

Computational certificates of quantumness

Ivan Šupić

Berlin, 14.05.2024.

Quantum bounds for compiled XOR and d -outcome CHSH games

arXiv: 2403.05502



Matilde Baroni

Quoc Huy Vu



Boris Bourdoncle

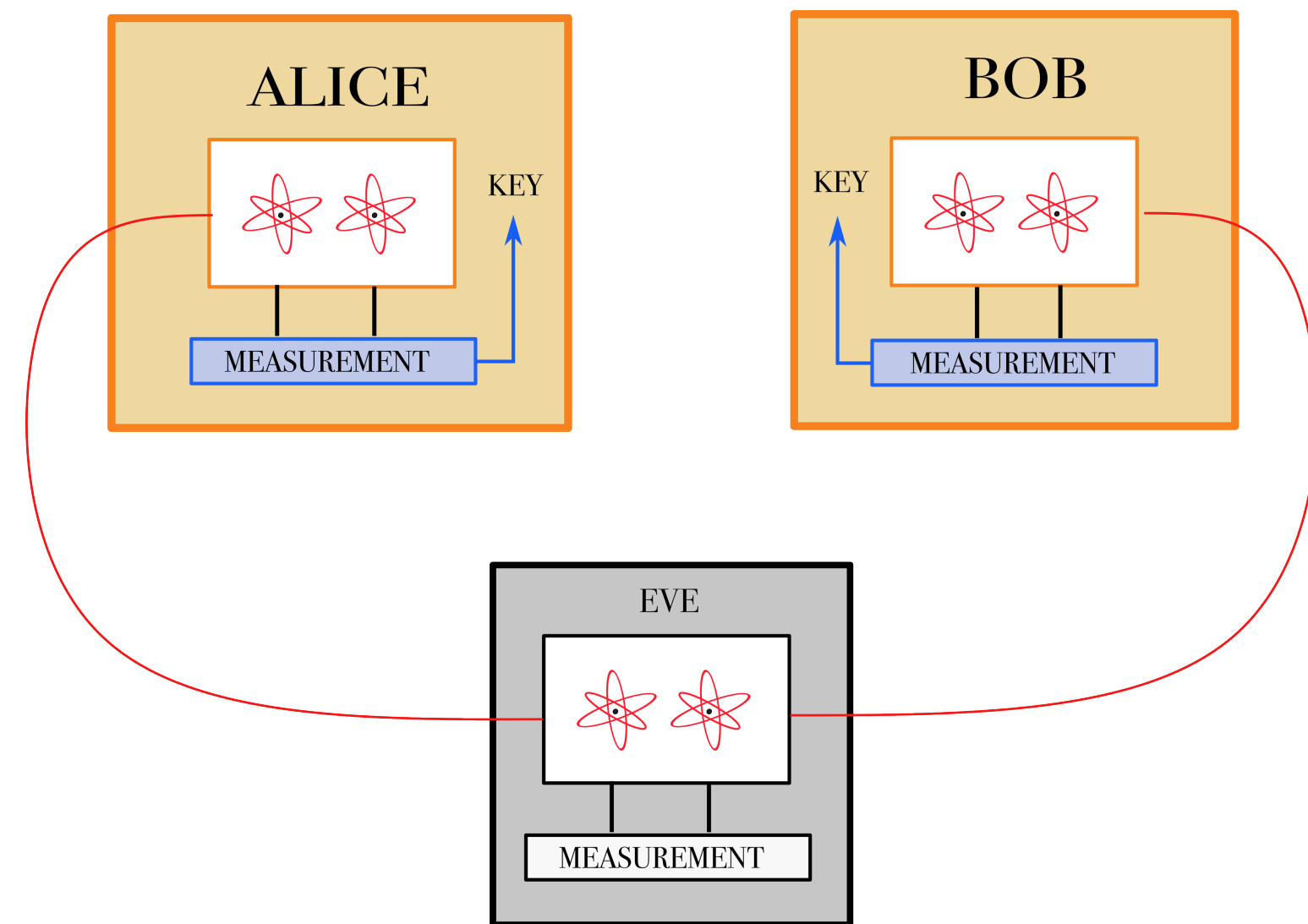


Eleni Diamanti



Damian Markham

Nonlocality & information-theoretic security



Nonlocality necessary for key in DIQKD

Self-testing - powerful tool for DI quantum certification

Condition: spatial separation!

Can we trade spatial separation for something else ?

Hint: post-quantum cryptography!

Nonlocal games

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

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

$$x \in \{0, 1, \dots, m_A - 1\}$$

$$y \in \{0, 1, \dots, m_B - 1\}$$

Winning probability

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

Optimal classical winning probability

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

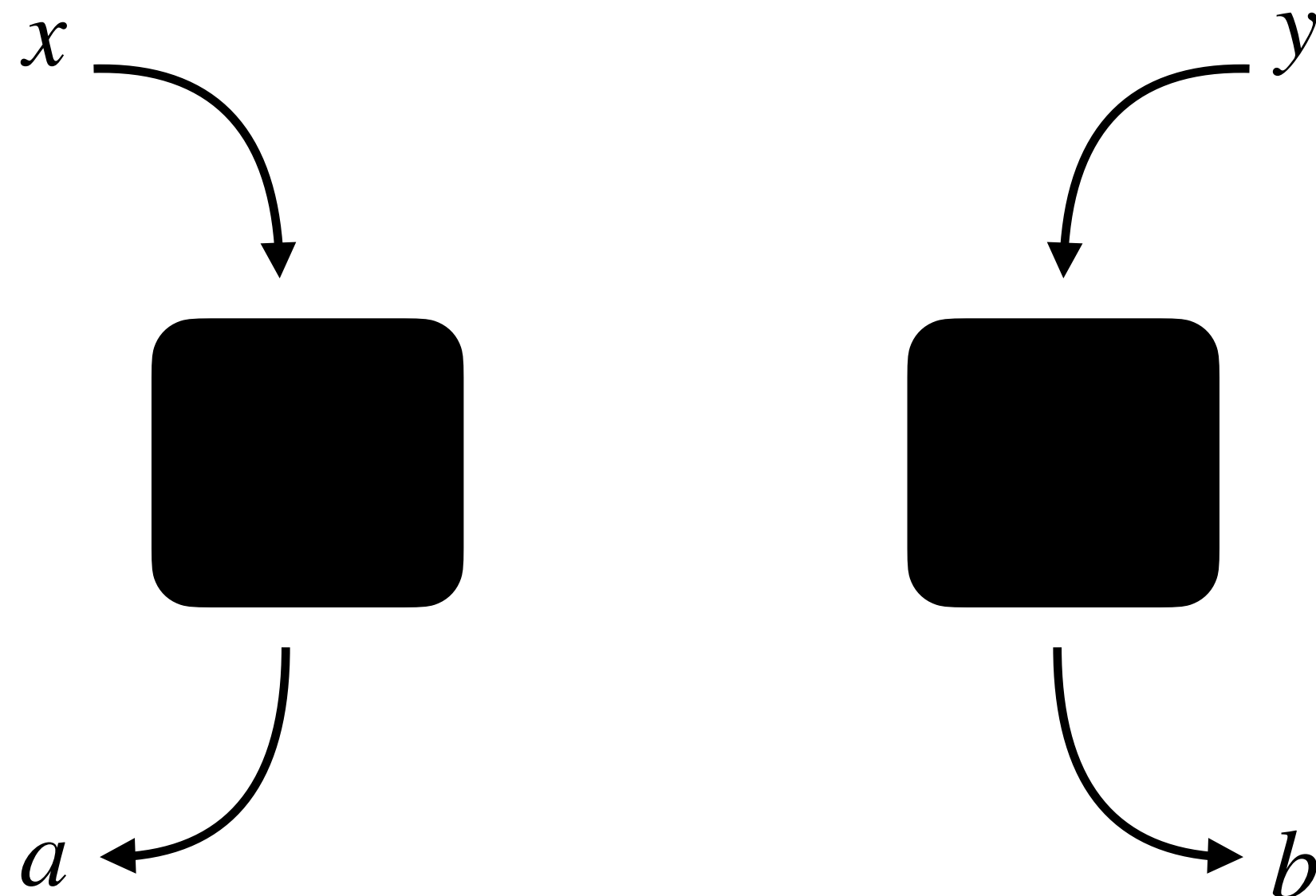
Quantum strategy $|\psi\rangle, \{M_{a|x}\}_{a,x}, \{N_{b|y}\}_{b,y}$

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

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

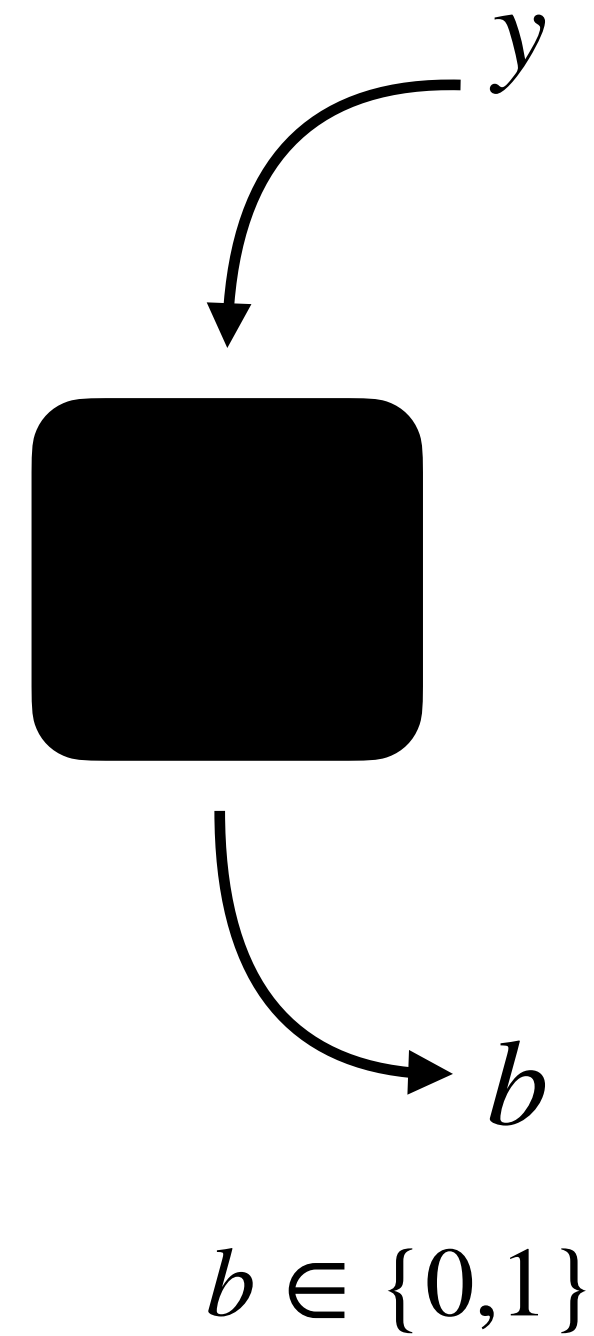
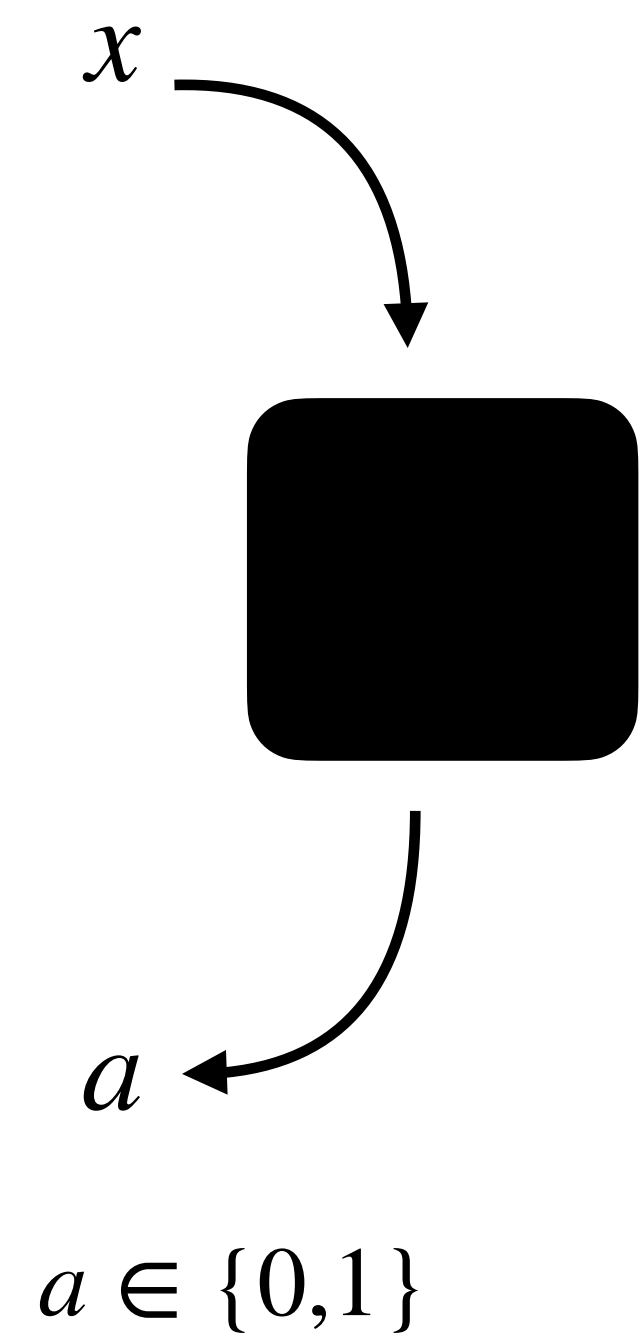


XOR games

$$x \in \{0, 1, \dots, m_A - 1\}$$

$$y \in \{0, 1, \dots, m_B - 1\}$$

$$V(x, y, a, b) = \begin{cases} 1, & \text{if } a \oplus b = f(x, y) \\ 0, & \text{otherwise} \end{cases}$$



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

$$\text{Bias } \xi = \sum_{x, y} q(x, y) (-1)^{f(x, y)} c_{x, y}, \text{ where}$$

$$c_{x, y} = \langle \psi | A_x \otimes B_y | \psi \rangle$$

$$\text{Winning probability } \omega = (1 + \xi)/2$$

$$\text{Game operator } \mathcal{B} = \sum_{x, y} q(x, y) (-1)^{f(x, y)} A_x \otimes B_y$$

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

Bell inequalities

$$x \in \{0, 1, \dots, m_A - 1\}$$

$$y \in \{0, 1, \dots, m_B - 1\}$$

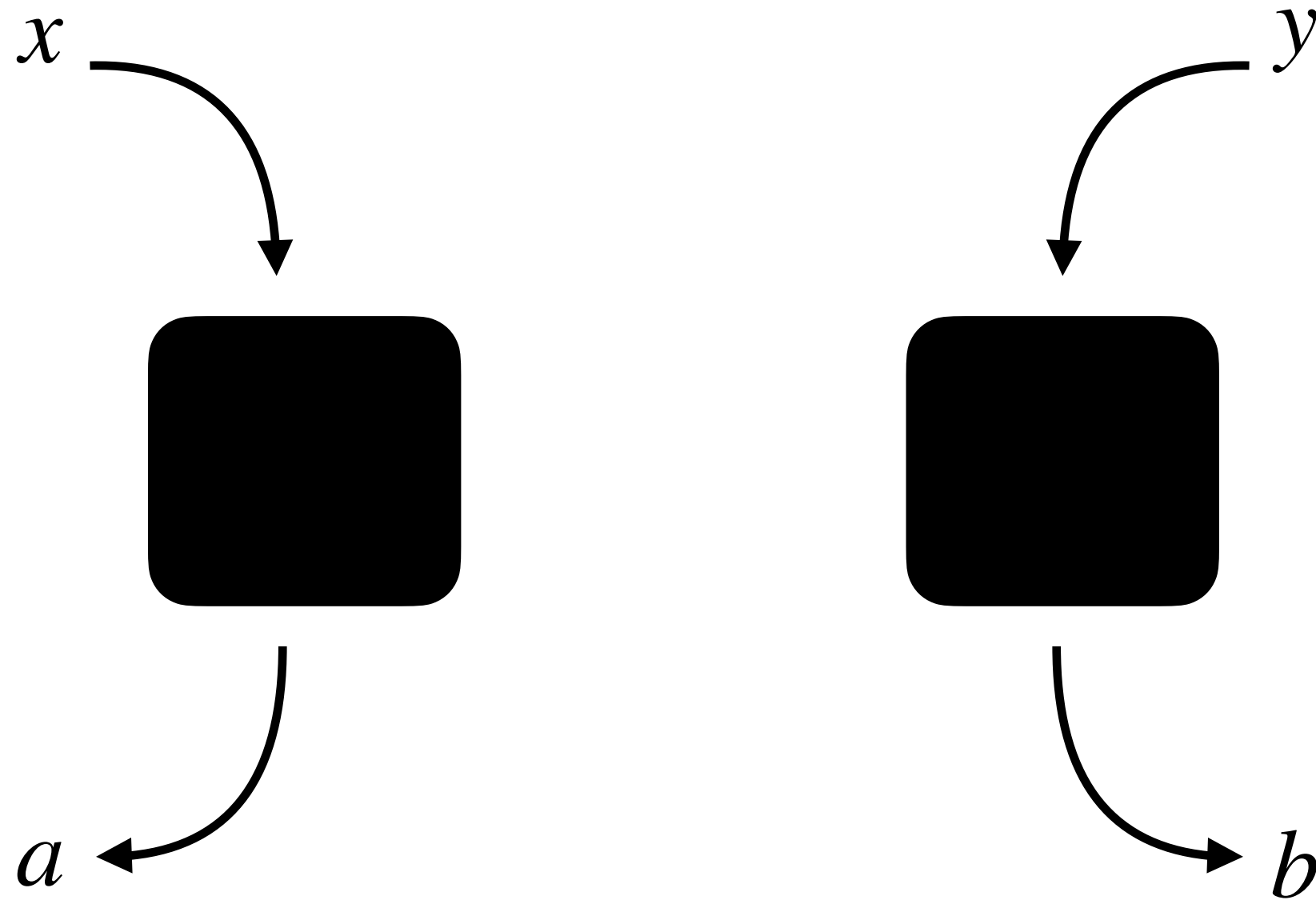
$$\gamma_{a,b,x,y} = q(x, y)V(x, y, a, b)$$

$$\text{Bell inequality } \sum_{x,y,a,b} \gamma_{a,b,x,y} p(a, b | x, y) \leq \beta_L$$

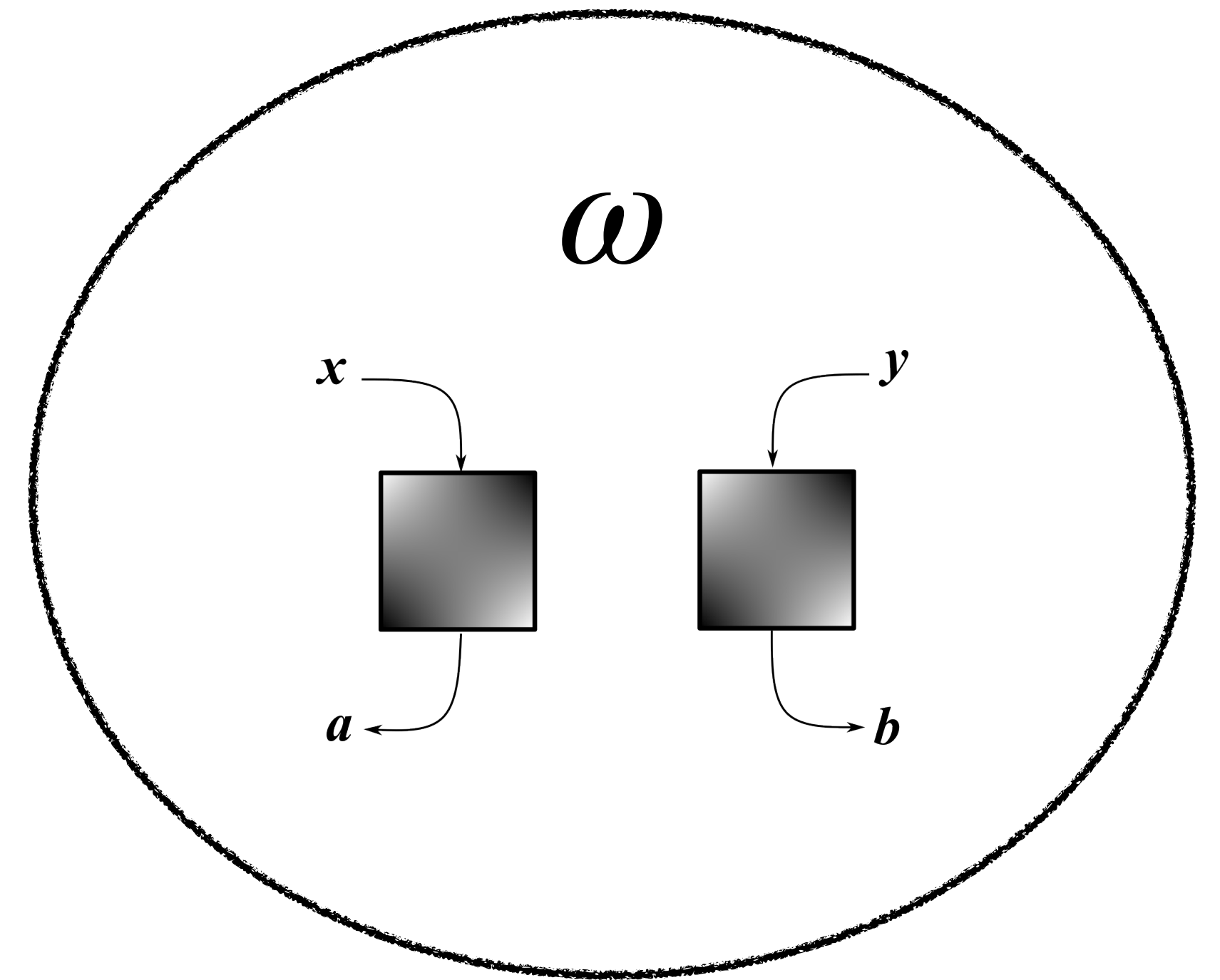
Quantum bound β_Q

$$\text{Bell operator } \mathcal{B} = \sum_{a,b,x,y} \gamma_{a,b,x,y} M_{a|x} \otimes N_{b|y}$$

Shifted Bell operator $\beta_Q \mathbb{I} - \mathcal{B}$

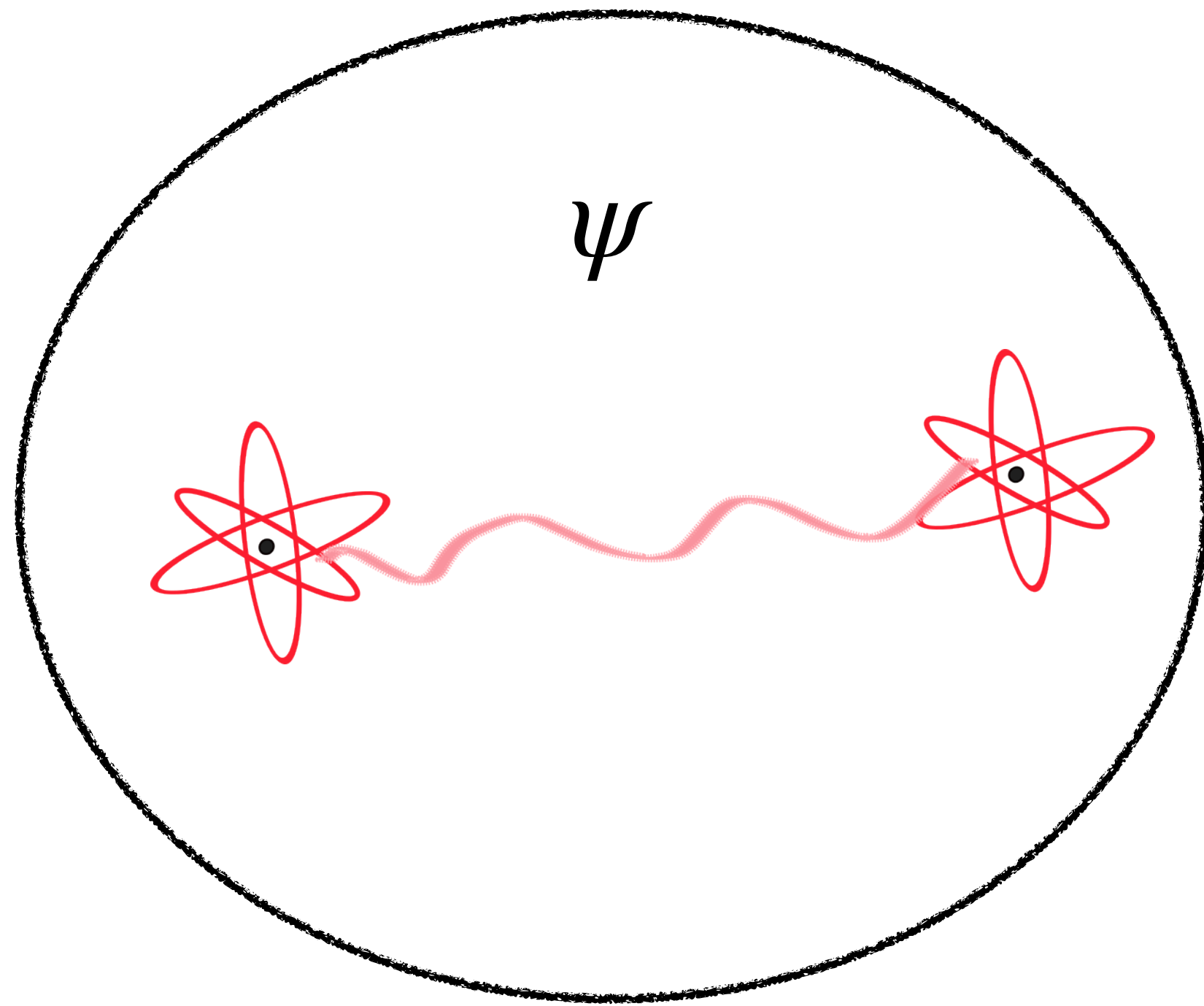


Device-independent paradigm

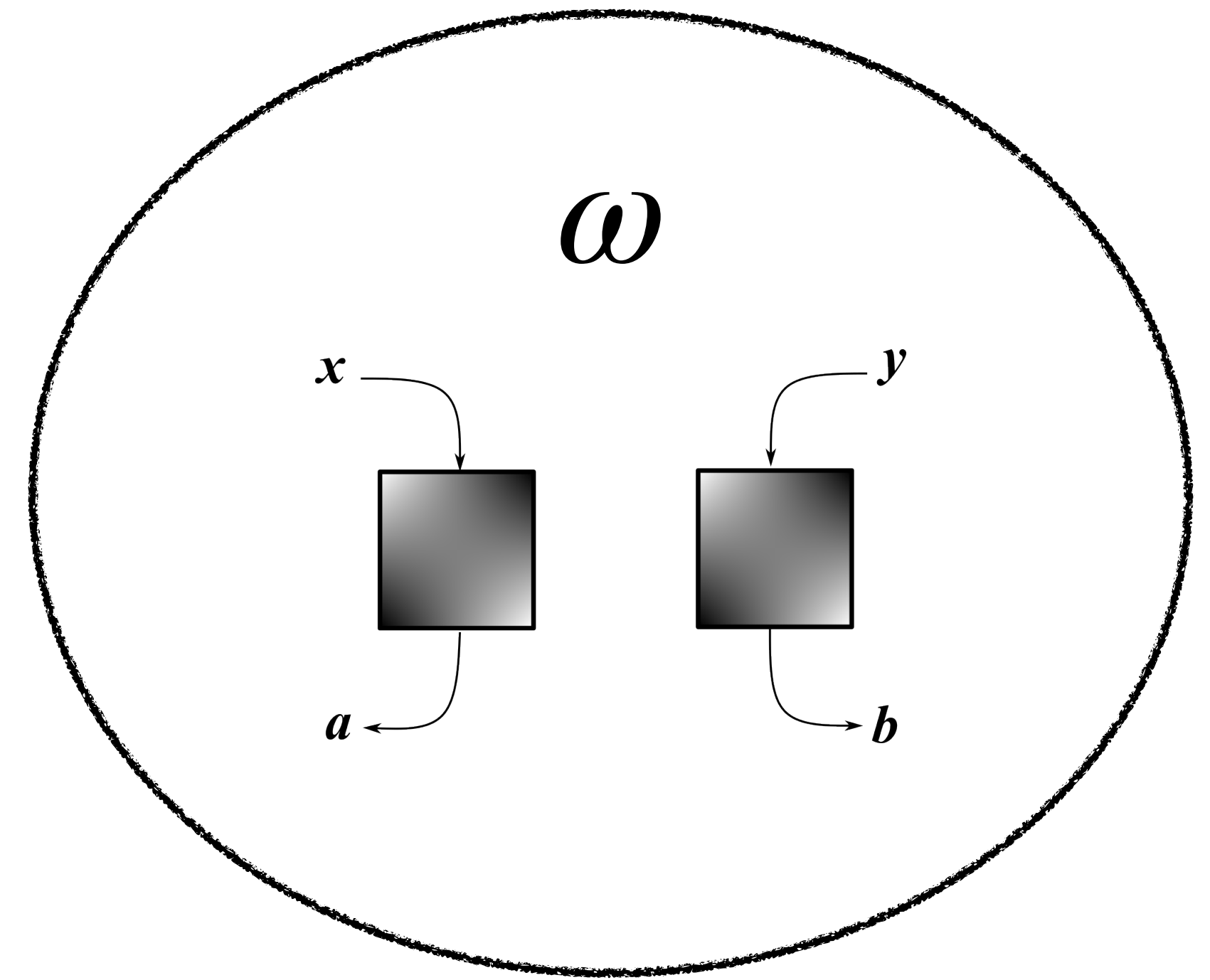


Nonlocal games

Device-independent paradigm

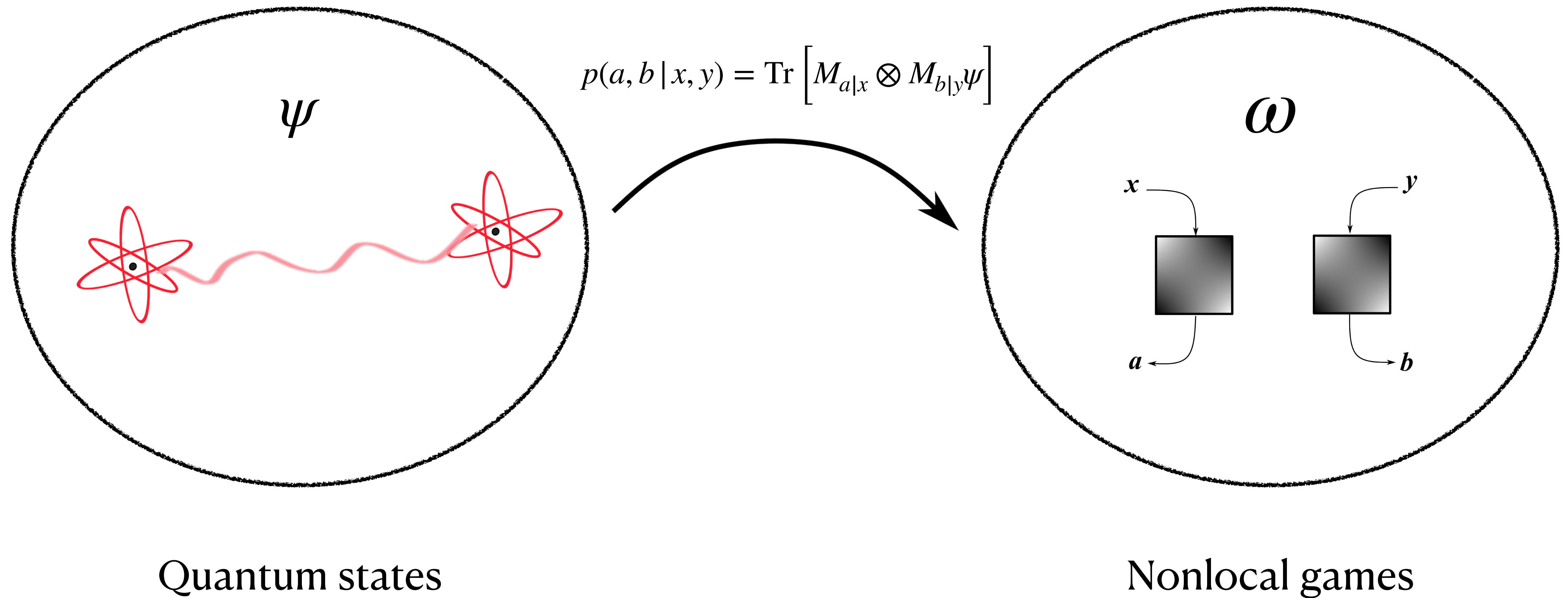


Quantum states

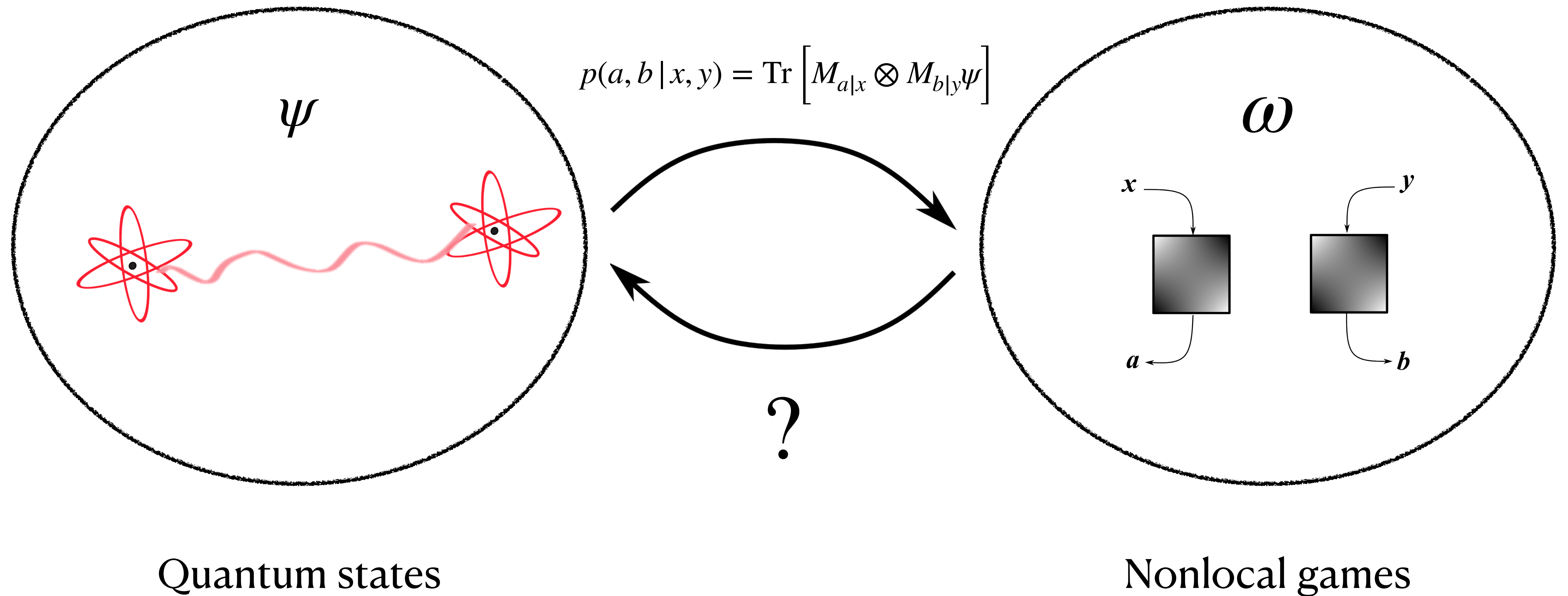


Nonlocal games

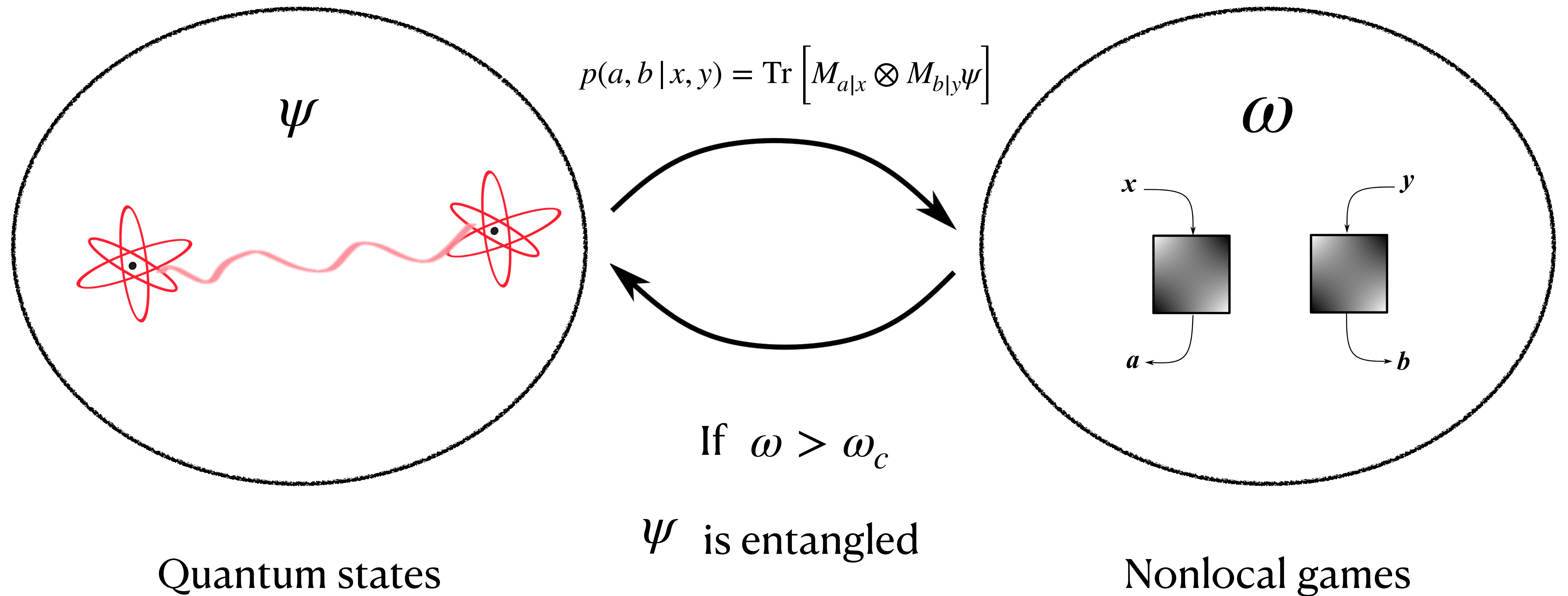
Device-independent paradigm



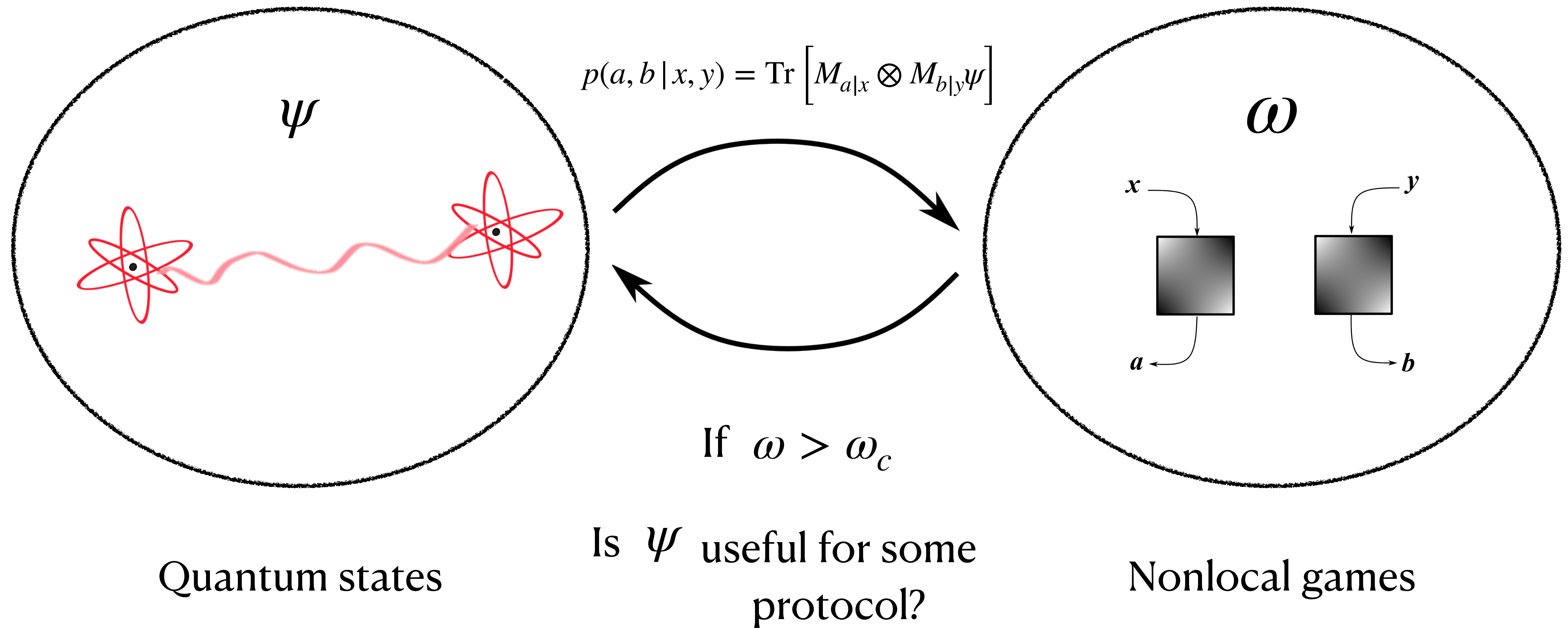
Device-independent paradigm



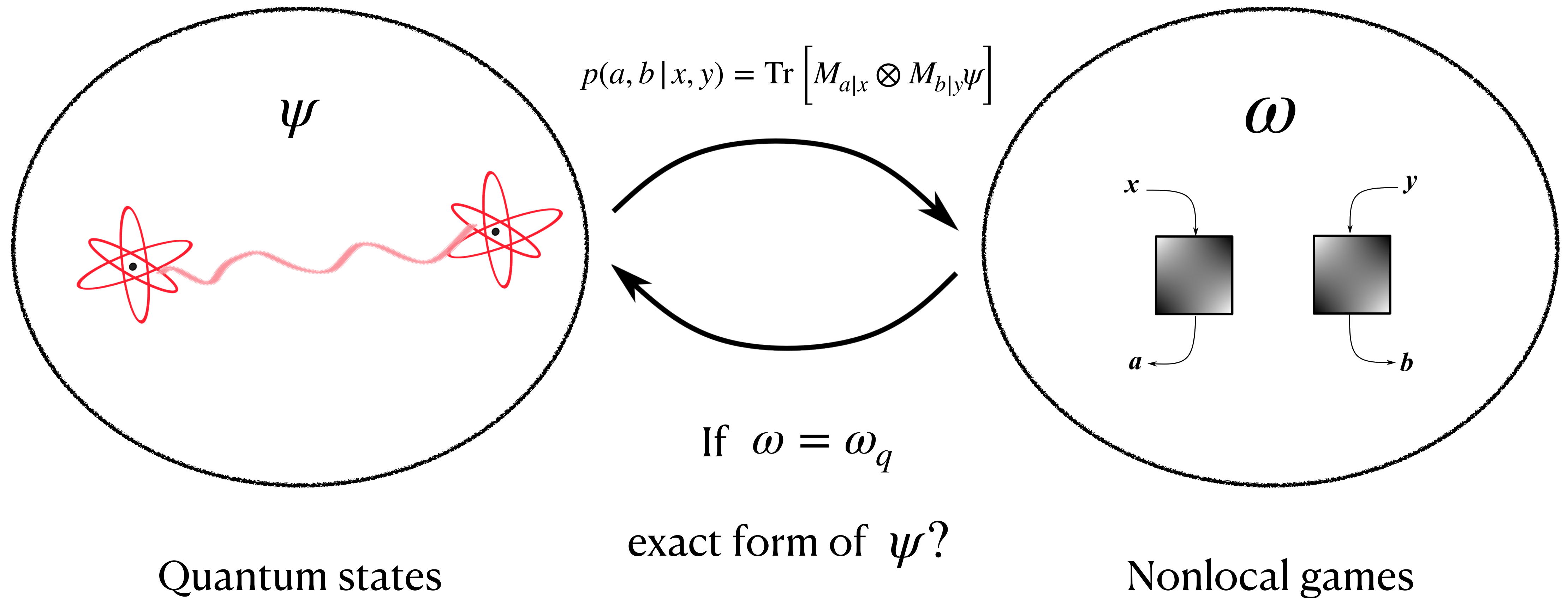
Device-independent paradigm



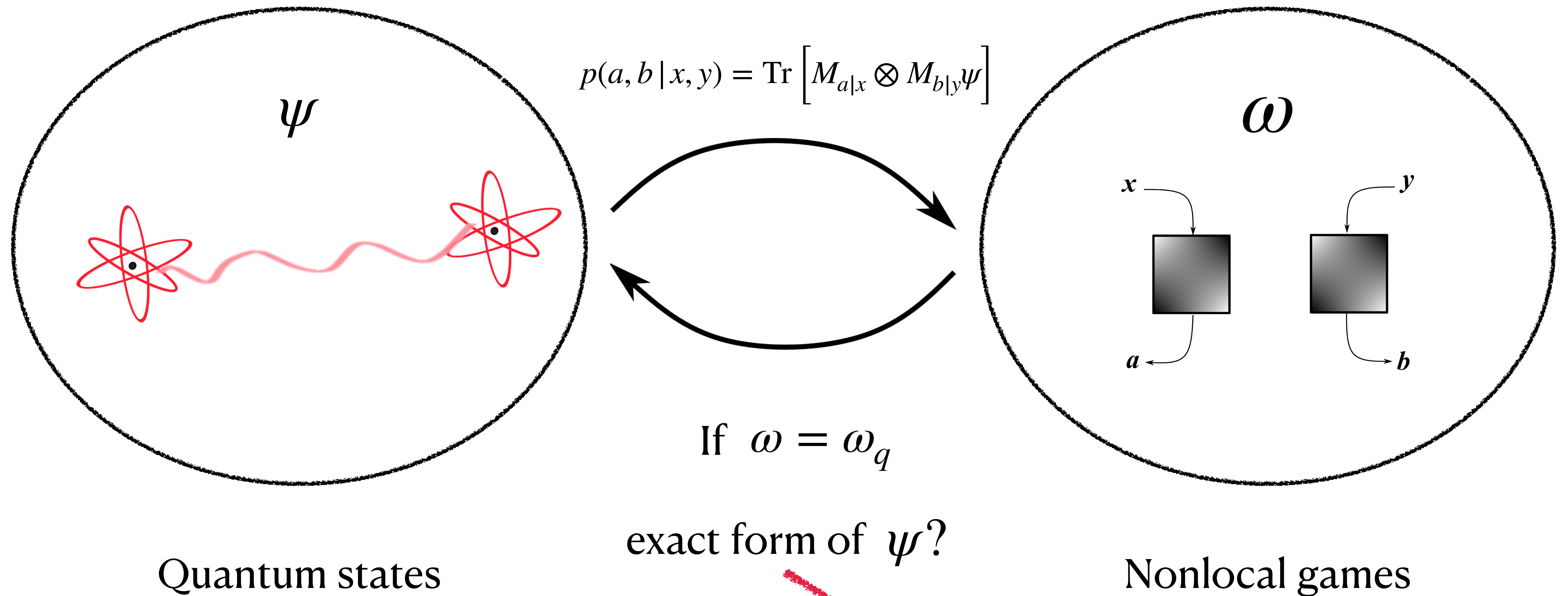
Device-independent paradigm



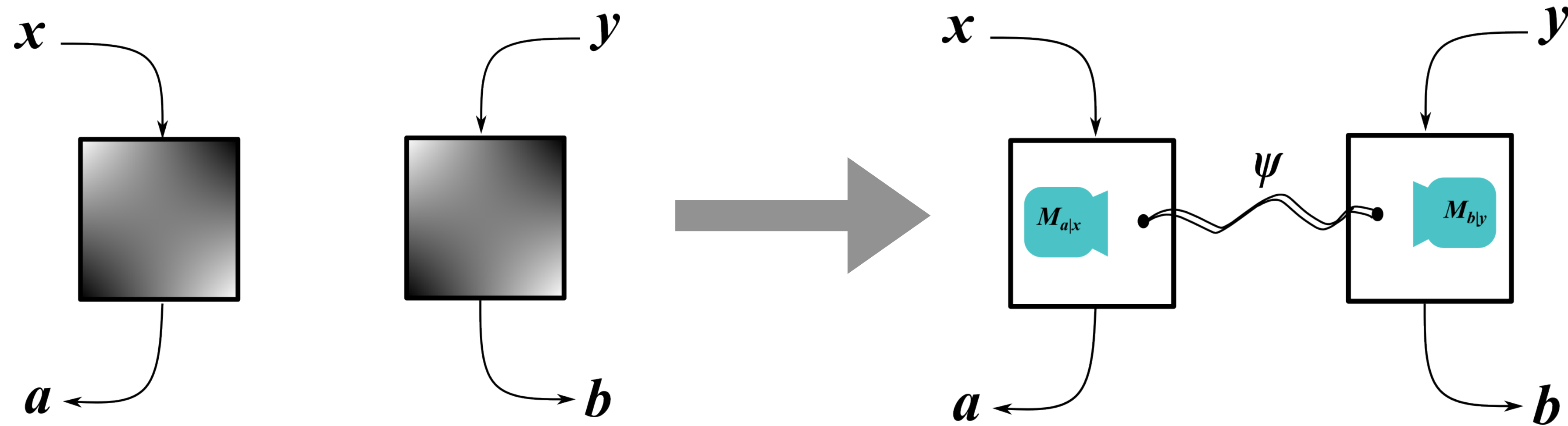
Device-independent paradigm



Device-independent paradigm



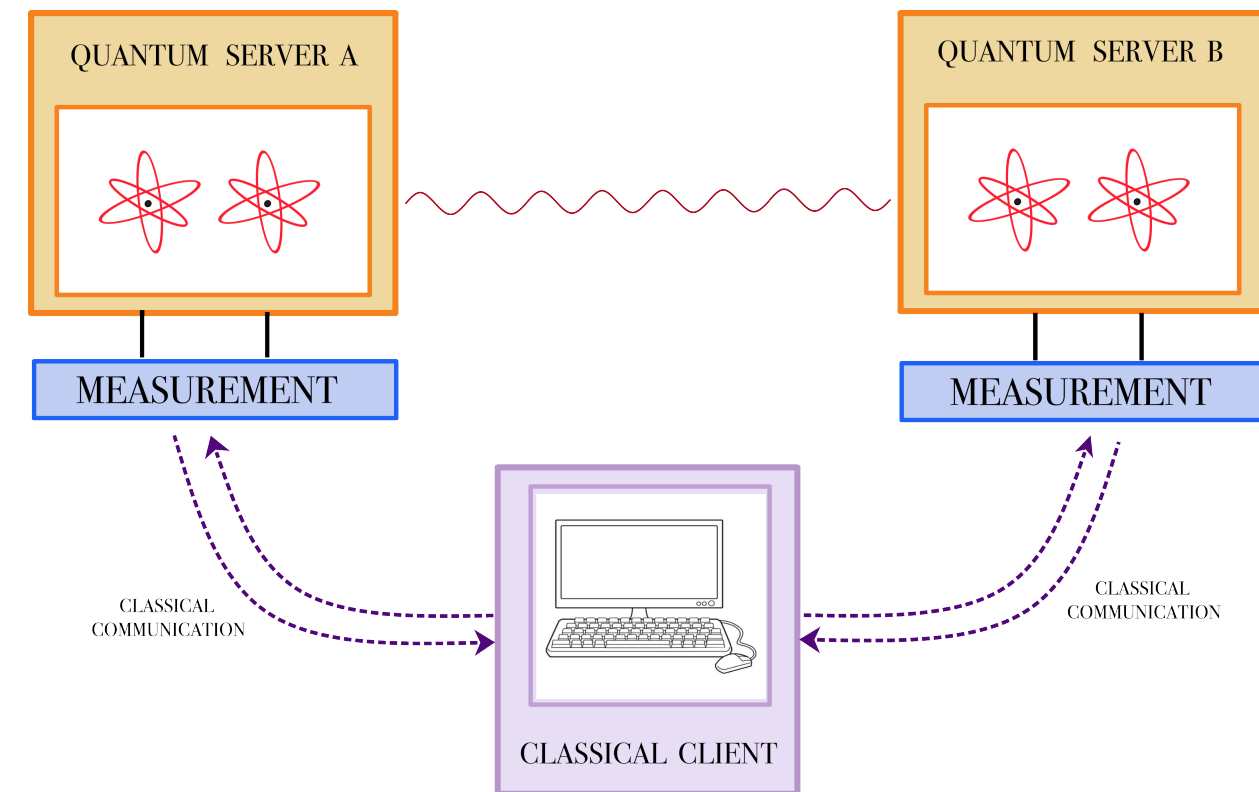
Device-independent paradigm



- 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

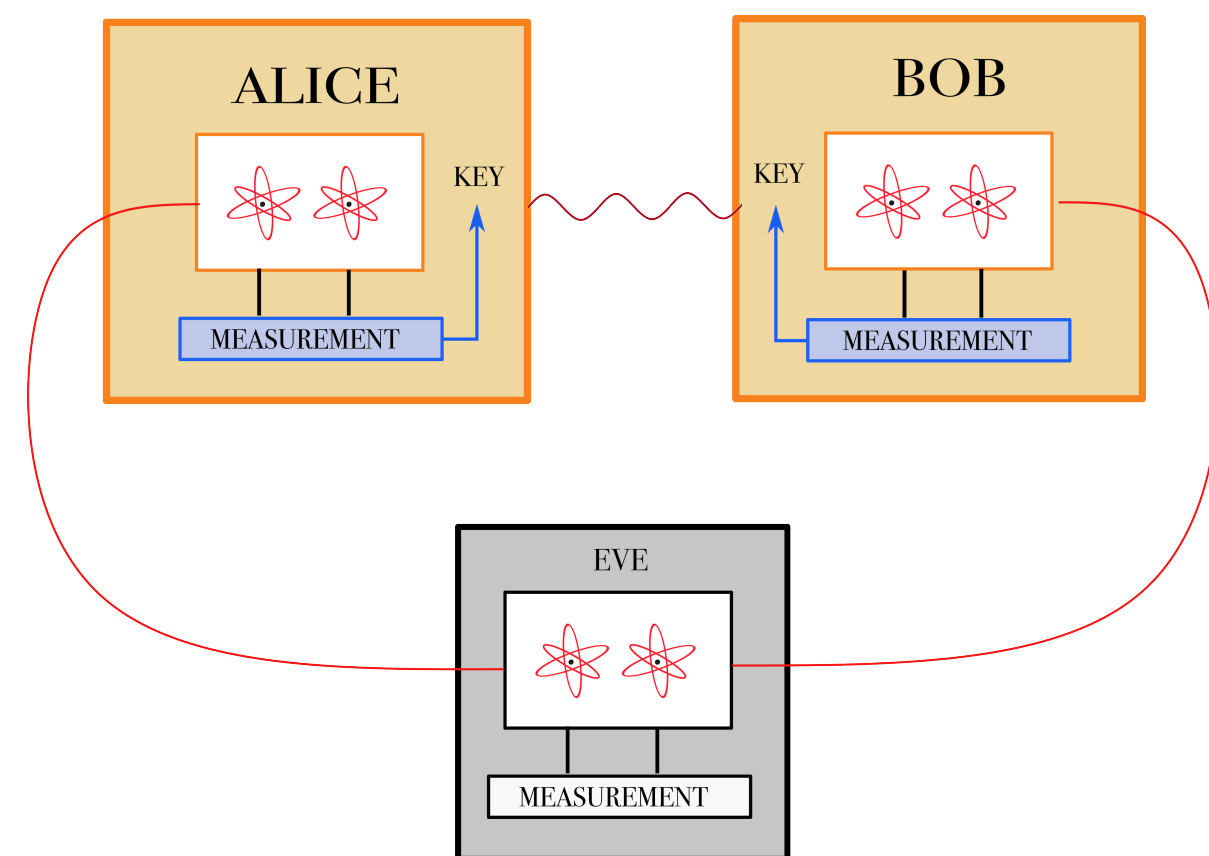
Nonlocal games and QI protocols

- Delegated quantum computation



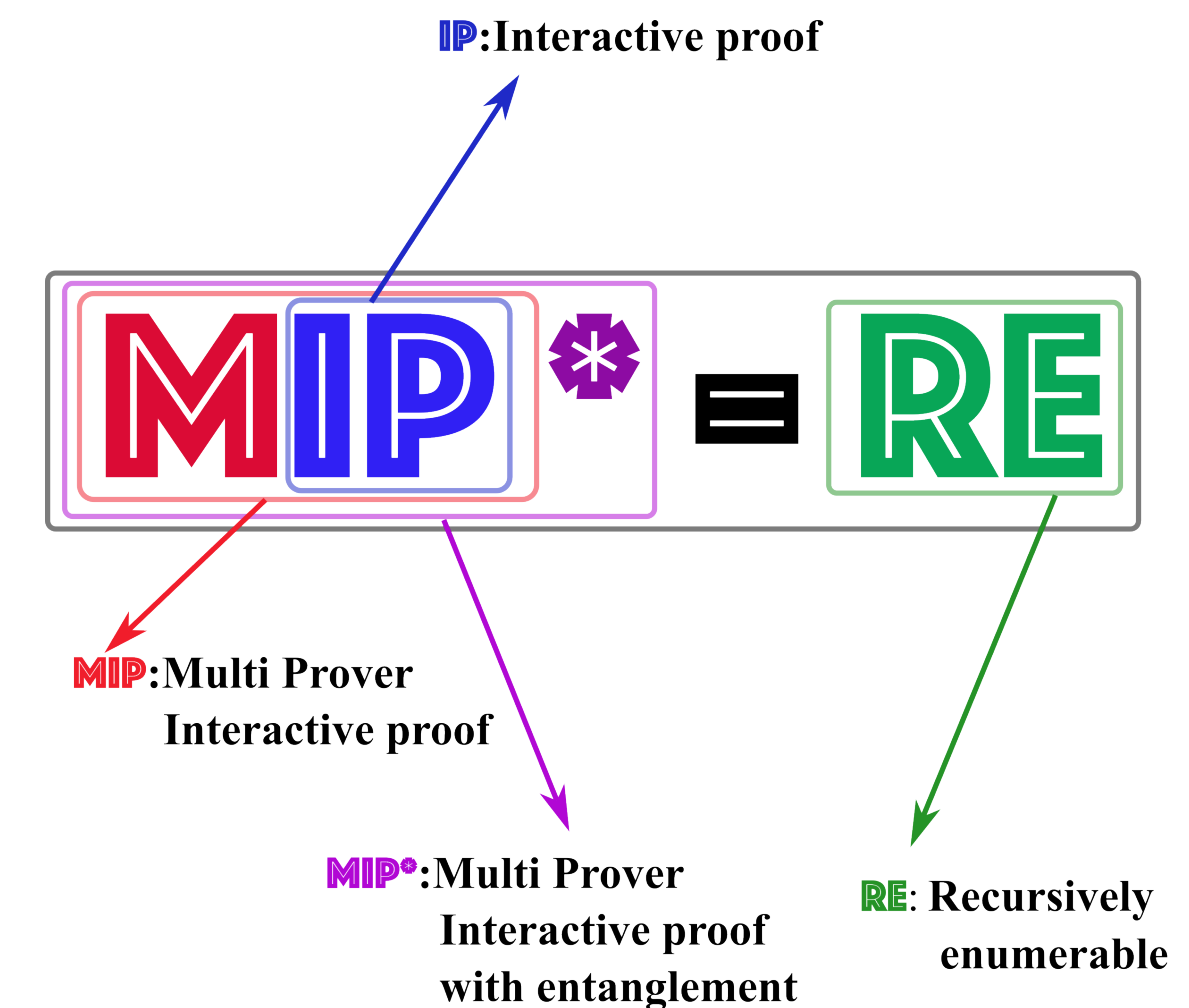
RUV: Nature, 496, 456-460 (2013)
Barz et al: Science, 335 (6066), 303-308

- Trust-free quantum key distribution



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

- Computational complexity



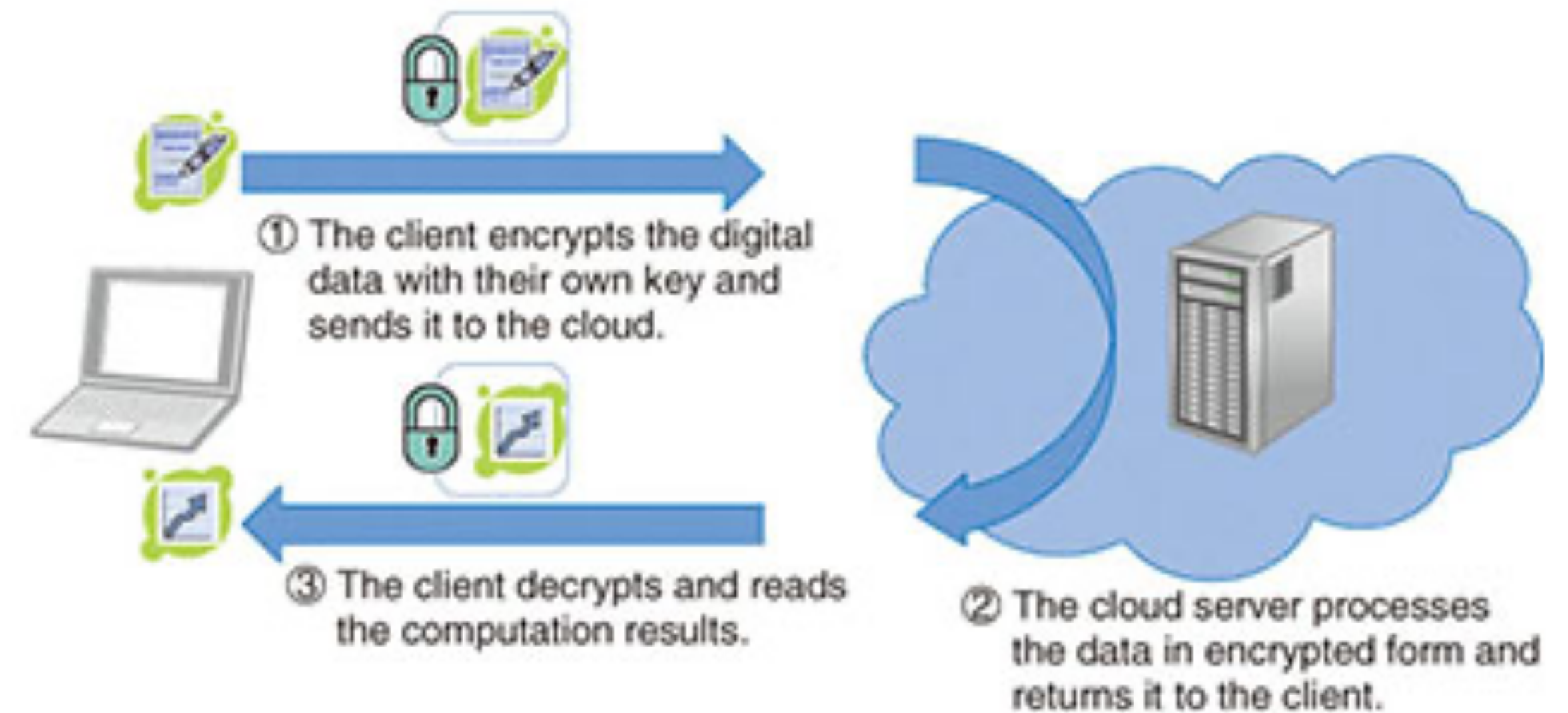
- Genuine randomness generation



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

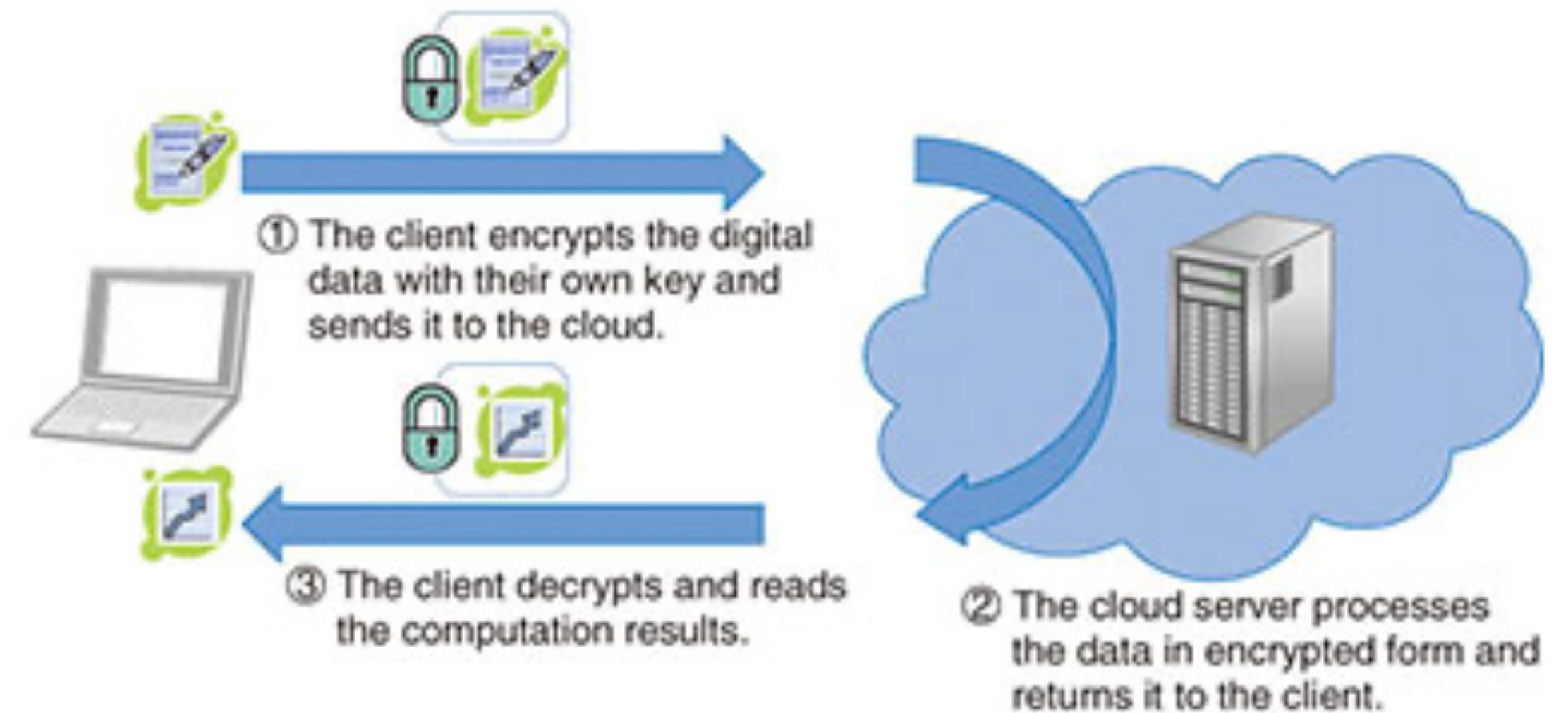
Quantum homomorphic encryption

- **Homomorphic** encryption: enables to execute computations directly on encrypted data without prior decryption
- Encryption and computation “commute”
- A cryptosystem allowing arbitrary computation on cypher texts is termed **fully homomorphic** encryption (Gentry09)
- Lattice-based cryptography (Ring learning with errors)
- **Quantum homomorphic** encryption : allowing for quantum computations on encrypted data (Mahadev18, Brakerski18)



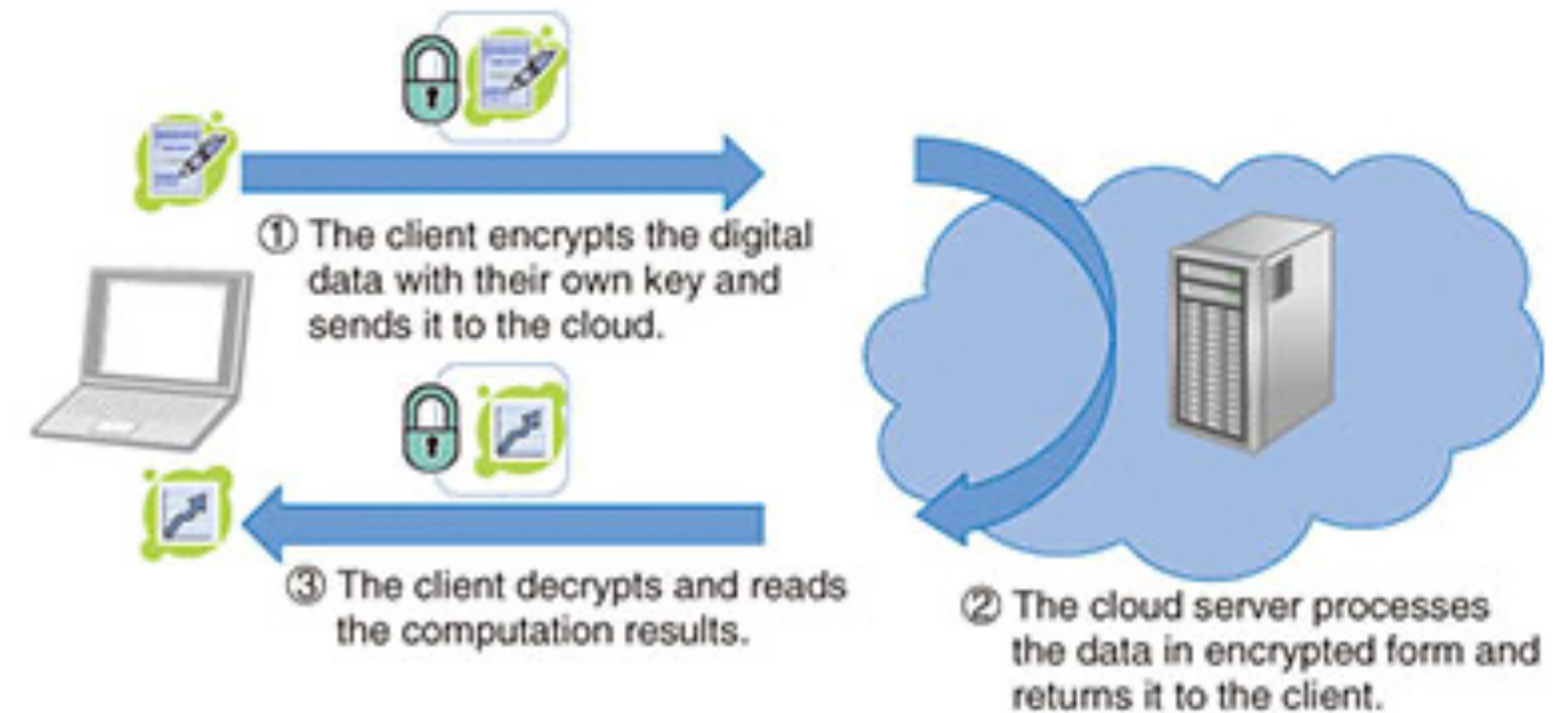
Quantum homomorphic encryption

- **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

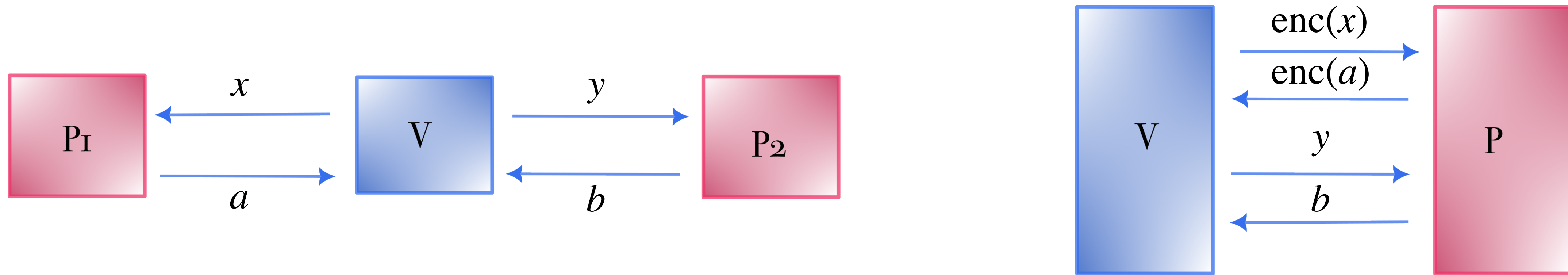


Quantum homomorphic encryption

- QHE scheme should satisfy the following two properties
 1. **Correctness with auxiliary input:** ensures that the evaluation part of the procedure preserves entanglement
 2. **IND-CPA security** (indistinguishability under chosen plaintext attack): Having a ciphertext, the adversary cannot do better in associating it to the plaintext than randomly guessing (up to a factor which is a negligible function of the security parameter κ)

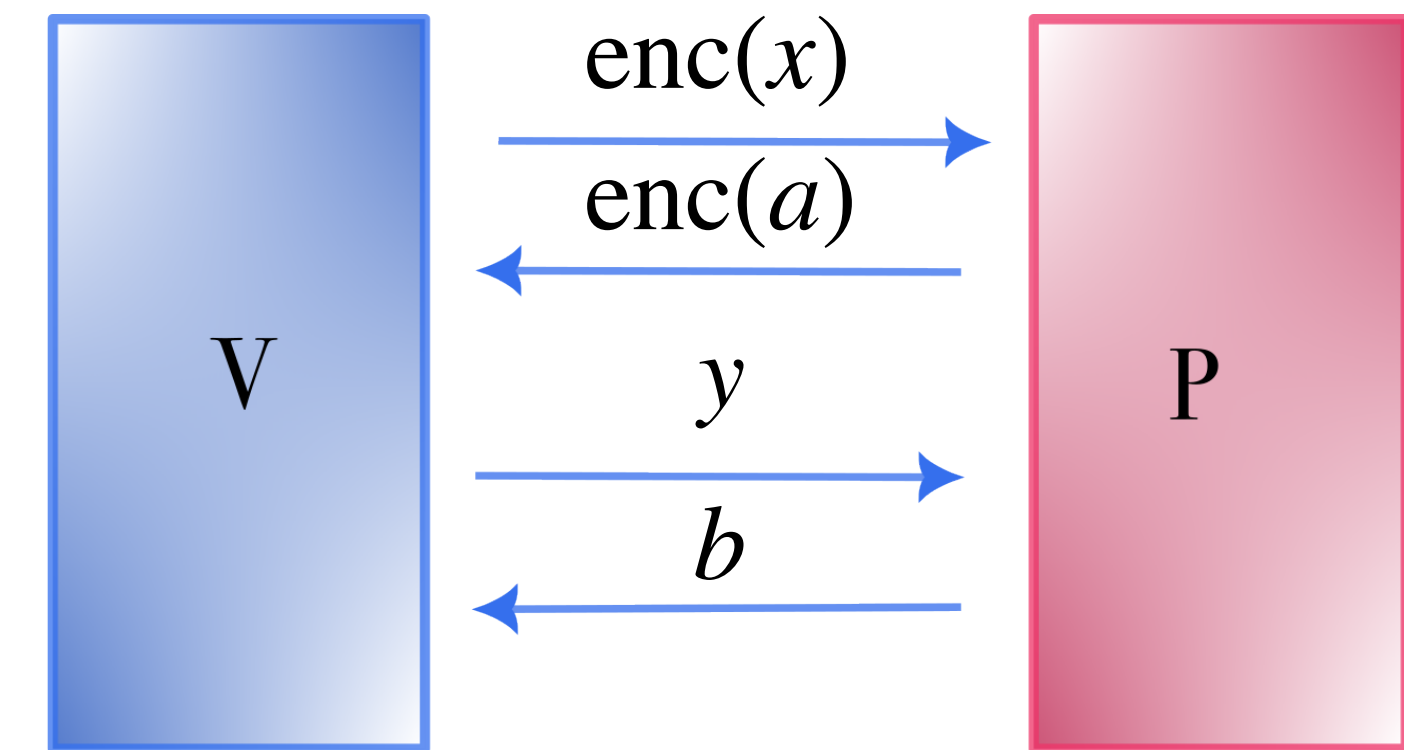
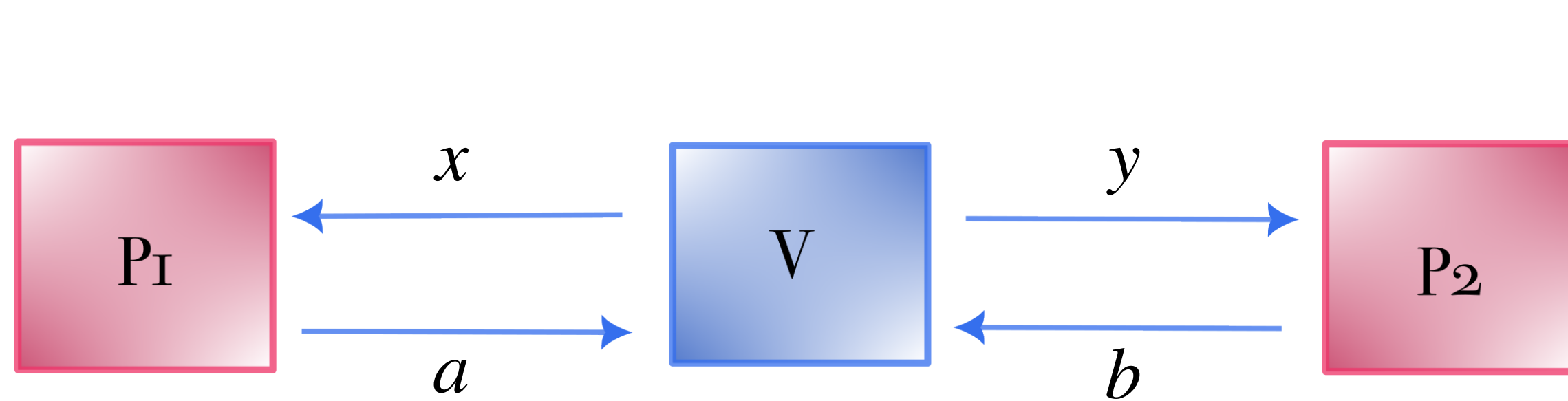


KLVY compilation protocol

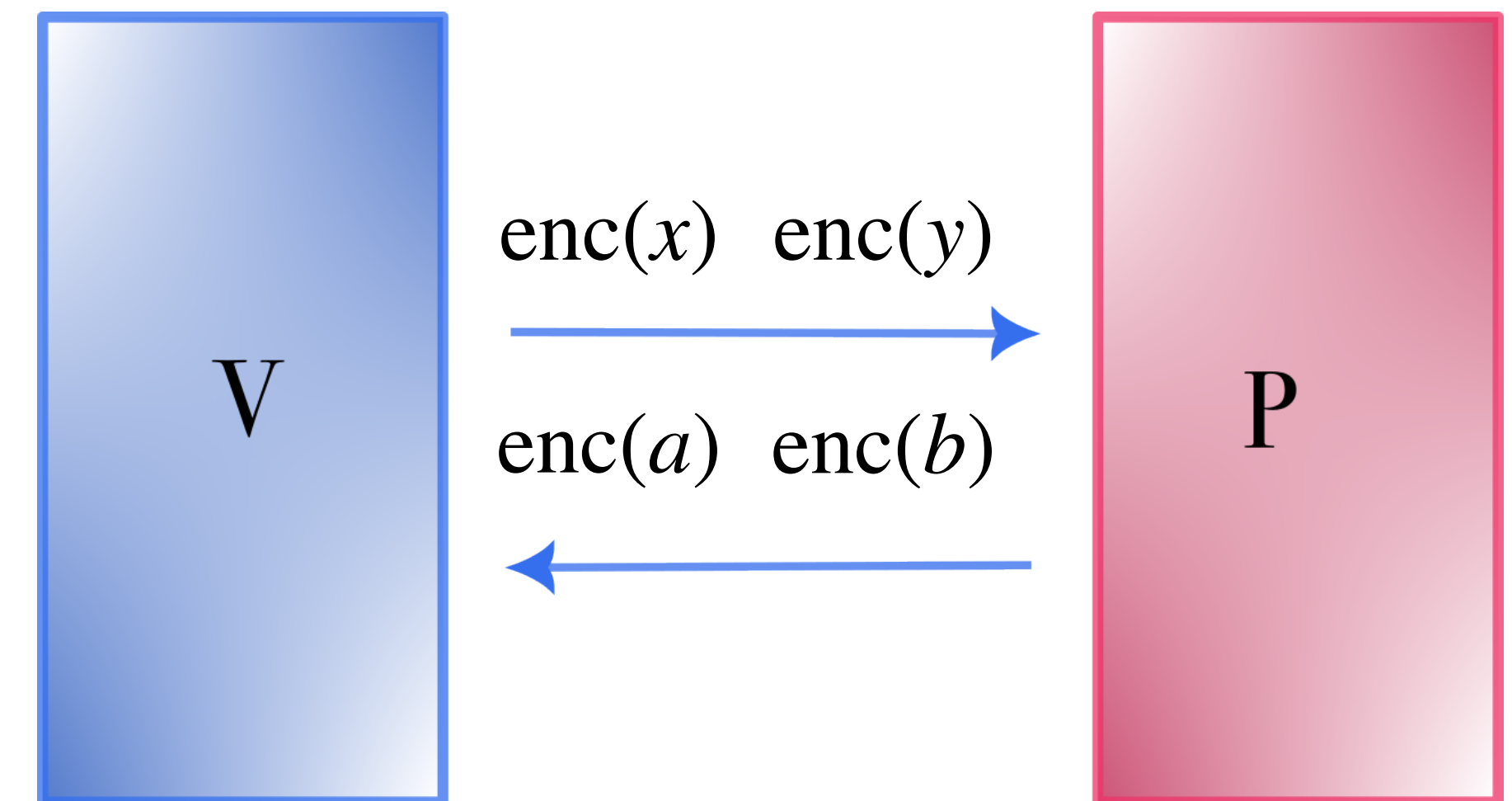


- Round 1: sample “Alice’s” input x and use the secret key sk to obtain encrypted input c , which is sent to the prover. The prover returns encrypted output α
- Round 2: sample “Bob’s” input y and send it to the prover in clear. The prover returns output b
- Verifier uses sk to get $a = \text{dec}(\alpha)$,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

Preservation of the local bound



- IND-CPA security ensures that the prover in the second round knows “nothing” about input x
- The prover has to commit to a (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



Quantum provers

- State of the prover $|\psi\rangle$
- Input c and output α : postmeasurement state $M_c^\alpha |\psi\rangle$, with M_c^α denoting a projector
- Followed by a possible unitary $|\psi_{c,\alpha}\rangle = U_{c,\alpha} M_c^\alpha |\psi\rangle = A_c^\alpha |\psi\rangle$, $\sum_\alpha A_c^{\alpha\dagger} A_c^\alpha = \mathbb{I}$
- Probability to get α given c is $\langle\psi| A_c^{\alpha\dagger} A_c^\alpha |\psi\rangle = \langle\psi| M_c^\alpha |\psi\rangle$
- Second round: projective measurement N_y^b
- Decrypted “observable” $A_x = \mathbb{E}_{c:\text{dec}(c)=x} \sum_\alpha (-1)^{\text{dec}(\alpha)} A_c^{\alpha\dagger} A_c^\alpha$
- For a and b bits we can define the decrypted correlator
 $\langle A_x, B_y \rangle = \mathbb{E}_{c:\text{dec}(c)=x} \sum_\alpha (-1)^{\text{dec}(\alpha)} \langle\psi_{\alpha,c}| B_y |\psi_{\alpha,c}\rangle$ - the expected value of $(-1)^{a+b}$ for inputs x and y

Preservation of the quantum bound: CHSH game

[1] Natarajan, Zhang; arXiv:2302.01545

[2] Brakerski, Gheorghiou, Kahanamoku-Meyer, Porat, Vidick; arXiv:2303.01293

- Compiled CHSH game, 2 players, 2 rounds, bit inputs and outputs
- [1] proves the preservation of the quantum bound in two ways: by using macroscopic locality, and by using crypto-SOS decomposition
- [2] proves the preservation of the quantum bound by using the Jordan's lemma
- Both also show that anti-commuting pair of observables is self-tested in the second round
- Is the quantum bound preserved for a general nonlocal game?

Properties of XOR games

- $|A_x\rangle = A_x |\psi\rangle, \quad |B_y\rangle = B_y |\psi\rangle; \quad |A\rangle = \sum_x |A_x\rangle \otimes |x\rangle, \quad |B\rangle = \sum_y |B_y\rangle \otimes |y\rangle$
- Correlation matrix: $C = \sum_{x,y} c_{x,y} |x\rangle\langle y|, \quad c_{x,y} = \langle A_x | B_y \rangle$
- Bias $\xi = \sum_{x,y} q(x,y)(-1)^{f(x,y)} c_{x,y}$
- Game operator $\mathcal{B} = \sum_{x,y} q(x,y)(-1)^{f(x,y)} A_x \otimes B_y$, the bias is given by $\xi = \langle \psi | \mathcal{B} | \psi \rangle$

Properties of XOR games

- Lemma(Tsirelson): Alice's optimal quantum strategy in an XOR game, encoded in the vector $|A_q\rangle$, is fully determined by Bob's optimal strategy $|B_q\rangle$ through a linear transformation. $|A_q\rangle = \mathbb{I} \otimes F |B_q\rangle$

- SOS-decomposition (1st order)

$$\xi_q \mathbb{I} - \mathcal{B} = \left(\sum_x \omega_x A_x - \sum_y F_{xy} \theta_y B_y \right)^2 + \left(\sum_x \omega'_x A_x - \sum_y F_{xy} \theta'_y B_y \right)^2 + \dots$$

- Expectation value

$$\xi_q \langle \psi | \psi \rangle - \langle \psi | \mathcal{B} | \psi \rangle = \langle \psi | \left(\sum_x \omega_x A_x - \sum_y F_{xy} \theta_y B_y \right)^2 | \psi \rangle + \langle \psi | \left(\sum_x \omega'_x A_x - \sum_y F_{xy} \theta'_y B_y \right)^2 | \psi \rangle + \dots$$

$$\xi_q - \xi \geq 0$$

- For $|\psi\rangle$ reaching the optimal winning probability we have

$$\sum_x \omega_x A_x |\psi\rangle = \sum_y F_{xy} \theta_y B_y |\psi\rangle, \dots \quad [\text{self-testing}]$$

Properties of XOR games

- Theorem (BVBMDŠ24): Let $\mathcal{B}$ be the game operator of an XOR game with optimal quantum bias ξ_q . Then the following holds

$$\xi_q \mathbb{I} - \mathcal{B} = \sum_x \frac{\lambda_x}{2} \left(A_x - \sum_y F_{x,y} B_y \right)^2 + P(B_y)$$

where λ_x -s and F_{xy} are found from the function $f(x, y)$ and question distribution $q(x, y)$ $P(B_y)$ is a positive degree-2 polynomial over Bob's measurement operators.

Crypto-SOS decomposition

COMPILED NONLOCAL GAME

$$|\psi_{c,\alpha}\rangle = U_{c,\alpha} M_c^\alpha |\psi\rangle = A_c^\alpha |\psi\rangle$$

$$\langle A_x, B_y \rangle = \mathbb{E}_{c:\text{dec}(c)=x} \sum_{\alpha} (-1)^{\text{dec}(\alpha)} \langle \psi_{\alpha,c} | B_y | \psi_{\alpha,c} \rangle$$

$$\langle B_y, B_{y'} \rangle = \sum_{y,y'} \mathbb{E}_x \mathbb{E}_{c:\text{dec}(c)=x} \sum_{\alpha} \langle \psi_{c,\alpha} | B_y B_{y'} | \psi_{c,\alpha} \rangle$$

$$\xi = \sum_{x,y} q(x,y) (-1)^{f(x,y)} \langle A_x, B_y \rangle$$

State prepared
for “Bob”

Correlator

Unobservable “Bob’s”
correlator

XOR bias

NONLOCAL GAME

$$|\psi_{a|x}\rangle = (M_{a|x} \otimes \mathbb{I}) |\psi\rangle \langle \psi| (M_{a|x} \otimes \mathbb{I})$$

$$\langle A_x, B_y \rangle = \langle \psi | A_x \otimes B_y | \psi \rangle$$

$$\langle B_y, B_{y'} \rangle = \langle \psi | \mathbb{I} \otimes B_y B_{y'} | \psi \rangle$$

$$\xi = \sum_{x,y} q(x,y) (-1)^{f(x,y)} \langle A_x, B_y \rangle$$

Crypto-SOS decomposition

COMPILED NONLOCAL GAME

$$\xi = \sum_{x,y} q(x,y)(-1)^{f(x,y)} \langle A_x, B_y \rangle$$

Pseudo-expectation value of the shifted game operator: $\langle \psi | \xi_q \mathbb{I} - \mathcal{B} | \psi \rangle$

NONLOCAL GAME

$$\xi = \sum_{x,y} q(x,y)(-1)^{f(x,y)} \langle A_x, B_y \rangle$$

Expectation value of the shifted game operator: $\langle \psi | \xi_q \mathbb{I} - \mathcal{B} | \psi \rangle$

Pseudo-expectation function and the preservation of the quantum bound

$$\tilde{\mathbb{E}}(A_x B_y) = \tilde{\mathbb{E}}(A_x B_y) = \langle A_x, B_y \rangle, \quad \tilde{\mathbb{E}}(A_x A_{x'}) = \delta_{xx'}, \quad \tilde{\mathbb{E}}(B_y B_{y'}) = \langle B_y, B_{y'} \rangle$$

$$\tilde{\mathbb{E}}(\mathcal{B}) = \sum_{x,y} q(x,y)(-1)^{f(x,y)} \tilde{\mathbb{E}}(A_x B_y) = \tilde{\xi}$$

What do we get when we attack with this pseudo-expectation function the shifted game operator:

$$\tilde{\mathbb{E}}(\xi_q \mathbb{I} - \mathcal{B}) = \tilde{\mathbb{E}} \left(\left(\sum_x \omega_x A_x - \sum_y F_{xy} \theta_y B_y \right)^2 \right) + \tilde{\mathbb{E}} \left(\left(\sum_x \omega'_x A_x - \sum_y F_{xy} \theta'_y B_y \right)^2 \right) + \dots$$

Pseudo-expectation function and the preservation of the quantum bound

- Lemma(BVBMĐŠ24): Let $P_x = A_x - \sum_y F_{x,y} B_y$ with A_x and $\{B_y\}_y$ binary observables.

Then there exists a negligible function $\delta_{\text{QHE}}(\kappa)$ such that $\tilde{\mathbb{E}}(P_x^\dagger P_x) \geq -\delta_{\text{QHE}}(\kappa)$.

- Proof outline: the pseudoexpectation gives a form of the expectation value of $(A_x - \sum_y F_{x,y} B_y)^2$, but when the full expression is developed there are terms that give us the desired expectation value only if

A. We have **IND-CPA security**

B. $\sum_y F_{x,y} B_y$ is **efficiently implementable by a quantum prover**

Pseudo-expectation function and the preservation of the quantum bound

$$\tilde{\mathbb{E}}(A_x B_y) = \tilde{\mathbb{E}}(A_x B_y) = \langle A_x, B_y \rangle, \quad \tilde{\mathbb{E}}(A_x A_{x'}) = \delta_{xx'}, \quad \tilde{\mathbb{E}}(B_y B_{y'}) = \langle B_y, B_{y'} \rangle$$

$$\tilde{\mathbb{E}}(\mathcal{B}) = \sum_{x,y} q(x,y)(-1)^{f(x,y)} \tilde{\mathbb{E}}(A_x B_y) = \tilde{\xi}$$

What do we get when we attack with this pseudo-expectation function the shifted game operator:

$$\tilde{\mathbb{E}} \left(\xi_q \mathbb{I} - \mathcal{B} \right) = \sum_x \frac{\lambda_x}{2} \tilde{\mathbb{E}} \left(\left(A_x - \sum_y F_{x,y} B_y \right)^2 \right) + \tilde{\mathbb{E}} \left(P \left(B_y \right) \right) \geq -\delta_{QHE}(\kappa)$$

Self-testing of qubit observables

- $\mathcal{B}_{\mu\nu\chi} = \cos(\mu + \nu)\cos(\mu + \chi)(\cos(\chi)A_0 - \cos(\nu)A_1) \otimes B_0 + \cos(\nu)\cos(\chi)(-\cos(\mu + \chi)A_0 + \cos(\mu + \nu)A_1) \otimes B_1$

T. P. Le, C. Meroni, B. Sturmfels, R. F. Werner, and T. Ziegler.

Quantum correlations in the minimal scenario. Quantum, 7:947, March 2023

- SOS decomposition in: L. Woollorton, P. Brown, and R. Colbeck. Device-independent quantum key distribution with arbitrarily small nonlocality, arXiv
- For every two qubit observables there exists a Bell inequality maximally violated by them
- Self-testing proof

Open questions

- General case
- Multipartite games

David Cui, Giulio Malavolta, Arthur Mehta, Anand Natarajan, Connor Paddock, Simon Schmidt, Michael Walter, and Tina Zhang.

A Computational Tsirelson's Theorem for the Value of Compiled XOR Games. Cryptology ePrint Archive, Paper 2024/348, 2024.

SATWAP inequalities

Salavrakos, Augusiak, Tura, Wittek, Acin, Pironio; PRL 119:040402 (2017)

- Generalisation of the CHSH inequality
- Maximally violated by the maximally entangled state (works for any local dimension)

- Measurements $\{M_{a|x}\}_{a=0}^{d-1}$, $\{N_{b|y}\}_{b=0}^{d-1}$

- Generalised observables

$$A_x^{(k)} = \sum_{a=0}^{d-1} \omega^{ak} M_{a|x}, \quad B_y^{(l)} = \sum_{b=0}^{d-1} \omega^{bl} N_{b|y}, \quad \omega = \exp \frac{2\pi i}{d}$$

- Not Hermitian, but $\left[A_x^{(k)}\right]^\dagger = A_x^{(d-k)}$, $\left[A_x^{(k)}\right]^\dagger A_x^{(k)} = \mathbb{I}$

SATWAP inequalities

Salavrakos, Augusiak, Tura, Wittek, Acin, Pironio; PRL 119:040402 (2017)

- Correlator $\langle A_x^{(k)} B_y^{(l)} \rangle = \sum_{a,b} \omega^{ak+bl} p(a, b | x, y)$
- The SATWAP Bell functional

$$\beta_d^{\text{SATWAP}} = \sum_{k=1}^{d-1} \left(a_k \langle A_1^{(k)} B_1^{(d-k)} \rangle + a_k^* \omega^k \langle A_1^{(k)} B_2^{(d-k)} \rangle + a_k^* \langle A_2^{(k)} B_1^{(d-k)} \rangle + a_k \langle A_2^{(k)} B_2^{(d-k)} \rangle \right)$$
- Bob's observables grouped $C_1^{(k)} = a_k B_1^{(d-k)} + a_k^* \omega^k B_2^{(d-k)}$, $C_2^{(k)} = a_k^* B_1^{(d-k)} + a_k B_2^{(d-k)}$
- The SATWAP functional $\beta_d^{\text{SATWAP}} = \sum_{k=1}^{d-1} \left(\langle A_1^{(k)} C_1^{(k)} \rangle + \langle A_2^{(k)} C_2^{(k)} \rangle \right) = \langle \psi | \mathcal{B}_d^{\text{SATWAP}} | \psi \rangle$
- The quantum bound $(\beta_d^{\text{SATWAP}})_Q = 2(d-1)$

SATWAP inequalities

Salavrakos, Augusiak, Tura, Wittek, Acin, Pironio; PRL 119:040402 (2017)

- Bob's observables grouped $C_1^{(k)} = a_k B_1^{(d-k)} + a_k^* \omega^k B_2^{(d-k)}$, $C_2^{(k)} = a_k^* B_1^{(d-k)} + a_k B_2^{(d-k)}$
- The SATWAP functional $\beta_d^{\text{SATWAP}} = \sum_{k=1}^{d-1} \left(\langle A_1^{(k)} C_1^{(k)} \rangle + \langle A_2^{(k)} C_2^{(k)} \rangle \right) = \langle \psi | \mathcal{B}_d^{\text{SATWAP}} | \psi \rangle$
- The quantum bound $(\beta_d^{\text{SATWAP}})_Q = 2(d-1)$
- $P_{x,k} = (A_x^k)^\dagger - C_x^{(k)}$
- The SOS decomposition $2(d-1)\mathbb{I} - \mathcal{B}_d^{\text{SATWAP}} = \frac{1}{2} \sum_{k=1}^{d-1} \left(P_{1,k}^\dagger P_{1,k} + P_{2,k}^\dagger P_{2,k} \right)$
- For a state maximally violating the SATWAP inequality we have $P_{x,k} | \psi \rangle = 0$

Preservation of the quantum bound of compiled SATWAP games

- Generalised correlators
- Generalised Gram-like matrix
- Pseudo-expectation of the sum-of-squares
- The quantum bound of the compiled SATWAP game, up to negligible function the same as the quantum bound of the SATWAP
- Negligible function is unavoidable, self-test must be robust