Title: Values for compiled XOR nonlocal games

Speakers: Connor Paddock

Collection: Foundations of Quantum Computational Advantage

Date: April 30, 2024 - 9:15 AM

URL: https://pirsa.org/24040093

Abstract: Nonlocal games are a foundational tool for understanding entanglement and constructing quantum protocols in settings with multiple spatially separated quantum devices. However, the spatial separation between devices can be difficult to enforce in practice. To this end, Kalai et al. (STOC '23) initiated the study of compiled nonlocal games. The KLVY compilation procedure transforms any k-prover nonlocal into a game with a classical verifier and a single cryptographically limited quantum prover. Kalai et al. showed that their compilation procedure is sound against classical provers and complete for entangled provers. Natarajan and Zhang (FOCS '23) showed that the compiled two-prover CHSH game is sound against quantum provers. I will discuss recent work, showing that the compiler is sound for any two-player XOR game. I will also discuss challenges and open questions in extending results from nonlocal games to the compiled setting.

Values for compiled XOR nonlocal games

Connor Paddock

University of Ottawa

1

Nonlocal games

- Players can share quantum state, but no communication allowed.

- Referee samples questions x and y from a distribution.

- Sends x to Alice and y to Bob

- Alice (resp. Bob) returns a (resp. b) to the referee.

- Referee checks if they win or lose.
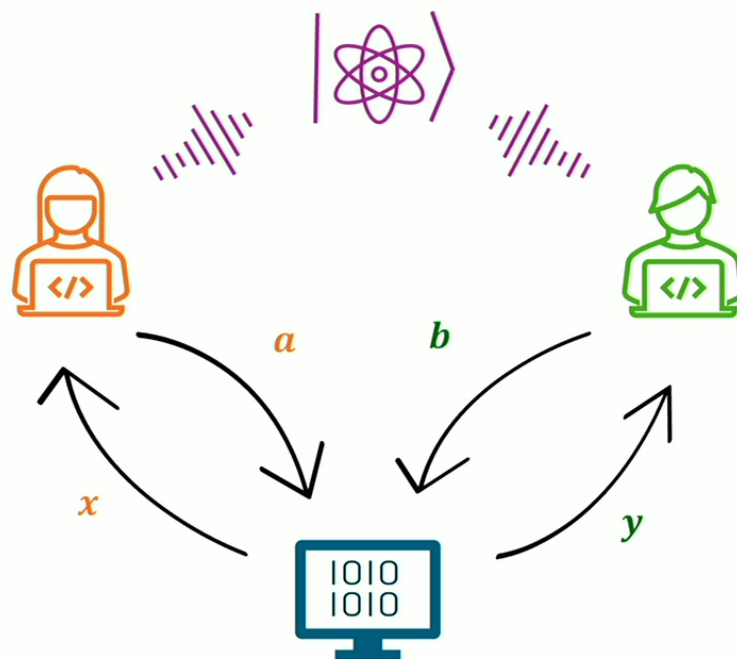
$$V(a, b, x, y) = \begin{cases} Win \\ Lose \end{cases}$$

Nonlocal games: what are they good for?

- Exhibiting quantum correlations and noncontextuality scenarios, e.g. [CHSH'69,Mer'93,Per'93]

- Device independent applications:
  - Quantum key distribution [VV'14]
  - Delegated quantum computing [CGJV'19]
  - Certifying entanglement [RUV'13]

- Complexity theoretic "power" of entanglement
  - MIP*=RE[JNVWY'22], whereas MIP=NEXP [BFL'91]

$$V(a, b, x, y) = \begin{cases} Win \\ Lose \end{cases}$$

3
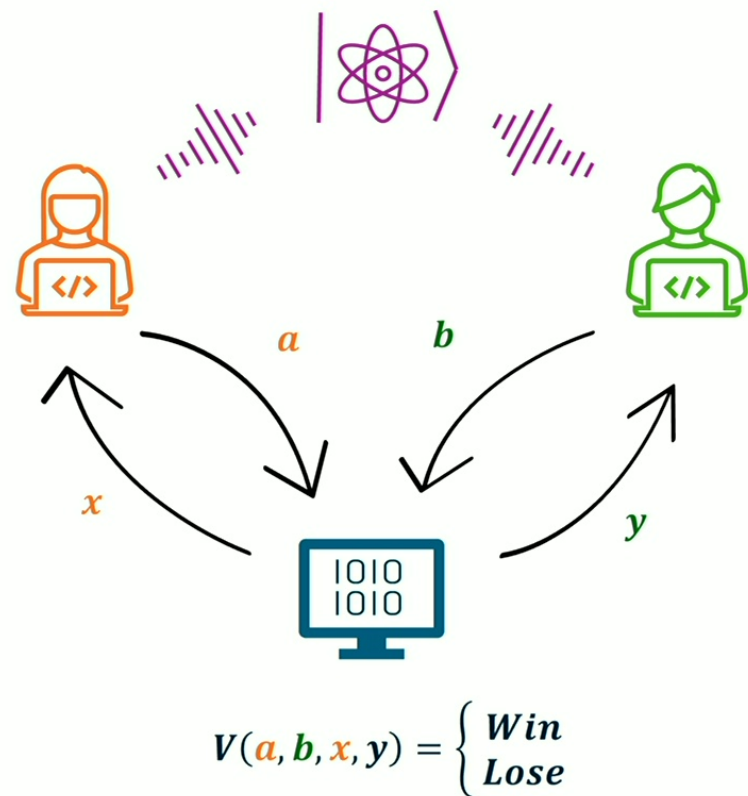
Simulating separations with cryptography

- KLVY (Kalai-Lombardi-Vaikuntanathan-Yang) compiler for nonlocal games [KLVY'23] :

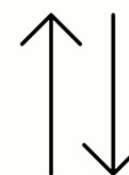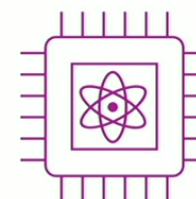"two-prover game G" $\mapsto$ "single-prover game $\mathcal{T}(G)$" s.t.

- "classical value of $\mathcal{T}(G)$" = "classical value of G" (up to small error)
- "quantum value of $\mathcal{T}(G)$" $\geq$ "quantum value for G"

Left open: "quantum value for $\mathcal{T}(G)$" $\leq$ "quantum value for G"

Theorem [CMMNPSWZ'24] (informal):

If G is an XOR game, then the quantum value of the compiled game is preserved under compilation.

Quantum prover

Classical verifier

Outline

- Values for nonlocal games

- Quantum homomorphic encryption

- The KLVY compiler for nonlocal games

- Compiled XOR nonlocal games

6

Nonlocal games
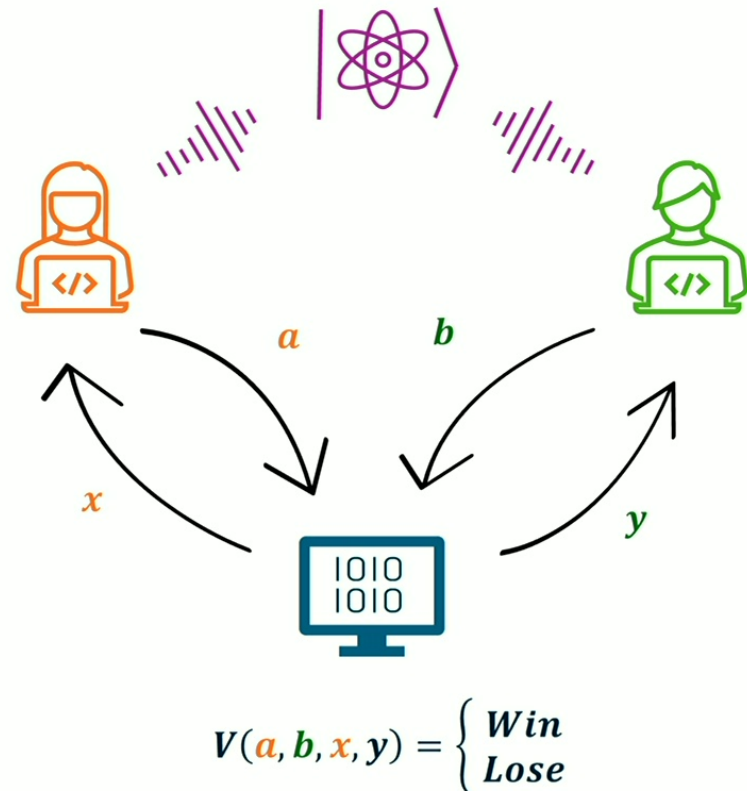
Two-player nonlocal games

- Winning probability:
$$\omega_q(G;S) = \sum_{abxy} \pi_{xy} V_{abxy}\, p(a,b|x,y)$$

- Quantum value: $\omega_q^*(G) = \sup_S \omega_q(G;S)$

- Quantum correlations:
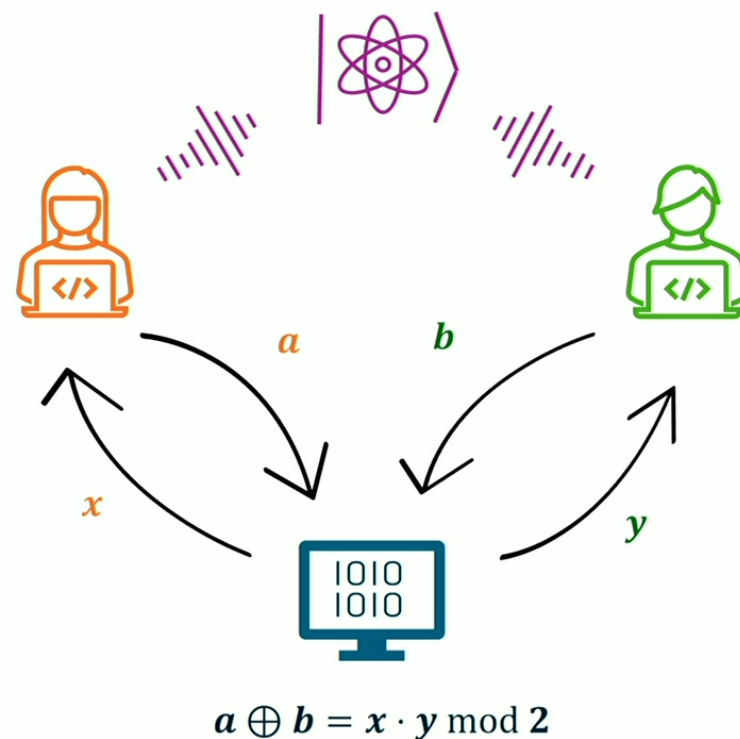$$p(a,b,x,y) = \langle\psi| M_a^x \otimes N_b^y |\psi\rangle$$

*Also have classical, quantum commuting, and non-signalling values.

$$V(a,b,x,y) = \begin{cases} Win \\ Lose \end{cases}$$

CHSH nonlocal game

- Referee uniformly samples bits x and y.

- Players return bits a and b

- Referee checks if $a \oplus b = x \cdot y$

- Expected win (bias) using quantum strategy is

$$p_{win} - p_{lose} = \frac{1}{4} \sum_{xy} (-1)^{xy} \langle \psi | A_x \otimes B_y | \psi \rangle$$

$$a \oplus b = x \cdot y \bmod 2$$
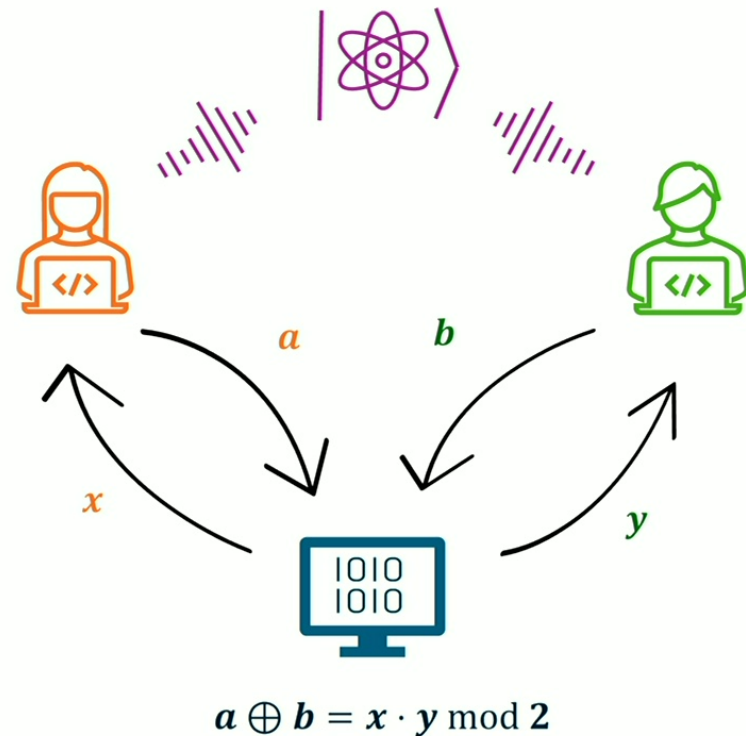
9

Remarkable properties of CHSH

- Quantum players can win with probability

$$\frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.85$$

- No classical players can win with probability greater than $\frac{3}{4} = 0.75$

- Any players attaining ≈ 0.85 must be:
  - using a state that is close to an EPR pair,
  - using observables close to $(\sigma_X \otimes \mathbb{1}, \sigma_Z \otimes \mathbb{1})$, and $(\mathbb{1} \otimes \frac{\sigma_X + \sigma_Z}{\sqrt{2}}, \mathbb{1} \otimes \frac{\sigma_X - \sigma_Z}{\sqrt{2}})$
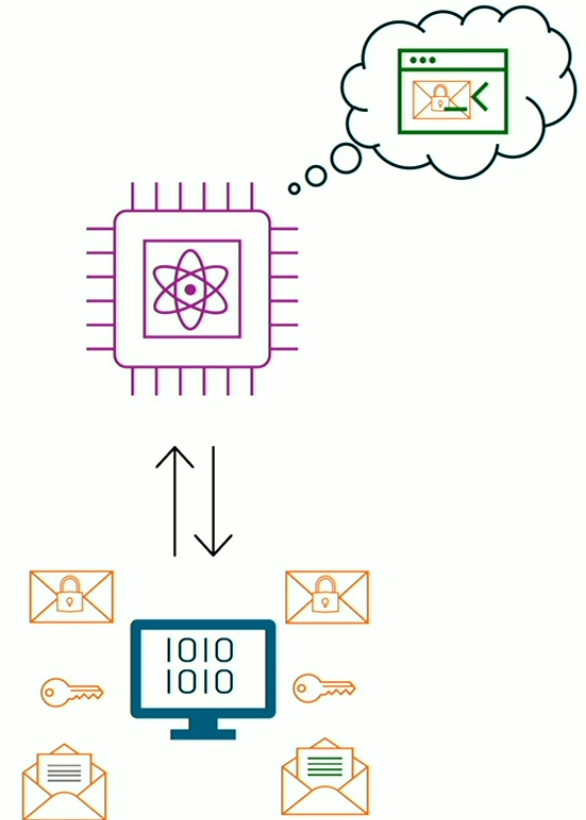
  * up to local isometries

$$a \oplus b = x \cdot y \bmod 2$$

10

Quantum homomorphic encryption

Quantum homomorphic encryption

- Verifier encrypts their data and provides it to the quantum prover

- Prover runs a quantum circuit on the encrypted data and returns the output to the verifier

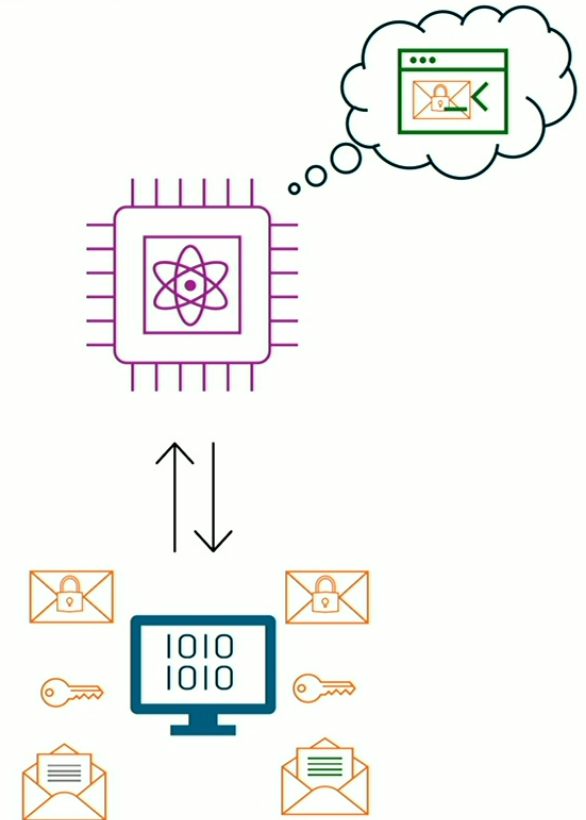- Verifier can decrypt the resulting output of the computation

12

Quantum homomorphic encryption

- Correctness: for any circuit C there exists $\hat{C}$ such that
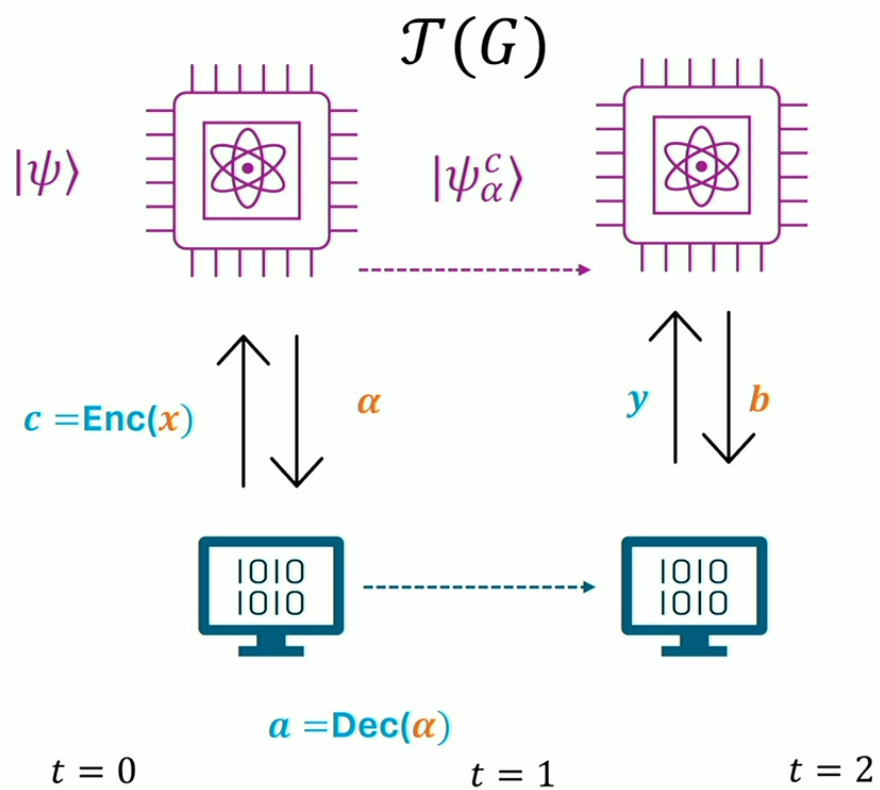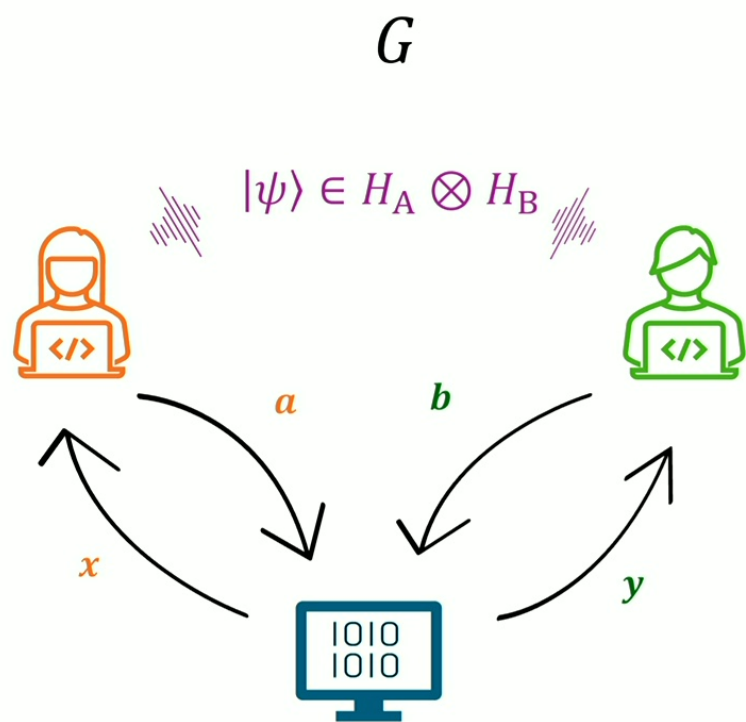$$Dec\left(\hat{C} \circ Enc(x)\right) = Dec(Enc(C(x)) = C(x)$$

- Security: prover cannot distinguish between any pair of messages encoded under same key.

- Proposed scheme [Mah'20] based on the hardness of LWE [Reg'05].

- Restrict the prover to be QPT (quantum polynomial time) in the security parameter $\lambda \in \mathbb{N}$ of the QHE scheme.

KLVY compiler for nonlocal games
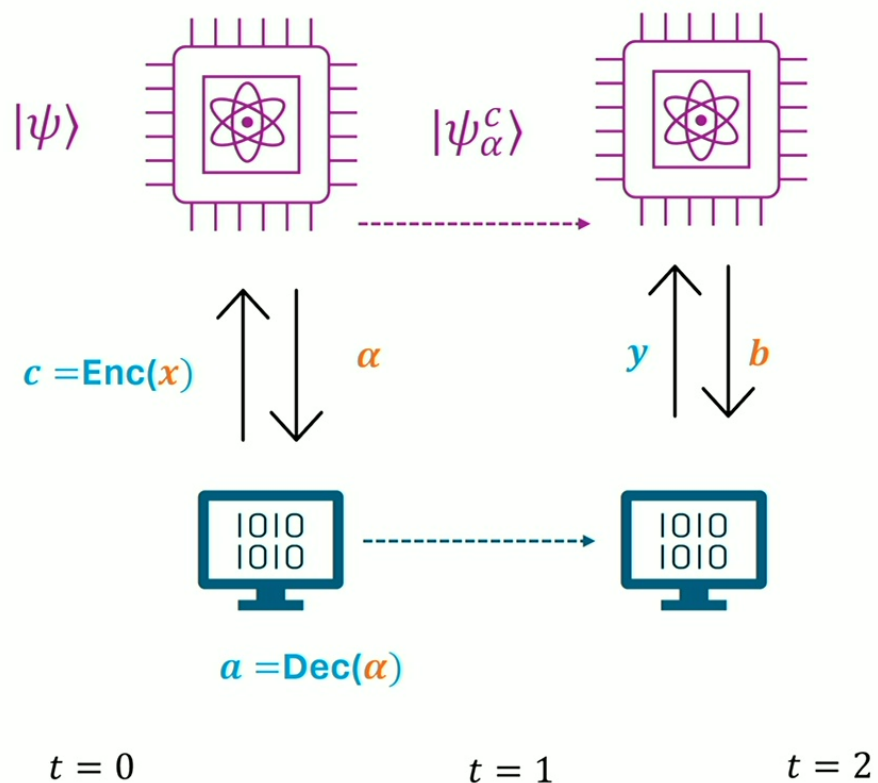

G

$|\psi\rangle \in H_A \otimes H_B$

a b

x y

$\mathcal{T}(G)$

$|\psi\rangle$ $|\psi_\alpha^c\rangle$

$c = \mathbf{Enc}(x)$ α y b

$a = \mathbf{Dec}(\alpha)$

$t = 0$ $t = 1$ $t = 2$

15

Trading nonlocality for cryptography

G	$\mathcal{T}(G)$
2-player 1-round	1-player 2-round
Tensor product Hilbert spaces	Single Hilbert space
Simultaneous measurement	Sequential measurements
Local unitaries	First player can apply global unitary
No runtime assumption	Runtime is O(poly(λ))

$|\psi\rangle$ $|\psi_\alpha^c\rangle$

$c = \mathbf{Enc}(x)$ α y b

$a = \mathbf{Dec}(\alpha)$

$t = 0$ $t = 1$ $t = 2$

16

Compiled CHSH game

- Referee uniformly samples bits x and y.

- Verifier sends $c = Enc(x)$ to prover. Prover returns output α.

- Prover sends y (in the clear) to prover. Prover returns with output b.

- Referee checks if $Dec(\alpha) \oplus b = x \cdot y$

$|\psi\rangle$ $|\psi_\alpha^c\rangle$

$c = Enc(x)$ α y b

$a = Dec(\alpha)$

$t = 0$ $t = 1$ $t = 2$
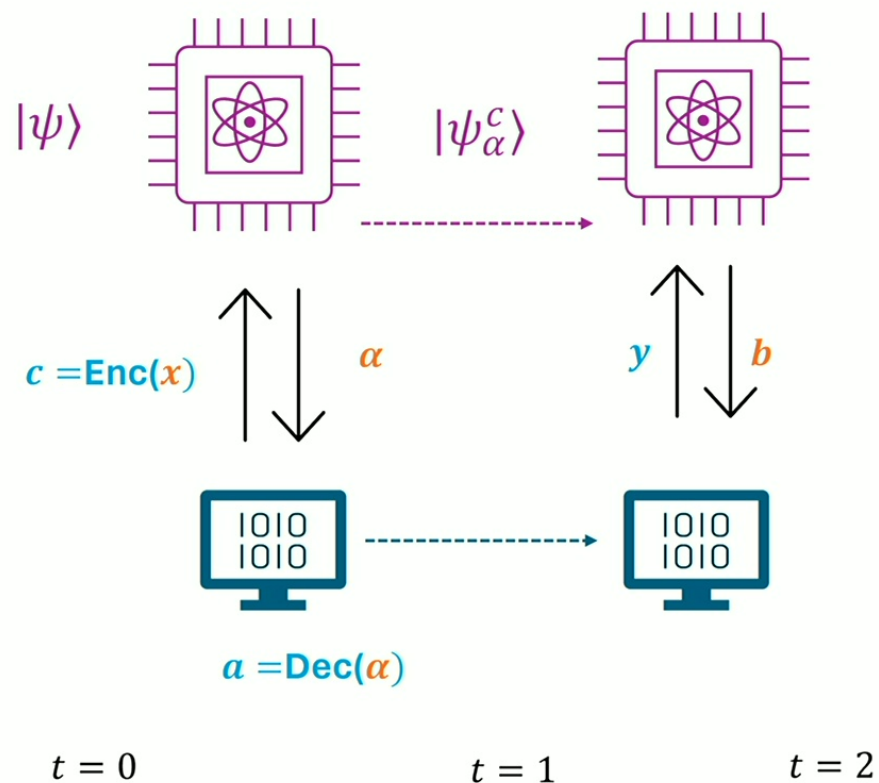
Classical values for compiled games

Theorem: [KLVY'23]

Let G be a nonlocal game and $\mathcal{T}(G)$ the corresponding compiled game. For any classical strategy S for G,

1. (completeness) there exists a classical strategy for the compiled game that wins with probability at least $\omega_c(G; S) - negl(\lambda)$, and

2. (soundness) any classical prover wins the compiled game with probability at most $\omega_c^*(G) + negl(\lambda)$.

*A function $\mathbb{N} \to \mathbb{R}$ is *negligible* if it smaller than every $poly(\cdot)^{-1}$ for sufficiently large $n \in \mathbb{N}$.

18

Quantum values for compiled games

Theorem: [KLVY'23]

Let G be a nonlocal game and $\mathcal{T}(G)$ the corresponding compiled game. For any quantum strategy S for G,

1. (completeness) there exists a quantum strategy for the compiled game that wins with probability at least $\omega_q(G; S) - negl(\lambda)$, and

2. (soundness)???

Could there be better compiled strategies than quantum (spatial) ones?

*A function $\mathbb{N} \to \mathbb{R}$ is *negligible* if it smaller than every $poly(\cdot)^{-1}$ for sufficiently large $n \in \mathbb{N}$.

19

Compiled XOR nonlocal games

20

XOR nonlocal games

- Questions $x \in [n]$ and $y \in [m]$

- Answers are $a \in \{0,1\}$ and $b \in \{0,1\}$

- Rule predicate $(1 + c_{xy}(-1)^{a \oplus b})/2$ for $c_{xy} \in \{\pm 1\}$

- Quantum correlations for XOR games are characterized by $\Gamma \in \mathbb{R}^{n \times m}$ s.t. $\Gamma_{xy} = \langle u_x | v_y \rangle$ where $|u_x\rangle, |v_y\rangle \in \mathbb{R}^D$ [Tsi'87]

- **Corollary**: $\beta_q^*(G) = \max_{|u_x\rangle, |v_y\rangle} \sum_{xy} G_{xy} \langle u_x | v_y \rangle$
  [CHTW'10]
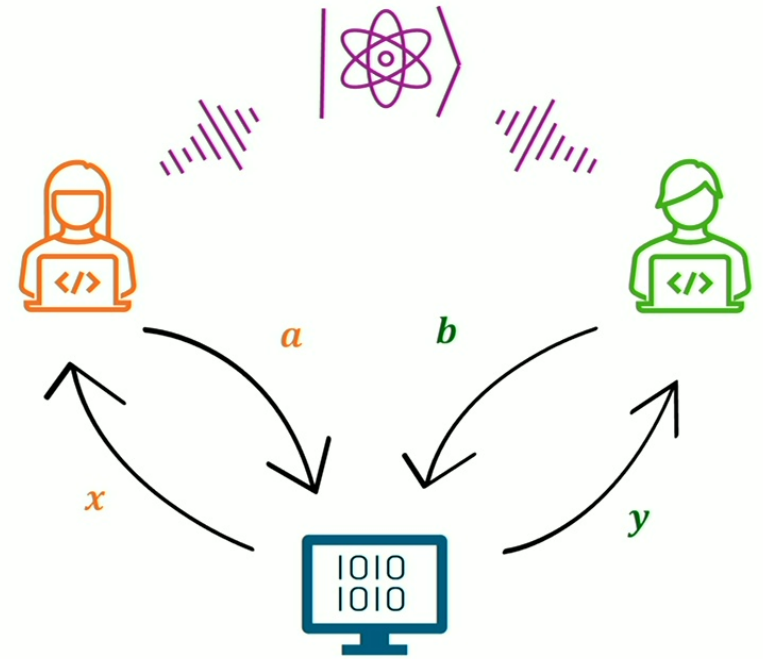
Quantum soundness for compiled XOR games

Theorem: [CMMNPSWZ'24]

Let G be an XOR game and $\mathcal{T}(G)$ the corresponding compiled game. Then any quantum prover wins $\mathcal{T}(G)$ with probability at most $\omega_q^*(G) + negl(\lambda)$.

*Proof techniques involve using SOS (sums-of-squares), cryptographic pseudo-expectations, and the game polynomials of XOR games, see arXiv:2402.17301 for details.

More results

- The quantum value is preserved in the case of compiled parallel repeated XOR games, e.g. CHSH(n)

- We obtain (one-sided) rigidity for Bob's observables for compiled XOR games.

- Rigidity results for compiled magic square game.

- "Nice" SOS (sums of squares) certificates for all XOR games

23

Open questions

- Is the quantum value preserved for all nonlocal games?

- Do we have a notion of self-testing for compiled games?

- How does the set of correlations arising from compiled games compare to other correlation sets?

- What are the limitations of such games?

24