Title: Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation

Speakers: Anne Broadbent

Collection: QPV 2023: Advances in quantum position verification

Date: September 18, 2023 - 1:00 PM

URL: https://pirsa.org/23090023

Popescu-Rohrlich Correlations Imply Efficient Instantaneous Nonlocal Quantum Computation

Anne Broadbent

uOttawa

QPV 2023: Advances in quantum position verification

Perimeter Institute, September 18 2023

PHYSICAL REVIEW A **94**, 022318 (2016)

Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation

Anne Broadbent[*,†]
Department of Mathematics and Statistics, University of Ottawa, Ottawa, Ontario, Canada K1N 6N5
(Received 7 January 2016; published 15 August 2016)

Draft circulated in 2011, arXiv posting in December 2015

Instantaneous Non-Local Computation of Low T-Depth Quantum Circuits

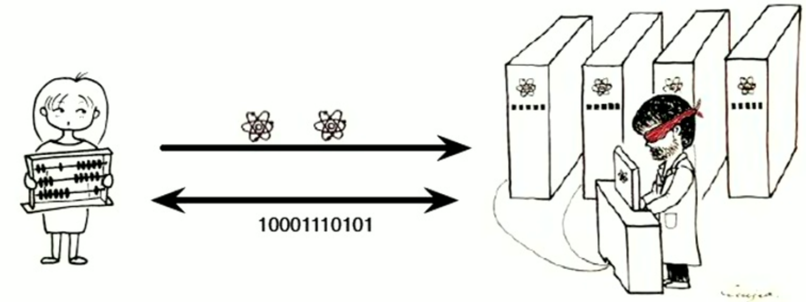
Florian Speelman[*]

Centrum Wiskunde & Informatica, Amsterdam, the Netherlands
f.speelman@cwi.nl

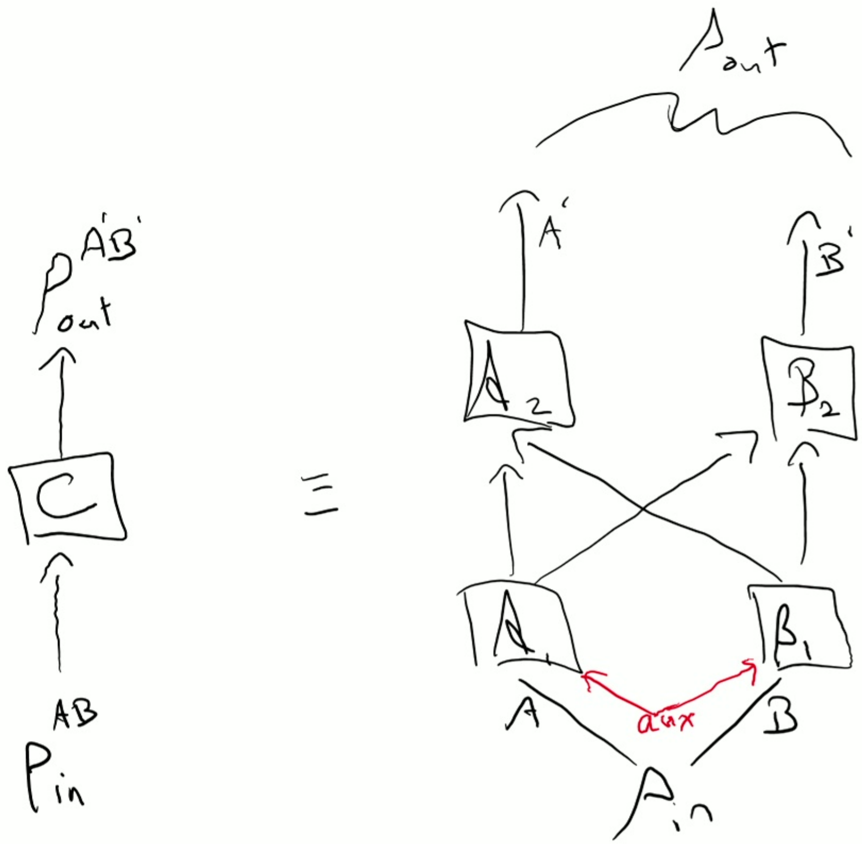
Universal Blind Quantum Computation

Anne Broadbent[1], Joseph Fitzsimons[1,2], Elham Kashefi[3 *]

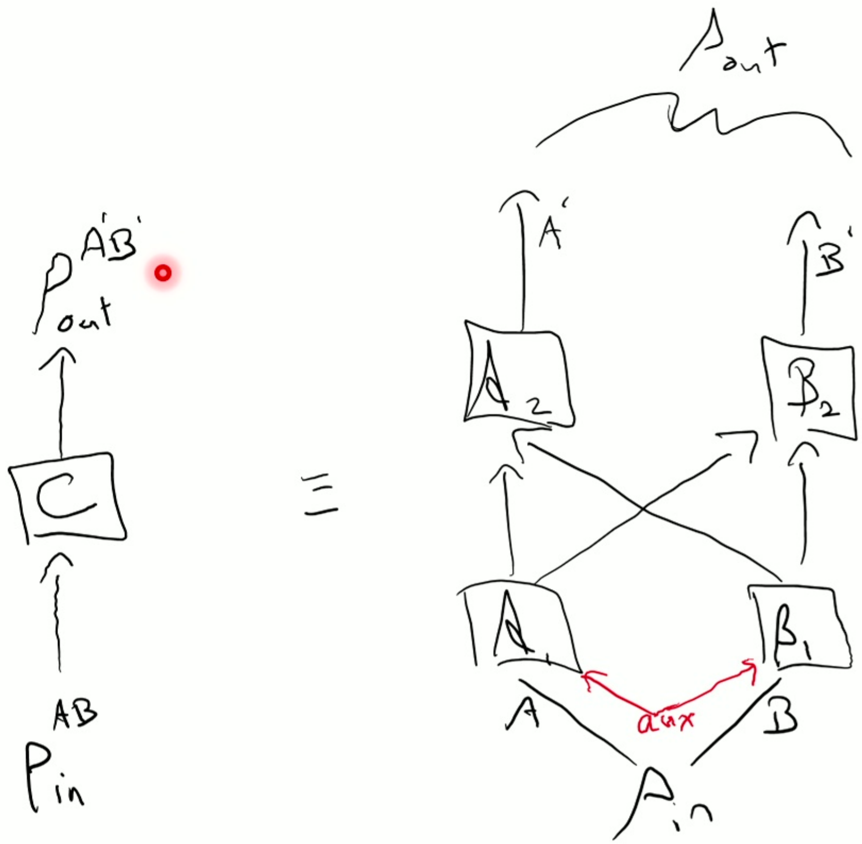
FOCS 2009



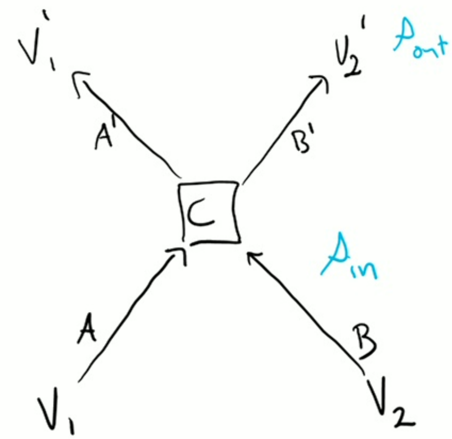
Instantaneous nonlocal quantum computation (INQC)



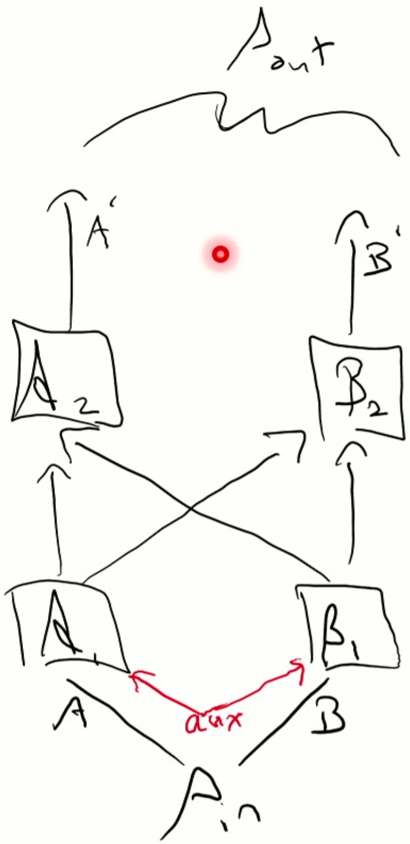
Instantaneous nonlocal quantum computation (INQC)



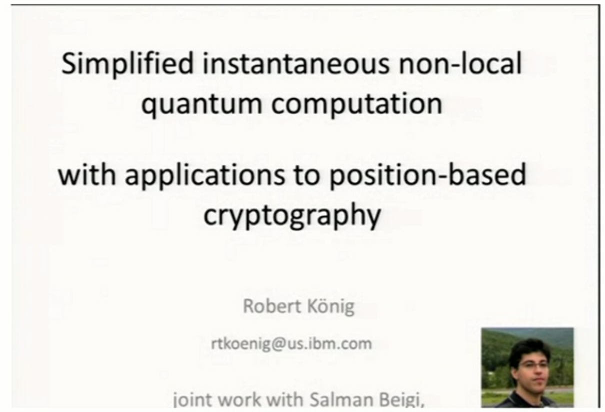
If a INQC protocol exists, then the following is not a secure QPV scheme:



Instantaneous nonlocal quantum computation

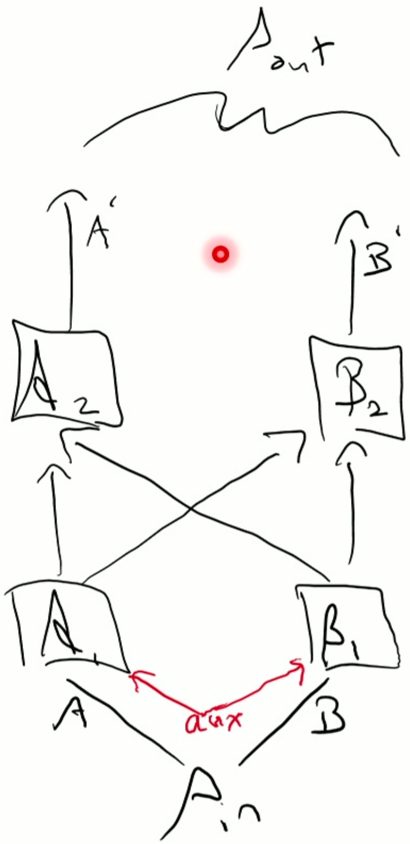


Always possible using exponential entanglement!

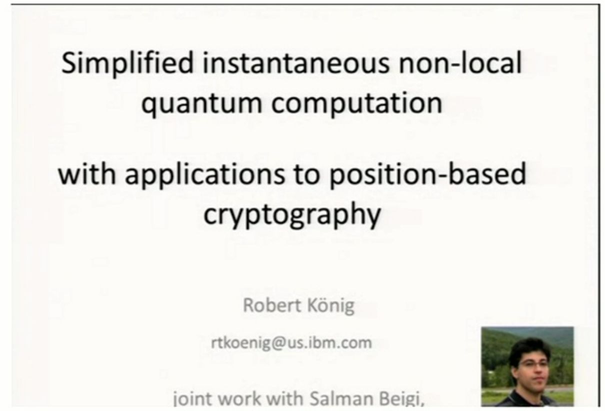


In principle, there is always an attack for QPV.

Instantaneous nonlocal quantum computation



Always possible using exponential entanglement!



In principle, there is always an attack for QPV.
But how about in practice?

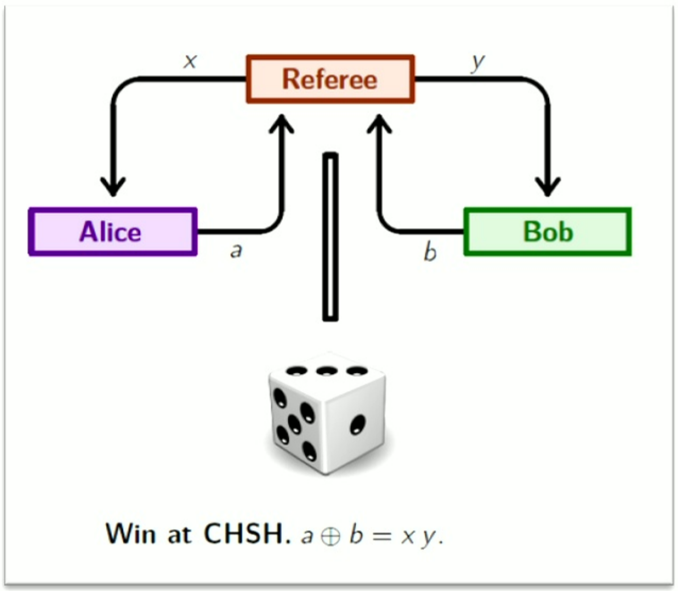
QPV could still be possible if we assume that adversaries cannot share exponential entanglement.

eg: Tomamichel, Fehr, Kaniewski ,Wehner (2013): QPV protocol secure against adversaries with at most linear entanglement

Adversarial model for QPV

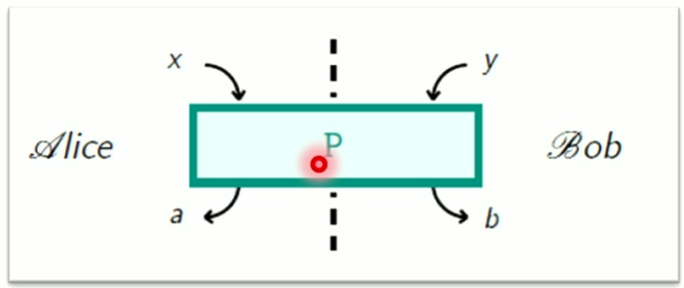
Could secure QPV be possible against adversaries that:

1) Are consistent with relativity (no super-luminal communication)
2) Share correlations that are beyond quantum ?
3) Share polynomial entanglement?



Figures by Pierre Botteron

Tsirelson's Bound: QM achieves the CHSH correlation with probability at most $\cos^2\frac{\pi}{8} \approx 0.85$



Popescu-Rohrlich (PR) Box:

$$P(a,b\,|\,x,y) = \begin{cases} 1/2, & a \oplus b = xy \\ 0 & \text{otherwise} \end{cases}$$

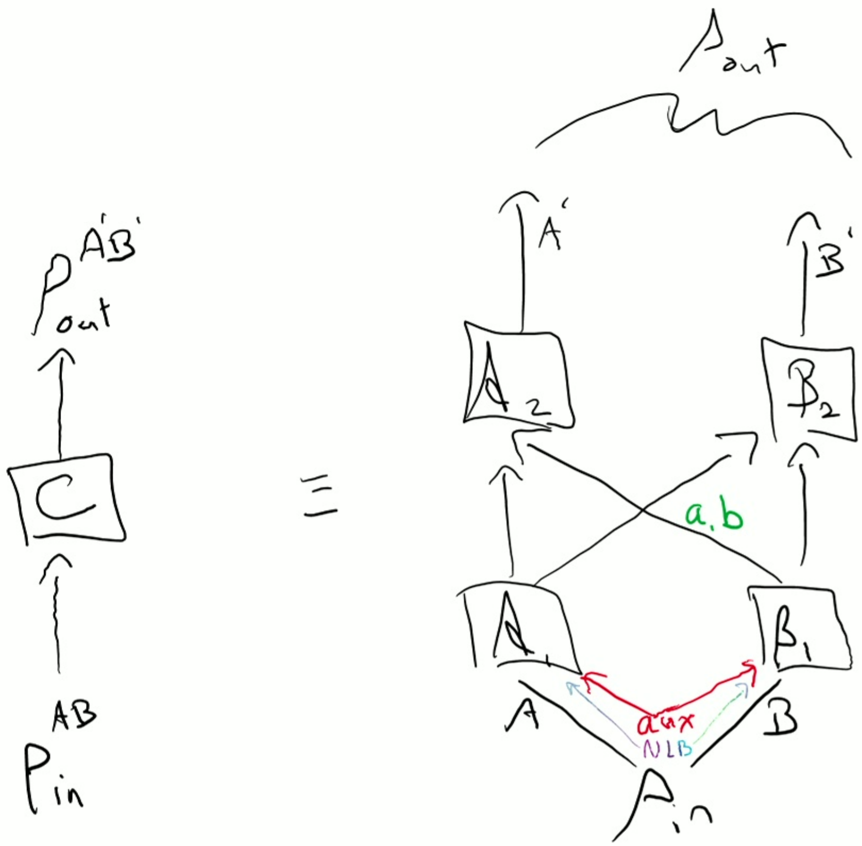
Main result

Instantaneous nonlocal quantum computation is possible using:

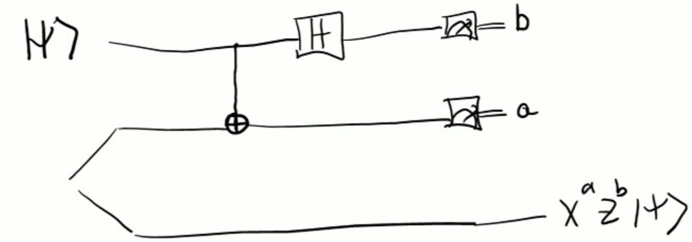
- a linear amount of shared entanglement
- Popescu-Rohrlich nonlocal Boxes (PR-Boxes)

Thus secure QPV is impossible against adversaries with the above resources.

Approaches

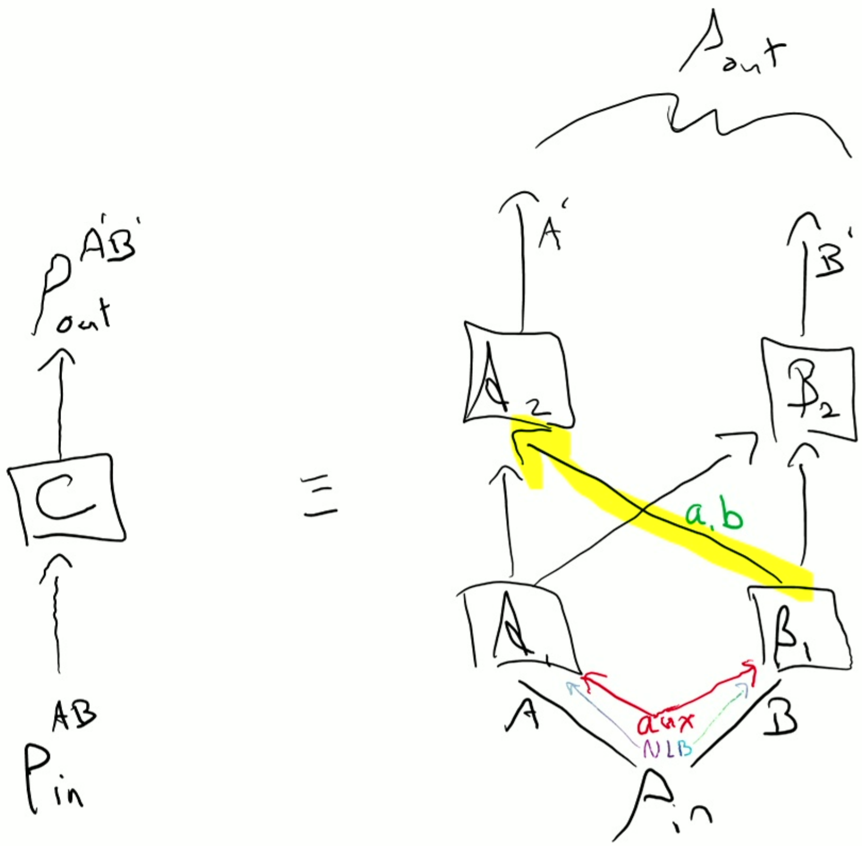


Teleportation:

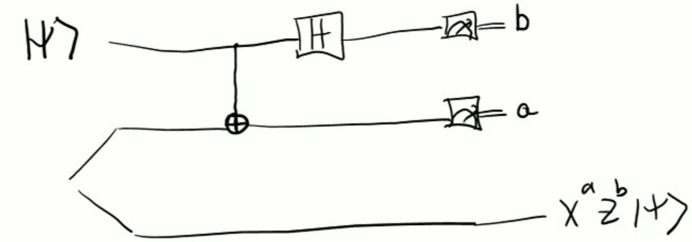


Attempt 1: Bob Teleports his input to Alice, then Alice does the computation *C*.

Approaches



Teleportation:

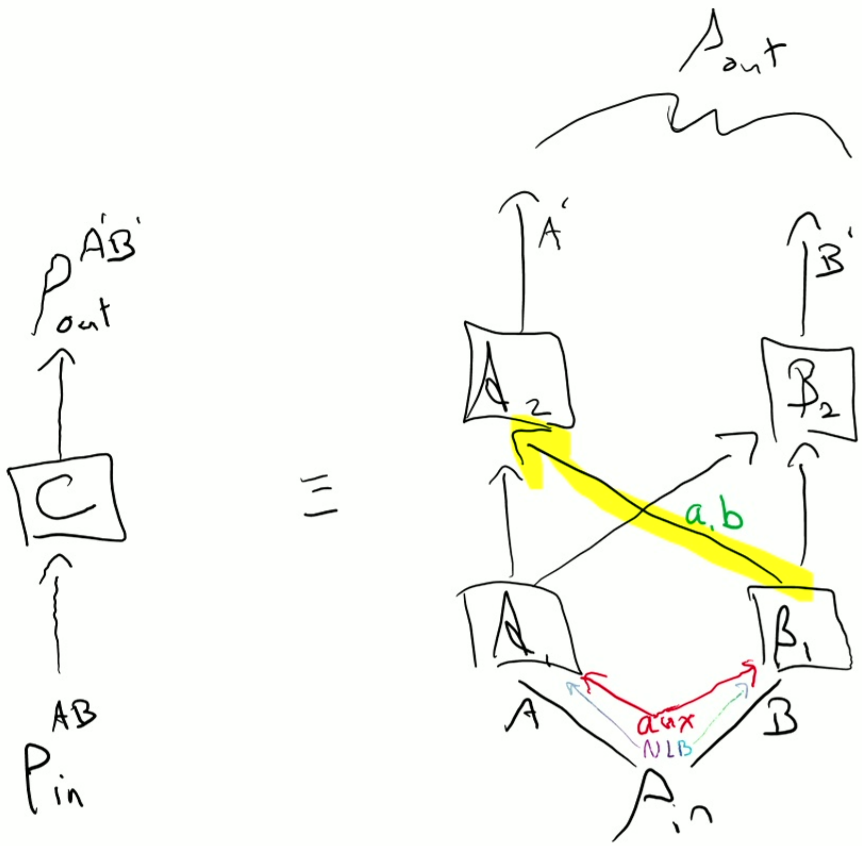


Attempt 1: Bob Teleports his input to Alice, then Alice does the computation *C*.

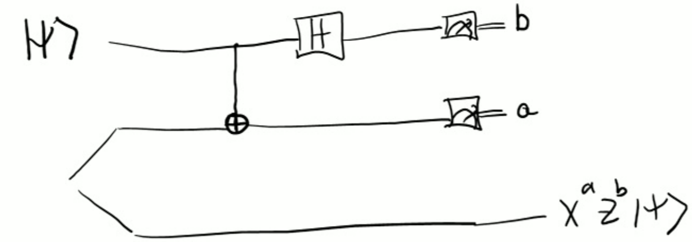
Problem: No way for Alice to return to Bob his part of the output

Solution: Don't send *a,b* to Alice!

Approaches



Teleportation:



Attempt 1: Bob Teleports his input to Alice, then Alice does the computation *C*.

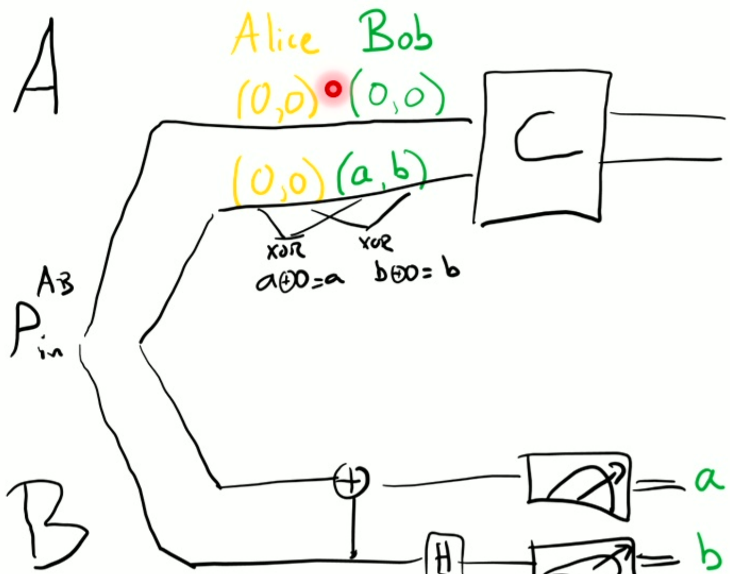
Problem: No way for Alice to return to Bob his part of the output

Solution: Don't send *a,b* to Alice!

Alice works with encrypted register.

Quantum One-Time Pad:

$$\rho \longmapsto \sum_{a,b\in\{0,1\}} X^a Z^b \rho Z^b X^a$$



Each wire for *C* has a distributed key that is the XOR of the keys that Alice and Bob each hold for the wire.

- All keys initially set to 0 except Bob's keys for the teleported registers are set to (a,b).
- Alice performs the quantum computation *C* on the encrypted data by decomposing C in a universal gateset and performing "gadgets" for each circuit element.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

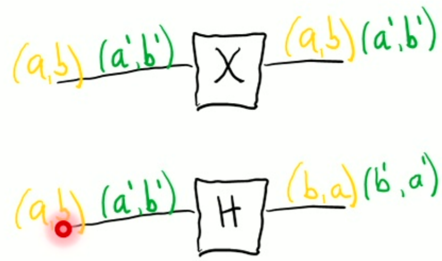
Pauli gates

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Clifford group gates

The Clifford Group is the set of operators that conjugate Pauli operators into Pauli operators.



$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

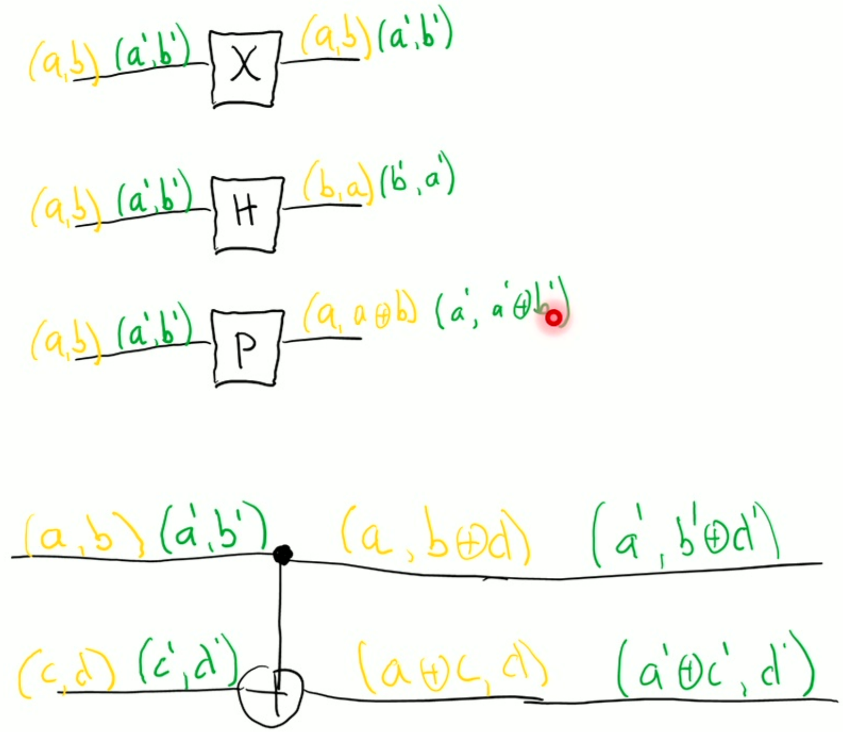
Pauli gates

$$\mathsf{P} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad \mathsf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\mathsf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Clifford group gates

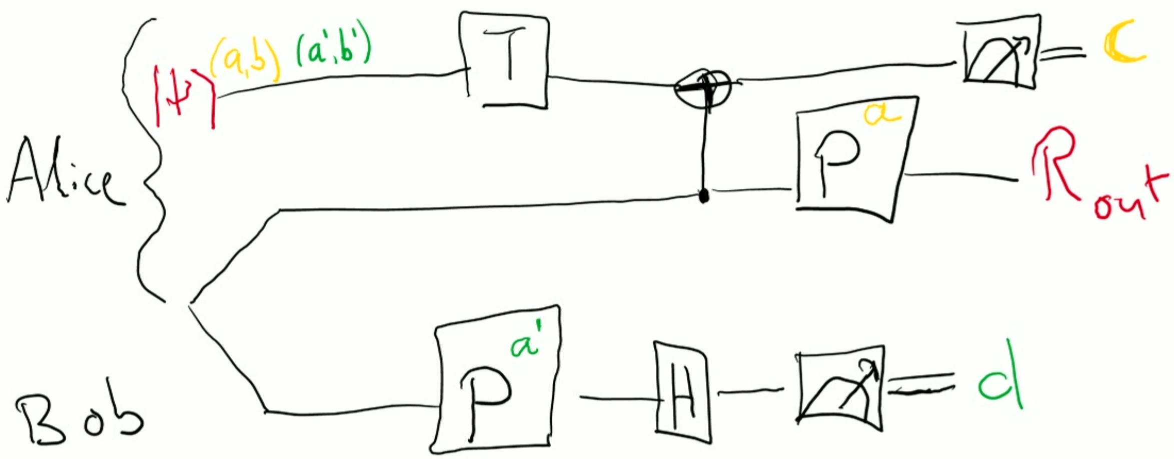
The Clifford Group is the set of operators that conjugate Pauli operators into Pauli operators.



$$\boxed{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Non-Clifford group gate

$$TX^aZ^b = X^aZ^{a\oplus b}P^aT$$

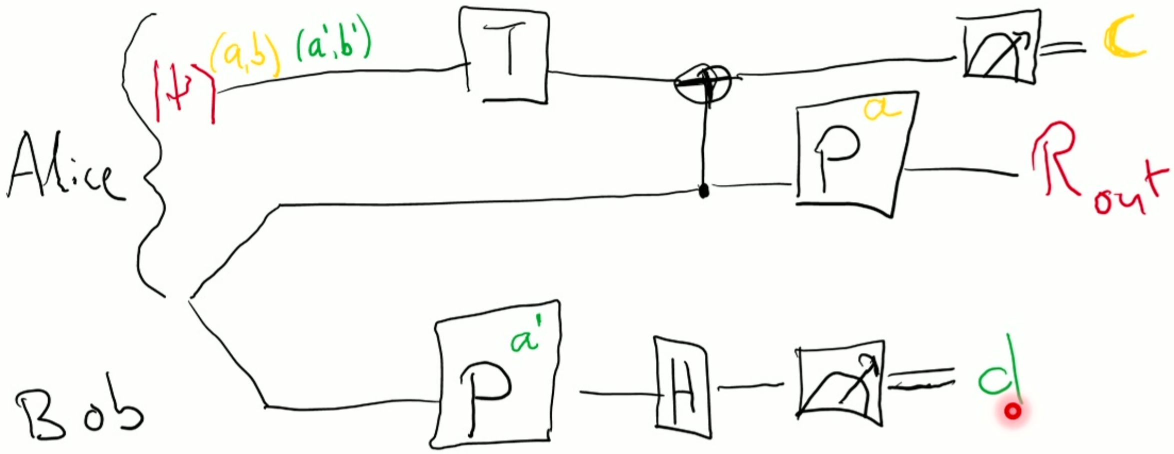


$$R_{out} = X^{a\oplus a'\oplus c}\, Z^{a\oplus a'\oplus b\oplus b'\oplus a\cdot c\oplus (a\oplus c)\cdot a'\oplus d}\, T|\psi\rangle$$

$$\boxed{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Non-Clifford group gate

$$TX^aZ^b = X^aZ^{a\oplus b}P^aT$$

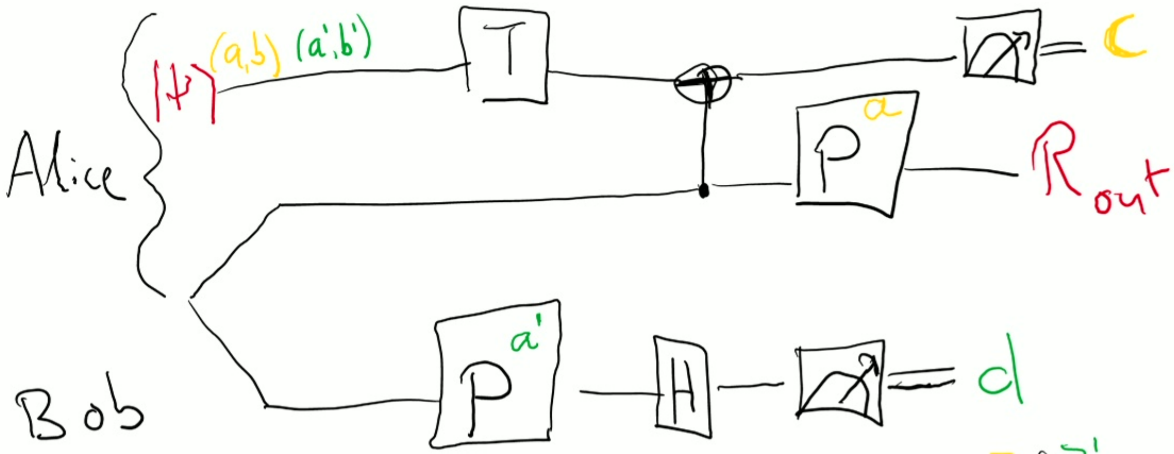


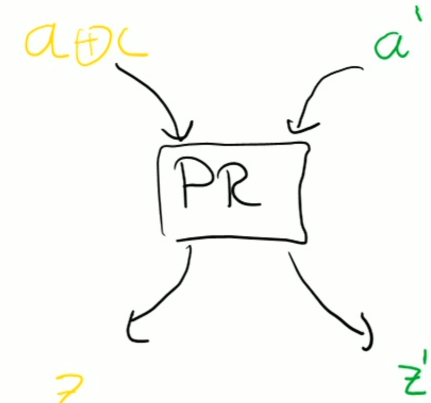
$$R_{out} = X^{a\oplus a'\oplus c}\, Z^{a\oplus a'\oplus b\oplus b'\oplus a\cdot c\oplus \underbrace{(a\oplus c)\cdot a'}_{\text{re-linearize with NLB}}\oplus d}\, T|\psi\rangle$$

$$\boxed{\mathsf{T}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Non-Clifford group gate

$$\mathsf{T}\mathsf{X}^a\mathsf{Z}^b = \mathsf{X}^a\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{T}$$



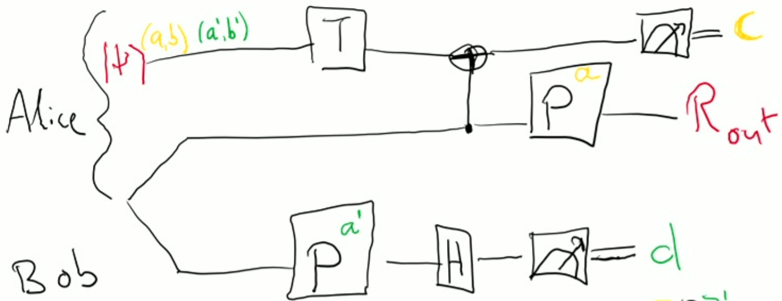


$$z \oplus z' = (a\oplus c)\cdot a'$$

$$R_{out} = X^{a\oplus a'\oplus c}\, Z^{a\oplus a'\oplus b\oplus b'\oplus a\cdot c\oplus \overbrace{\cancel{(a\oplus c)\cdot a'}}^{z\oplus z'}\oplus d}\, T|\psi\rangle$$

re-linearize with NLB

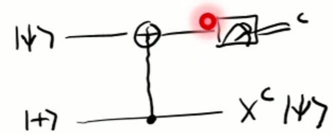
Correctness



$$R_{out} = X^{a \oplus a' \oplus c} Z^{a \oplus a' \oplus b \oplus b' \oplus a \cdot c \oplus \overset{z \oplus z'}{\cancel{(a \oplus c) \cdot a'}} \oplus d} T|\psi\rangle$$

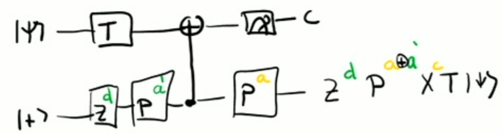
re-linearize with NLB

Start with X-teleportation circuit (Zhou, Leung, Chuang 2020)



$|+\rangle = H|0\rangle$

Add gates; diagonal *Z*, *P* commute with control



Substitute input

$$|\psi\rangle \leftarrow X^{a \oplus a'} Z^{b \oplus b'} |\psi\rangle$$

Simplify (details omitted), obtain key update

Note that Bob's circuit prepares the qubit $P^{a'} Z^{d} |+\rangle$

Final Round

- Alice sends Bob his output registers via teleportation; Alice computes the final Pauli key on her side.
- Both parties simultaneously exchange all classical keys.
- Local XOR calculations allow all parties to locally decrypt.

Conclusion

Instantaneous nonlocal quantum computation is possible using:

- 1 PR Box per T-gate
- *I*+ *T*+ *O* EPR pairs
  - *I*: Bob's input #qubits
  - *T*: # T-gates in *C*
  - *O*: Bob's output #qubits

These same resources break all QPV candidates!

Conclusion

Instantaneous nonlocal quantum computation is possible using:

- 1 PR Box per T-gate
- *I*+ *T*+ *O* EPR pairs
  - *I*: Bob's input #qubits
  - *T*: # T-gates in *C*
  - *O*: Bob's output #qubits

These same resources break all QPV candidates!

If QPV turns out to be possible against efficient quantum adversaries, it will be in part thanks to the fact that QM is not maximally nonlocal.

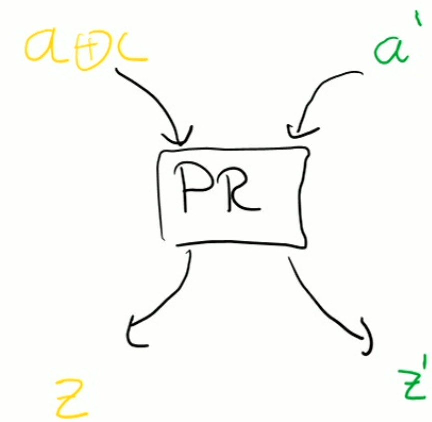
Open Question

- Can we tolerate noise in the PR Box in our results?

PRL **96,** 250401 (2006) PHYSICAL REVIEW LETTERS week ending 30 JUNE 2006

Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial

Gilles Brassard,[1] Harry Buhrman,[2,3] Noah Linden,[4] André Allan Méthot,[1] Alain Tapp,[1] and Falk Unger[3]



$$z \oplus z' = (a \oplus c) \cdot a'$$

Furter Directions

Alternate adversarial models for QPV

Could secure QPV be meaningful and possible against adversaries :

Furter Directions

Alternate adversarial models for QPV

Could secure QPV be meaningful and possible against adversaries :

1. That are bound by some computational assumptions?
   - One-way functions?
   - Pseudo-random quantum states?
2. That are bound by other models?
   - Noisy quantum storage
   - Low-depth quantum computation
   - Limited circuit architecture (circuit connectivity, etc.).
   - Other NISQ considerations (Noisy Intermediate-Scale Quantum Computation)

Thank you!