Title: Attacking QPV with instantaneous non-local computation of low T-depth quantum circuits

Speakers: Florian Speelman

Collection: QPV 2023: Advances in quantum position verification

Date: September 21, 2023 - 9:30 AM

URL: https://pirsa.org/23090021

arXiv:1511.02839

Instantaneous non-local computation of low T-depth quantum circuits

Florian Speelman

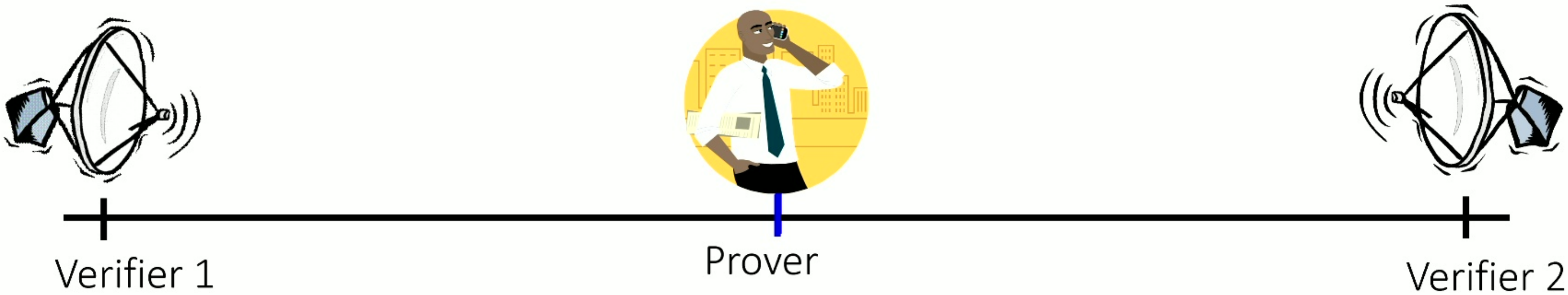
QPV 2023
September 21, 2023

QuSoft
Research Center for Quantum Software

Overview

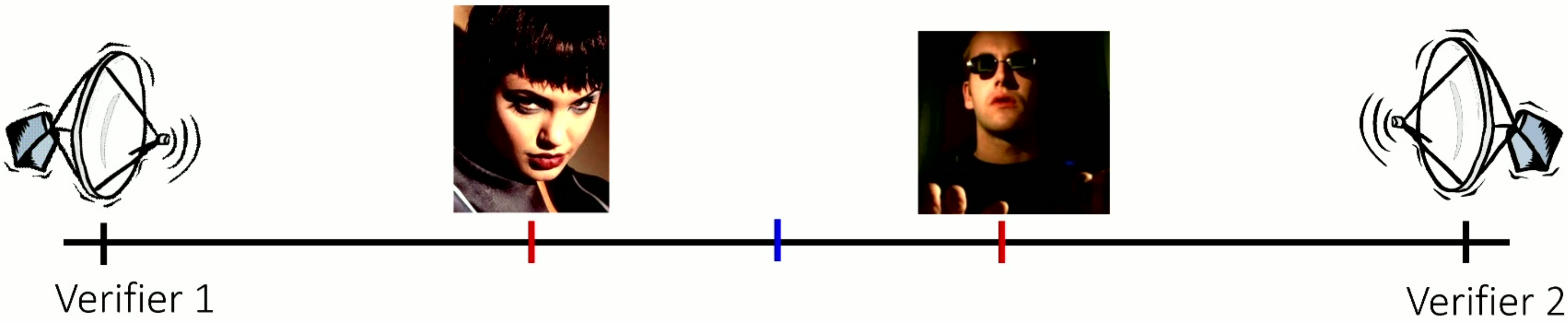
- Introducing QPV + INQC
- Warm-up: Clifford group protocol
- INQC for circuits with low T count
- The garden-hose model
- INQC for circuits with low T depth

Position Verification

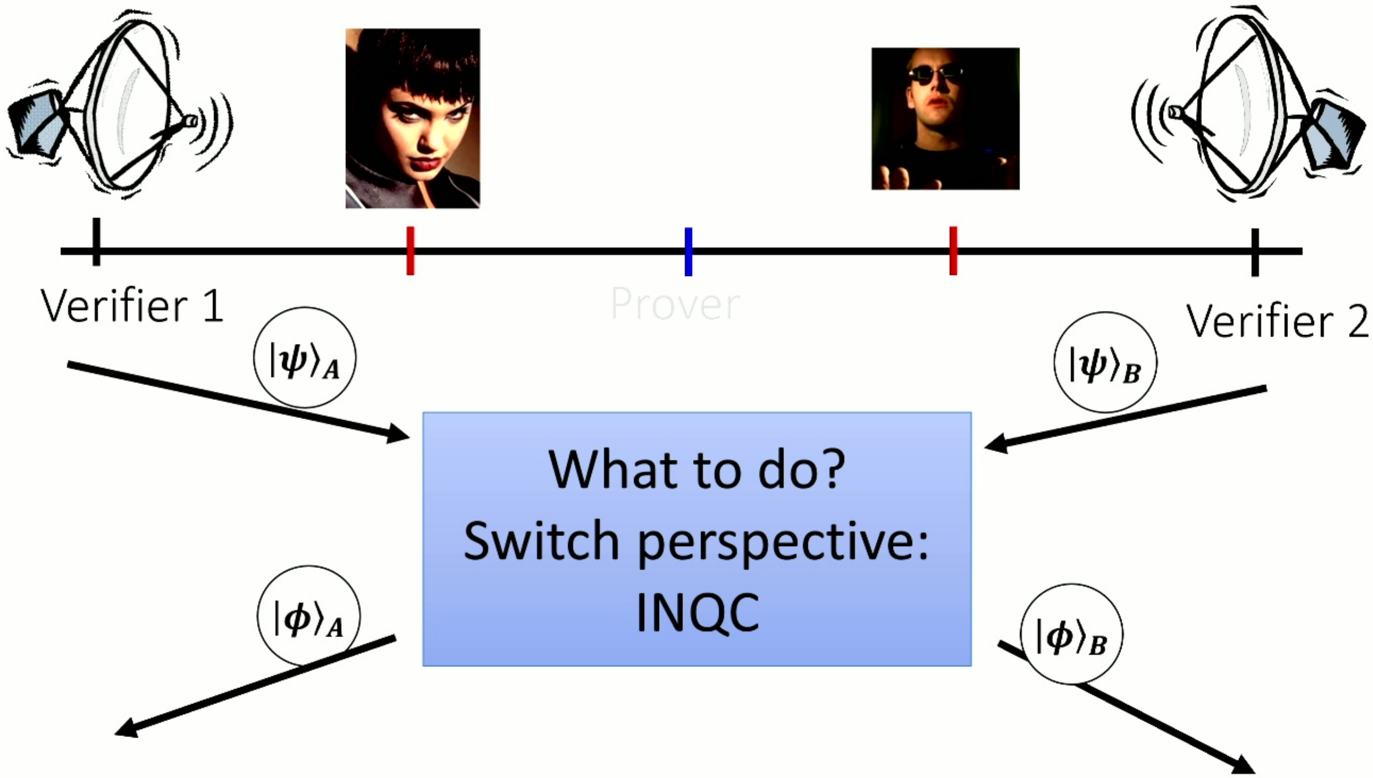


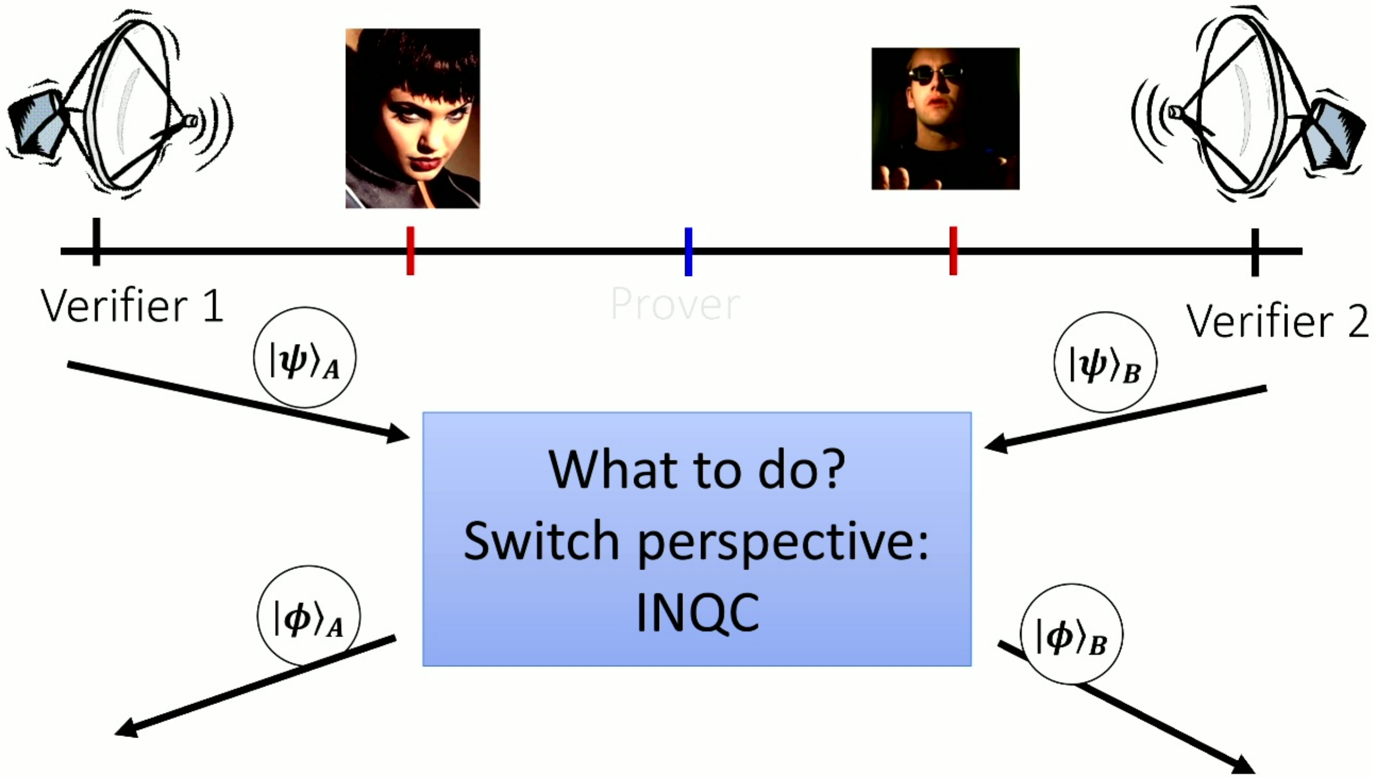
- Prover convince verifiers he is at a particular position
- Assumptions:
  - nothing faster than speed of light
  - **verifiers can coordinate**
  - disregard local computation time (for now)

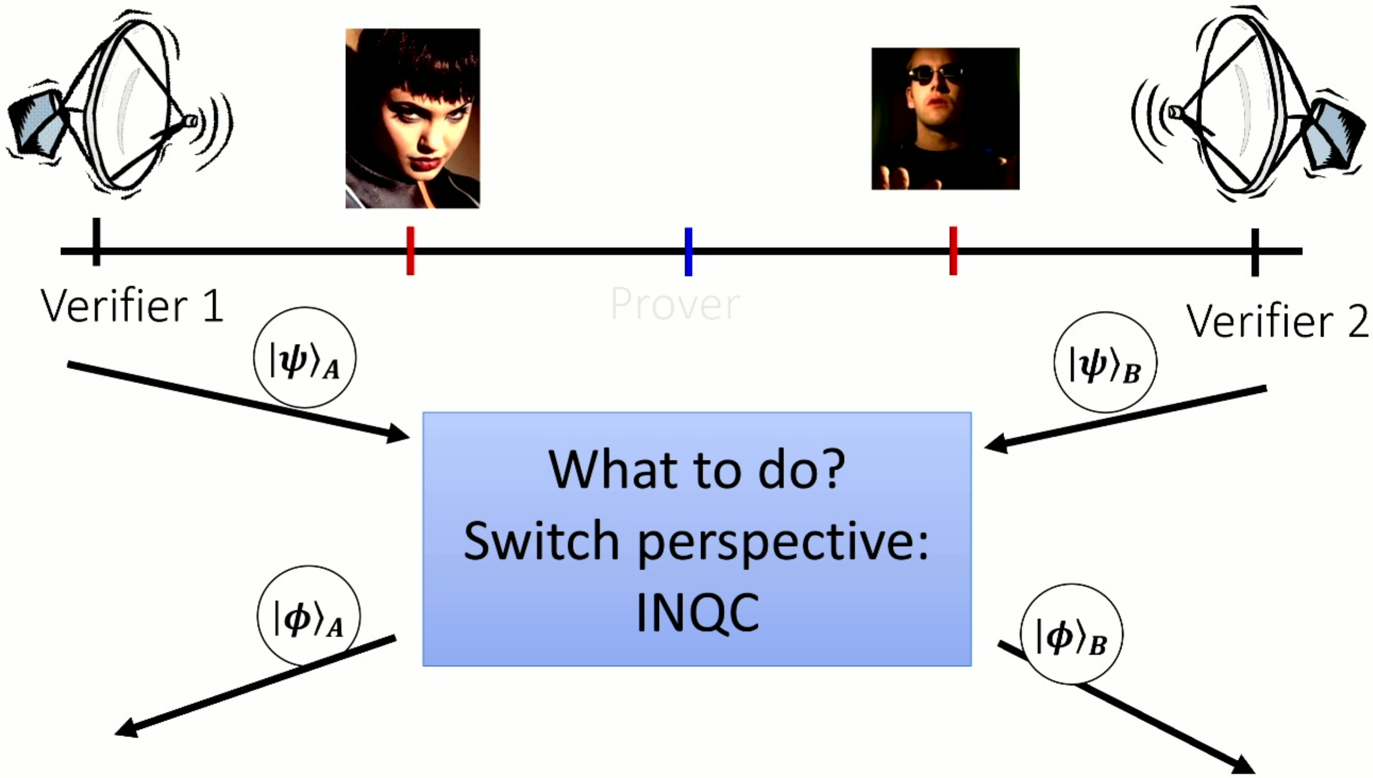
Position Verification



- Prover convince verifiers he is at a particular position
- Assumptions:
  - nothing faster than speed of light
  - **verifiers can coordinate**
  - disregard local computation time (for now)
- attackers are a coalition of (fake) provers

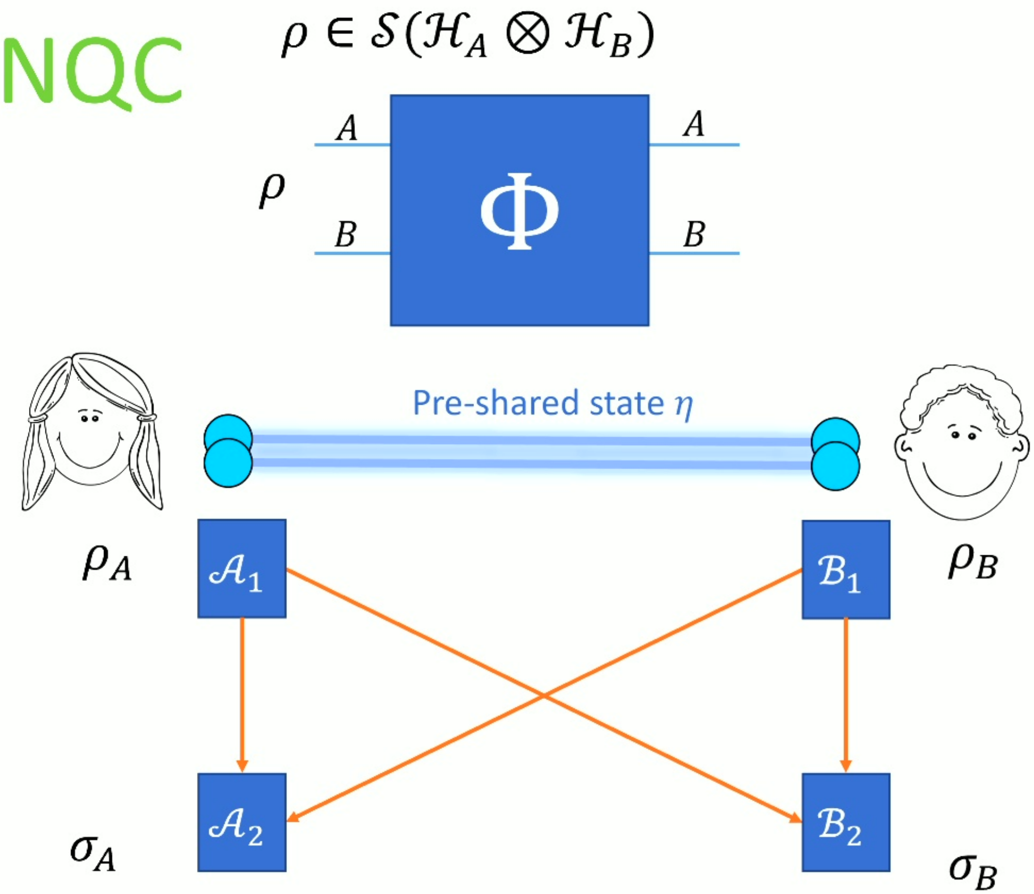

Verifier 1
Prover
Verifier 2
$|\psi\rangle_A$
$|\psi\rangle_B$
What to do?
Switch perspective:
INQC
$|\phi\rangle_A$
$|\phi\rangle_B$


Verifier 1
Prover
Verifier 2
$|\psi\rangle_A$
$|\psi\rangle_B$
What to do?
Switch perspective:
INQC
$|\phi\rangle_A$
$|\phi\rangle_B$



Verifiers check that they received
the correct quantum state in time

INQC



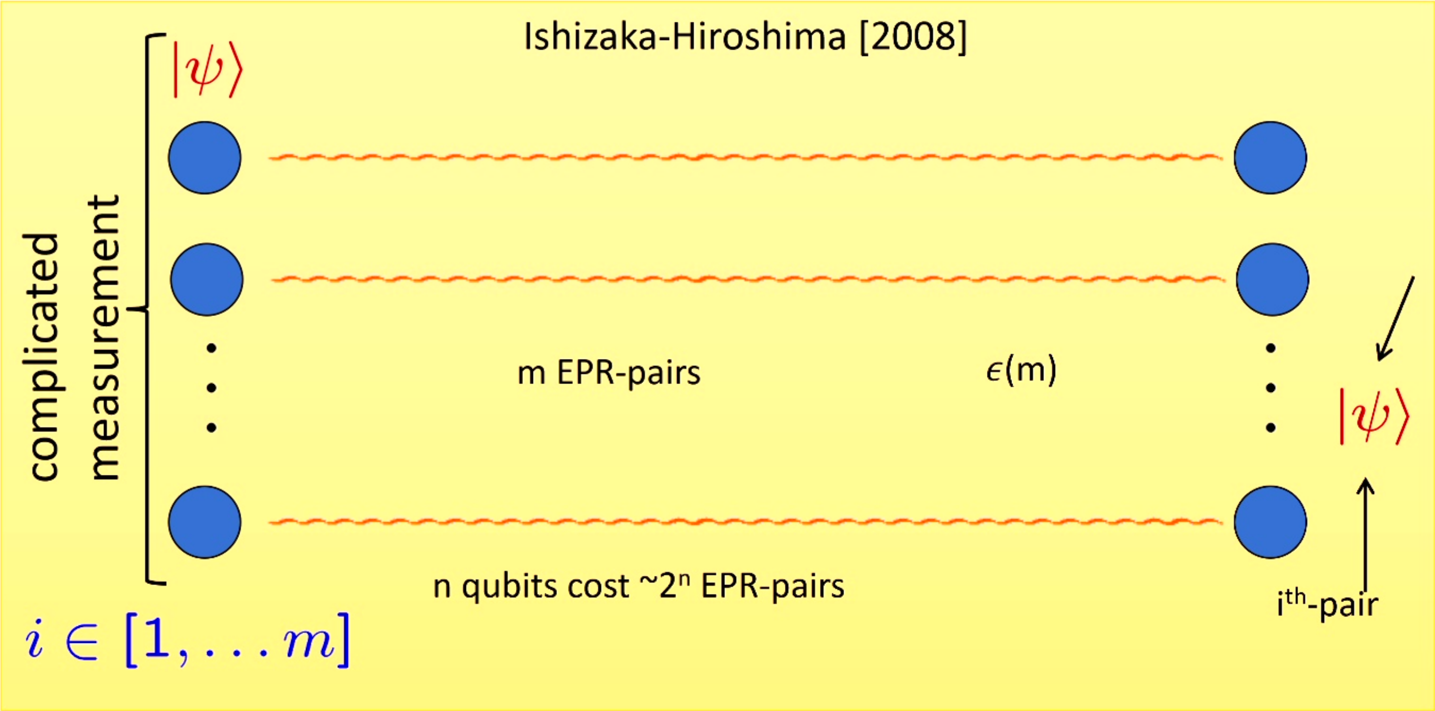
Alice and Bob perform an operation
with only a single round of simultaneous communication

$$\sigma = \Phi(\rho)$$

Good protocol means:
$$\|\Phi(\cdot) - (\mathcal{A}_2 \otimes \mathcal{B}_2)(\mathcal{A}_1 \otimes \mathcal{B}_1)(\cdot \otimes \eta)\|_\diamond \le \epsilon$$

General protocol: port-based teleportation

- Harry's Monday talk
- [Beigi König 2011] $O(n\frac{2^{8n}}{\epsilon^2})$ EPR pairs



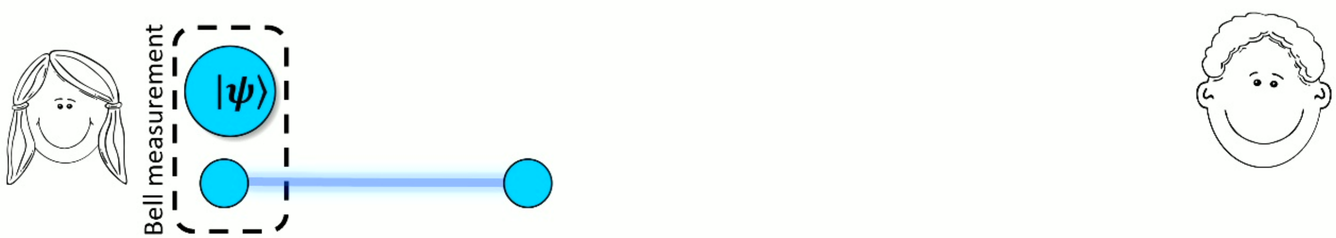
- But what if we want to do a simpler operation?

Teleportation

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

EPR pair: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Teleportation transfers quantum information using classical bits + EPR pair



The Clifford group

- Generated by $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

- Commutation maps Pauli operators to Paulis (normalizer of Pauli group)
  e.g. $HX = ZH$, $PZ = ZP$, $PX = XZP$

Interaction with teleportation corrections:

The Clifford group

- Generated by $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

- Commutation maps Pauli operators to Paulis (normalizer of Pauli group)
  e.g. $HX = ZH,$ $PZ = ZP,\ PX = XZP$

Interaction with teleportation corrections:

$$PX^aZ^b = X^aZ^{a\oplus b}P$$
$$HX^aZ^b = X^bZ^aH$$
$$CNOT X^{a_1}Z^{b_1}X^{a_2}Z^{b_2} = X^{a_1}Z^{b_1+b_2}X^{a_1+a_2}Z^{b_2}CNOT$$

The Clifford group

- Generated by $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, $P = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$, $CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$

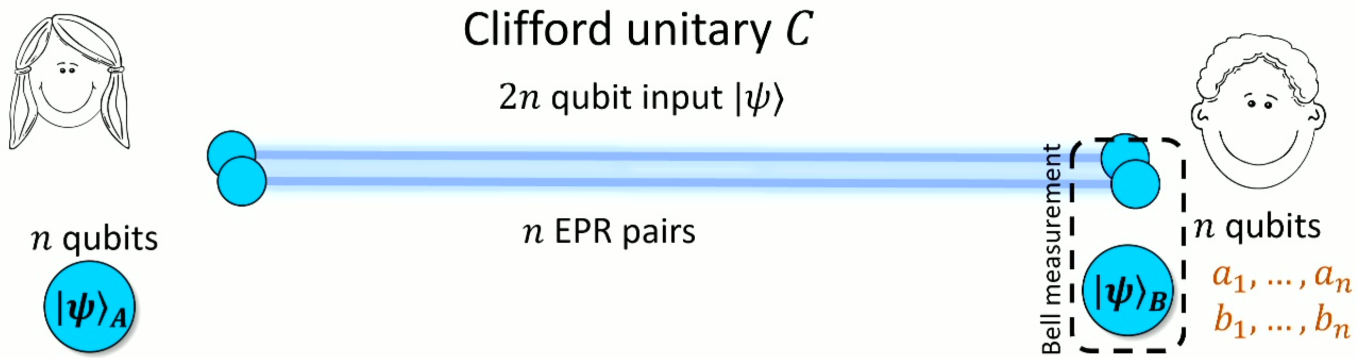
- Commutation maps Pauli operators to Paulis (normalizer of Pauli group)
  e.g. $HX = ZH,$ $PZ = ZP,\ PX = XZP$

Interaction with teleportation corrections:

$$PX^aZ^b = X^aZ^{a\oplus b}P$$
$$HX^aZ^b = X^bZ^aH$$
$$CNOT X^{a_1}Z^{b_1}X^{a_2}Z^{b_2} = X^{a_1}Z^{b_1+b_2}X^{a_1+a_2}Z^{b_2}CNOT$$

- Not a universal gate set
  Classical simulation possible

Warmup: clifford group protocol



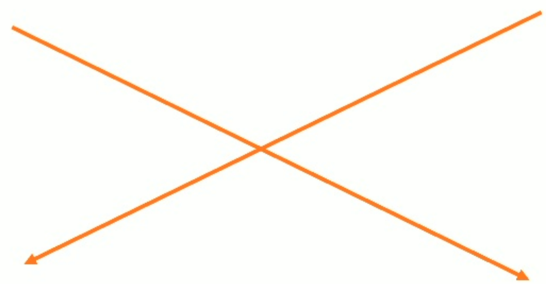
$I^{\otimes n} \otimes X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} |\psi\rangle$

U

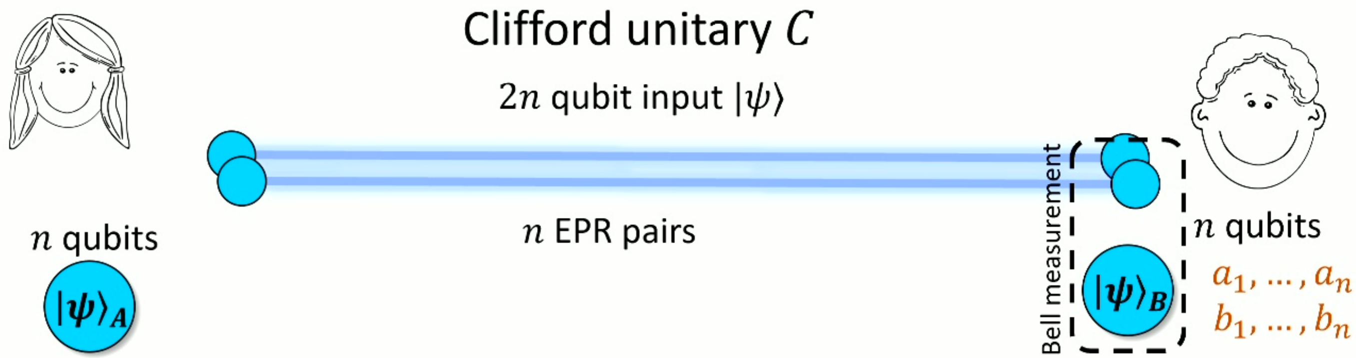
$$C\left(I^{\otimes n} \otimes X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}\right)|\psi\rangle = \left(X^{c_1} Z^{d_1} \otimes \cdots \otimes X^{c_{2n}} Z^{d_{2n}}\right) C |\psi\rangle$$

Send Bob's n qubits back

Send $c_1, \ldots, c_n, d_1, \ldots, d_n$



Warmup: clifford group protocol



$I^{\otimes n} \otimes X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} |\psi\rangle$

U

$C\left(I^{\otimes n} \otimes X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}\right)|\psi\rangle =$
$\left(X^{c_1} Z^{d_1} \otimes \cdots \otimes X^{c_{2n}} Z^{d_{2n}}\right) C |\psi\rangle$

Send Bob's n qubits back

Send $c_1, \dots, c_n, d_1, \dots, d_n$

Locally apply
$X^{c_1} Z^{d_1} \otimes \cdots X^{c_n} Z^{d_n}$

Locally apply
$X^{c_{n+1}} Z^{d_{n+1}} \otimes \cdots X^{c_{2n}} Z^{d_{2n}}$

Extending the gate set: T gate

T gate (also known as $\frac{\pi}{8}$ gate) is given by $\mathrm{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Clifford+T can perform all quantum operations (universal set)

T gate on an uncorrected qubit:

$$TX = PXT$$
$$TZ = ZT$$

$$TX^aZ^b|\psi\rangle = P^aX^aZ^bT|\psi\rangle$$

Extending the gate set: T gate

T gate (also known as $\frac{\pi}{8}$ gate) is given by $\mathrm{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Clifford+T can perform all quantum operations (universal set)

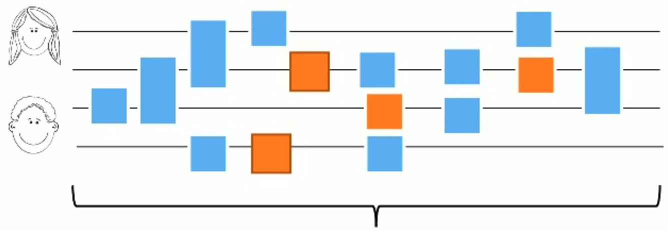
T gate on an uncorrected qubit:

$$TX = PXT$$
$$TZ = ZT$$

$$TX^aZ^b|\psi\rangle = P^aX^aZ^bT|\psi\rangle$$

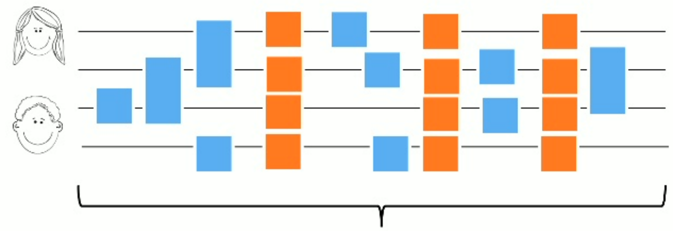
Handle the unwanted P gate in some way

Overview of results



T-count k

Entanglement $O(n2^k)$

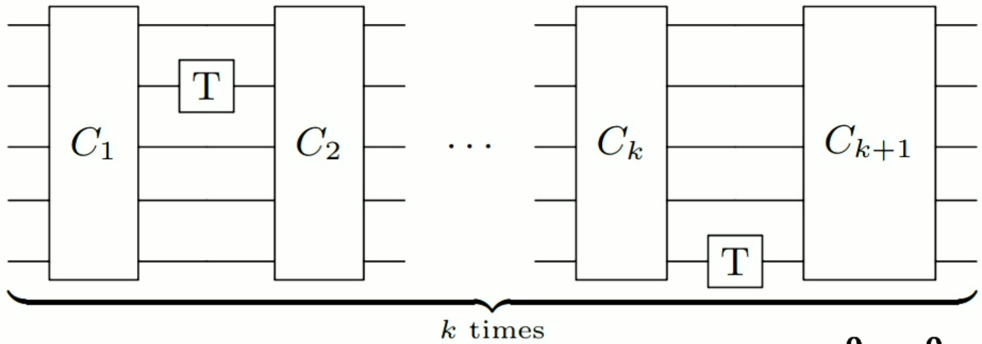


T-depth d

Entanglement $O(n^d)$

(No error, exactly simulates the circuit)

Also see: Monday's talk by Anne ➔ with PR-boxes we can do INQC of all poly-size circuits efficiently



Step 0: Bob teleports his $n/2$ qubits to Alice, holds $\mathrm{X}^{\boldsymbol{b_x^0}}\mathrm{Z}^{\boldsymbol{b_z^0}}|\psi_0\rangle$

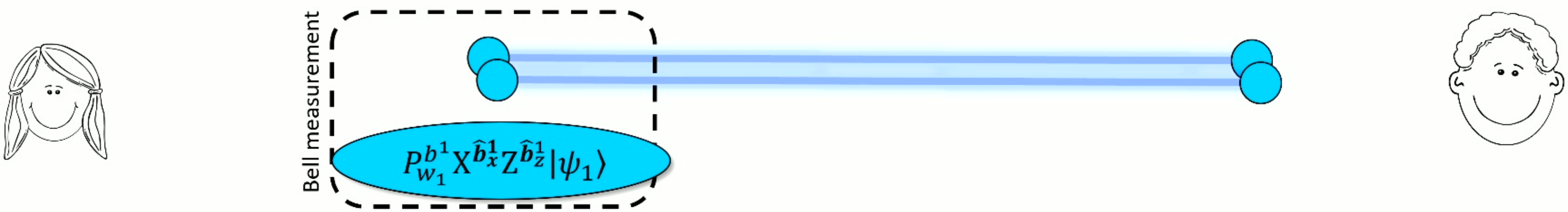
Step 1.a: Alice performs $C_1\mathrm{X}^{\boldsymbol{b_x^0}}\mathrm{Z}^{\boldsymbol{b_z^0}}|\psi_0\rangle = \mathrm{X}^{\widehat{\boldsymbol{b}}_x^{\boldsymbol{1}}}\mathrm{Z}^{\widehat{\boldsymbol{b}}_z^1}C_1|\psi_0\rangle$

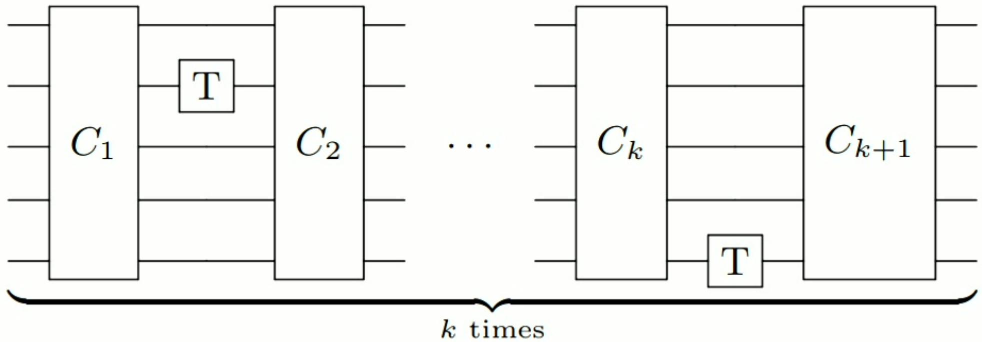
Step 1.b: Alice performs T on some wire w_1

$$\mathrm{T}_{w_1}\mathrm{X}^{\widehat{\boldsymbol{b}}_x^{\boldsymbol{1}}}\mathrm{Z}^{\widehat{\boldsymbol{b}}_z^1}C_1|\psi_0\rangle = P_{w_1}^{b^1}\mathrm{X}^{\widehat{\boldsymbol{b}}_x^{\boldsymbol{1}}}\mathrm{Z}^{\widehat{\boldsymbol{b}}_z^1}TC_1|\psi_0\rangle := P_{w_1}^{b^1}\mathrm{X}^{\widehat{\boldsymbol{b}}_x^{\boldsymbol{1}}}\mathrm{Z}^{\widehat{\boldsymbol{b}}_z^1}|\psi_1\rangle$$

with b^1 the w_1 entry of $\widehat{\boldsymbol{b}}_{\boldsymbol{x}}^{\boldsymbol{1}}$

Step 1.c: Alice teleports all qubits to Bob





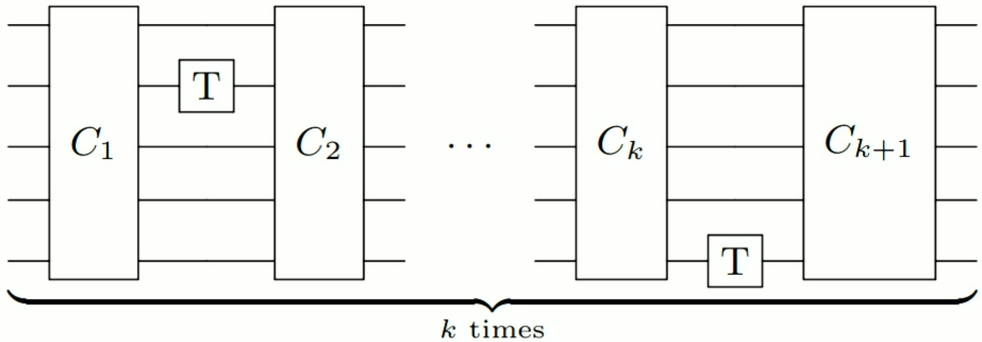
Step 1.d: Bob undoes old Paulis and applies $\left(P_{w_1}^{b^1}\right)^{-1}$

$$\left(P_{w_1}^{b^1}\right)^{-1} \mathrm{X}^{\boldsymbol{a_x^1}} \mathrm{Z}^{\boldsymbol{a_z^1}} P_{w_1}^{b^1} |\psi_1\rangle = \mathrm{Z}_{w_1}^{a^1 b^1} \mathrm{X}^{\boldsymbol{a_x^1}} \mathrm{Z}^{\boldsymbol{a_z^1}} |\psi_1\rangle$$

$\mathrm{Z}_{w_1}^{a^1}$

Step 1.e: Alice corrects extra Z if needed. Now one of the groups is back to starting invariant!

➔ Alice holds the qubits and Bob the teleportation corrections

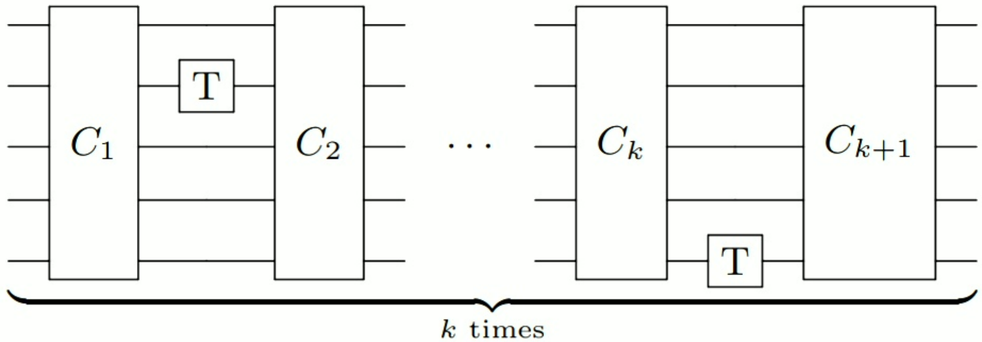


Step 1.d: Bob undoes old Paulis and applies $\left(P_{w_1}^{b^1}\right)^{-1}$

$$\left(P_{w_1}^{b^1}\right)^{-1} \mathrm{X}^{a_x^1} \mathrm{Z}^{a_z^1} P_{w_1}^{b^1} |\psi_1\rangle = \mathrm{Z}_{w_1}^{a^1 b^1} \mathrm{X}^{a_x^1} \mathrm{Z}^{a_z^1} |\psi_1\rangle$$

Step 1.e: Alice corrects extra Z if needed. Now one of the groups is back to starting invariant!

➔ Alice holds the qubits and Bob the teleportation corrections

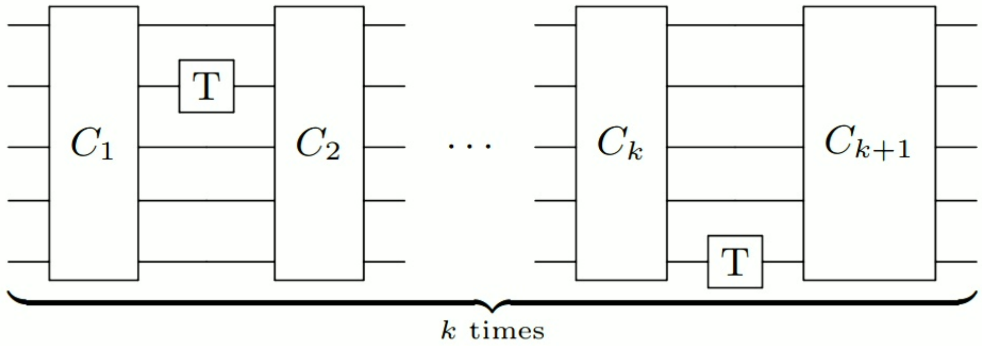


Step 1.d: Bob undoes old Paulis and applies $\left(P_{w_1}^{b^1}\right)^{-1}$

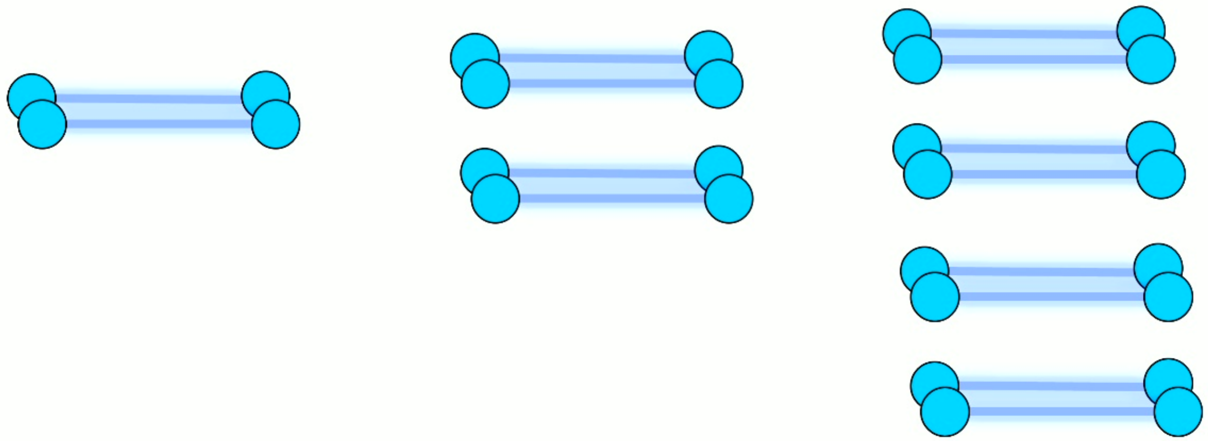
$$\left(P_{w_1}^{b^1}\right)^{-1} X^{\boldsymbol{a}_x^1} Z^{\boldsymbol{a}_z^1} P_{w_1}^{b^1} |\psi_1\rangle = Z_{w_1}^{a^1 b^1} X^{\boldsymbol{a}_x^1} Z^{\boldsymbol{a}_z^1} |\psi_1\rangle$$

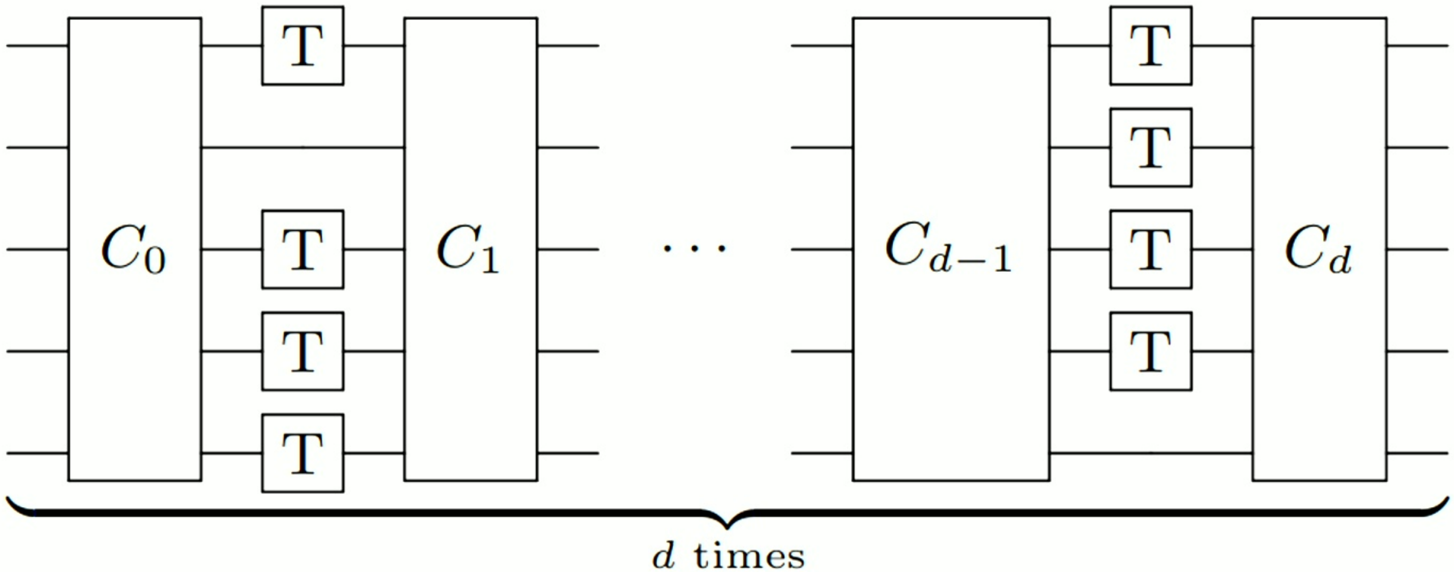
Step 1.e: Alice corrects extra Z if needed. Now one of the groups is back to starting invariant!

➔ Alice holds the qubits and Bob the teleportation corrections



Step i: same as step 1, but Alice acts on all 2^{i-1} groups in parallel!





T-depth d

INQC with entanglement $O(n^d)$

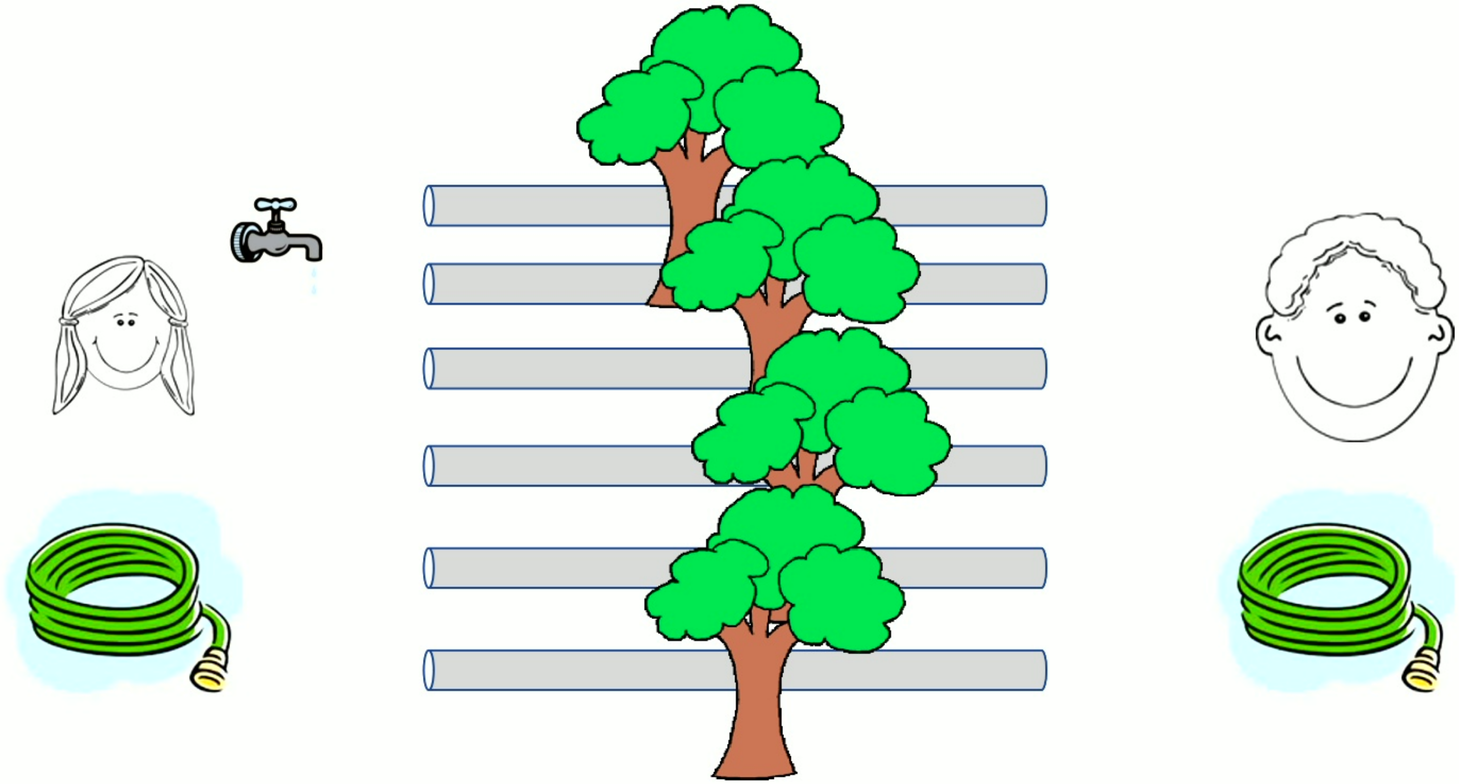
Main Lemma

$P^{f(x,y)}|\psi\rangle, x$ $\qquad\qquad$ y

$X^{g(x',y')}Z^{h(x',y')}|\psi\rangle, x'$ $\qquad\qquad$ y'

Consumes ebit dependent on garden-hose complexity of f
Garden-hose complexity of g, h is **linear** in garden-hose complexity of f

The Garden-Hose Model



share s waterpipes

The Garden-Hose Model

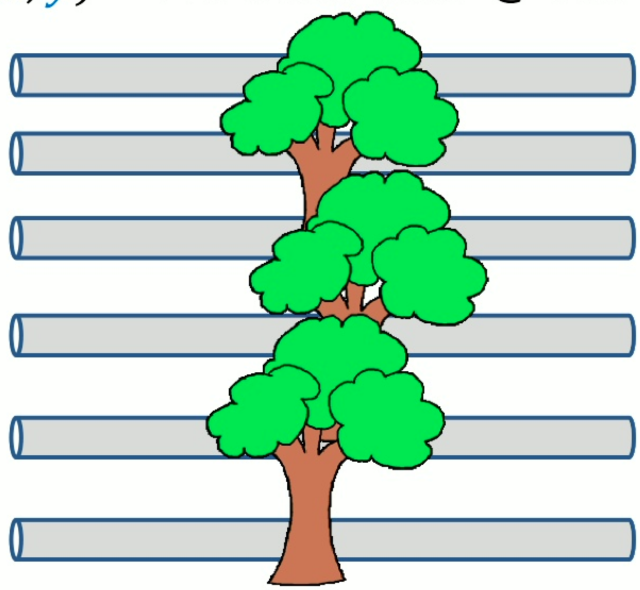
$$f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$

$f(x, y) = 0$ if water exits @ Alice

$f(x, y) = 1$ if water exits @ Bob

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$



- based on their inputs, players connect pipes with pieces of hose
- Alice also connects a water tap

The Garden-Hose Model

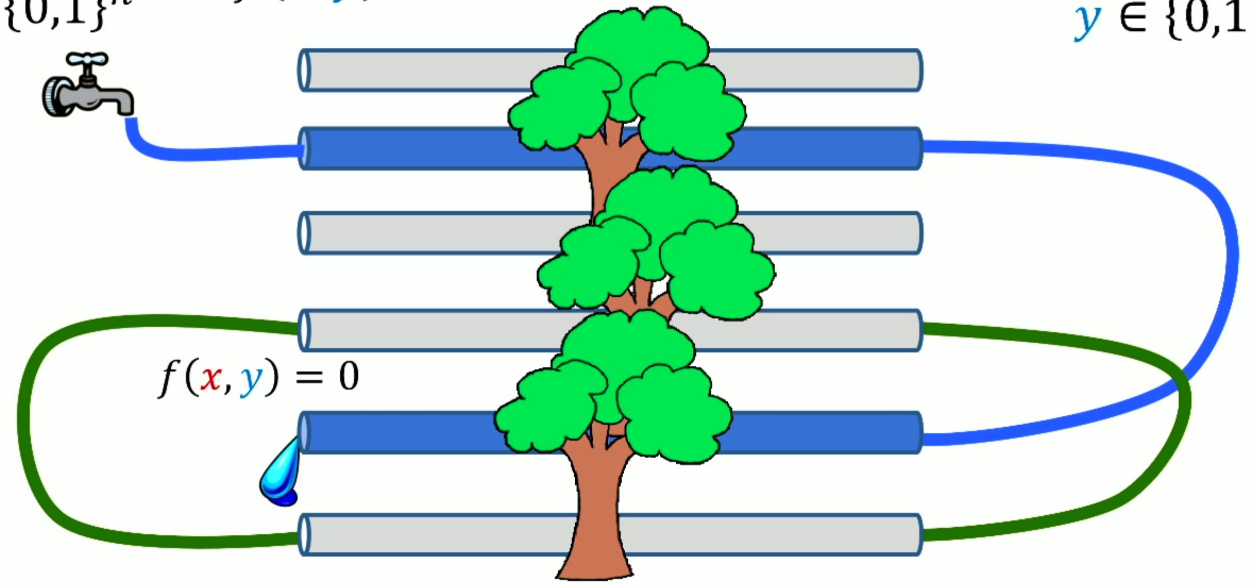
$$f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$

$f(x, y) = 0$ if water exits @ Alice

$f(x, y) = 1$ if water exits @ Bob

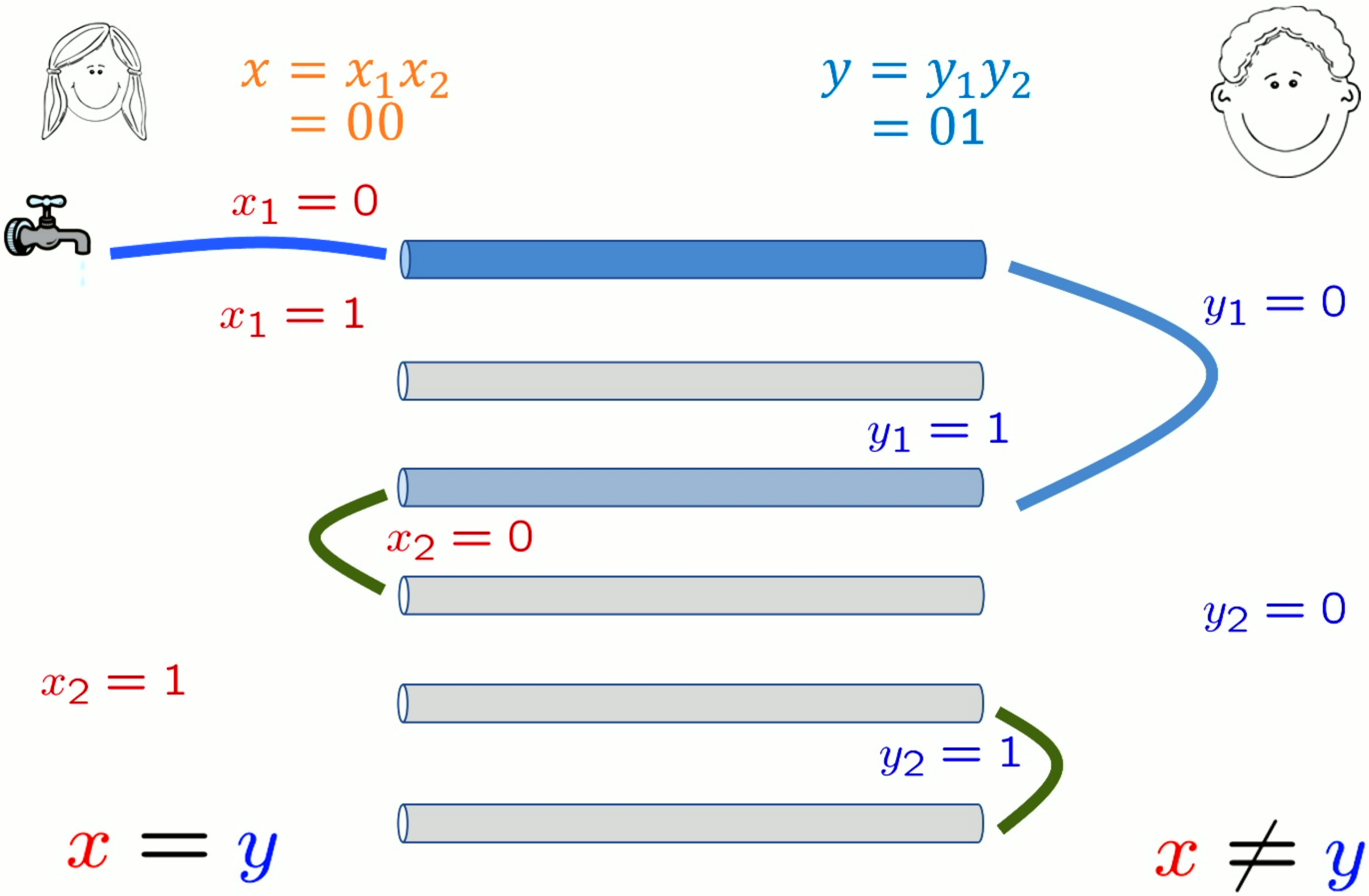
$x \in \{0,1\}^n$

$y \in \{0,1\}^n$



- based on their inputs, players connect pipes with pieces of hose
- Alice also connects a water tap

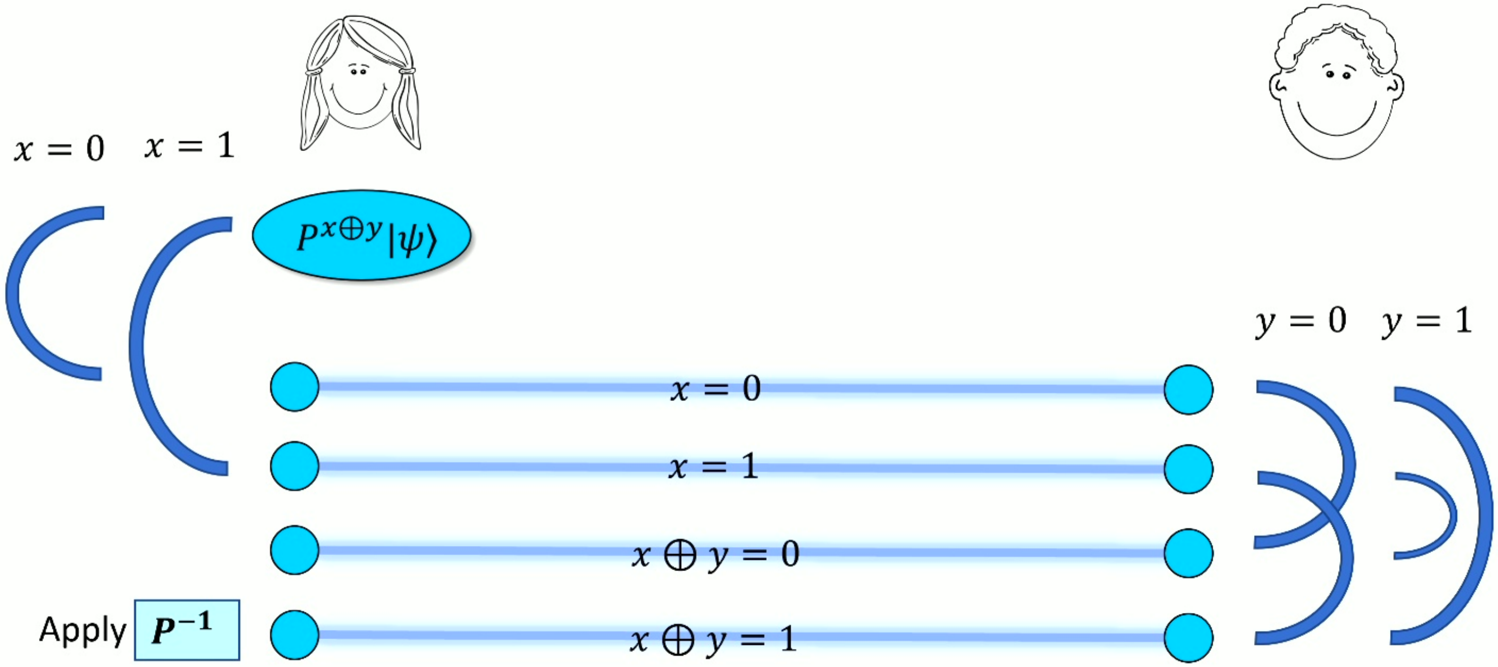
Example: Inequality on Two Bits



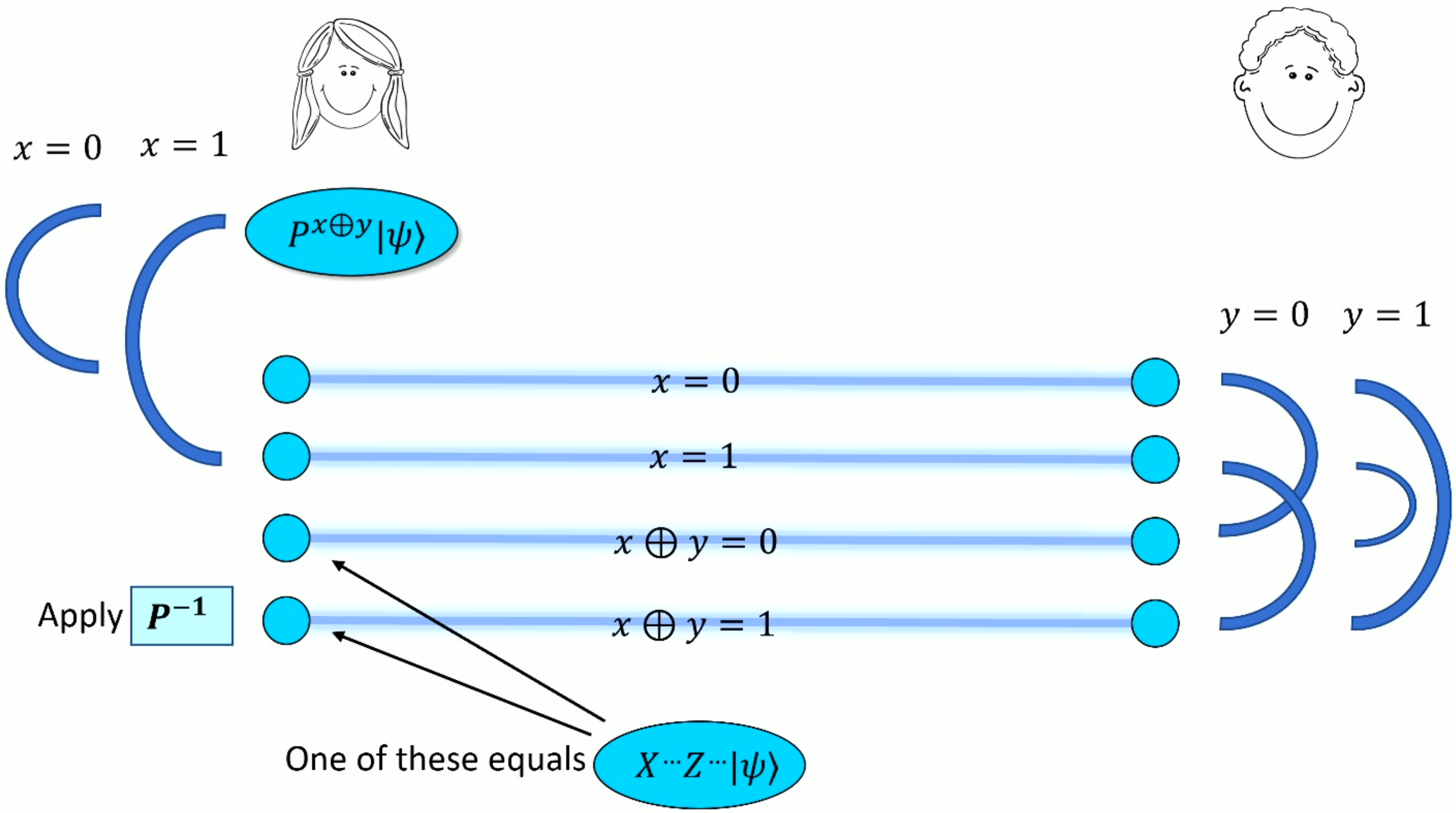
Some facts about Garden-hose complexity

- Inspired by attacks on routing QPV protocol
- Every f has $GH(f) \leq$ exponential
- f in logspace $\Rightarrow GH(f)$ is polynomial
  - Using Barrington's theorem (see Harry's talk)
- exists f with $GH(f)$ exponential (counting)
- for $g \in \{\text{equality, IP, majority}\}$:
$$GH(g) \geq n/\log n$$
  - using techniques from communication complexity

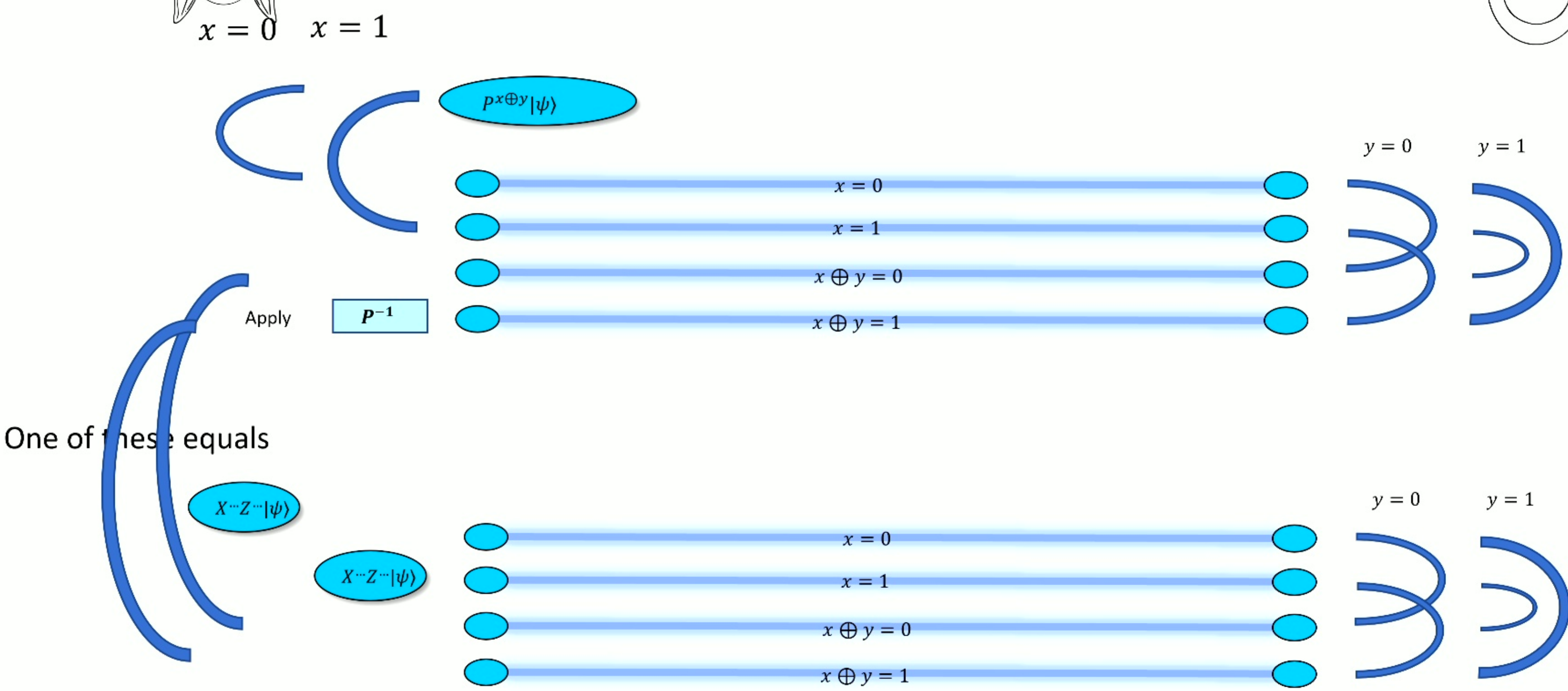
The garden-hose complexity describes how much entanglement we need to undo a correction. Example:



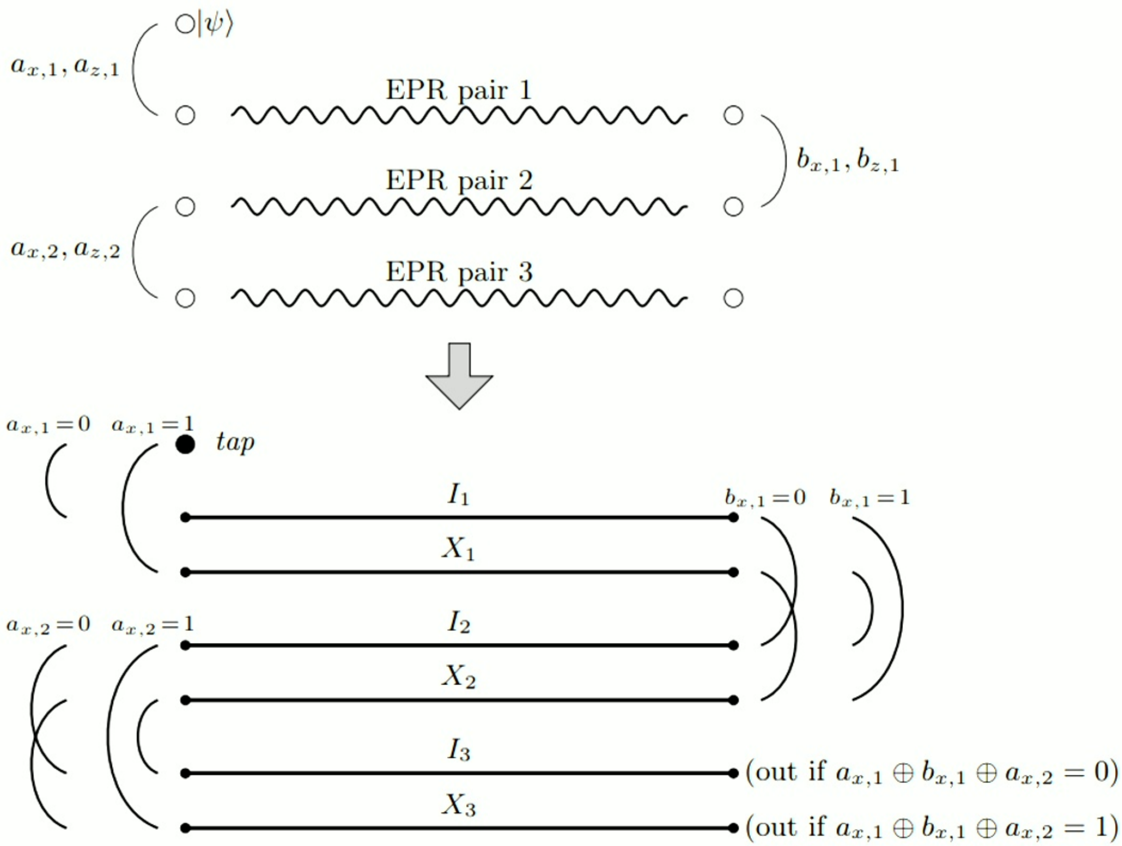
The garden-hose complexity describes how much entanglement we need to undo a correction. Example:



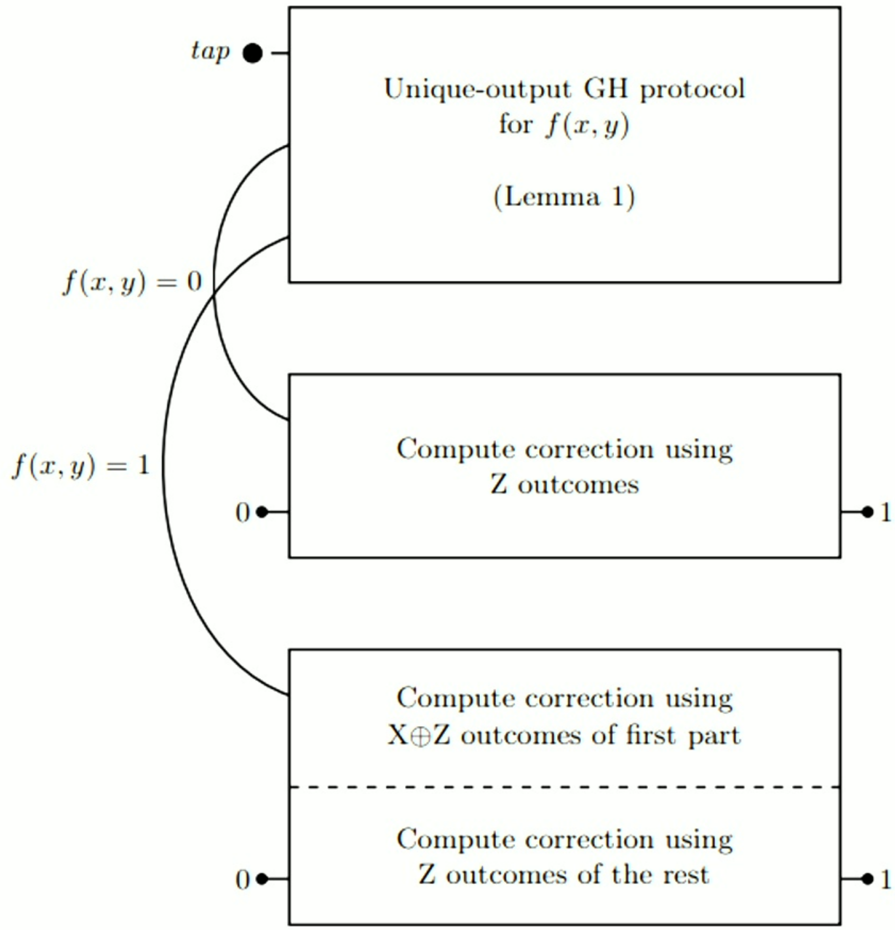
Observation 1: Previous attempt would lose track of qubit, but we can repeat the protocol in reverse to find it again



Observation 2: the garden-hose complexity of computing the Pauli corrections resulting from teleporting a qubit back-and-forth **k** times is linear in **k**.
"The garden-hose complexity of executing a garden-hose protocol of f linear in $\mathrm{GH}(f)$"



Correction to observation 2: The protocol is not just teleportations, but also involves some inverse phase gates if $f(x, y) = 1$ – what about the Z correction?



Lemma proof

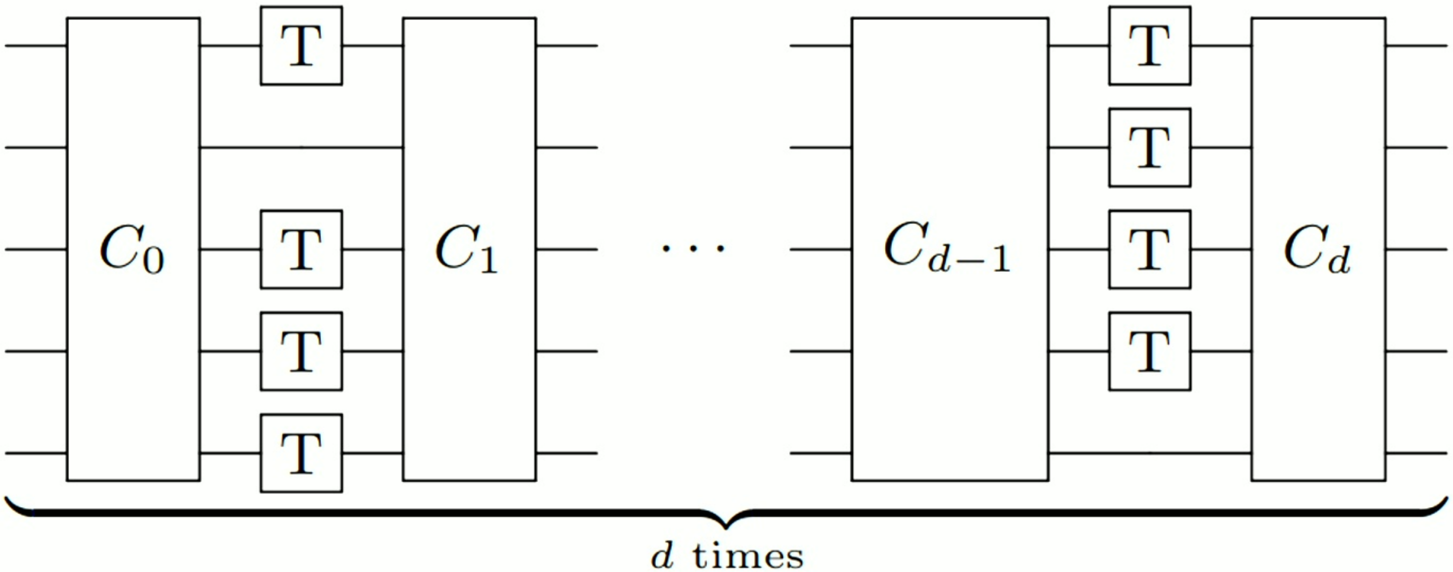
Alice starts with $P^{f(x,y)}|\psi\rangle$, x

Bob starts with y

- By **observation 1**: Alice and Bob perform the protocol to undo P, using $2\mathrm{GH}(f)$ EPR pairs

$X^{g(x',y')}Z^{h(x',y')}|\psi\rangle$, x' y'

- By **observation 2:** $\mathrm{GH(g)} \leq 4\mathrm{GH}(f) + 1$, $\mathrm{GH(h)} \leq 11\mathrm{GH}(f) + 2$



T-depth d

INQC with entanglement $O(n^d)$

We now know how handle T gates, put it all together

Proof sketch (INQC for T-depth)

- Every step, Alice holds qubits of the form $\bigotimes_i X^{g_i(x,y)} Z^{h_i(x,y)} |\psi\rangle$ with x, y teleportation corrections of Alice, Bob
- Clifford step: permute and sum functions
  - GH becomes approx $\leq \sum_i GH(g_i) + GH(h_i)$

Proof sketch (INQC for T-depth)

- Every step, Alice holds qubits of the form $\bigotimes_i X^{g_i(x,y)} Z^{h_i(x,y)} |\psi\rangle$ with x, y teleportation corrections of Alice, Bob
- Clifford step: permute and sum functions
  - GH becomes approx $\leq \sum_i GH(g_i) + GH(h_i)$
- T layer step:
  - For each qubit, $GH(g'_i) \leq 4GH(g_i') + 1$ and $GH(h'_i) \leq 11GH(h_i') + 2$

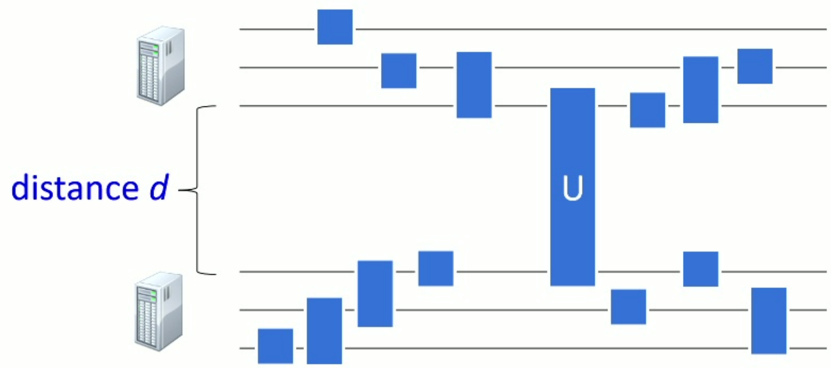
- Together (with some extras): complexity $(68n)^d$

INQC overview

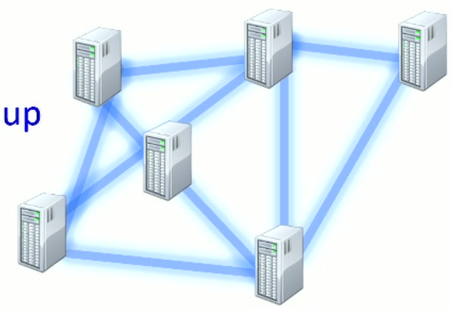
Circuit type	Result
General circuits	[Vaidman 2003, BCFGGOS 2011] $2^{\log(\frac{1}{\epsilon})}\ 2^{O(n)}$ EPR pairs [Beigi König 2011] $O(n\frac{2^{8n}}{\epsilon^2})$ EPR pairs
Two qubit circuits	[Gonzales Chitambar 2019] $8\log(\frac{1}{\epsilon}) + 22$
Clifford + T-count k	$O(n2^k)$ [Broadbent 2016] $O(n+k)$ with PR boxes *(Monday talk)*
Clifford + T-count d	$O((68n)^d)$
Small light-cone circuits	[Dolev Cree 2022]

Bonus application: distributed computing

- Quantum computation over spatially separated locations
- Normally executing U takes time 2*d*
  (send relevant qubit back and forth)
- Improved to time *d*, since we can make the communication simultaneous
- Trade entanglement for time
- Faster intelligent routing



More room for speed up with more parties / repeaters?



Bonus application: Homomorphic encryption

Classical case

Encrypt data so that another party can perform calculations on the encrypted data

Many applications

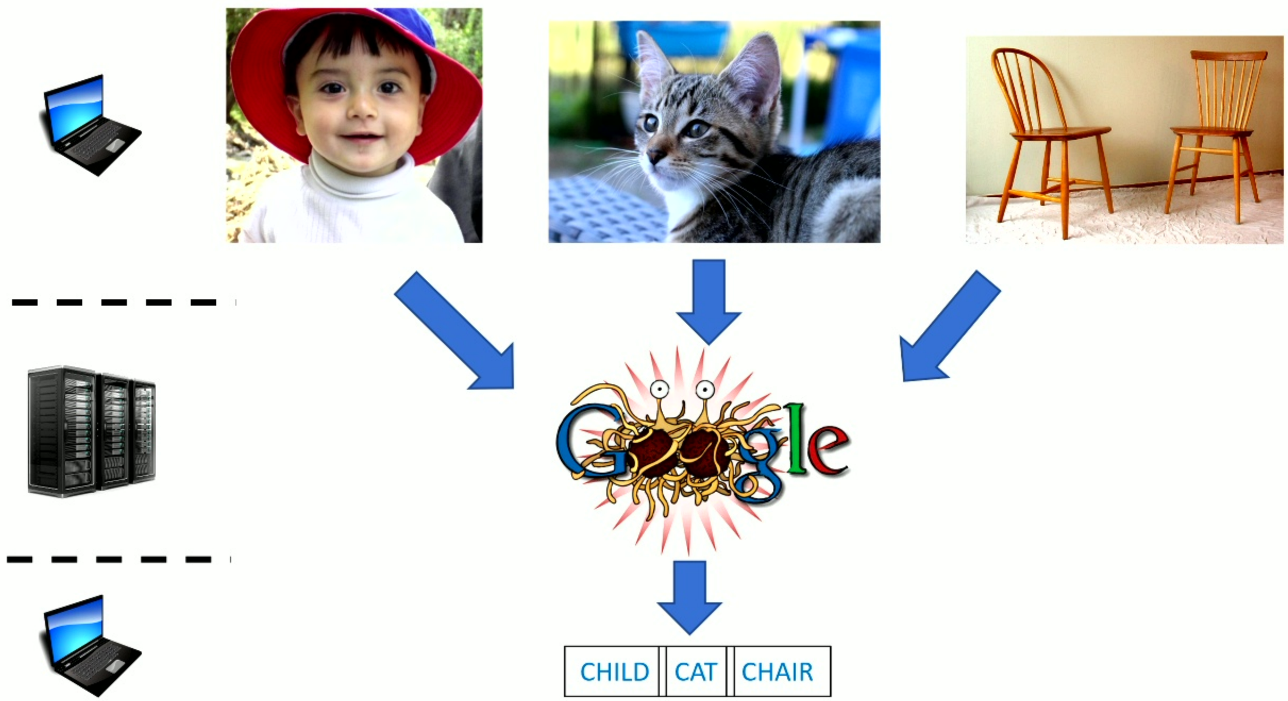
CHILD

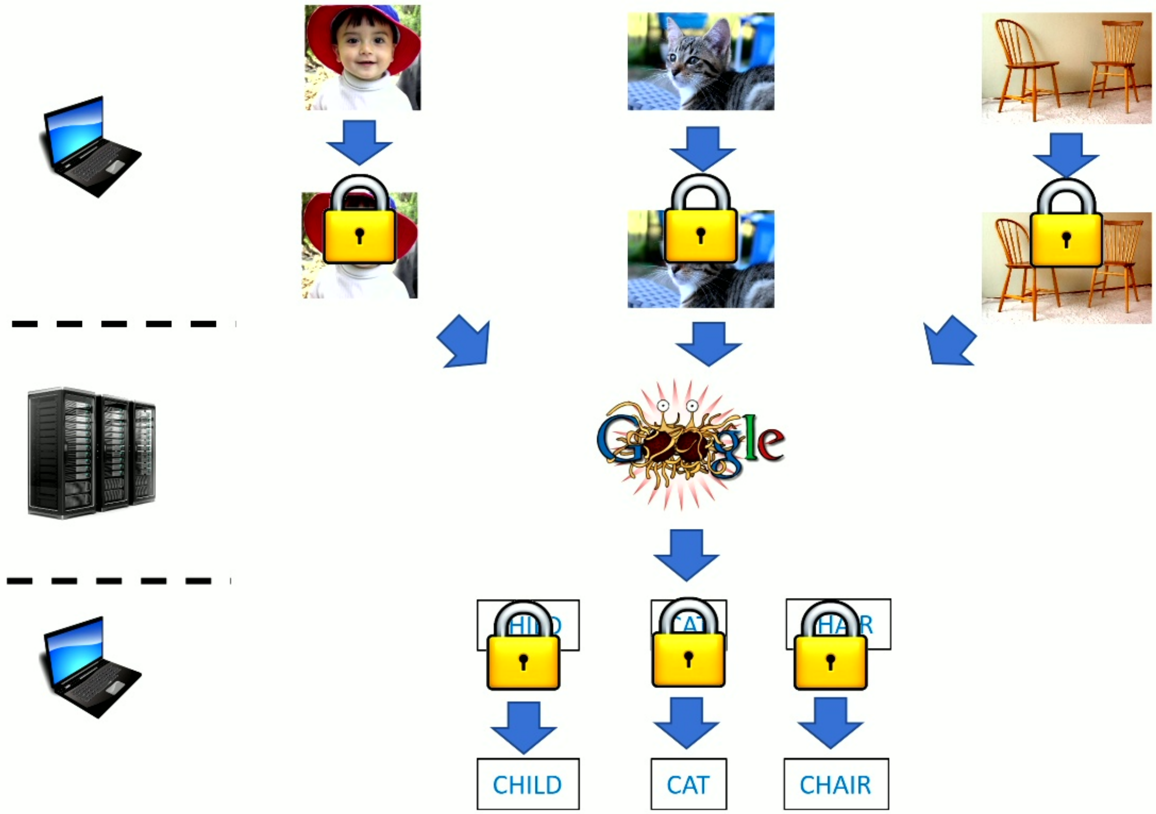
CAT

CHAIR

Tagging

Google DeepMind


CHILD
CAT
CHAIR

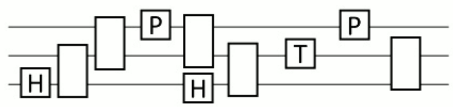

CHILD
CAT
CHAIR

Quantum Homomorphic Encryption

Encrypt *quantum state*, instead of classical data

$$\rho \to \mathrm{QEnc}(\rho)$$

Execute *quantum circuit* on encrypted data



Quantum one-time pad ↔ uncorrected quantum teleportation
We can use the main lemma as a starting point
[DSS 2016]

Open questions (many)

- What about other circuit classes?
  - Fermions / match gates, CV, qudits…
- New tricks such as code-routing [Cree May 2023] better than garden-hose model?

Open questions (many)

- What about other circuit classes?
  - Fermions / match gates, CV, qudits…
- New tricks such as code-routing [Cree May 2023] better than garden-hose model?
- Resource-bounded version with more parties? Extending [Dolev 2019]
- Optimal error-dependence for INQC? Most protocols grow $\frac{1}{\epsilon^c}$, is this fundamental? Exception: [Gonzales Chitambar 2019]
- Lower bounds?

- (Details:) $(68n)^d$ is clearly not the right number. Proper gate teleportation easy way to reduce this.

Open questions (many)

- What about other circuit classes?
  - Fermions / match gates, CV, qudits…
- New tricks such as code-routing [Cree May 2023] better than garden-hose model?
- Resource-bounded version with more parties? Extending [Dolev 2019]
- Optimal error-dependence for INQC? Most protocols grow $\frac{1}{\epsilon^c}$, is this fundamental? Exception: [Gonzales Chitambar 2019]
- Lower bounds?