KAIST

November 14, 2023

QUANTUM POSITION VERIFICATION AND TIME-CONSTRAINED STATE DISCRIMINATION

ERIC CHITAMBAR

ARXIV:2311.00677

ARXIV:2312.XXXXX

<u>Work with friends</u>:

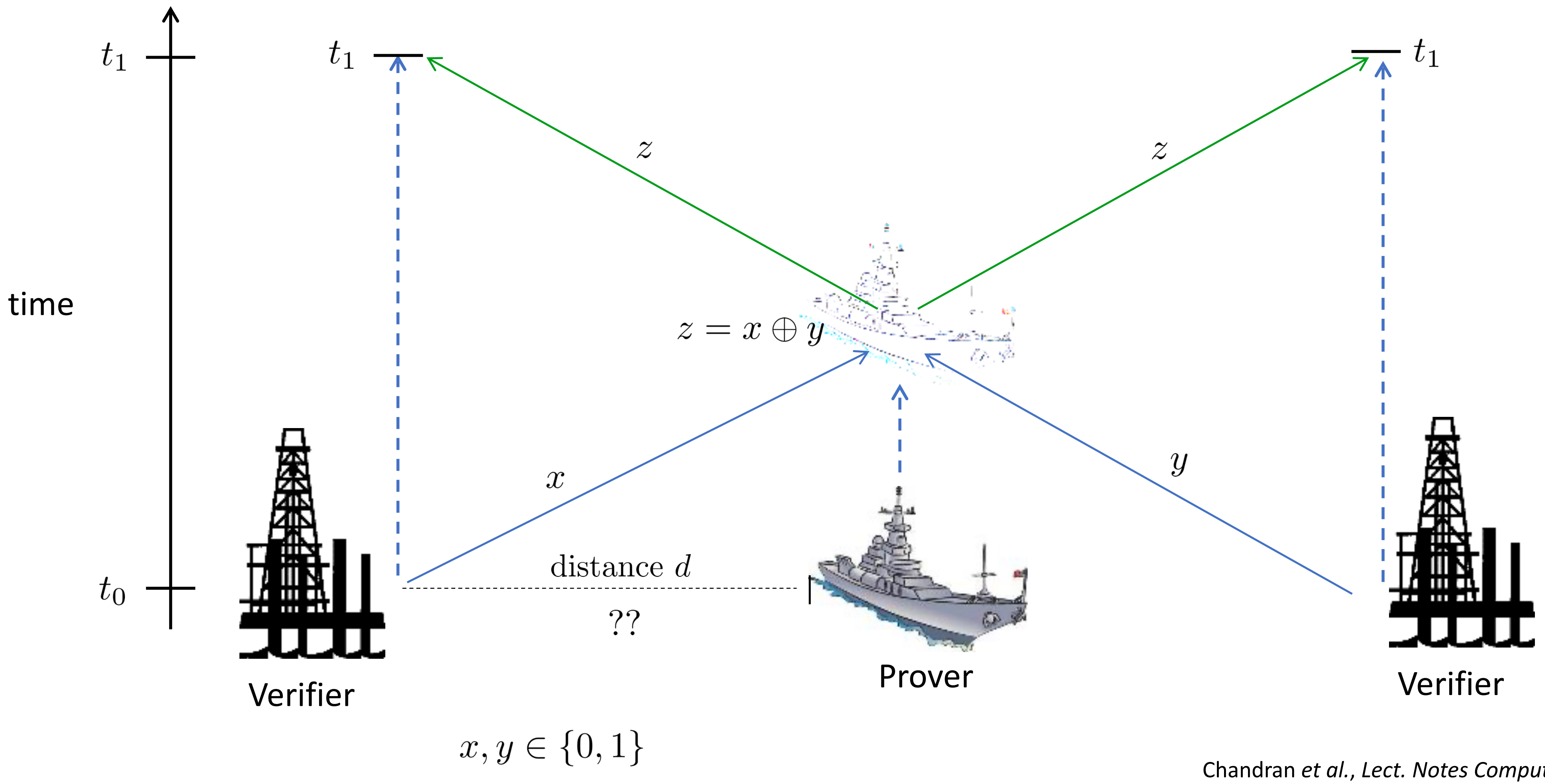
Rene Allerstorfer
Andrew Conrad
Ian George
Paul Kwiat
Philip Lunel

Outline of talk

1. Introduce the cryptographic task of quantum position verification (QPV)
2. Make a connection to AdS/CFT correspondence (one slide)
3. Describe QPV as a quantum state discrimination problem under restricted communication
4. Compare QPV product state discrimination protocols using classical versus quantum communication

Classical Position Verification

- **Goal:** Verify that the prover is truly a distance d from the leftmost verifier.

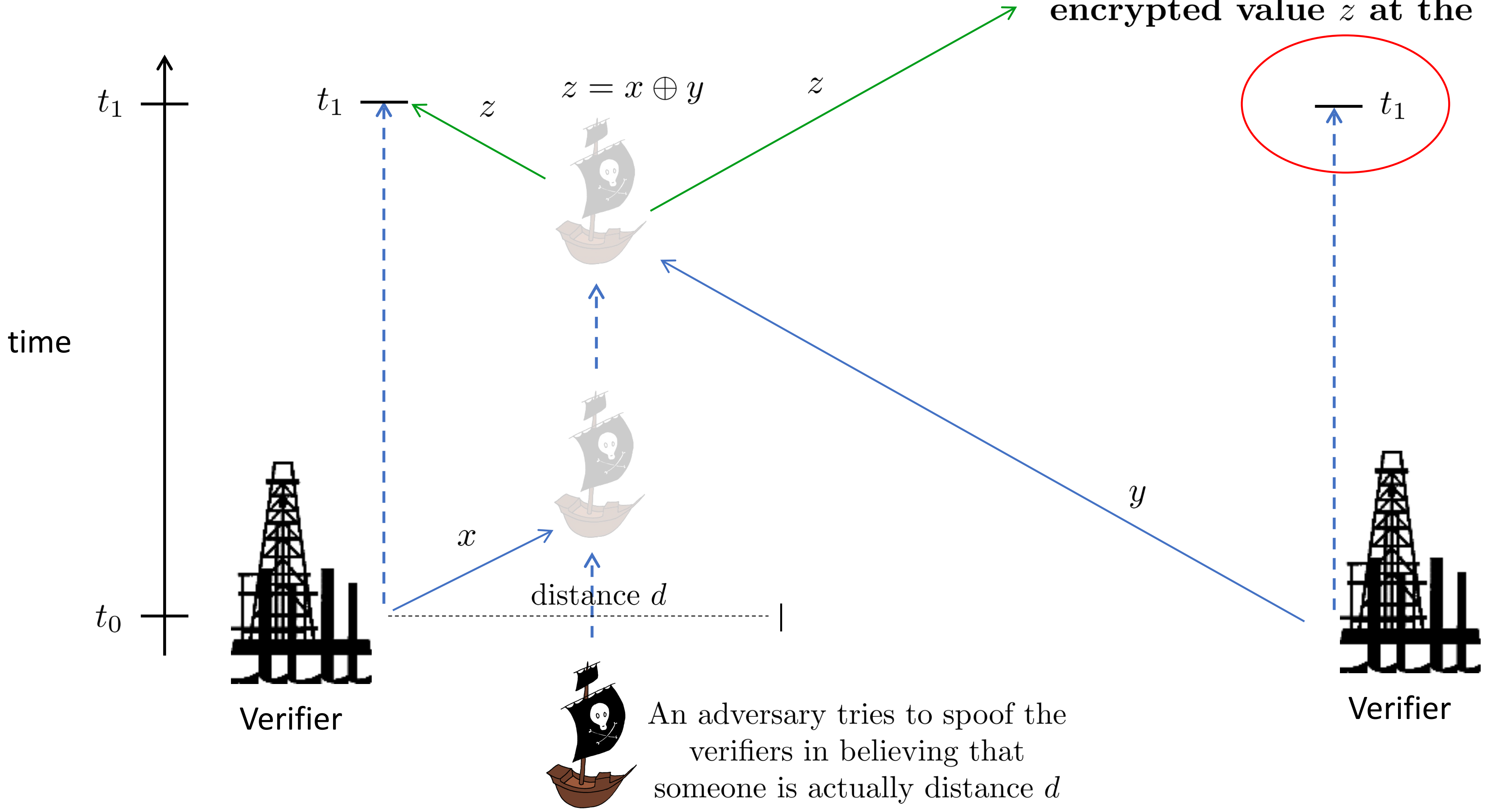


Chandran *et al.*, *Lect. Notes Comput. Sci.* (2009).

Classical Position Verification

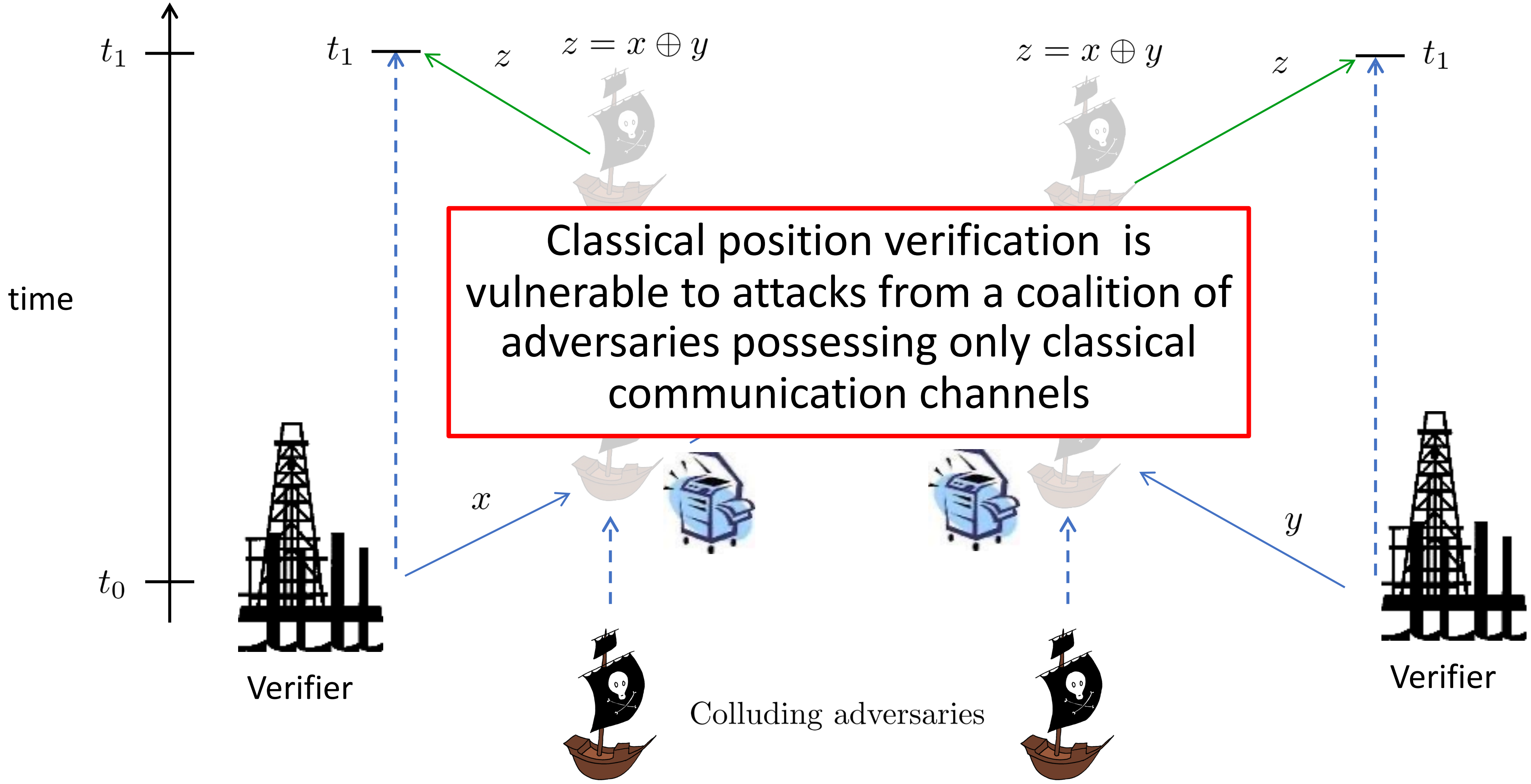
- Why does this work?

The second verifier won't receive the encrypted value z at the right time!



Classical Position Verification

- Not so fast...



Quantum Position Verification (QPV)

$x, y \in \{0, 1\}$

$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =: |+\rangle$

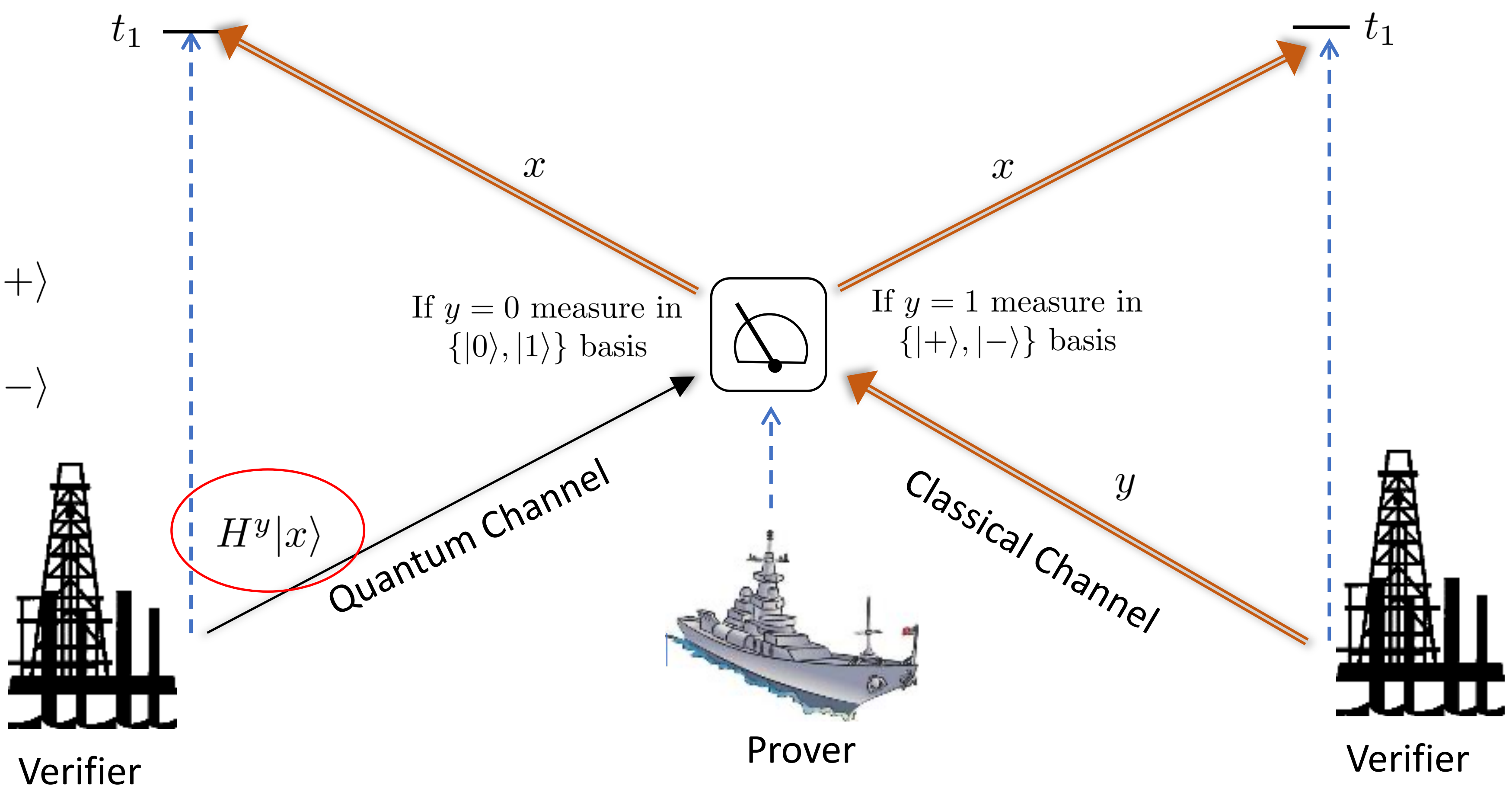
$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =: |-\rangle$

$H^0|0\rangle = |0\rangle$

$H^0|1\rangle = |1\rangle$

So the verifier sends one of the BB84 states:

$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



Chandran *et al.*, *Lect. Notes Comput. Sci.* (2009).
Kent *et al.*, *PRA* (2011).

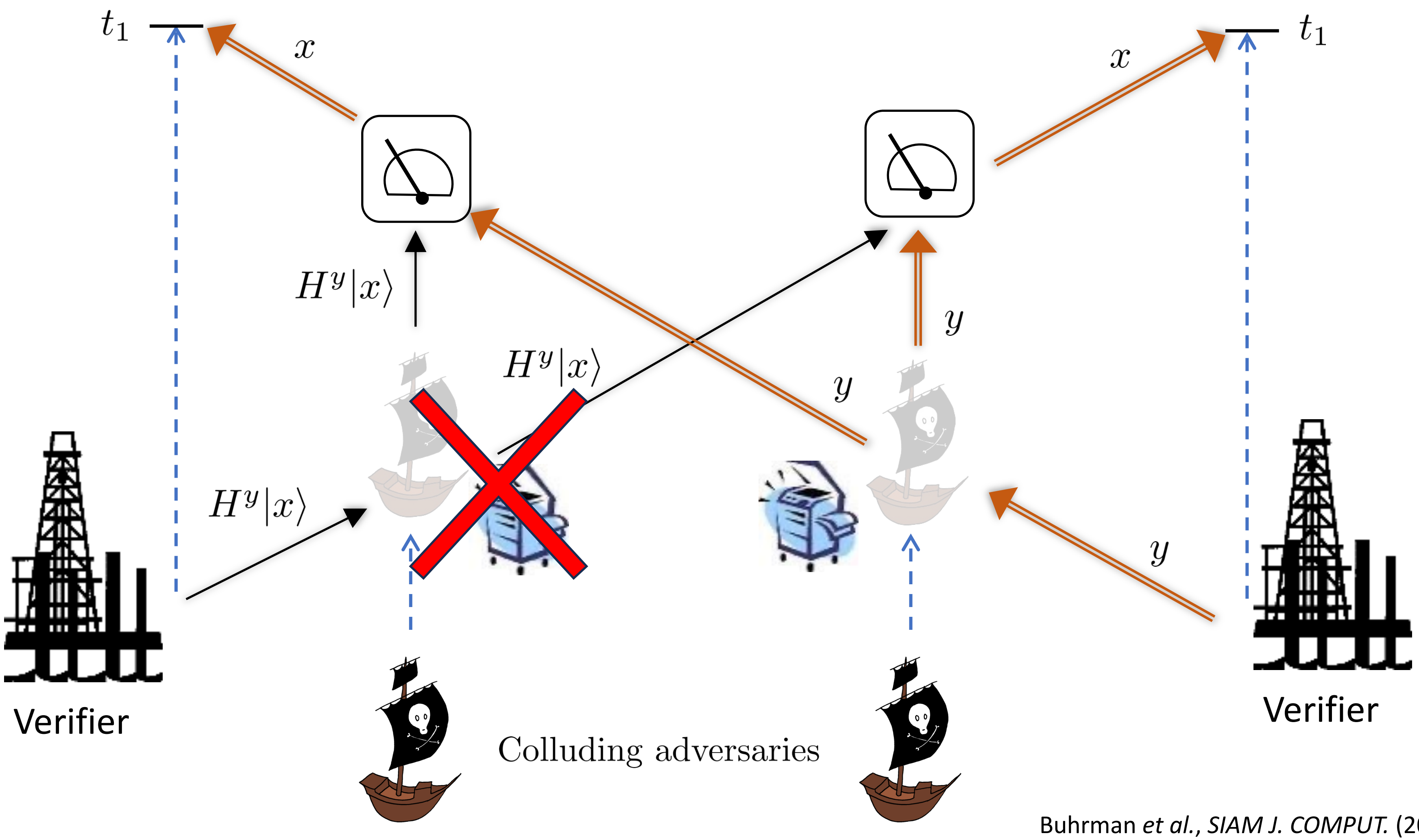
Quantum Position Verification (QPV)

- Is it secure? What about the classical attack?

Not possible due to quantum no-cloning principle!

$$H^y|x\rangle \rightarrow H^y|x\rangle \otimes H^y|x\rangle$$

Not physically realizable



Buhrman *et al.*, *SIAM J. COMPUT.* (2014).

Quantum Position Verification (QPV)

- Is it secure?

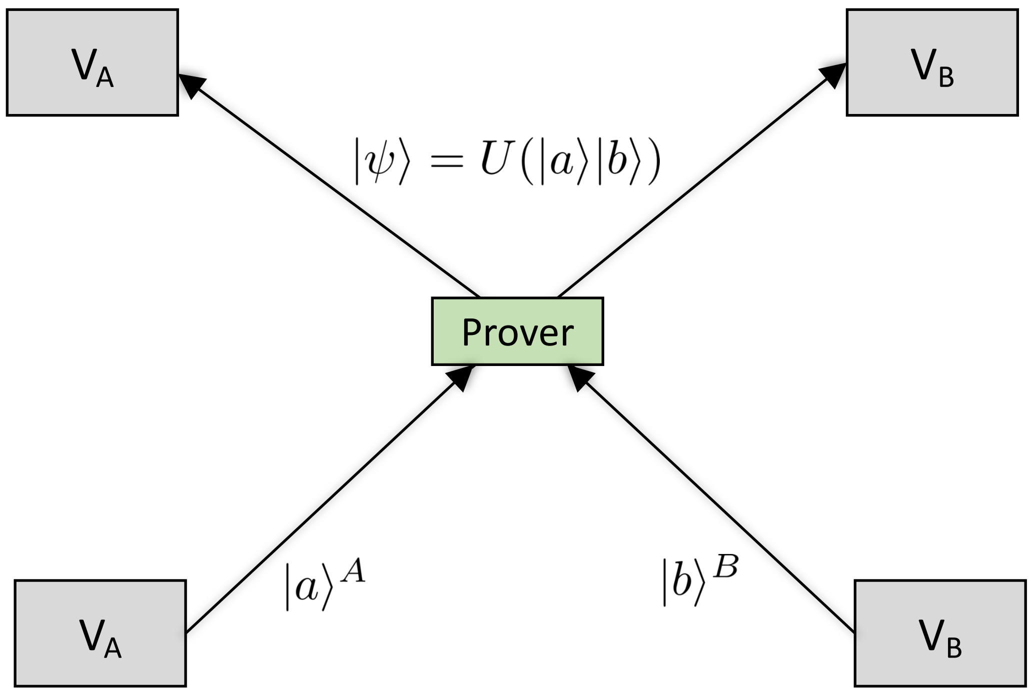
- Cloning attacks fail, but what about others?

- The prover is asked to perform some quantum computation U on the inputs $|a\rangle|b\rangle$ and return $|\psi\rangle = U(|a\rangle|b\rangle)$ within the correct time.

- **Intuition:** The unitary U should not be local:

$$U \neq U^A \otimes U^B.$$

A general QPV protocol



Honest QPV computation

Quantum Position Verification (QPV)

- Is it secure?

- The dishonest adversaries attempt to implement the computation U in spatially separated laboratories.

- Additionally they can have some pre-shared entanglement.

This is sometimes referred to as "**instantaneous nonlocal computation**".

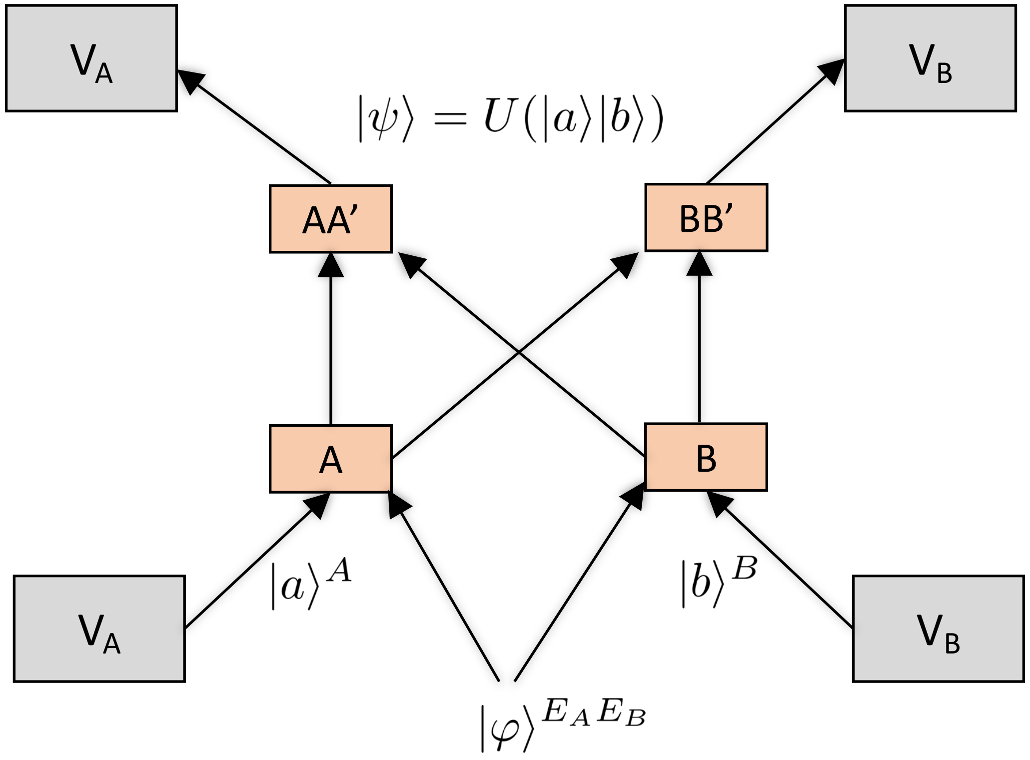
Bad news:

Given enough entanglement, the adversaries can implement *any* quantum computation U.

Good news:

There are certain computations that cannot be implemented unless the adversaries have a linear amount of entanglement.

A general QPV protocol



Dishonest QPV computation

Buhrman *et al.*, *SIAM J. COMPUT.* (2014). Beigi and König, *NJP* (2011). Bluhm *et al.*, *Nat Phys* (2022).

Quantum Position Verification (QPV)

- **Fundamental Question**: How much entanglement is needed to break quantum position verification?

- The best known attack is based on "Port-Based Teleportation":

Beigi and König, *New J. Phys.* (2011)

For n qubits sent from the verifier, QPV becomes insecure if adversaries use O(*exp(n)*) ebits.

- It is unknown whether attacks are possible that use a sub-exponential number of ebits for the hackers.

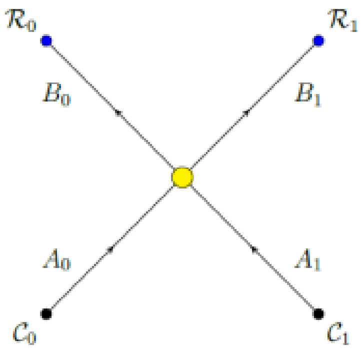
Open problem!!

- Assuming a high entanglement cost for hacking, secure quantum position verification might be a good candidate for implementation on first-generation quantum networks.

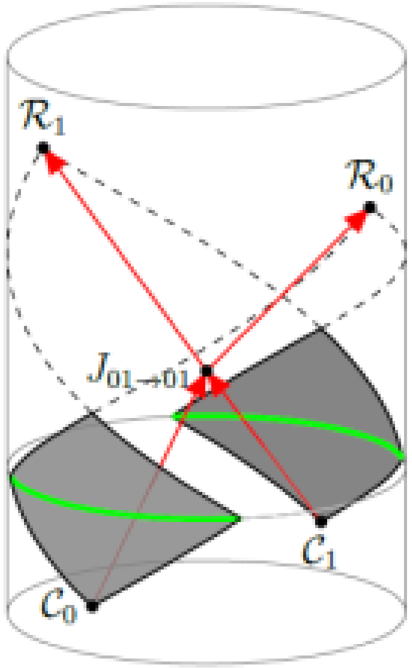
- However, the time delay in measurement by the prover could be problematic.

Connection to AdS/CFT correspondence

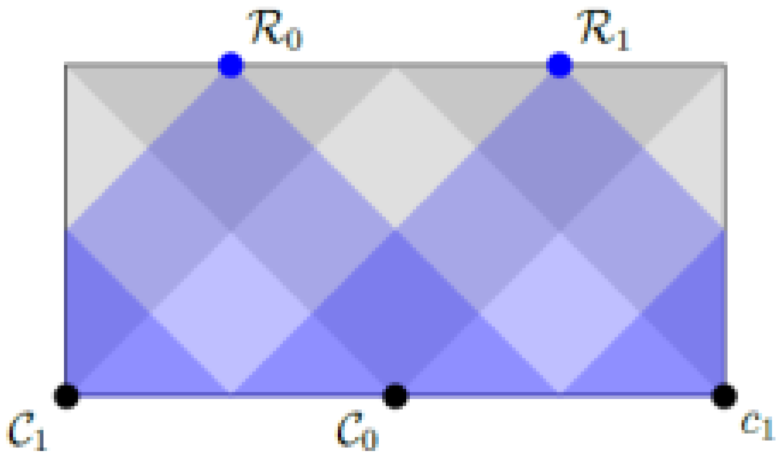
- The AdS/CFT correspondence proposes that quantum gravity in $(d+1)$-dim anti-de Sitter space (**the bulk**) can be described by a d-dim non-gravitational conformal field theory (**the boundary**).



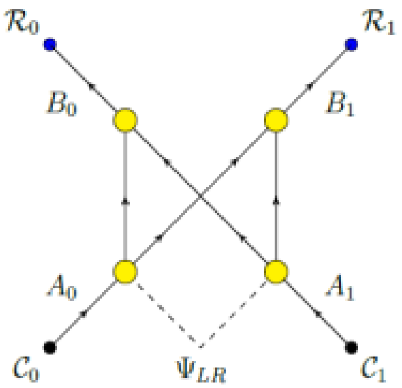
Honest QPV computation



The computation in the bulk



The computation on the boundary



Dishonest QPV computation

Puzzle: There is no causally consistent spacetime point for the computation to occur.

Proposed solution: Bulk computation = Honest QPV
Boundary computation = Dishonest QPV

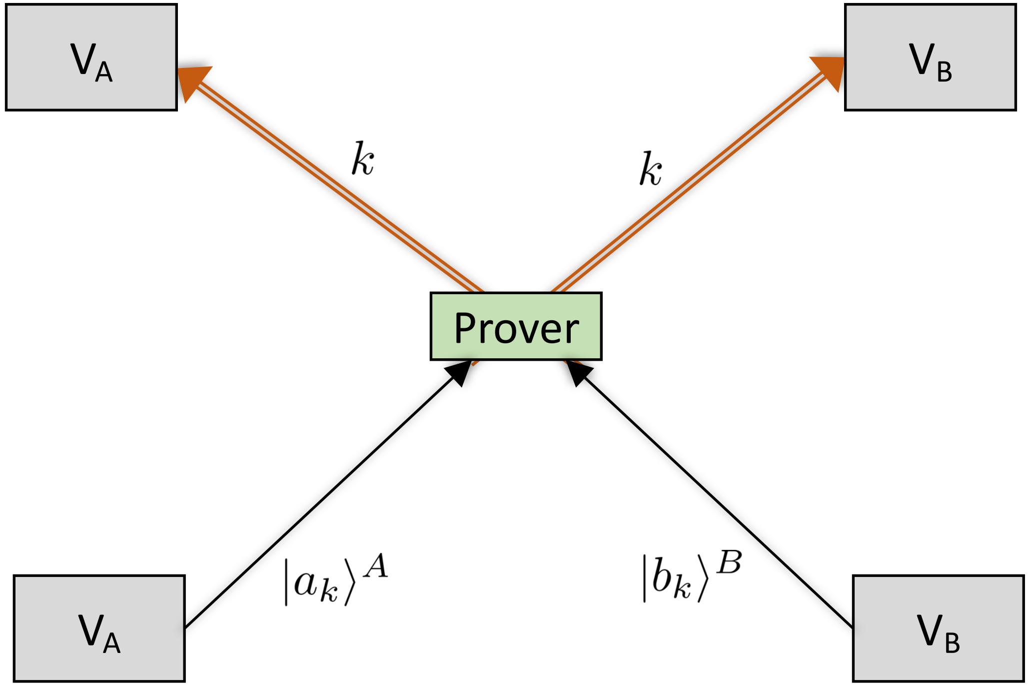
Please read Alex May's paper: *Quantum* **6**, 864 (2022).

QPV and state discrimination

- Let us consider a family of QPV protocols based on state discrimination.

A family of orthogonal states

$$\begin{cases} |\psi_1\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B \\ |\psi_2\rangle^{AB} = |1\rangle^A \otimes |0\rangle^B \\ |\psi_3\rangle^{AB} = |+\rangle^A \otimes |1\rangle^B \\ |\psi_4\rangle^{AB} = |-\rangle^A \otimes |1\rangle^B \end{cases}$$



- The prover needs to identify which bipartite state $|\psi_k\rangle^{AB}$ was sent by the verifiers.

QPV and state discrimination

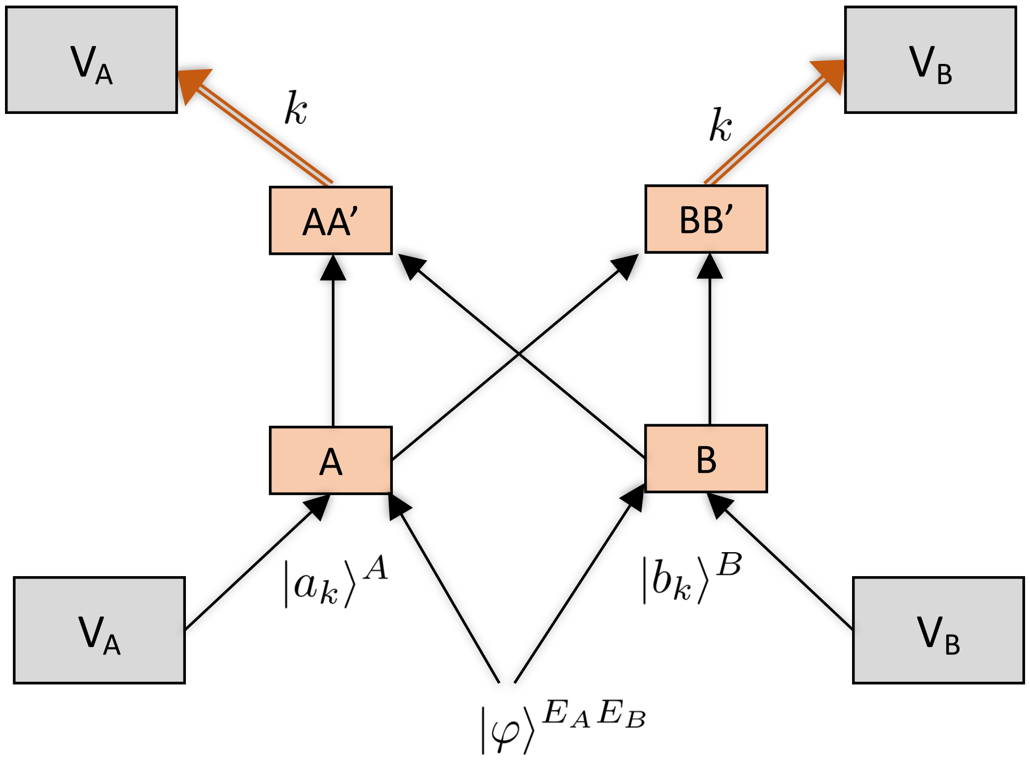
- In order to be secure, the orthogonality of the encoded states $|\psi_k\rangle$ must be sufficiently nonlocal.

- They should not be distinguishable by local operations and simultaneous communication.

- Different adversarial models to consider:

  – Local operations and simultaneous quantum communication (**LOSQC**)

  – Entanglement-assisted local operations and simultaneous quantum communication (**eLOSQC**)



QPV and state discrimination

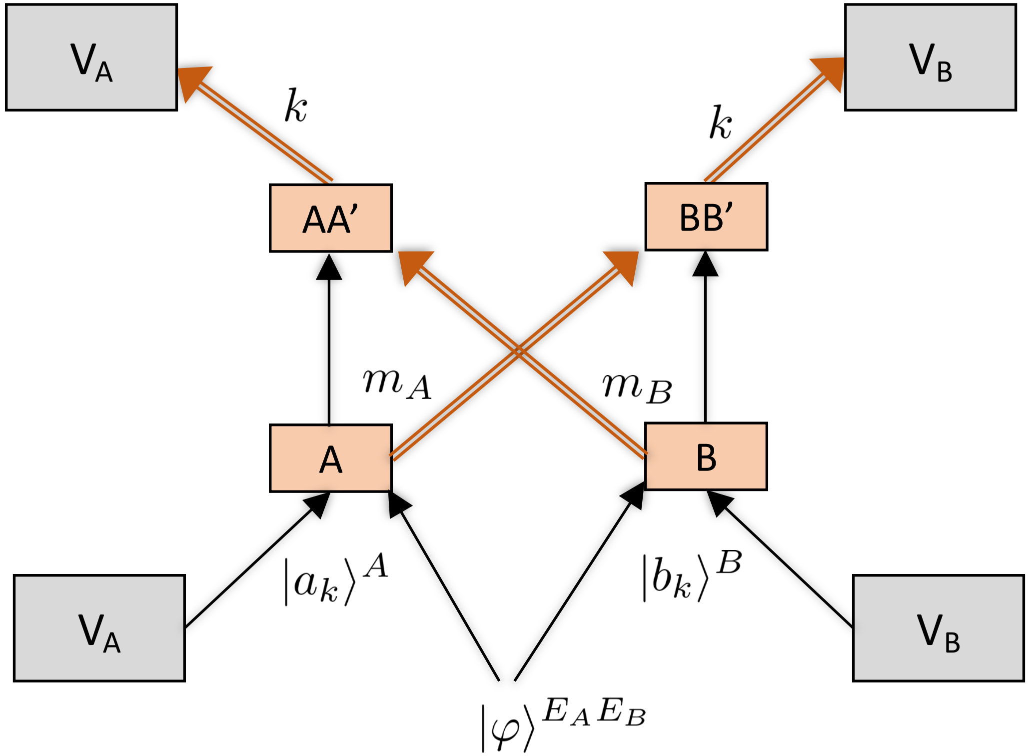
- In order to be secure, the orthogonality of the encoded states $|\psi_k\rangle$ must be sufficiently nonlocal.

- They should not be distinguishable by
  local operations and
  simultaneous communication.

- Different adversarial models to consider:

  - Local operations and simultaneous classical communication (**LOSCC**)

  - Entanglement-assisted local operations and simultaneous classical communication (**eLOSCC**)

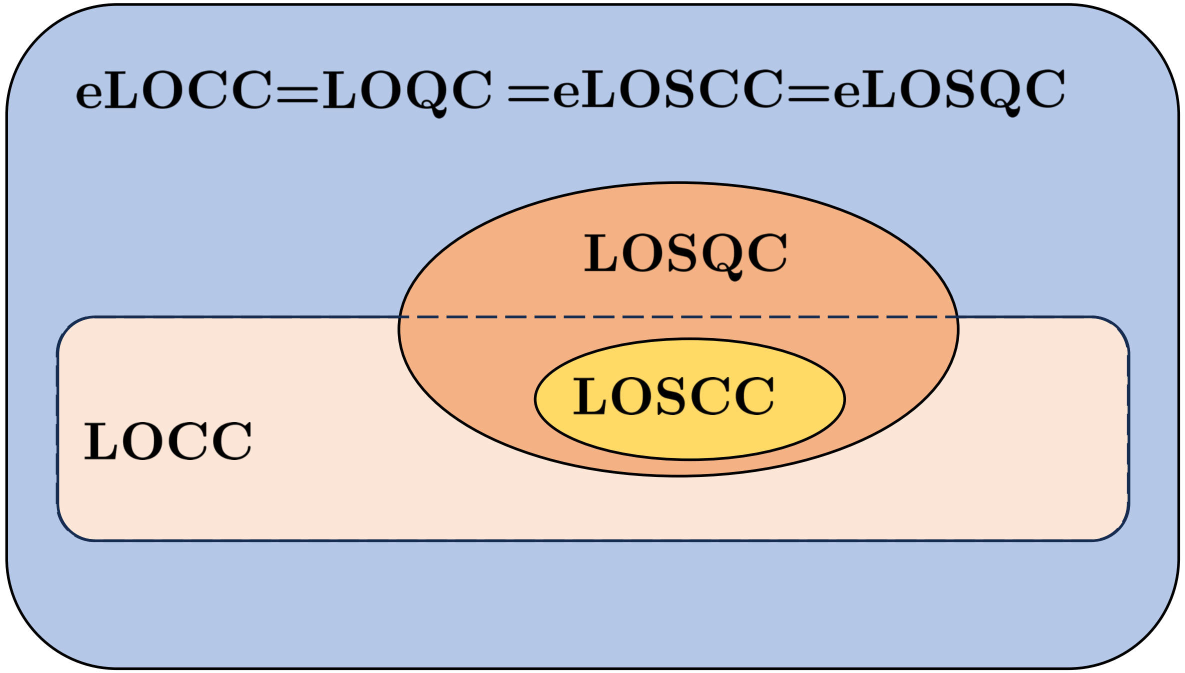


Different operational classes

- These should be compared to standard:

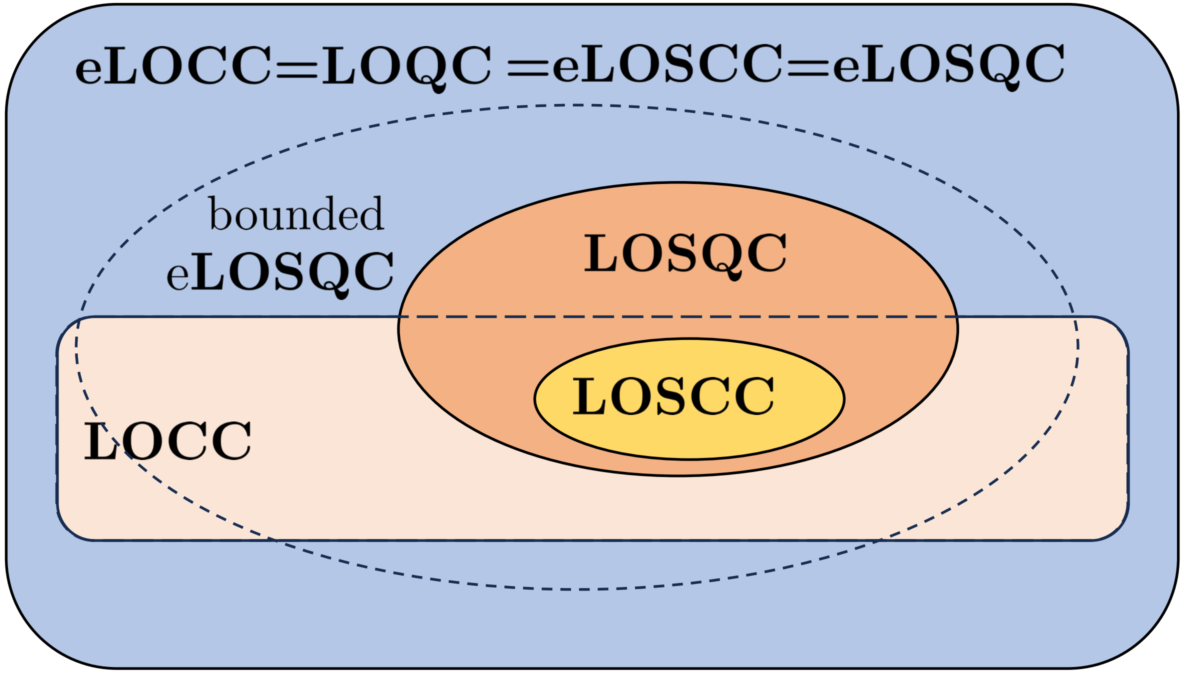
  - Local operations and classical communication (**LOCC**)
  - Entanglement-assisted local operations and classical communication (**eLOCC**)
  - Local operations and quantum communication (**LOQC**)

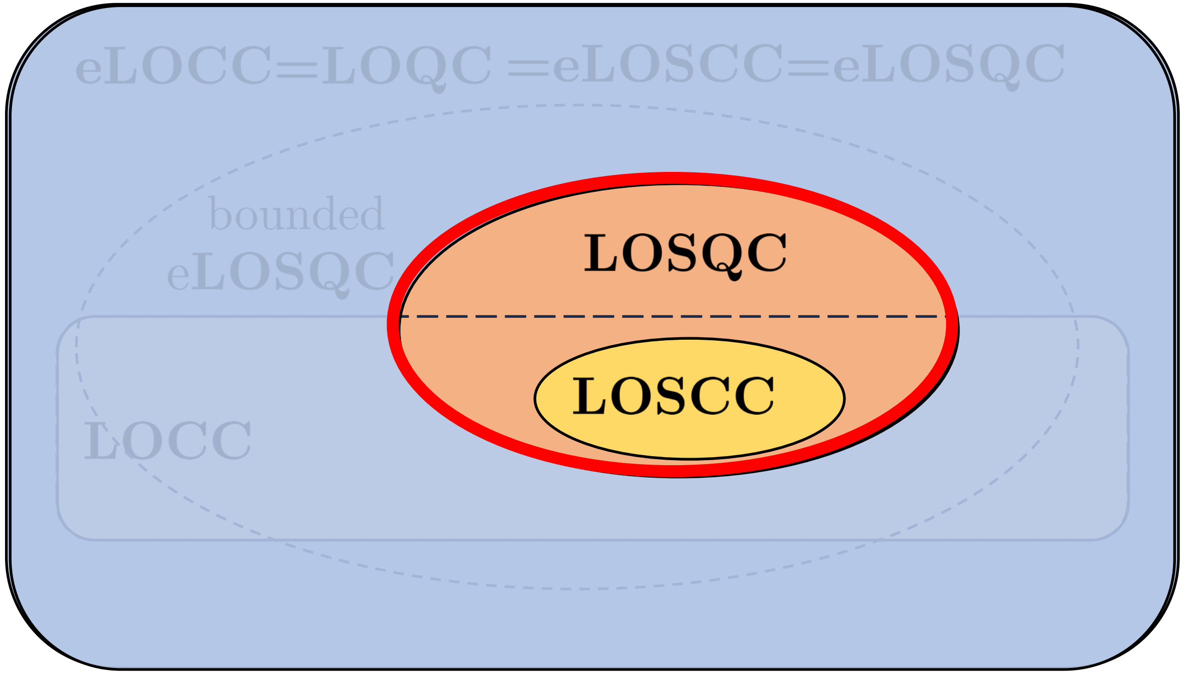
Unrestricted classical communication



- Only a few papers (motivated by QPV) have explored the relationship between these operational classes.

Different operational classes





- The intermediate regime of **bounded entanglement** is where most QPV analysis sits.

- Every family of orthogonal $\{|\psi_k\rangle\}_k$ that is difficult to discriminate using a class of operations constitutes a good QPV scheme under attacks from that class.

- The **no pre-shared entanglement** model is the simplest to analyze, but even in this scenario relatively little is known.

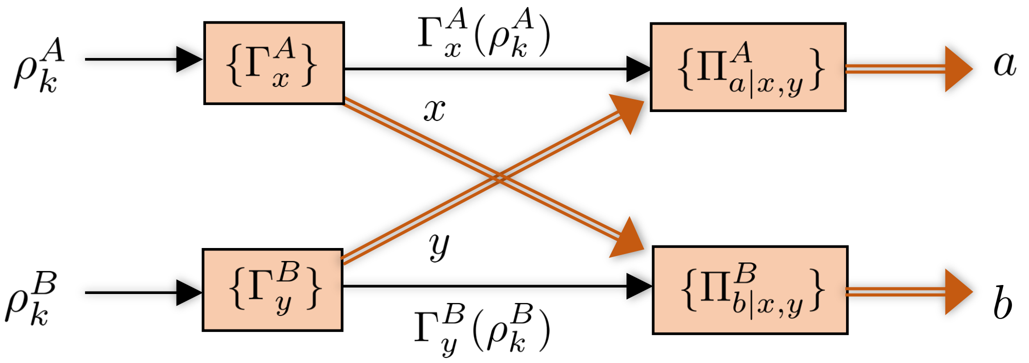
- Simplify the problem even further:
  How well can a family of orthogonal **product states**

  $$\{|\psi_k\rangle = |a_k\rangle^A |b_k\rangle^A\}_k$$

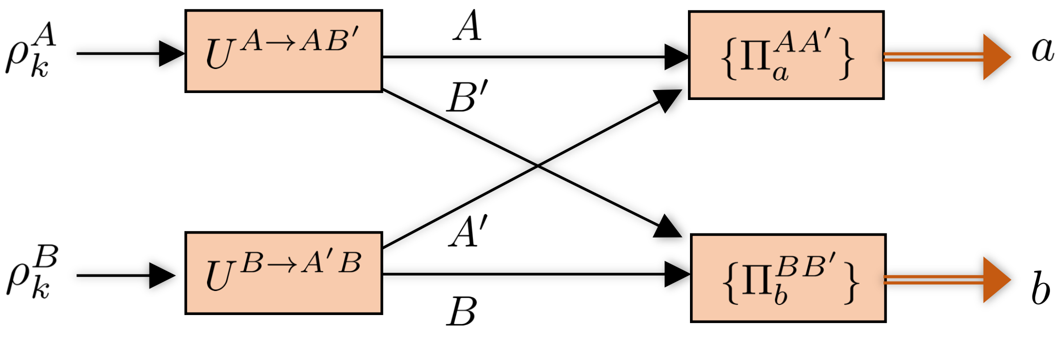
  be distinguished by LOSCC and LOSQC?

The structure of LOSCC and LOSQC protocols

- The structure of LOSCC protocols:



- The structure of LOSQC protocols:



- Does the quantum communication help?

Yes!

Consider the symmetric and anti-symmetric projectors:

$$\rho_+^{AB'} = \tfrac{1}{3}(|\Phi^+\rangle\langle\Phi^+| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|)$$

$$\rho_-^{AB'} = |\Psi^-\rangle\langle\Psi^-|$$

Take two copies: $\rho_+^{AB'} \otimes \rho_+^{A'B}$

$\rho_-^{AB'} \otimes \rho_-^{A'B}$

- Perfectly distinguishable by LOSQC but not LOSCC.

Allerstorfer, Buhrman, Speelman, Lunel, arXiv:2208.04341.

- But these involve distinguishing entangled states.

What about for product states?

Distinguishing orthogonal product states

- This problem has a rich history in quantum information theory.
  - Any $2 \otimes 2$ family of orthogonal product states can be perfectly distinguished by LOCC.

Walgate and Hardy, **PRL** 89, 147901 (2002).

$$\begin{cases} |\psi_1\rangle = |0\rangle \otimes |\theta\rangle & |\psi_3\rangle = |1\rangle \otimes |\phi\rangle \\ |\psi_2\rangle = |0\rangle \otimes |\theta^{\perp}\rangle & |\psi_4\rangle = |1\rangle \otimes |\phi^{\perp}\rangle \end{cases}$$

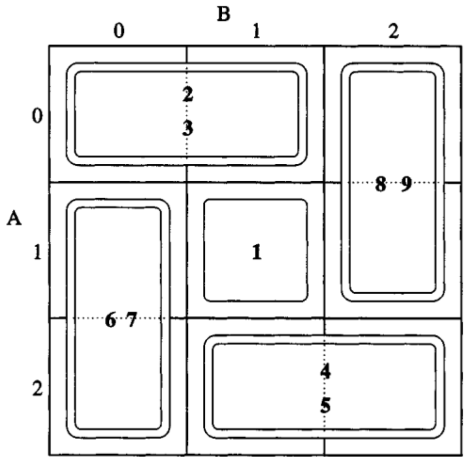
  - Any $2 \otimes n$ family of orthogonal product states can be perfectly distinguished by LOCC.

Bennett, DiVincenzo, Mor, Shor, Smolin, Terhal, **PRL** 82, 5385 (1999).

  - There exists orthogonal product state that cannot be distinguished by LOCC

"Nonlocality without entanglement"

$$\begin{cases} |\psi_1\rangle = |1\rangle \otimes |1\rangle & |\psi_4\rangle = |2\rangle \otimes |1+2\rangle & |\psi_7\rangle = |1-2\rangle \otimes |0\rangle \\ |\psi_2\rangle = |0\rangle \otimes |0+1\rangle & |\psi_5\rangle = |2\rangle \otimes |1-2\rangle & |\psi_8\rangle = |0+1\rangle \otimes |2\rangle \\ |\psi_3\rangle = |0\rangle \otimes |0-1\rangle & |\psi_6\rangle = |1+2\rangle \otimes |0\rangle & |\psi_8\rangle = |0-1\rangle \otimes |2\rangle \end{cases}$$



Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin, Wootters, **PRA** 59, 1070 (1999).

Distinguishing orthogonal product states

Proposition [I.George, R. Allerstorfer, P. Lunel, E.C.]:

- For perfect discrimination of $2 \otimes 2$ orthogonal product states, LOSQC=LOSCC and the states must have the form:

$$\begin{cases} |\psi_1\rangle = |0\rangle \otimes |0\rangle & |\psi_3\rangle = |1\rangle \otimes |0\rangle \\ |\psi_2\rangle = |0\rangle \otimes |1\rangle & |\psi_4\rangle = |1\rangle \otimes |1\rangle \end{cases}$$

- A $2 \otimes n$ family of orthogonal product states can be perfectly distinguished by LOSC iff it has the form:

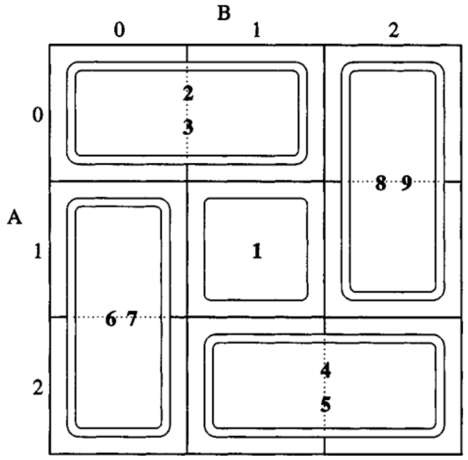
$$\begin{cases} \left.\begin{array}{l} |0\rangle^A \otimes |j\rangle^B \\ |1\rangle^A \otimes (x_j|j\rangle + y_j|j+1\rangle)^B \end{array}\right\} \text{ for } \quad j \in \{0, 2, 4, ..., 2m\} \\ |g_i\rangle^A \otimes |i\rangle^B \quad \text{for} \quad i > 2m+1 \end{cases}$$

- For arbitrary dimensions, the necessary and sufficient conditions are unknown! (Open problem)

Distinguishing orthogonal product states

- But what about the sausage states?

$$\left\{ \begin{array}{lll} |\psi_1\rangle = |1\rangle \otimes |1\rangle & |\psi_4\rangle = |2\rangle \otimes |1+2\rangle & |\psi_7\rangle = |1-2\rangle \otimes |0\rangle \\ |\psi_2\rangle = |0\rangle \otimes |0+1\rangle & |\psi_5\rangle = |2\rangle \otimes |1-2\rangle & |\psi_8\rangle = |0+1\rangle \otimes |2\rangle \\ |\psi_3\rangle = |0\rangle \otimes |0-1\rangle & |\psi_6\rangle = |1+2\rangle \otimes |0\rangle & |\psi_8\rangle = |0-1\rangle \otimes |2\rangle \end{array} \right.$$



- These states cannot be distinguished by LOSCC.

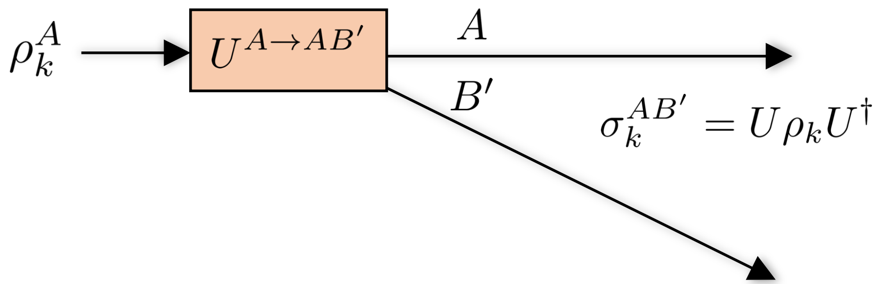
- They also cannot be distinguished by LOSQC (see theorem below).

- What about two copies of the states: $\{|\psi_k\rangle^{\otimes 2} = |a_k\rangle^{\otimes 2} \otimes |b_k\rangle^{\otimes 2}\}$? $\Longrightarrow$
  - Distinguishable by LOSQC
  - Distinguishable by LOSCC

Conjecture:

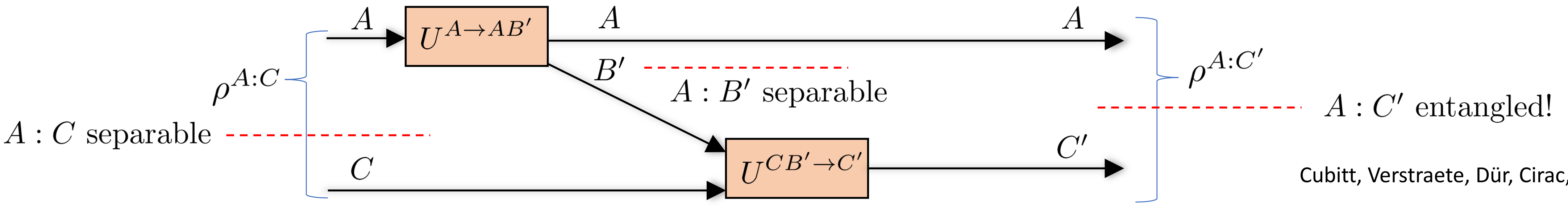
Two copies of any set of orthogonal product states is sufficient for LOSCC discrimination (or at least the ensemble must have a large number of states).

LOSQC is more powerful than LOSCC



- Distinguish between two types of quantum communication:
  - **Separable communication**, i.e. $\sigma_k^{AB'}$ is separable for all k.
  - **Entangled communication**, i.e. $\sigma_k^{AB'}$ is entangled for some k.

- Separable communication can be used to perform non-classical tasks, like entanglement distribution.



Cubitt, Verstraete, Dür, Cirac, **PRL** 91, 037902 (2003).

Theorem [I.George, R. Allerstorfer, P. Lunel, E.C.]:

The four states can be perfectly distinguished by LOSQC only if entangled communication is used:

$$\left\{ \begin{array}{ll} |\psi_1\rangle = |0\rangle \otimes |0+1\rangle & |\psi_3\rangle = |1\rangle \otimes |0+2\rangle \\ |\psi_2\rangle = |0\rangle \otimes |0-1\rangle & |\psi_4\rangle = |1\rangle \otimes |0-2\rangle \end{array} \right.$$

LOSQC state discrimination with error

- Perfect state discrimination is interesting from a fundamental persective, but not for practical QPV.
- **QPV question:**

  Given an ensemble $\{|\psi_k\rangle\}_k$, what is the smallest error probability in state discrimination using LOSQC?

Theorem [I.George, R. Allerstorfer, P. Lunel, E.C.]:

Let $\{|\psi_k\rangle^{AB} = |a_k\rangle^A |b_k\rangle^B\}_k$ be an ensemble of product states that contains four states of the form

$$\begin{aligned}
|\psi_0\rangle^{AB} &= |a_0\rangle^A |b_0\rangle^B, \\
|\psi_1\rangle^{AB} &= |a_1\rangle^A |b_1\rangle^B, \\
|\psi_2\rangle^{AB} &= |a_2\rangle^A (\cos\theta |b_0\rangle + e^{i\phi}\sin\theta |b_1\rangle)^B \\
|\psi_3\rangle^{AB} &= |a_3\rangle^A (\cos\theta |b_0\rangle - e^{i\phi}\sin\theta |b_1\rangle)^B,
\end{aligned}$$

with $\langle a_0|a_1\rangle \neq 0$. Suppose Alice and Bob can identify each state with at least probability $1-\epsilon$ using some LOBQC protocol. Then

$$2\epsilon + \frac{4\sqrt{\epsilon(1-\epsilon)}}{|\langle a_0|a_1\rangle|^2} + \sqrt{1 - |\langle a_2|a_3\rangle|^2} > 1.$$

LOSQC state discrimination with error

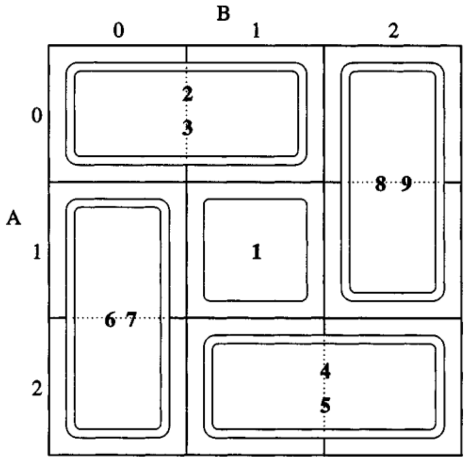
Example: Generalized BB84 states:

$$
\begin{aligned}
|\psi_0\rangle^{AB} &= |0\rangle^A \otimes |0\rangle^B, \\
|\psi_1\rangle^{AB} &= |0\rangle^A \otimes |1\rangle^B, \\
|\psi_2\rangle^{AB} &= |1\rangle^A \otimes (\cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle)^B \\
|\psi_3\rangle^{AB} &= |1\rangle^A \otimes (\cos\theta|0\rangle - e^{i\phi}\sin\theta|1\rangle)^B
\end{aligned}
$$

The LOSQC error probability P_{err} is lower bounded as: $P_{err} > \frac{1}{4}\left(\frac{1}{2} - \frac{1}{\sqrt{5}}\right) \approx 1.3\%.$

- But what about the sausage states?

Example:



The LOSQC error probability P_{err} is lower bounded as:

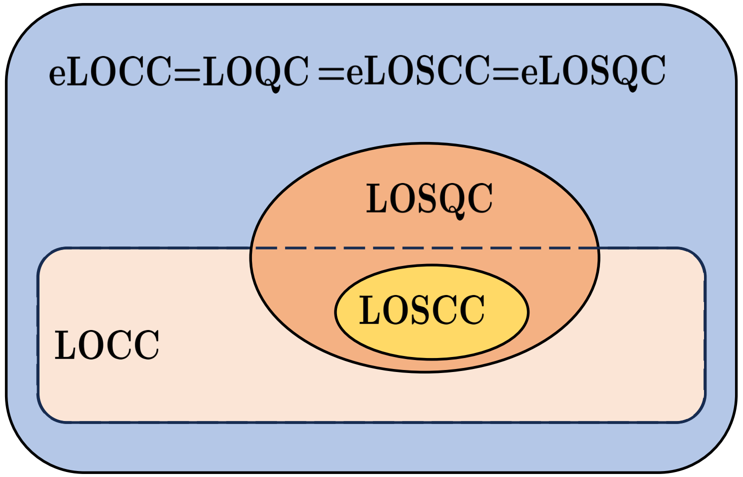
$$P_{err} > \frac{1}{9}\left(\frac{1}{2} - \frac{2}{\sqrt{17}}\right) \approx .16\%.$$

Open problems and future directions

- What are the necessary and sufficient conditions for product state discrimination under LOSCC and LOSQC?

- **Copy complexity**: How many copies of an ensemble state do Alice and Bob need before they can perfectly discriminate by LOSCC?

$$\{|\psi_k\rangle^{\otimes n} = |a_k\rangle^{\otimes n} \otimes |b_k\rangle^{\otimes n}\}$$



- What families of states are distinguishable by LOSQC but not LOCC?

- **Most important question for QPV**:
  What are the entanglement costs for state discrimination under eLOSCC and eLOSQC?

- **Example: BB84 states**:

$$\begin{cases} |\psi_1\rangle^{AB} = |0\rangle^A \otimes |0\rangle^B & |\psi_3\rangle^{AB} = |+\rangle^A \otimes |1\rangle^B \\ |\psi_2\rangle^{AB} = |1\rangle^A \otimes |0\rangle^B & |\psi_4\rangle^{AB} = |-\rangle^A \otimes |1\rangle^B \end{cases}$$

One ebit suffices for perfect discrimination

Lo and Lau **PRA** 83, 012322 (2011).


Thank You!