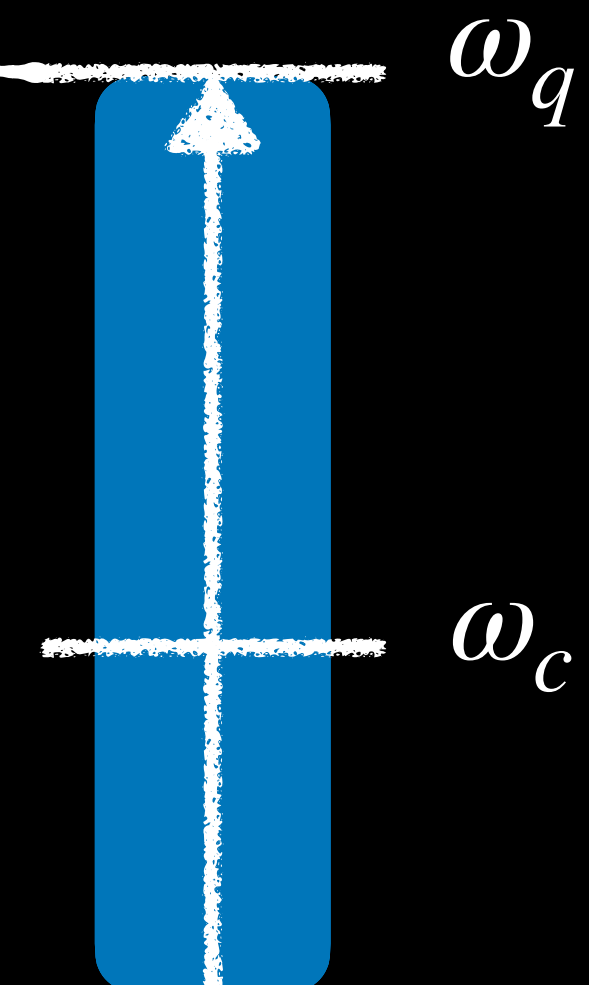
EXACT SELF-TESTING : DEFINITION



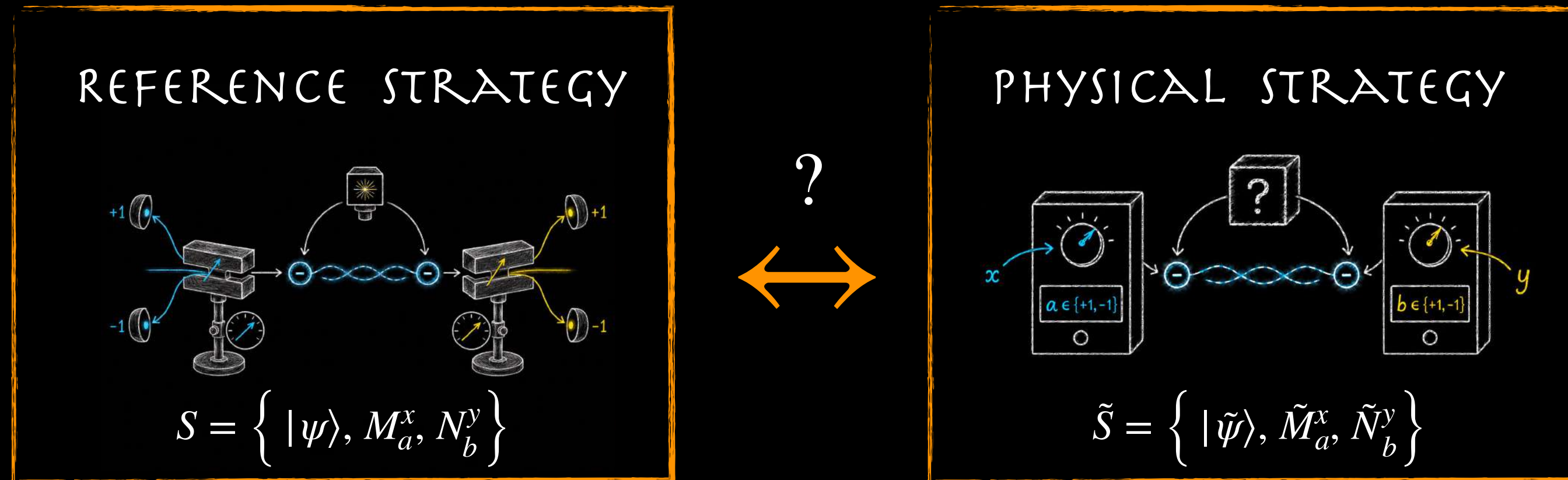
$$\Phi_A \otimes \Phi_B$$



SELF-TESTING
EVENT

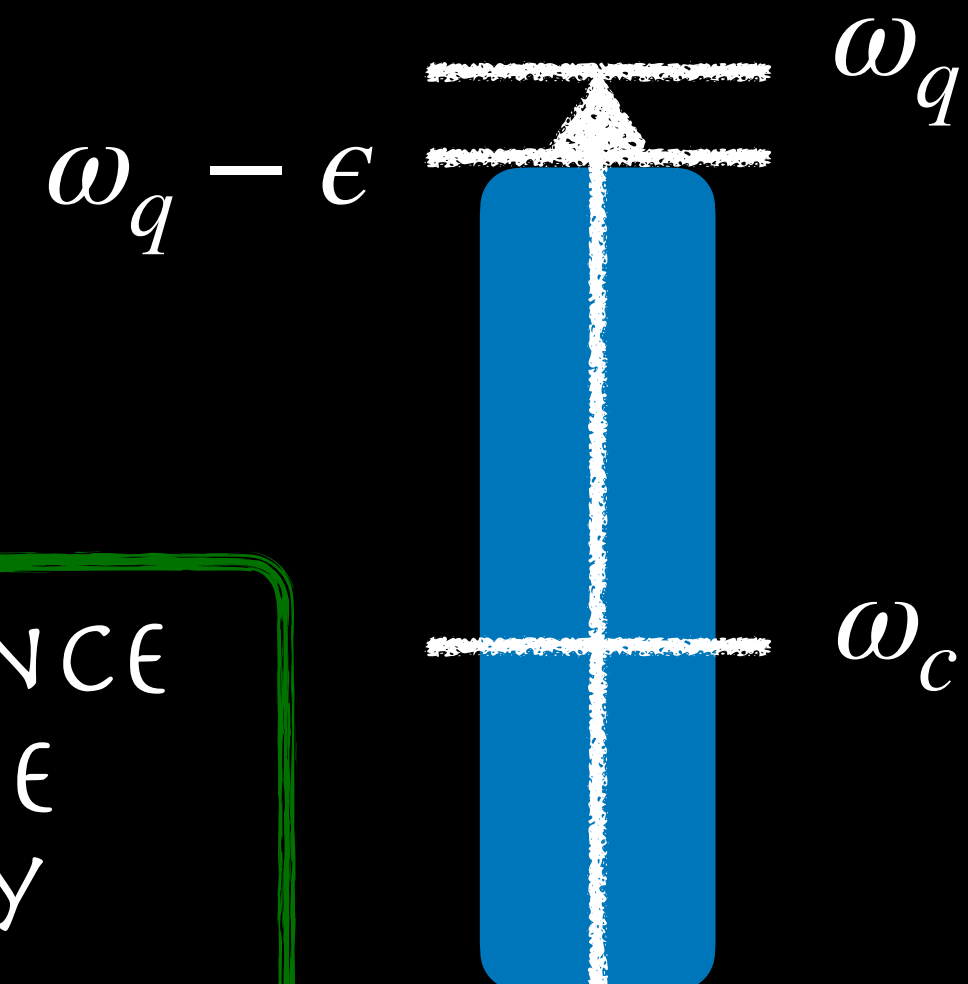


ROBUST SELF-TESTING



! unavoidable noise and errors,
finite statistics,
irrational numbers...

COULD LOCAL ISOMETRIES BRING
PHYSICAL STRATEGY CLOSE TO THE
REFERENCE ONE?

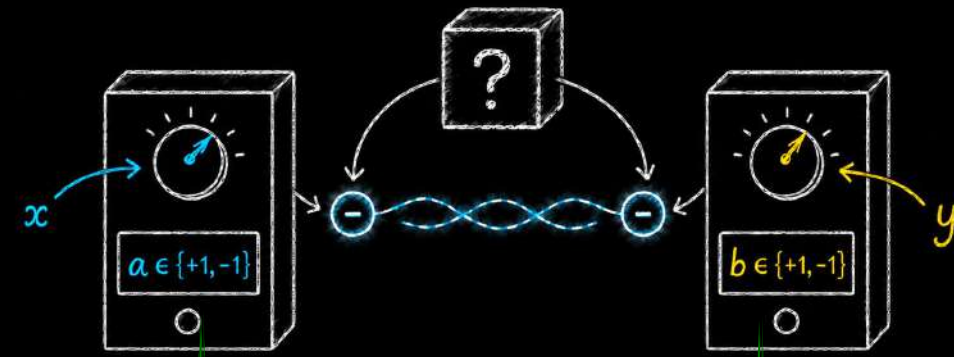


NAIVE DEFINITION: AN EVENT ROBUSTLY SELF-TESTS THE REFERENCE STRATEGY S IF EVERY PHYSICAL STRATEGY $\tilde{S}$ REPRODUCING THE EVENT UP TO A SMALL ERROR MUST HAVE A LOCAL ISOMETRY MAPPING IT CLOSE TO THE REFERENCE STRATEGY.

ROBUST SELF-TESTING

$$\Phi_A \otimes \Phi_B [|\tilde{\psi}\rangle] \approx |\psi\rangle \otimes |\text{junk}\rangle$$

PHYSICAL STRATEGY



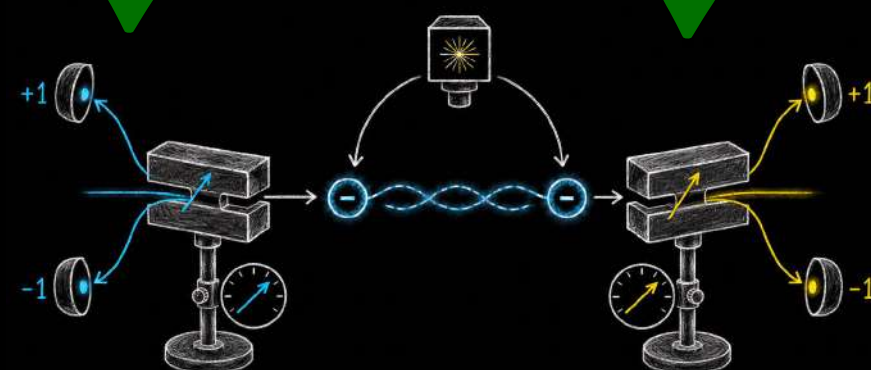
$$\tilde{S} = \{ |\tilde{\psi}\rangle, \tilde{M}_a^x, \tilde{N}_b^y \}$$

Φ_A



Φ_B

REFERENCE STRATEGY



$$S = \{ |\psi\rangle, M_a^x, N_b^y \}$$

ROBUST SELF-TESTING

$$\Lambda_A \otimes \Lambda_B [|\tilde{\psi}\rangle] \approx |\psi\rangle$$

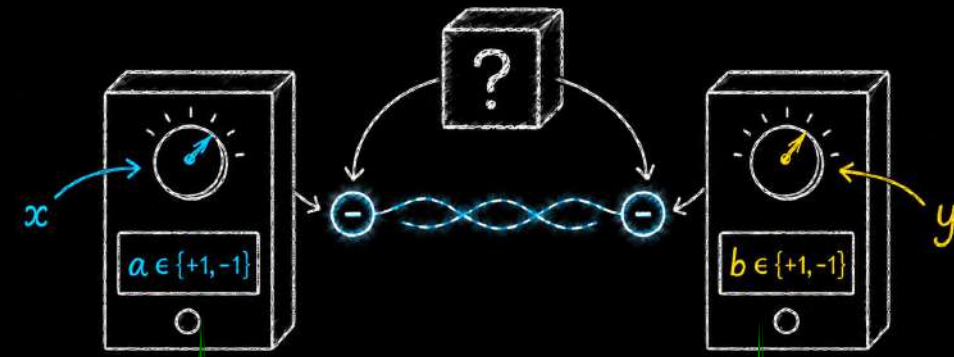
FIDELITY: $\langle \psi | \Lambda_A \otimes \Lambda_B (\tilde{\psi}) | \psi \rangle$

FIDELITY OPTIMISED
OVER ALL
EXTRACTION MAPS:

$$\max_{\Lambda_A, \Lambda_B} \langle \psi | \Lambda_A \otimes \Lambda_B (\rho) | \psi \rangle$$

Kaniewski
PRL 117, 070402 [2016]

PHYSICAL STRATEGY



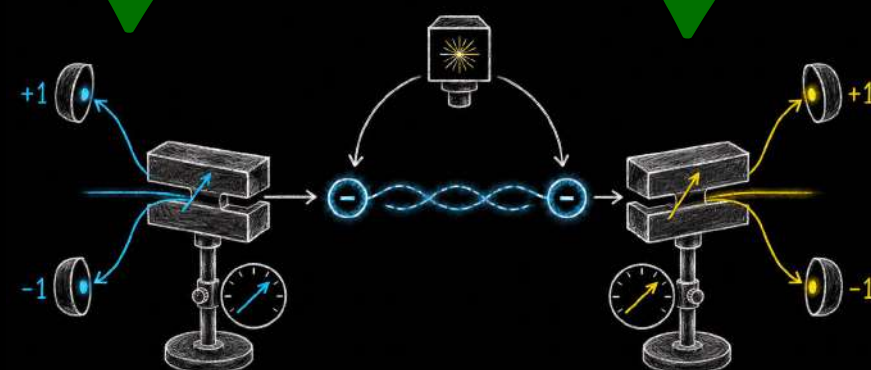
$$\tilde{S} = \{ |\tilde{\psi}\rangle, \tilde{M}_a^x, \tilde{N}_b^y \}$$

Λ_A



Λ_B

REFERENCE STRATEGY

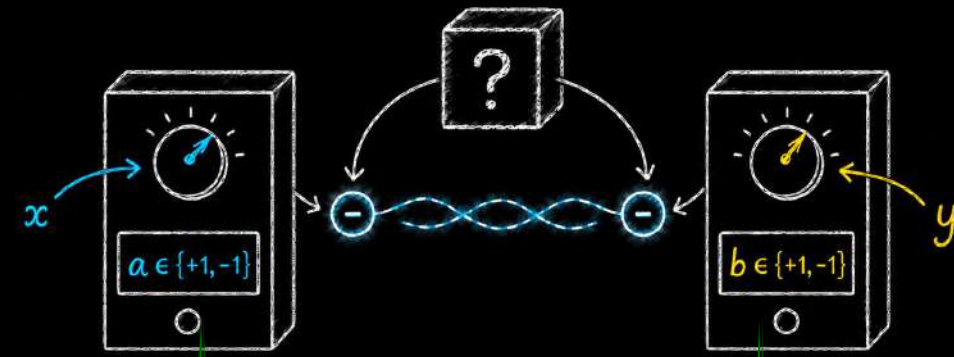


$$S = \{ |\psi\rangle, M_a^x, N_b^y \}$$

AN EVENT ROBUSTLY SELF-TESTS THE REFERENCE STATE $|\psi\rangle$ IF FROM EVERY PHYSICAL STATE $\tilde{\psi}$ REPRODUCING THE EVENT UP TO A SMALL ERROR ϵ THE EXTRACTABILITY OF THE REFERENCE STATE IS $1 - f(\epsilon)$, WHERE $\lim_{\epsilon \rightarrow 0} f(\epsilon) = 0$.

ROBUST SELF-TESTING

PHYSICAL STRATEGY



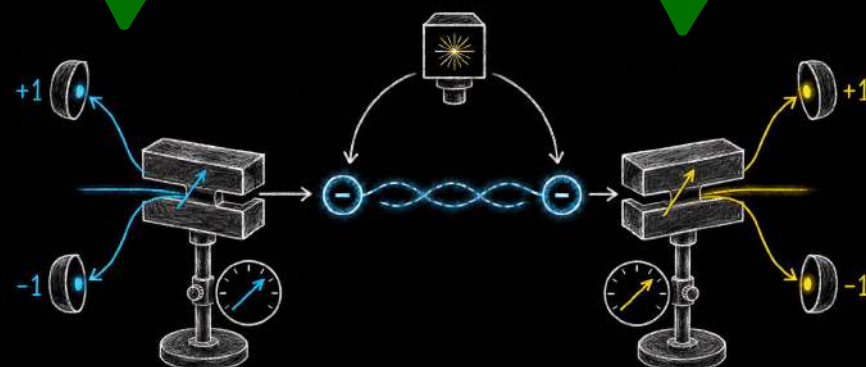
$$\tilde{S} = \{ |\tilde{\psi}\rangle, \tilde{M}_a^x, \tilde{N}_b^y \}$$

Λ_A



Λ_B

REFERENCE STRATEGY



$$S = \{ |\psi\rangle, M_a^x, N_b^y \}$$

$$\text{SCORE: } \omega_q - \epsilon$$

MINIMIZE
EXTRACTABILITY:

$$\min_{\tilde{\psi}: \omega(\tilde{\psi}) = \omega_q - \epsilon} \max_{\Lambda_A, \Lambda_B} \langle \psi | \Lambda_A \otimes \Lambda_B(\rho) | \psi \rangle$$

Kaniewski
PRL 117, 070402 [2016]

ASSUMPTIONS IN SELF-TESTING

Hilbert space is
finite-dimensional!



ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



In black-box
scenarios we can always
use Neimark dilation of
POVMs

ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



In black-box
scenarios we can always
use Neimark dilation of
POVMs



In black-box
scenarios we can always
purify the state.

ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



In black-box
scenarios we can always
use Neimark dilation of
POVMs



In black-box
scenarios we can always
purify the state.



The state we share has a
full rank!

ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



In black-box
scenarios we can always
use Neimark dilation of
POVMs



In black-box
scenarios we can always
purify the state.



The state we share has a
full rank!



We work with IID
sources!

ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



In black-box
scenarios we can always
use Neimark dilation of
POVMs



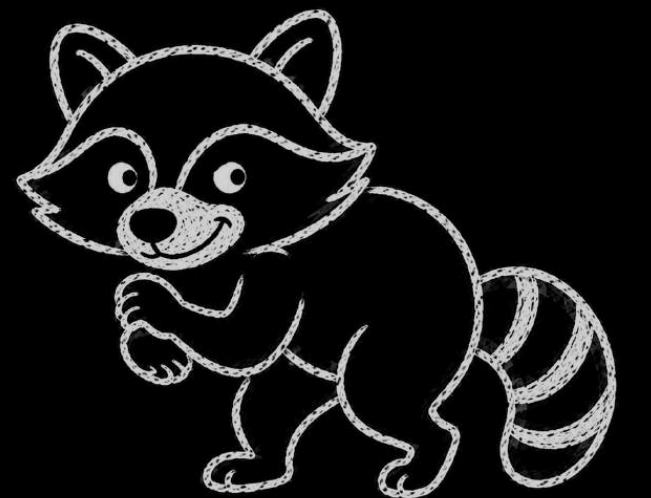
In black-box
scenarios we can always
purify the state.



The state we share has a
full rank!



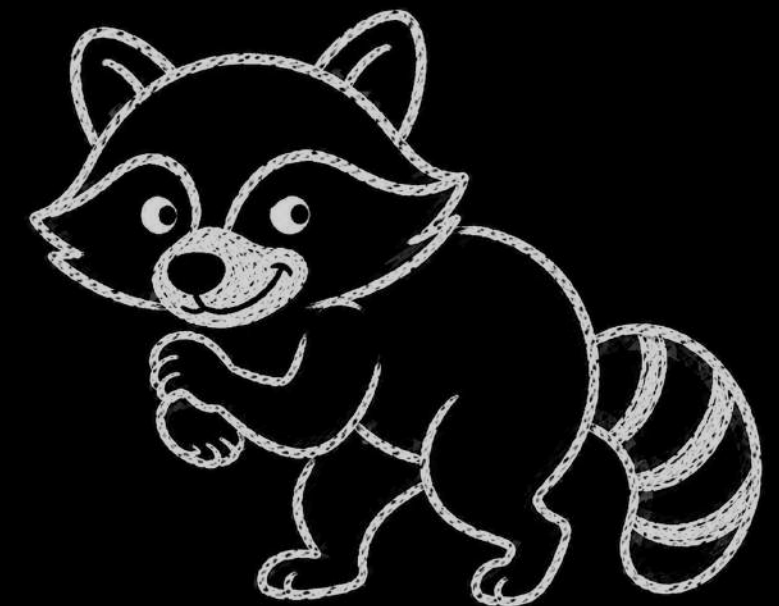
We work with IID
sources!



ASSUMPTIONS IN SELF-TESTING



LET $\mathcal{C}$ BE A CLASS OF QUANTUM STRATEGIES. AN EVENT $\mathcal{C}$ -SELF-TESTS THE REFERENCE STRATEGY S IF EVERY PHYSICAL STRATEGY $\tilde{S}$ REPRODUCING THE EVENT AND BELONGING TO $\mathcal{C}$ MUST BE RELATED TO THE REFERENCE STRATEGY S THROUGH A LOCAL ISOMETRY.



ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



For most
applications it is a fair
assumption. When not we can
work with self-testing in the
commuting operator
model !

ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



In black-box
scenarios we can always
purify the state.



For most
applications it is a fair
assumption. When not we can
work with self-testing in the
commuting operator
model !



Valid, if local isometries/
extraction channels act
trivially on the purification
Hilbert space.

ASSUMPTIONS IN SELF-TESTING



Hilbert space is
finite-dimensional!



In black-box
scenarios we can always
purify the state.



We work with IID
sources!



For most
applications it is a fair
assumption. When not we can
work with self-testing in the
commuting operator
model !



Valid, if local isometries/
extraction channels act
trivially on the purification
Hilbert space.



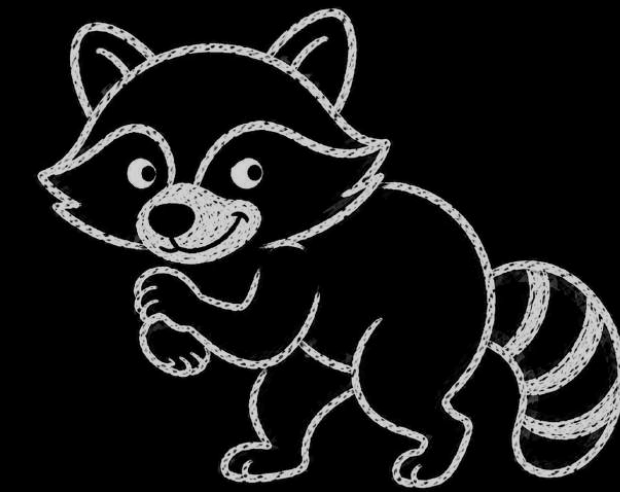
For cryptographic
applications we need to
generalise the result to
non-IID sources.

ASSUMPTIONS IN SELF-TESTING



To get my self-testing statement I assumed the state is pure, measurements are PVM and the state has full rank

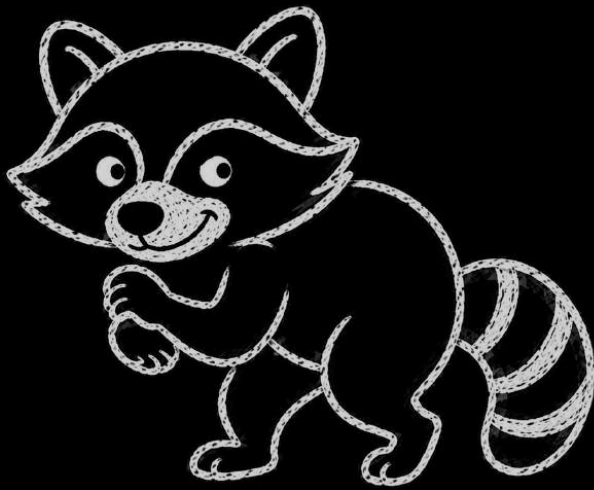
I might get something from there !



ASSUMPTIONS IN SELF-TESTING



To get my self-testing statement I assumed the state is pure, measurements are PVM and the state has full rank



I might get something from there !



Could you remove either a PVM or a full rank assumption?



Actually I can, not both, but one of them I can choose!



EPR SELF-TESTING

$$\omega = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$$

$$\omega_c = 2 \qquad \omega_q = 2\sqrt{2}$$

CHSH inequality (game) is rigid: the maximal value (robustly) self-tests EPR pair and anticommuting measurements performed by both Alice and Bob without assumptions!

STATE SELF-TESTING

All bipartite states

Coladangelo, Goh, Scarani
Nat. Comm. 8, 15485 [2017]

$$\alpha_0|00\rangle + \alpha_1|11\rangle + \alpha_2|22\rangle + \alpha_3|33\rangle$$

STATE SELF-TESTING

All bipartite states

Coladangelo, Goh, Scarani
Nat. Comm. 8, 15485 [2017]

$$\alpha_0 |00\rangle + \alpha_1 |11\rangle + \alpha_2 |22\rangle + \alpha_3 |33\rangle$$

Self-testing partially entangled states
through tilted CHSH inequalities

Bamps, Pironio
PRA 91,5 [2015]

STATE SELF-TESTING

All bipartite states

Coladangelo, Goh, Scarani
Nat. Comm. 8, 15485 [2017]

$$\alpha_0 |00\rangle + \alpha_1 |11\rangle + \alpha_2 |22\rangle + \alpha_3 |33\rangle$$

The equation $\alpha_0 |00\rangle + \alpha_1 |11\rangle + \alpha_2 |22\rangle + \alpha_3 |33\rangle$ is shown. The first two terms, $\alpha_0 |00\rangle + \alpha_1 |11\rangle$, are enclosed in a blue oval. The next two terms, $\alpha_2 |22\rangle + \alpha_3 |33\rangle$, are enclosed in a green oval. Two white arrows point from the bottom of these ovals towards the text 'Self-testing partially entangled states through tilted CHSH inequalities'.

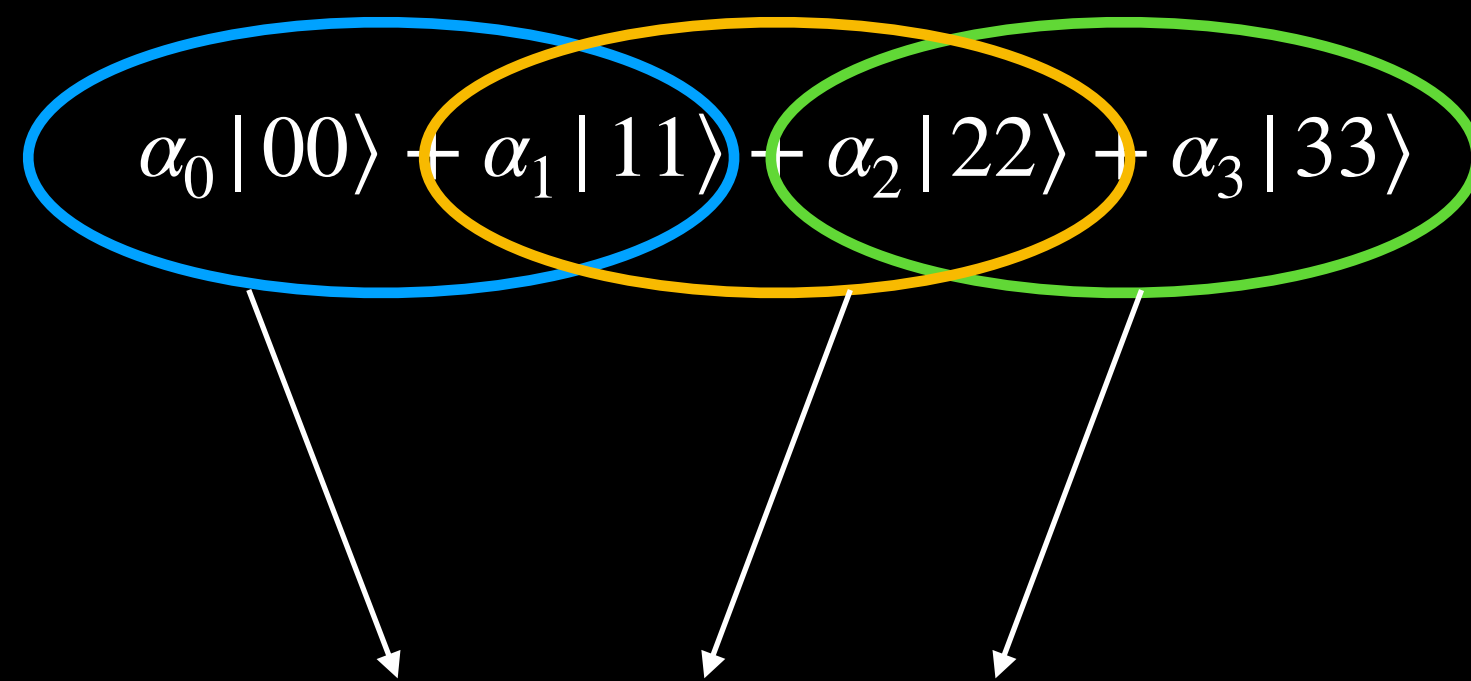
Self-testing partially entangled states
through tilted CHSH inequalities

Bamps, Pironio
PRA 91,5 [2015]

STATE SELF-TESTING

All bipartite states

Coladangelo, Goh, Scarani
Nat. Comm. 8, 15485 [2017]



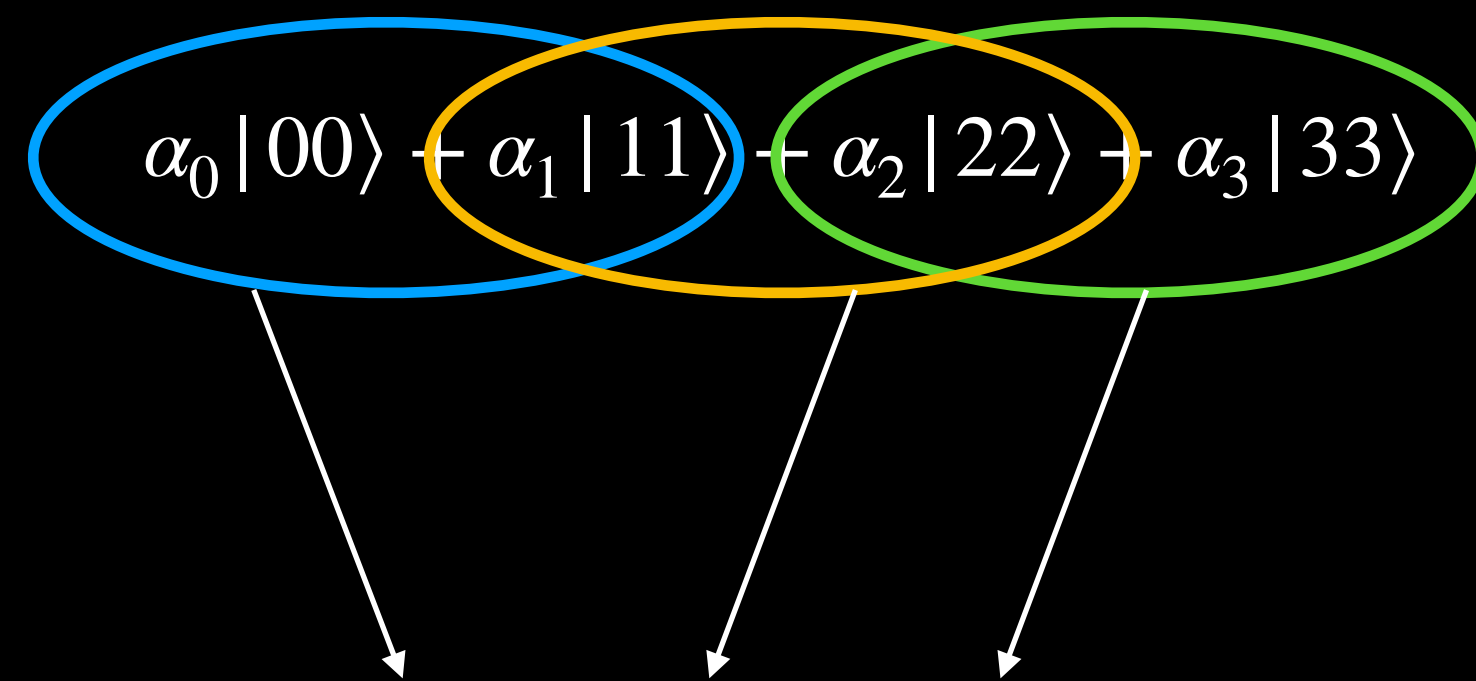
Self-testing partially entangled states
through tilted CHSH inequalities

Bamps, Pironio
PRA 91,5 [2015]

STATE SELF-TESTING

All bipartite states

Coladangelo, Goh, Scarani
Nat. Comm. 8, 15485 [2017]

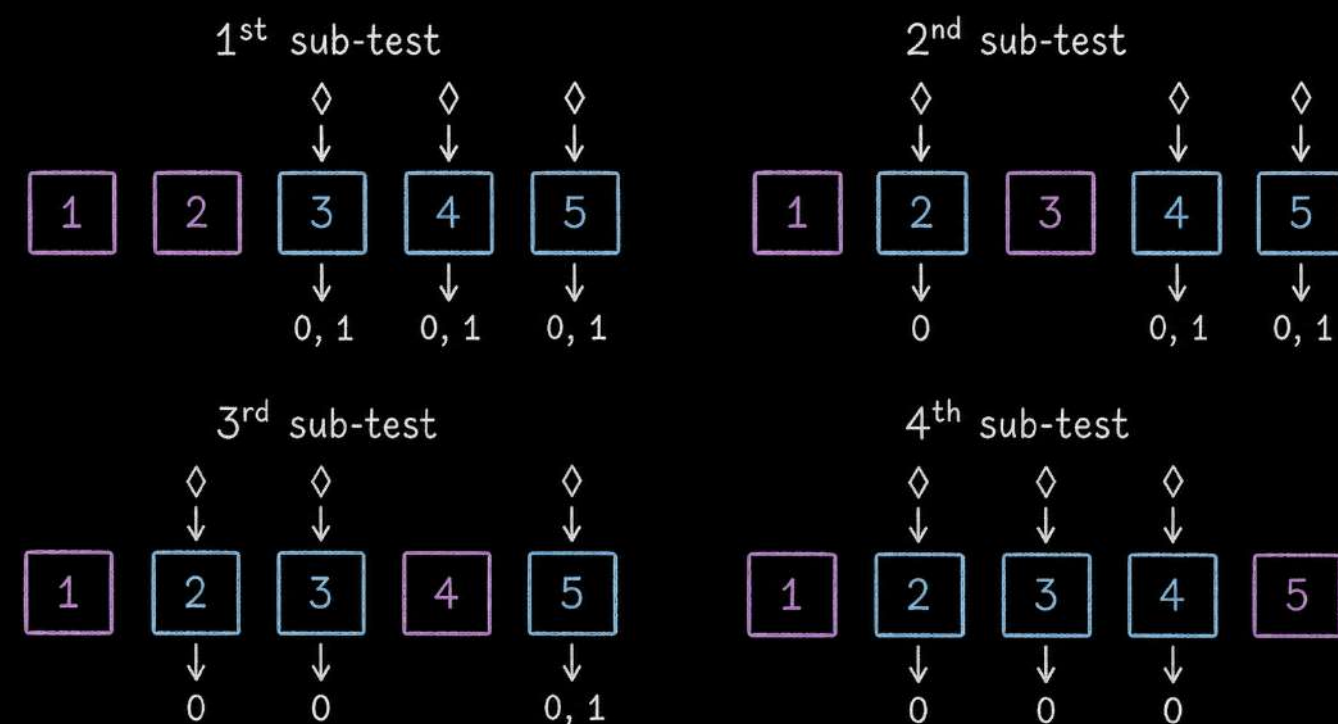
$$\alpha_0 |00\rangle + \alpha_1 |11\rangle + \alpha_2 |22\rangle + \alpha_3 |33\rangle$$


Self-testing partially entangled states
through tilted CHSH inequalities

Bamps, Pironio
PRA 91,5 [2015]

All qubit multipartite states

Balanzo-Juando, Coladangelo, Augusiak,
Acin, Šupić
Nat. Comm. [2026]



STATE SELF-TESTING

All bipartite states

Coladangelo, Goh, Scarani
Nat. Comm. 8, 15485 [2017]

$$\alpha_0 |00\rangle + \alpha_1 |11\rangle + \alpha_2 |22\rangle + \alpha_3 |33\rangle$$

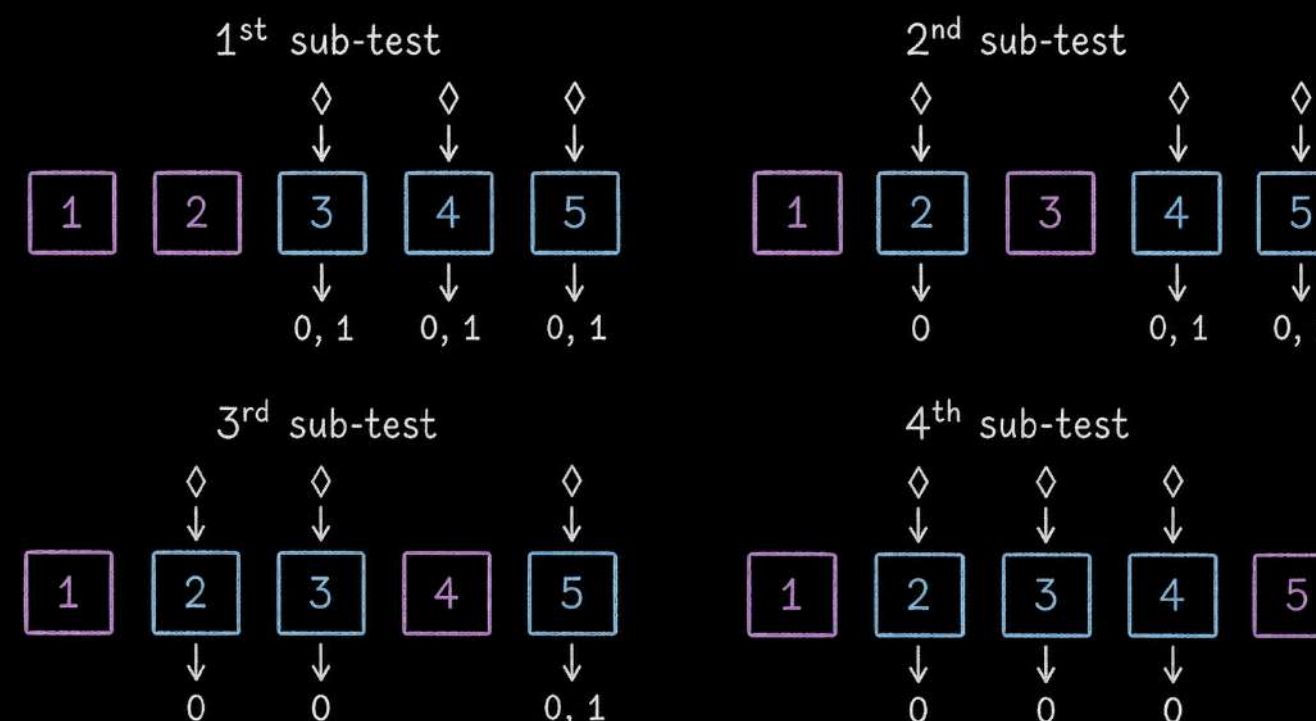
The expression $\alpha_0 |00\rangle + \alpha_1 |11\rangle + \alpha_2 |22\rangle + \alpha_3 |33\rangle$ is shown with four overlapping ellipses: a blue one around $\alpha_0 |00\rangle$, an orange one around $\alpha_1 |11\rangle$, a yellow one around $\alpha_2 |22\rangle$, and a green one around $\alpha_3 |33\rangle$. Arrows point from each ellipse towards the text 'Self-testing partially entangled states through tilted CHSH inequalities'.

Self-testing partially entangled states
through tilted CHSH inequalities

Bamps, Pironio
PRA 91,5 [2015]

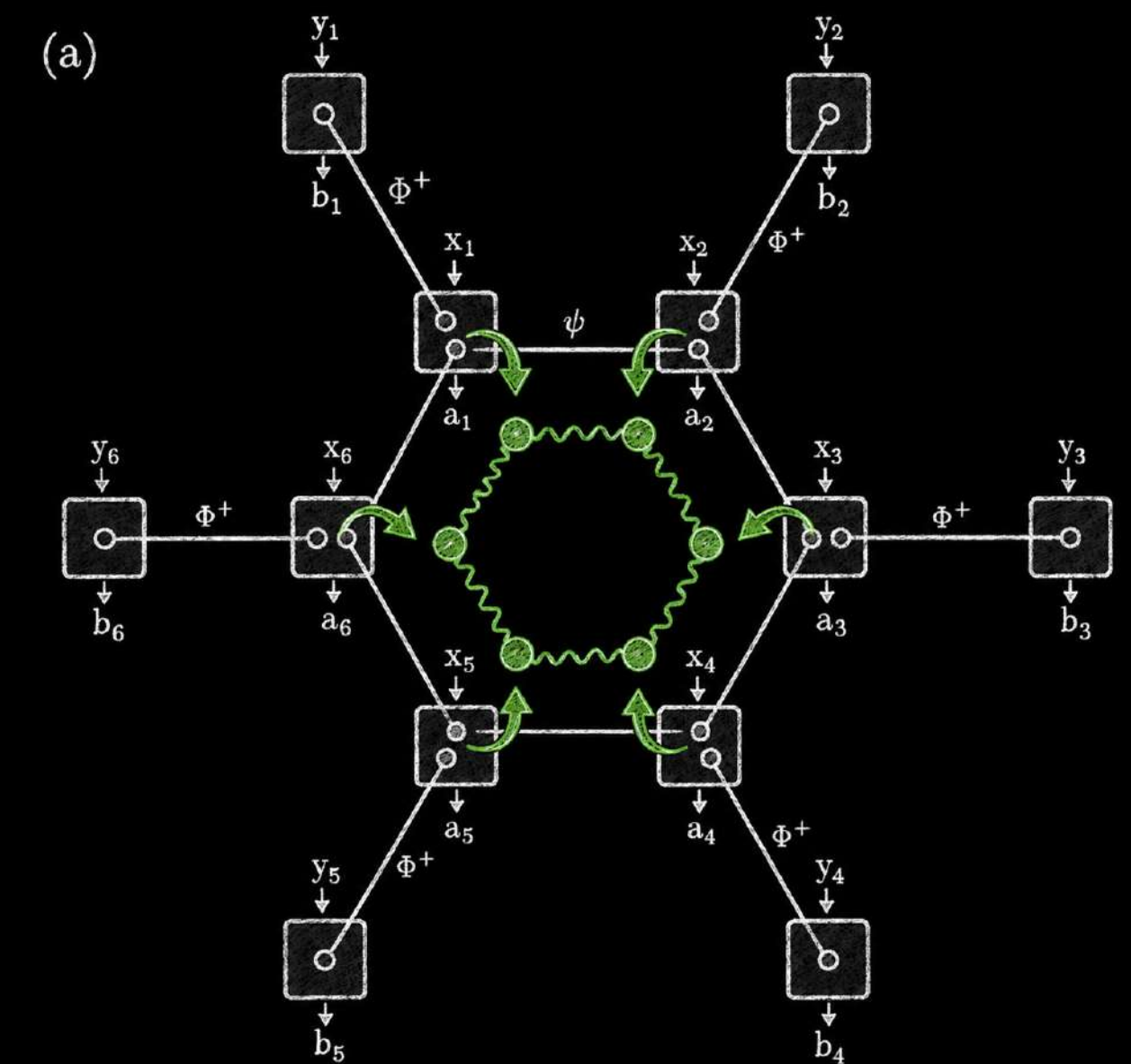
All qubit multipartite states

Balanzo-Juando, Coladangelo, Augusiak,
Acin, Šupić
Nat. Comm. [2026]

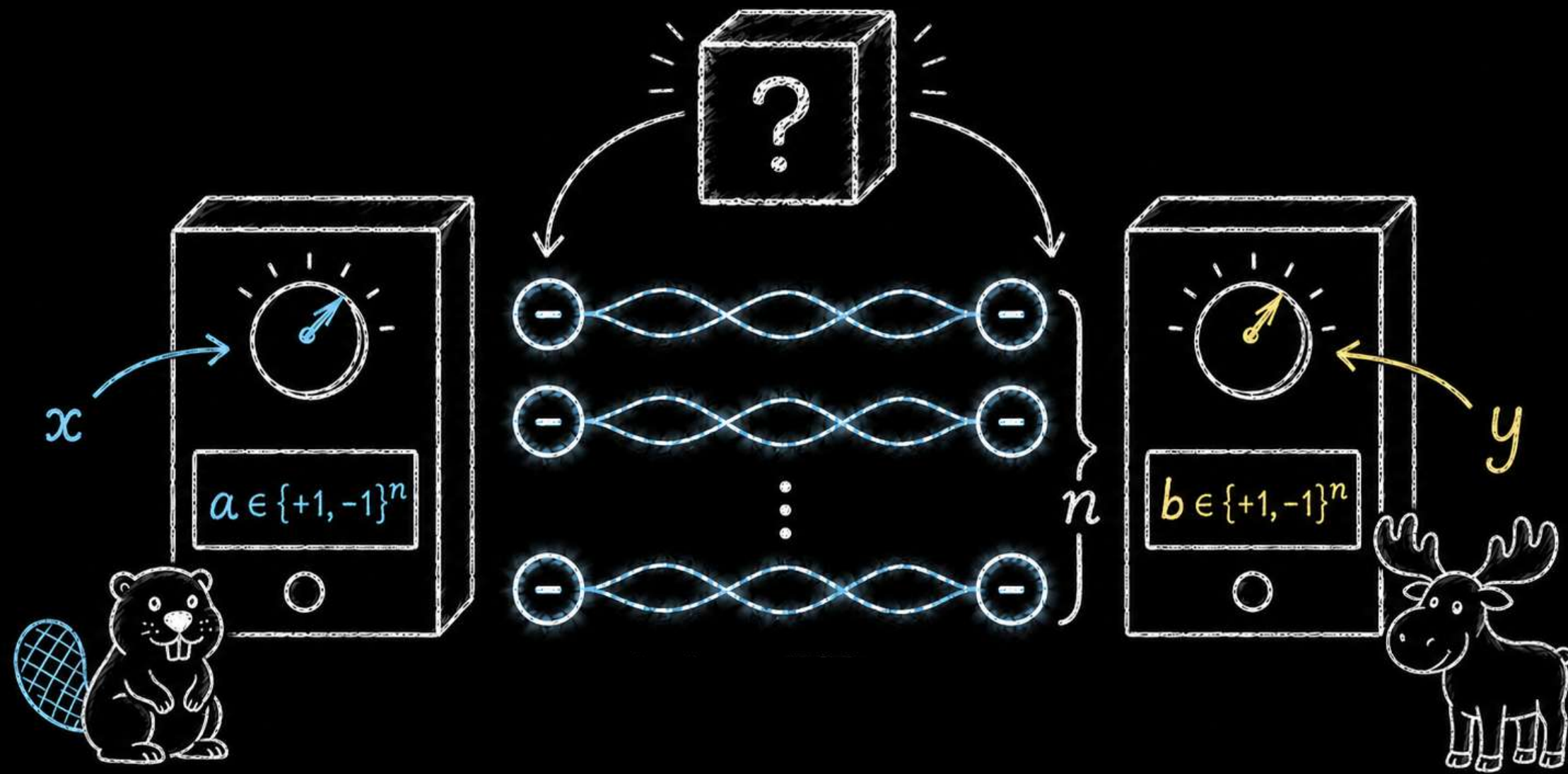


All states in networks

Šupić, Bowles, Renou, Acin, Hoban
Nat. Phys. 19,5 [2023]



SCALING UP : n EPR PAIRS

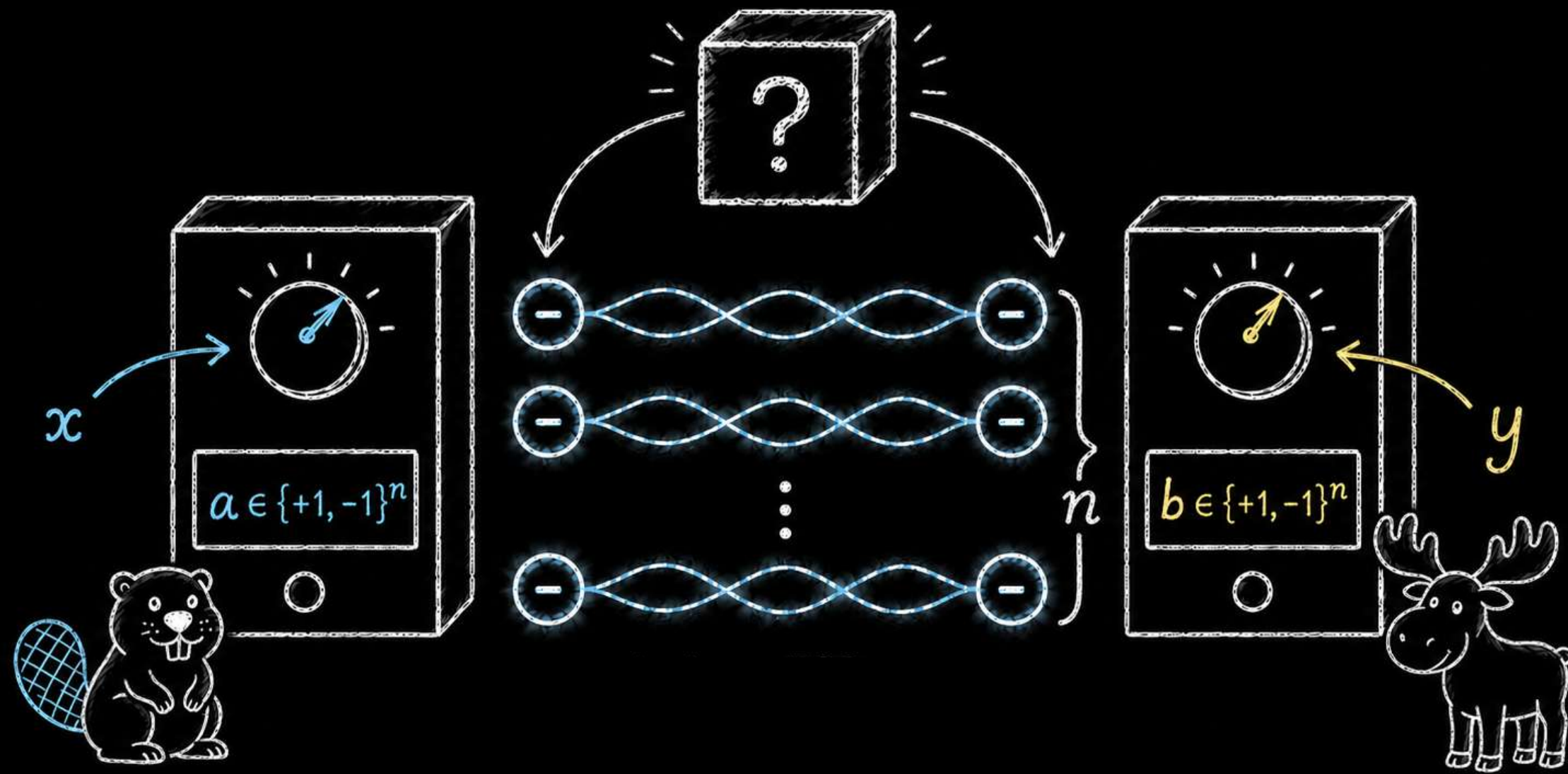


NAIVE APPROACH: PLAY n CASH GAMES IN PARALLEL

QUESTIONS HAVE LENGTH n

ROBUSTNESS DEGRADES AS n GROWS, PAIRS ARE EXTRACTED ONE BY ONE.

SCALING UP : n EPR PAIRS



NAIVE APPROACH: PLAY n CASH GAMES IN PARALLEL

QUESTIONS HAVE LENGTH n

ROBUSTNESS DEGRADES AS n GROWS, PAIRS ARE EXTRACTED ONE BY ONE.

THE FACT THAT WE WILL NEED

THERE ARE NONLOCAL GAMES THAT ROBUSTLY SELF-TEST n EPR PAIRS AND PAULI-BASIS MEASUREMENTS ON THEM, USING QUESTIONS OF LENGTH $O(\log n)$ WITH ROBUSTNESS INDEPENDENT OF n .

Proof: Act 3

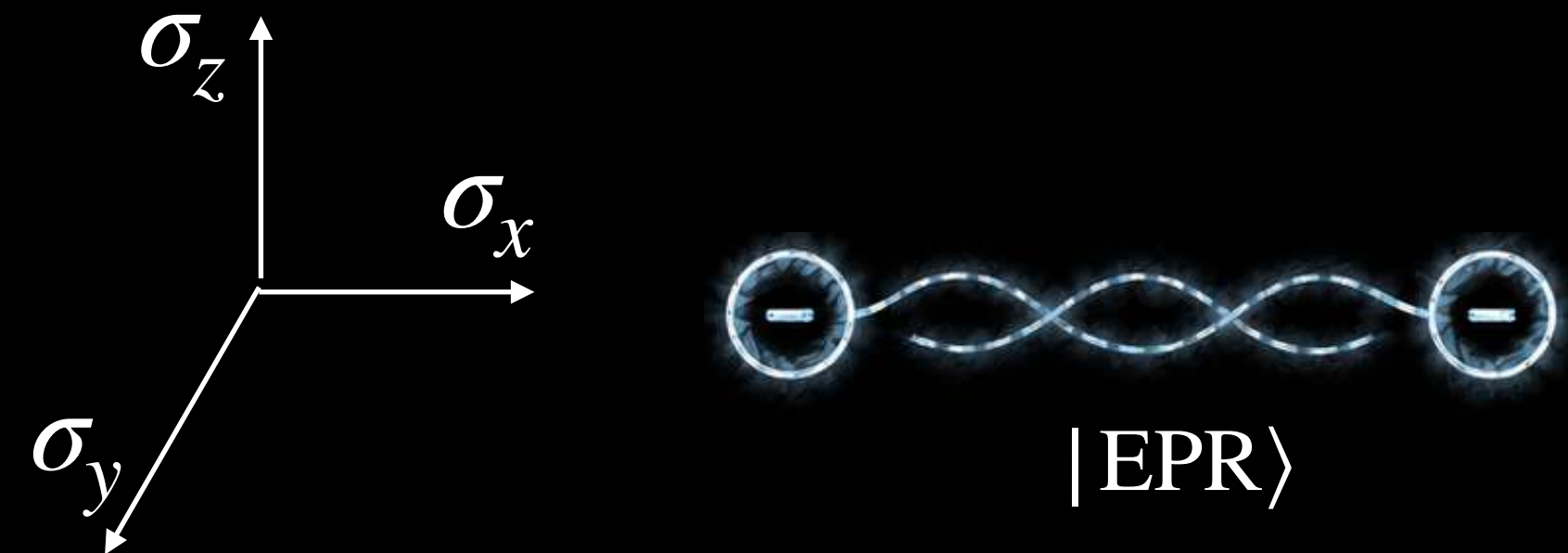
★ ACT 2 : SOME APPLICATIONS

APPLICATIONS IN CRYPTOGRAPHY

PRIVATE DI RANDOMNESS AND QKD

Acin, Pironio, Vertesi, Wittek
PRA 93 [2016]

- MAXIMAL
RANDOMNESS FROM
QUBIT STATES
- **GISIN'S ELEGANT BELL
INEQUALITY** SELF-TESTS
**THREE PAULIS ON
ALICE'S SIDE** AND AN
EPR PAIR
- THREE PAULIS ARE
TOMOGRAPHICALLY
COMPLETE



$$\langle EPR | A_x \otimes B_y | EPR \rangle = \frac{1}{2} \text{Tr}[A_x B_y^T]$$

B_y IS A FOUR-OUTCOME POVM
(TETRAHEDRON)

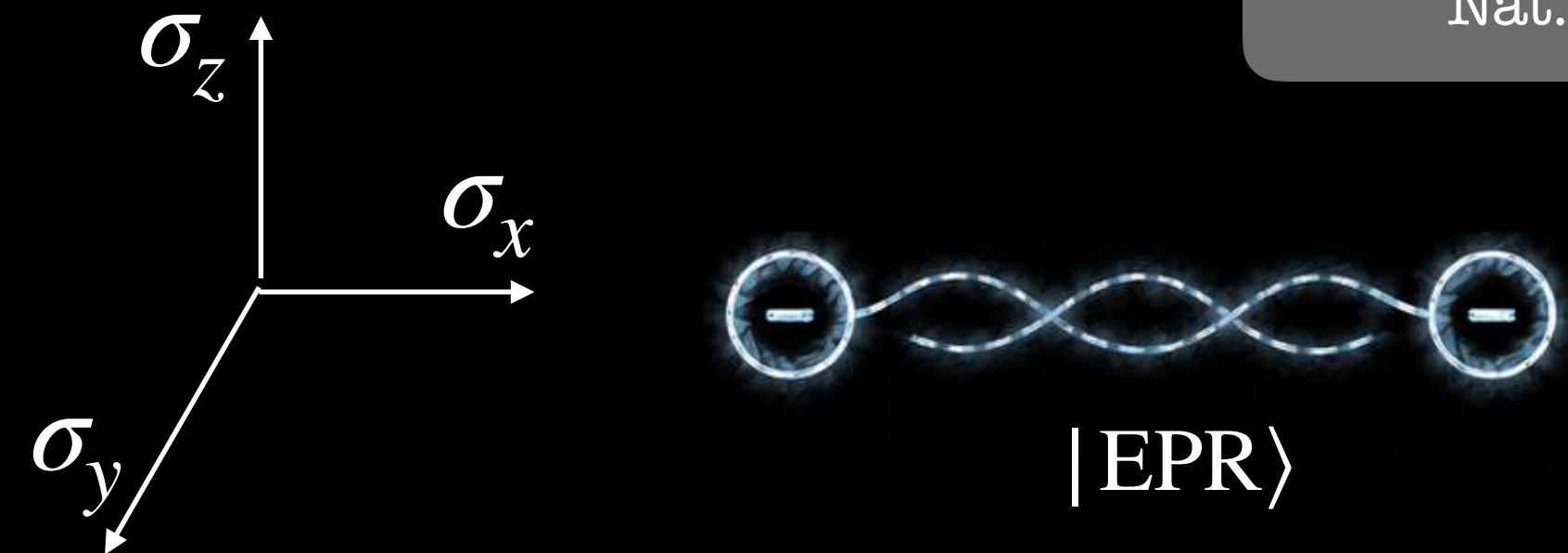
APPLICATIONS IN CRYPTOGRAPHY

PRIVATE DI RANDOMNESS AND QKD

Acin, Pironio, Vertesi, Wittek
PRA 93 [2016]

Farkas, Volcic, Storgaard, Chen,
Mancinska
Nat. Phys. 22, 2 [2026]

- MAXIMAL
RANDOMNESS FROM
QUBIT STATES
- **GISIN'S ELEGANT BELL
INEQUALITY** SELF-TESTS
**THREE PAULIS ON
ALICE'S SIDE** AND AN
EPR PAIR
- THREE PAULIS ARE
TOMOGRAPHICALLY
COMPLETE



$2 \log(d)$

$$\langle EPR | A_x \otimes B_y | EPR \rangle = \frac{1}{2} \text{Tr}[A_x B_y^T]$$

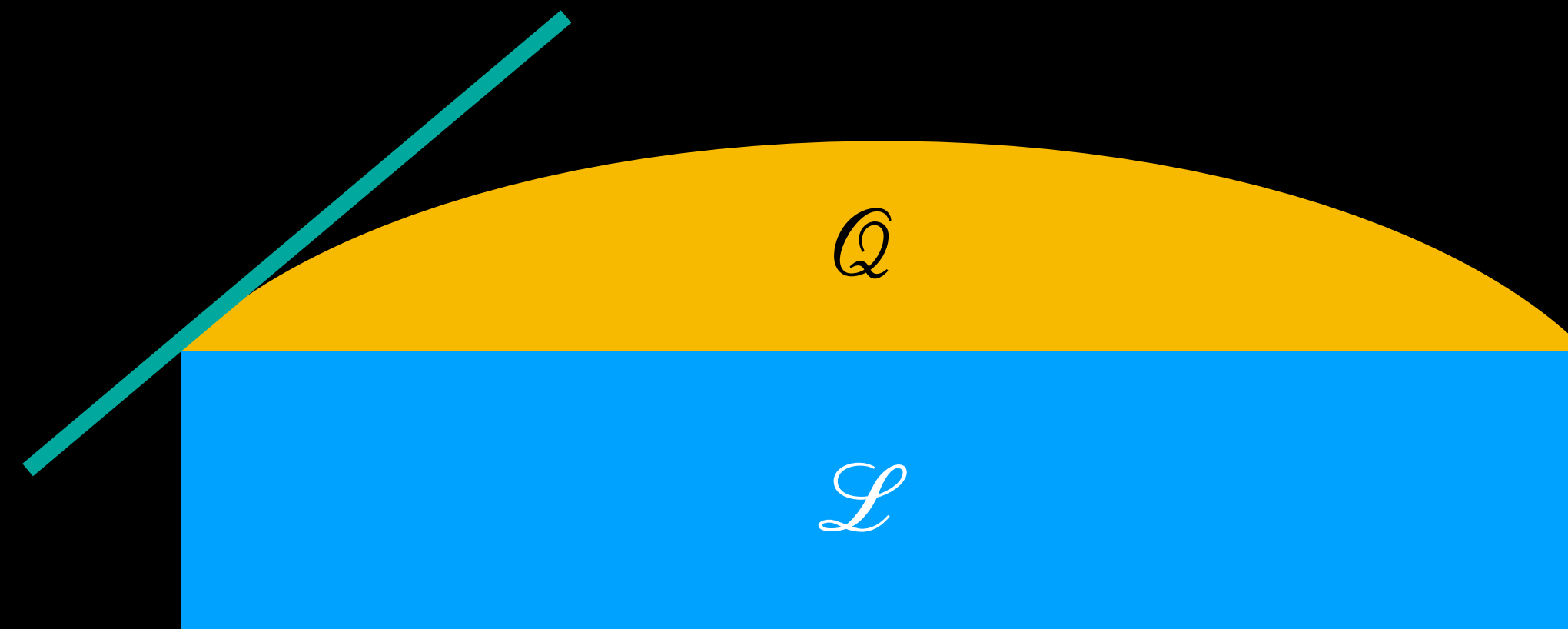
B_y IS A FOUR-OUTCOME POVM
(TETRAHEDRON)

APPLICATIONS IN CRYPTOGRAPHY

PRIVATE RANDOMNESS AND QKD

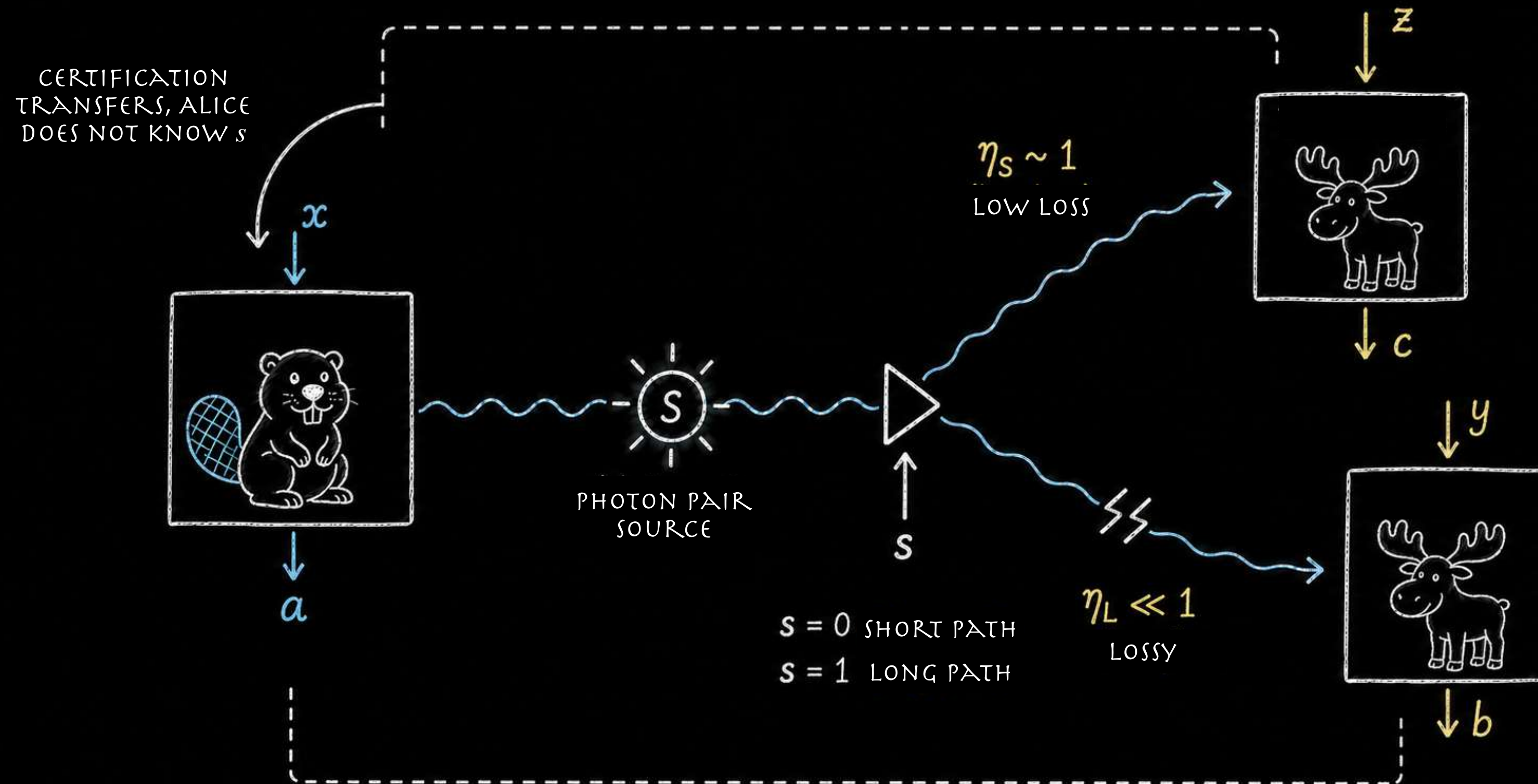
- MAXIMAL RANDOMNESS FROM ARBITRARY SMALL NONLOCALITY
- BELL OPERATOR: $\cos(\theta + \phi)\cos(\theta + \omega)A_0(\cos \omega B_0 - \cos \phi B_1) + \cos \phi \cos \omega A_1 (-\cos(\theta + \omega)B_0 + \cos(\theta + \phi)B_1)$
- MAXIMAL VIOLATION SELF-TESTS THE STRATEGY: $|\psi\rangle = \frac{|00\rangle + i|11\rangle}{\sqrt{2}}$, $A_0 = \sigma_x$, $A_1 = \cos \theta \sigma_x + \sin \theta \sigma_y$
 $B_0 = \cos \phi \sigma_x + \sin \phi \sigma_y$, $B_1 = \cos \omega \sigma_x + \sin \omega \sigma_y$

Wooltorton, Brown, Colbeck
PRL 132(21) [2024]



APPLICATIONS IN CRYPTOGRAPHY

TESTING ROUND



1. SHORT RANGE TEST REACHES A HIGH CHSH VALUE: SELF-TEST OF THE SOURCE AND ALICE'S MEASUREMENTS

2. THE SOURCE AND ALICE'S DEVICES ARE THE SAME IN BOTH CONFIGURATIONS

3. EFFECTIVELY KEY IS GENERATED IN A SEMI-DEVICE-INDEPENDENT MANNER

Chaturvedi, Viola, Pawłowski
npj QI 10, 7 [2024]

Lobo, Pauwels, Pironio
Quantum 8, 1332 [2024]

Le Roy-Deloison, Lobo, Pauwels,
Pironio
PRX Quantum 6, 020311 [2025]

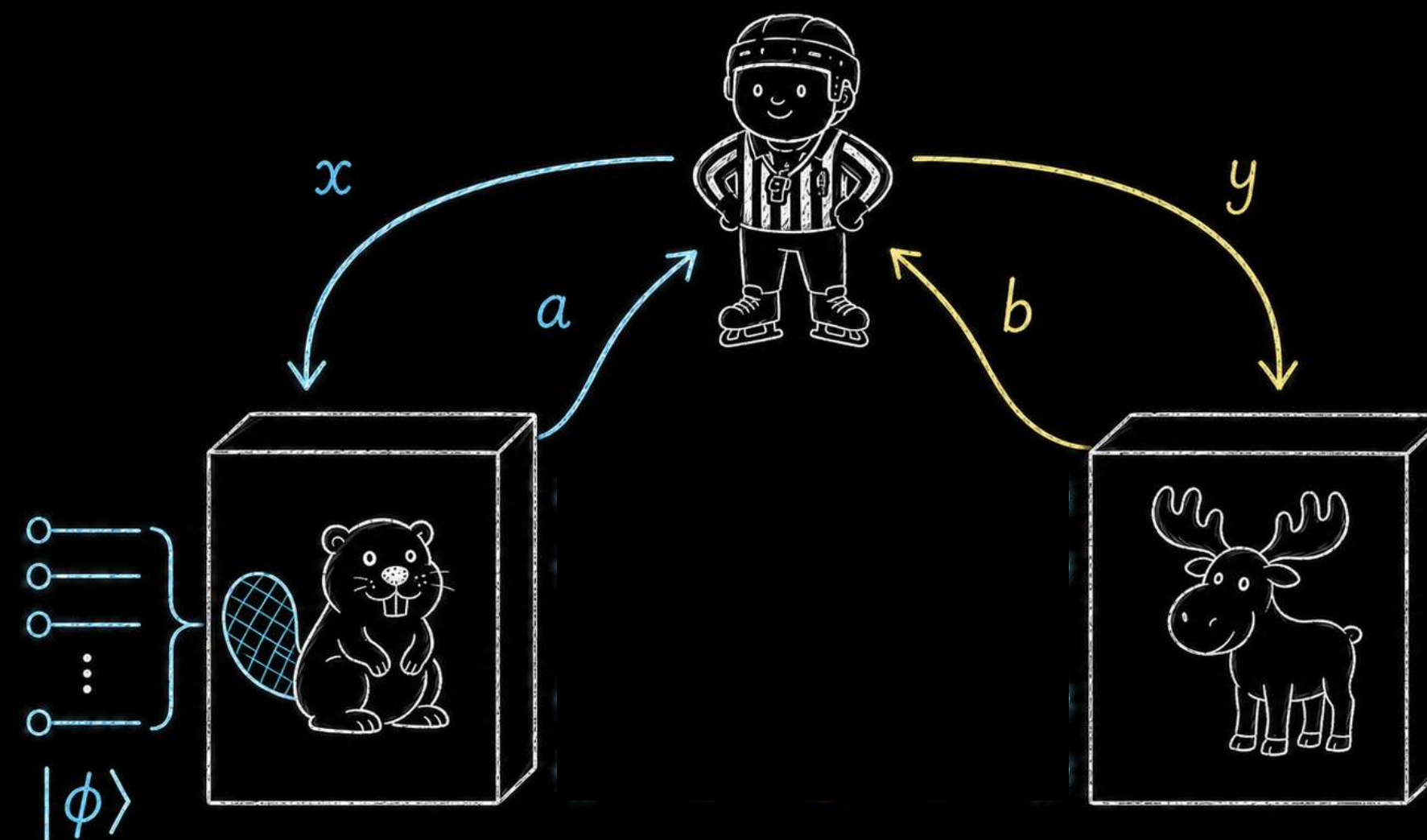
PROOF OF QUANTUM KNOWLEDGE

A PROOF OF KNOWLEDGE CONVINCES A VERIFIER THAT THE PROVER HAS SOMETHING, A PRIVATE KEY OR A CREDENTIAL, WITHOUT REVEALING IT.

FORMALISED BY AN EXTRACTOR: GIVEN ORACLE ACCESS TO ANY PROVER THAT MAKES THE VERIFIER ACCEPT IT RECONSTRUCTS THE SECRET.

QUANTUM VERSION:

1. WITNESS IS A QUANTUM STATE (GROUND STATE OF A LOCAL HAMILTONIAN)
2. THE VERIFIER IS CLASSICAL, IT CANNOT RECEIVE A QUBIT
3. THE WITNESS CANNOT BE COPIES

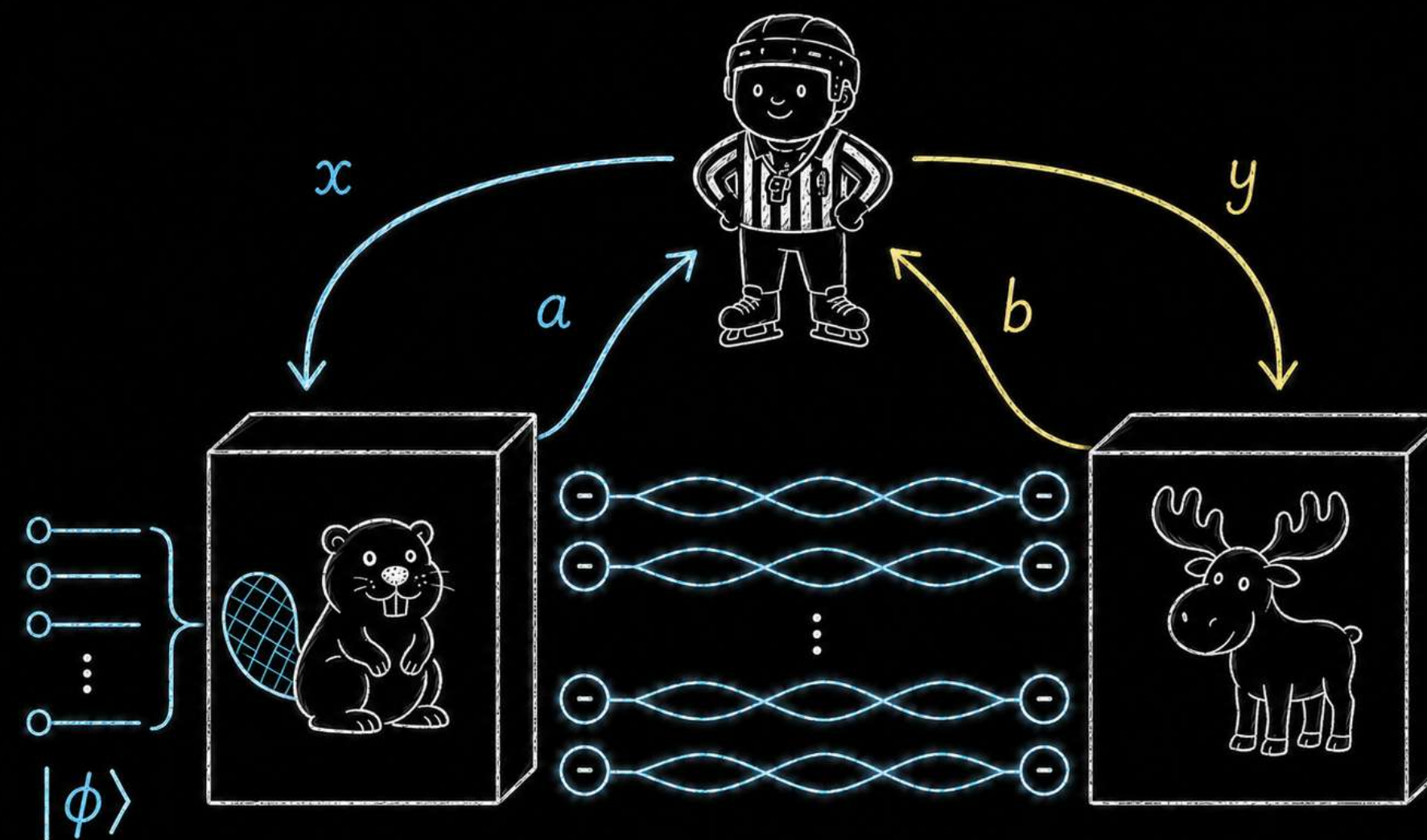


PROOF OF QUANTUM KNOWLEDGE

SELF-TESTING ROUND: VERIFIER ENSURES THAT PROVERS SHARE n EPR PAIRS AND PAULI MEASUREMENTS

ENERGY ROUND: PROVER ALICE IS ASKED TO TELEPORT HER QUANTUM WITNESS TO BOB, AND BOB GETS THE SAME QUESTION AS IN THE SELF-TESTING ROUND.

EXTRACTION ISOMETRY (A PARTICULAR ONE, THE SWAP GATE) IS USED AS THE EXTRACTOR OF THE WITNESS!



Broadbent, Grilo, Hara, Mehta,
arXiv: 2503.13699 [2025]

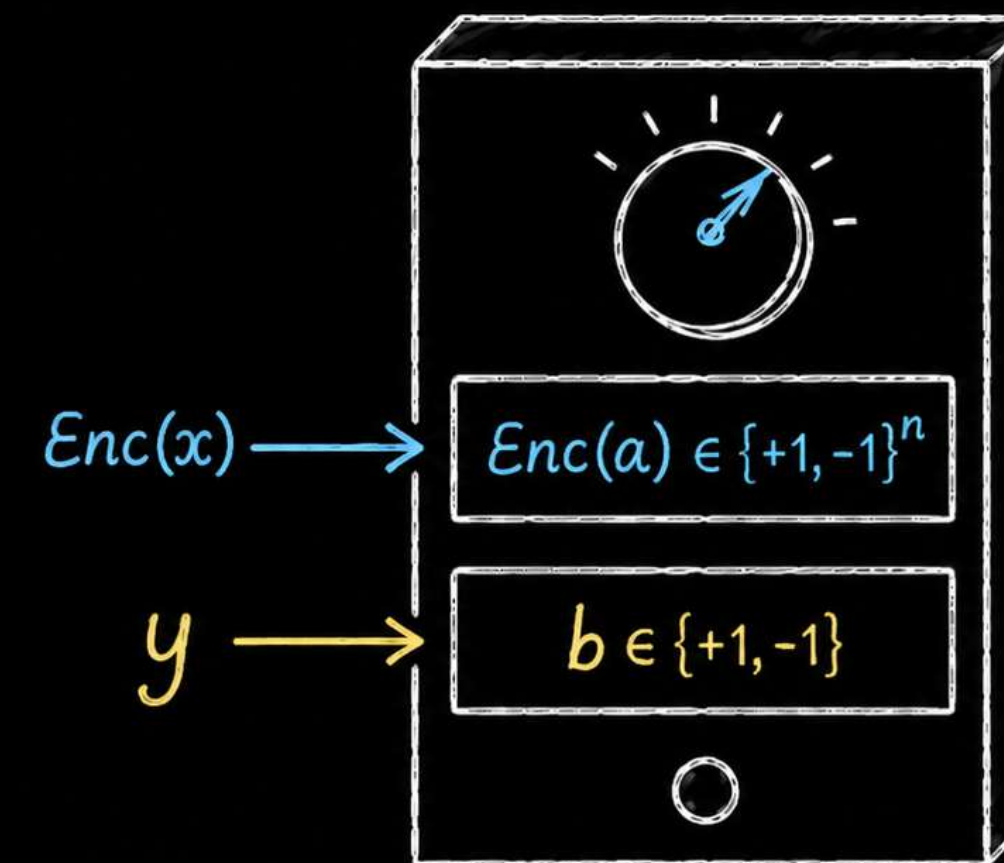
COMPILED NONLOCAL GAMES

PROOFS OF QUANTUMNESS AND A WAY OUT OF THE TWO-DEVICE PROBLEM

NONLOCAL GAMES REQUIRE SPATIAL SEPARATION, A CONDITION THAT IS NOT EASY TO IMPOSE, AND IN MANY ARCHITECTURES IT IS NOT POSSIBLE.

Kalai, Lombardi, Vaikuntanathan, Yang
STOC [2023]

IND-CPA SECURITY OF QHE ENCRYPTION ENSURES THAT THE PROVER CANNOT GUESS x BETTER THAN RANDOMLY GUESSING. IN FACT THE SECURITY EMULATES THE LOCALITY CONDITION FROM BELL TESTS!



FOR ALL GAMES CLASSICAL BOUND IS PRESERVED THROUGH THE COMPILATION, AND FOR MOST GAMES (NON-PATHOLOGICAL ONES) THE QUANTUM BOUND IS PRESERVED ALSO.

RIGIDITY OF COMPILED NONLOCAL GAMES

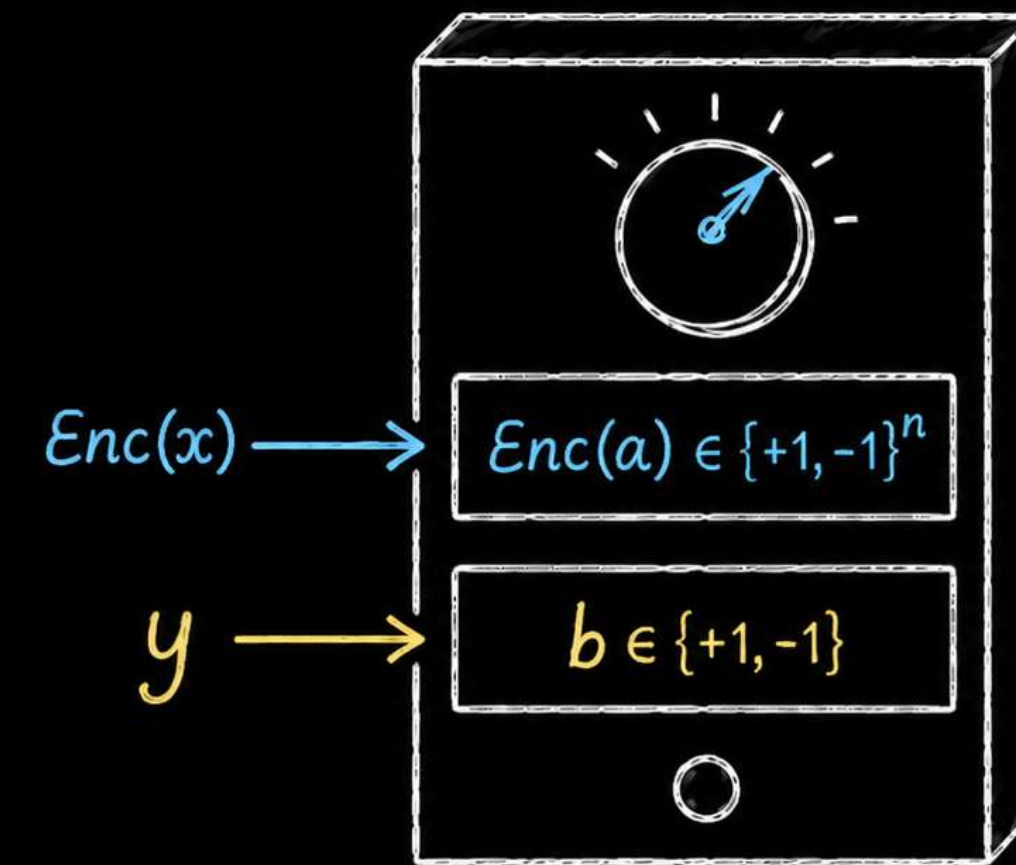
PROOFS OF QUANTUMNESS AND A WAY OUT OF THE TWO-DEVICE PROBLEM

WHY IS IT HARD?

NO TENSOR PRODUCT STRUCTURE

HOW TO DEFINE LOCALITY AND
ENTANGLEMENT FOR A SINGLE DEVICE?

HOW TO DEAL WITH ENCRYPTED
OPERATIONS?



WHAT IS KNOWN?

THE STATE COMING TO THE SECOND
ROUND AND THE MEASUREMENTS
PERFORMED IN THE SECOND ROUND
CAN BE SELF-TESTED FOR A FAIRLY
LARGE CLASS OF GAMES

Natarajan, Zhang
FOCS [2023]

Cui, Malavolta, Mehta, Natarajan, Paddock, Schmidt, Walter, Zhang
Quantum 10 [2026]

Baroni, Vu, Bourdoncle, Diamanti, Markham, Šupić
Quantum 9 [2025]

Mehta, Paddock, Woollerton
TQC [2025]

SUCCINCT ARGUMENT FOR QMA

COMMUNICATION
AND VERIFIER'S TIME
ARE *polylog* IN THE
SIZE OF
COMPUTATION

SOUND AGAINST
COMPUTATIONALLY
BOUNDED PROVERS

QUANTUM NPA

CLAIM: THIS
HAMILTONIAN HAS A
LOW-ENERGY GROUND
STATE
WITNESS: QUANTUM STATE

SUCCINCT ARGUMENT FOR QMA

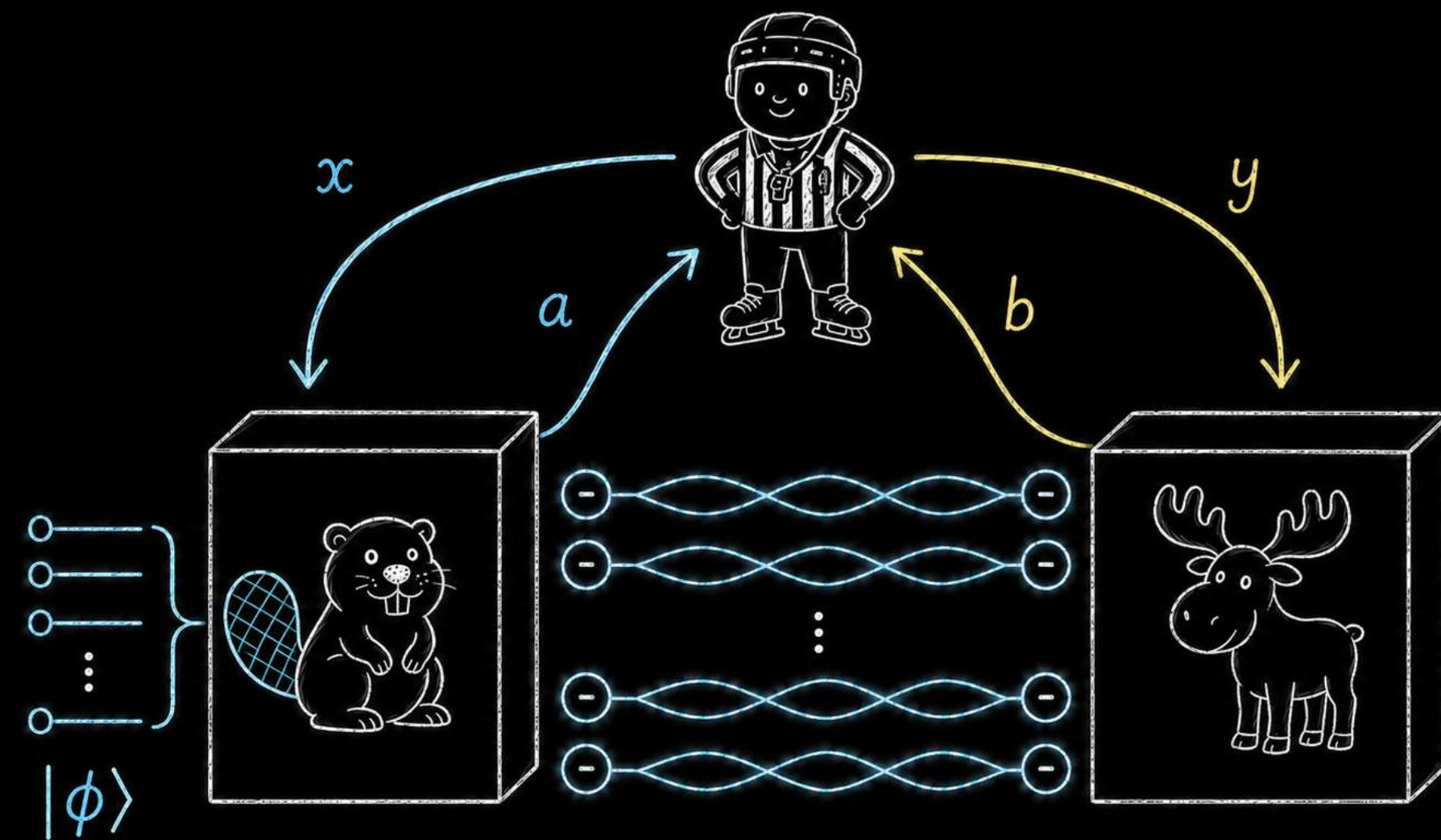
COMMUNICATION
AND VERIFIER'S TIME
ARE *polylog* IN THE
SIZE OF
COMPUTATION

SOUND AGAINST
COMPUTATIONALLY
BOUNDED PROVERS

QUANTUM NPA

CLAIM: THIS
HAMILTONIAN HAS A
LOW-ENERGY GROUND

STATE
WITNESS: QUANTUM STATE



SUCCINCT ARGUMENT FOR QMA

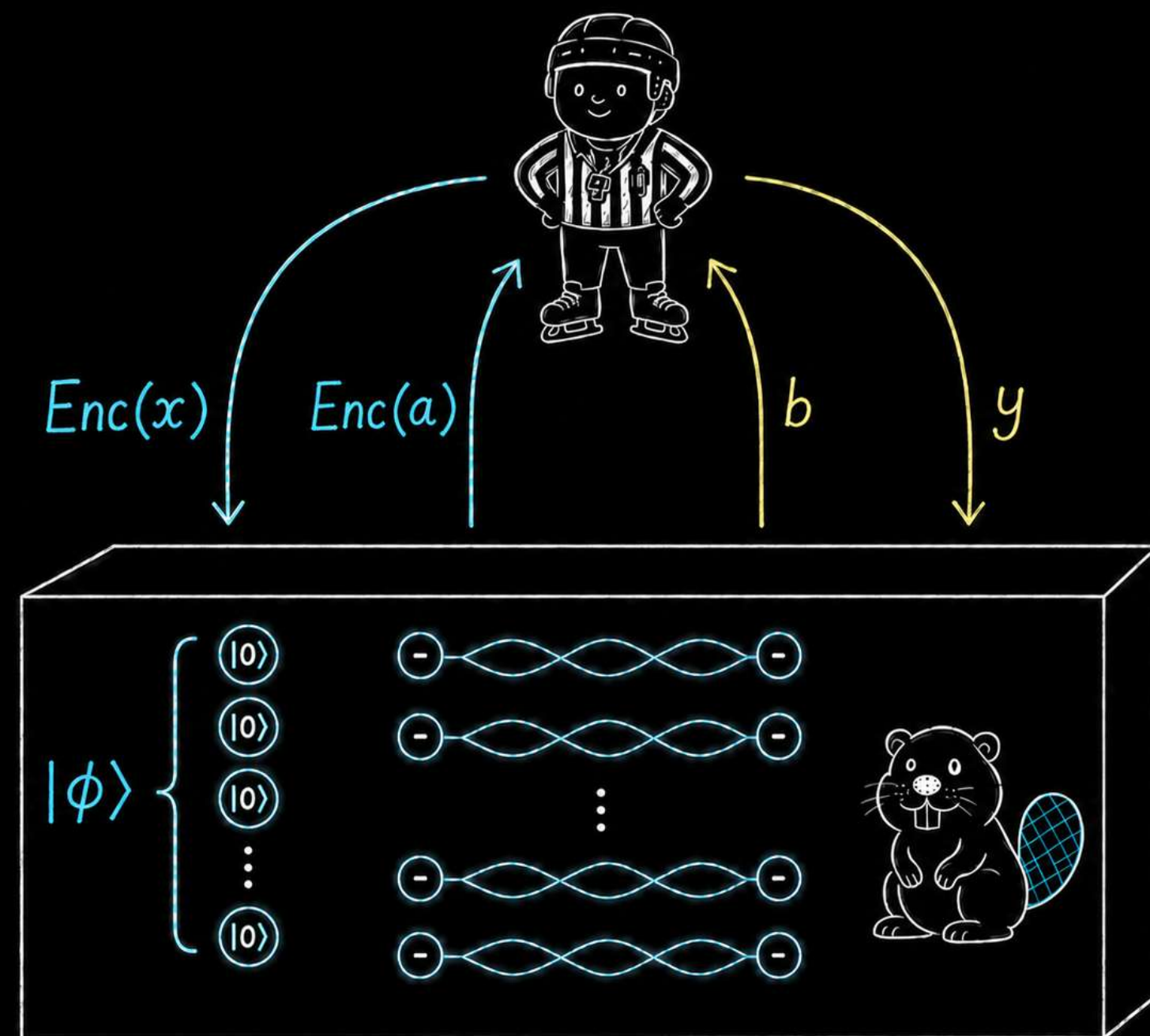
COMMUNICATION
AND VERIFIER'S TIME
ARE *polylog* IN THE
SIZE OF
COMPUTATION

SOUND AGAINST
COMPUTATIONALLY
BOUNDED PROVERS

QUANTUM NPA

CLAIM: THIS
HAMILTONIAN HAS A
LOW-ENERGY GROUND

STATE
WITNESS: QUANTUM STATE



SUCCINCT ARGUMENT FOR QMA

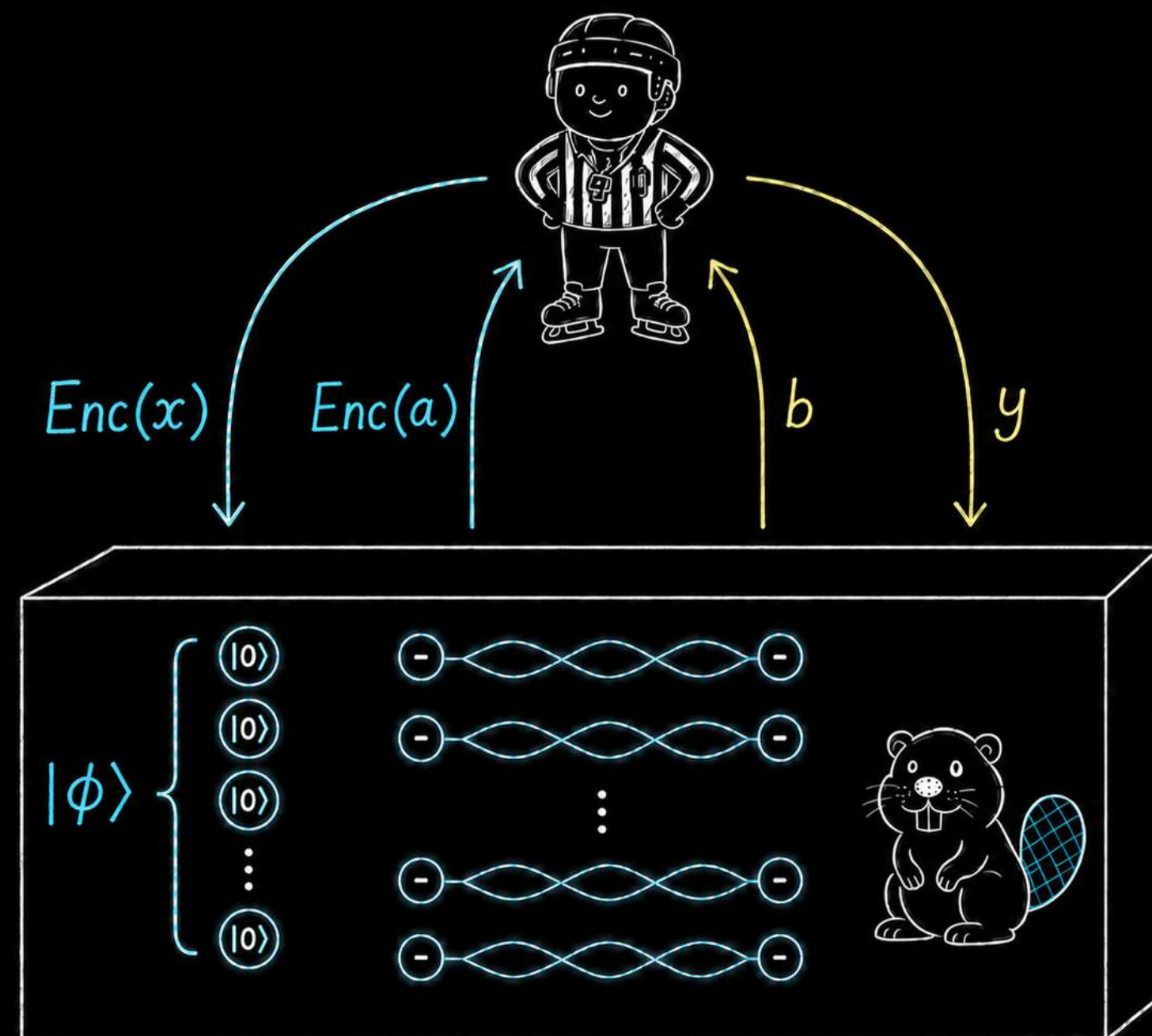
COMMUNICATION
AND VERIFIER'S TIME
ARE *polylog* IN THE
SIZE OF
COMPUTATION

SOUND AGAINST
COMPUTATIONALLY
BOUNDED PROVERS

QUANTUM NPA

CLAIM: THIS
HAMILTONIAN HAS A
LOW-ENERGY GROUND

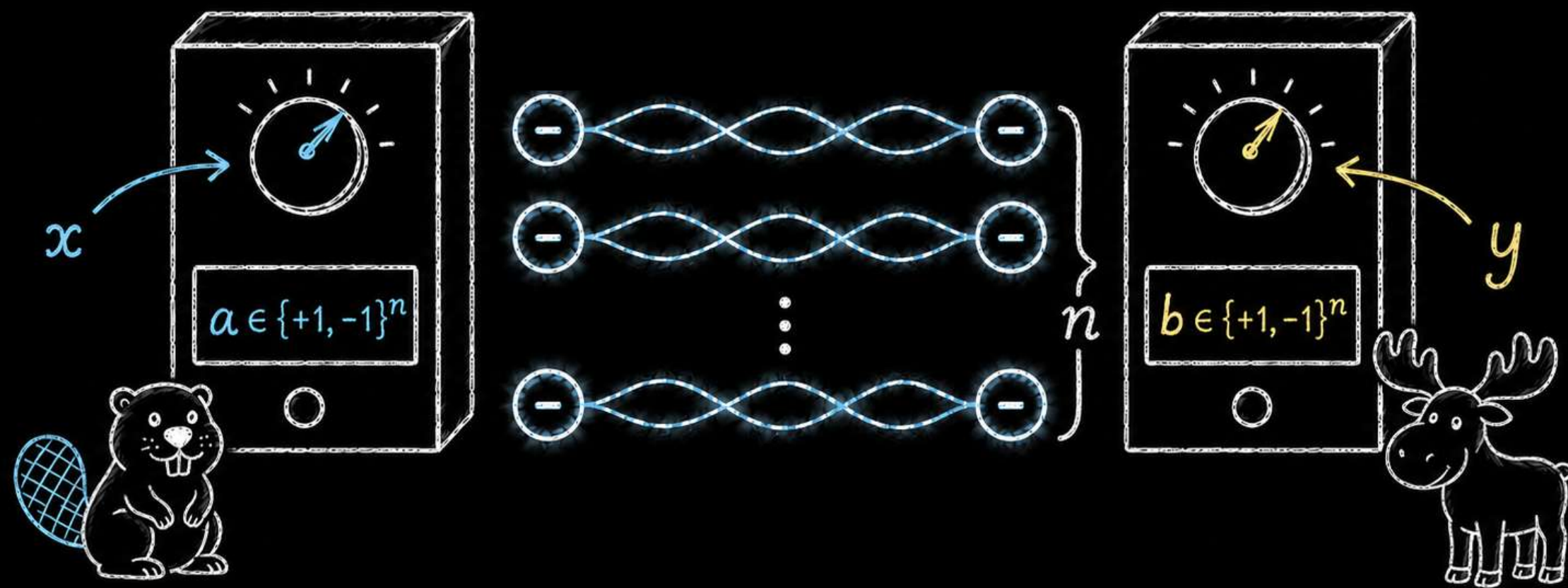
STATE
WITNESS: QUANTUM STATE



THE PROTOCOL IS SIMILAR IN STRUCTURE
TO THE ONE PROVIDING THE PROOF OF
KNOWLEDGE.

THE GAMES USED FOR SELF-TESTING ARE
COMPILED, AND RIGIDITY OF THE SECOND
ROUND OPERATIONS IS ENOUGH FOR THE
CONSTRUCTION OF THE ARGUMENT!

VERIFICATION OF COMPUTING



TESTING ROUND

SELF-TEST THE STATE AND
MEASUREMENTS THAT ALLOW
UNIVERSAL QUANTUM COMPUTING

COMPUTATION ROUND

GIVE THE PROVERS THE INPUT FOR
COMPUTATION

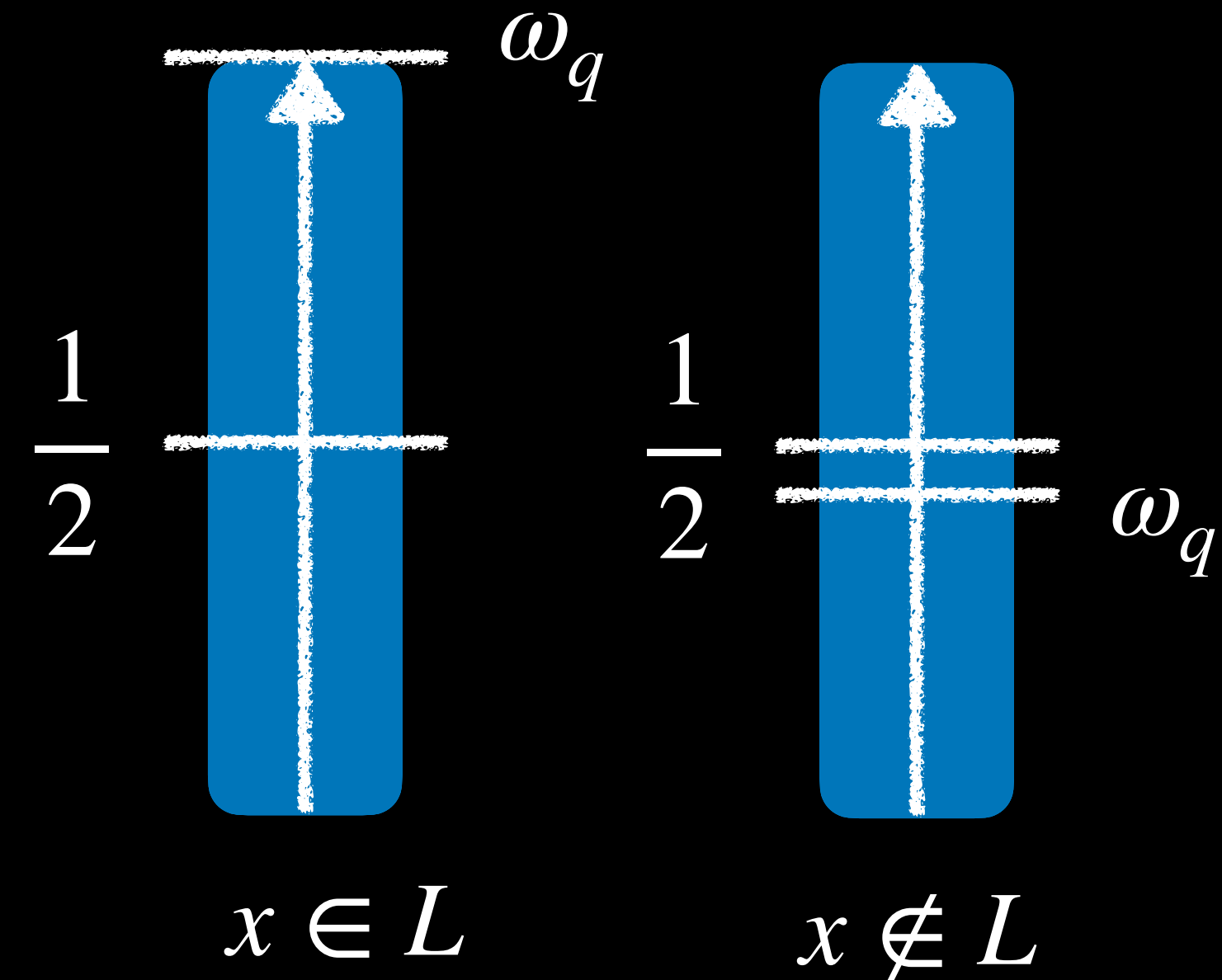
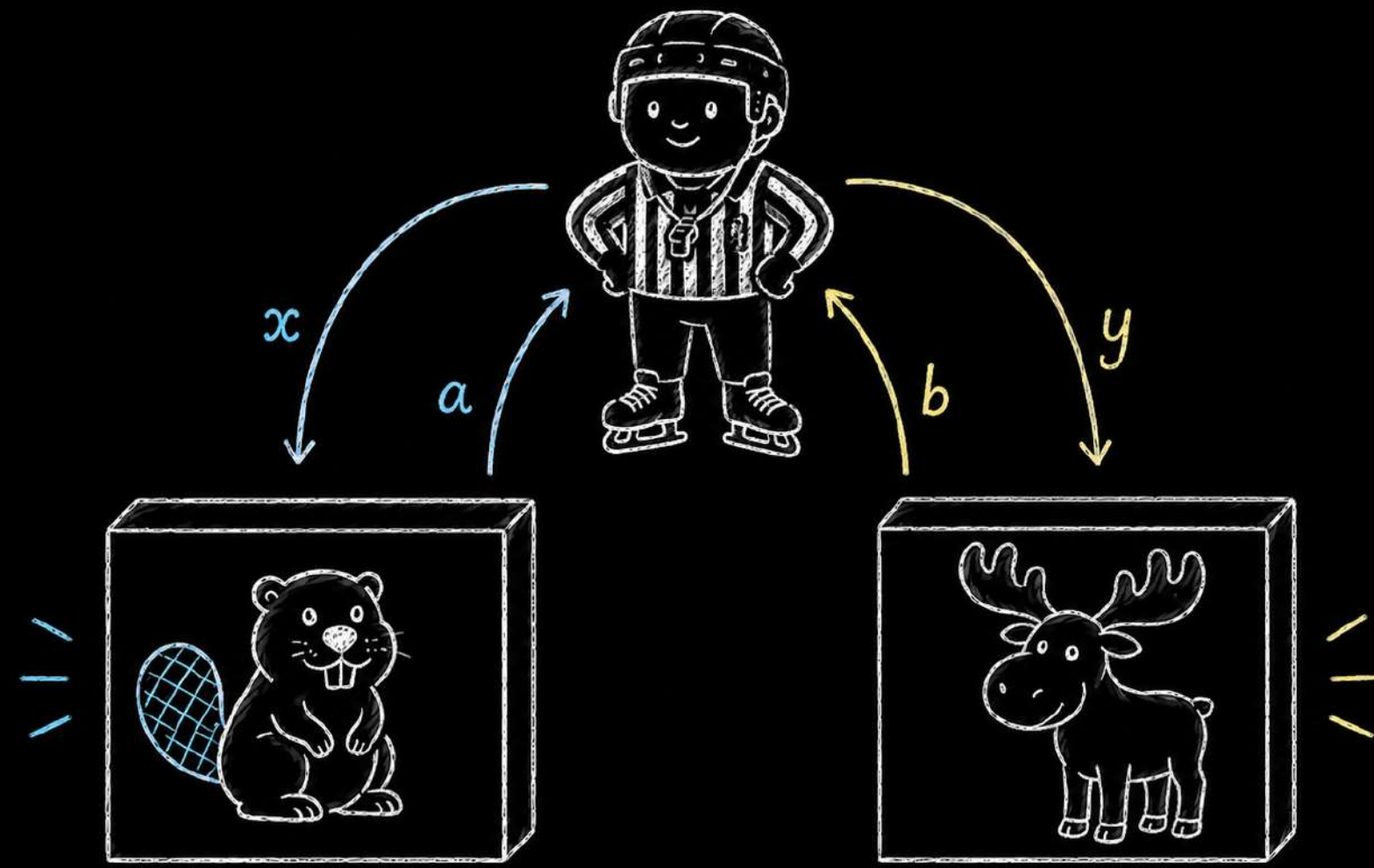
ALL THE MEASUREMENTS USED IN
COMPUTATION HAVE TO BE SELF-
TESTED !

Reichardt, Unger, Vazirani
Nature 496(7446) [2013]

Coladangelo, Grilo, Jeffery, Vidick
TACT [2019]

Broadbent, Mehta, Zhao
arXiv: 2304.03448 [2023]

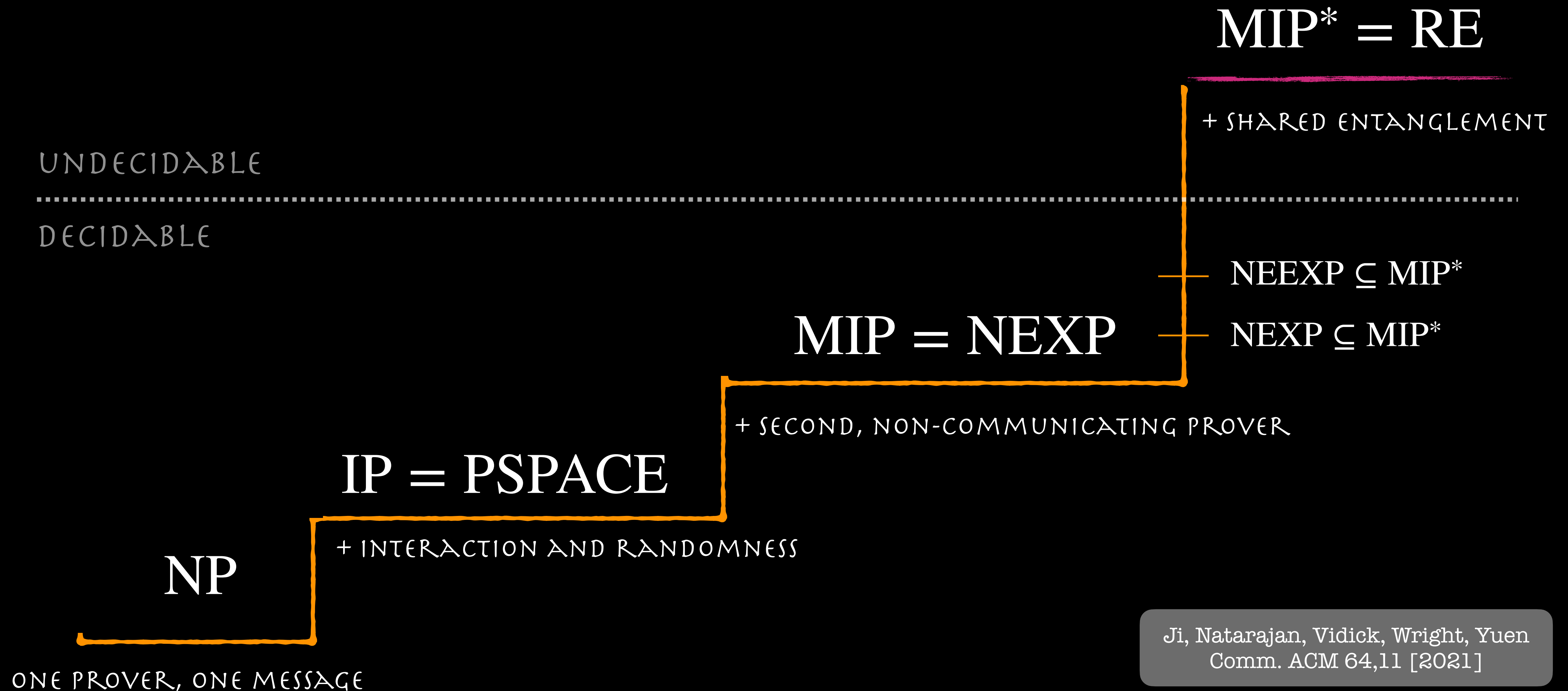
APPLICATIONS IN COMPLEXITY



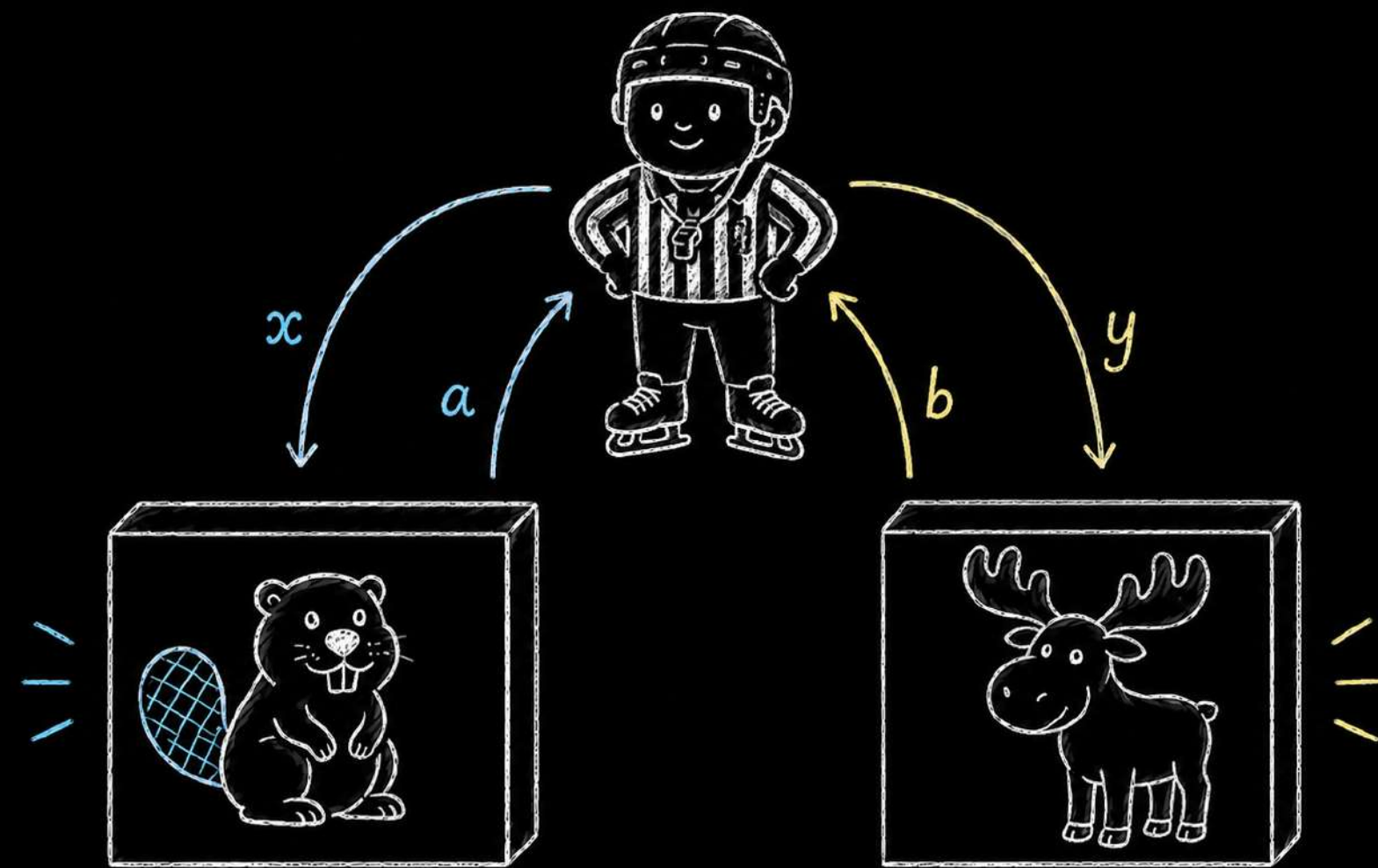
$L \in \text{MIP}^*$ IFF THERE IS A POLY-TIME MAP $x \rightarrow G_x$ WITH $\omega_q(G_x) = 1$ WHEN $x \in L$, AND $\omega_q(G_x) \leq \frac{1}{2}$ WHEN $x \notin L$.

GIVEN ANY TURING MACHINE M , YOU CAN EFFICIENTLY WRITE DOWN A NONLOCAL GAME THAT HAS A PERFECT QUANTUM STRATEGY EXACTLY WHEN M HALTS.

APPLICATIONS IN COMPLEXITY

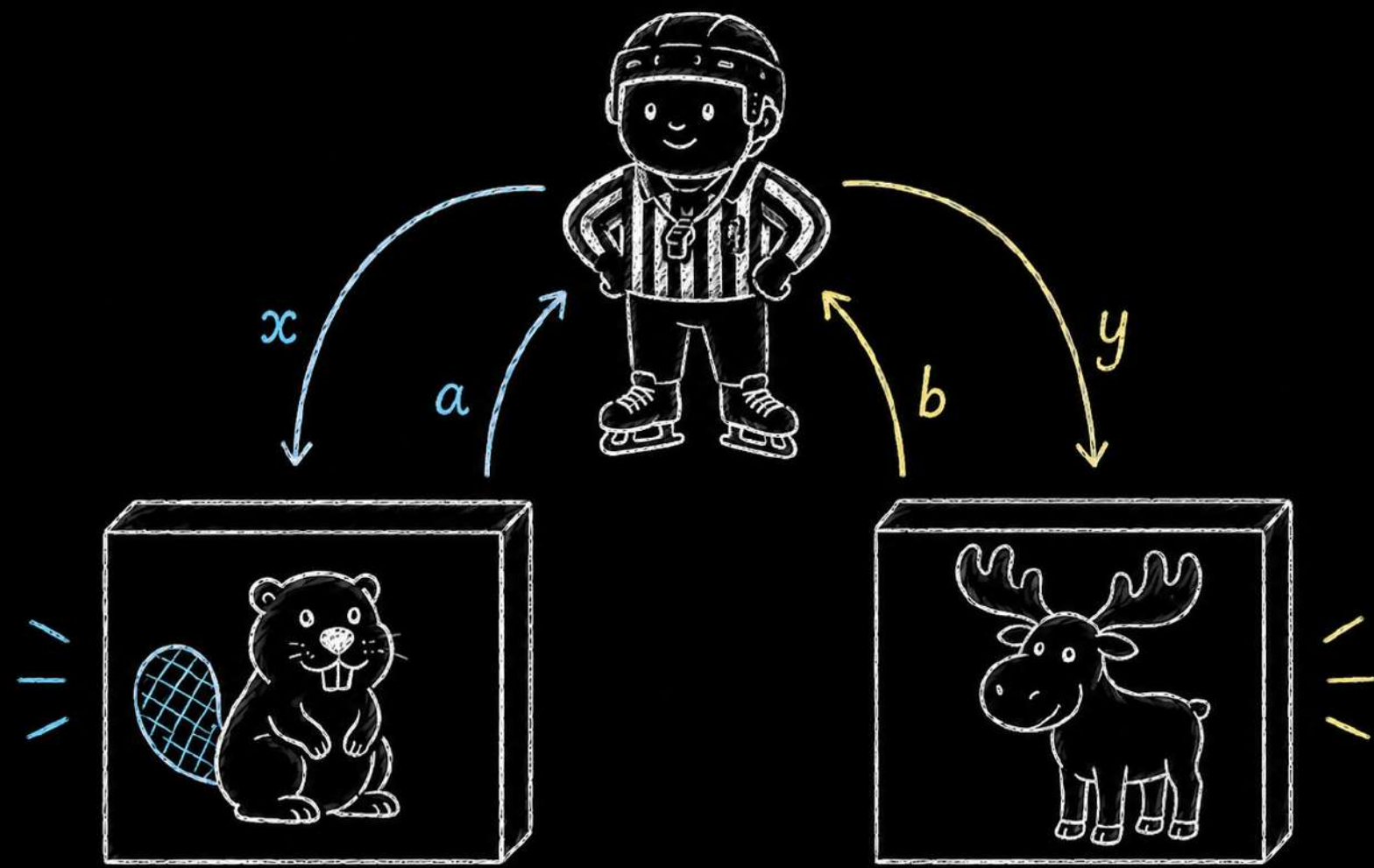


APPLICATIONS IN COMPLEXITY



PROVERS HAVE ADDITIONAL
RESOURCE: ENTANGLEMENT
WHICH COULD HELP THEM TO
CHEAT, SOUNDNESS SHOULD
BREAK?

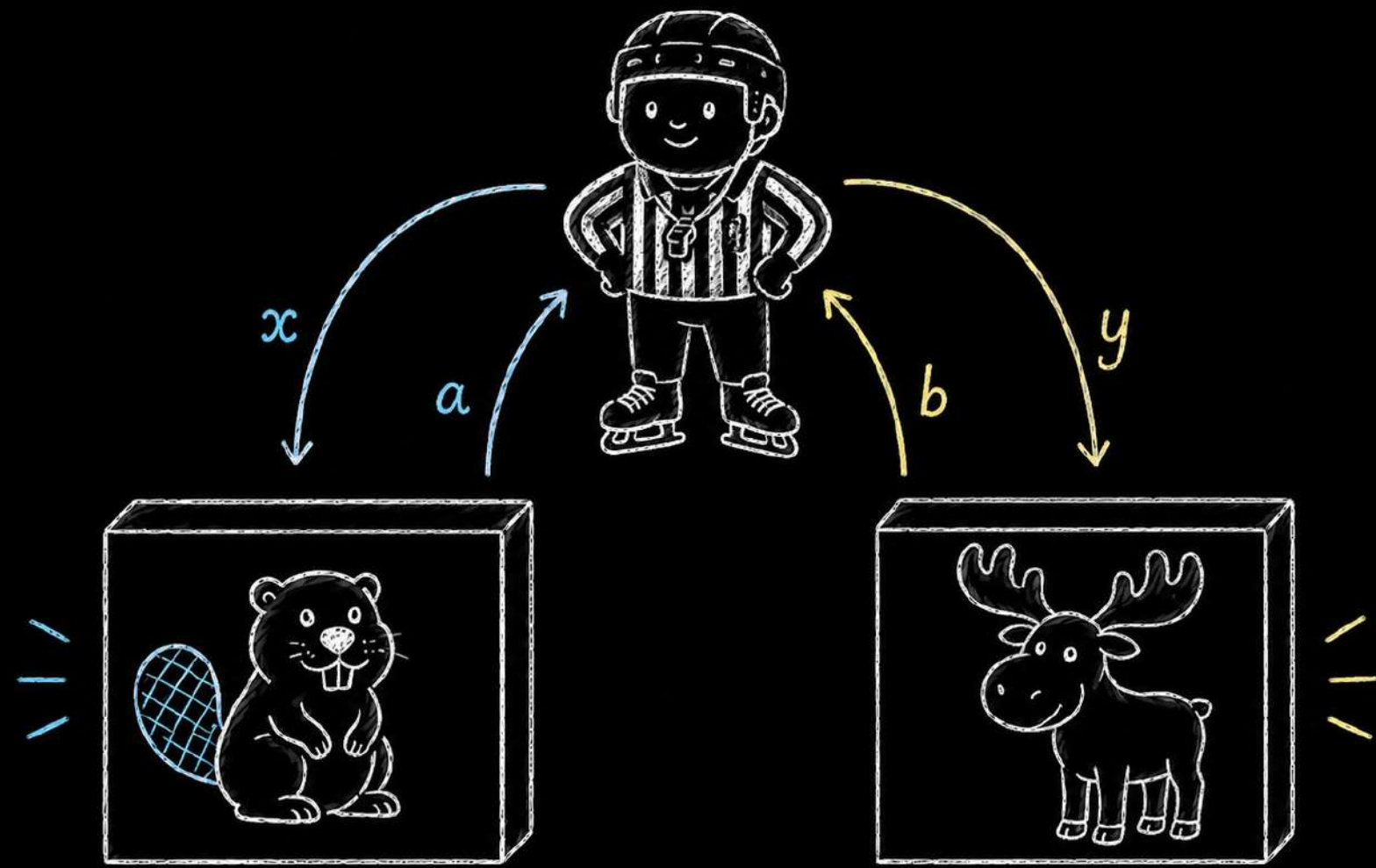
APPLICATIONS IN COMPLEXITY



1. FORCE PROVERS TO USE
ENTANGLEMENT IN A CERTAIN
WAY THAT WILL NOT ALLOW
THEM TO CHEAT!

PROVERS HAVE ADDITIONAL
RESOURCE: ENTANGLEMENT
WHICH COULD HELP THEM TO
CHEAT, SOUNDNESS SHOULD
BREAK?

APPLICATIONS IN COMPLEXITY

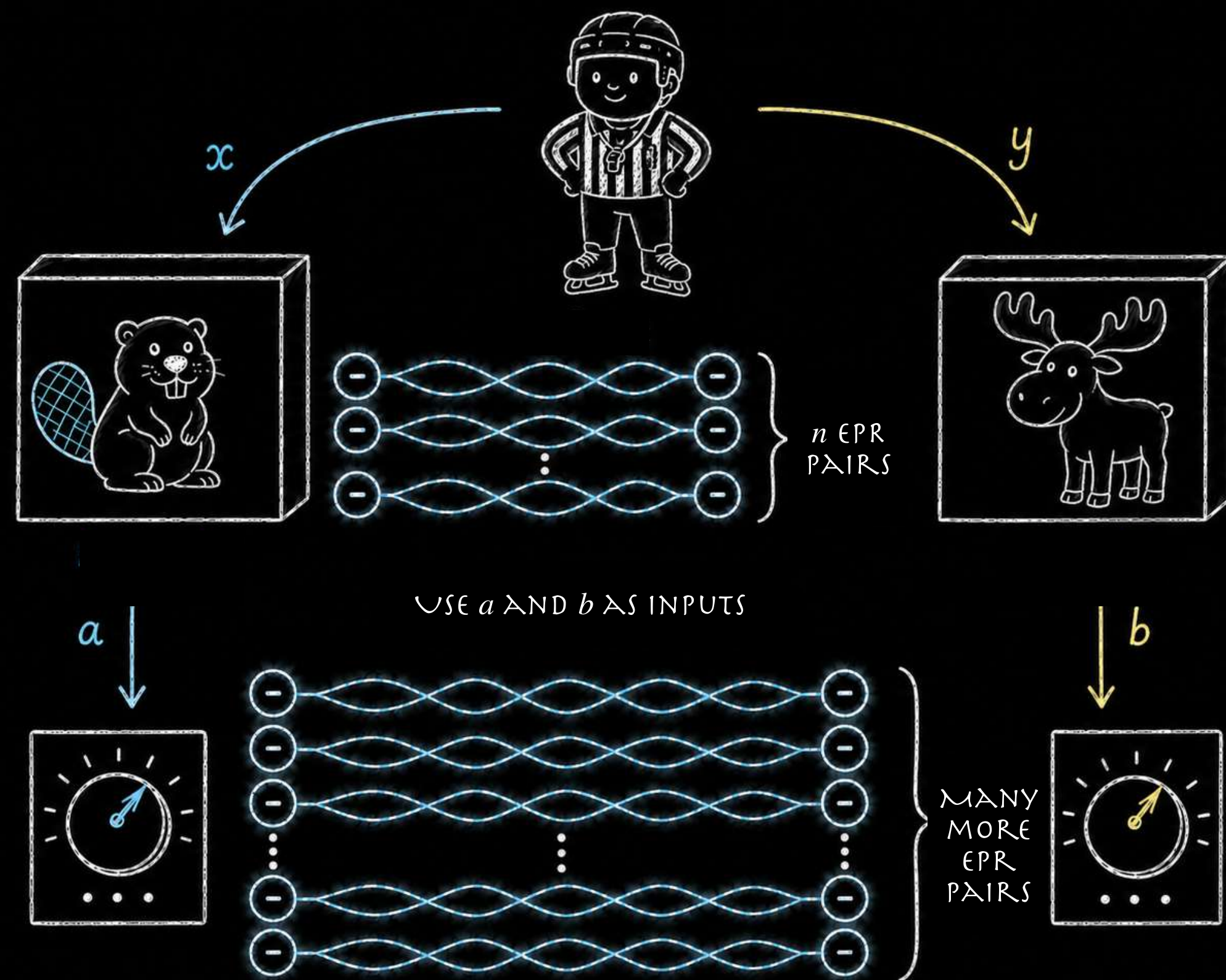


PROVERS HAVE ADDITIONAL
RESOURCE: ENTANGLEMENT
WHICH COULD HELP THEM TO
CHEAT, SOUNDNESS SHOULD
BREAK?

1. FORCE PROVERS TO USE
ENTANGLEMENT IN A CERTAIN
WAY THAT WILL NOT ALLOW
THEM TO CHEAT!

2. INPUTS FOR PROBLEMS WHOSE
SOLUTIONS VERIFIER NEEDS TO
VERIFY ARE TOO LONG, EVEN TO
JUST BE READ, PARALLEL SELF-
TESTING PROVIDES SOLUTION:
EXPONENTIALLY LARGE SYSTEM
CAN BE VERIFIED WITH "SHORT
INPUTS"

APPLICATIONS IN COMPLEXITY



INTROSPECTION

PROVERS ARE DOING THE
VERIFIER'S JOB, THEY ARE
SAMPLING A CORRECT INPUT
DISTRIBUTION BY THEMSELVES!

THEY DO NOT KNOW EACH
OTHER'S INPUTS BECAUSE THEY
MEASURE IN THE
COMPLEMENTARY BASES.

★ ACT III : MAIN TECHNIQUES

CHSH RIGIDITY: SUMMERS & WERNER

- a_0 and a_1 self-adjoint elements of Alice's C^* algebra
- b_0 and b_1 self-adjoint elements of Bob's C^* algebra
- They commute (no tensor product a priori)

- A state σ just assigns expectation value to

$$\chi = \frac{1}{2} (a_0(b_0 + b_1) + a_1(b_0 - b_1))$$

- GNS representation gives us a Hilbert space, and a unit vector inside it $|\Omega\rangle$, and representations of self-adjoint elements: A_0, A_1, B_0, B_1

$$A = \frac{1}{2} (A_0 + iA_1),$$

$$B = \frac{1}{2\sqrt{2}} (B_0 + B_1 + i(B_0 - B_1))$$

$$AA^\dagger + A^\dagger A = \frac{1}{2} (A_0^2 + A_1^2) \leq 1,$$

$$BB^\dagger + B^\dagger B = \frac{1}{2} (B_0^2 + B_1^2) \leq 1$$

CHSH RIGIDITY: SUMMERS & WERNER

- $\sqrt{2}\sigma(\chi) = 4\text{Re}\langle\Omega|A^\dagger B|\Omega\rangle$
- Since quantum value is $2\sqrt{2}$, and norm of $A|\Omega\rangle$ and $B|\Omega\rangle$ are at most 1, it must be $A|\Omega\rangle = B|\Omega\rangle$, and A_i and B_i are sharp observables
- Since A_i and B_j commute we have $AA|\Omega\rangle = BB|\Omega\rangle$

- This reduces to $(A_0A_1 + A_1A_0)|\Omega\rangle = (B_0^2 - B_1^2)|\Omega\rangle$
- As B_0 and B_1 are sharp, A_0 and A_1 anticommute on the support of the state
- Symmetrical analysis shows that Bob's observables also anti-commute on the support of the state.

CHSH RIGIDITY: TSIRELSON

- Given
 $[A_k, B_l] = 0$, $\|A_k\|$, $\|B_l\| \leq 1$
 , density matrix W ,
 $c_{kl} = \text{Tr}(A_k B_l W)$,
 $\beta = c_{00} + c_{01} + c_{10} - c_{11}$
- Vectorise:
 $\langle X, Y \rangle_W = \text{Re Tr}(Y^* X W)$: the
 observables become vectors,
 $\|A_k\|_W, \|B_l\|_W \leq 1$,
 $\langle A_k, B_l \rangle_W = c_{kl}$

- Bound=geometry:
 $\beta = \langle A_0, B_0 + B_1 \rangle + \langle A_1, B_0 - B_1 \rangle \leq$
 $\leq \sqrt{2}(\|B_0 + B_1\|^2 + \|B_0 - B_1\|^2)^{1/2}$
 $\beta \leq \sqrt{2}(2\|B_0\|^2 + 2\|B_1\|^2)^{1/2} \leq 2\sqrt{2}$,
 Cauchy-Schwarz + parallelogram
 inequalities
- Saturation gives rigid geometry:
 $\beta = 2\sqrt{2}$ forces two orthonormalisation
 frames at 45 degrees: $A_k^2 W = W$,
 $\sqrt{2}A_1 W = (B_0 + B_1)W, \dots$,
 $\{A_0, A_1\}W = 0$, $\{B_0, B_1\}W = 0$

CHSH RIGIDITY: TSIRELSON

- From non degeneracy to operator inequalities: B -monomials on $\text{ran } W$ span $\mathcal{H}$, so $A_k^2 = \mathbb{I}$, $B_l^2 = \mathbb{I}$, $\{A_0, A_1\} = 0$, $\{B_0, B_1\} = 0$, this is a representation of two Clifford algebras
- Representation theory: two anticommuting involutions are unitarily equivalent to $\sigma_z \otimes \mathbb{I}$ and $\sigma_x \otimes \mathbb{I}$, and Hilbert space is isomorphic to $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{R}$

- State: the top eigenvalue of $\sqrt{2}(\sigma_z \otimes \sigma_z + \sigma_x \otimes \sigma_x) \otimes \mathbb{I}$ is $2\sqrt{2}$ and the corresponding eigenvector is $|\Phi_+\rangle$

CHSH RIGIDITY: SOS DECOMPOSITIONS

- Shifted Bell operator

$$4\mathbb{I} - \sqrt{2}(A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1) \\ = \left(A_0 - \frac{B_0 + B_1}{\sqrt{2}}\right)^2 + \left(A_1 - \frac{B_0 - B_1}{\sqrt{2}}\right)^2$$

- $4 - \sqrt{2}\beta = \langle\psi|\left(A_0 - \frac{B_0 + B_1}{\sqrt{2}}\right)^2|\psi\rangle + \langle\psi|\left(A_1 - \frac{B_0 - B_1}{\sqrt{2}}\right)^2|\psi\rangle$

- For a state $|\psi\rangle$ reaching the maximal violation we thus have

$$\left(A_0 - \frac{B_0 + B_1}{\sqrt{2}}\right)|\psi\rangle = 0, \quad \left(A_1 - \frac{B_0 - B_1}{\sqrt{2}}\right)|\psi\rangle = 0$$

- $A_0|\psi\rangle = \frac{B_0 + B_1}{\sqrt{2}}|\psi\rangle, \quad A_1|\psi\rangle = \frac{B_0 - B_1}{\sqrt{2}}|\psi\rangle$

- $(A_0A_1 + A_1A_0)|\psi\rangle = 0$

- $(B_0B_1 + B_1B_0)|\psi\rangle = 0$

CHSH RIGIDITY: SWAP ISOMETRY

$$(A_0A_1 + A_1A_0)|\psi\rangle = 0$$

$$(B_0B_1 + B_1B_0)|\psi\rangle = 0$$

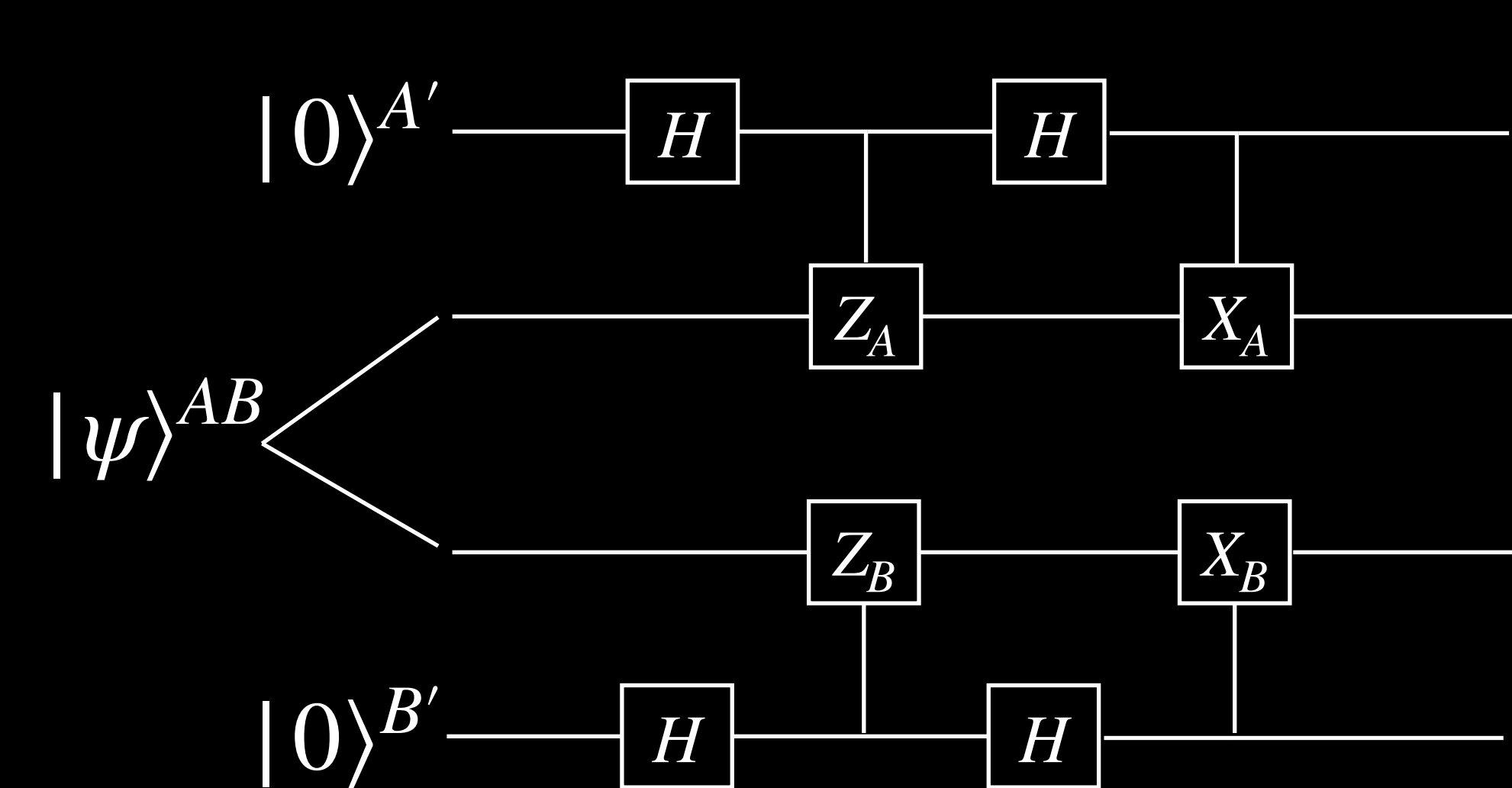
$$A_0|\psi\rangle = \frac{B_0 + B_1}{\sqrt{2}}|\psi\rangle, \quad A_1|\psi\rangle = \frac{B_0 - B_1}{\sqrt{2}}|\psi\rangle$$

$$Z_A = A_0, \quad X_A = A_1$$

$$Z_B = \frac{B_0 + B_1}{\sqrt{2}}, \quad X_B = \frac{B_0 - B_1}{\sqrt{2}}$$

$$Z_A|\psi\rangle = Z_B|\psi\rangle, \quad X_A|\psi\rangle = X_B|\psi\rangle$$

Directly construct the SWAP isometry



$$\begin{aligned}
 4\text{SWAP}(|00\rangle^{A'B'}|\psi\rangle^{AB}) &= |00\rangle^{A'B'}(\mathbb{I} + Z_A)(\mathbb{I} + Z_B)|\psi\rangle^{AB} \\
 &+ |10\rangle^{A'B'}X_A(\mathbb{I} - Z_A)(\mathbb{I} + Z_B)|\psi\rangle^{AB} \\
 &+ |01\rangle^{A'B'}(\mathbb{I} + Z_A)X_B(\mathbb{I} - Z_B)|\psi\rangle^{AB} \\
 &+ |11\rangle^{A'B'}X_A(\mathbb{I} - Z_A)X_B(\mathbb{I} - Z_B)|\psi\rangle^{AB}
 \end{aligned}$$

CHSH RIGIDITY: SWAP ISOMETRY

$$(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi\rangle = (\mathbb{I} + Z_A)(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A = A_0, \quad X_A = A_1$$

$$(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) |\psi\rangle = 2(\mathbb{I} + Z_A) |\psi\rangle$$

$$Z_B = \frac{B_0 + B_1}{\sqrt{2}}, \quad X_B = \frac{B_0 - B_1}{\sqrt{2}}$$

$$(\mathbb{I} - Z_A)(\mathbb{I} - Z_B) |\psi\rangle = 2(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A |\psi\rangle = Z_B |\psi\rangle, \quad X_A |\psi\rangle = X_B |\psi\rangle$$

Directly construct the SWAP isometry

$$\begin{aligned}
 4\text{SWAP}(|00\rangle^{A'B'} |\psi\rangle^{AB}) &= 2|00\rangle^{A'B'} (\mathbb{I} + Z_A) |\psi\rangle^{AB} \\
 &\quad + 0 \\
 &\quad + 0 \\
 &\quad + 2|11\rangle^{A'B'} X_A X_B (\mathbb{I} - Z_A) |\psi\rangle^{AB}
 \end{aligned}$$

CHSH RIGIDITY: SWAP ISOMETRY

$$(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi\rangle = (\mathbb{I} + Z_A)(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A = A_0, \quad X_A = A_1$$

$$(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) |\psi\rangle = 2(\mathbb{I} + Z_A) |\psi\rangle$$

$$Z_B = \frac{B_0 + B_1}{\sqrt{2}}, \quad X_B = \frac{B_0 - B_1}{\sqrt{2}}$$

$$(\mathbb{I} - Z_A)(\mathbb{I} - Z_B) |\psi\rangle = 2(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A |\psi\rangle = Z_B |\psi\rangle, \quad X_A |\psi\rangle = X_B |\psi\rangle$$

Directly construct the SWAP isometry

$$\begin{aligned}
 4\text{SWAP}(|00\rangle^{A'B'} |\psi\rangle^{AB}) &= 2|00\rangle^{A'B'} (\mathbb{I} + Z_A) |\psi\rangle^{AB} \\
 &\quad + 0 \\
 &\quad + 0 \\
 &\quad + 2|11\rangle^{A'B'} X_A (\mathbb{I} - Z_A) X_A |\psi\rangle^{AB}
 \end{aligned}$$

CHSH RIGIDITY: SWAP ISOMETRY

$$(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi\rangle = (\mathbb{I} + Z_A)(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A = A_0, \quad X_A = A_1$$

$$(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) |\psi\rangle = 2(\mathbb{I} + Z_A) |\psi\rangle$$

$$Z_B = \frac{B_0 + B_1}{\sqrt{2}}, \quad X_B = \frac{B_0 - B_1}{\sqrt{2}}$$

$$(\mathbb{I} - Z_A)(\mathbb{I} - Z_B) |\psi\rangle = 2(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A |\psi\rangle = Z_B |\psi\rangle, \quad X_A |\psi\rangle = X_B |\psi\rangle$$

Directly construct the SWAP isometry

$$\begin{aligned}
 4\text{SWAP}(|00\rangle^{A'B'} |\psi\rangle^{AB}) &= 2|00\rangle^{A'B'} (\mathbb{I} + Z_A) |\psi\rangle^{AB} \\
 &\quad + 0 \\
 &\quad + 0 \\
 &\quad + 2|11\rangle^{A'B'} (\mathbb{I} + Z_A) X_A X_A |\psi\rangle^{AB}
 \end{aligned}$$

CHSH RIGIDITY: SWAP ISOMETRY

$$(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi\rangle = (\mathbb{I} + Z_A)(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A = A_0, \quad X_A = A_1$$

$$(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) |\psi\rangle = 2(\mathbb{I} + Z_A) |\psi\rangle$$

$$Z_B = \frac{B_0 + B_1}{\sqrt{2}}, \quad X_B = \frac{B_0 - B_1}{\sqrt{2}}$$

$$(\mathbb{I} - Z_A)(\mathbb{I} - Z_B) |\psi\rangle = 2(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A |\psi\rangle = Z_B |\psi\rangle, \quad X_A |\psi\rangle = X_B |\psi\rangle$$

Directly construct the SWAP isometry

$$\begin{aligned}
 4\text{SWAP}(|00\rangle^{A'B'} |\psi\rangle^{AB}) &= 2|00\rangle^{A'B'} (\mathbb{I} + Z_A) |\psi\rangle^{AB} \\
 &\quad + 0 \\
 &\quad + 0 \\
 &\quad + 2|11\rangle^{A'B'} (\mathbb{I} + Z_A) |\psi\rangle^{AB}
 \end{aligned}$$

CHSH RIGIDITY: SWAP ISOMETRY

$$(\mathbb{I} + Z_A)(\mathbb{I} - Z_B) |\psi\rangle = (\mathbb{I} + Z_A)(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A = A_0, \quad X_A = A_1$$

$$(\mathbb{I} + Z_A)(\mathbb{I} + Z_B) |\psi\rangle = 2(\mathbb{I} + Z_A) |\psi\rangle$$

$$Z_B = \frac{B_0 + B_1}{\sqrt{2}}, \quad X_B = \frac{B_0 - B_1}{\sqrt{2}}$$

$$(\mathbb{I} - Z_A)(\mathbb{I} - Z_B) |\psi\rangle = 2(\mathbb{I} - Z_A) |\psi\rangle$$

$$Z_A |\psi\rangle = Z_B |\psi\rangle, \quad X_A |\psi\rangle = X_B |\psi\rangle$$

Directly construct the SWAP isometry

$$\begin{aligned}
 & |0\rangle^{A'} \text{---} [H] \text{---} [H] \text{---} \text{---} SWAP(|00\rangle^{A'B'} |\psi\rangle^{AB}) = \frac{|00\rangle^{A'B'} + |11\rangle^{A'B'}}{\sqrt{2}} \otimes \frac{\mathbb{I} + Z_A}{\sqrt{2}} |\psi\rangle^{AB} \\
 & \begin{array}{c} | \psi \rangle^{AB} \\ \swarrow \quad \searrow \end{array} \begin{array}{c} \text{---} [Z_A] \text{---} [X_A] \text{---} \\ \text{---} [Z_B] \text{---} [X_B] \text{---} \end{array} \\
 & |0\rangle^{B'} \text{---} [H] \text{---} [H] \text{---} \\
 & = |\text{EPR}\rangle^{AB} \otimes |\text{aux}\rangle^{A'B'}
 \end{aligned}$$

CHSH RIGIDITY: JORDAN'S LEMMA

$$VA_0V^\dagger = \begin{bmatrix} \blacksquare & & & & \\ & \blacksquare & & & \\ & & \blacksquare & & \\ & & & \blacksquare & \\ & & & & \blacksquare \end{bmatrix}$$

$$VA_1V^\dagger = \begin{bmatrix} \blacksquare & & & & \\ & \blacksquare & & & \\ & & \blacksquare & & \\ & & & \blacksquare & \\ & & & & \blacksquare \end{bmatrix}$$

A few steps and we get result: For any two anti-commuting observables X and Z there is a unitary U such that

$$UZU^\dagger = \sigma_z \otimes \mathbb{I}, \quad UXU^\dagger = \sigma_x \otimes \mathbb{I}$$

Applying to Alice's and Bob's observables we thus obtain

$$\begin{aligned} UA_0U^\dagger &= \sigma_z \otimes \mathbb{I} & UA_1U^\dagger &= \sigma_x \otimes \mathbb{I} \\ UB_0U^\dagger &= \frac{\sigma_z + \sigma_x}{\sqrt{2}} \otimes \mathbb{I} & UB_1U^\dagger &= \frac{\sigma_z - \sigma_x}{\sqrt{2}} \otimes \mathbb{I}. \end{aligned}$$

So the Bell operator then is

$\sqrt{2}(\sigma_z \otimes \sigma_z + \sigma_x \otimes \sigma_x) \otimes \mathbb{I} \otimes \mathbb{I}$ and the eigenstate corresponding to the largest eigenvalue ($2\sqrt{2}$) is the EPR pair

MAYERS-YAO SELF-TEST

- Mayers-Yao:

$$\langle \psi | A_0 B_0 | \psi \rangle = 1, \quad \langle \psi | A_0 B_1 | \psi \rangle = 0, \quad \langle \psi | A_0 B_2 | \psi \rangle = 1/\sqrt{2},$$
$$\langle \psi | A_1 B_0 | \psi \rangle = 0, \quad \langle \psi | A_1 B_1 | \psi \rangle = 1, \quad \langle \psi | A_1 B_2 | \psi \rangle = 1/\sqrt{2},$$

$$\vec{a}_k = A_k |\psi\rangle, \quad \vec{b}_l = B_l |\psi\rangle,$$

$$\langle \vec{a}_0, \vec{b}_0 \rangle = 1, \quad \langle \vec{a}_1, \vec{b}_1 \rangle = 1, \quad \langle \vec{a}_0, \vec{b}_1 \rangle = 0, \quad \langle \vec{a}_1, \vec{b}_0 \rangle = 0$$

$$\langle \vec{a}_0, \vec{b}_2 \rangle = \langle \vec{a}_1, \vec{b}_2 \rangle = \frac{1}{\sqrt{2}}$$

MAYERS-YAO SELF-TEST

- Mayers-Yao:

$$\begin{aligned}\langle \psi | A_0 B_0 | \psi \rangle &= 1, & \langle \psi | A_0 B_1 | \psi \rangle &= 0, & \langle \psi | A_0 B_2 | \psi \rangle &= 1/\sqrt{2}, \\ \langle \psi | A_1 B_0 | \psi \rangle &= 0, & \langle \psi | A_1 B_1 | \psi \rangle &= 1, & \langle \psi | A_1 B_2 | \psi \rangle &= 1/\sqrt{2},\end{aligned}$$

$$\vec{a}_k = A_k |\psi\rangle, \quad \vec{b}_l = B_l |\psi\rangle,$$

$$\langle \vec{a}_0, \vec{b}_0 \rangle = 1, \quad \langle \vec{a}_1, \vec{b}_1 \rangle = 1, \quad \langle \vec{a}_0, \vec{b}_1 \rangle = 0, \quad \langle \vec{a}_1, \vec{b}_0 \rangle = 0$$

$$\langle \vec{a}_0, \vec{b}_2 \rangle = \langle \vec{a}_1, \vec{b}_2 \rangle = \frac{1}{\sqrt{2}}$$

$$\vec{a}_0 = \vec{b}_0$$



MAYERS-YAO SELF-TEST

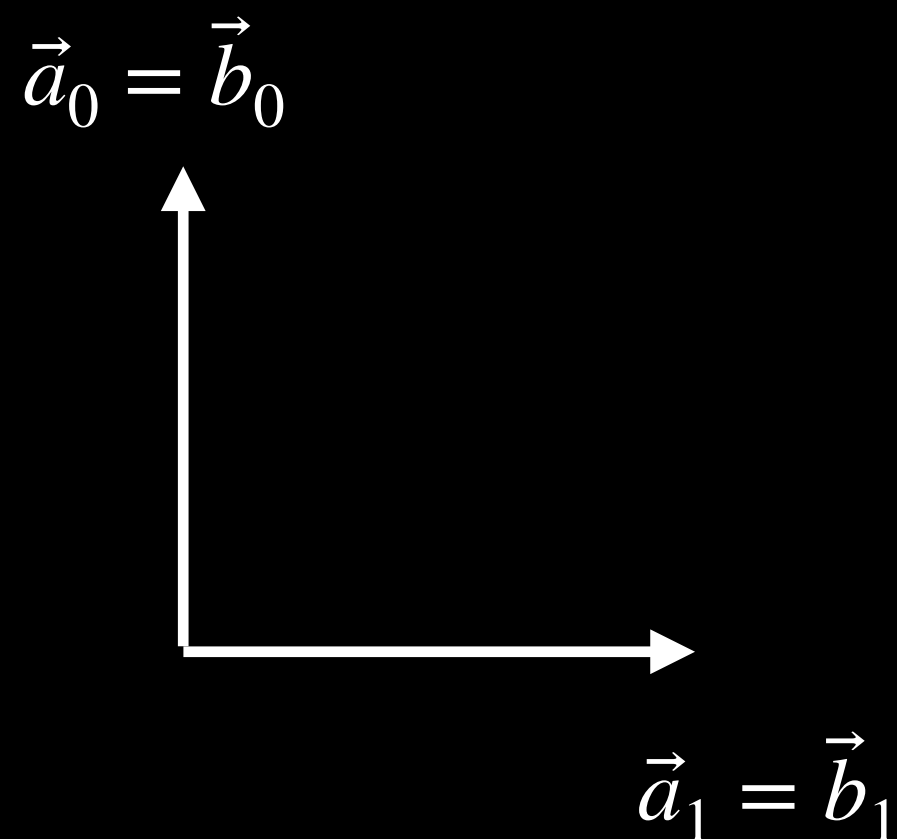
- Mayers-Yao:

$$\begin{aligned}\langle \psi | A_0 B_0 | \psi \rangle &= 1, & \langle \psi | A_0 B_1 | \psi \rangle &= 0, & \langle \psi | A_0 B_2 | \psi \rangle &= 1/\sqrt{2}, \\ \langle \psi | A_1 B_0 | \psi \rangle &= 0, & \langle \psi | A_1 B_1 | \psi \rangle &= 1, & \langle \psi | A_1 B_2 | \psi \rangle &= 1/\sqrt{2},\end{aligned}$$

$$\vec{a}_k = A_k |\psi\rangle, \quad \vec{b}_l = B_l |\psi\rangle,$$

$$\langle \vec{a}_0, \vec{b}_0 \rangle = 1, \quad \langle \vec{a}_1, \vec{b}_1 \rangle = 1, \quad \langle \vec{a}_0, \vec{b}_1 \rangle = 0, \quad \langle \vec{a}_1, \vec{b}_0 \rangle = 0$$

$$\langle \vec{a}_0, \vec{b}_2 \rangle = \langle \vec{a}_1, \vec{b}_2 \rangle = \frac{1}{\sqrt{2}}$$



MAYERS-YAO SELF-TEST

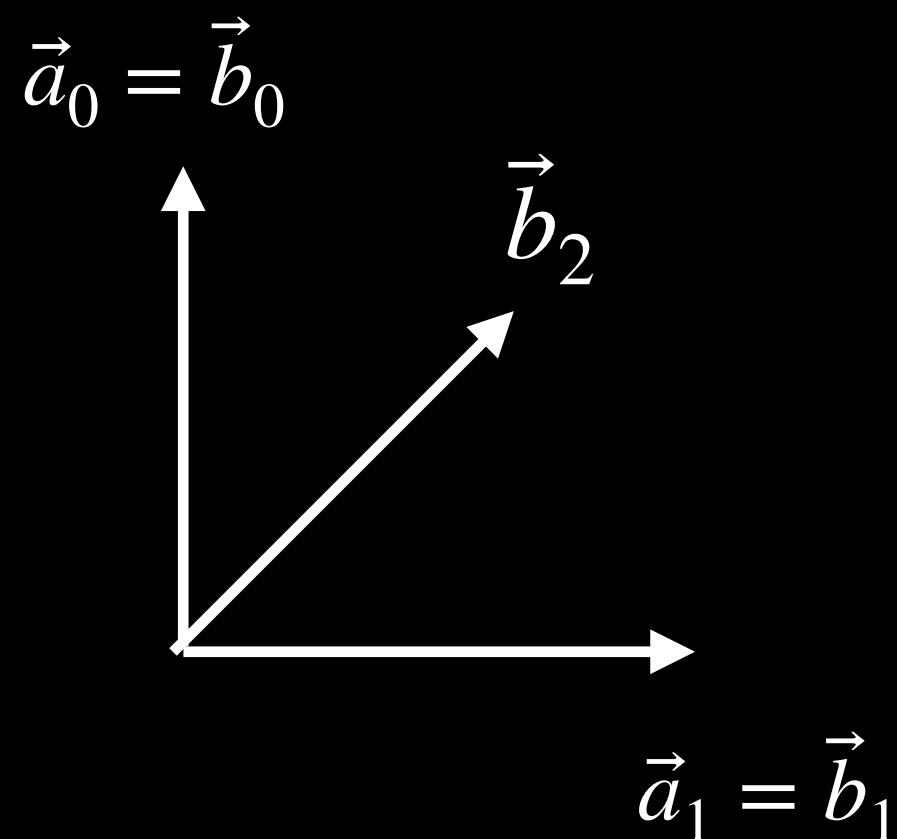
- Mayers-Yao:

$$\langle \psi | A_0 B_0 | \psi \rangle = 1, \quad \langle \psi | A_0 B_1 | \psi \rangle = 0, \quad \langle \psi | A_0 B_2 | \psi \rangle = 1/\sqrt{2},$$
$$\langle \psi | A_1 B_0 | \psi \rangle = 0, \quad \langle \psi | A_1 B_1 | \psi \rangle = 1, \quad \langle \psi | A_1 B_2 | \psi \rangle = 1/\sqrt{2},$$

$$\vec{a}_k = A_k |\psi\rangle, \quad \vec{b}_l = B_l |\psi\rangle,$$

$$\langle \vec{a}_0, \vec{b}_0 \rangle = 1, \quad \langle \vec{a}_1, \vec{b}_1 \rangle = 1, \quad \langle \vec{a}_0, \vec{b}_1 \rangle = 0, \quad \langle \vec{a}_1, \vec{b}_0 \rangle = 0$$

$$\langle \vec{a}_0, \vec{b}_2 \rangle = \langle \vec{a}_1, \vec{b}_2 \rangle = \frac{1}{\sqrt{2}}$$



MAYERS-YAO SELF-TEST

- Mayers-Yao:

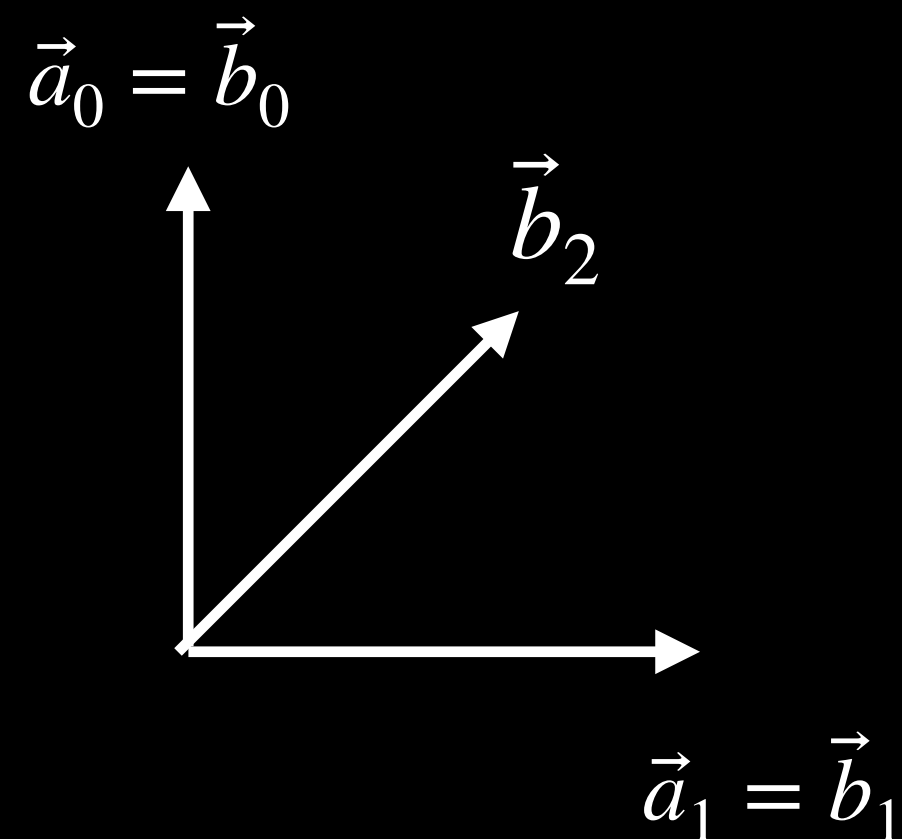
$$\langle \psi | A_0 B_0 | \psi \rangle = 1, \quad \langle \psi | A_0 B_1 | \psi \rangle = 0, \quad \langle \psi | A_0 B_2 | \psi \rangle = 1/\sqrt{2},$$

$$\langle \psi | A_1 B_0 | \psi \rangle = 0, \quad \langle \psi | A_1 B_1 | \psi \rangle = 1, \quad \langle \psi | A_1 B_2 | \psi \rangle = 1/\sqrt{2},$$

$$\vec{a}_k = A_k |\psi\rangle, \quad \vec{b}_l = B_l |\psi\rangle,$$

$$\langle \vec{a}_0, \vec{b}_0 \rangle = 1, \quad \langle \vec{a}_1, \vec{b}_1 \rangle = 1, \quad \langle \vec{a}_0, \vec{b}_1 \rangle = 0, \quad \langle \vec{a}_1, \vec{b}_0 \rangle = 0$$

$$\langle \vec{a}_0, \vec{b}_2 \rangle = \langle \vec{a}_1, \vec{b}_2 \rangle = \frac{1}{\sqrt{2}}$$



$$\vec{b}_2 = \frac{1}{\sqrt{2}} \vec{b}_0 + \frac{1}{\sqrt{2}} \vec{b}_1$$

$$B_2 |\psi\rangle = \frac{B_0 + B_1}{\sqrt{2}} |\psi\rangle$$

$$B_2 B_2 |\psi\rangle = |\psi\rangle + \frac{\{B_0, B_1\}}{\sqrt{2}} |\psi\rangle$$

$$\{B_0, B_1\} |\psi\rangle = 0$$

ROBUSTNESS BOUNDS

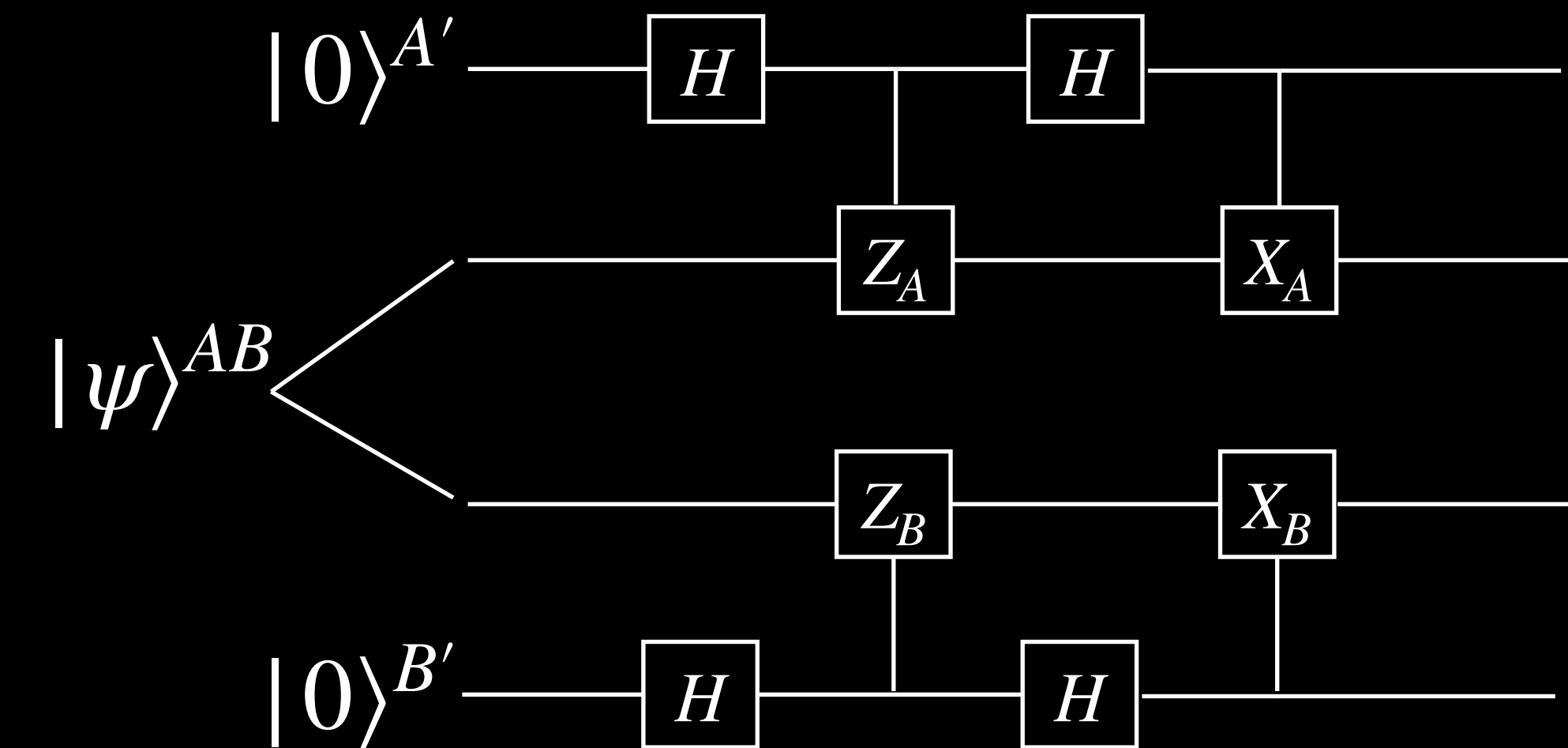
$$\min_{\rho: \beta(\rho)=2\sqrt{2}-\epsilon} \max_{\Lambda_A, \Lambda_B} \langle \text{EPR} | \Lambda_A \otimes \Lambda_B(\rho) | \text{EPR} \rangle$$

Yang, Vertesi, Bancal, Scarani,
Navascues
PRL 113, 4 [2014]

Working with a specific isometry we get rid of maximization, but then we have a lower bound on extractability

SWAP method chooses the SWAP isometry

$$\min_{\rho: \beta(\rho)=2\sqrt{2}-\epsilon} \langle \text{EPR} | \text{SWAP}(\rho) | \text{EPR} \rangle$$



$$4\text{SWAP}(|00\rangle^{A'B'}|\psi\rangle^{AB}) = \sum_{ij=0}^1 |ij\rangle^{A'B'} X_A^i (\mathbb{I} + (-1)^i Z_A) X_B^j (\mathbb{I} + (-1)^j Z_B) |\psi\rangle^{AB}$$

$$16\text{SWAP}(|00\rangle^{A'B'}|\psi\rangle^{AB}) = \sum_{ijkl=0}^1 |ij\rangle\langle kl|^{A'B'} S_{ij} |\psi\rangle\langle\psi|^{AB} S_{kl}^\dagger$$

$$\text{SWAP}(\rho) = \text{Tr}_{AB} 16\text{SWAP}(|00\rangle^{A'B'}|\psi\rangle^{AB}) = \sum_{ijkl=0}^1 |ij\rangle\langle kl|^{A'B'} S_{ij} |\psi\rangle\langle\psi|^{AB} S_{kl}^\dagger$$

$$\text{SWAP}(\rho) = \text{Tr}_{AB} 16\text{SWAP}(|00\rangle^{A'B'}|\psi\rangle^{AB}) = \sum_{ijkl=0}^1 |ij\rangle\langle kl|^{A'B'} S_{ij} |\psi\rangle\langle\psi|^{AB} S_{kl}^\dagger$$

$$\text{SWAP}(\rho) = \sum_{ijkl=0}^1 |ij\rangle\langle kl|^{A'B'} \langle\psi| R_{ijkl} |\psi\rangle$$

$$\min_{\rho: \beta(\rho)=2\sqrt{2}-\epsilon} \langle \text{EPR} | \text{SWAP}(\rho) | \text{EPR} \rangle = \min_{\rho: \beta(\rho)=2\sqrt{2}-\epsilon} \sum_{ijkl=0}^1 \langle\psi| \tilde{R}_{ijkl} |\psi\rangle$$

Use NPA hierarchy for minimization!

ROBUSTNESS BOUNDS

$$\min_{\rho: \beta(\rho)=2\sqrt{2}-\epsilon} \max_{\Lambda_A, \Lambda_B} \langle \psi | \Lambda_A \otimes \Lambda_B(\rho) | \psi \rangle$$

Kaniewski
PRL 117, 070402 [2016]

Bell operator $\mathcal{B}$ and Bell value $\text{Tr}[\mathcal{B}\psi]$

Reference state: $\tilde{\psi}$

Operator inequality $\Lambda_A^\dagger \otimes \Lambda_B^\dagger(\tilde{\psi}) \geq s\mathcal{B} + \mu$ implies $\Xi \geq s\beta + \mu$

1. Apply Jordan's lemma
2. Choose extraction maps (some kind of dephasing channel)
3. Prove the operator inequality!

REPRESENTATION THEORY APPROACH

GOWERS-HATAMI THEOREM

$$X^2|\psi\rangle = \mathbb{I}|\psi\rangle \quad Z^2|\psi\rangle = \mathbb{I}|\psi\rangle \quad \{X, Z\}|\psi\rangle = 0$$

Pauli group

$$X^2 = \mathbb{I} \quad Z^2 = \mathbb{I}; \quad \{X, Z\} = 0$$

$\xleftarrow{\pi}$

$$x, z, e, x^2 = e, z^2 = e, xz = -zx$$

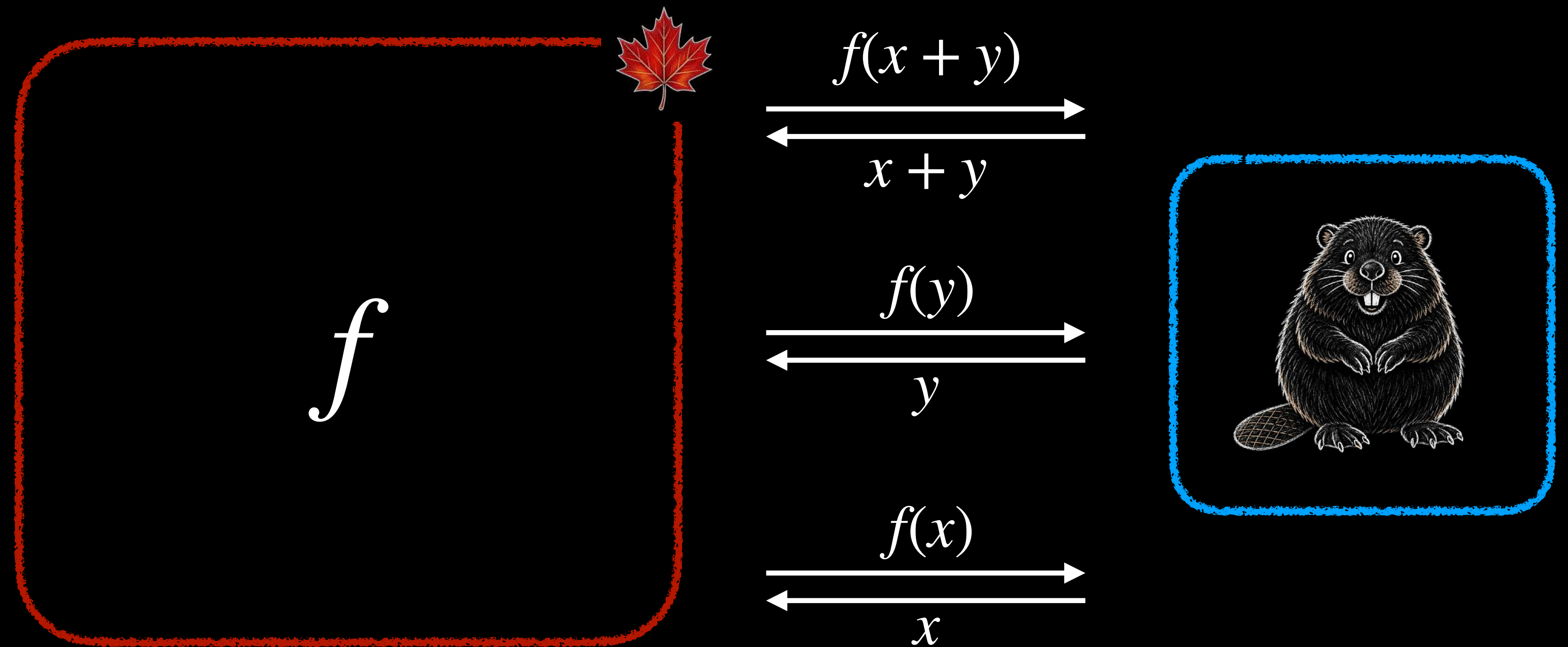
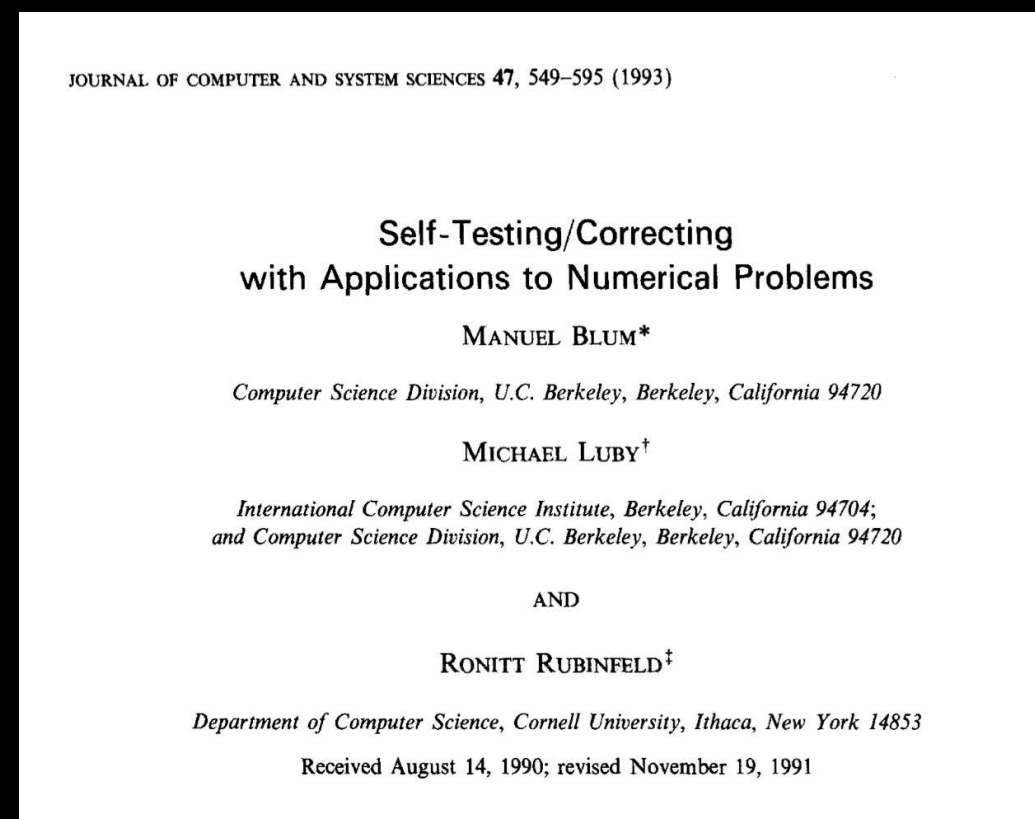
$$\|X^2|\psi\rangle - |\psi\rangle\| \leq \epsilon$$

$$\|Z^2|\psi\rangle - |\psi\rangle\| \leq \epsilon$$

$$\|XZ|\psi\rangle + ZX|\psi\rangle\| \leq \epsilon$$

Is there a representation of the Pauli group such that X and Z are close to it?

GOWERS-HATAMI THEOREM



Passing the test implies that the function is close to some linear function

GOWERS-HATAMI THEOREM

STABILITY OF APPROXIMATE REPRESENTATIONS

$$x, z, e, x^2 = e, z^2 = e, xz = -xz$$

$$(x, z, e) \xrightarrow{f: G \rightarrow U(\mathcal{H})} (X, Z, \mathbb{I})$$

$\exists$ isometry $V: \mathcal{H} \rightarrow \mathcal{K}$
 $\exists$ representation ϕ such that
 $\|Vf(g) - \phi(g)V\|_{\psi}^2 \leq \sqrt{\epsilon}$

$$\|X^2|\psi\rangle - |\psi\rangle\| \leq \epsilon$$

$$\|Z^2|\psi\rangle - |\psi\rangle\| \leq \epsilon$$

$$\|XZ|\psi\rangle + ZX|\psi\rangle\| \leq \epsilon$$

$$V^*\phi(g)V = \mathbb{E}_{h \in G} f(h)^* f(hg)$$

ALGEBRAIC APPROACH

C* ALGEBRAS

C* algebra = Banach algebra over a field of complex numbers with a map $x \rightarrow x^*$

- A. $x^{**} = x$
- B. $(x + y)^* = x^* + y^*$ $(xy)^* = y^*x^*$
- C. $(\lambda x)^* = \bar{\lambda}x^*$
- D. $\|xx^*\| = \|x\|\|x^*\|$

Example: algebra of bounded operators on a Hilbert space

State on the algebra: a unit positive functional $\phi : \mathcal{A} \rightarrow \mathbb{C}$

Representation: a homomorphism

$$\pi : \mathcal{A} \rightarrow B(\mathcal{H})$$

GNS representation:

Every state ϕ induces a representation $\pi_\phi : \mathcal{A} \rightarrow B(\mathcal{H}_\phi)$ and a unit cyclic vector $|\Omega_\phi\rangle$, such that $\phi(a) = \langle \Omega_\phi | \pi_\phi(a) | \Omega_\phi \rangle$

Cyclic: $\pi(\mathcal{A})|\Omega_\phi\rangle = \mathcal{H}_\phi$

UNIVERSAL C^* ALGEBRAS

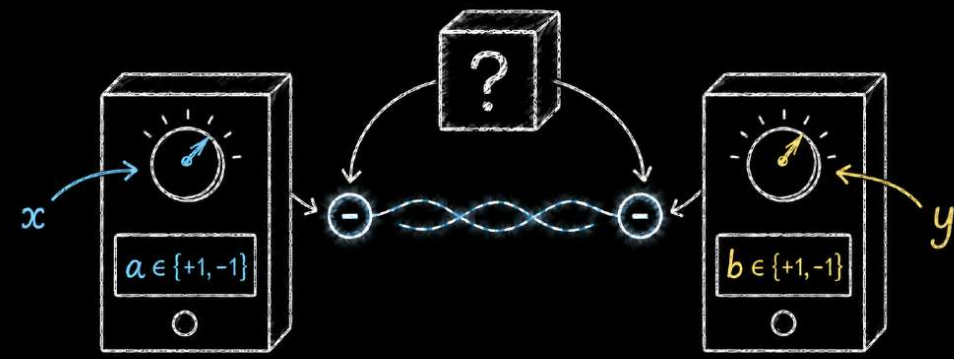
Universal C^* algebra

Fix set of generators g and a relations between them r , run over every concrete realization of the relations and take the largest operator norm that ever occurs.

Universality property

For every instant of operators satisfying the relations, there is a representation from the universal C^* algebra to the concrete algebra, such that the generators are mapped to the operators satisfying relations

UNIVERSAL POVM ALGEBRAS



Alice's POVMs: M_a^x

Bob's POVMs: N_b^y

Shared state: ρ

Define generators $\mathfrak{m}_a^x, \mathfrak{n}_b^y$

Choose relations $\mathfrak{m}_a^x, \mathfrak{n}_b^y \geq 0$, $\sum_a \mathfrak{m}_a^x = 1$, $\sum_b \mathfrak{n}_b^y = 1$

Universal POVM algebra: $\mathcal{A}_A \otimes_{\min} \mathcal{A}_B$

Universality property: There is a representation π such that $\pi(\mathfrak{m}_a^x \otimes \mathfrak{n}_b^y) = M_a^x \otimes N_b^y$

Shared state ρ induces an algebraic state ϕ_ρ ,

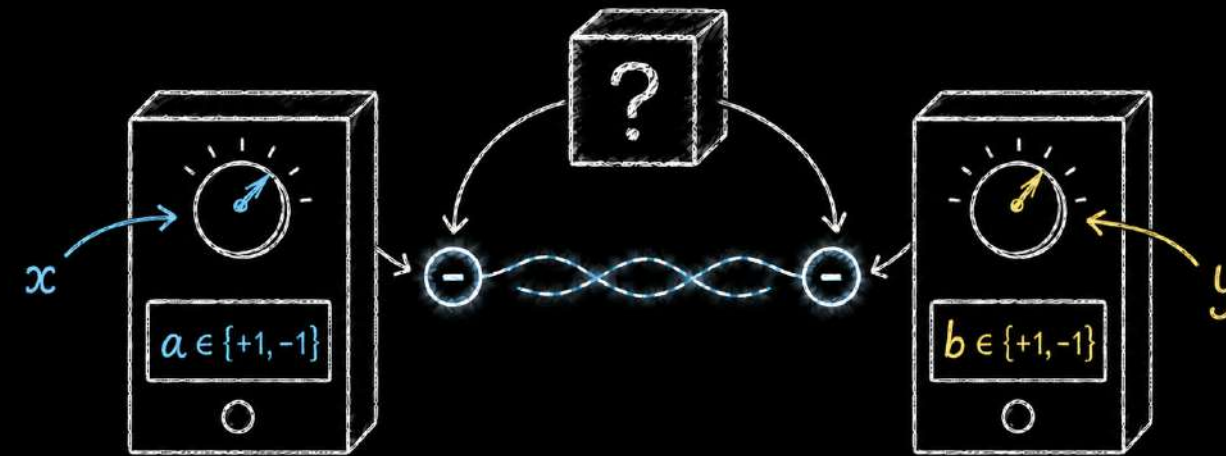
such that $\phi_\rho(\mathfrak{a}) = \text{Tr}[\rho\pi(\mathfrak{a})]$

Correlations are obtained as this state evaluated on generators

$$\phi_\rho(\mathfrak{m}_a^x \otimes \mathfrak{n}_b^y) = \text{Tr}[\rho M_a^x \otimes N_b^y] = p(a, b | x, y)$$

ABSTRACT SELF-TESTING

Paddock, Slofstra, Zhao, Zhou
AHP 25(10), [2024]



Alice's POVMs: M_a^x

“Alice’s” generators $\mathfrak{m}_a^x$

Bob's POVMs: N_b^y

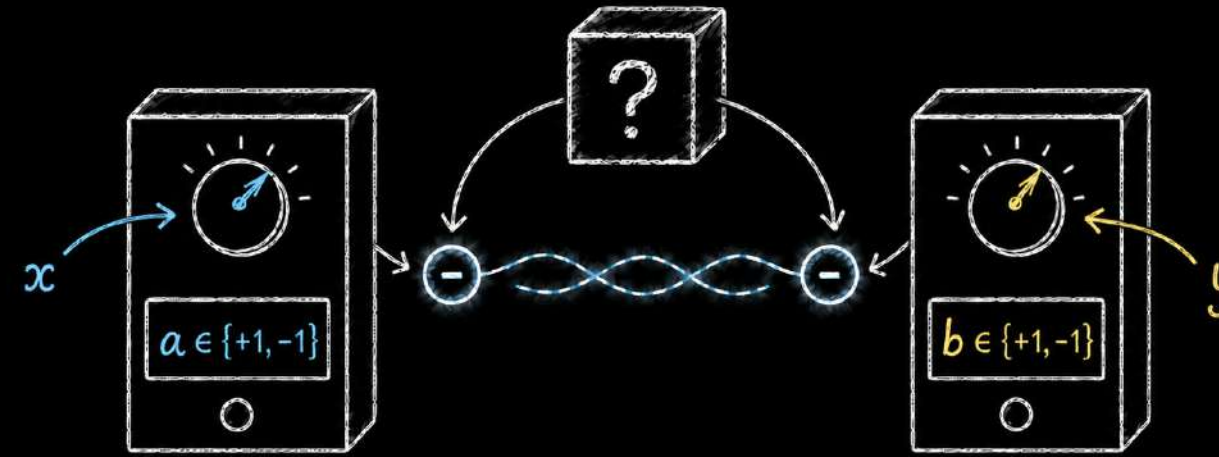
“Bob’s” generators $\mathfrak{n}_b^y$

Shared state: ρ

Algebraic state ϕ_ρ

LET S BE A SUBSET OF STATES ON THE UNIVERSAL POVM ALGEBRA. AN EVENT IS AN ABSTRACT SELF-TEST FOR S IF THERE IS A UNIQUE STATE IN S COMPATIBLE WITH THE EVENT.

ABSTRACT SELF-TESTING



Paddock, Slofstra, Zhao, Zhou
AHP 25(10), [2024]

$$|\psi\rangle \quad \{M_a^x, N_b^y\} \xleftarrow{\pi} \{\mathfrak{m}_a^x, \mathfrak{n}_b^y\} \xrightarrow{\bar{\pi}} \{\bar{M}_a^x, \bar{N}_b^y\} \quad |\bar{\psi}\rangle$$

$$\phi_\psi(\Pi(\mathfrak{m}_a^x \otimes \mathfrak{n}_b^y)) = \langle \psi | \Pi \left(\pi(\mathfrak{m}_a^x) \otimes \pi(\mathfrak{n}_b^y) \right) | \psi \rangle \quad \phi_{\bar{\psi}}(\Pi(\mathfrak{m}_a^x \otimes \mathfrak{n}_b^y)) = \langle \bar{\psi} | \Pi \left(\bar{\pi}(\mathfrak{m}_a^x) \otimes \bar{\pi}(\mathfrak{n}_b^y) \right) | \bar{\psi} \rangle$$

$$\phi_\psi(\Pi(\mathfrak{m}_a^x \otimes \mathfrak{n}_b^y)) = \langle \psi | \Pi \left(M_a^x \otimes N_b^y \right) | \psi \rangle \quad \phi_{\bar{\psi}}(\Pi(\mathfrak{m}_a^x \otimes \mathfrak{n}_b^y)) = \langle \bar{\psi} | \Pi \left(\bar{M}_a^x \otimes \bar{N}_b^y \right) | \bar{\psi} \rangle$$

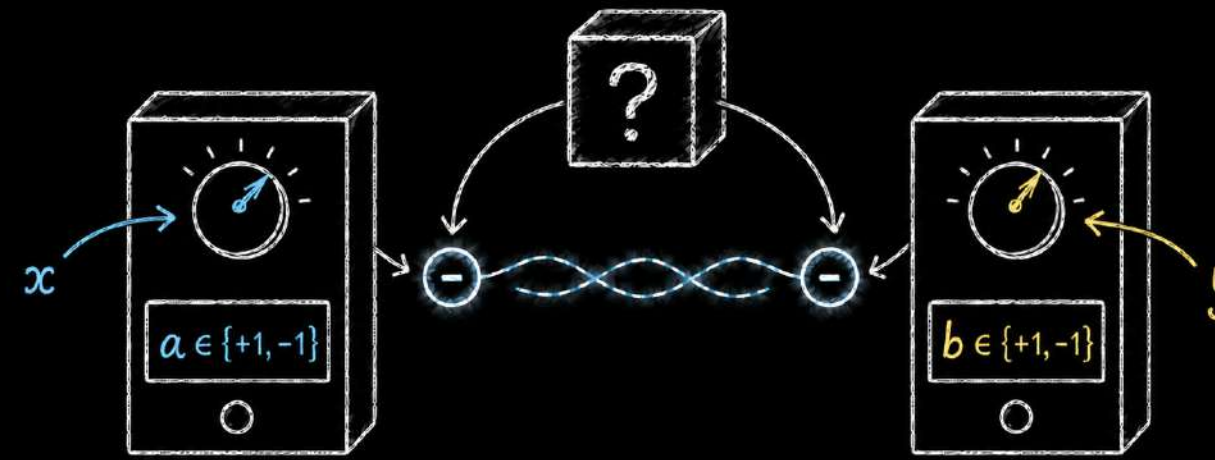
The state is unique !

$$\langle \psi | \Pi \left(M_a^x \otimes N_b^y \right) | \psi \rangle = \langle \bar{\psi} | \Pi \left(\bar{M}_a^x \otimes \bar{N}_b^y \right) | \bar{\psi} \rangle$$

All moments for two strategies are equal!

ABSTRACT SELF-TESTING

Paddock, Slofstra, Zhao, Zhou
AHP 25(10), [2024]



$$\{\mathfrak{m}_a^x, \mathfrak{n}_b^y\}$$

$$\phi$$

GNS representation: $\mathcal{H}_\phi, \pi_\phi, |\Omega_\phi\rangle$

Self-tested strategy: $\{\pi_\phi(\mathfrak{m}_a^x), \pi_\phi(\mathfrak{n}_b^y), |\Omega_\phi\rangle\}$

All minimal GNS representations are unitarily equivalent.

“Junk” and isometry come from non-minimal GNS representations.

ABSTRACT SELF-TESTING : CONSEQUENCES

Algebraic definition can be adapted to different quantum models, for example commuting operator model, as opposed to the tensor product model

It allows to move more freely between different strategies, for example it identifies cases in which PVM assumption can be harmlessly introduced.

Algebraic definition keeps the essential algebraic content of strategies, it is essential for defining self-testing in other scenarios, for example sequential ones!

Robust self-testing defined as uniqueness of amenable tracial state!

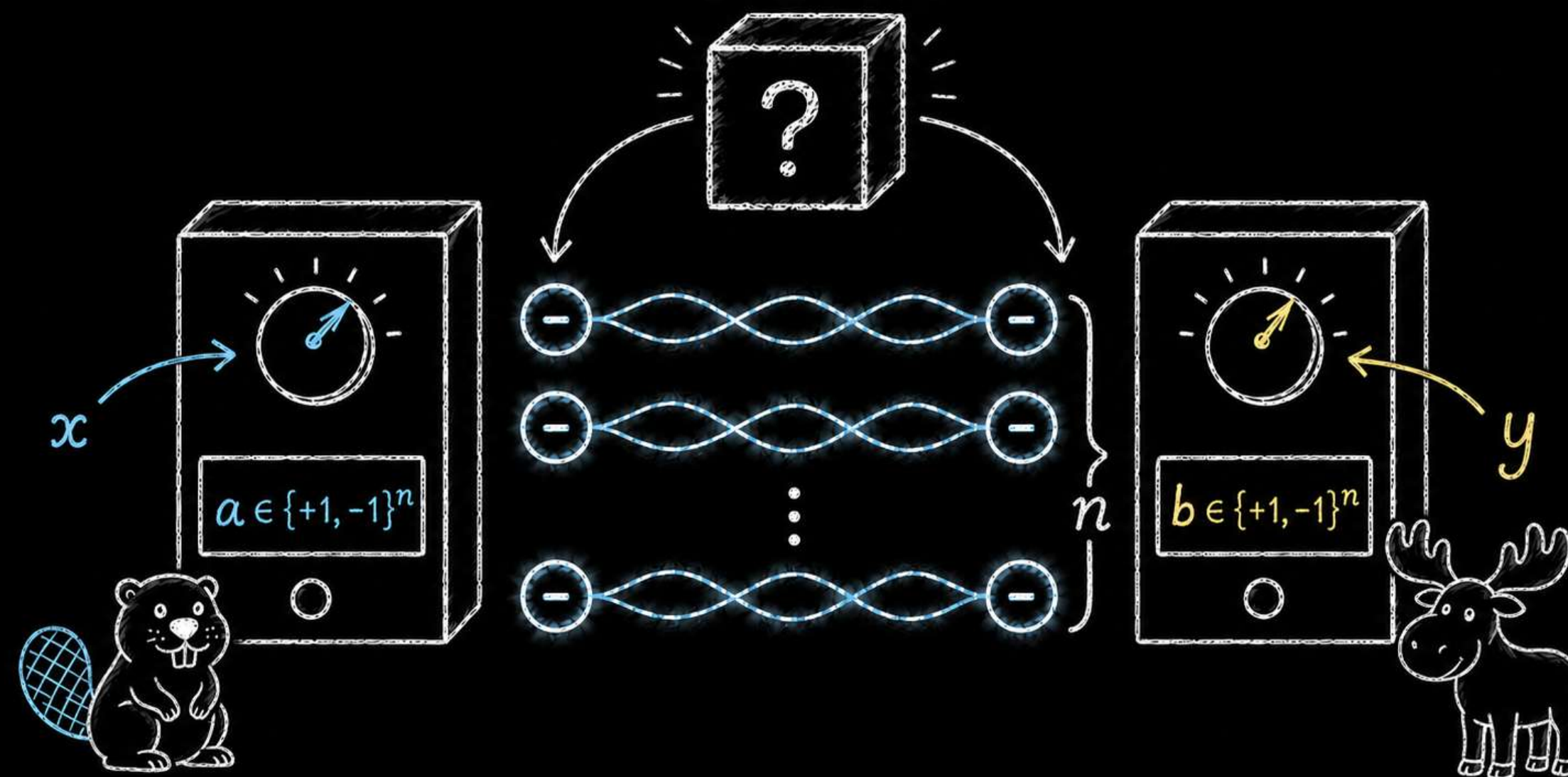
PARALLEL SELF-TESTING

Coladangelo
QIC 17 (9&10) [2017]

McKague
NJP 18 (4) [2016]

Šupić, Bowles, Cavalcanti
Quantum 5 (418) [2021]

Aim: certify that Alice and Bob share n EPR pairs



Approach: make them play n CHSH games, maximal score for all games robustly self-tests n EPR pairs

EPR pairs are extracted one by one, hence robustness deteriorates with every new extracted pair.

Problem: robustness function $f(\epsilon)$ depends also on n . Robustness decreases significantly when number of tested pairs increases.

$$\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$$

PARALLEL SELF-TESTING

Natarajan, Vidick
STOC [2017]

Instead of extracting pair by pair certify global algebraic relations

For all n -bit strings a and b on Alice's side certify existence of observables

$X(a), Z(b)$, which are in ideal case $\bigotimes_{i=1}^n \sigma_x^{a_i}$ and $\bigotimes_{i=1}^n \sigma_z^{b_i}$

These global observables satisfy the following reactions

$$X(a)X(b) = X(a + b) \quad Z(a)Z(b) = Z(a + b) \quad X(a)Z(b) = (-1)^{ab}Z(b)X(a)$$

Linearity in X

Linearity in Z

Anti-commutation

These relations are presentation of n -qubit Pauli group

PARALLEL SELF-TESTING

Natarajan, Vidick
STOC [2017]

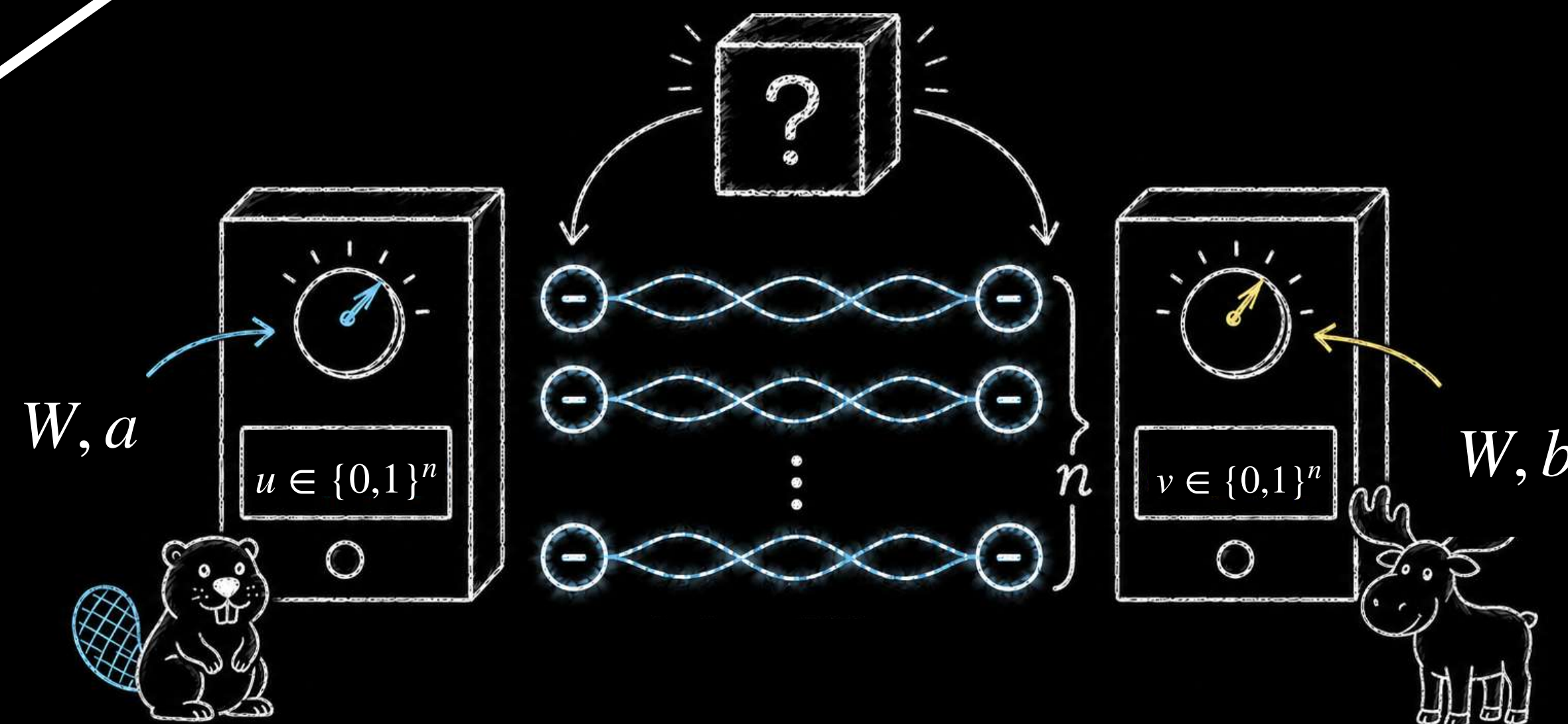
$$X(a)X(b) = X(a + b) \quad Z(a)Z(b) = Z(a + b) \quad X(a)Z(b) = (-1)^{\langle a, b \rangle} Z(b)X(a)$$

Linearity in X

Linearity in Z

Anti-commutation

Oracularized version of
BLR linearity testing



Magic square game

Input: Basis type W and n -bit
string a/b

Input length: $2n$

Output: Hadamard encoding of
the obtained outputs u and v :
 $\alpha = (-1)^{a \cdot u}$ and $\beta = (-1)^{b \cdot v}$
Output length: 2

GH gives robustness that does
not depend on n because we
work with global observables

PARALLEL SELF-TESTING

Natarajan, Vidick
FOCS [2018]

$$X(a)X(b) = X(a + b)$$

Linearity in X

$$Z(a)Z(b) = Z(a + b)$$

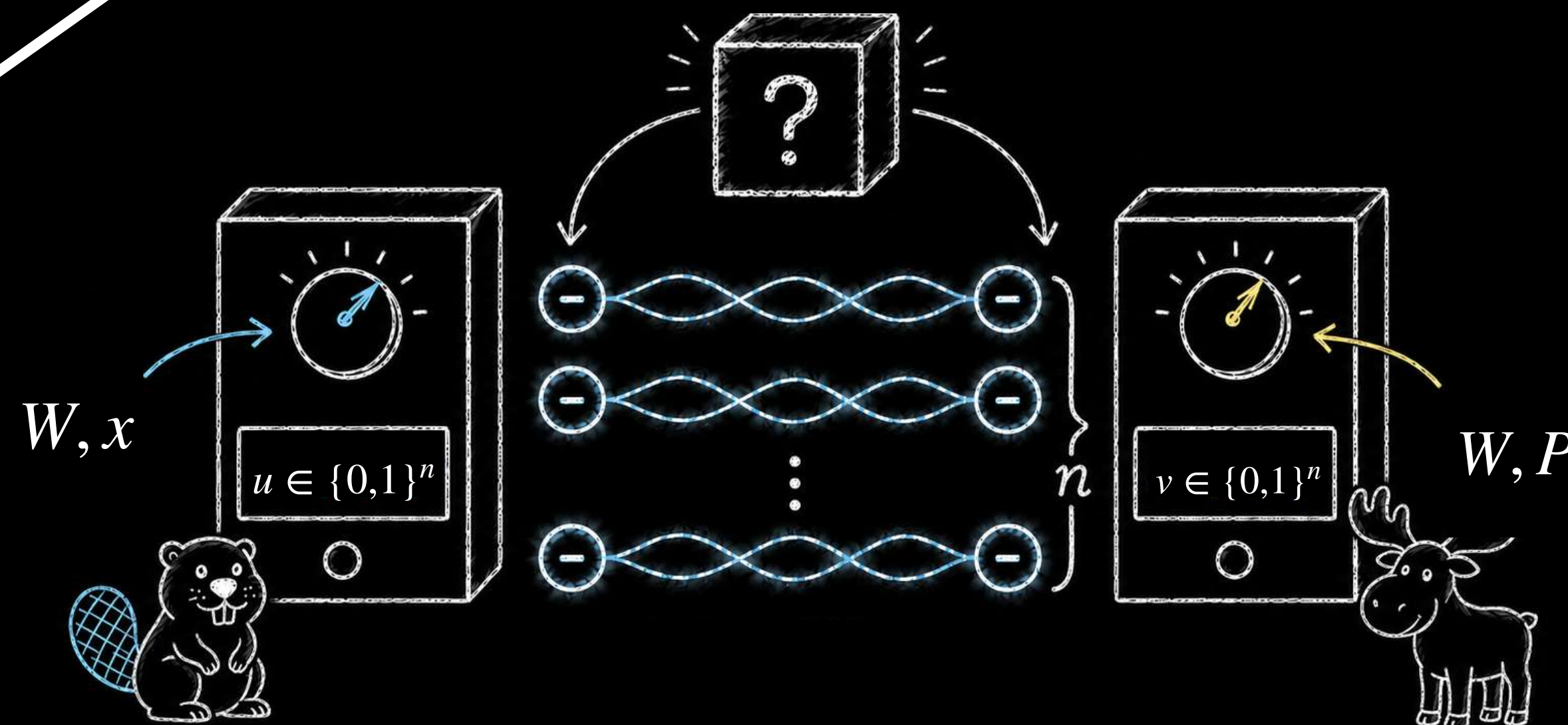
Linearity in Z

$$X(a)Z(b) = (-1)^{\langle a, b \rangle} Z(b)X(a)$$

Anti-commutation

$$a, b \in \mathbb{F}_q^N$$

Raz-Safra plane-vs-point
low-degree testing



Magic square game

Input: Basis type W and a point $x \in \mathbb{F}_q^N$ for one player or a plane P from $\mathbb{F}_q^N$ for the other
Input length: $O(\log n)$

Output: Reed-Muller encoding of obtained outputs u and v

Output length: $\text{poly}(\log \log n)$

GH gives robustness that does not depend on n because we work with global observables

WHAT CAN WE HEAR?

THE QUESTION WE STARTED WITH

CAN QUANTUM THEORY PASS THE TEST OF CARTESIAN METHODOLOGICAL DOUBT?

YES - UP TO LOCAL ISOMETRY!

THAT RESIDUAL FREEDOM IS NOT A WEAKNESS, BUT A DOUBT NO EXPERIMENT CAN EVER REMOVE.

STILL OPEN

- ROBUSTNESS THAT DOES NOT DECAY WITH THE SYSTEM SIZE
- FIDELITY ACCUMULATION THEOREM
- SELF-TESTING OF MULTIPARTITE STATES WITH CONSTANT NUMBER OF INPUTS
- SELF-TESTING OF MULTIPARTITE QUDIT STATES
- MORE TECHNIQUES FOR ROBUST SELF-TESTING

SELF-TESTING BEGAN AS A QUESTION OF TRUSTING A DEVICE
IT ENDED-UP DESCRIBING THE LIMITS OF WHAT CAN BE COMPUTED