



Nonlocality-driven certification without locality

Ivan Šupić
LIP6, Sorbonne University

27. August 2024, Sapporo

Certification of quantumness

- How to verify that a given computing machine is actually quantum?
- Ask it to solve a computational problem with clear time separation needed to solve the problem classically and quantumly.



Certification of quantumness

- How to verify that a given computing machine is actually quantum?
- Ask it to solve a computational problem with clear time separation needed to solve the problem classically and quantumly.



Certification of quantumness

- How to verify that a given computing machine is actually quantum?
- Ask it to solve a computational problem with clear time separation needed to solve the problem classically and quantumly.



Certification of quantumness

- How to verify that a given computing machine is actually quantum?
- Ask it to solve a computational problem with clear time separation needed to solve the problem classically and quantumly.



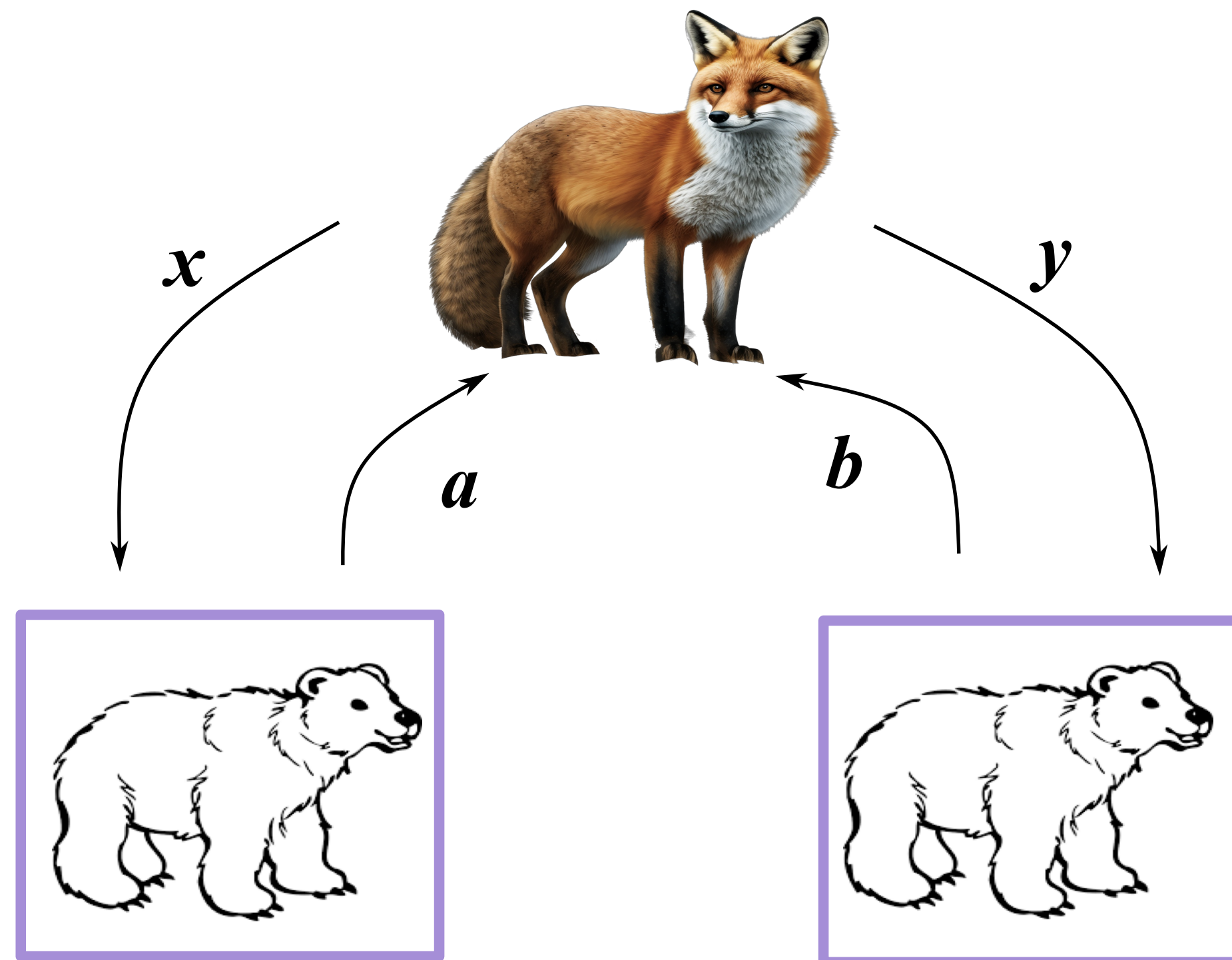
Fundamental yet observable?

- Sampling tasks
- Interactive proofs
- **Embed certification in computing**

Nonlocal games

x and y drawn from the probability distribution $q(x, y)$

Game rule $V(x, y, a, b) \in \{0, 1\}$



Winning probability

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

Optimal classical winning probability

$$\omega_c = \max_{f,g} \sum_{x,y,t} p(t) q(x, y) V(x, y, f(x, t), g(y, t))$$

Quantum strategy $|\psi\rangle, \{M_{a|x}\}_{a,x}, \{N_{b|y}\}_{b,y}$

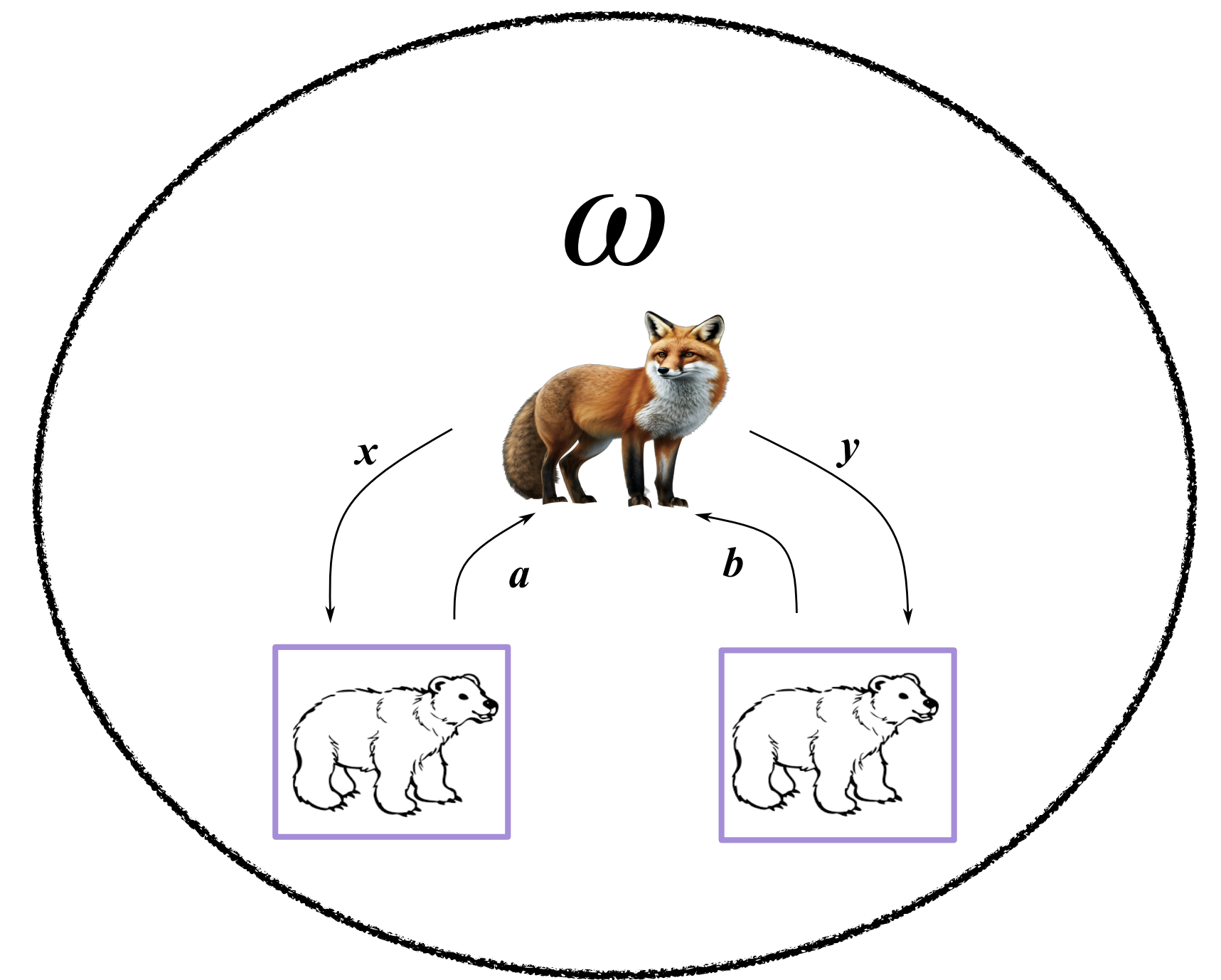
Quantum winning probability

$$\omega_q = \sum_{x,y} q(x, y) \langle \psi | M_{a|x} \otimes N_{b|y} | \psi \rangle V(x, y, a, b)$$

Optimal quantum winning probability

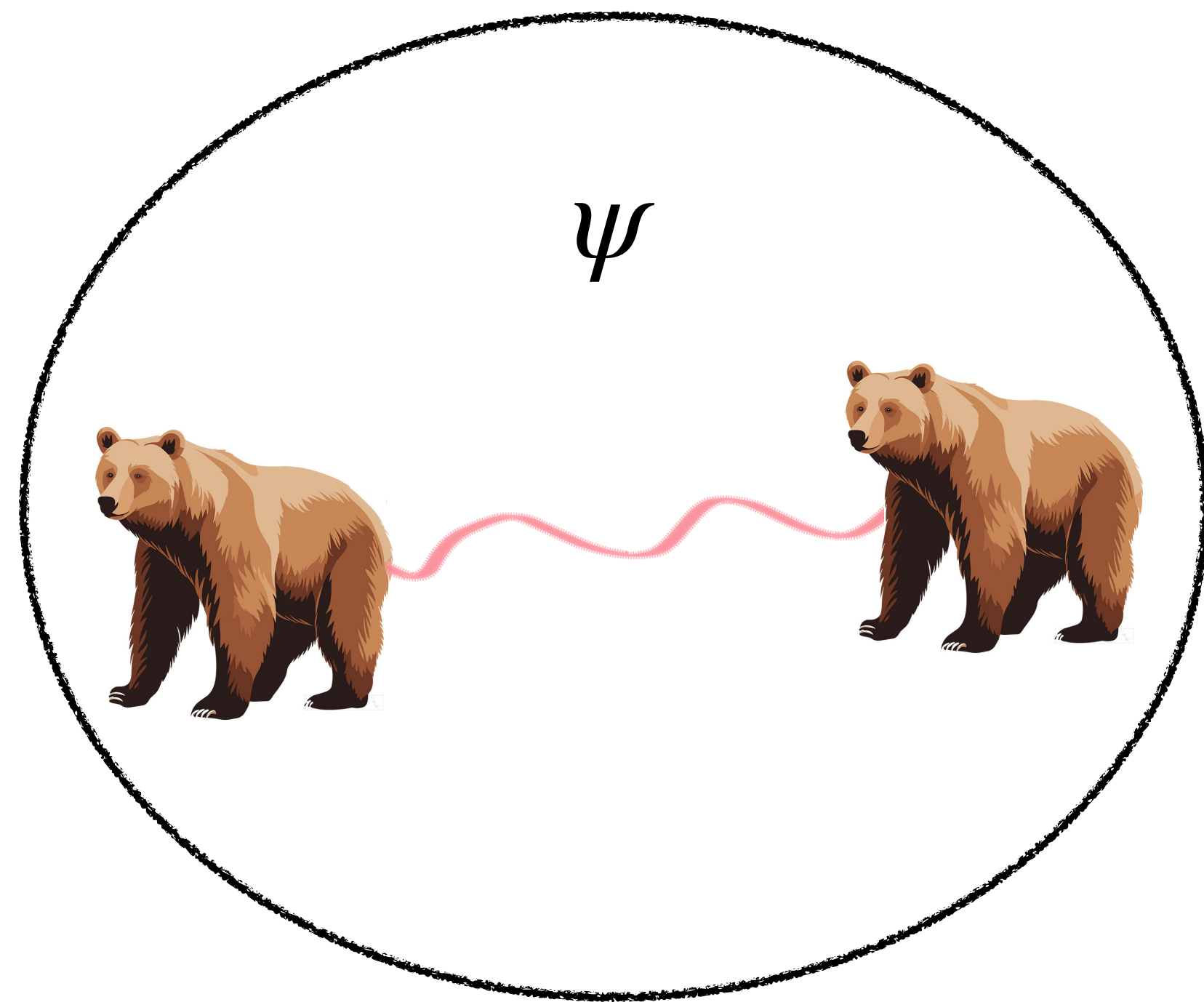
$$\omega_Q = \max_{M_{a|x}, N_{b|y}, |\psi\rangle} \omega_q$$

Device-independent paradigm

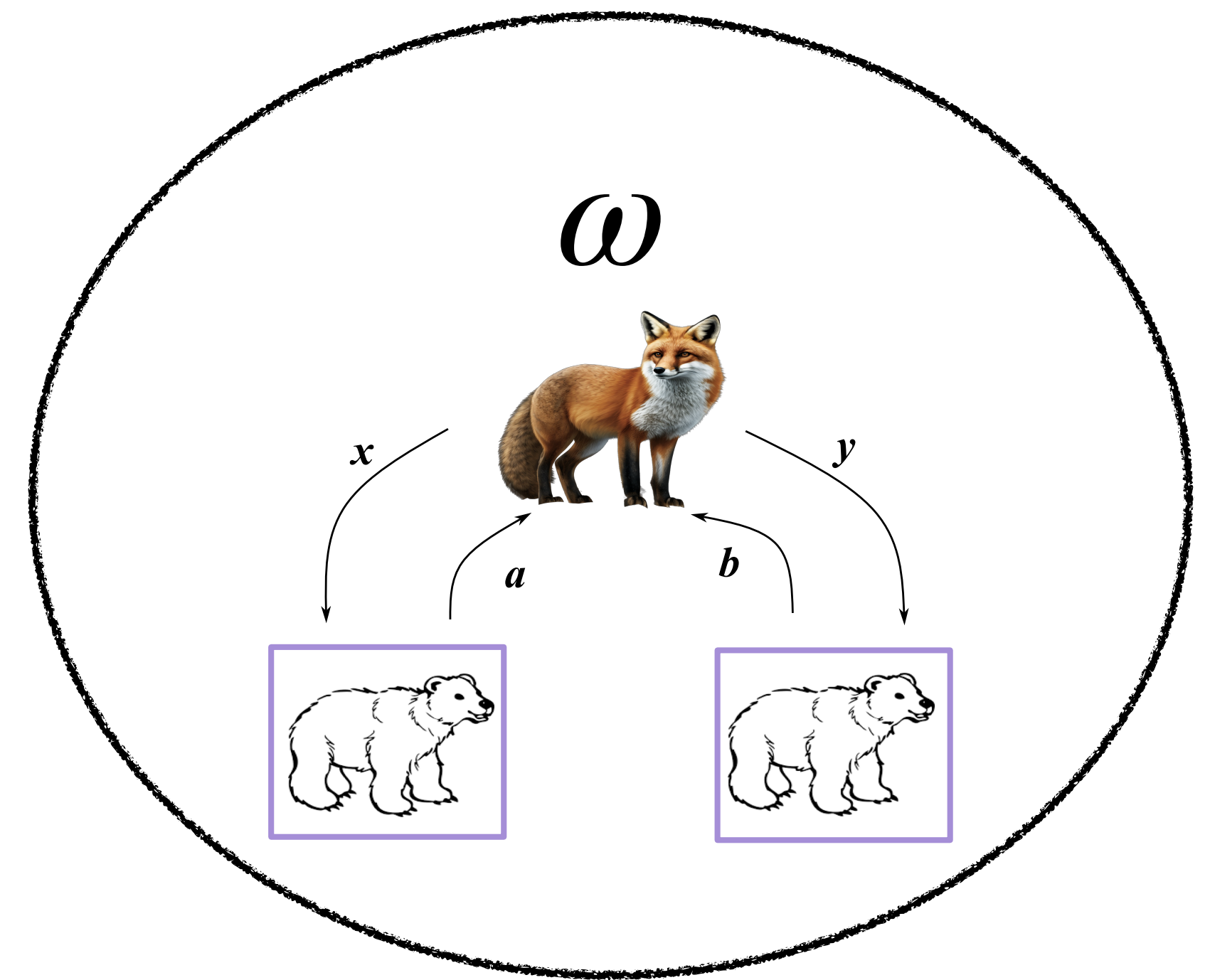


Nonlocal games

Device-independent paradigm

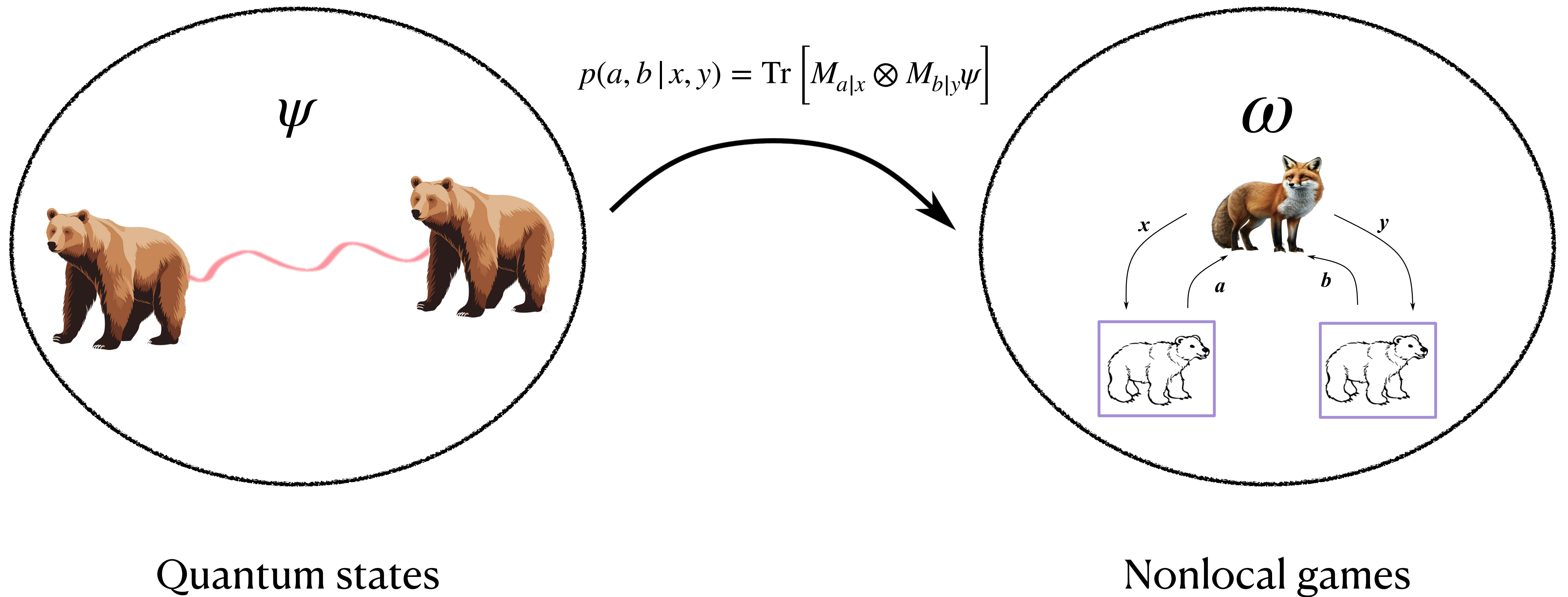


Quantum states

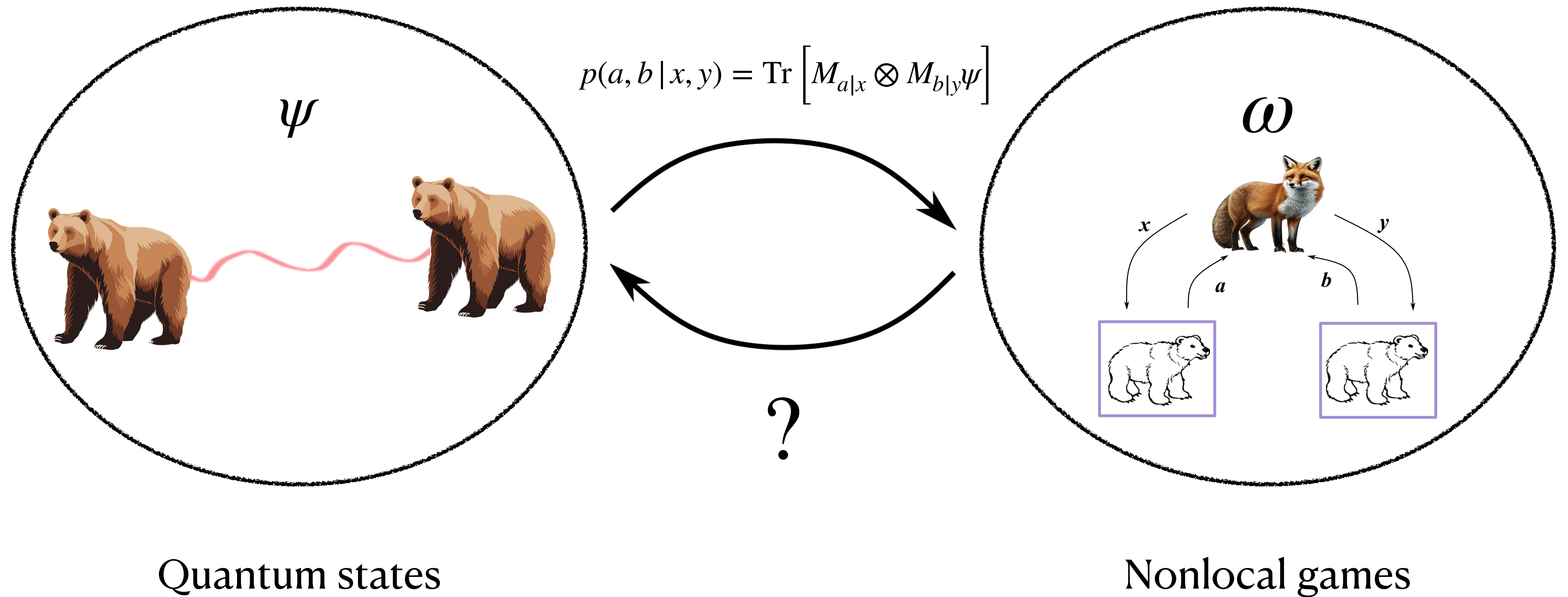


Nonlocal games

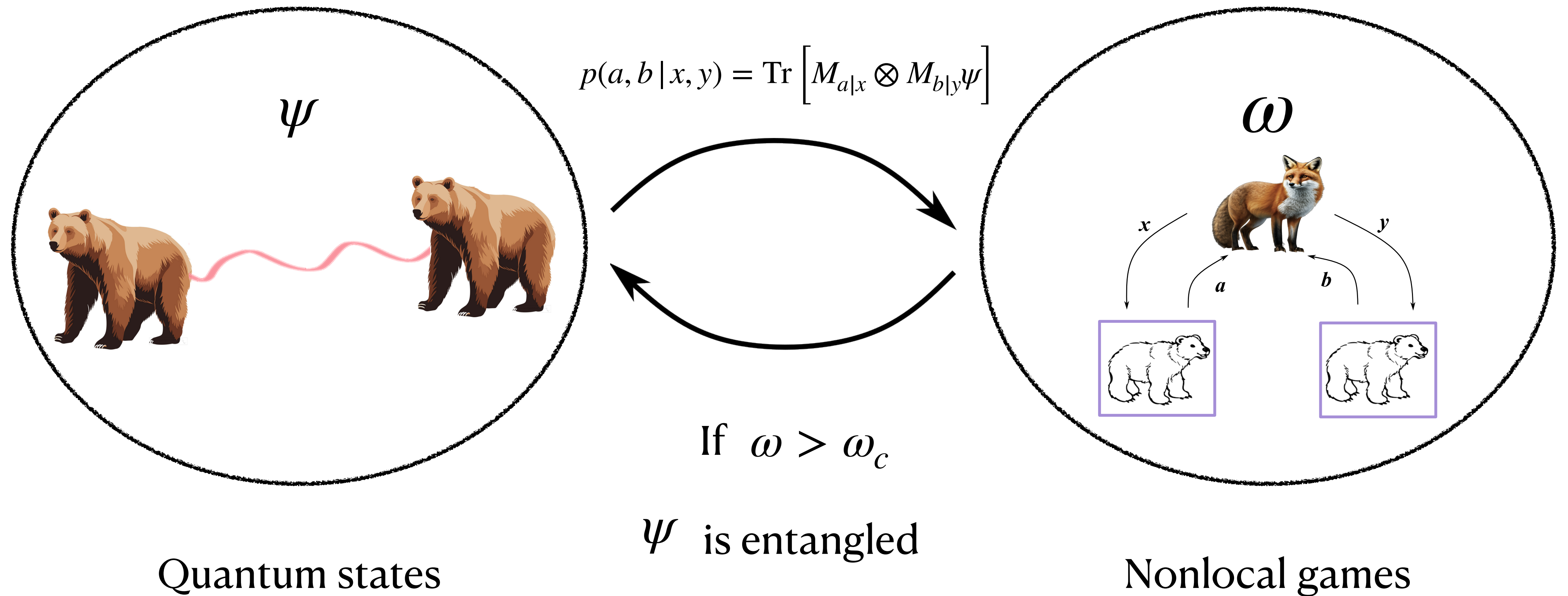
Device-independent paradigm



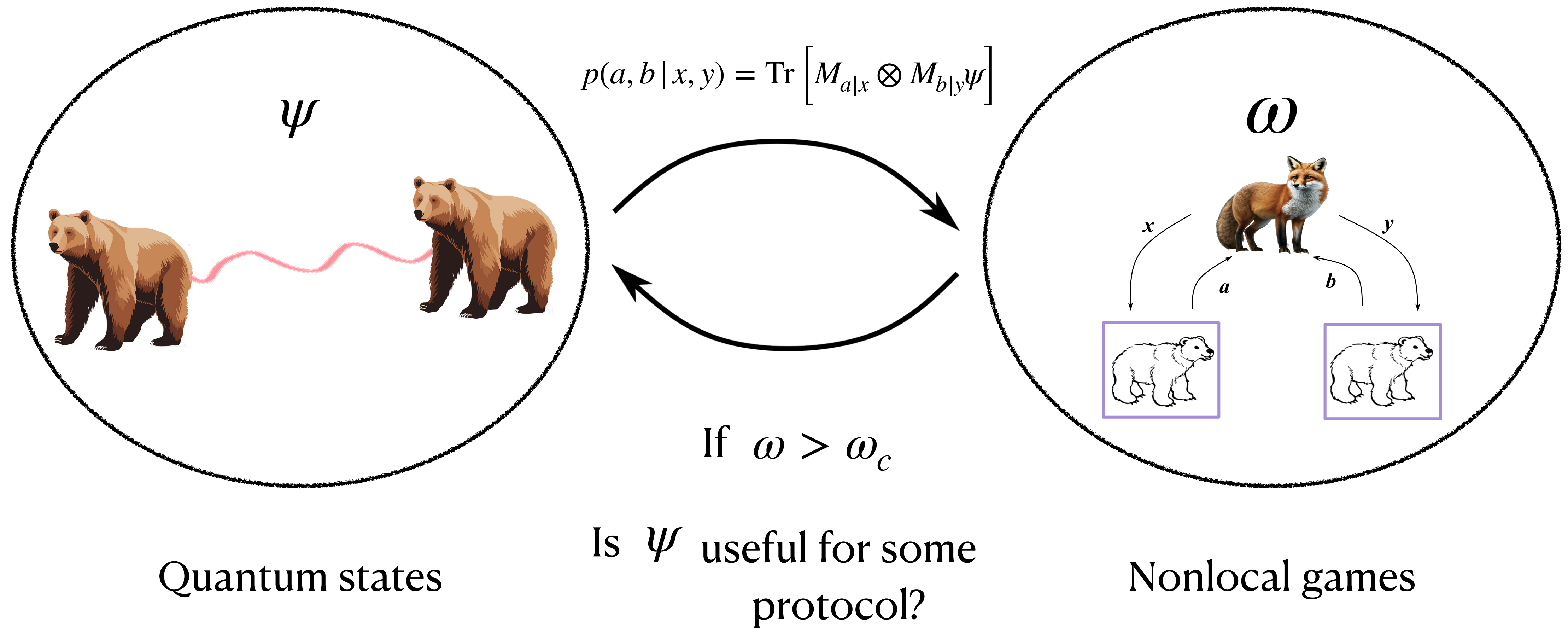
Device-independent paradigm



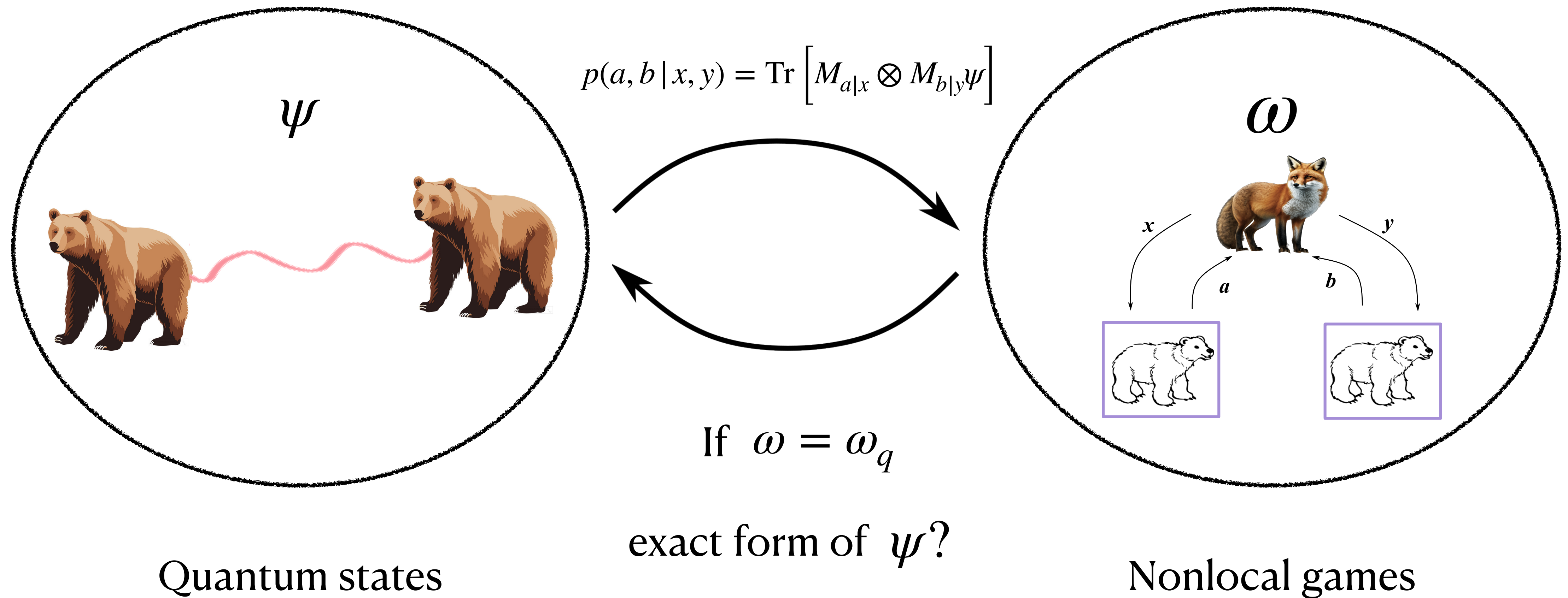
Device-independent paradigm



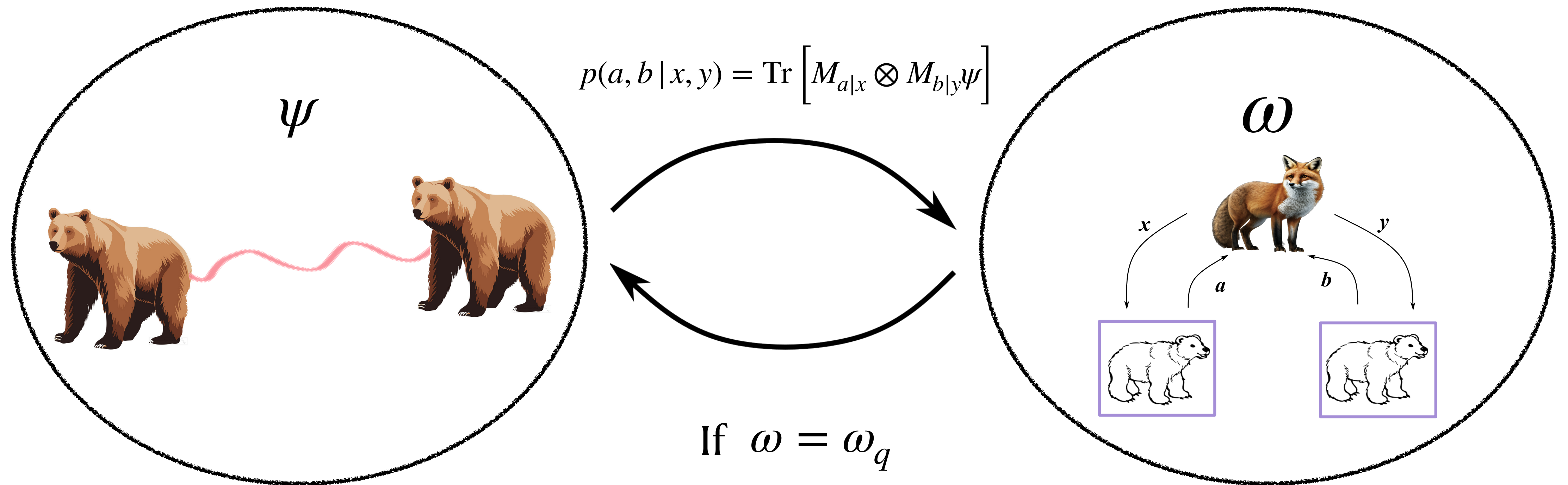
Device-independent paradigm



Device-independent paradigm



Device-independent paradigm

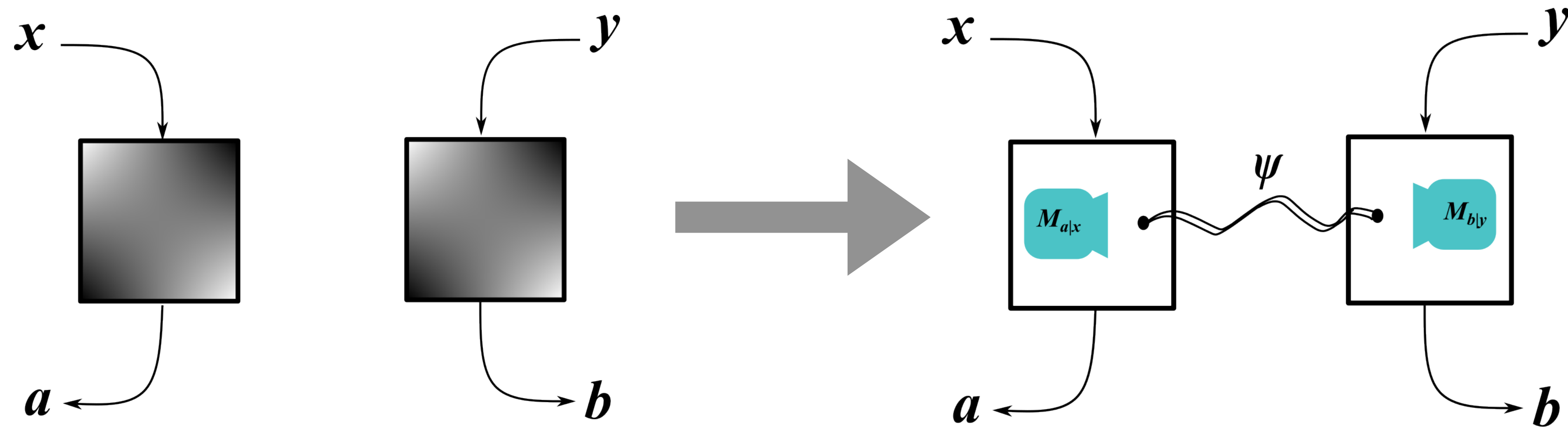


Quantum states

exact form of ψ ?

Nonlocal games

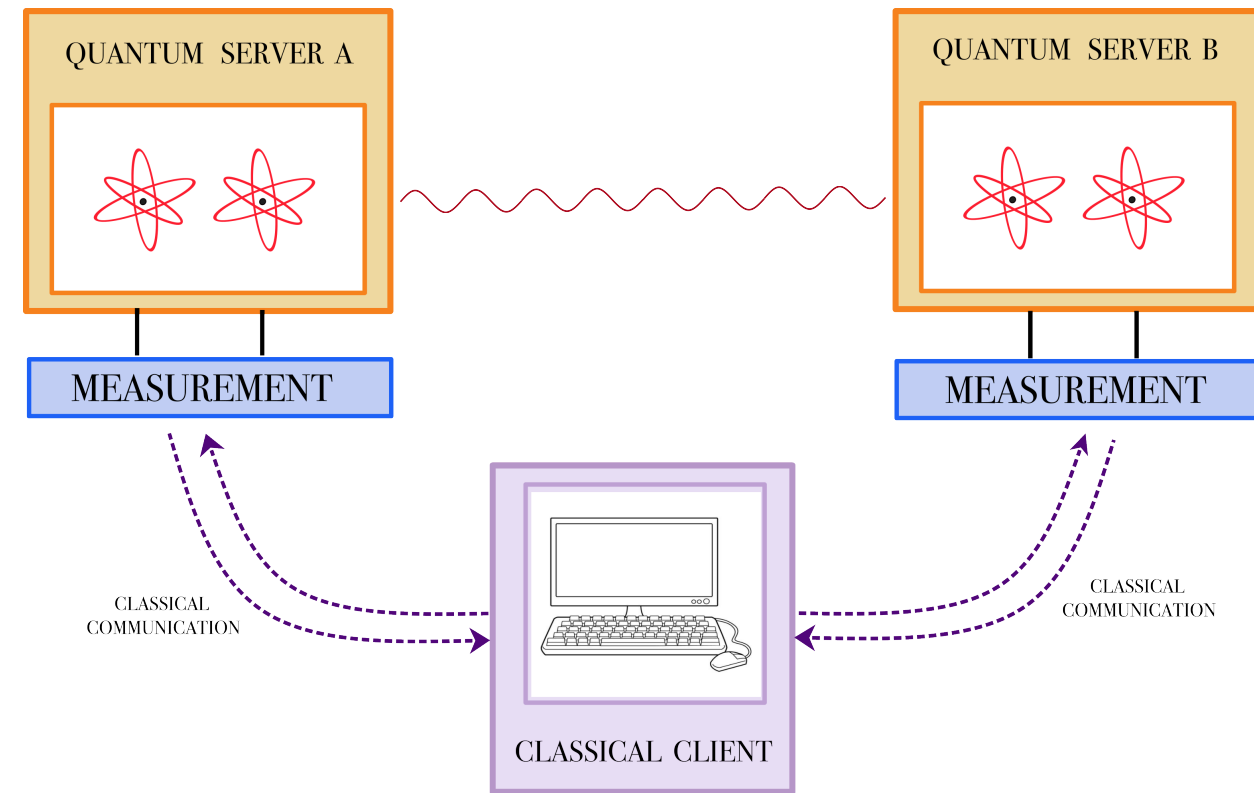
Device-independent paradigm



- Self-testing: inferring the exact form of the quantum state just from the score obtained in a quantum game
- Trust-free verification of quantum states
- Crucial for development of trust-free information protocols

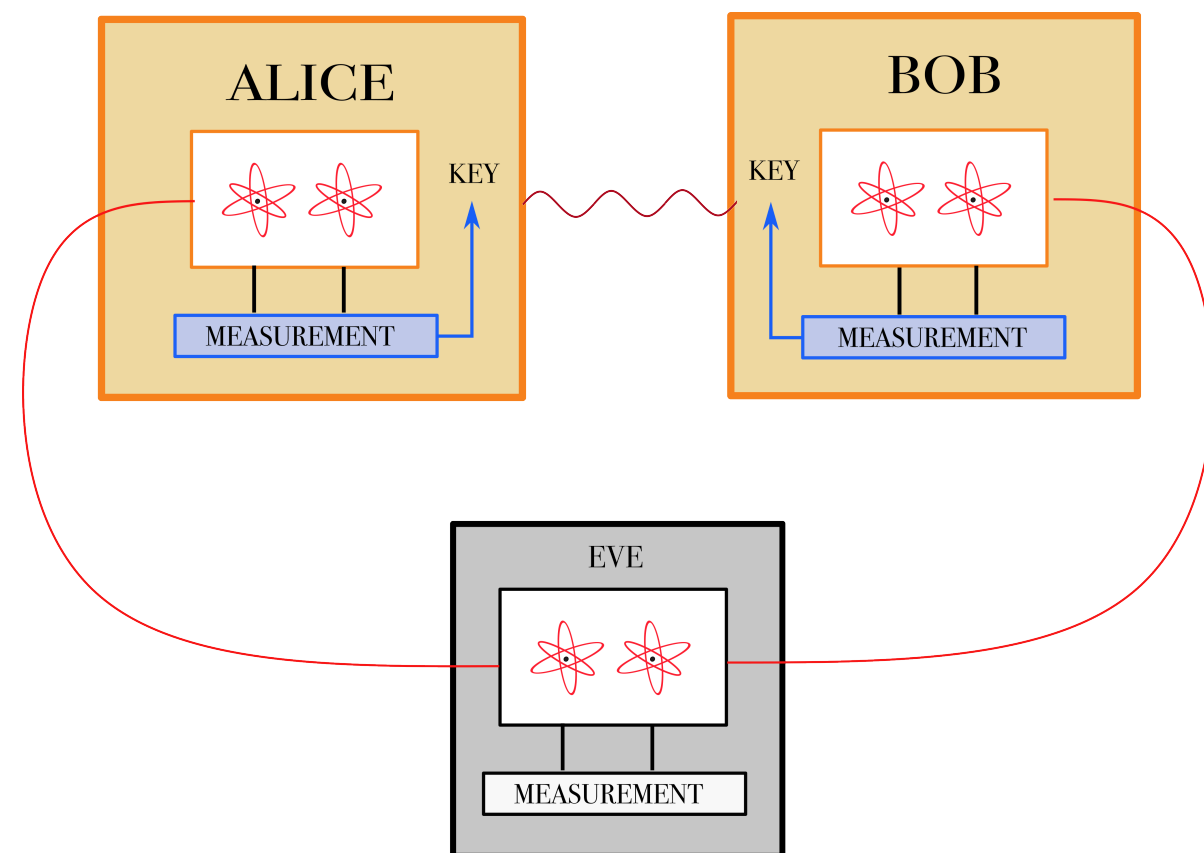
Self-testing

- Delegated quantum computation



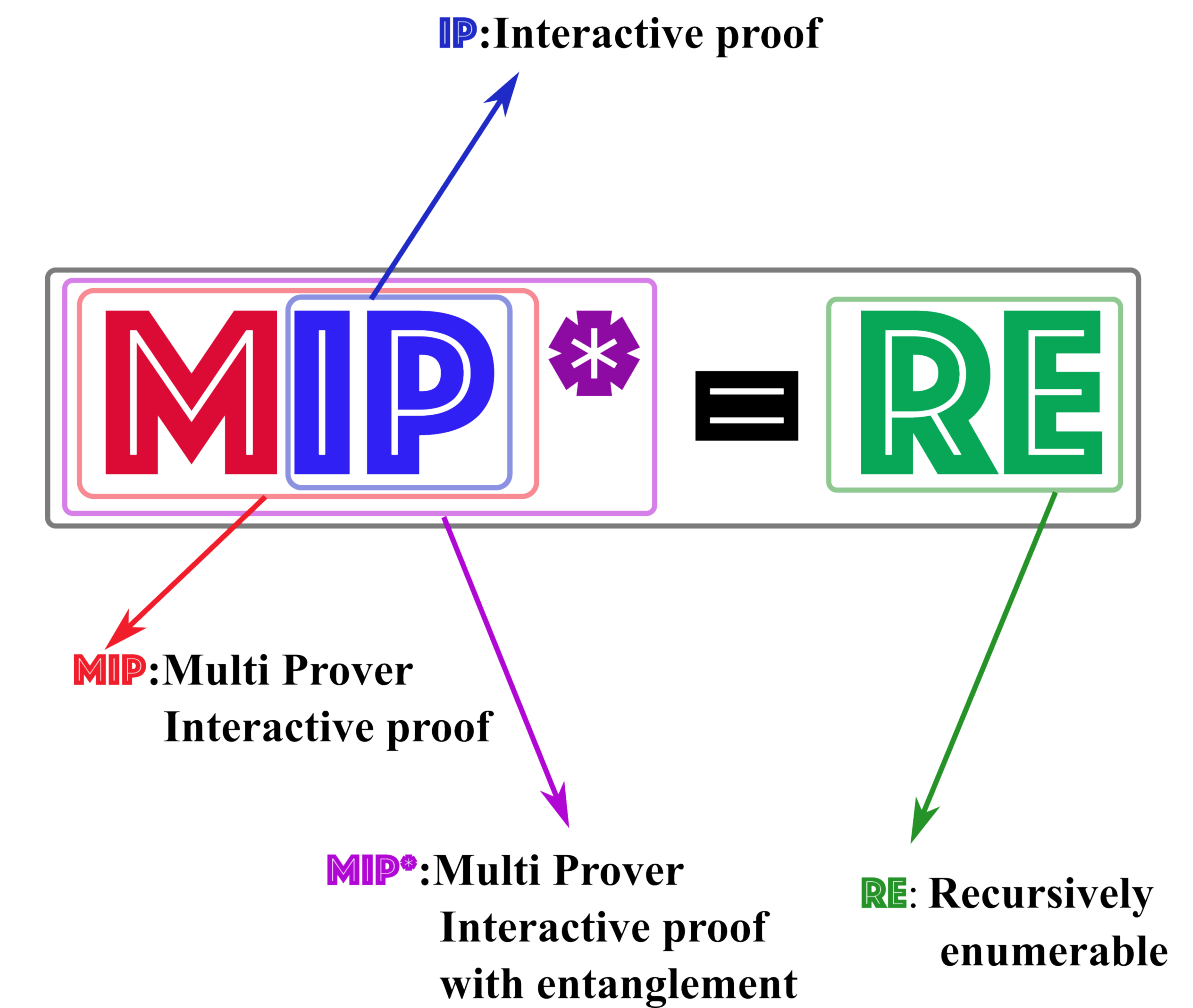
RUV: Nature, 496, 456-460 (2013)
Barz et al: Science, 335 (6066), 303-308

- Trust-free quantum key distribution



Nadlinger et al:
Nature 607 (7920) (2021)

- Computational complexity

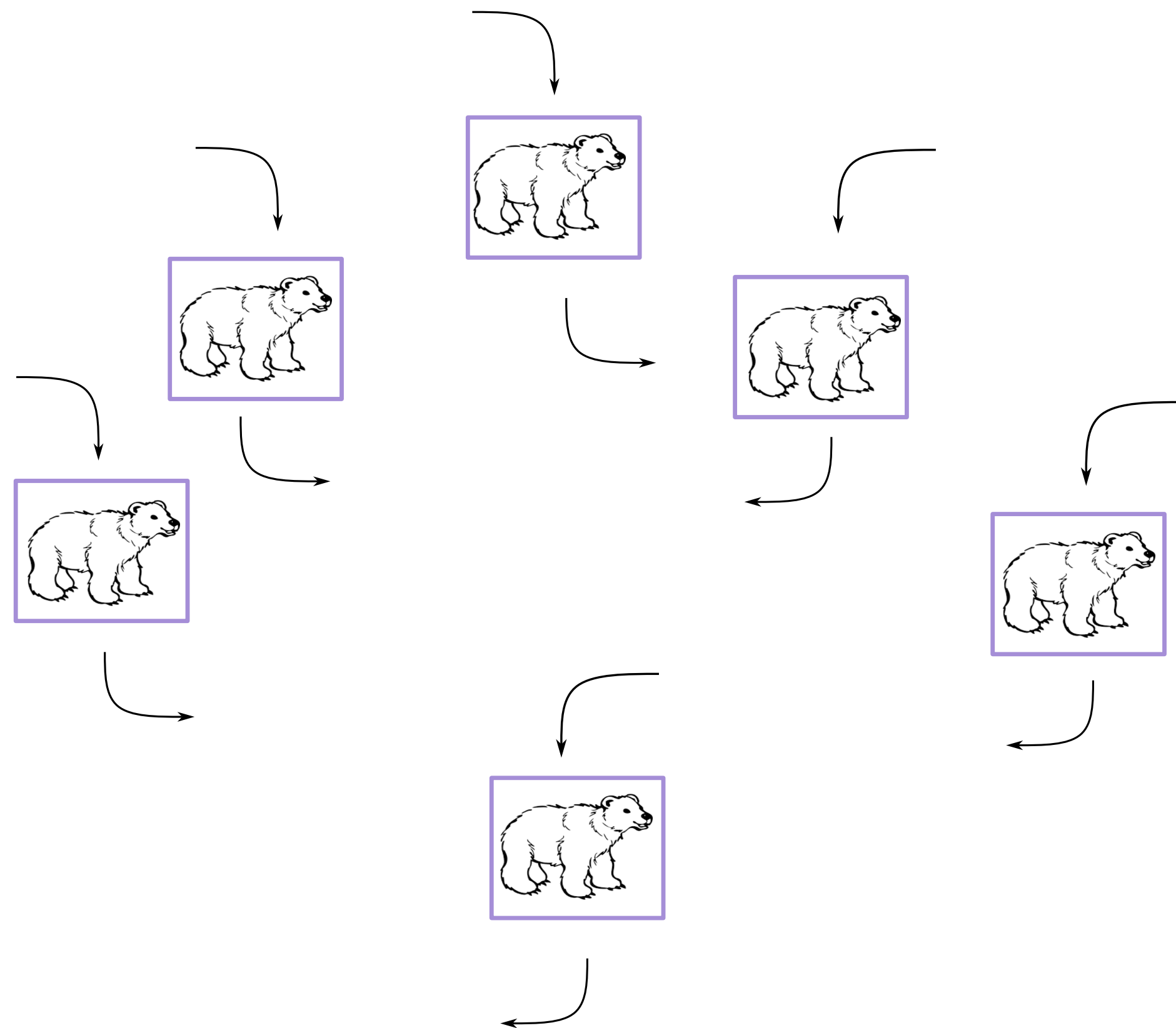


- Genuine randomness generation

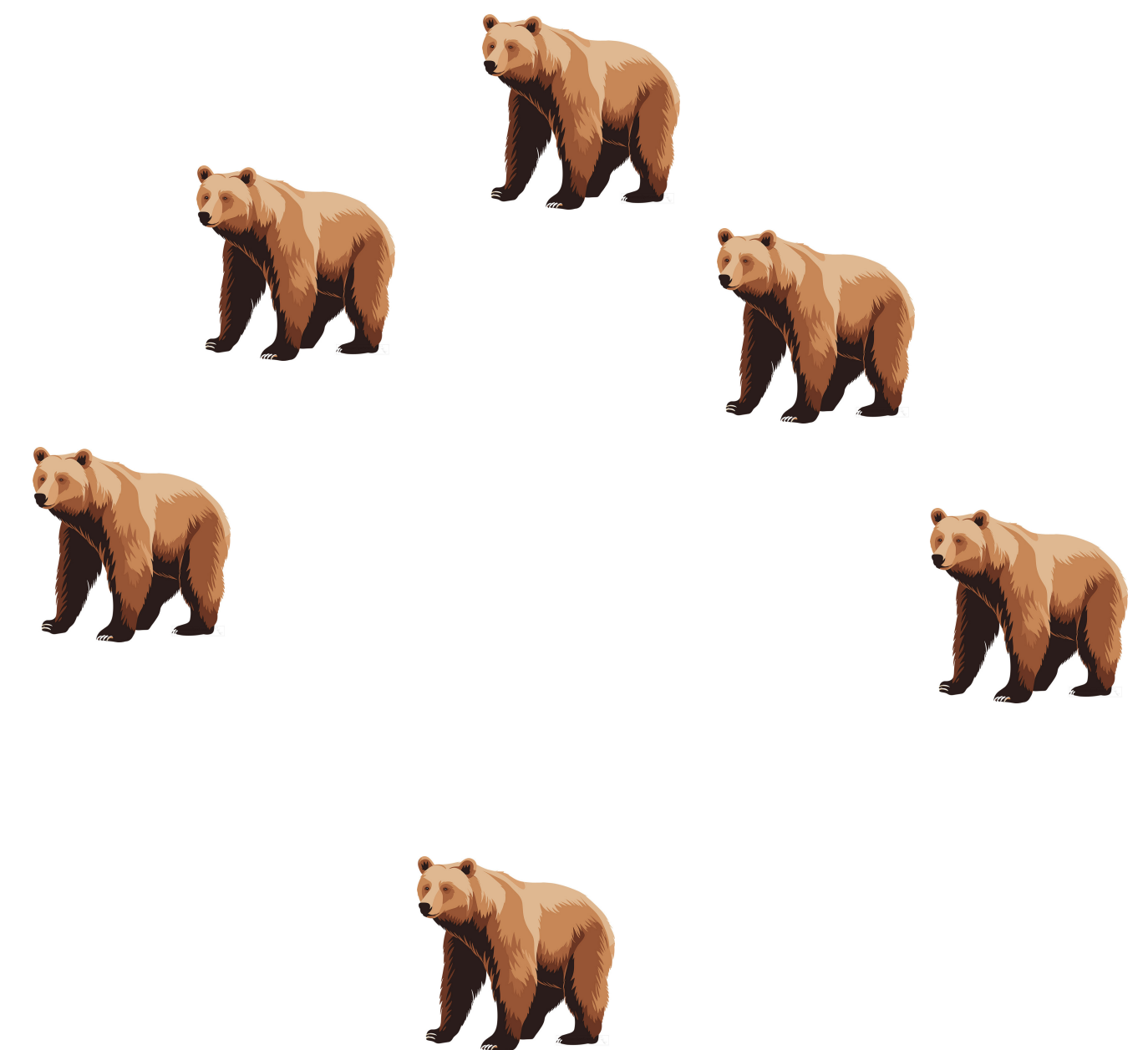


Pironio et al:
Nature 464 (7291) (2020)

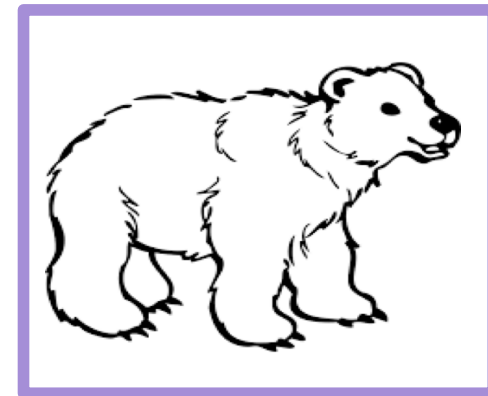
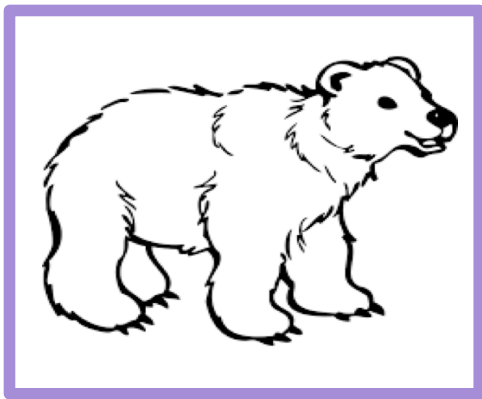
Self-testing



Local isometry

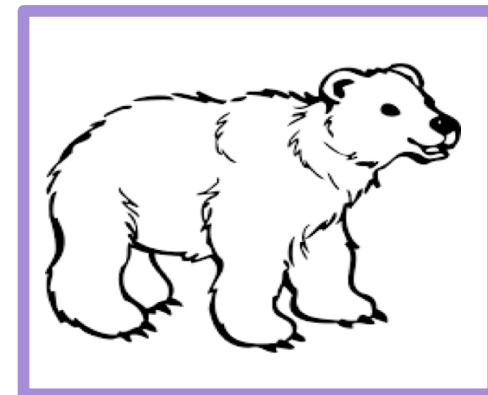
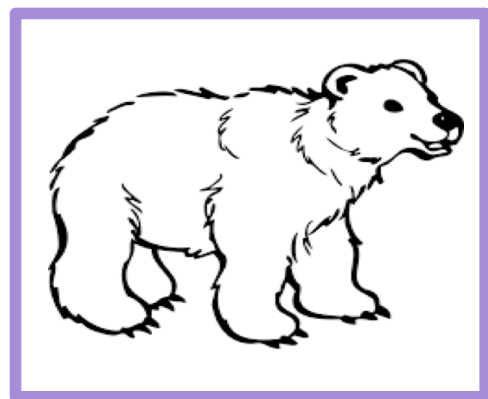


Applying to computing



Self-testing relies on spatial separation!

Applying to computing



Self-testing relies on spatial separation!

Computing devices are integral.

Provers are computationally bounded

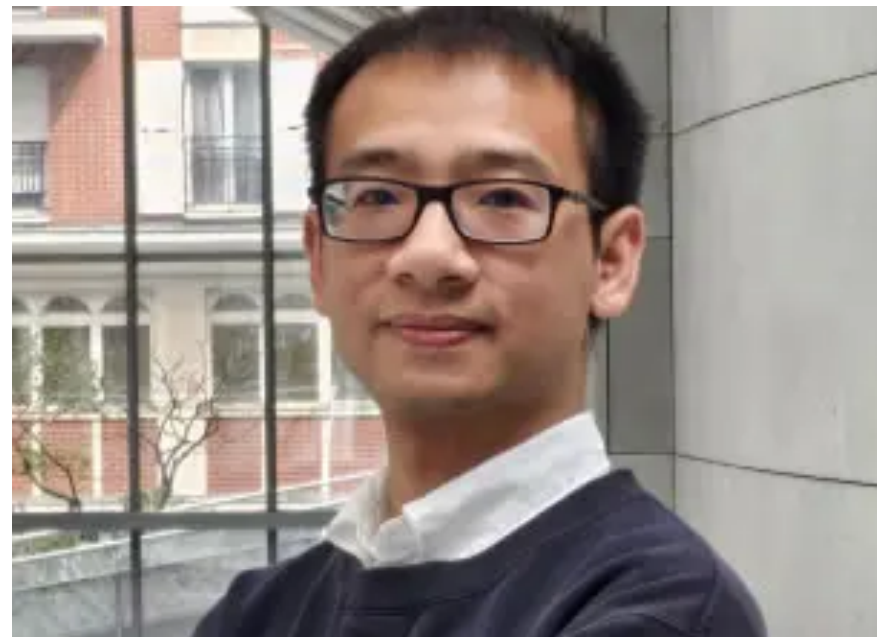
Quantum bounds for compiled XOR and d -outcome CHSH games

arXiv: 2403.05502

M. Baroni



Q. H. Vu



B. Bourdoncle



E. Diamanti



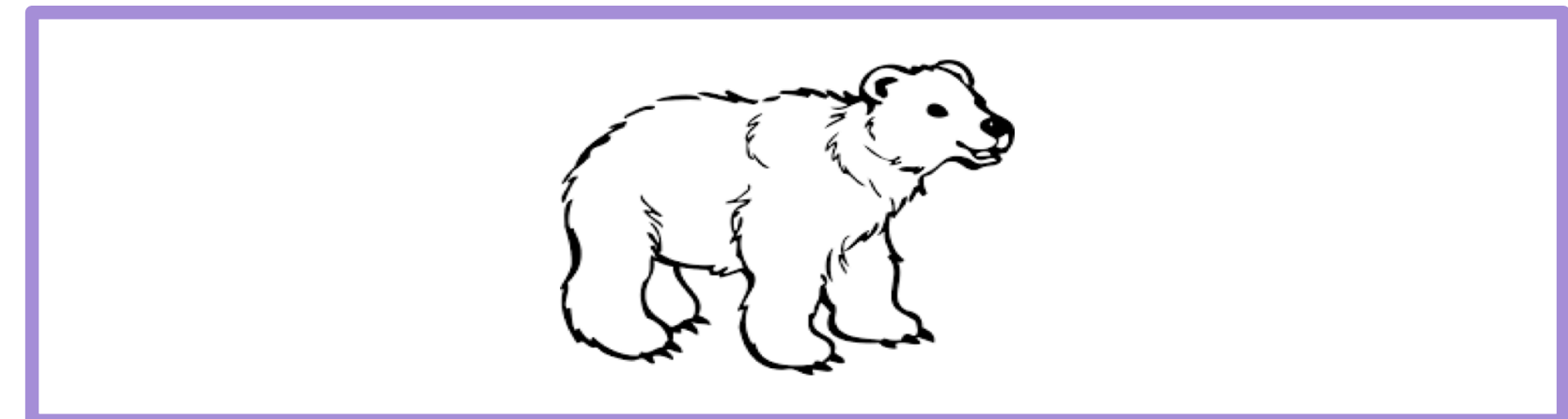
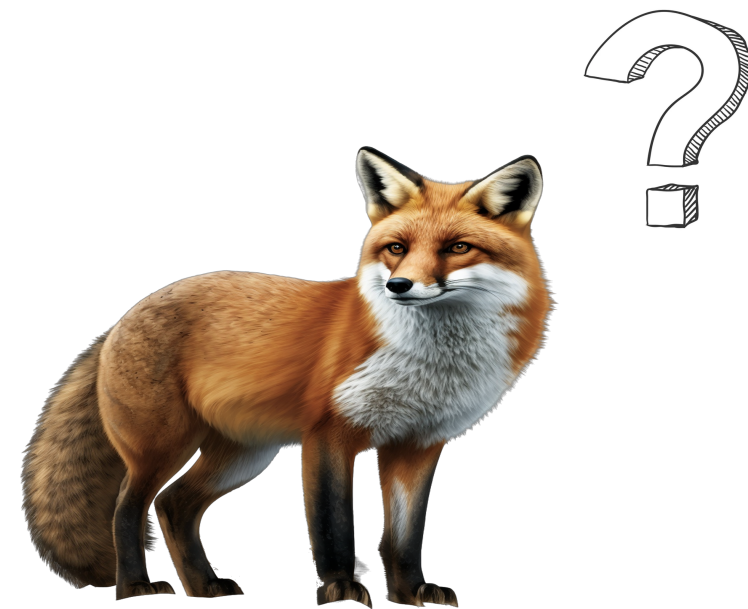
D. Markham



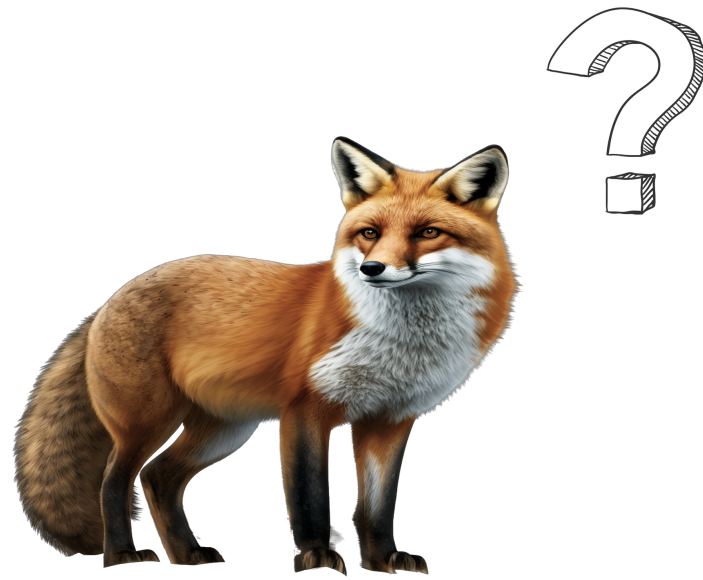
Contributed talk

Friday 14:50

Single-device self-testing

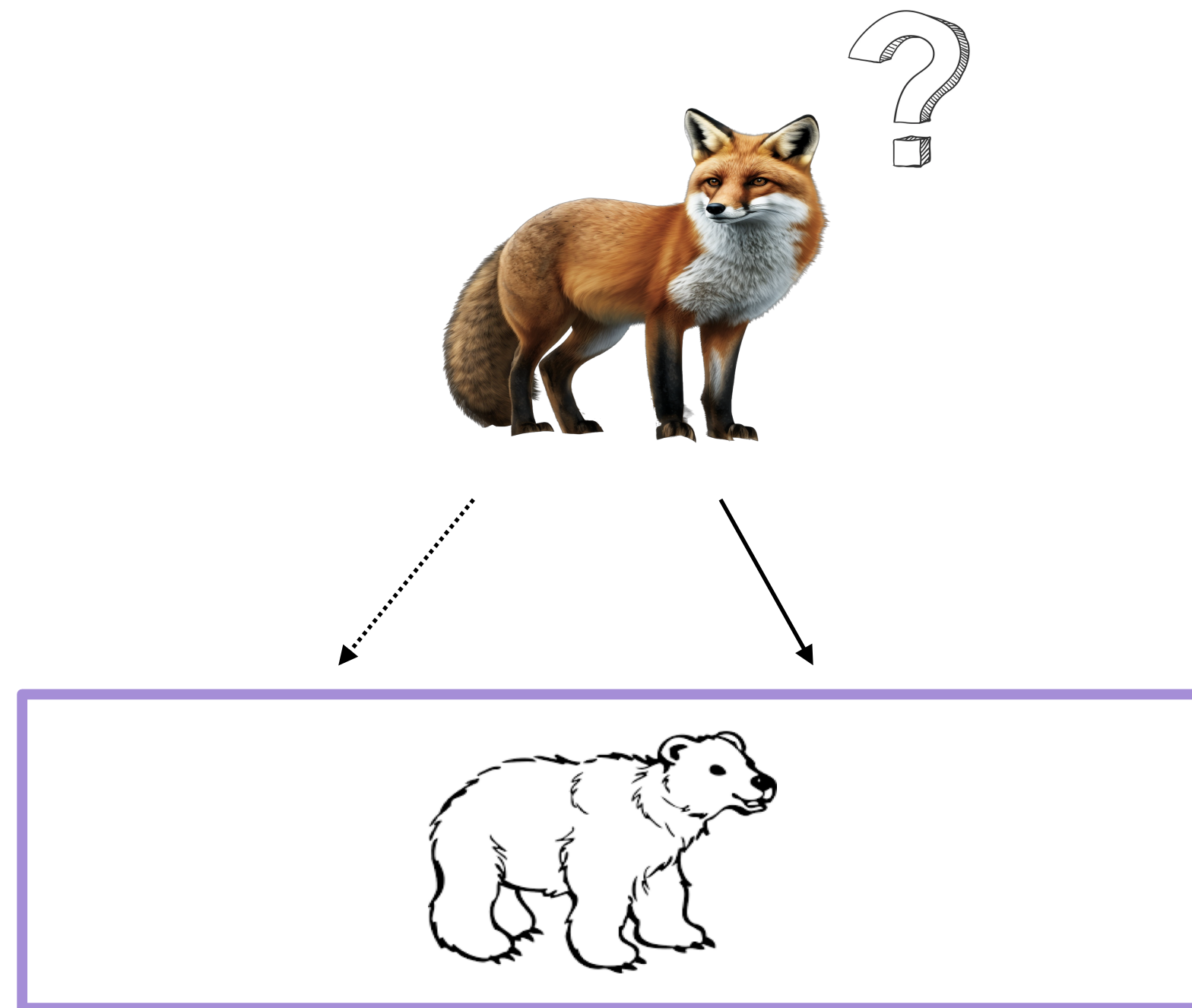


Let us “formalize”



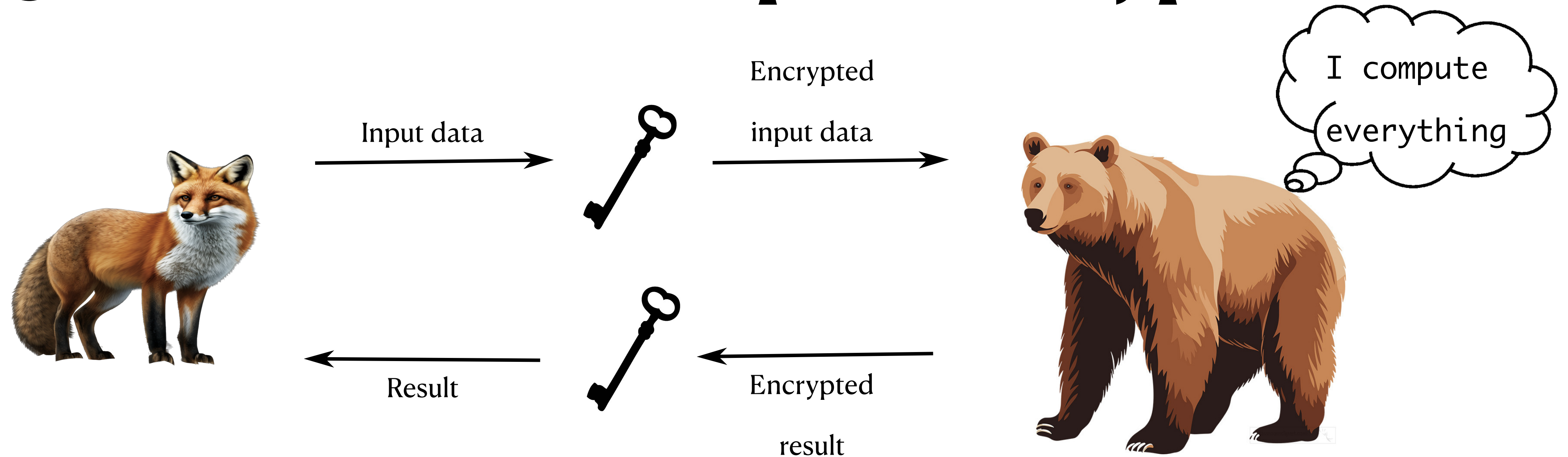
- Bell scenario offers a plenty of ways to certify various quantum resources
- The certification hinges on the assumption of no-signalling (locality of operations)
- Without localised constituents is there any way that one integral system can exhibit a quantum-classical separation so clearly present in the Bell scenario?
- Can a single untrusted prover convince a very suspicious verifier that it perform operations of both “Alice and Bob”?

Cryptography aids



- Encryption instead no-signalling
- Encrypted information cannot be leaked
- Can the circuit that “Alice” would do be completely encrypted ?
- If we want to preserve classical-quantum separation, the encryption should be secure against classical provers.
- If we want to preserve quantum certification, the encryption should be secure against quantum provers (post-quantum cryptography)

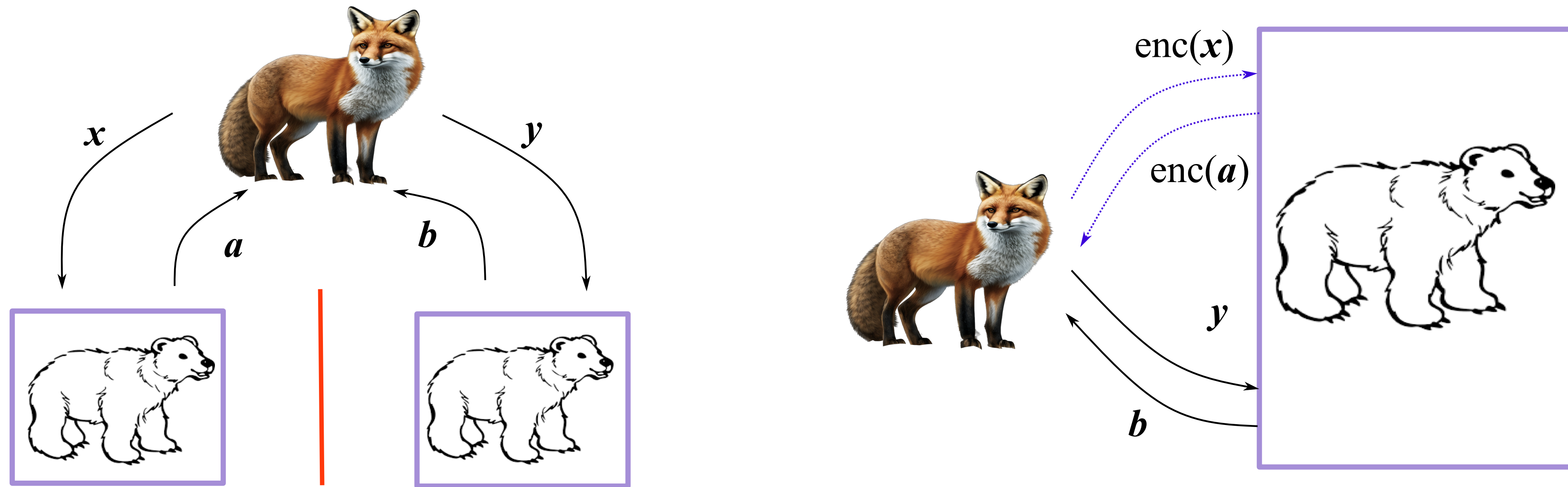
Quantum homomorphic encryption



- **QPT algorithm:** A quantum algorithm is QPT if it can be implemented by a family of quantum circuits with size polynomial in the security parameter κ
- **QHE:** encryption scheme consisting of four QPT algorithms
 1. **Generation** of a secret key from a security parameter
 2. **Encryption** of the input with the secret key, ciphertext obtained
 3. **Evaluation** of a quantum circuit on the ciphertext
 4. **Decryption** of the output of the evaluation with the secret key

Compiled nonlocal games

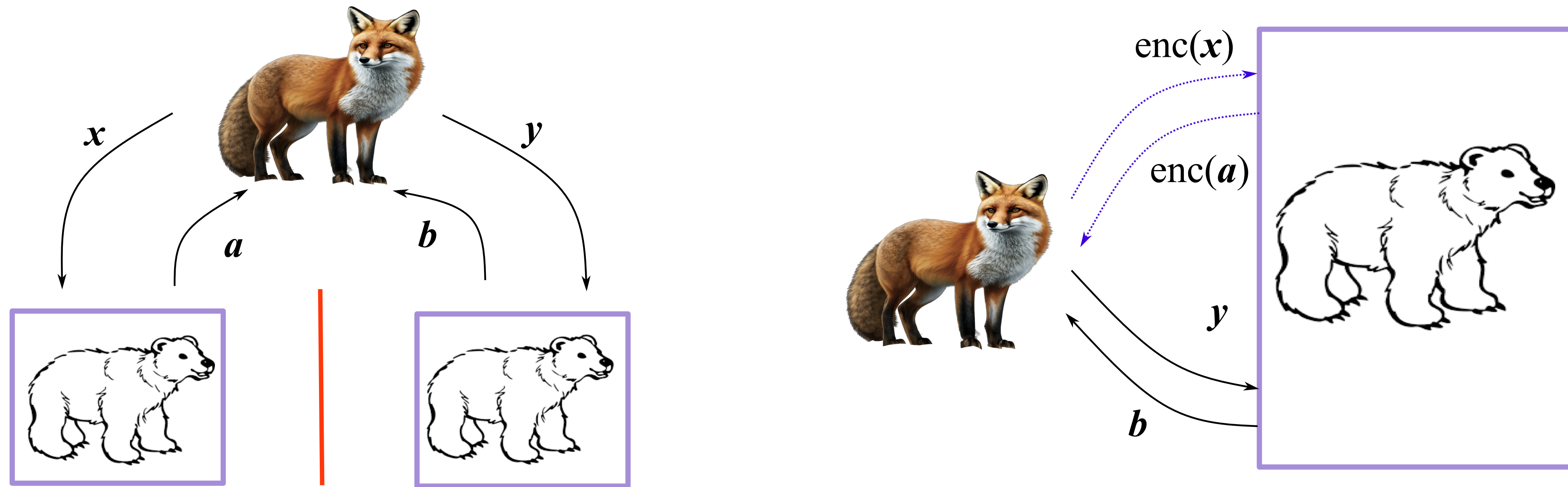
Kalai, Lombardi, Vaikuntanathan, Yang; STOC23



- Round 1: sample “Alice’s” input x and use the secret key sk to obtain encrypted input c , which is sent to the prover. The prover returns encrypted output α
- Round 2: sample “Bob’s” input y and send it to the prover in clear. The prover returns output b
- Verifier uses sk to get $a = \text{dec}(\alpha)$, and checks whether the game winning condition $V(x, y, a, b)$ is satisfied

Compiled nonlocal games

Kalai, Lombardi, Vaikuntanathan, Yang; STOC23



- IND-CPA security ensures that the prover in the second round knows “nothing” about input x
- The prover has to commit to α (and consequently a) before obtaining the input y
- The security of encryption **and** the sequential nature of the protocol ensure the preservation of the local bound

Progress with compiled nonlocal games

- KLVY compiling preserves the local bound
- The quantum bound of a compiled game is lower bounded by the quantum bound of the original nonlocal game

Kalai, Lombardi, Vaikuntanathan, Yang; STOC23

- The quantum bound of the compiled CHSH game is preserved

*Natarajan, Zhang; IEEE FOCS 2023
Brakerski, Gheorghiou, Kahanamoku-Meyer,
Porat, Vidick; arXiv 2023*

- The quantum bound of the compiled Magic square game is preserved

*Cui, Malavolta, Mehta, Natarajan, Paddock,
Schmidt, Walter, Zhang; arXiv 2024*

Our results

Baroni, Vu, Bourdoncle, Diamanti, Markham, IŠ; arXiv:2403.05502

- Compiled XOR games preserve the quantum bound!
- XOR games: $V(x, y, a, b) = \begin{cases} 1, & \text{if } a \oplus b = f(x, y) \\ 0, & \text{otherwise} \end{cases}$
- Compiled d-CHSH games [*Salavrakos, Augusiak, Tura, Wittek, Acin, Pironio; PRL2017*]
- d-CHSH games are a generalisation of the CHSH, 2 inputs per party, d outputs
- Self-testing of any qubit observable in the setting of compiled nonlocal games
[using a family of Bell inequalities with SOS decomposition provided in *Wooltorton, Brown, and Colbeck, PRL2024*]

More progress and future

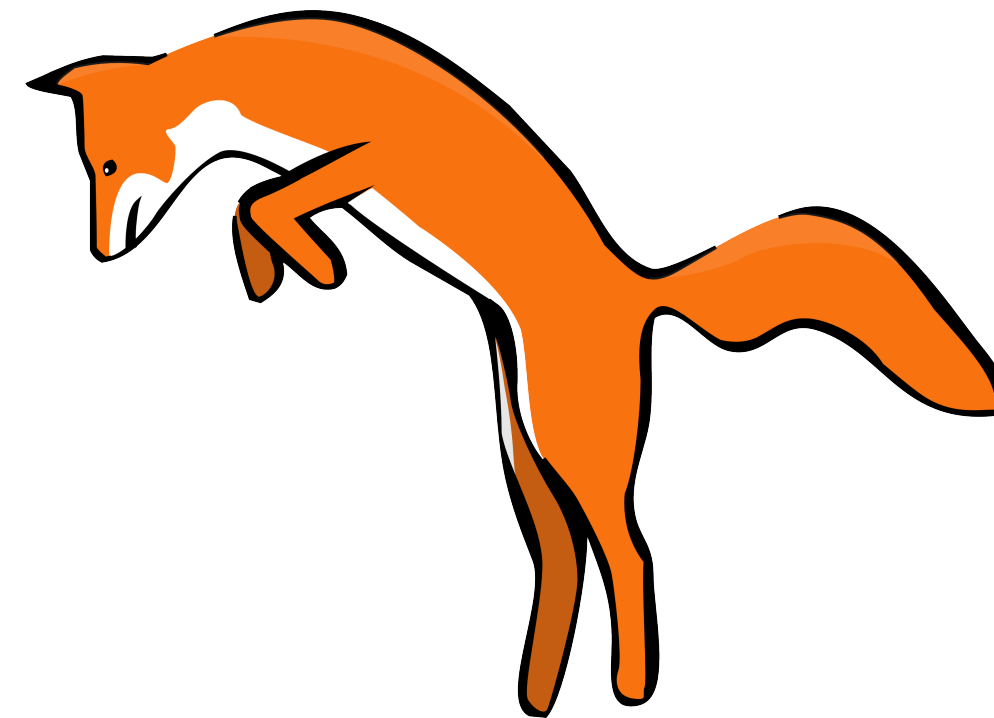
- Self-testing from all compiled XOR games [*Cui, Malavolta, Mehta, Natarajan, Paddock, Schmidt, Walter, Zhang; arXiv 2024*]

More progress and future

- Self-testing from all compiled XOR games [*Cui, Malavolta, Mehta, Natarajan, Paddock, Schmidt, Walter, Zhang; arXiv 2024*]
- Very recent: The quantum bound of all compiled nonlocal games is upper bounded by the quantum bound in the commuting operator model [*Kulpe, Malavolta, Paddock, Schmidt, Walter, arXiv August 2024*]

More progress and future

- Self-testing from all compiled XOR games [*Cui, Malavolta, Mehta, Natarajan, Paddock, Schmidt, Walter, Zhang; arXiv 2024*]
- Very recent: The quantum bound of all compiled nonlocal games is upper bounded by the quantum bound in the commuting operator model [*Kulpe, Malavolta, Paddock, Schmidt, Walter, arXiv August 2024*]



Encryption instead of locality

Recap

- Secure encryption can be used to simulate the locality condition [appropriate type of security necessary]
- The protocol becomes sequential
- Encryption must be fully homomorphic
- Compiling multipartite nonlocal games ?

Self-testing graph states permitting bounded classical communication

arXiv:2404.03496

U. I. Meyer



F. Grosshans

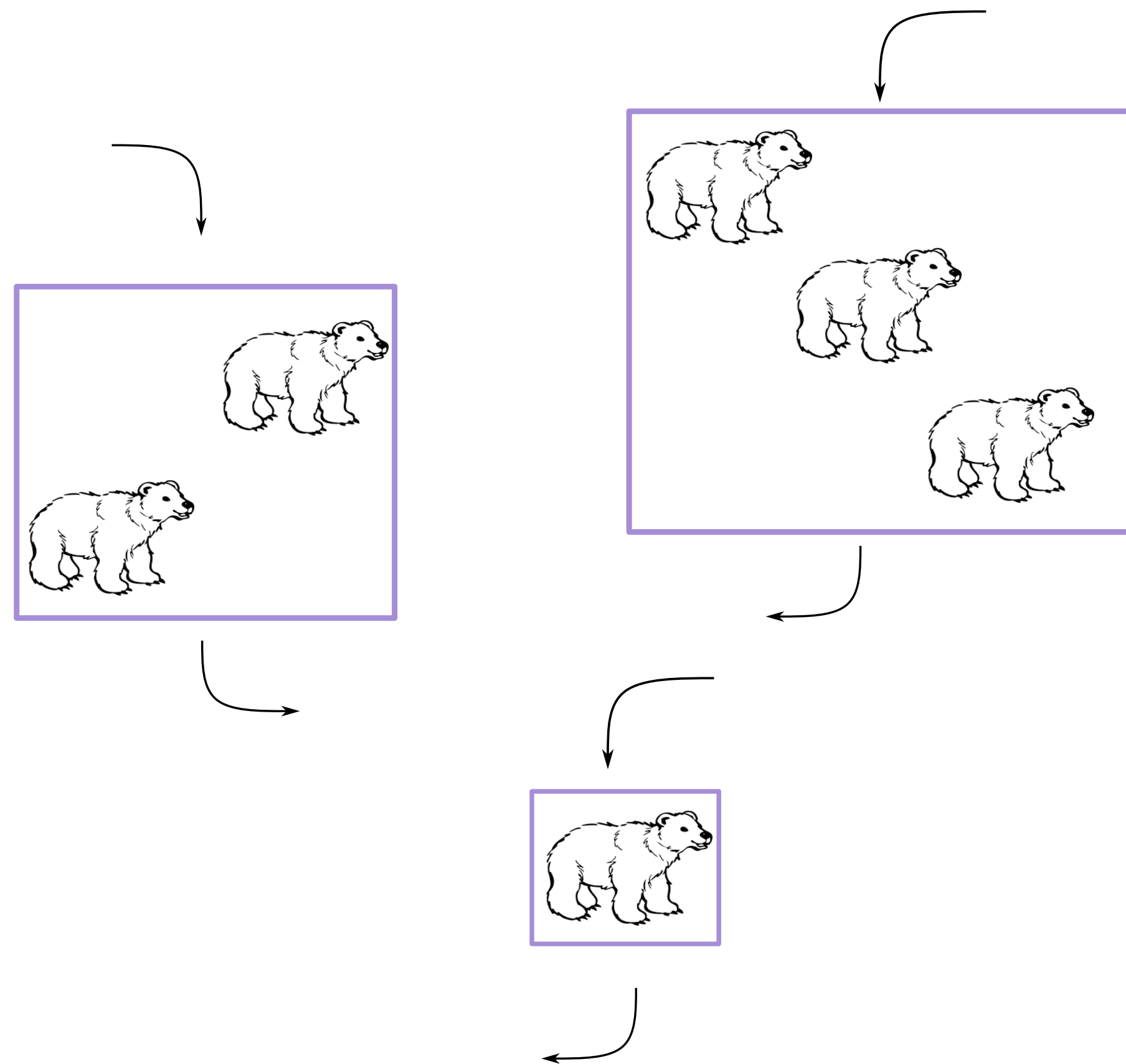


D. Markham



Bell nonlocality with communication

What if no-signalling cannot be ensured?

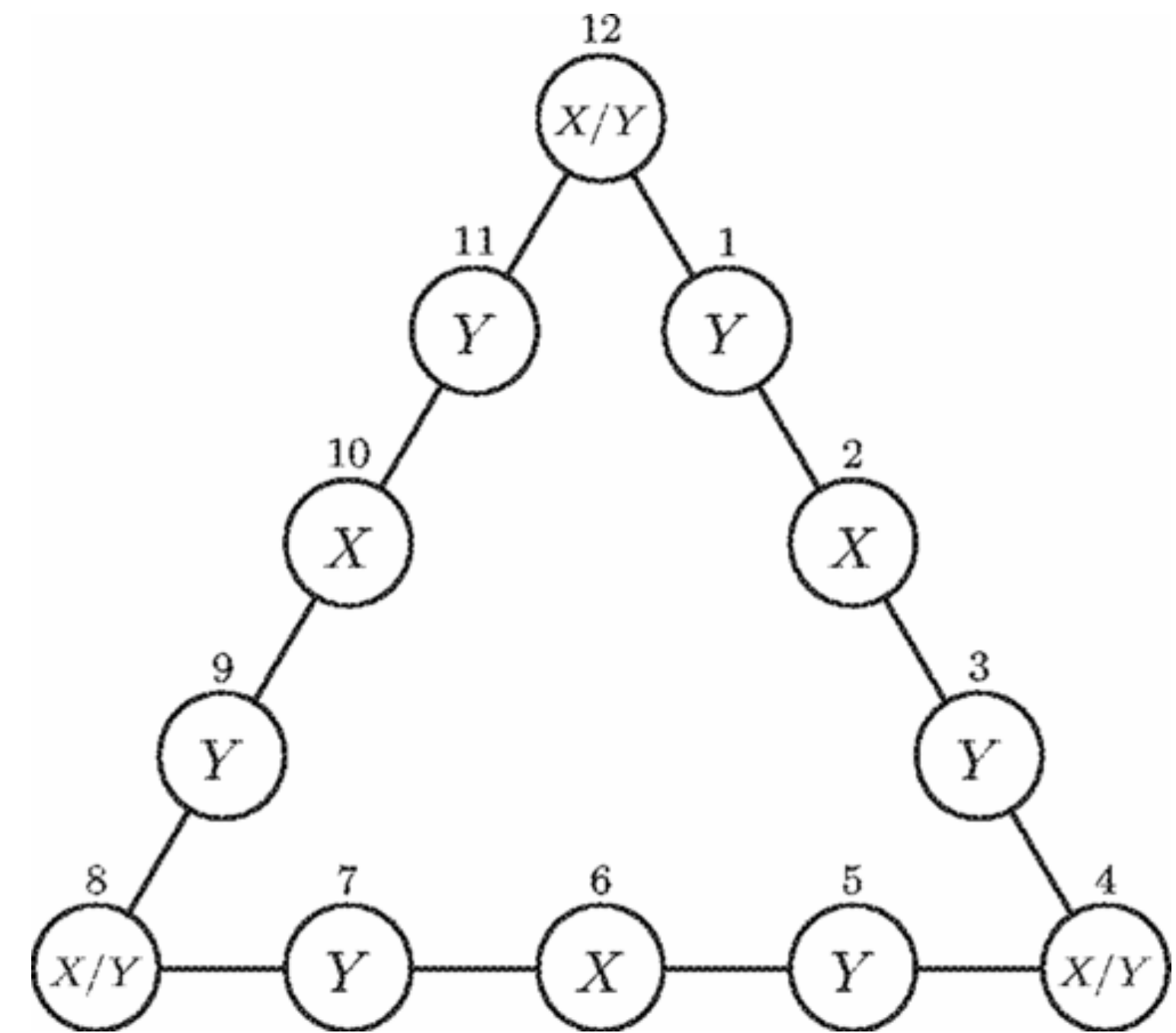
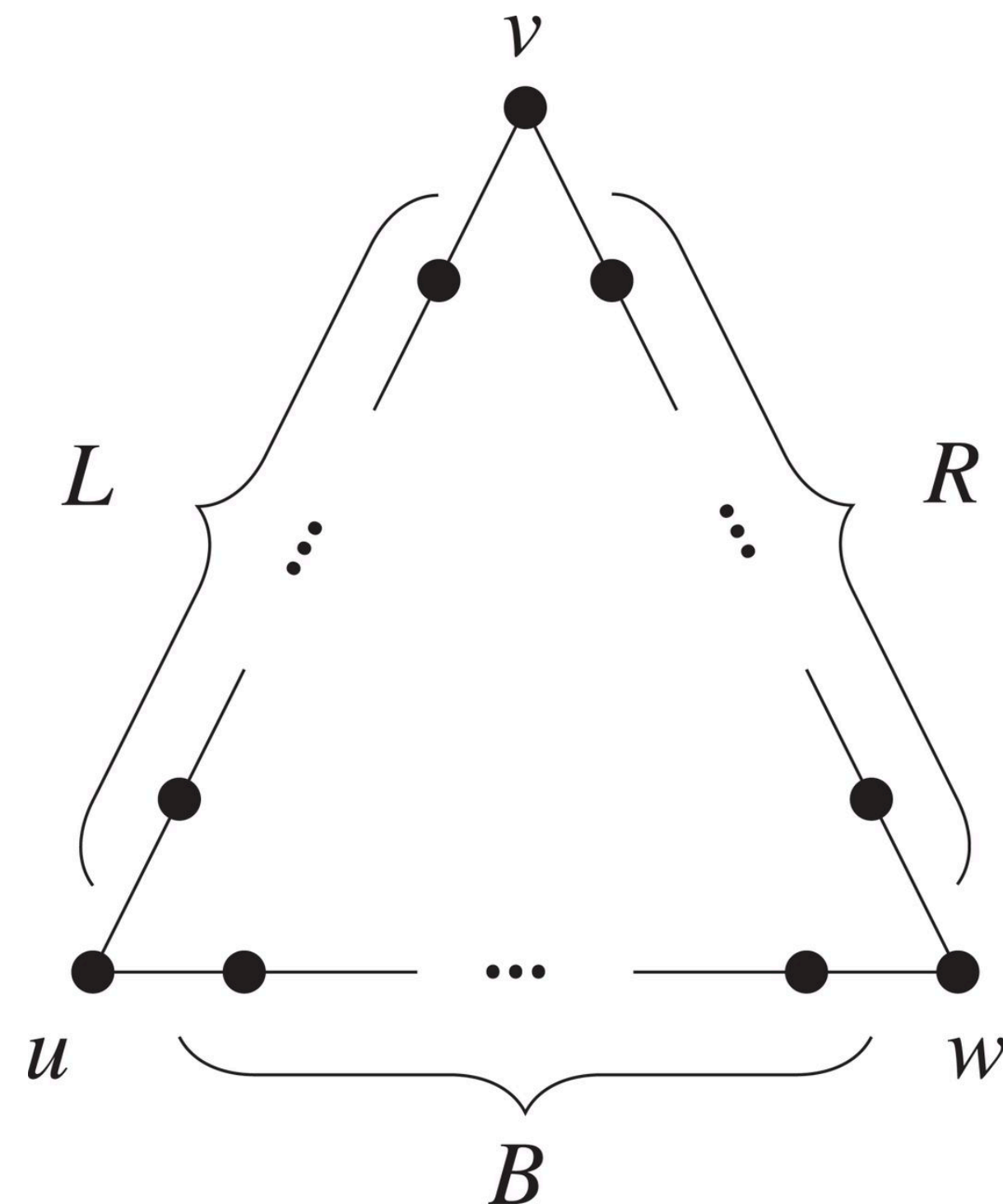


- Locality loophole in Bell experiments
- Integrated photonics experiments
- Colluding parties

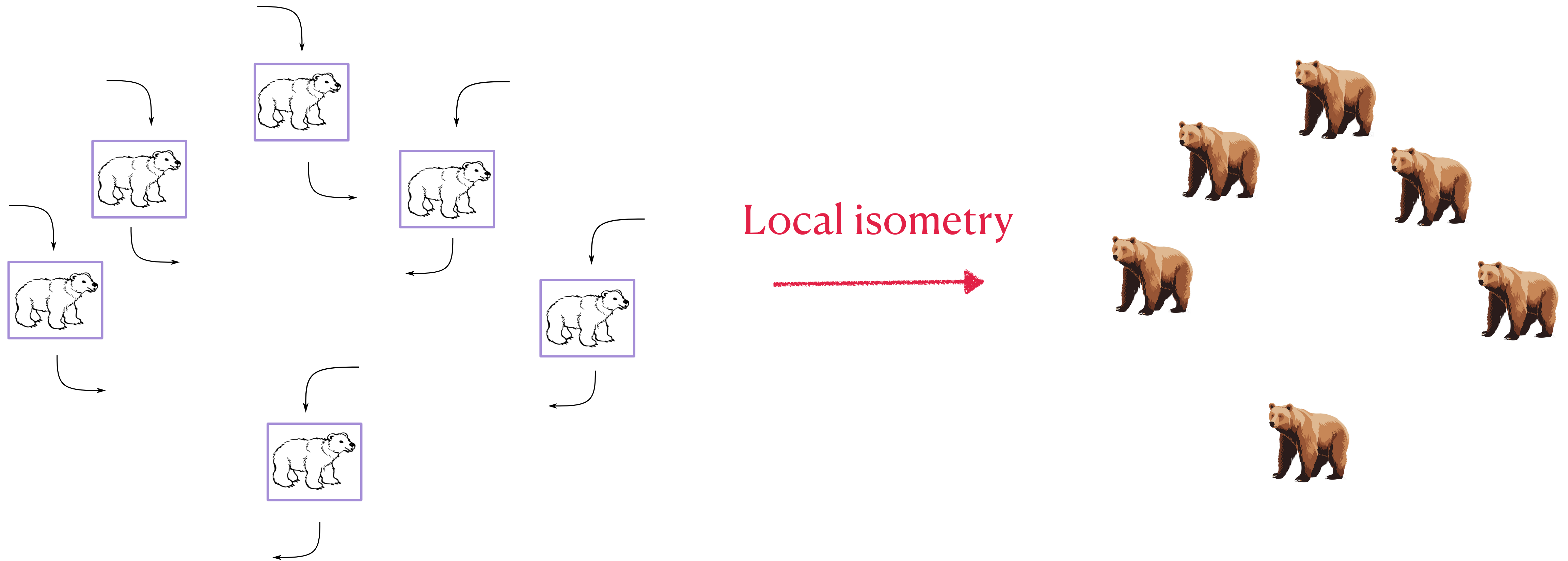
Computational motivation

Quantum advantage with shallow circuits!

- Bravyi, Gosset, Koenig (2018)
- Barrett, Caves, Eastin, Elliott, Pironio (2007)

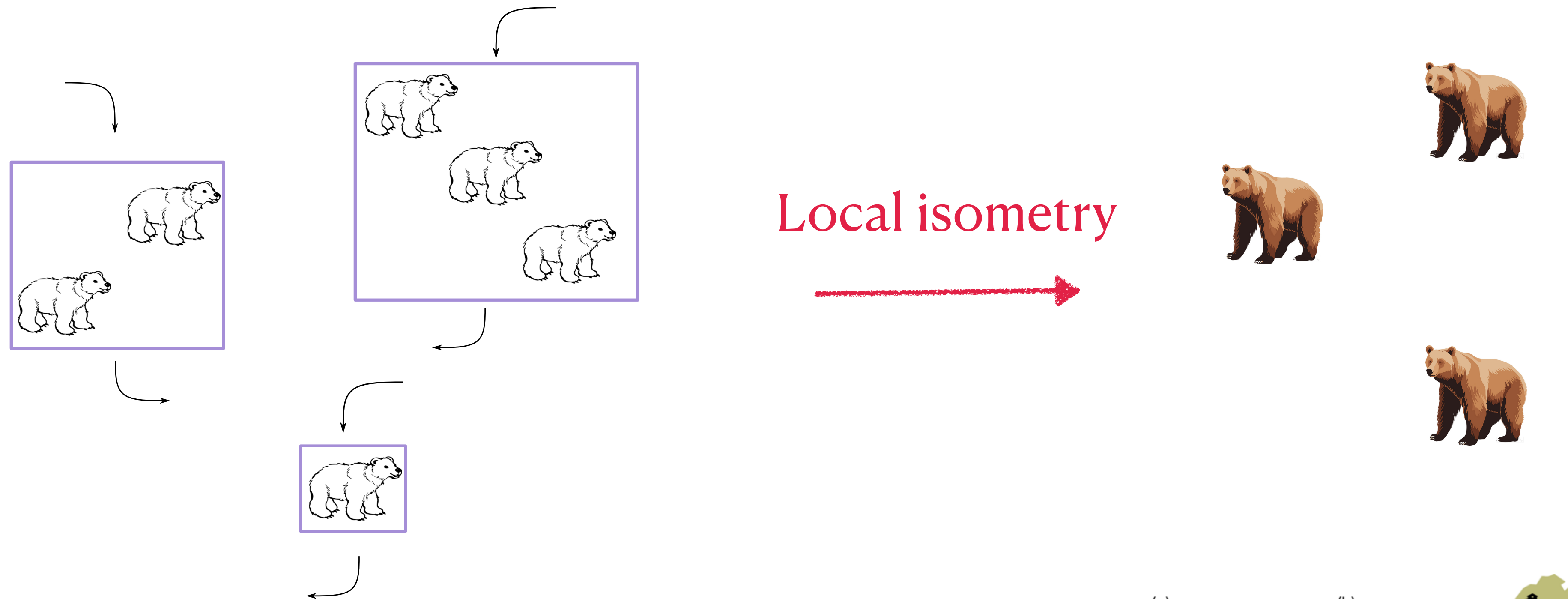


Self-testing with communication



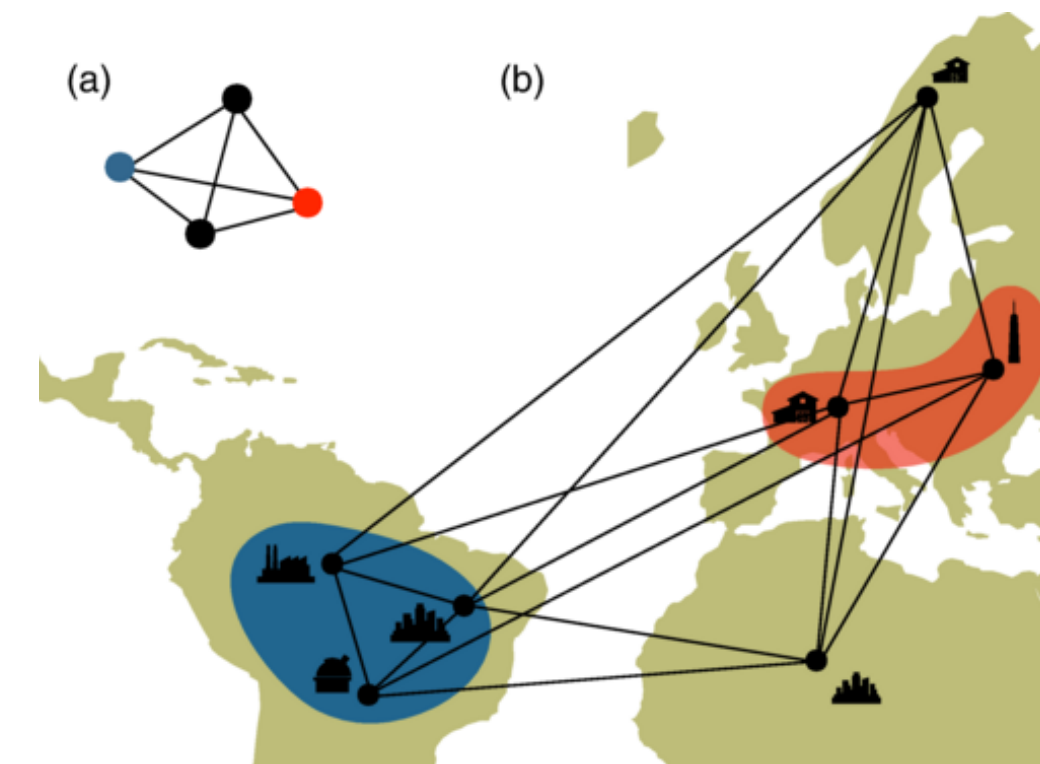
Self-testing with communication

- Intuition: Classical communication destroys nonlocality



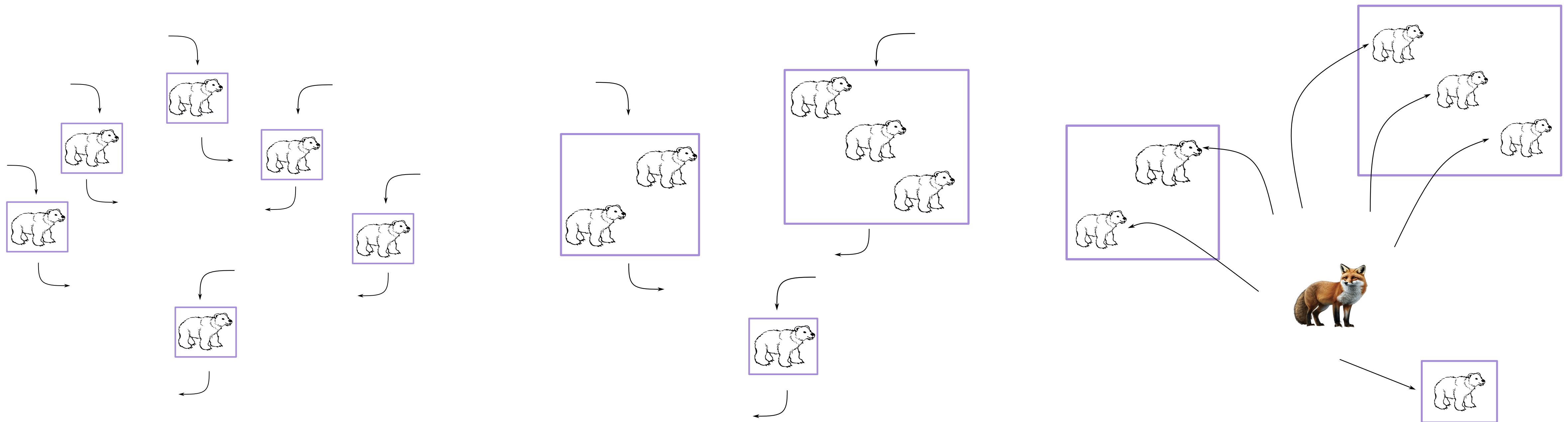
Self-Testing with Dishonest Parties and Device-Independent Entanglement Certification in Quantum Communication Networks

Gláucia Murta and Flavio Baccari
Phys. Rev. Lett. **131**, 140201 – Published 3 October 2023

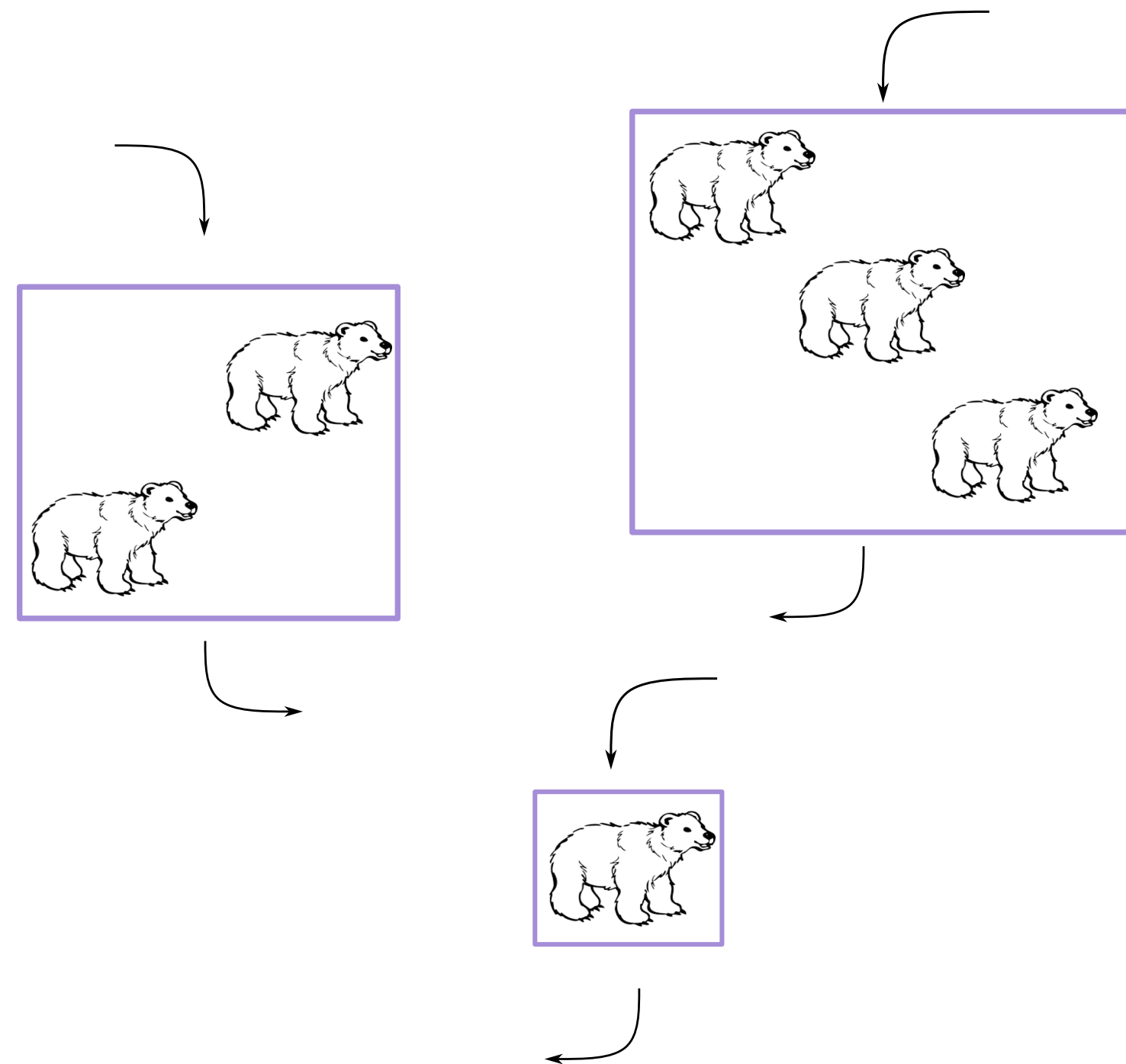


Self-testing with communication

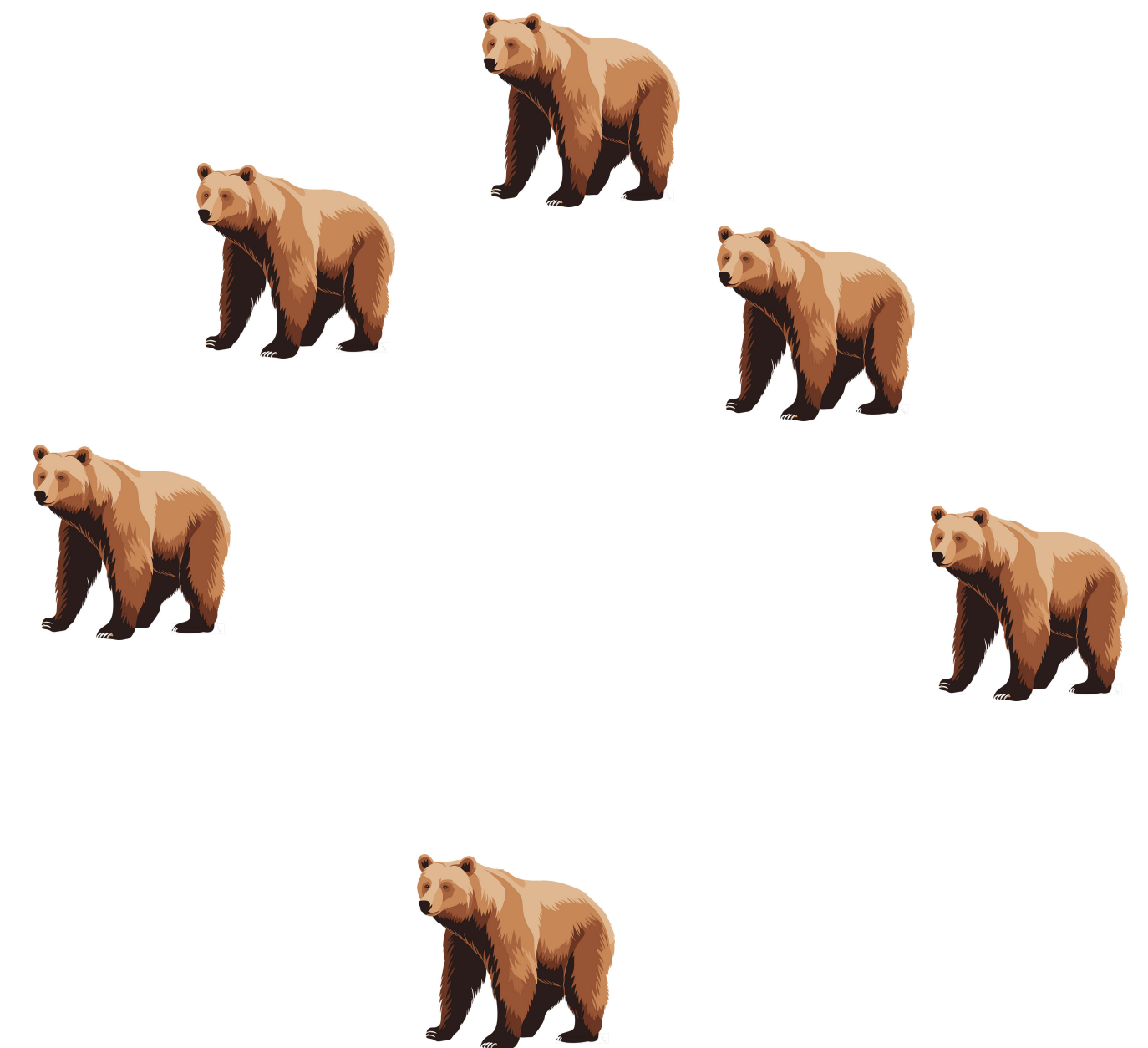
- More intuition: Power of interaction
- Provers cheat by communicating
- Verifier asks questions and does not care about the answer!



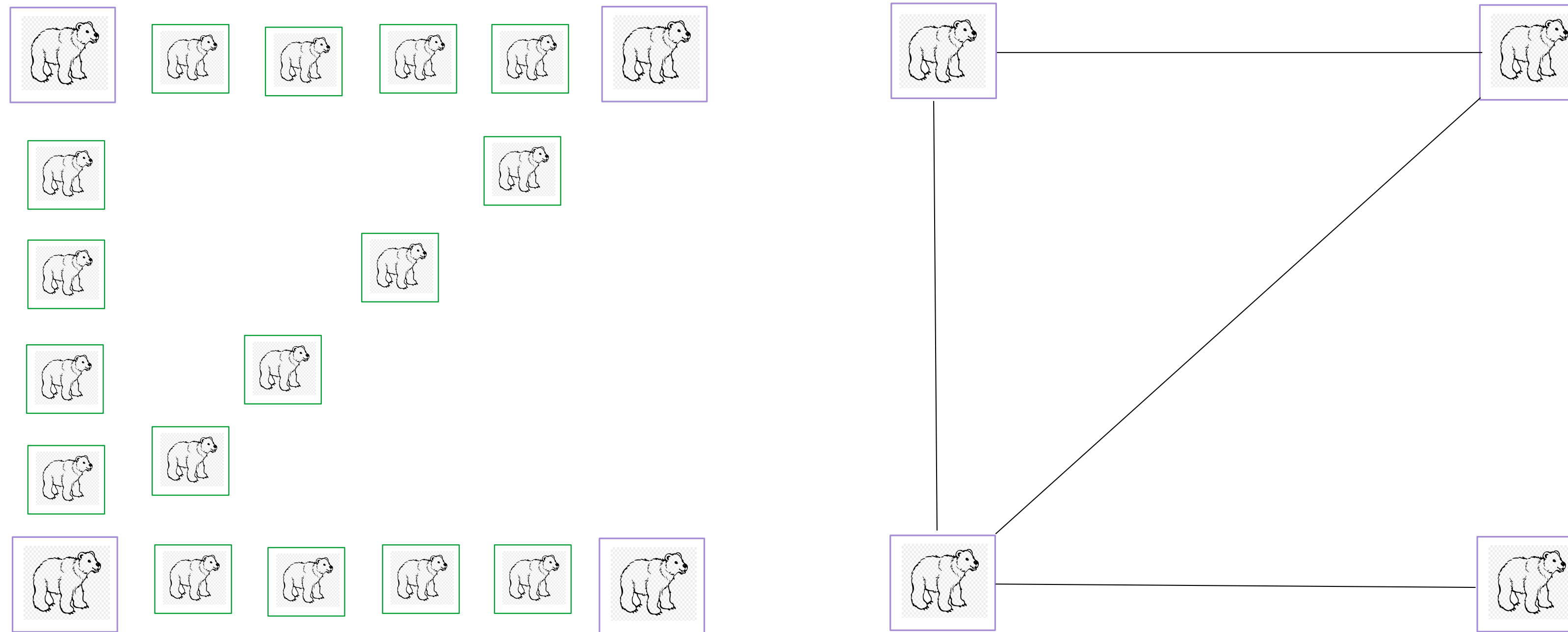
Self-testing with communication



Local isometry

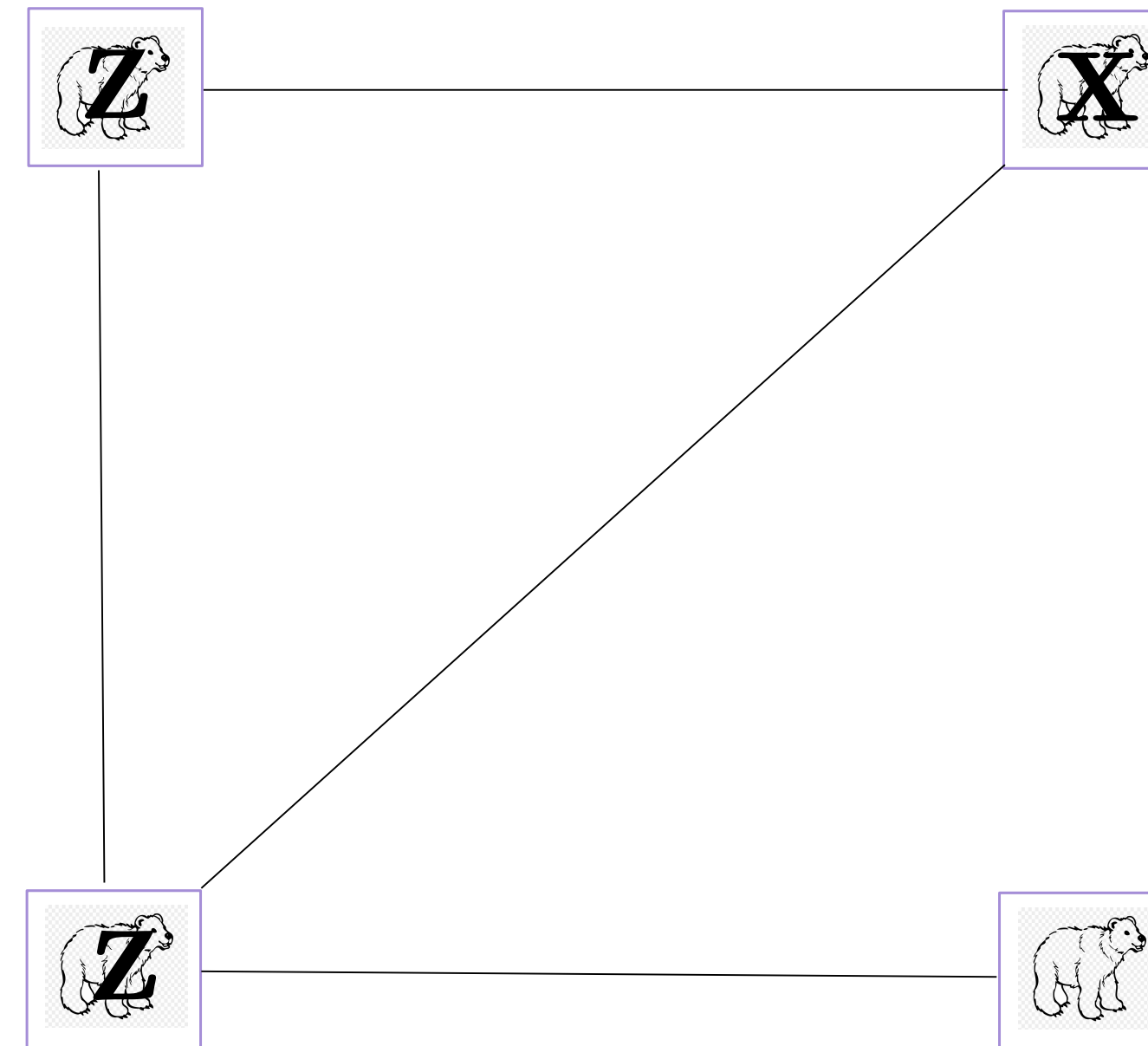
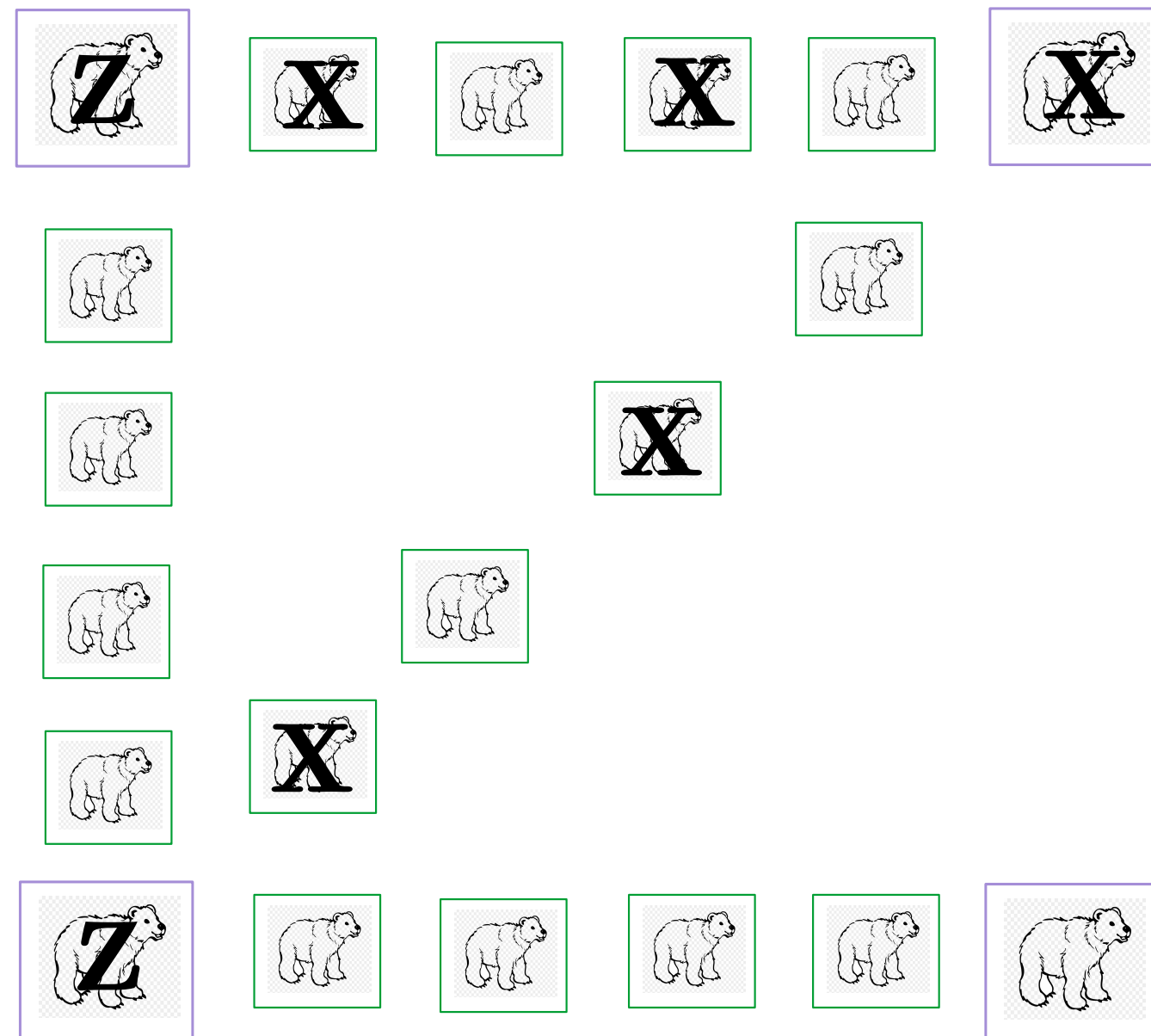


Inflated graph states



Given a graph $G = (V, E)$, its d -inflated graph $G' = (V', E')$ replaces all edges with a connected chain of $2d$ vertices bridging the original edge. The new vertices $V' = V \cup W$ consist of those from the original graph V , referred to as **power** vertices, and the new **chain** vertices $W = \{r(u, v); r = 1, \dots, 2d, (u, v) \in E\}$. The new edges are $(u, 1(u, v)), (1(u, v), 2(u, v)), \dots, ((2d)(u, v), v) \in E'$

Self-testing inflated graph states



Self-testing recipe:

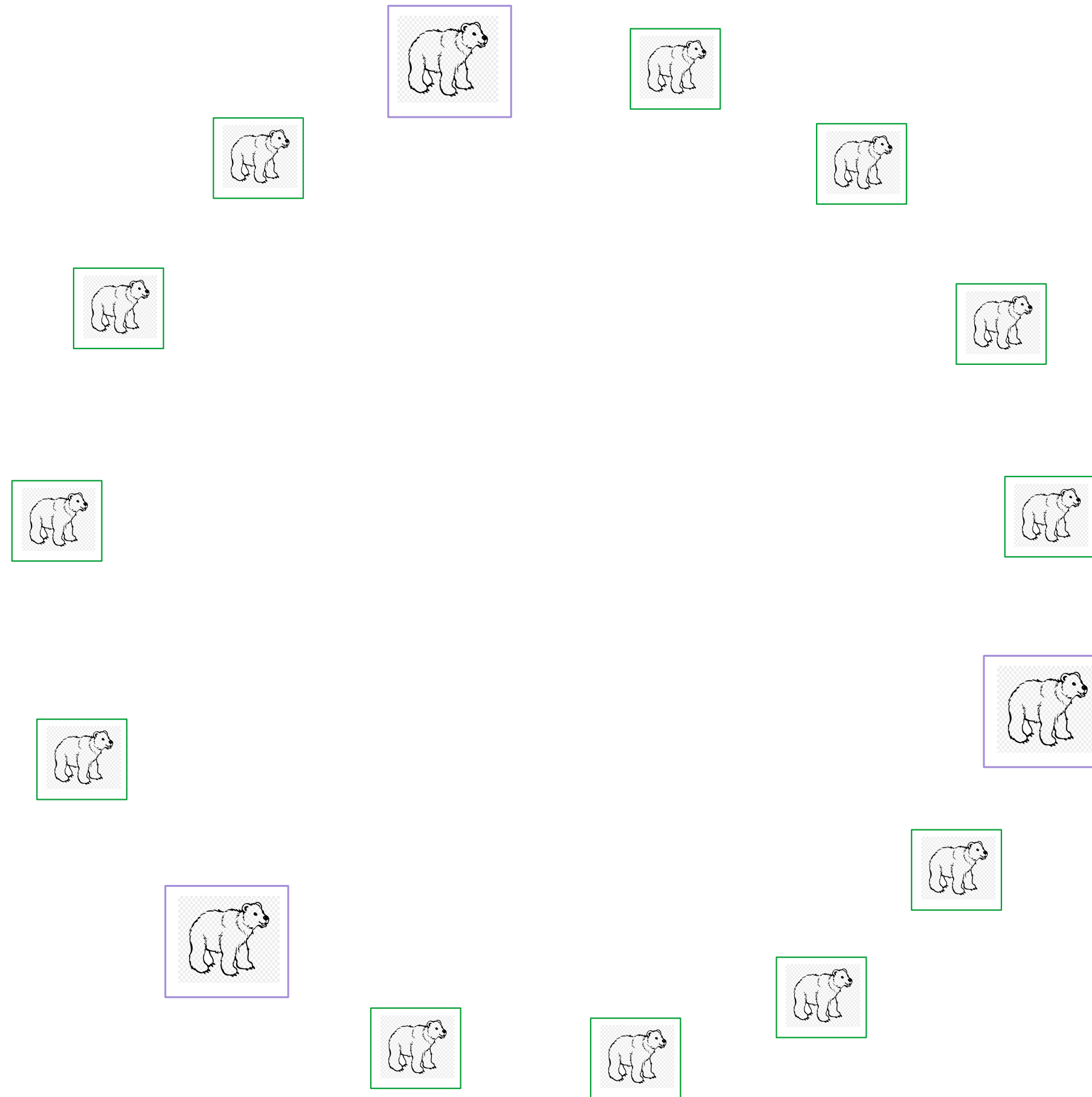
Measure stabilisers of the inflated graph states, containing on chain vertices either X or nothing.

Always **ask** chain vertices to measure X .

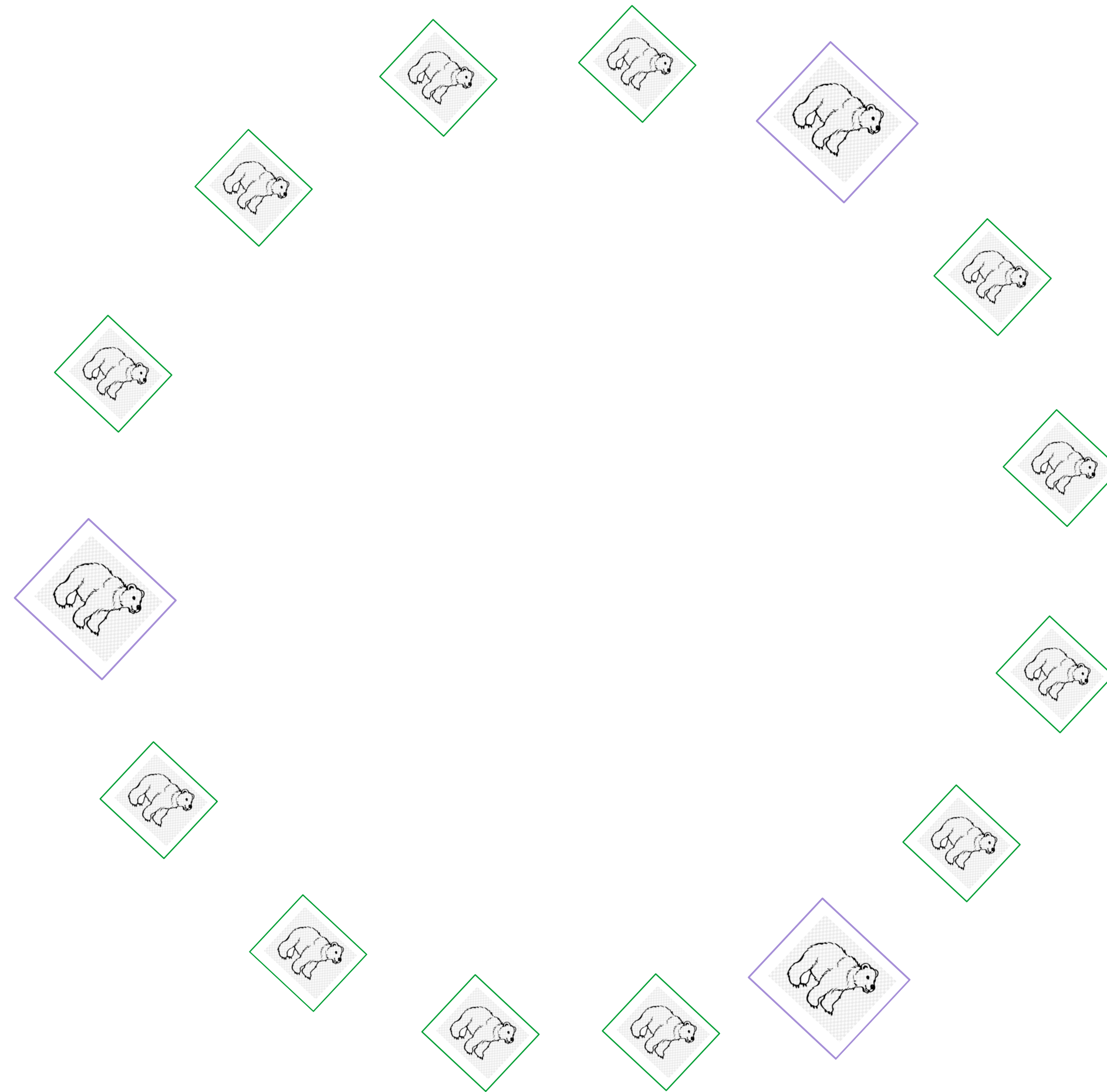
Self-testing statement (informal):

Upon measuring X on all chain vertices, the postmeasured states is locally isometric to the (non-inflated) graph state.

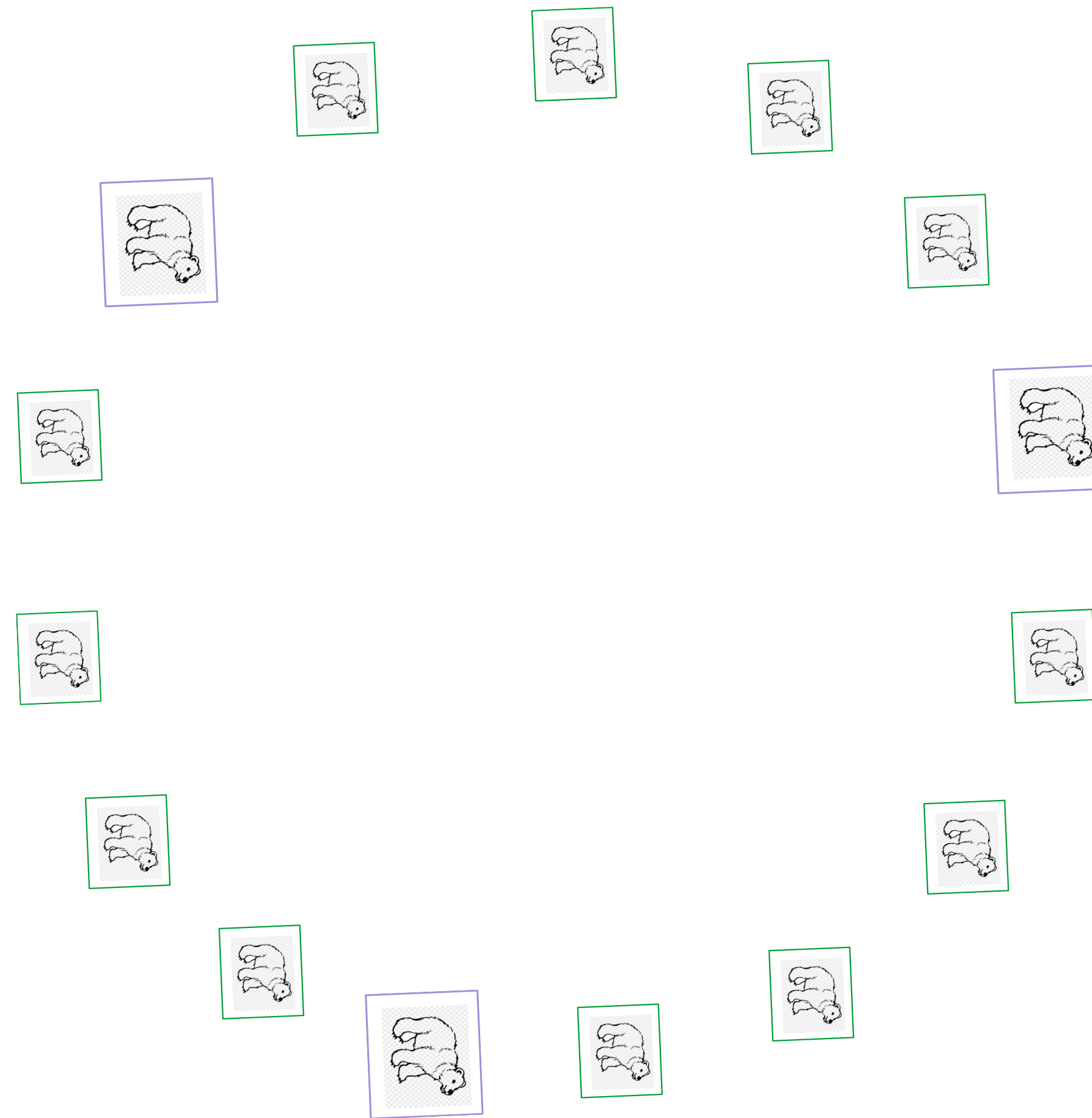
Self-testing the full state with communication



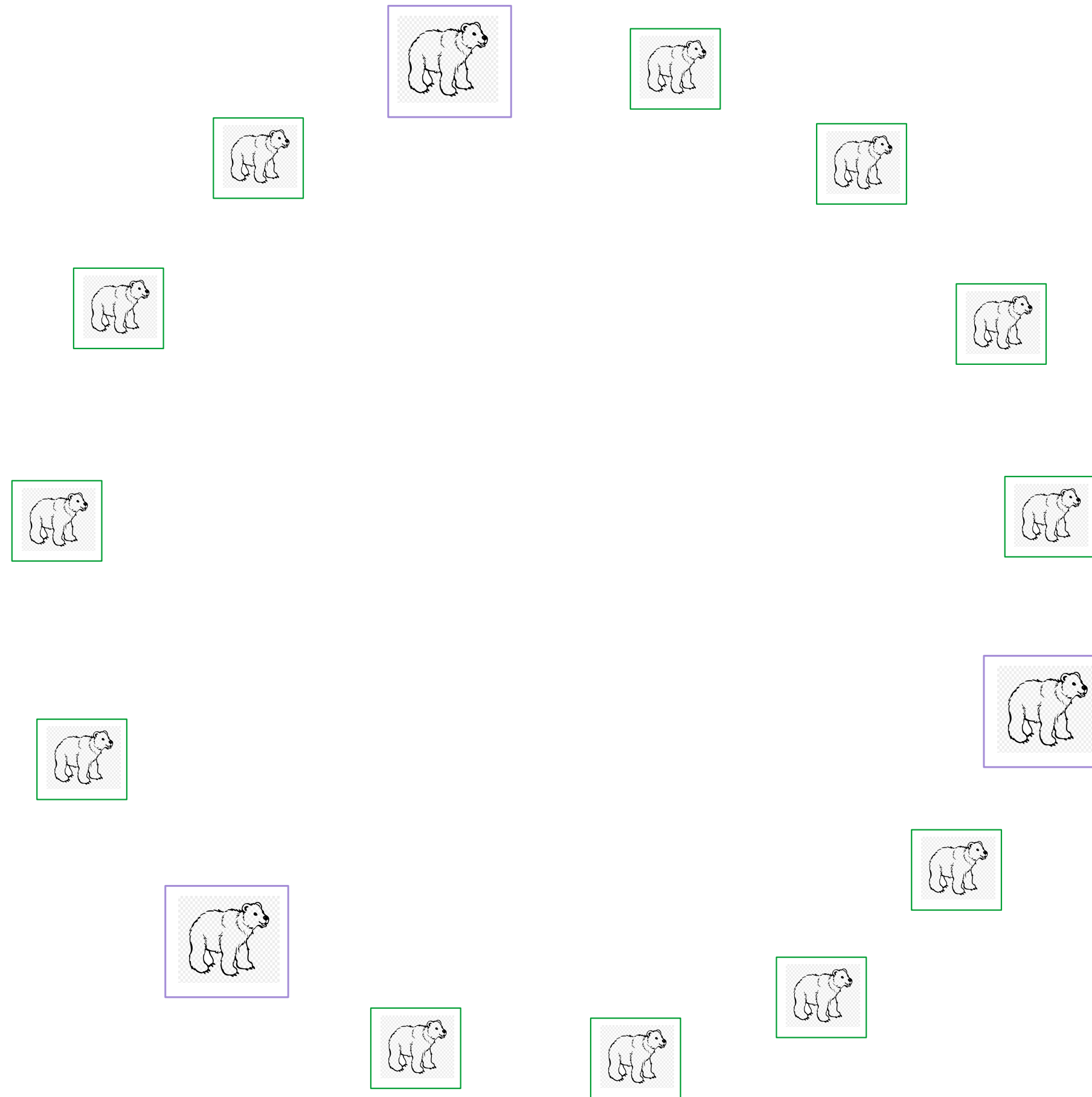
Self-testing the full state with communication



Self-testing the full state with communication



Self-testing the full state with communication



- Repeat self-testing correlations $2d + 1$ times, with every vertex once playing the role of the power vertex

All multipartite qubit states can be self-tested
arXiv:2409.xxxxx

M. Balanzo



A. Coladangelo



R. Augusiak

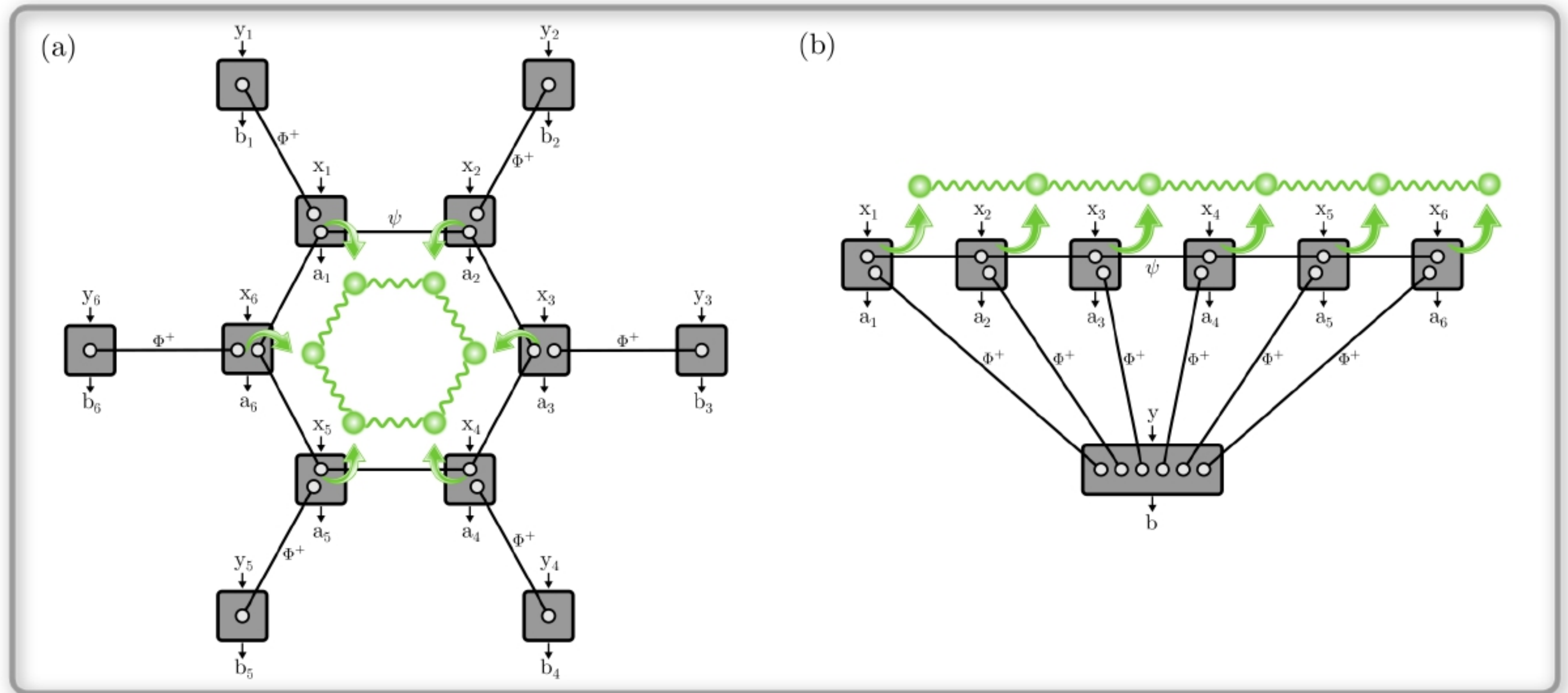


A. Acin

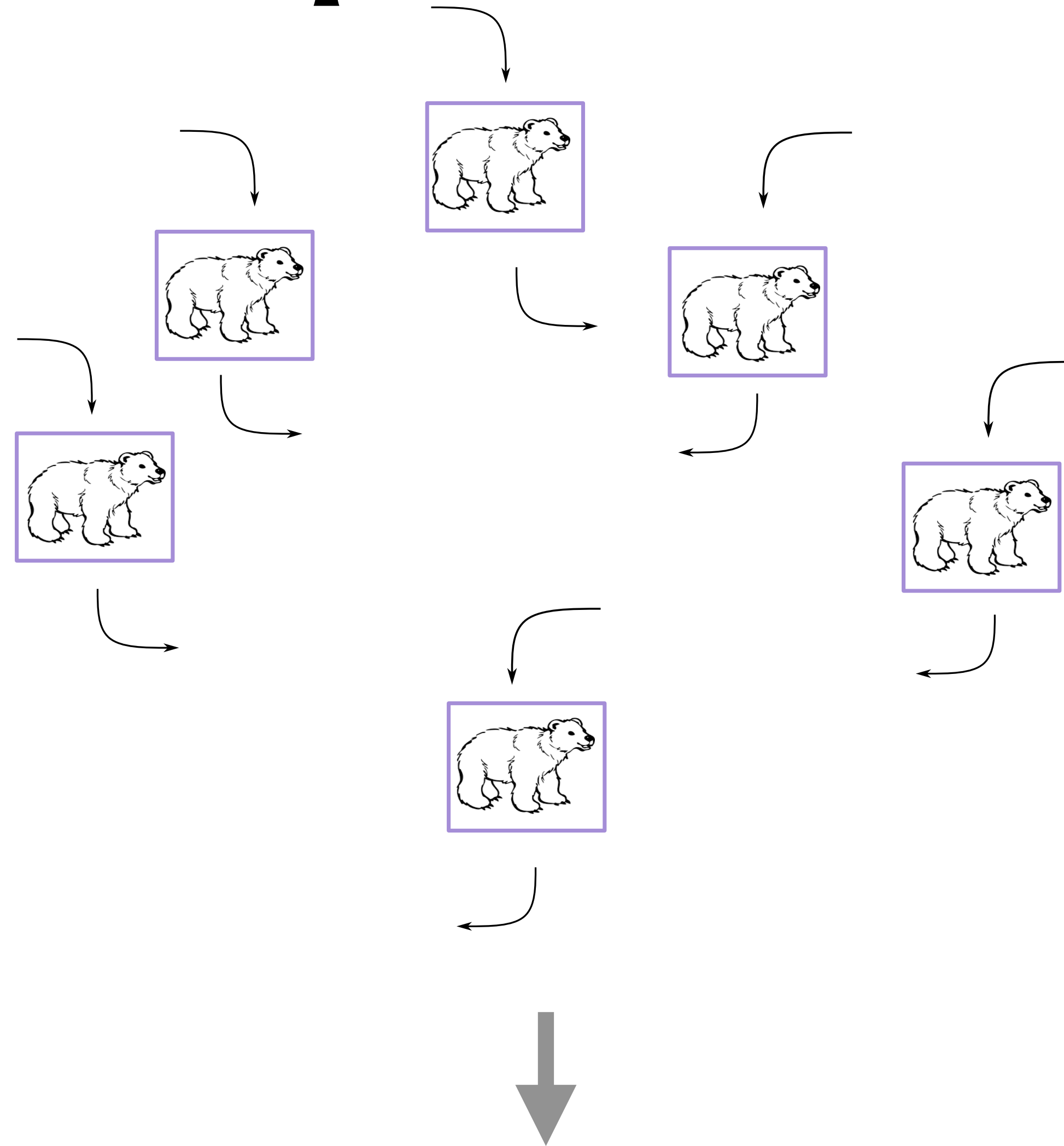


Network self-testing

Quantum networks self-test all entangled states [Šupić, Bowles, Renou, Acín, Hoban, NatPhys2023]



Multipartite states



Correlation $p(a_1, \dots, a_n | x_1 \dots x_n)$

Idea for self-testing

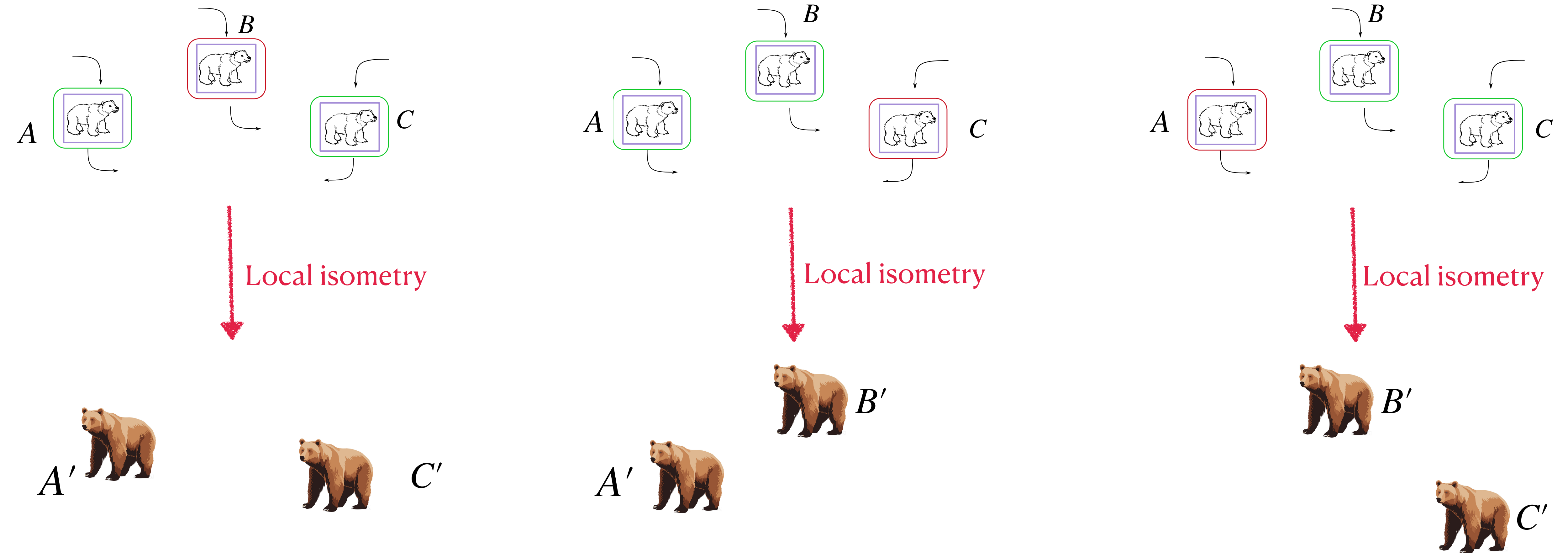
Use successive self-testing of bipartite states for all possible bipartitions
→ different sub-tests.

To do this, project the rest of the parties + assume the bipartite state is entangled*.

Self-test the bipartite entangled state and the measurements.

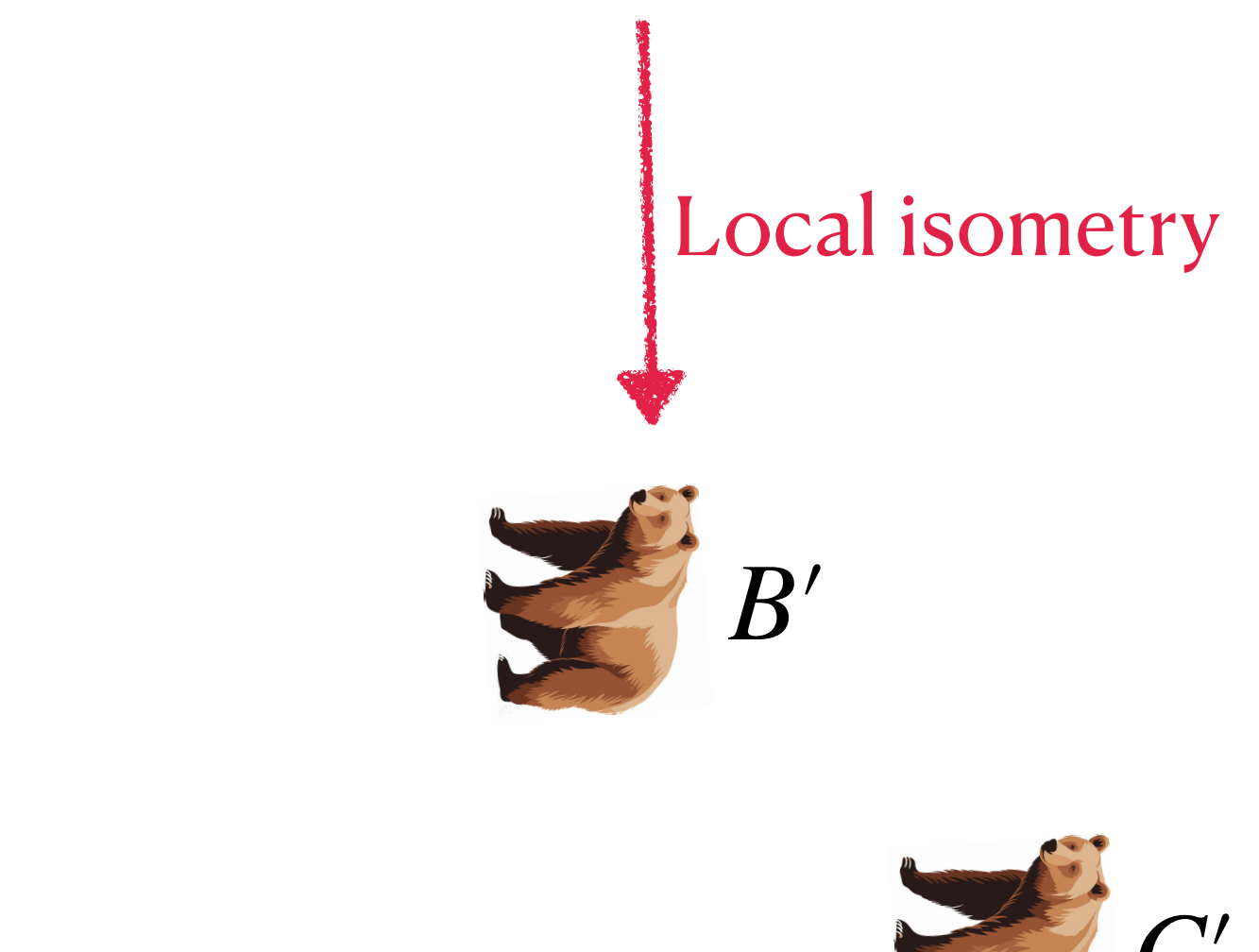
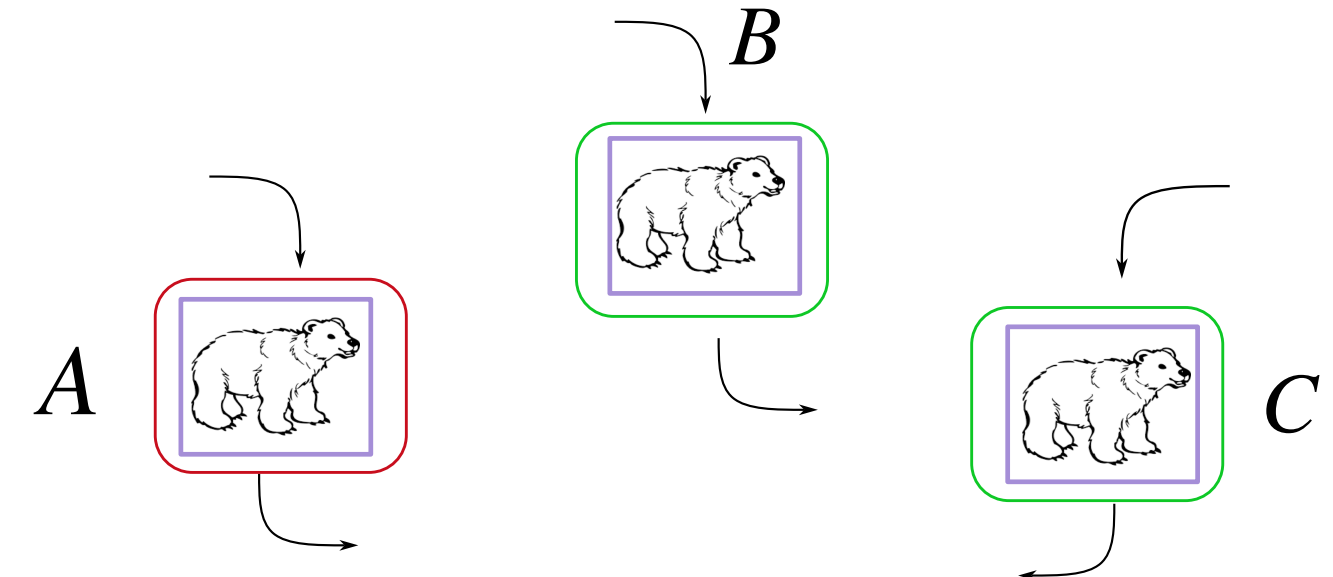
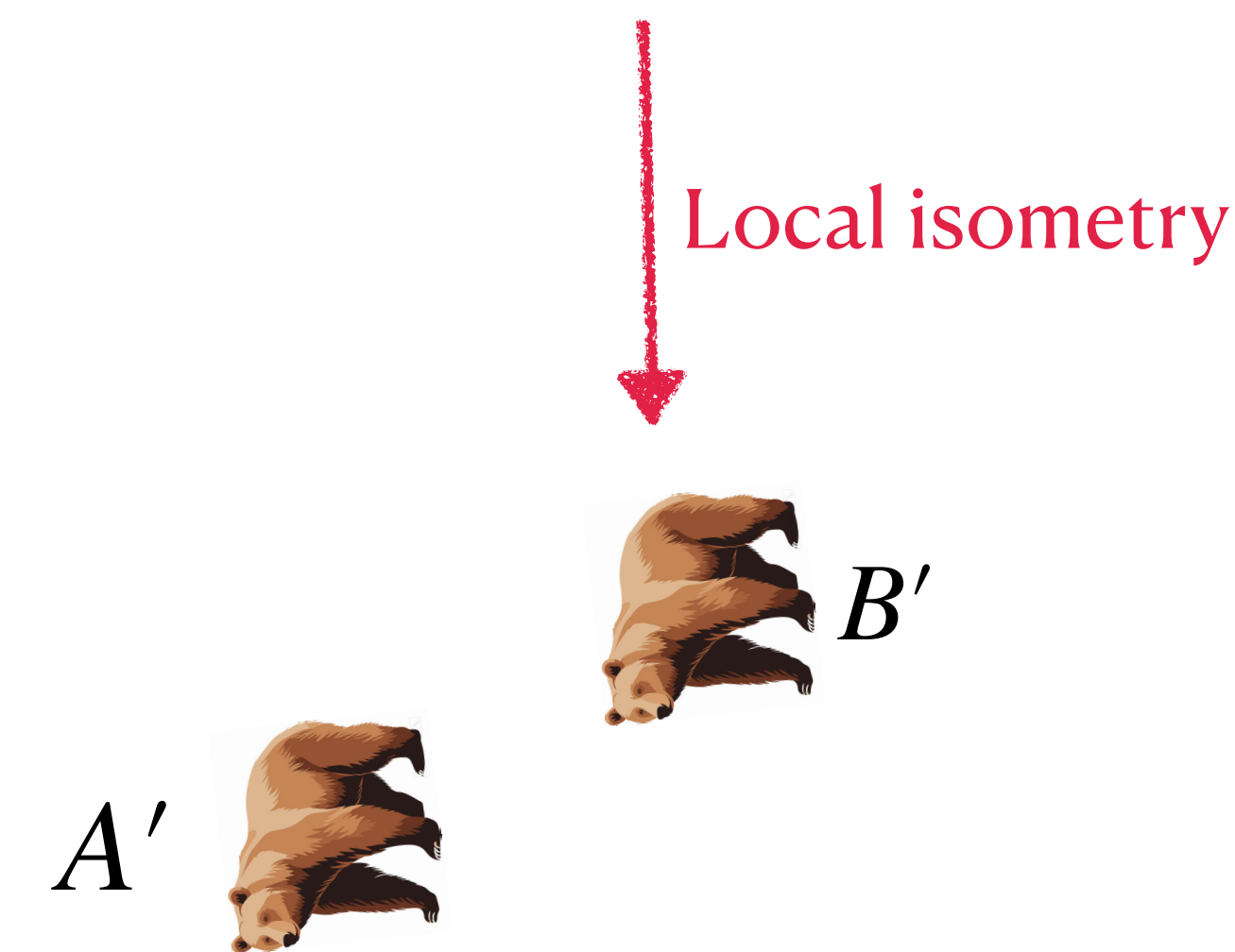
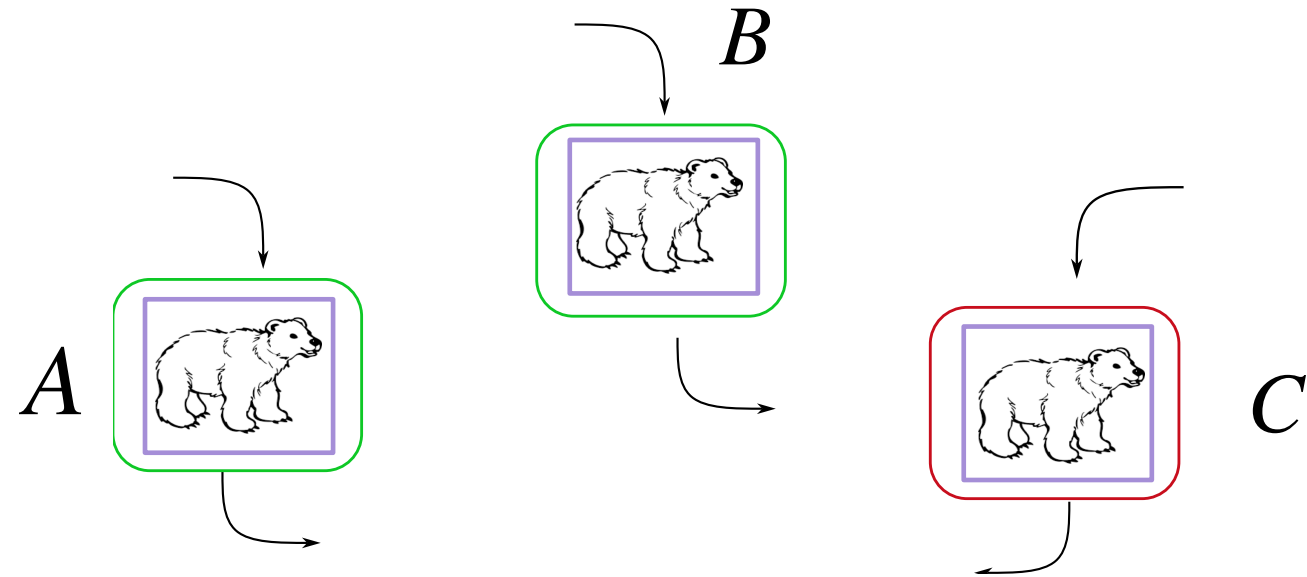
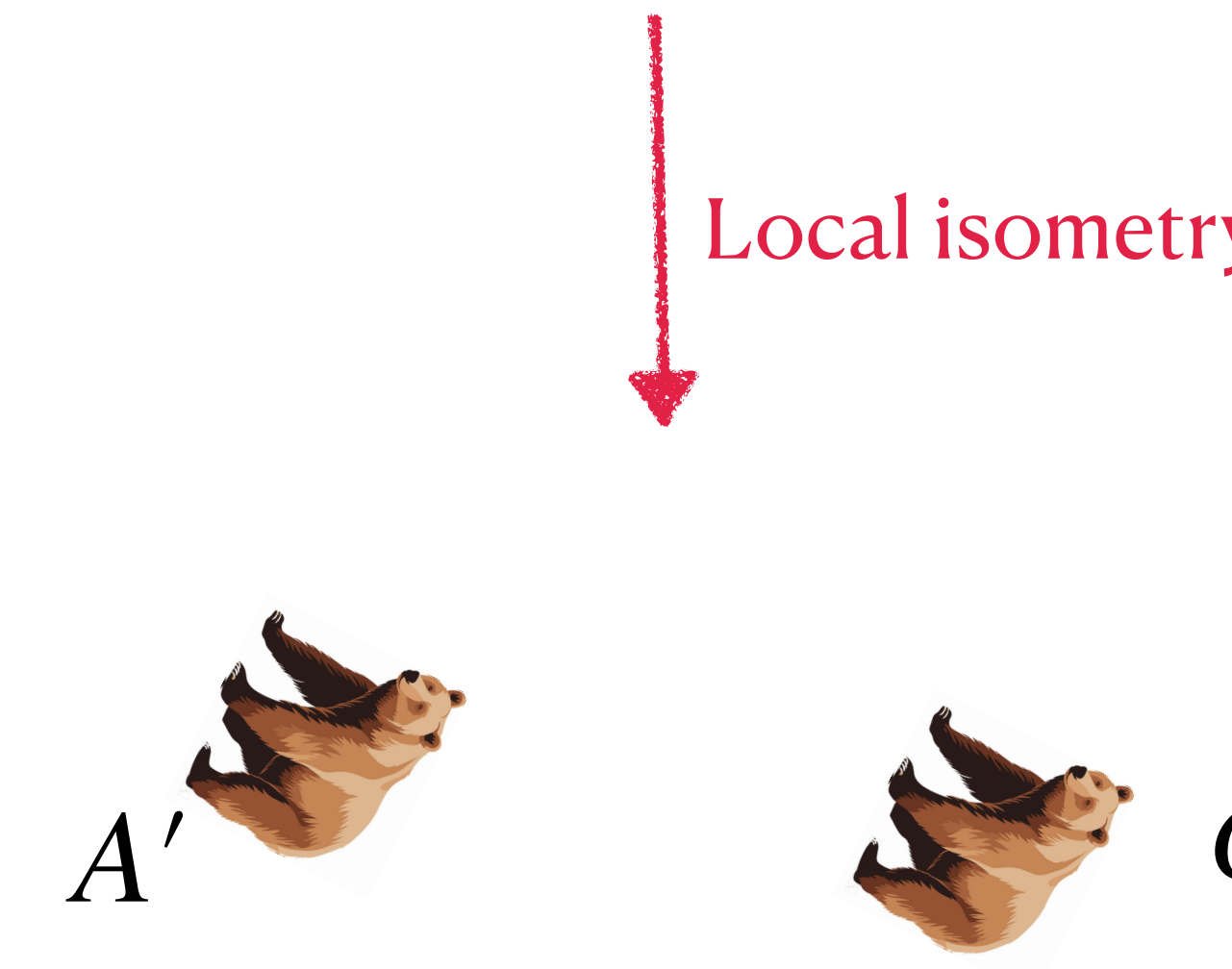
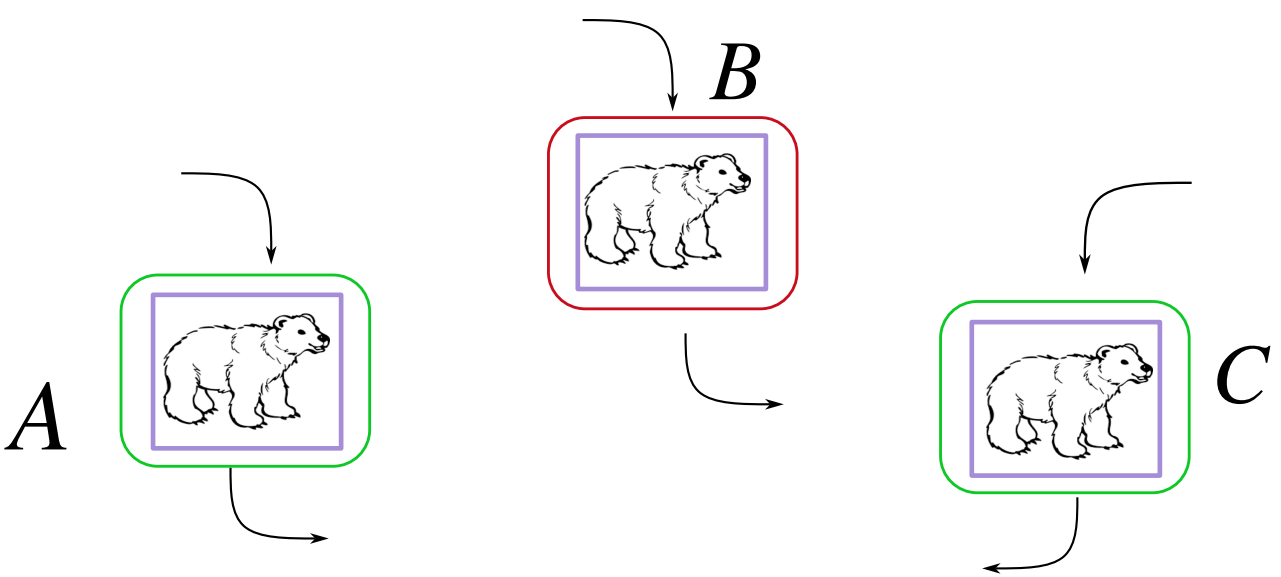
[*] M. Zwerger, W. Dür, J-D. Bancal, and P. Sekatski. PRL, 122(6):060502, (2019).

Idea for self-testing

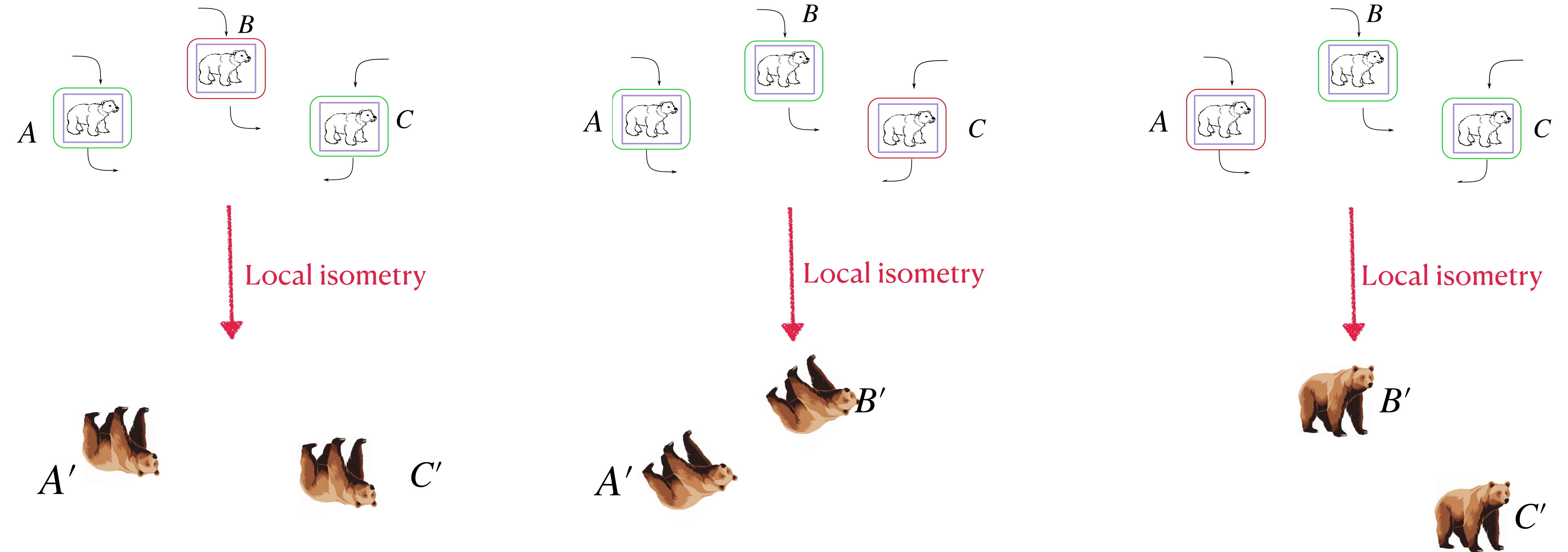


Solve a marginal problem!

Idea for self-testing



Idea for self-testing



Tripartite states

If we knew the bases this marginal problem would be easy to solve, the only state that could pass all the sub-tests would be our target state $\rightarrow$ but we don't know the bases.

How do we combine the three tests and make sure that the six marginal states correspond to the target state?

Need to understand the relation between the measurements the parties use to project and those they use when they are being self-tested.

Tripartite states

Measurement lemma: allowing us to fix a “measurement reference frame”.

Each of the measurements used to project are also self-tested: reveals the relation between measurements used to self-test and measurements used to project, or ensuring that they are related in the way we expect.

Tripartite states

Final statement

In the end, we are able to certify that

$$|\psi\rangle_{ABCP} = |\psi\rangle_{A'B'C'} \otimes |\phi^+\rangle_{A''B''C''P} + |\psi^*\rangle_{A'B'C'} \otimes |\phi^-\rangle_{A''B''C''P}$$

$$|\psi\rangle = \sum_{ijk} \lambda_{ijk} |ijk\rangle$$

LU-equivalent to its
complex conjugate

$\implies$ It is possible to self-test every pure entangled state of 3 qubits locally
unitarily equivalent to its complex conjugate