

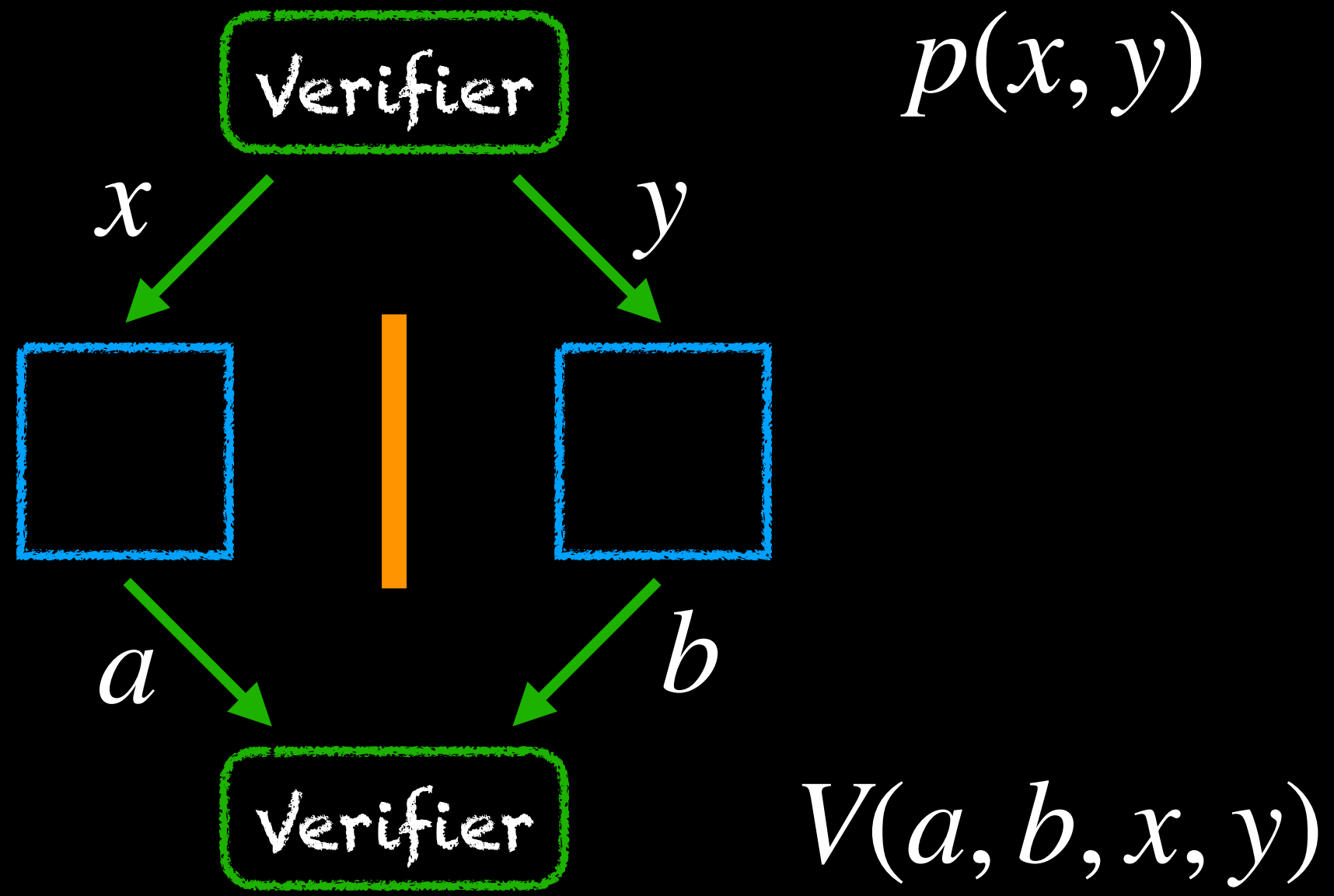
Compiled nonlocal games

Nonlocality: driver for single-device quantum advantage

Ivan Šupić

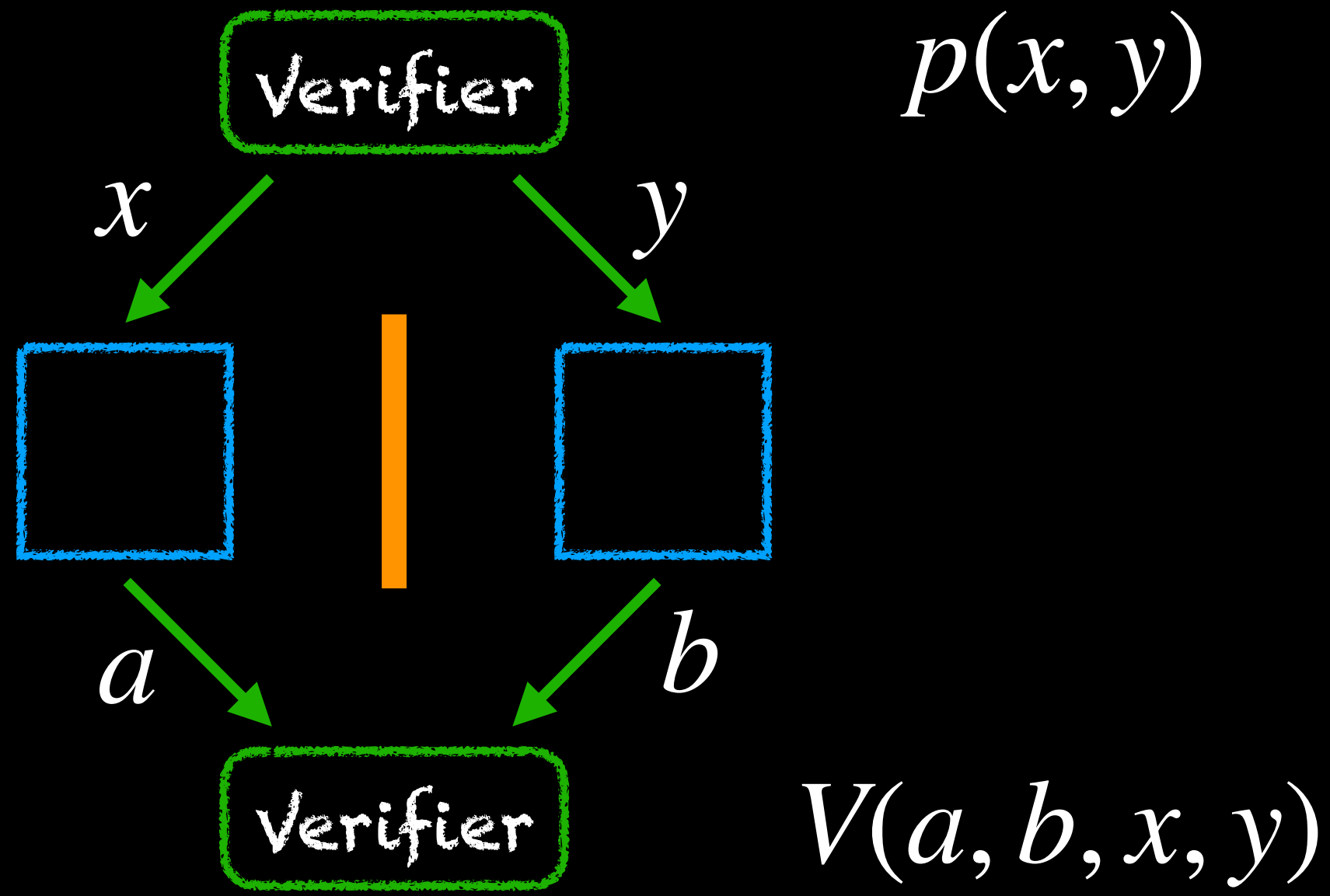
CNRS, University Grenoble-Alpes

Nonlocal games



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

Nonlocal games



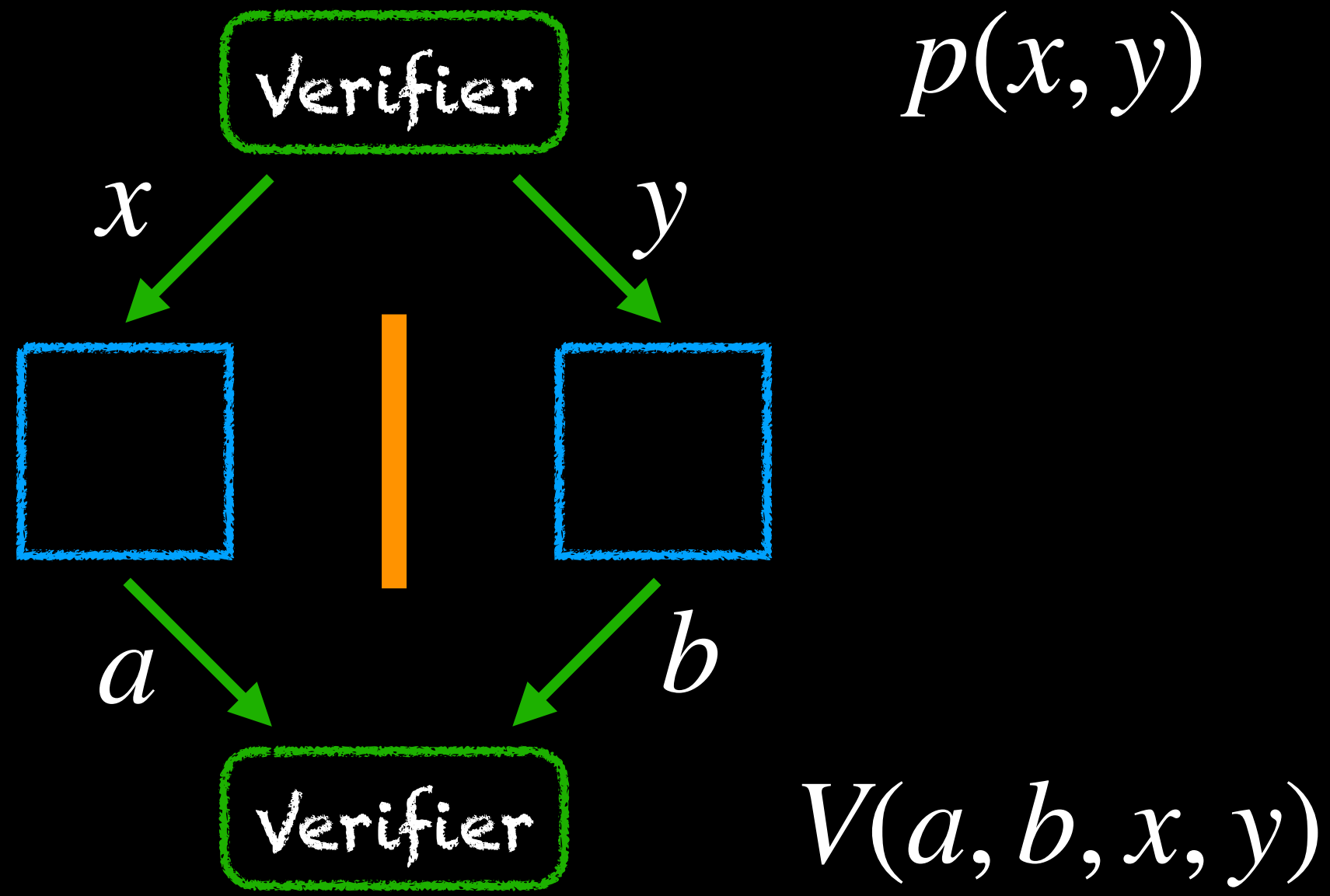
$$\omega = \sum_{a,b,x,y} p(x, y) p(a, b | x, y) V(a, b, x, y)$$

Classical
value

ω_c

$$p(a, b | x, y) = \int d\lambda p(a | x, \lambda) p(b | y, \lambda)$$

Nonlocal games



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

Quantum
value

ω_q

$$p(a, b | x, y) = \text{Tr} \left[M_a^x \otimes N_b^y \rho \right]$$

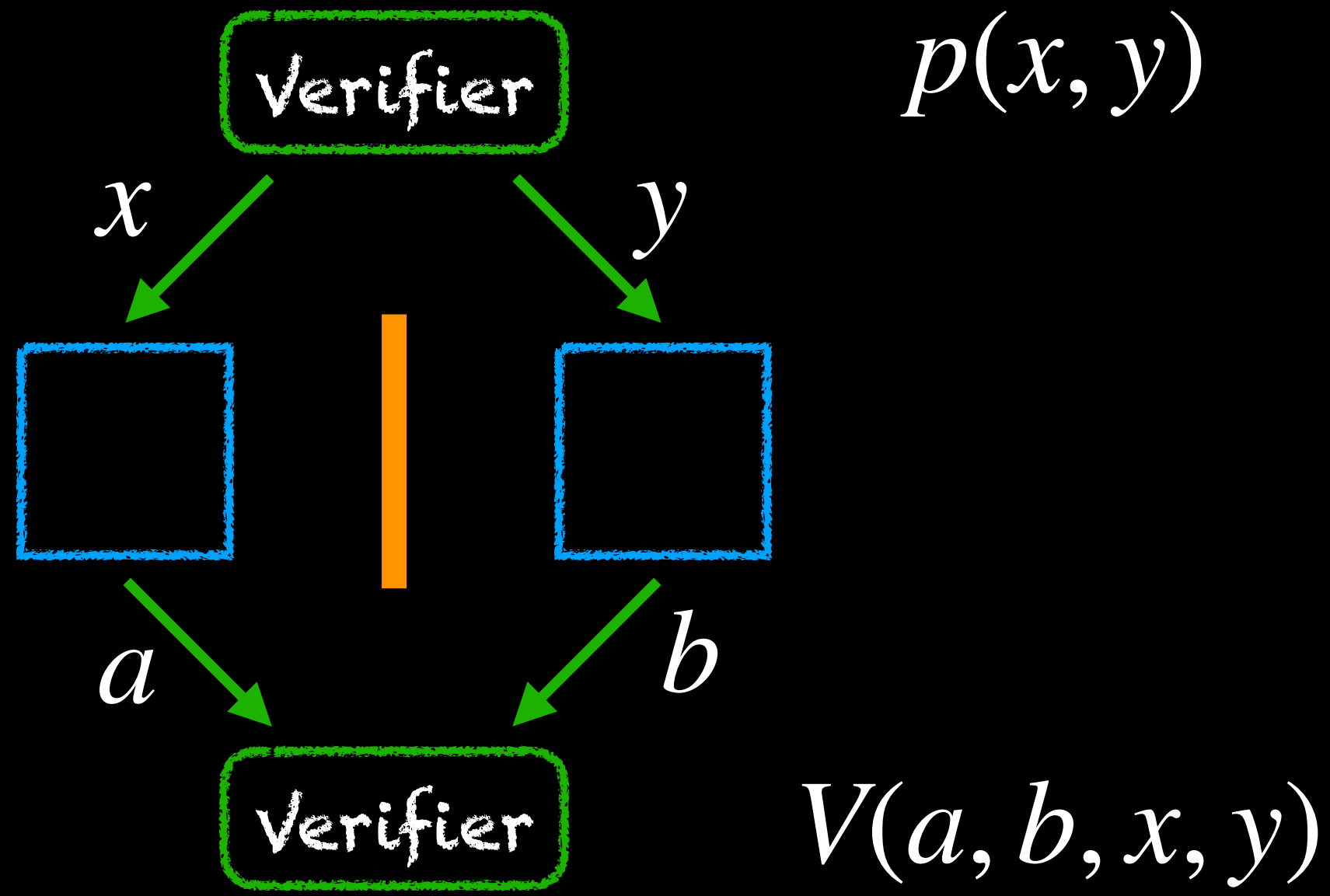
[Bell]

Classical
value

ω_c

$$p(a, b | x, y) = \int d\lambda p(a | x, \lambda) p(b | y, \lambda)$$

Nonlocal games



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

Non-signalling
value

ω_{ns}

$$p(a | x, y) = p(a | x), \quad p(b | x, y) = p(b | y)$$

[Popescu, Rohrlich]

Quantum
value

ω_q

$$p(a, b | x, y) = \text{Tr} \left[M_a^x \otimes N_b^y \rho \right]$$

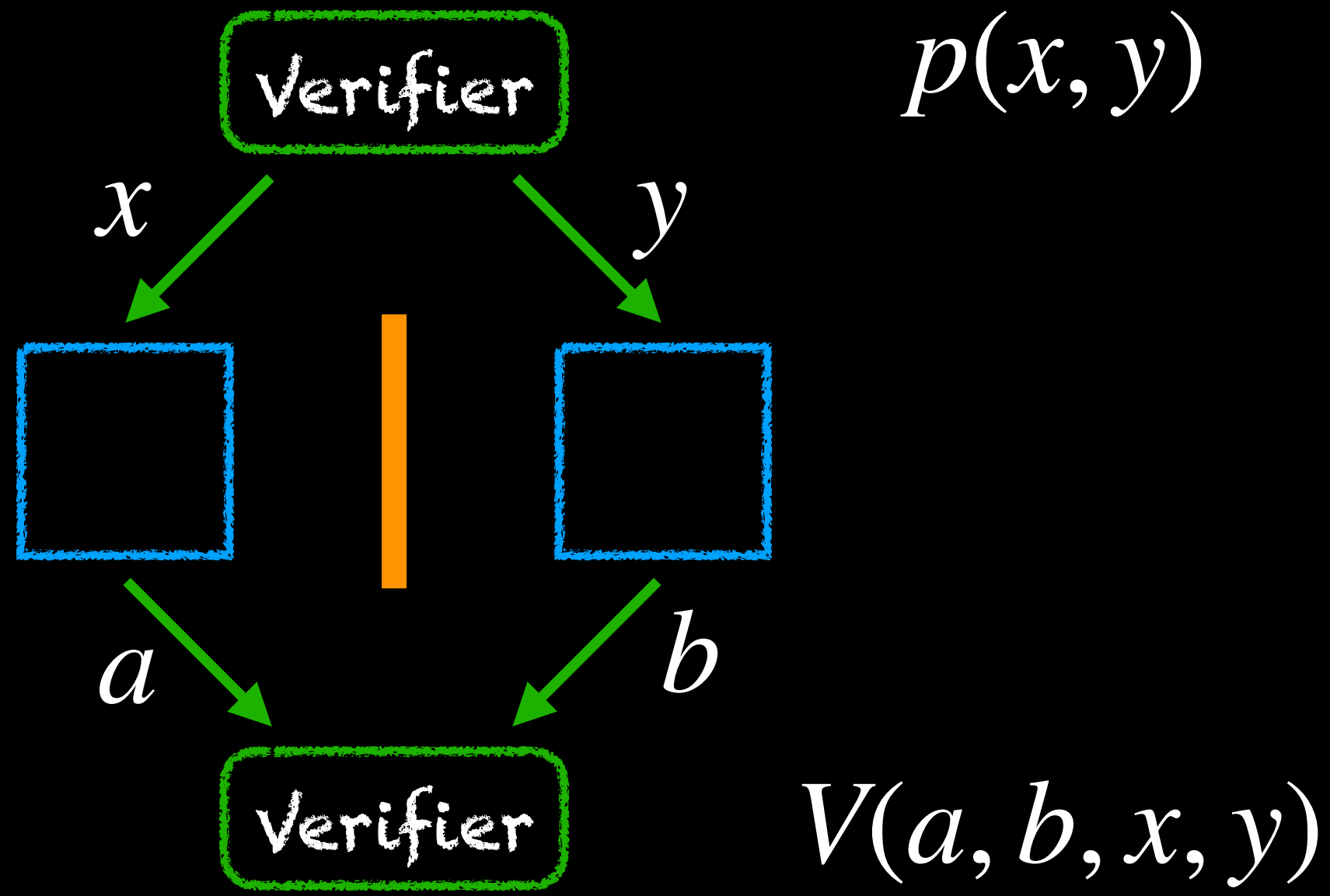
[Bell]

Classical
value

ω_c

$$p(a, b | x, y) = \int d\lambda p(a | x, \lambda) p(b | y, \lambda)$$

Nonlocal games



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

Non-signalling
value

ω_{ns}

$$p(a | x, y) = p(a | x), \quad p(b | x, y) = p(b | y)$$

[Popescu, Rohrlich]

Quantum
commuting
operator value

ω_{qc}

$$p(a, b | x, y) = \text{Tr} \left[M_a^x N_b^y \rho \right]$$

[MIP* = RE]

Quantum
value

ω_q

$$p(a, b | x, y) = \text{Tr} \left[M_a^x \otimes N_b^y \rho \right]$$

[Bell]

Classical
value

ω_c

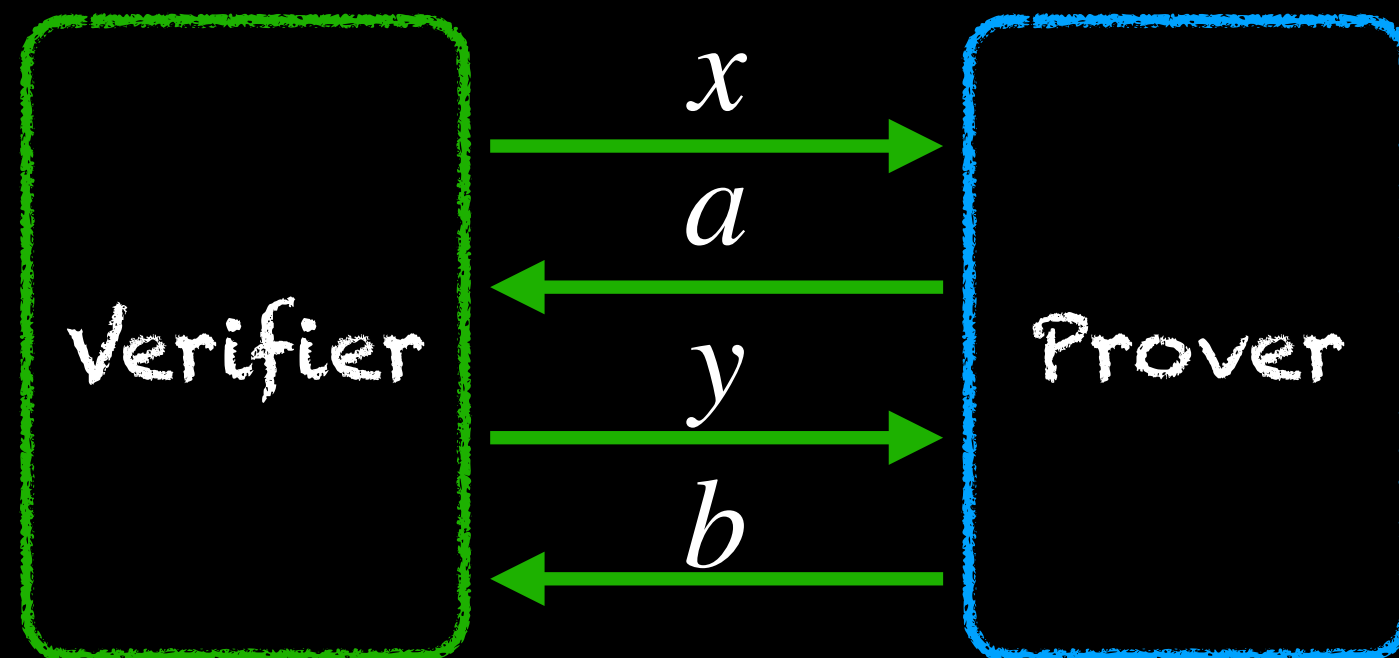
$$p(a, b | x, y) = \int d\lambda p(a | x, \lambda) p(b | y, \lambda)$$

Single-prover version

Can we remove the spatial separation requirement and play non-local games with a single (efficient) device?

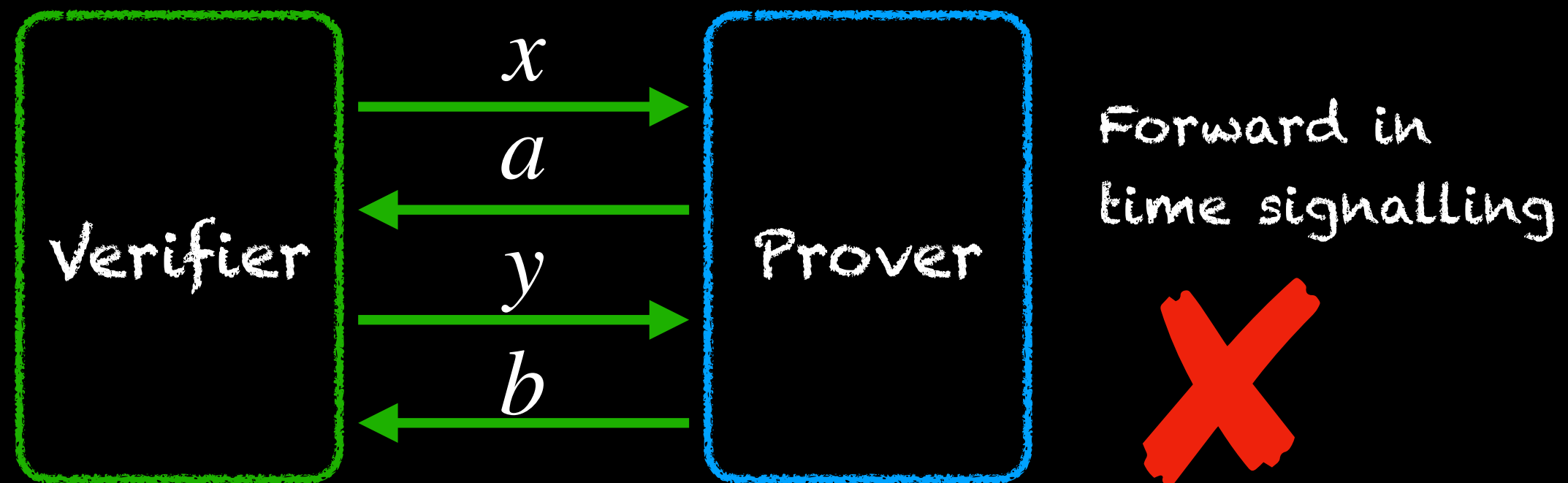
Single-prover version

Can we remove the spatial separation requirement and play non-local games with a single (efficient) device?



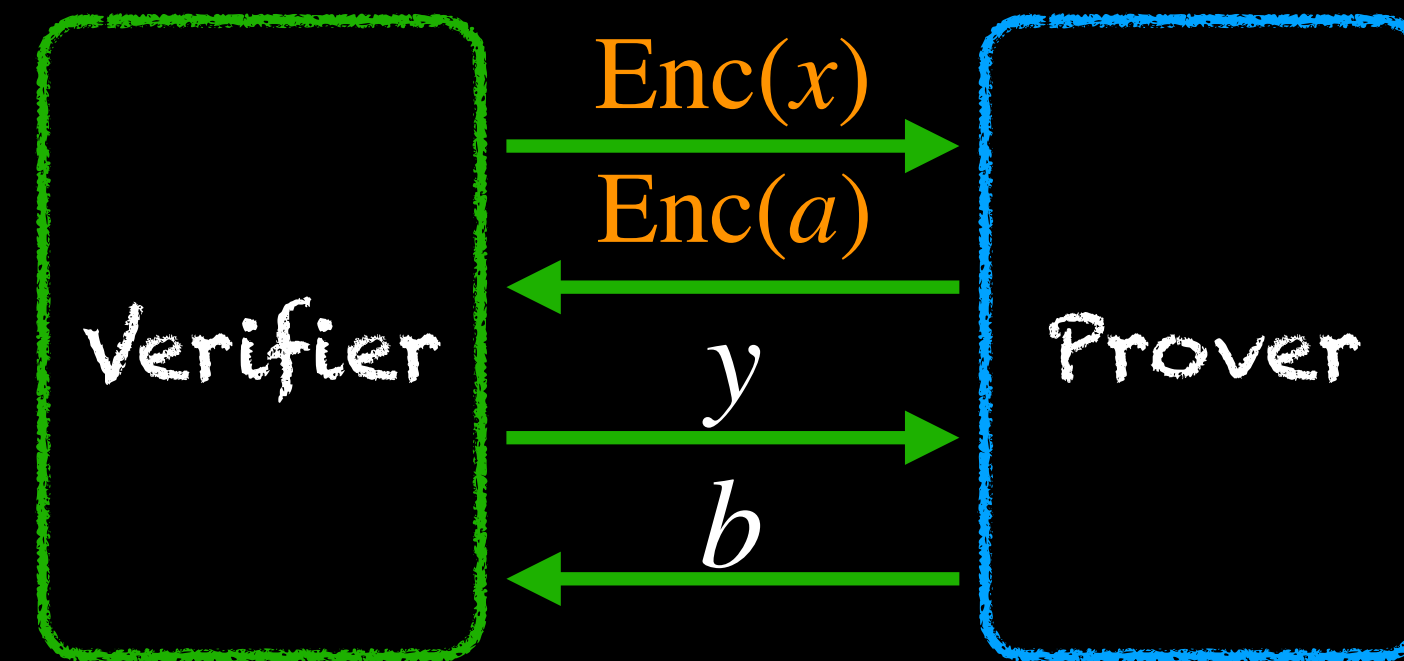
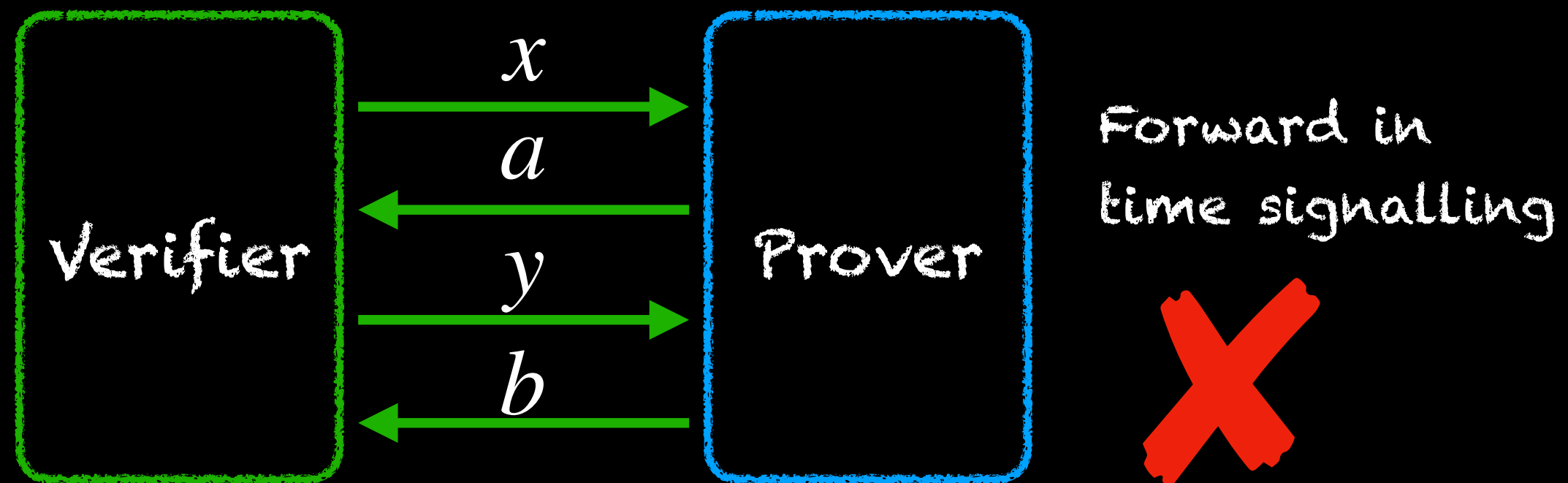
Single-prover version

Can we remove the spatial separation requirement and play non-local games with a single (efficient) device?



Single-prover version

Can we remove the spatial separation requirement and play non-local games with a single (efficient) device?

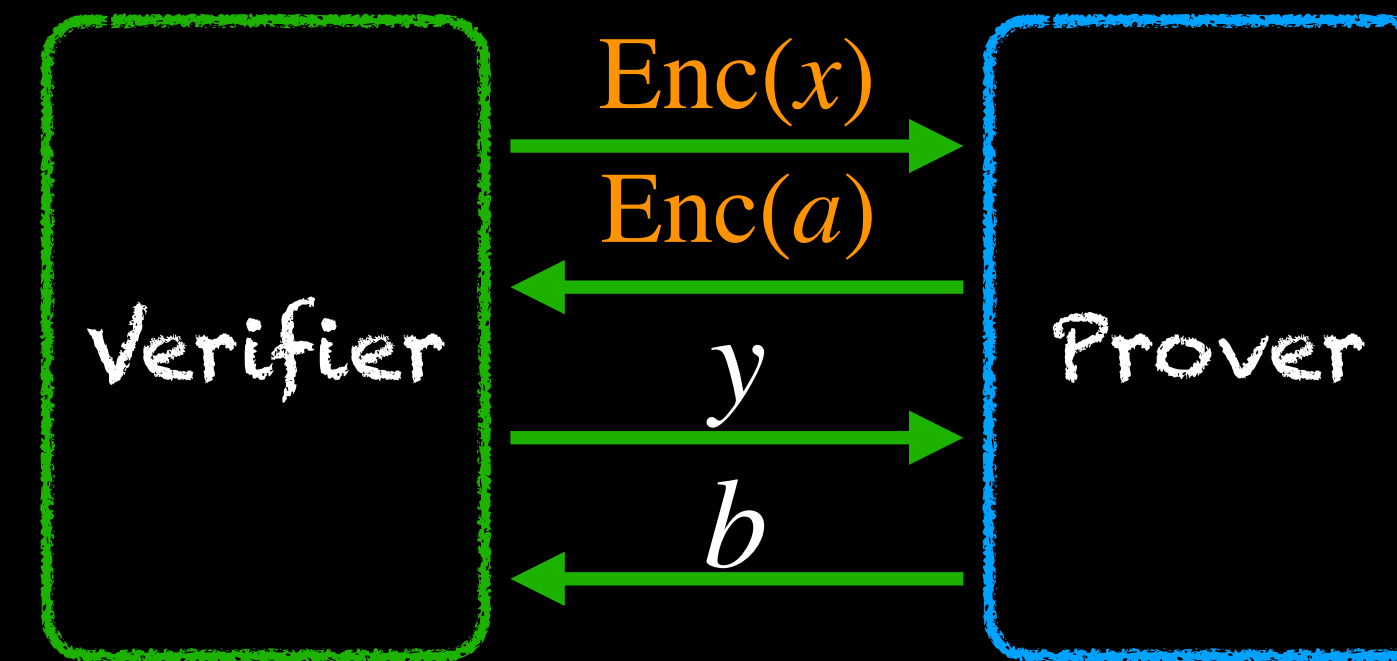
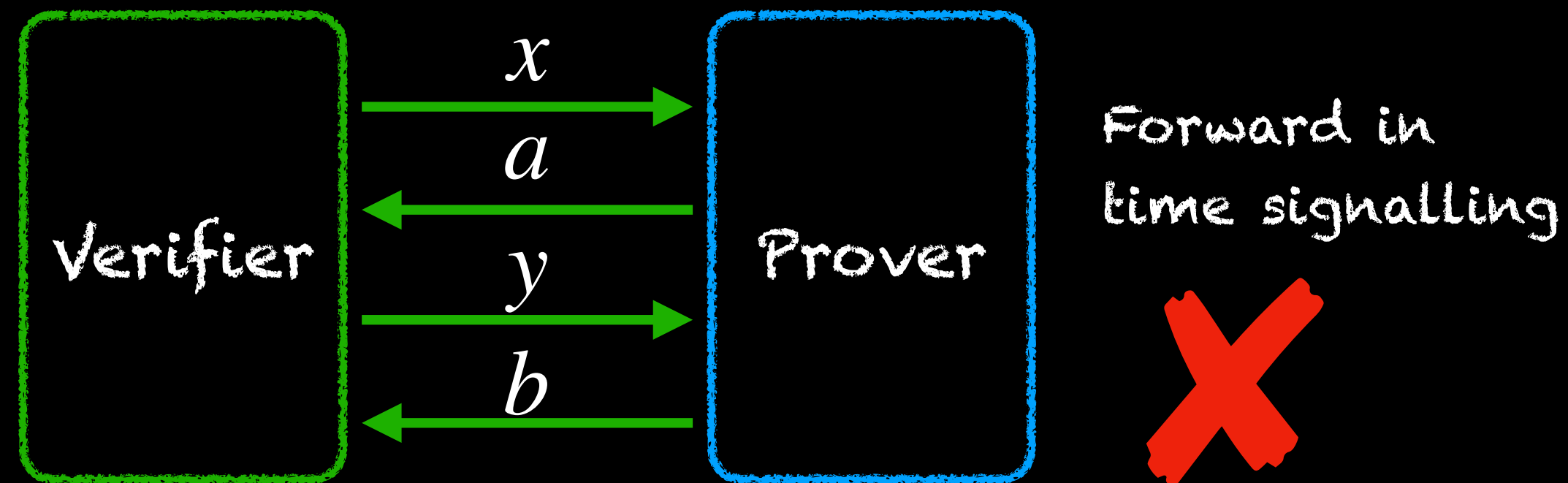


Secure encryption:
no-signalling !

But how can a prover do anything useful without knowing input?

Single-prover version

Use cryptography to force the prover to simulate spacelike players



Secure encryption:
no-signalling !

But how can a prover do anything useful without knowing input?

Homomorphic encryption!

Computation can be done on encrypted data.

Computation and encryption commute

Mahadev, Brakerski

KL $\forall$ Y compiler

Kalai, Lombardi, Vaikuntanathan, Yang

Quantum homomorphic encryption

Security parameter choice

Algo 1: Secret key generation

Algo 2: Input encryption

Algo 3: (Quantum) evaluation

Algo 4: Output decryption

Quantum homomorphic encryption

Security parameter choice

Algo 1: Secret key generation

Algo 2: Input encryption

Algo 3: (Quantum) evaluation

Algo 4: Output decryption

IND-CPA security: adversary's advantage in guessing the input compared to random guessing is negligible function of the security parameter

Correctness with auxiliary input: Implementing the encrypted circuit does not break entanglement

Quantum homomorphic encryption

Security parameter choice

Algo 1: Secret key generation

Algo 2: Input encryption

Algo 3: (Quantum) evaluation

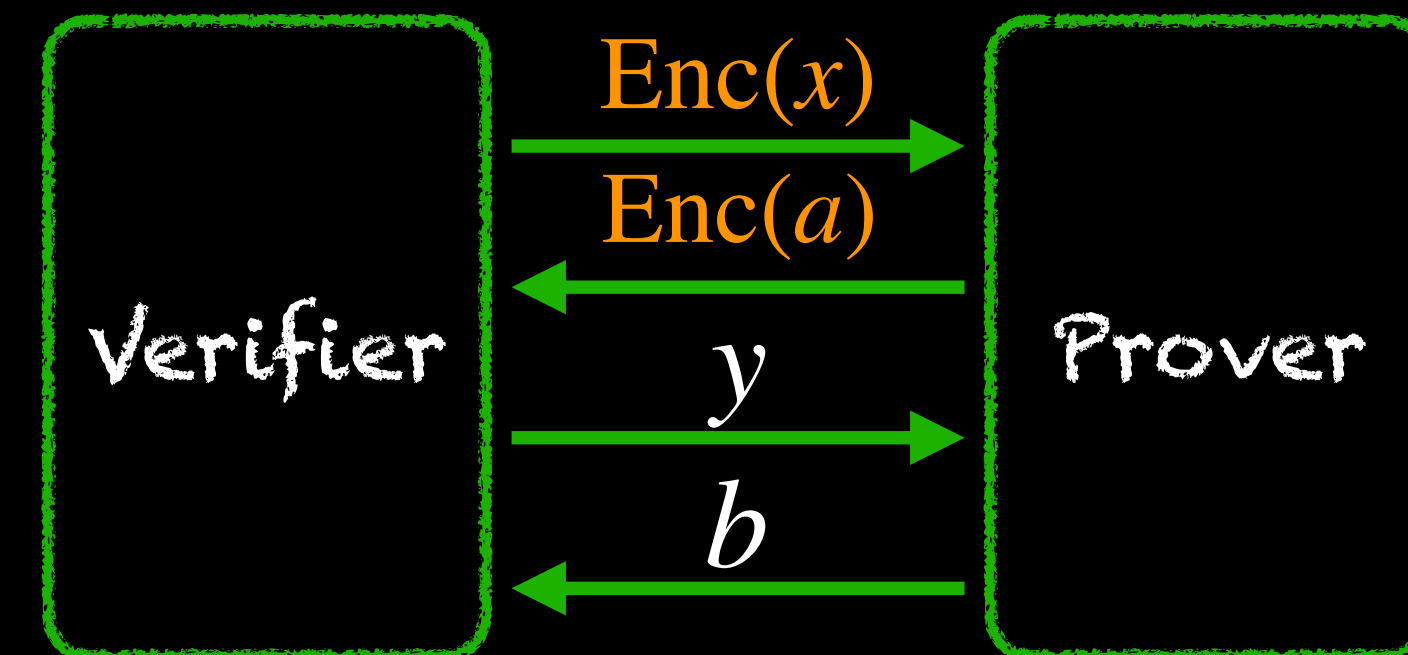
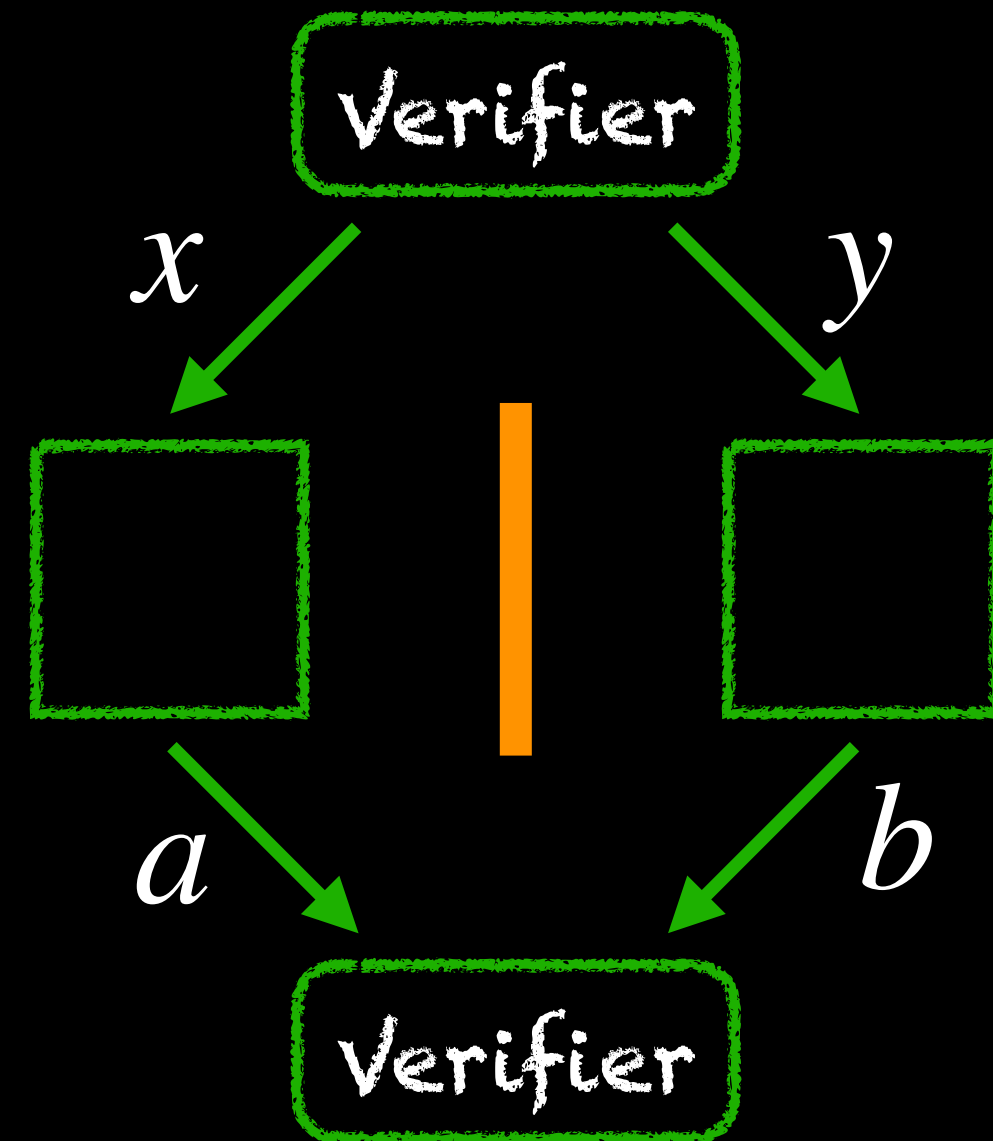
Algo 4: Output decryption

IND-CPA security: adversary's advantage in guessing the input compared to random guessing is negligible function of the security parameter

Correctness with auxiliary input: Implementing the encrypted circuit does not break entanglement

1. Adversary is computationally bounded!
2. Learning with errors is hard for quantum computers

Classical provers

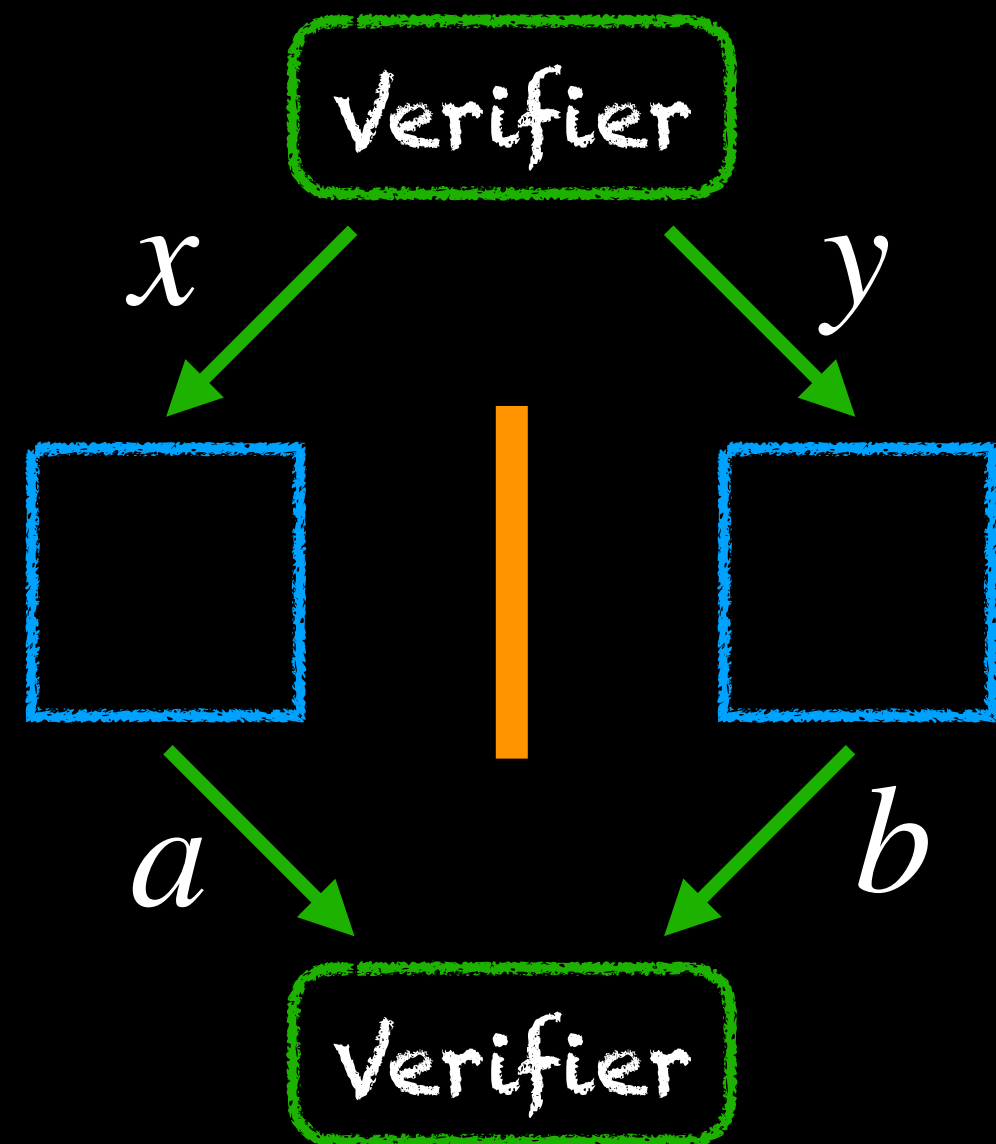


ω_c

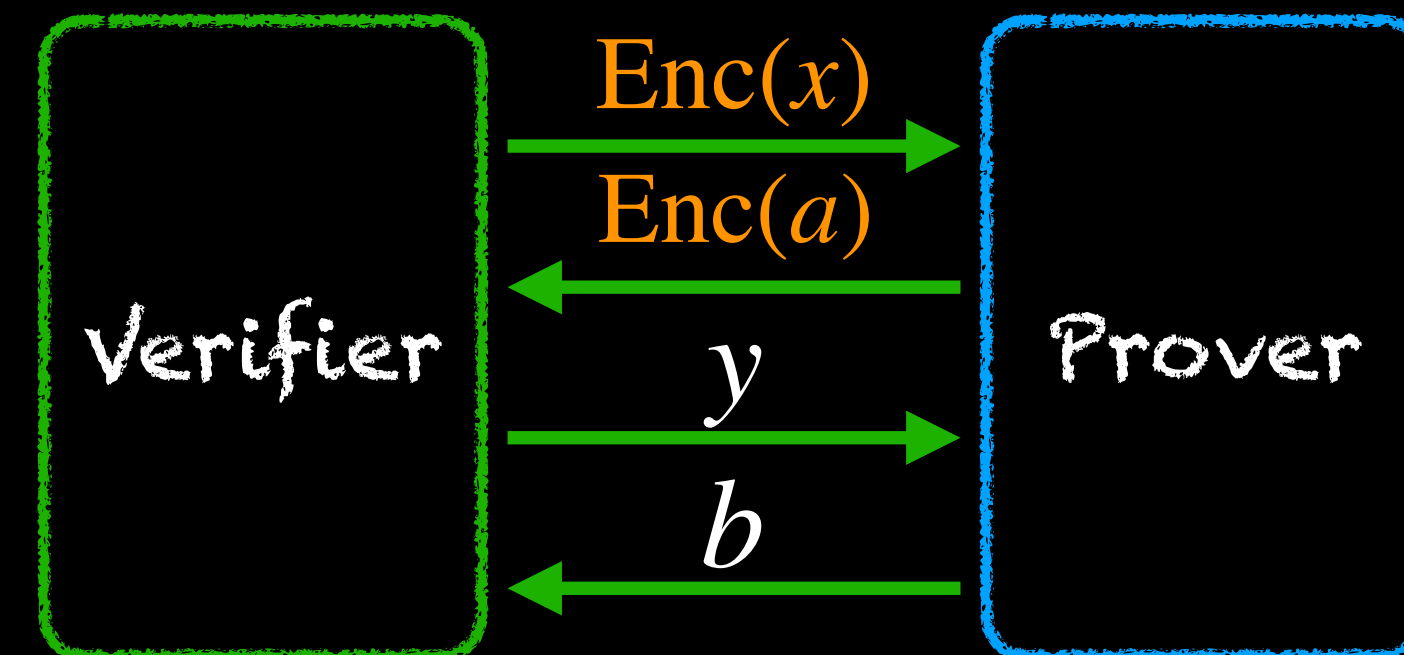
$\omega_c + \text{negl}(\lambda)$

Kalai, Lombardi, Vaikuntanathan, Yang

Quantum provers



ω_q



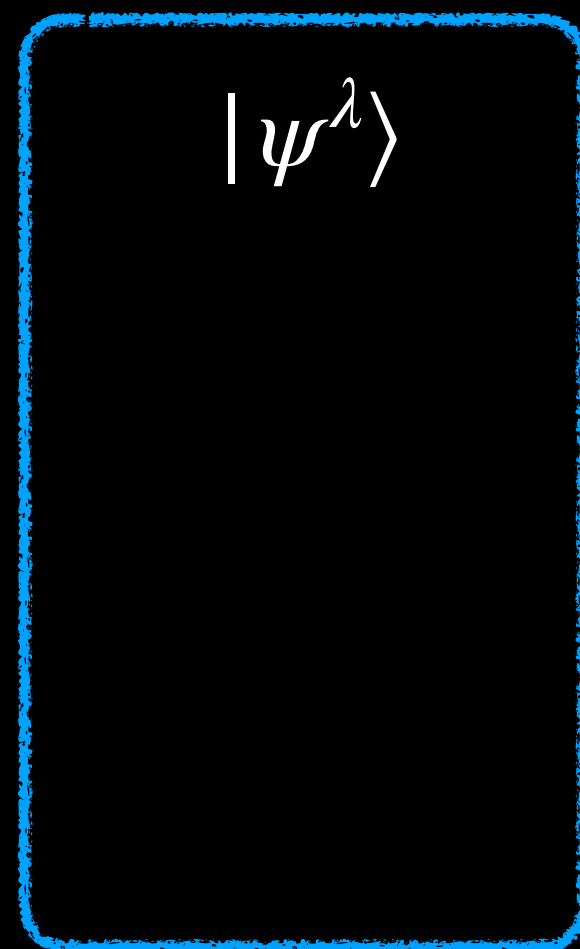
$\geq \omega_q$

Kalai, Lombardi, Vaikuntanathan, Yang

Quantum advantage from any nonlocal game

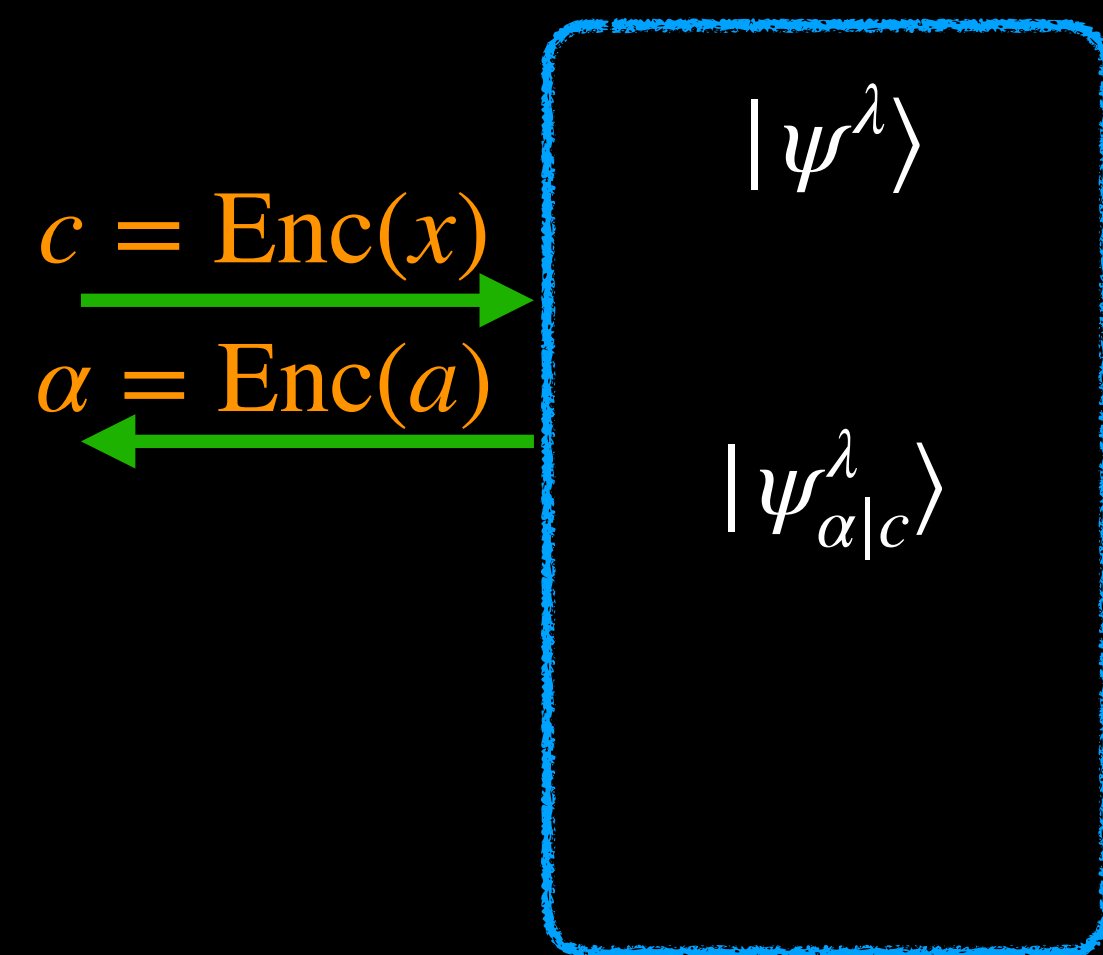
Quantum provers

What prover does?



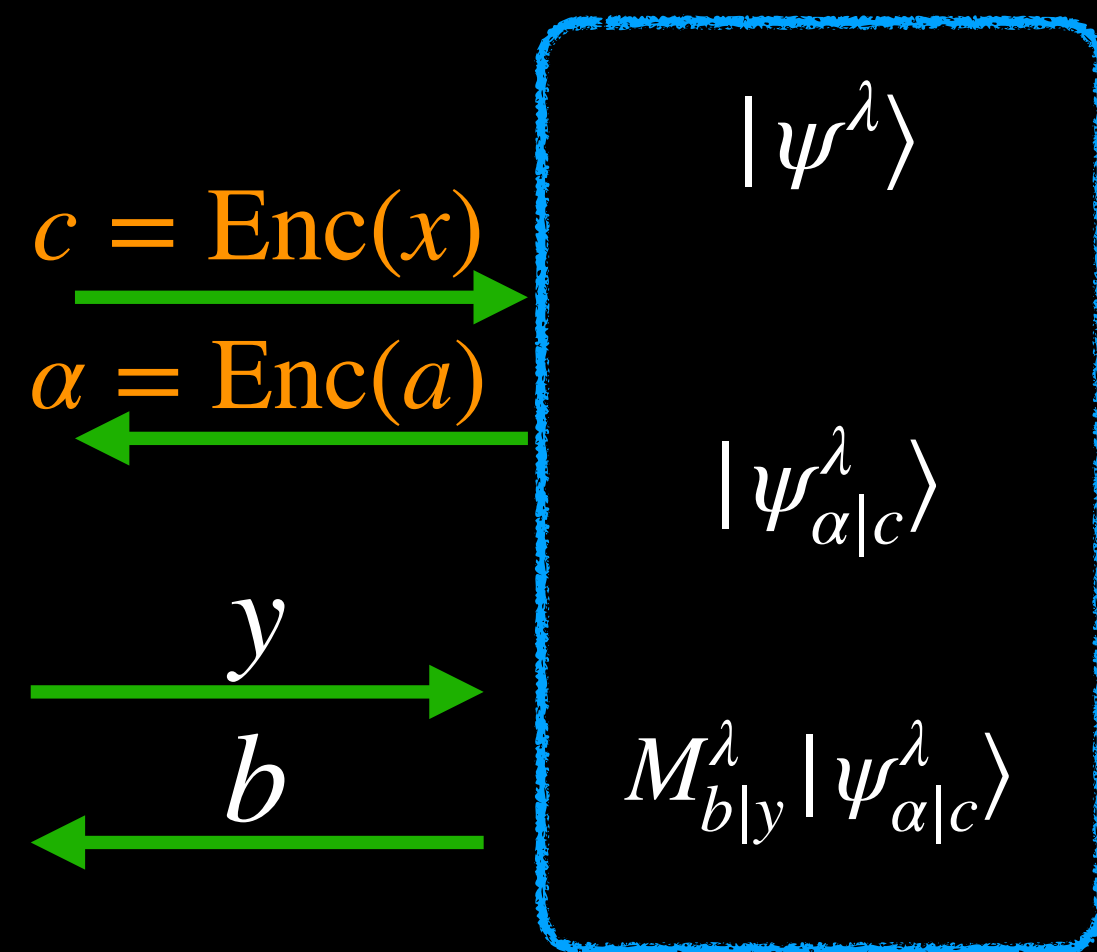
Quantum provers

What prover does?



Quantum provers

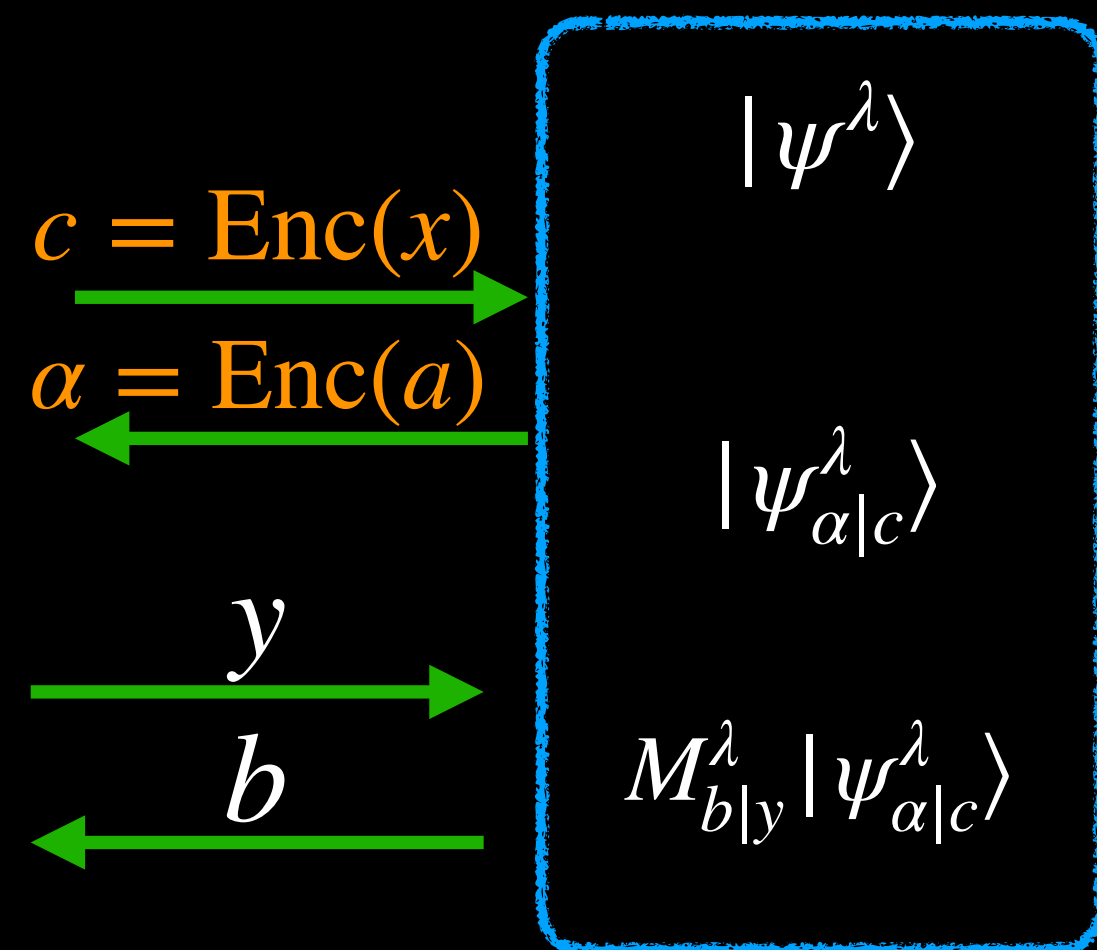
What prover does?



$$p(\alpha, b | c, y) = \langle \psi_{\alpha|c}^\lambda | M_{b|y}^\lambda | \psi_{\alpha|c}^\lambda \rangle$$

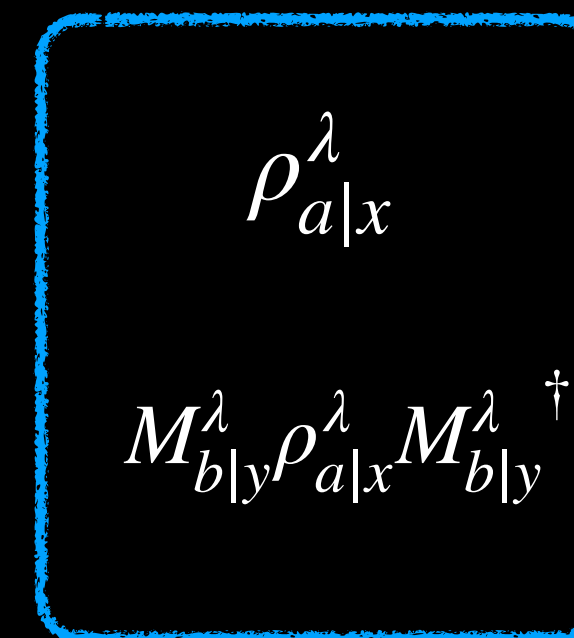
Quantum provers

What prover does?



$$p(\alpha, b | c, y) = \langle \psi_{\alpha|c}^\lambda | M_{b|y}^\lambda | \psi_{\alpha|c}^\lambda \rangle$$

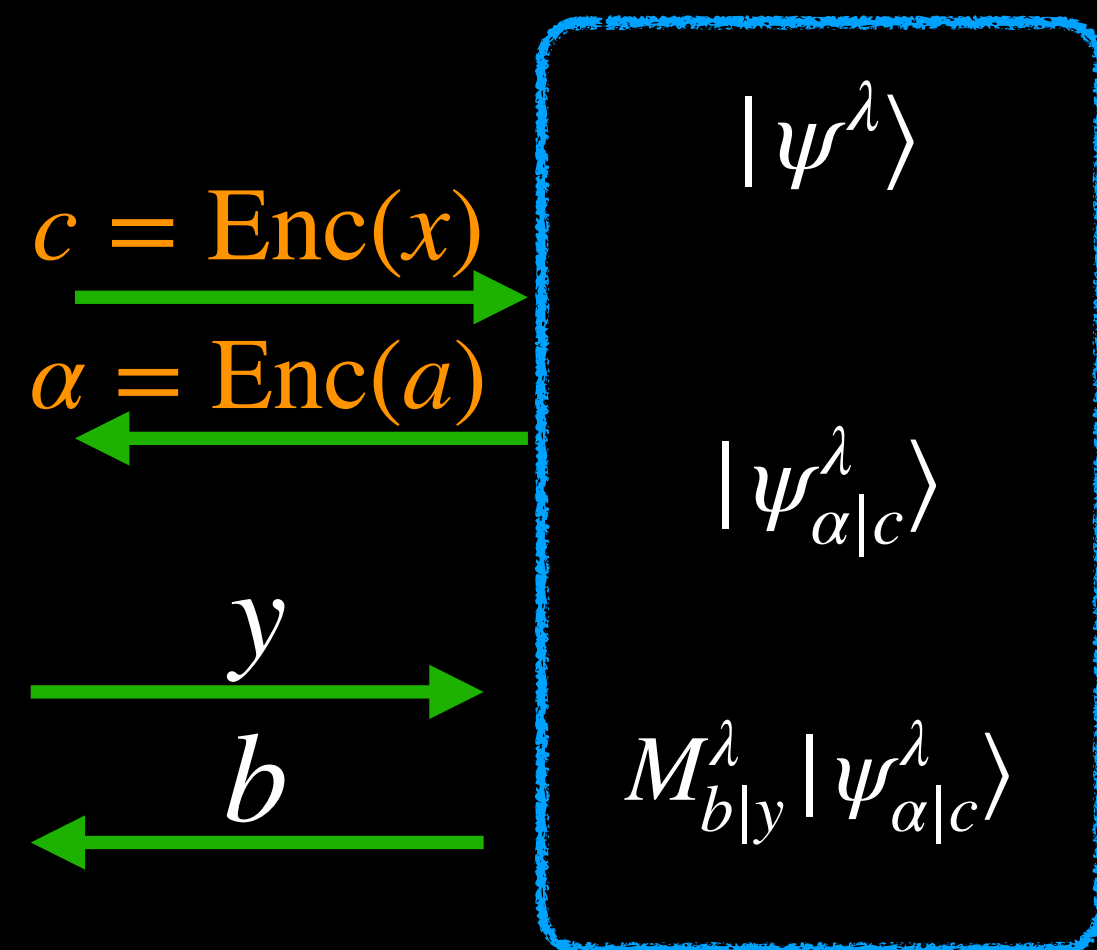
How verifier describes?



$$p(a, b | x, y) = \text{Tr} \left[M_{b|y}^\lambda \rho_{a|x}^\lambda \right]$$

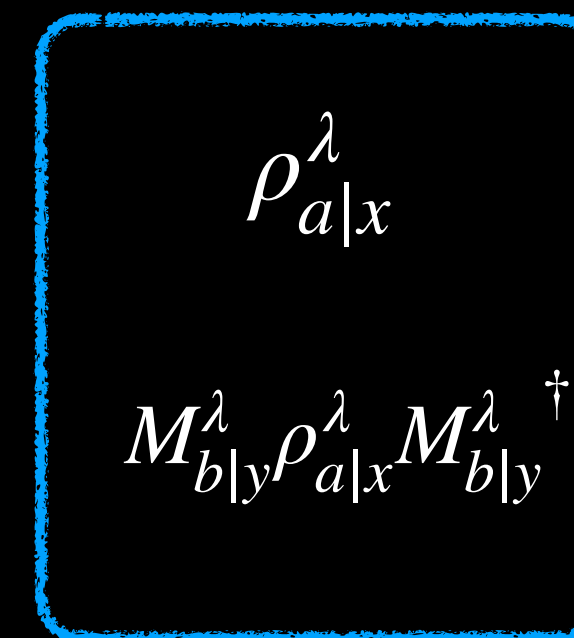
Quantum provers

What prover does?



$$p(\alpha, b | c, y) = \langle \psi_{\alpha|c}^\lambda | M_{b|y}^\lambda | \psi_{\alpha|c}^\lambda \rangle$$

How verifier describes?



$$p(a, b | x, y) = \text{Tr} \left[M_{b|y}^\lambda \rho_{a|x}^\lambda \right]$$

$$\text{Encryption security (IND-CPA): } \sum_a \rho_{a|x}^\lambda \approx_\lambda \sum_a \rho_{a|x'}^\lambda$$

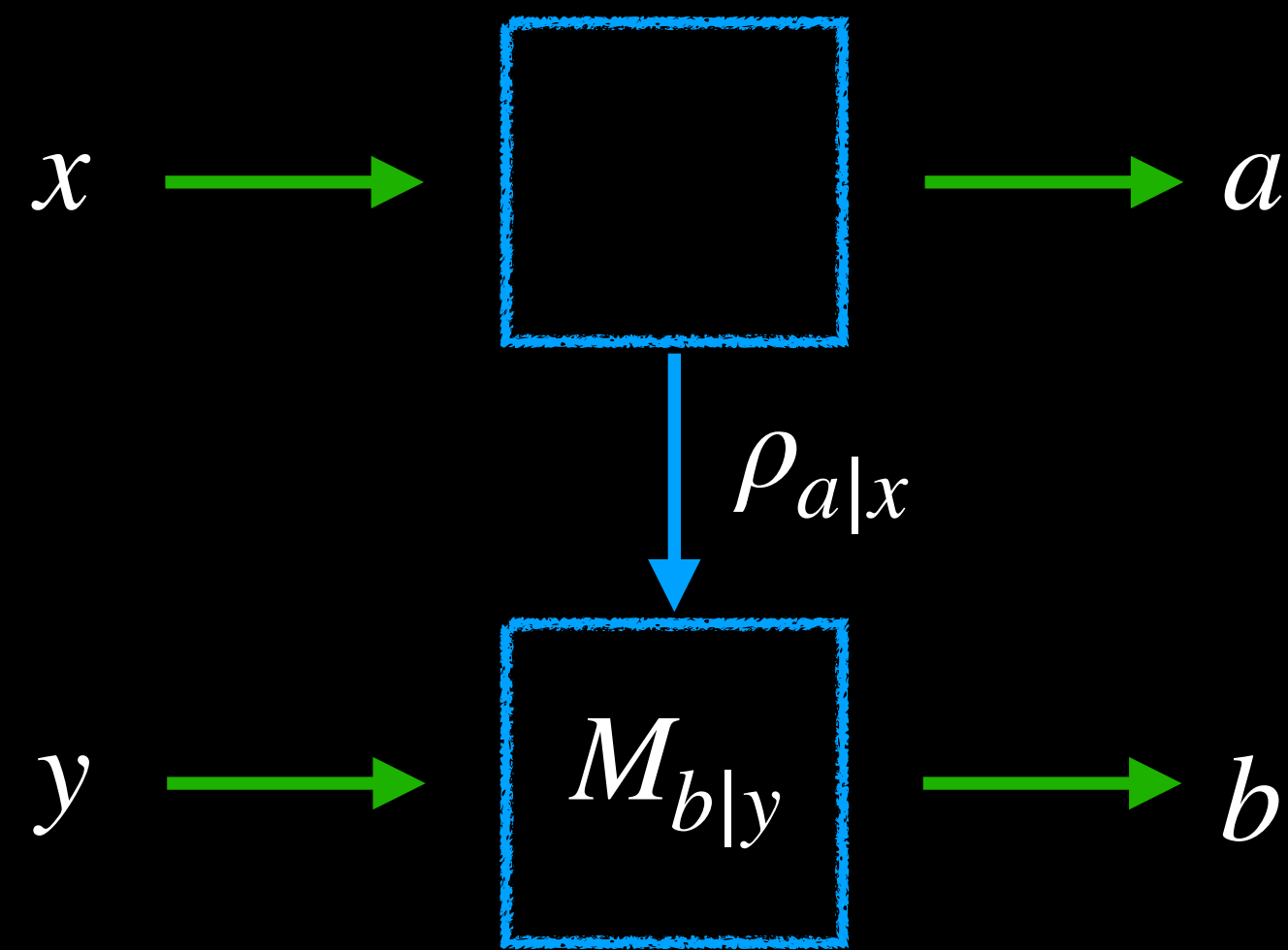
No efficient measurement can distinguish marginal states

Computational indistinguishability

Sequential games

Idealisation!

From quantum prover's strategy we construct a quantum strategy for prepare-and-measure game!

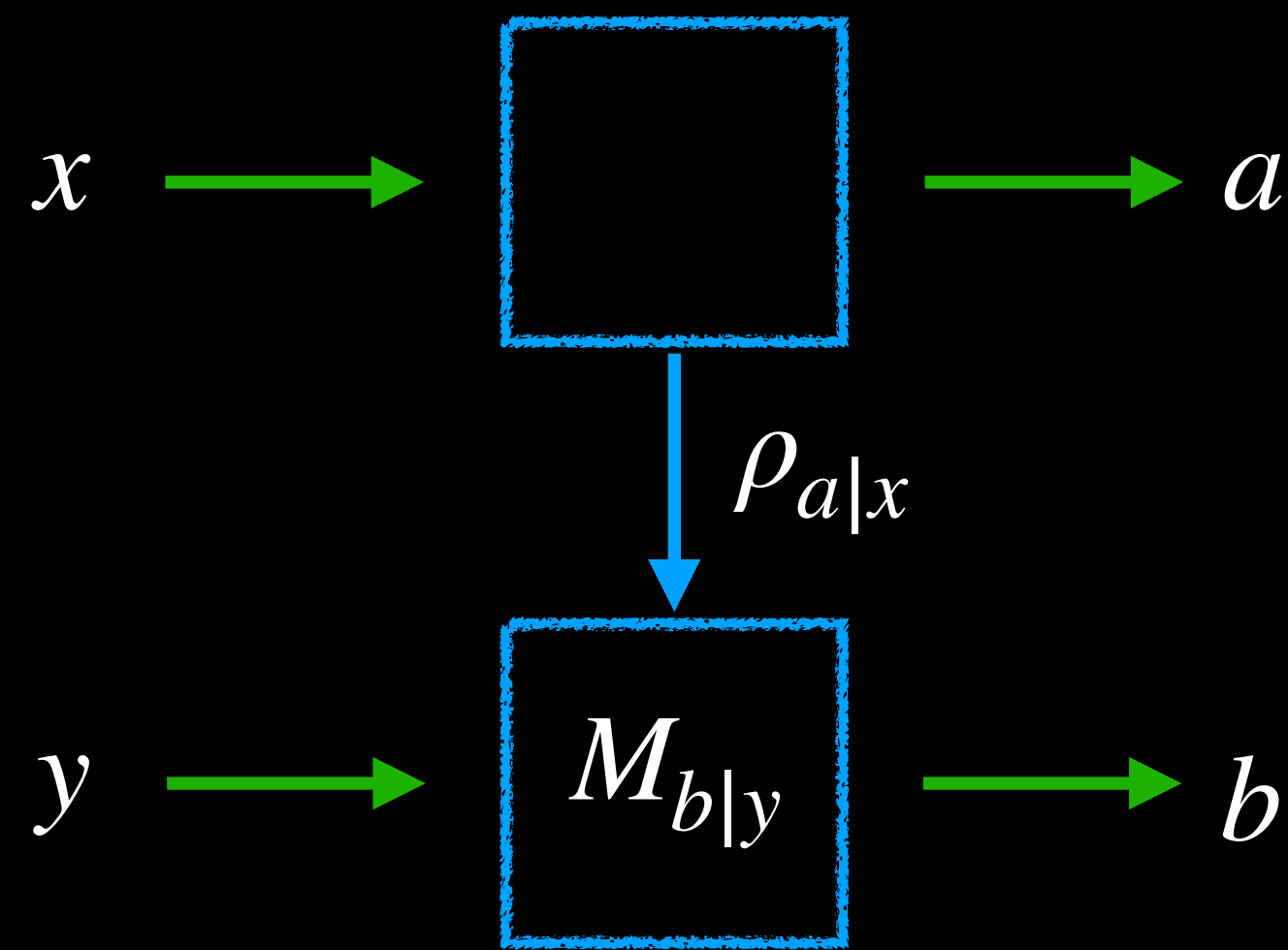


$$p(a, b | x, y) = \text{Tr} \left[M_{b|y} \rho_{a|x} \right]$$

Sequential games

Idealisation!

From quantum prover's strategy we construct a quantum strategy for prepare-and-measure game!



$$p(a, b | x, y) = \text{Tr} \left[M_{b|y} \rho_{a|x} \right]$$

Preparation equivalence

$$\sum_a \rho_{a|x} = \sum_a \rho_{a|x'}$$

Spekkens

S-G-HJW theorem

$$\rho_{a|x} = \text{Tr}_A \left[M_{a|x} \otimes M_{b|y} \rho \right]$$

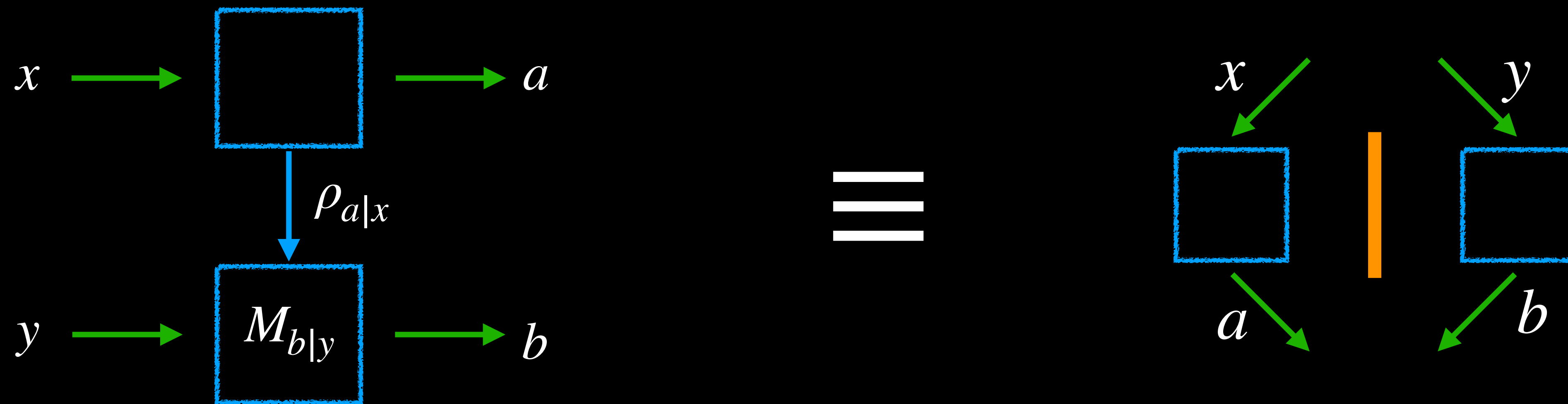
Schrodinger

Gisin

Hughston, Jozsa, Wootters

$$p(a, b | x, y) = \text{Tr} \left[M_{a|x} \otimes M_{b|y} \rho \right]$$

Sequential games



The set of quantum correlations stemming from sequential games with preparation equivalence is the same as the set of quantum Bell correlations.

Security parameter

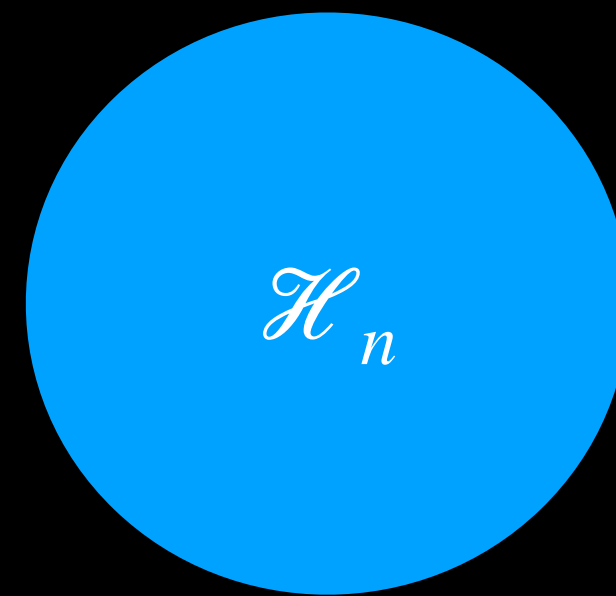
The size of ciphertexts and dimension of Hilbert space grow with λ

For every λ states after the first round are computationally indistinguishable:

$$\rho_x \approx_\lambda \rho_{x'}$$

Not secure

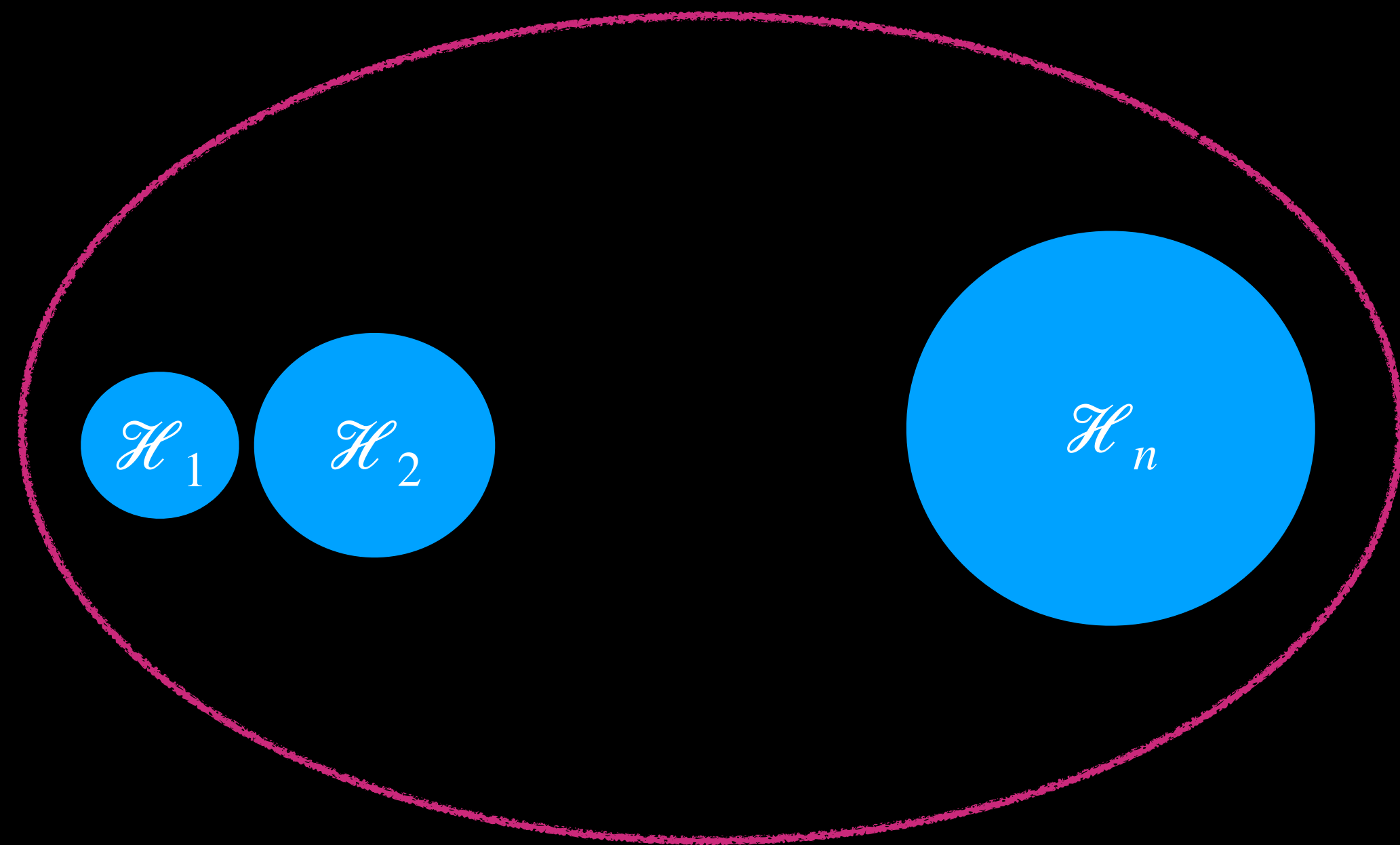
Very secure λ



In the limit $\lambda \rightarrow \infty$ we expect to have perfect indistinguishability, but what is the limiting strategy?

Asymptotic Limit

Universal C^* algebra



Universal POVM algebra: Slofstra

Generated by $\check{f}_{b|y} \in \mathcal{A}_B$ that are

1. Self-adjoint
2. Positive
3. sums to identity

Universality property: For every concrete realisation of this algebra on $\mathcal{H}_\lambda$ there is a representation π_λ such that

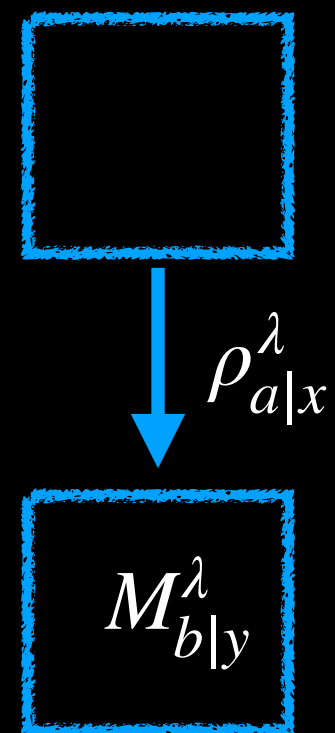
$$\pi_\lambda(\check{f}_{b|y}) = M_{b|y}^\lambda$$

Asymptotic Limit

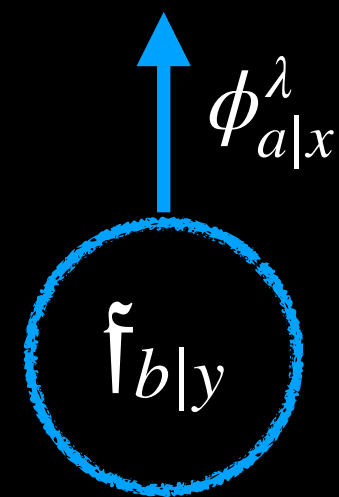
Algebraic description of correlations:

Define algebraic state: $\phi_{a|x}^\lambda(\tilde{\mathbf{f}}) = \text{Tr} \left[\rho_{a|x}^\lambda \pi_\lambda(\tilde{\mathbf{f}}) \right]$

$$\phi_{a|x}^\lambda(\tilde{\mathbf{f}}_{b|y}) = p^\lambda(a, b | x, y)$$



$$p^\lambda(a, b | x, y) = \phi_{a|x}^\lambda(\tilde{\mathbf{f}}_{b|y})$$



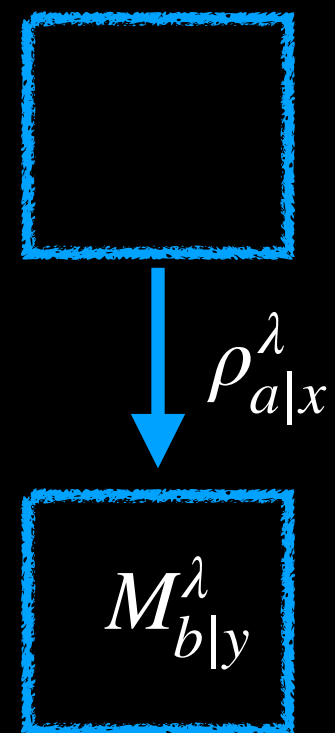
$$p^\lambda(a, b | x, y) = \text{Tr} \left[M_{b|y}^\lambda \rho_{a|x}^\lambda \right]$$

Asymptotic Limit

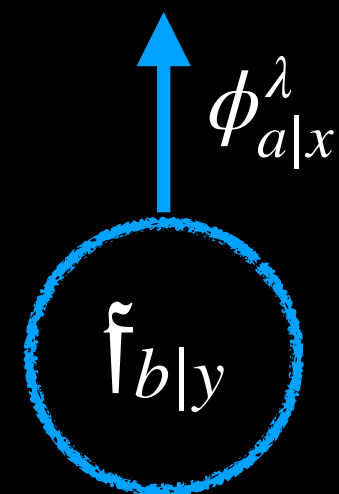
Algebraic description of correlations:

Define algebraic state: $\phi_{a|x}^\lambda(\tilde{f}) = \text{Tr} \left[\rho_{a|x}^\lambda \pi_\lambda(\tilde{f}) \right]$

$$\phi_{a|x}^\lambda(\tilde{f}_{b|y}) = p^\lambda(a, b | x, y)$$



$$p^\lambda(a, b | x, y) = \phi_{a|x}^\lambda(\tilde{f}_{b|y})$$



$$p^\lambda(a, b | x, y) = \text{Tr} \left[M_{b|y}^\lambda \rho_{a|x}^\lambda \right]$$

Banach-Alaoglu theorem:

Unit ball of the set of algebraic states is compact.

We can define limit states:

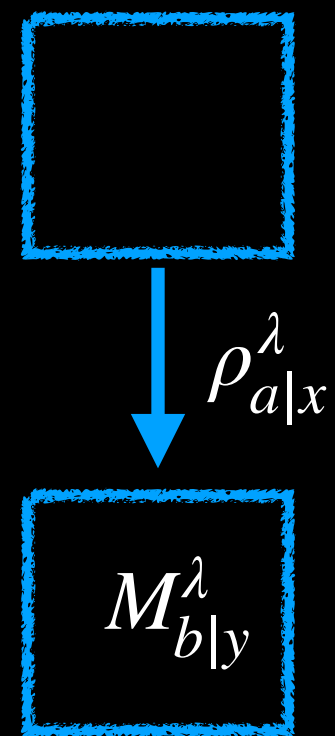
$$\phi_{a|x} = \lim_{\lambda \rightarrow \infty} \phi_{a|x}^\lambda$$

Asymptotic Limit

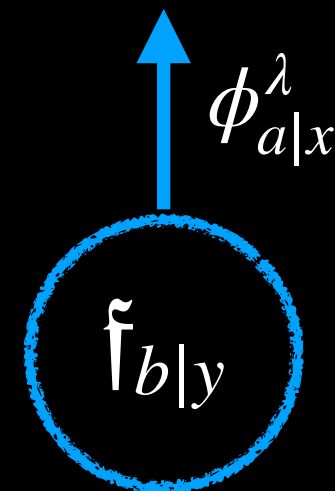
Algebraic description of correlations:

Define algebraic state: $\phi_{a|x}^\lambda(\tilde{f}) = \text{Tr} \left[\rho_{a|x}^\lambda \pi_\lambda(\tilde{f}) \right]$

$$\phi_{a|x}^\lambda(\tilde{f}_{b|y}) = p^\lambda(a, b | x, y)$$



$$p^\lambda(a, b | x, y) = \phi_{a|x}^\lambda(\tilde{f}_{b|y})$$



$$p^\lambda(a, b | x, y) = \text{Tr} \left[M_{b|y}^\lambda \rho_{a|x}^\lambda \right]$$

We can define limit states:

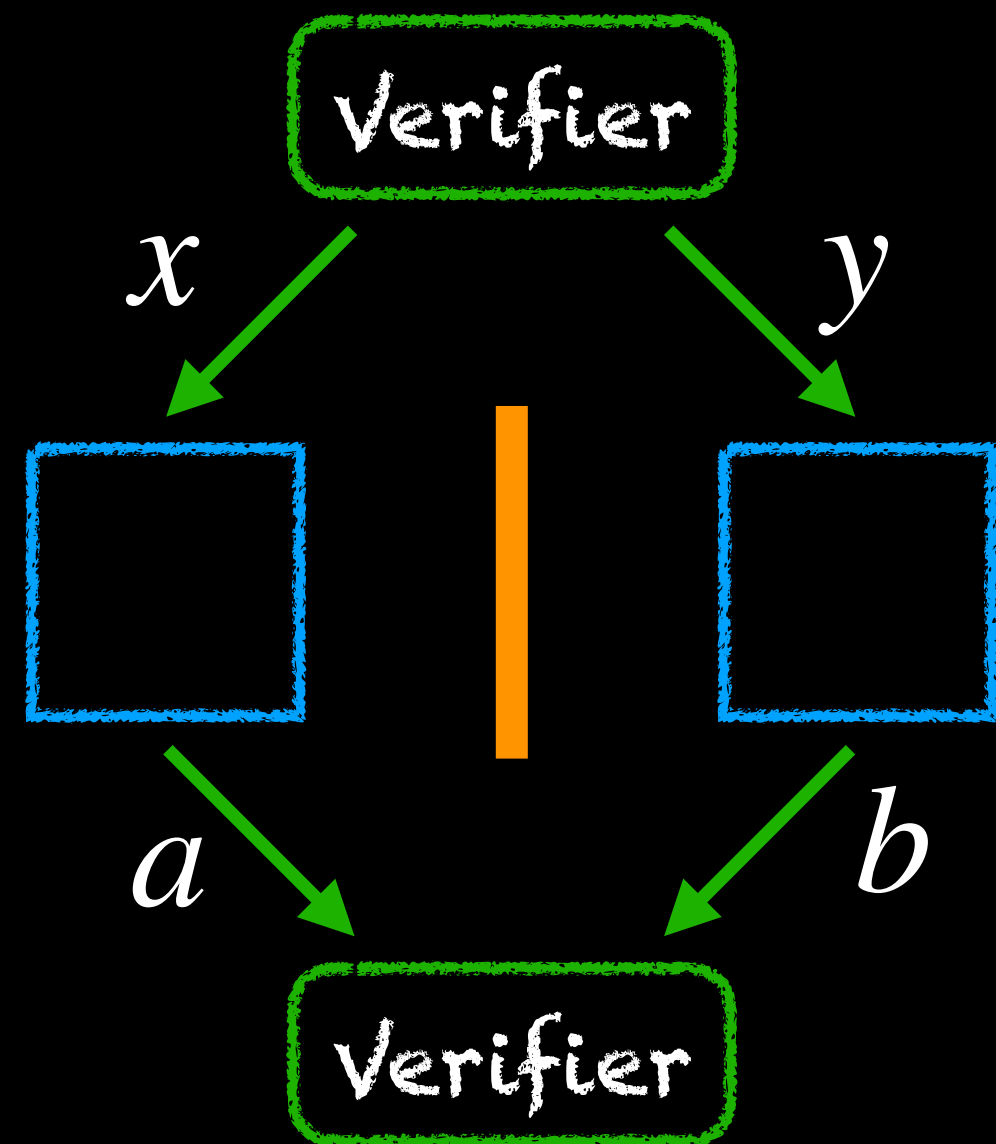
$$\phi_{a|x} = \lim_{\lambda \rightarrow \infty} \phi_{a|x}^\lambda$$

Limiting marginal states will satisfy perfect no-signalling (efficient measurements fill the full algebra!):

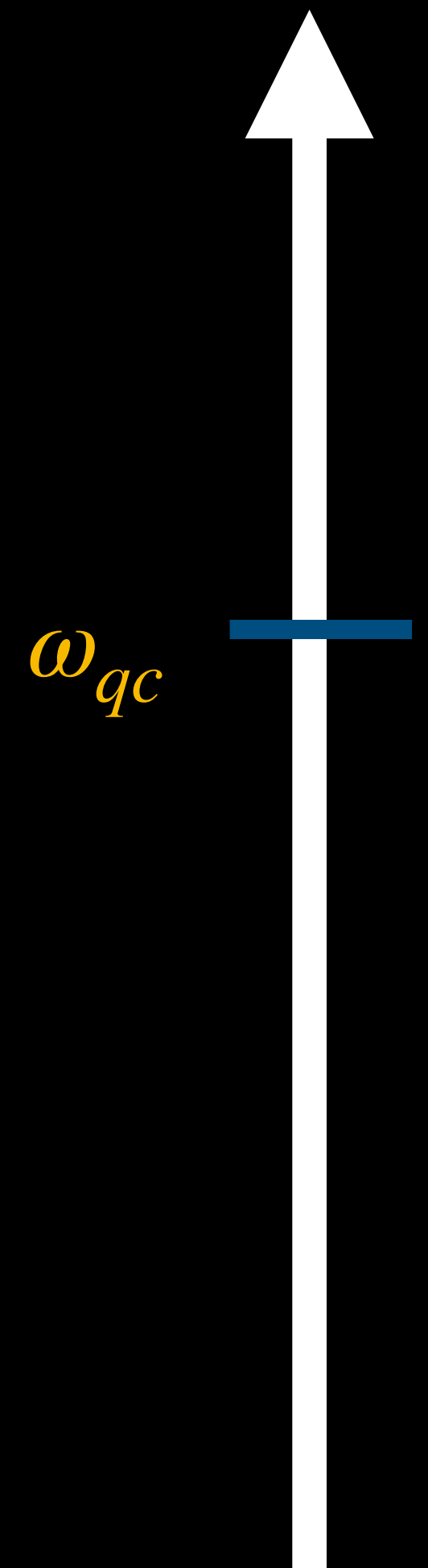
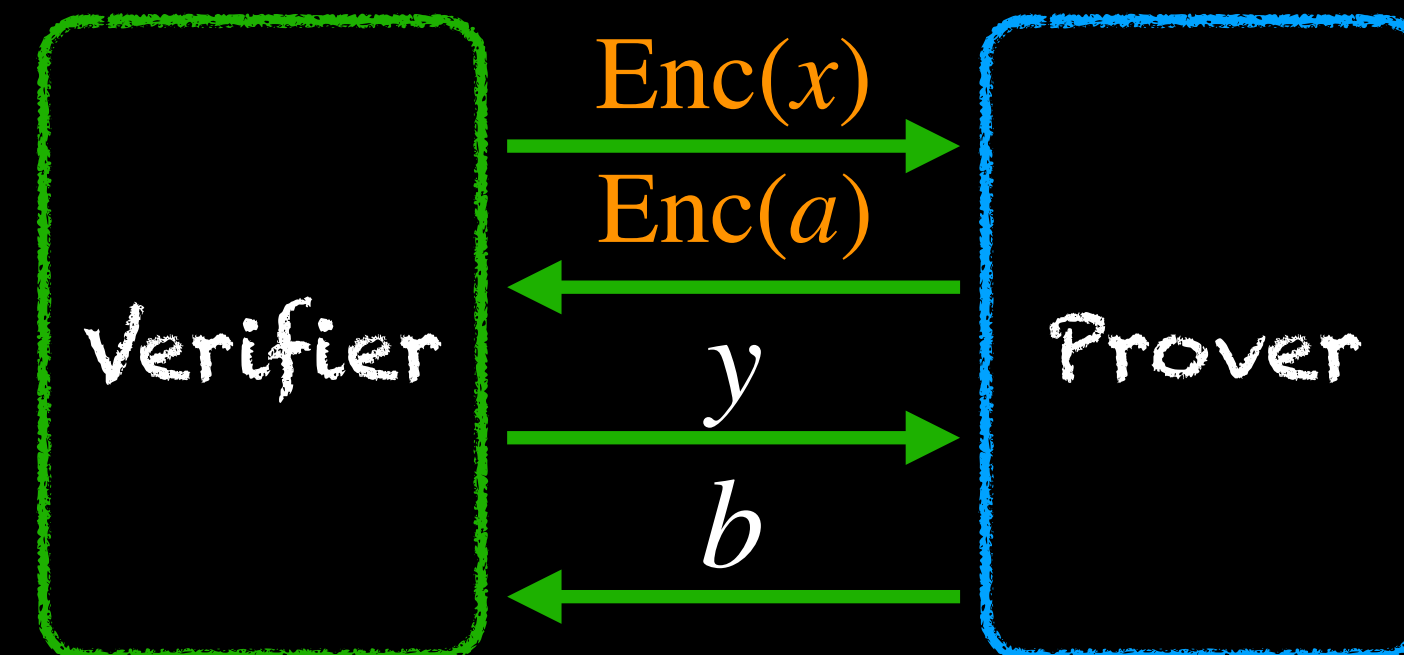
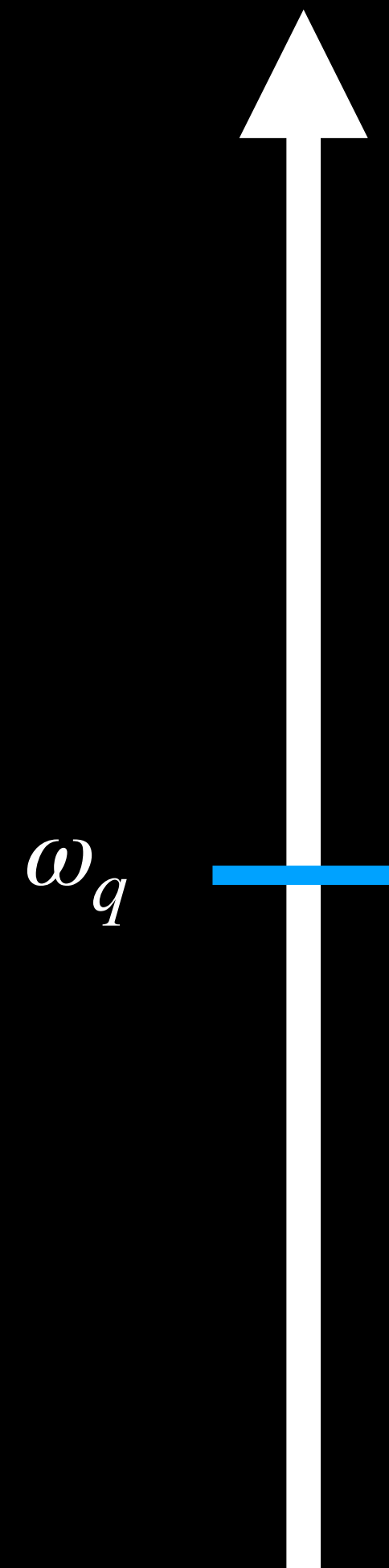
$$\sum_a \phi_{a|x} = \sum_a \phi_{a|x'}$$

Algebraic equivalent of S-G-HJW theorem is called Radon-Nikodym theorem, and it allows to get: $\phi_{a|x}(\tilde{f}_{b|y}) = \langle \Omega_\phi | M_{a|x} M_{b|y} | \Omega_\phi \rangle$

Quantum provers



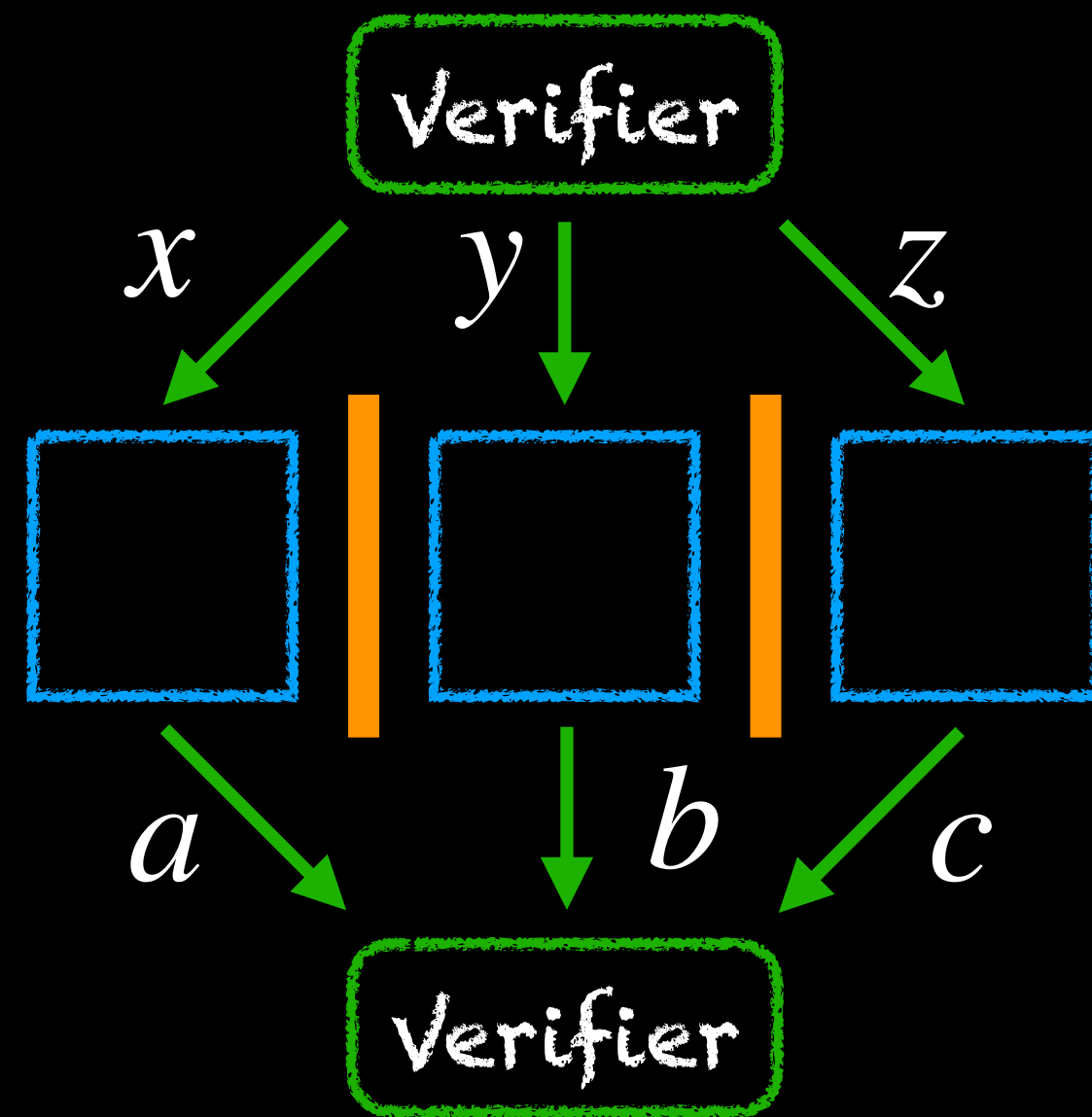
$$p(a, b | x, y) = \text{Tr} \left[M_a^x \otimes N_b^y \rho \right]$$



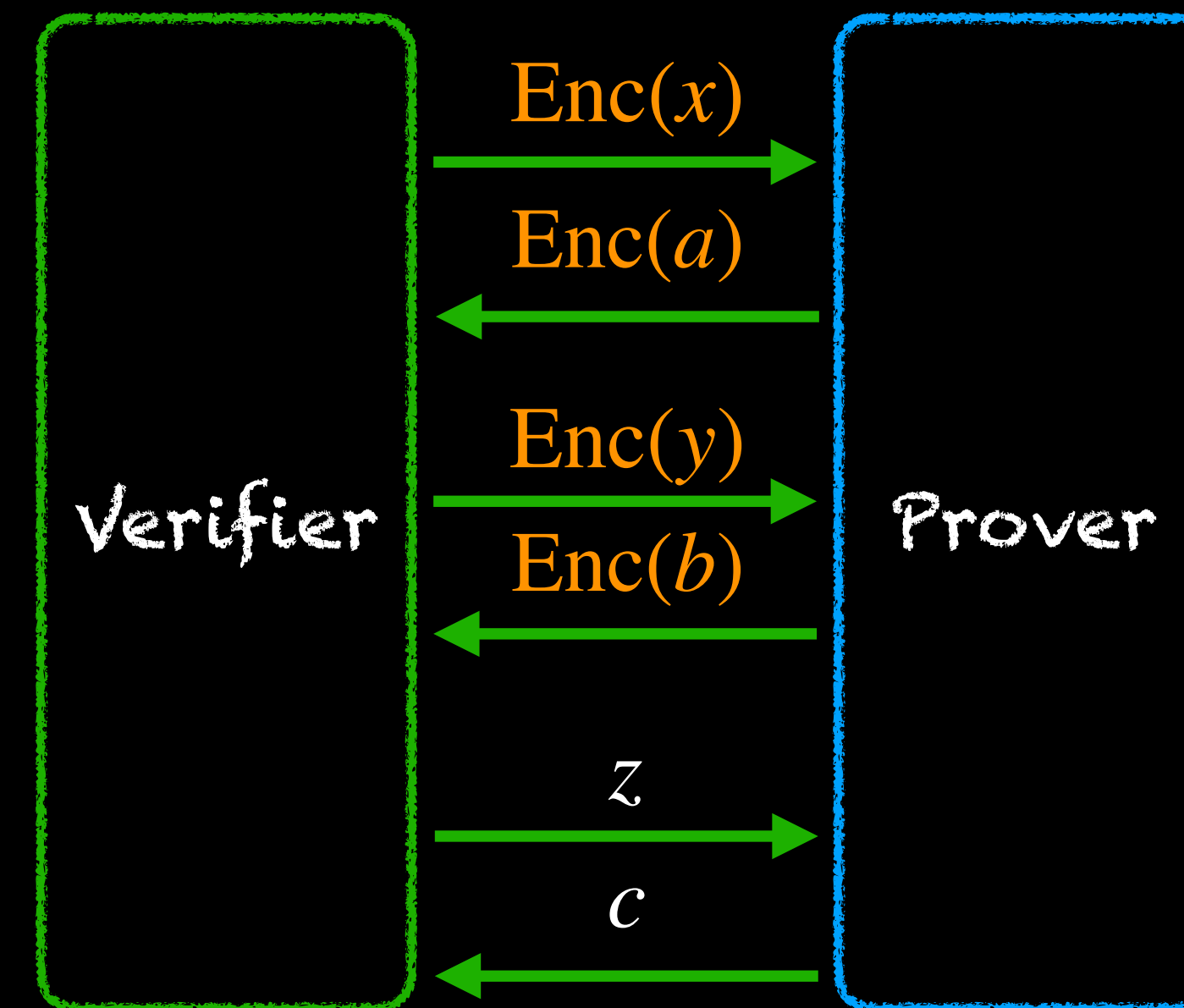
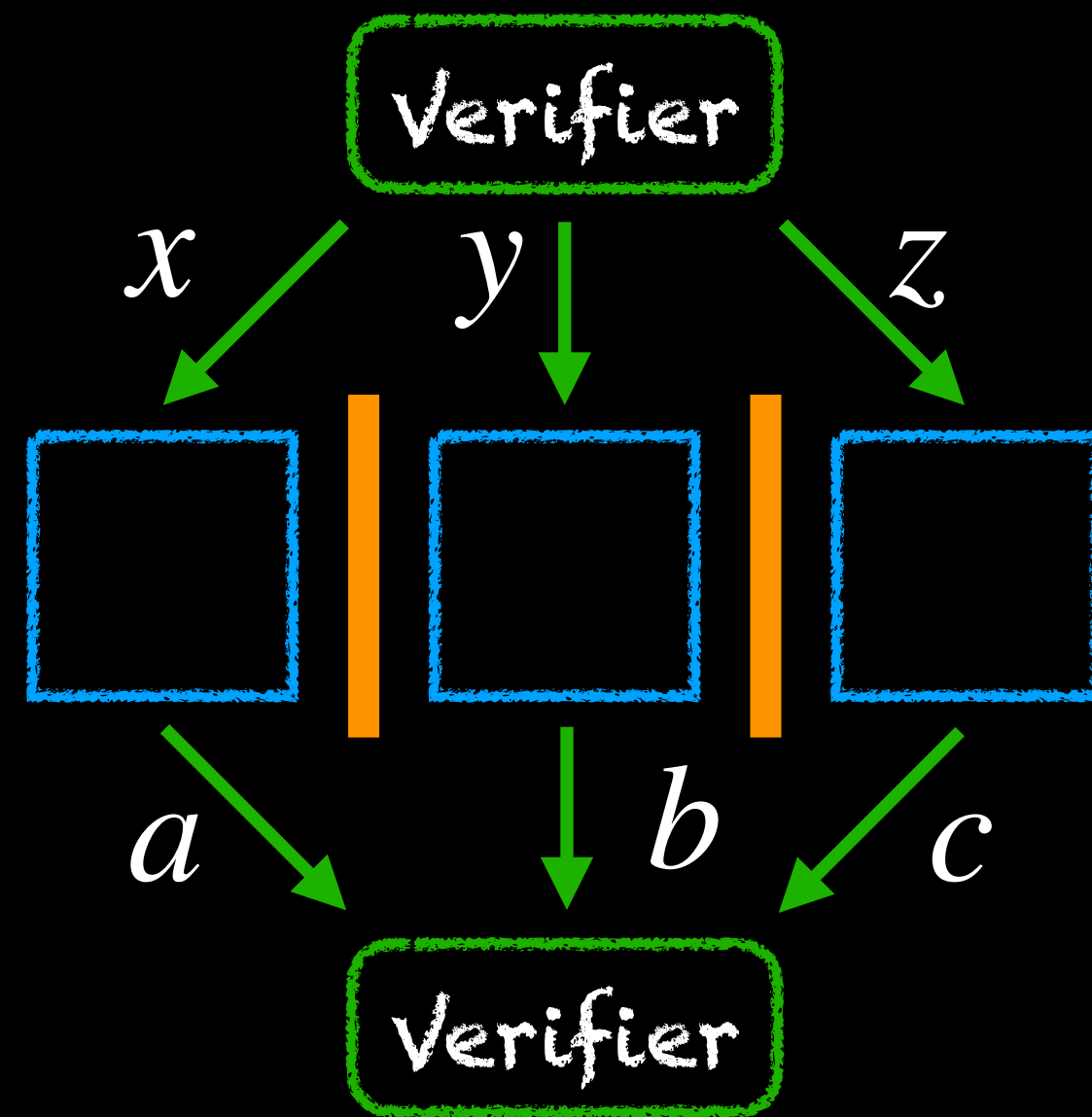
$$p(a, b | x, y) = \text{Tr} \left[M_a^x N_b^y \rho \right]$$

$$\left[M_a^x, N_b^y \right] = 0$$

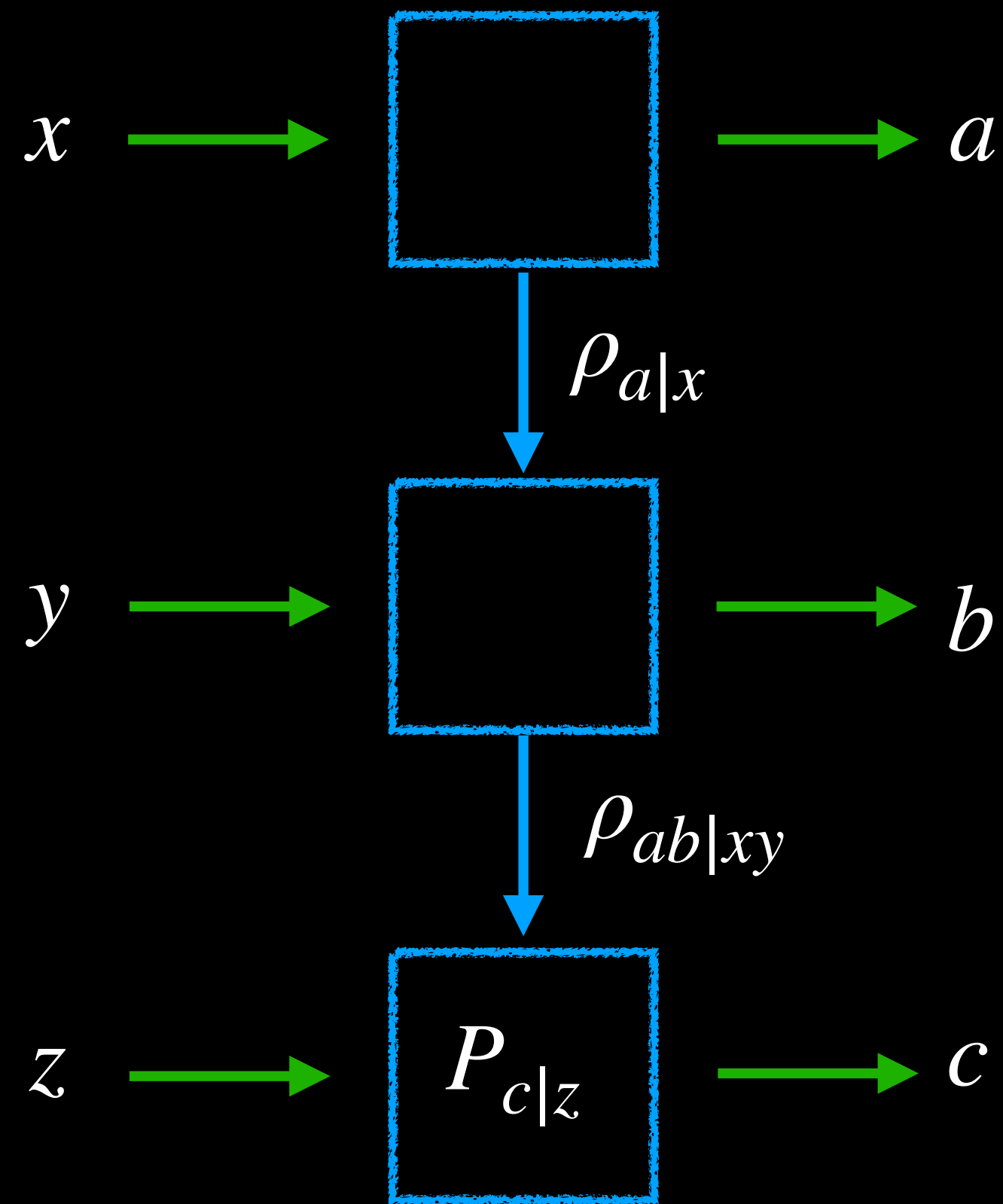
Multipartite games



Multiparty games

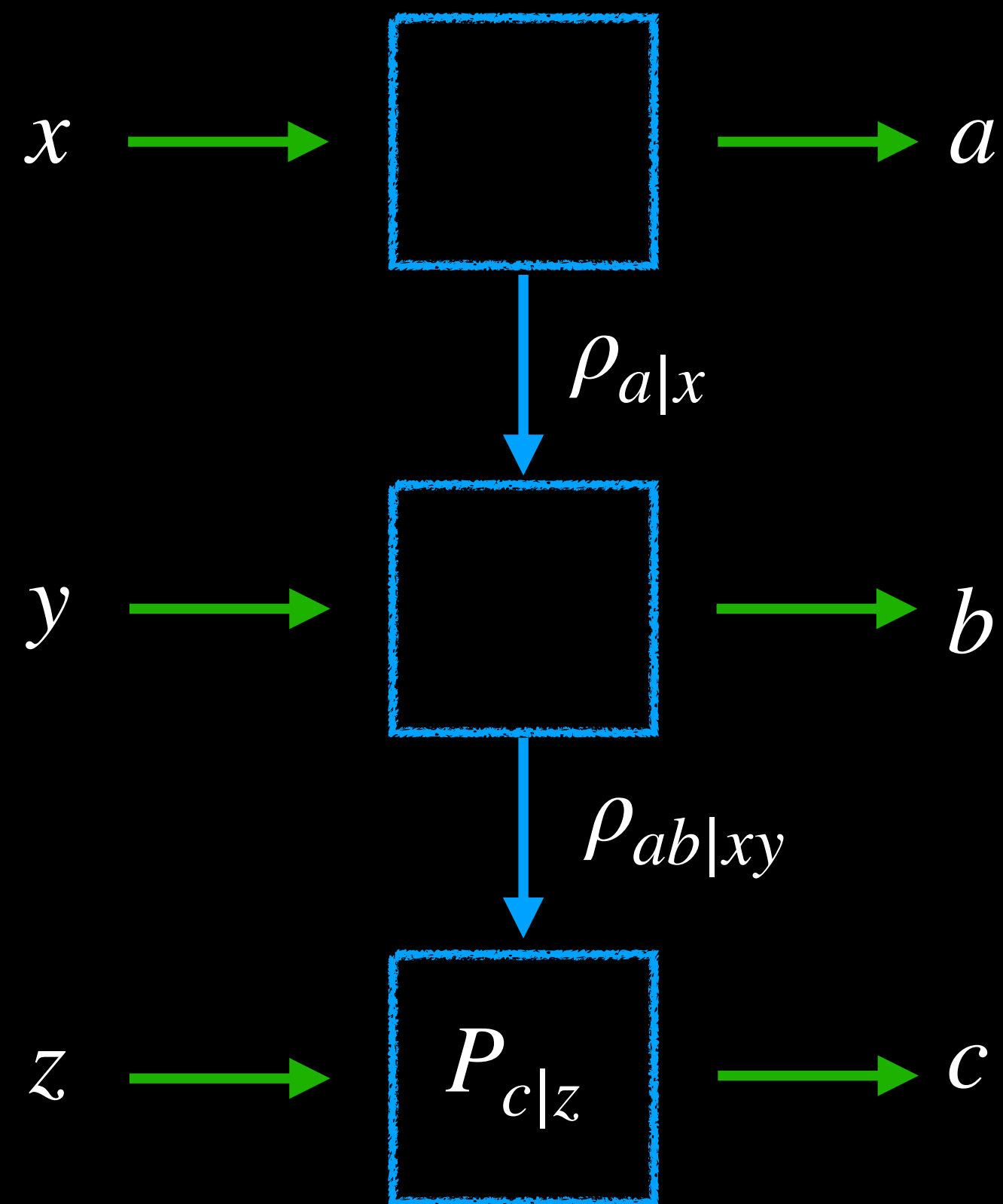


Multiround sequential games



$$p(a, b, c | x, y, z) = \text{Tr} \left[P_{c|z} \rho_{a,b|x,y} \right]$$

Multiround sequential games



$$\rho_x = \sum_a \rho_{a|x}$$

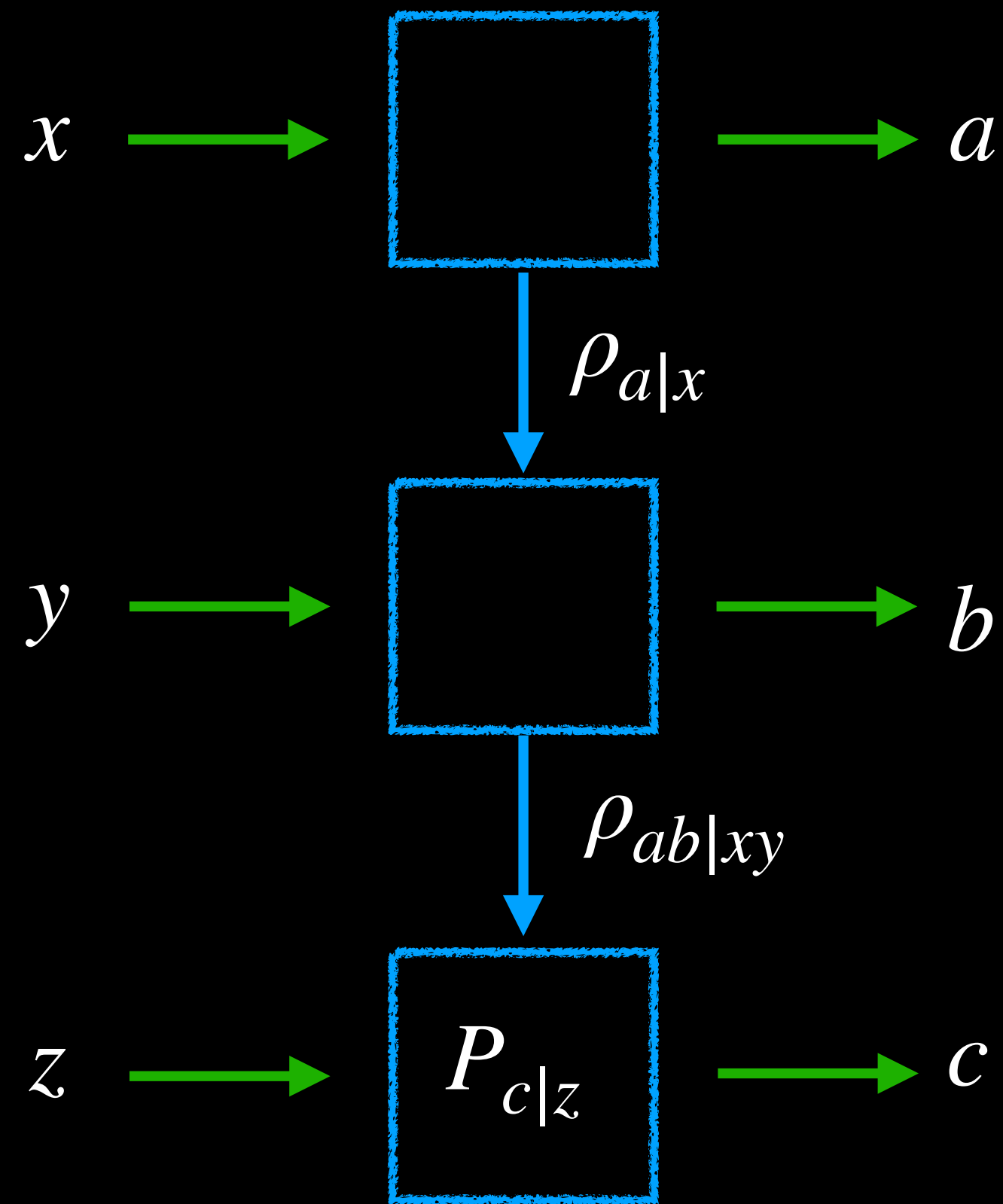
$$\rho_x = \rho_{x'}$$

$$\rho_{xy} = \sum_{ab} \rho_{ab|xy}$$

$$\rho_{xy} = \rho_{x'y'}$$

$$p(a, b, c | x, y, z) = \text{Tr} \left[P_{c|z} \rho_{a,b|x,y} \right]$$

Multiround sequential games



$$p(a, b, c | x, y, z) = \text{Tr} \left[P_{c|z} \rho_{a,b|x,y} \right]$$

$$\rho_x = \sum_a \rho_{a|x}$$

$$\rho_x = \rho_{x'}$$

Sainz, Brunner, Cavalcanti, Skrzypczyk, Vertesi

$$\rho_{xy} = \sum_{ab} \rho_{ab|xy}$$

$$\rho_{xy} = \rho_{x'y'}$$

Post-quantum
steering

In general, no $M_{a|x}$, $N_{b|y}$
and ρ such that

$$\rho_{a,b|x,y} = \text{Tr}_{AB} \left[M_{a|x} \otimes N_{b|y} \otimes \mathbf{1} \rho \right]$$

Multiround sequential games

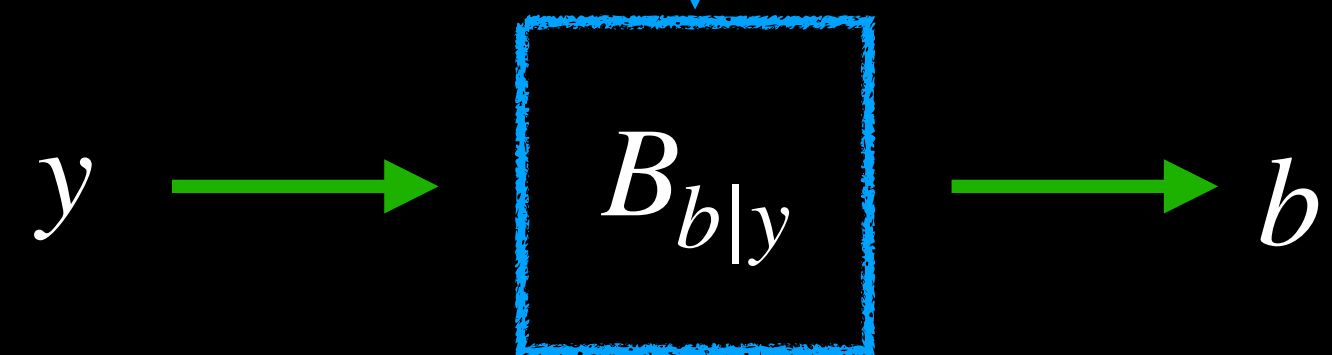


$$\rho_{a|x}$$

$$\rho_x = \sum_a \rho_{a|x}$$

$$\rho_x = \rho_{x'}$$

Preparation equivalence

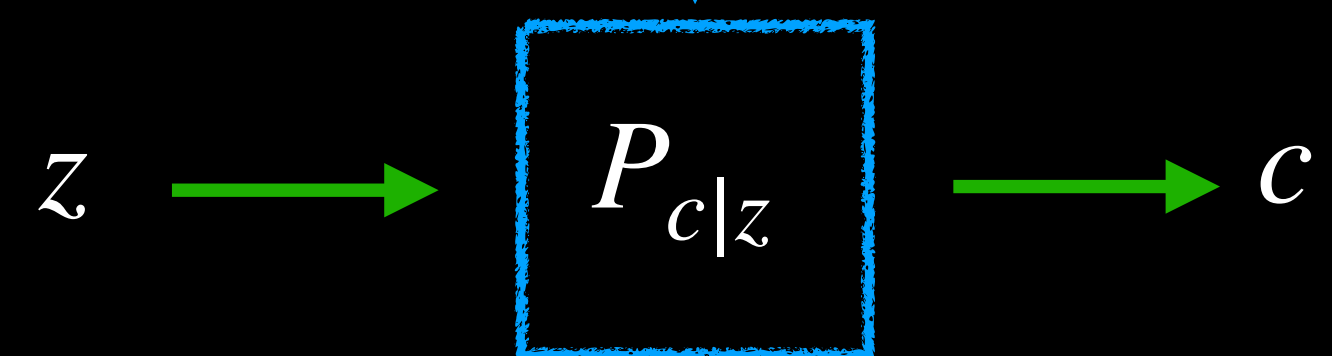


$$\rho_{ab|xy} = B_{b|y}(\rho_{a|x})$$

$$B_y = \sum_b B_{b|y}$$

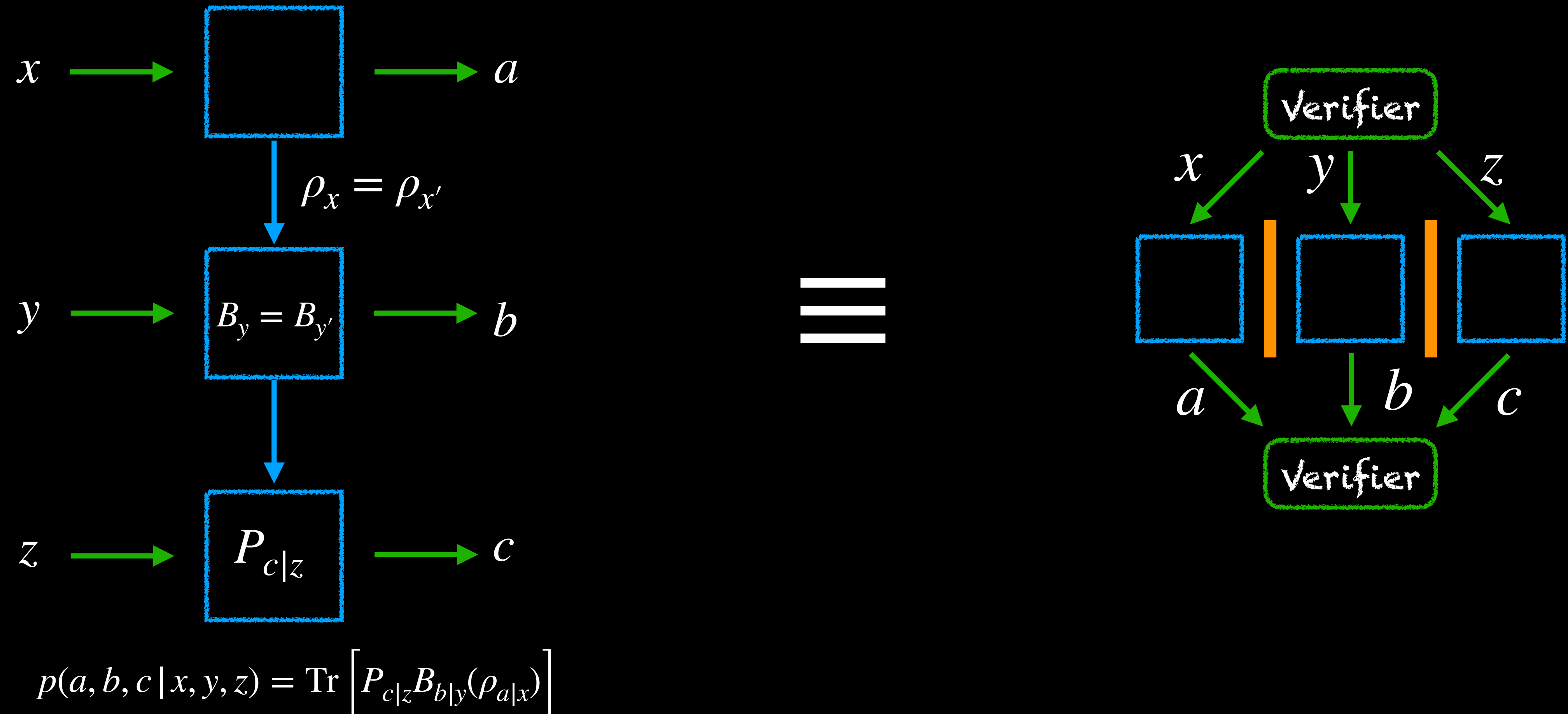
$$B_y = B_{y'}$$

Transformation equivalence



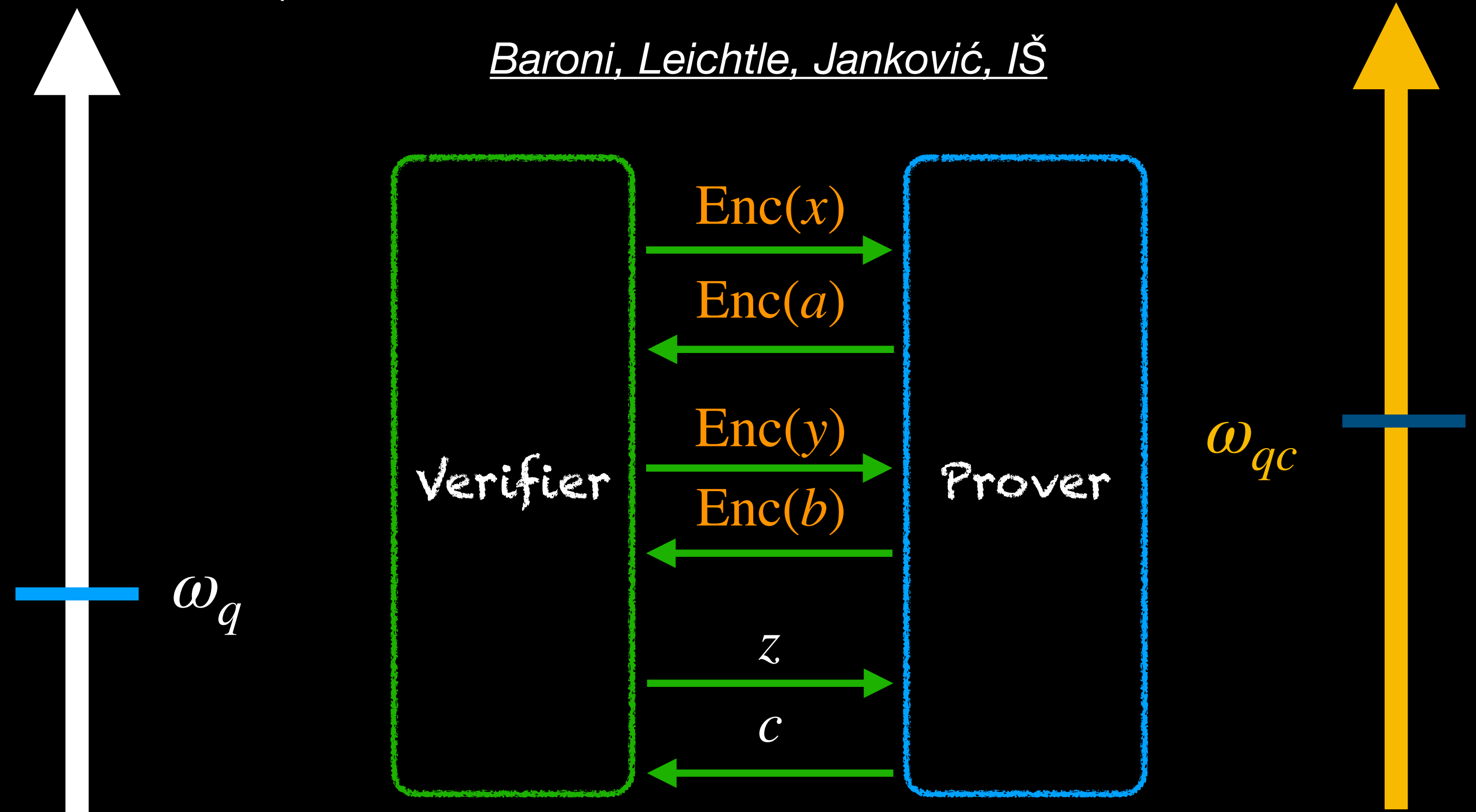
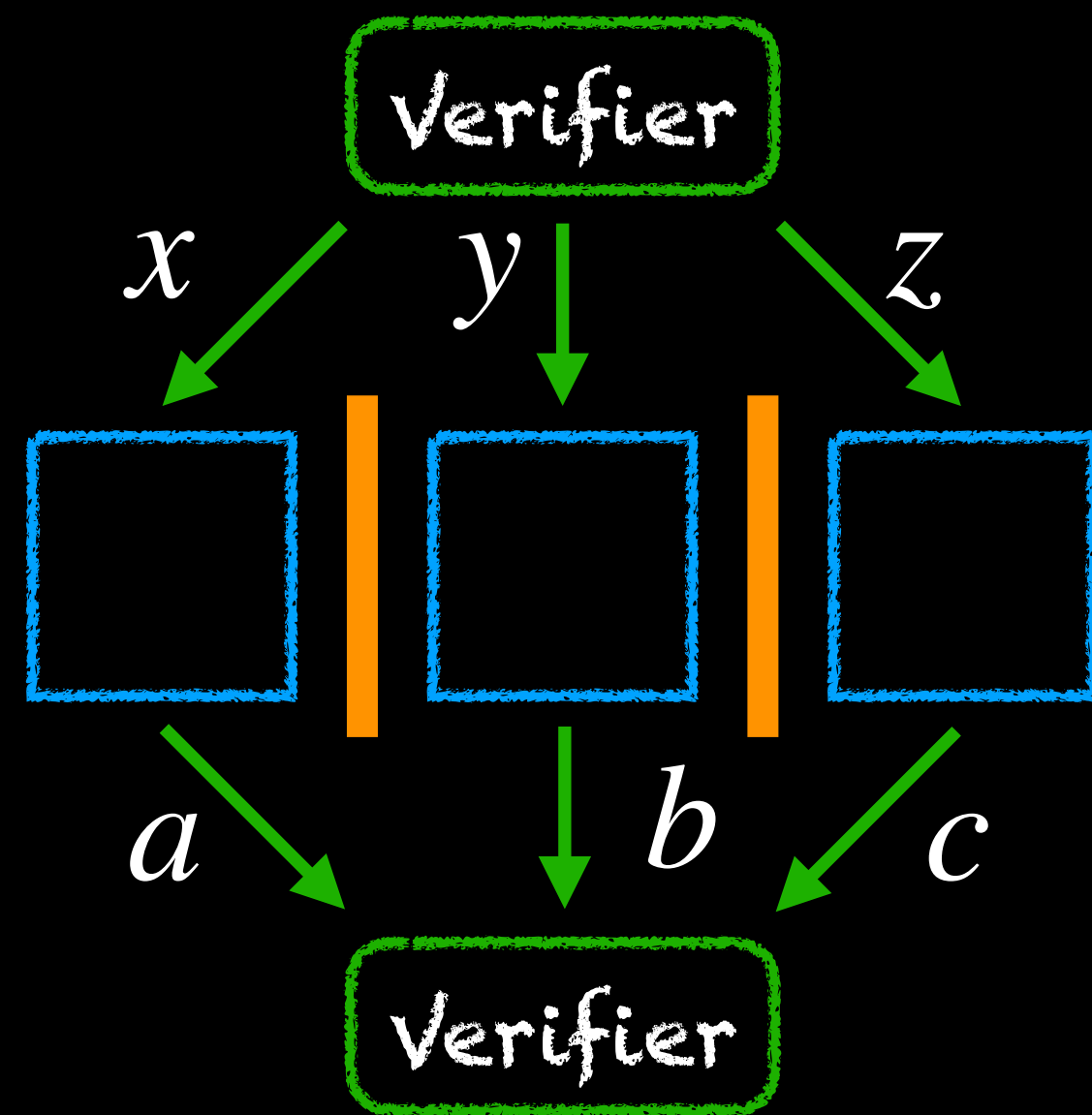
$$p(a, b, c | x, y, z) = \text{Tr} \left[P_{c|z} B_{b|y}(\rho_{a|x}) \right]$$

Multiround sequential games



Quantum bound for compiled nonlocal games

Baroni, Leichtle, Janković, IŠ



Universal C^* algebras

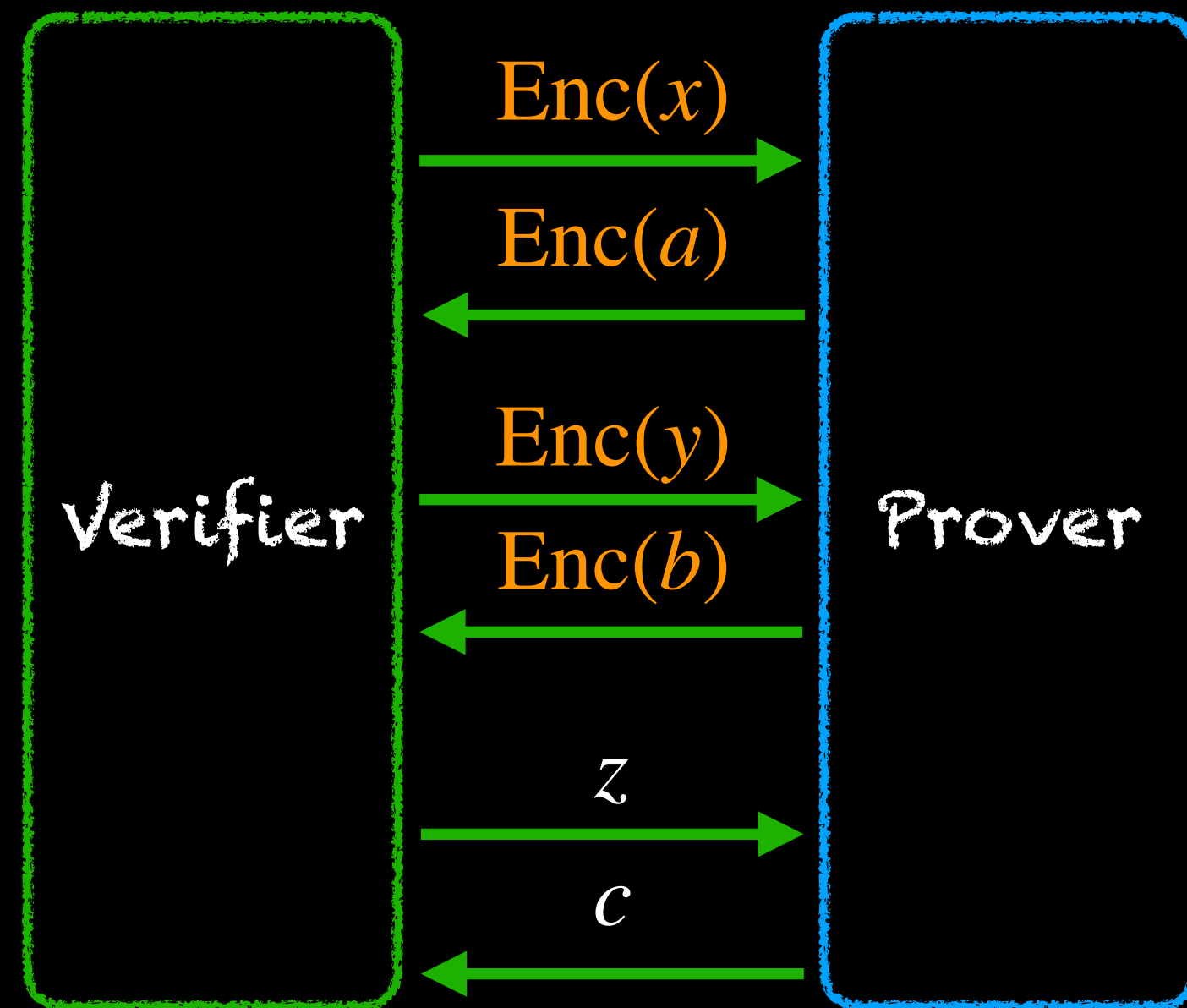
Radon-Nikodym
theorem for CP maps

Composition of
Radon-Nikodym
derivatives

Block-encoding
techniques to establish
computational
indistinguishability

Finite security-parameter analysis

Baroni, Klep, Leichtle, Renou, Tendick, IŠ, Xu



$$\rho_x^\lambda \approx_\lambda \rho_{x'}^\lambda$$

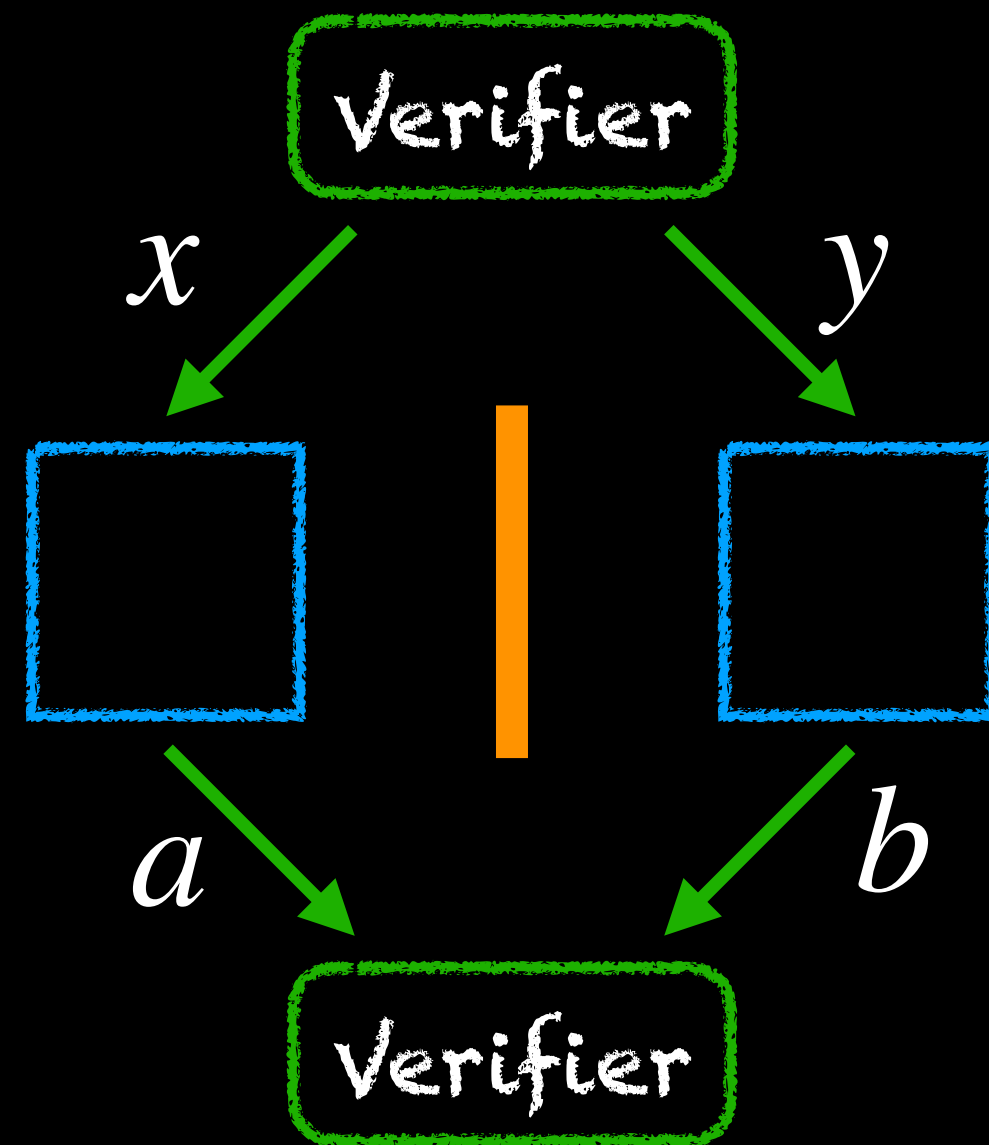
$$B_y^\lambda \approx_\lambda B_{y'}^\lambda$$

$$\omega_\lambda \leq \omega_{qc} + \text{negl}(\lambda)$$

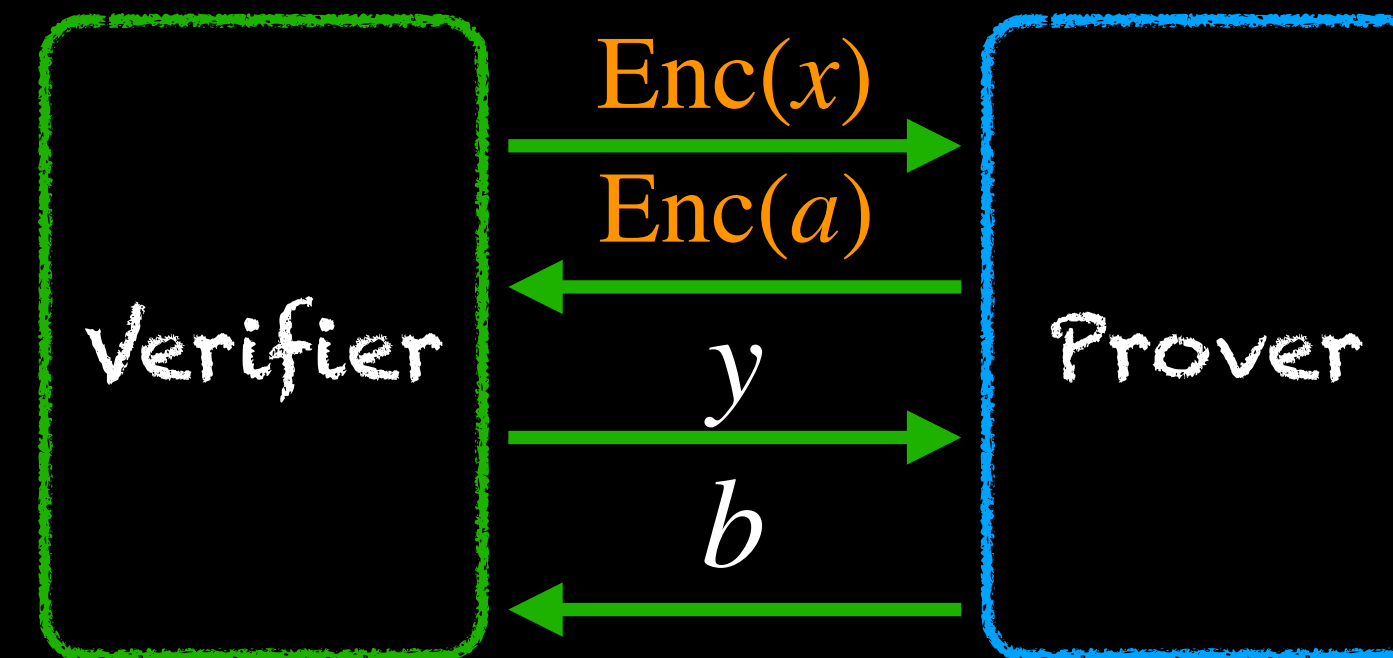
NPA hierarchy for sequential games with preparation and transformation equivalences

Geometric arguments, small departures from no-signalling produce moments close to those in the sequential NPA.

Self-testing?



Maximal quantum score self-tests
the state and measurements



Maximal quantum score self-tests
the states after the first round
and the second round
measurements.

Kulpe, Malavolta, Paddock, Schmidt, Walter

Self-testing of the state before
the first round, and the first-
round operations: work in
progress

Verification of quantum computing



Can a classical user convince themselves that they are interacting with a quantum device?

Make it solve a BQP-universal problem!

Nonlocal approach:

- requires at least two devices
- information theoretic security

Kashefi, Broadbendt, Fitzsimons, Reichardt,
Unger, Vazirani, Grilo, Vidick, Coladangelo,
Jeffery



Computational approach:

- single device
- computational security

Mahadev

Nonlocality and Computer science

$MIP^* = RE$,

$MIP_{CO} = coRE$

Computational Bell inequalities
Computational entanglement theory

Unclonable bit encryption

Quantum PCP ?