

Verification of quantum computation

Alex Bredariol Grilo



<https://abgrilo.github.io/viasm.html>



A bit of complexity theory

Decision problems

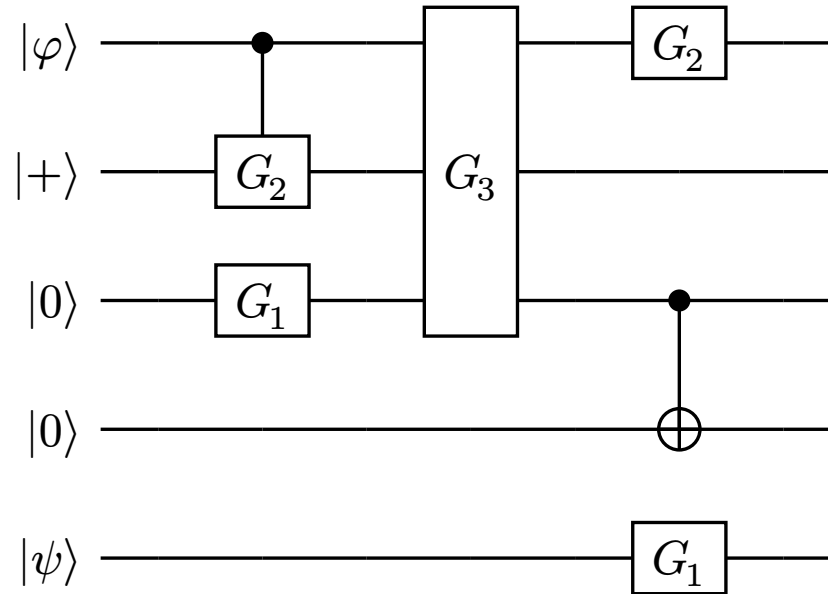
Promise problem: $L_{\text{yes}}, L_{\text{no}} \subseteq \{0, 1\}^*$ such that $L_{\text{yes}} \cap L_{\text{no}} = \emptyset$

Example

- Is n a prime?
- Does a graph G have a Hamiltonian cycle?
- Does n have a prime factor between ℓ and u ?

Quantum circuits

1. Fix a gateset $\mathcal{G} = \{G_1, G_2, \dots\}$ (usually on a constant number of qubits)
2. Fix the number of qubits
3. Compose gates from $\mathcal{G}$ on those qubits
4. Add measurements at the end

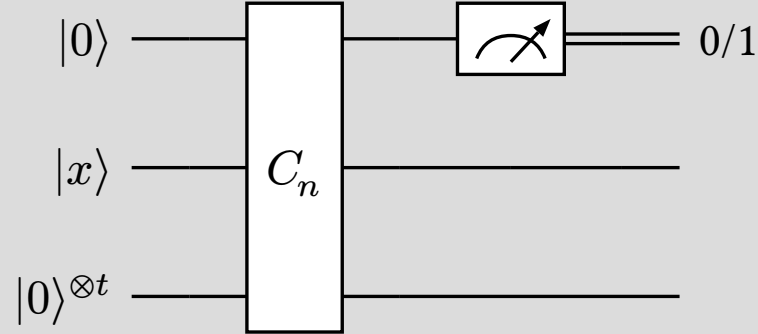


A circuit has a fixed number of input qubits

Quantum algorithms for decision problems

Family of circuit $\{C_n\}_{n \in \mathbb{N}}$

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



$C_n(x)$ - random variable of the measurement outcome after applying C_n on input x .

Which decision problems can be efficiently solved by quantum circuits?

Complexity class - BQP

Definition: A promise problem $L = (L_{\text{yes}}, L_{\text{no}})$ is BQP if there exists a family of circuits $\{C_n\}_{n \in \mathbb{N}}$ such that C_n is composed by at most $\text{poly}(n)$ gates and:

- If $x \in L_{\text{yes}}$, then $C_{|x|}(x) = 1$ with probability at least $\frac{2}{3}$
- If $x \in L_{\text{no}}$, then $C_{|x|}(x) = 1$ with probability at most $\frac{1}{3}$

Remark: The parameters $\frac{2}{3}/\frac{1}{3}$ can be amplified to $1 - \text{negl}(n)/\text{negl}(n)$, without loss of generality.

BQP vs. complexity classes

What we know:

- $\text{BPP} \subseteq \text{BQP} \subseteq \text{PSPACE}$

What we believe:

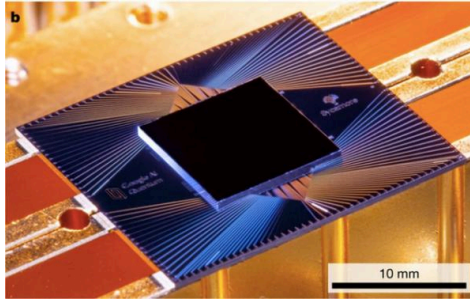
- $P \subseteq \text{BPP} \subsetneq \text{BQP}$
- $\text{NP} \not\subseteq \text{BQP}$
- $\text{BQP} \not\subseteq \text{NP}$

Interesting problems in BQP and not known to be in BPP:

- factoring
- discrete logarithm
- Hamiltonian simulation
- oracle problems (Simons's, Bernstein Vazirani)
- sampling problems (Forrelation)
- Quantum Machine Learning problems?

Quantum computers are expected to be more powerful than classical ones

Who will afford quantum computers?



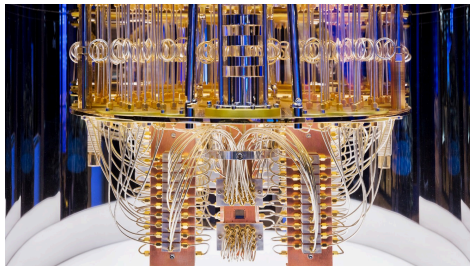
Quantum computers will likely be expensive
We won't have them everywhere

At least in the foreseeable future

How to run quantum computation?

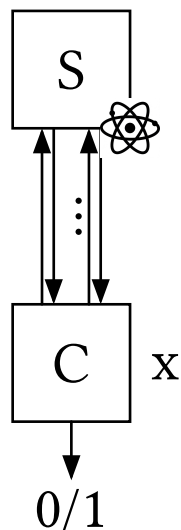
1. Send your input to a quantum server
2. Receive the answer
3. Use it for your applications

How can we trust the server's answer?



Delegation of quantum computation

Ideal solution



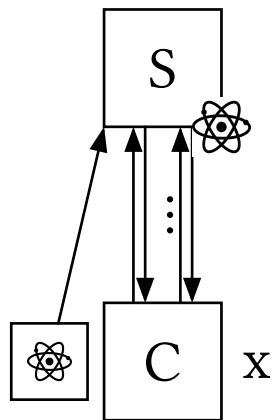
Goal: Interactive proof system

- the client runs poly-time classical computation
- the honest server runs poly-time quantum computation
- at the end of the protocol the client accepts or rejects
- **Correctness:**
If $x \in L_{\text{yes}}$, honest server makes the client accept whp
- **Security:**
If $x \in L_{\text{no}}$, client rejects whp even if server is malicious

Open question: Achieve a protocol with these properties

Let's consider more relaxed models

Relaxed models - almost classical client



Client is able to perform simple quantum operations

- Prepare and send one-qubit states, or
- Measure single qubits

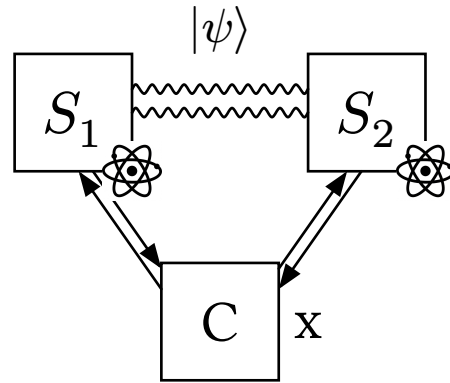
Pros

- Very efficient protocols
- Somewhat fault-tolerant
- Privacy of client's computation

Cons

- Client has trusted quantum devices
- Quantum communication

Relaxed models - multiple servers



Client delegates her computation to entangled servers

Pros

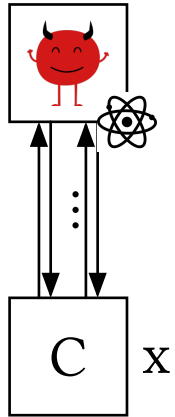
- Efficient protocols
- Only classical communication is needed
- Privacy of client's computation

Cons

- Entanglement requirement
- Terrible noise-resilience
- Only works for decision problems

Relaxed models - computational soundness

Security against bounded malicious servers



Pros

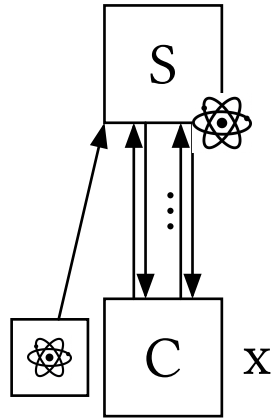
- One server
- Only classical communication is needed

Cons

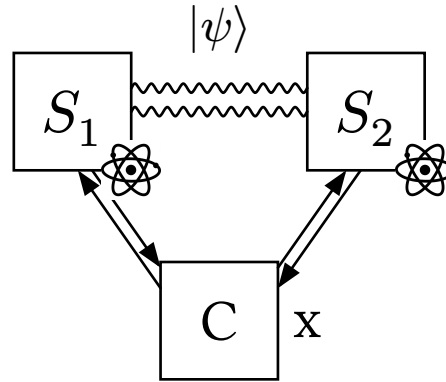
- Known protocols from LWE/FHE
- Computational security
- Huge overhead

Relaxed models - comparison

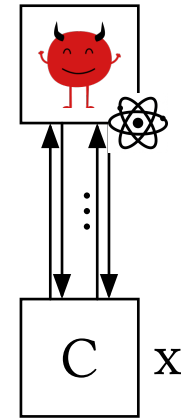
Almost classical



Multiple servers



Comp. soundness

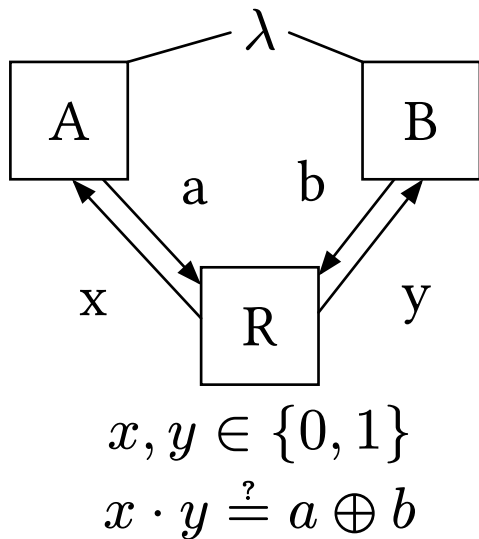


Goal of today's lecture:

1. Recipe from almost classical client to multiple servers
2. Recipe from multiple servers to computational soundness
3. A secure protocol for almost classical client

Recipe from almost classical client to multiple servers

CHSH game



1. A and B share a common strategy, and then they are not allowed to communicate anymore
2. R picks two random bits x, y
3. R sends x to A and y to B
4. A answers with a and B answers with b
5. A and B win if $x \cdot y = a \oplus b$

What is the maximum winning probability for A and B?

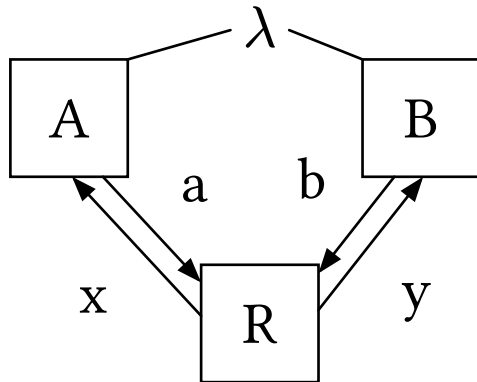
It depends on what we mean by strategies.

Classical strategies for CHSH

Classical strategy: λ is a bit-string of arbitrary size

Trivial strategy: $a = b = 0$.

Notice that $a \oplus b = 0$.



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

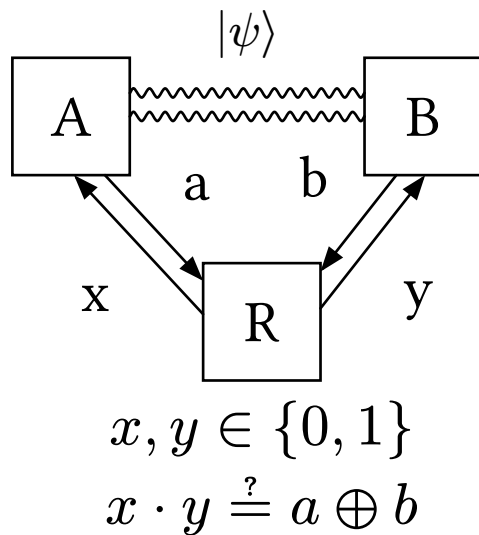
$$x \cdot y \stackrel{?}{=} a \oplus b$$

x	y	$x \cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

$$\Pr[\text{A and B win}] = \frac{3}{4}.$$

Theorem. All classical strategies have acceptance probability $\leq \frac{3}{4}$.

CHSH game - quantum strategies



Quantum strategy: A and B share a quantum state and apply measurements to answer back to R

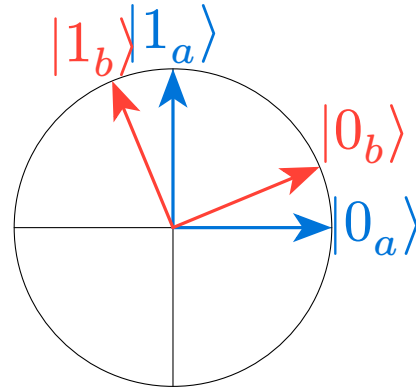
Consider the following quantum strategy:

1. A and B share an EPR pair $|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. They measure in the following bases:

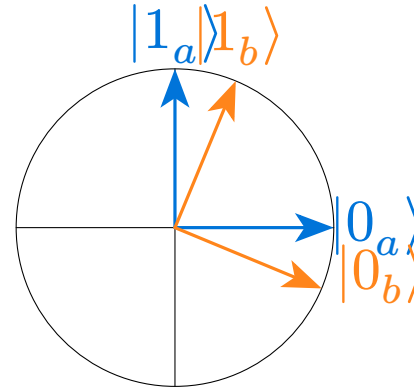
Input	A's basis	B's basis
0	$\{ 0\rangle, 1\rangle\}$	$\{\cos(\frac{\pi}{8}) 0\rangle + \sin(\frac{\pi}{8}) 1\rangle, \sin(\frac{\pi}{8}) 0\rangle - \cos(\frac{\pi}{8}) 1\rangle\}$
1	$\{ +\rangle, -\rangle\}$	$\{\cos(\frac{\pi}{8}) 0\rangle - \sin(\frac{\pi}{8}) 1\rangle, \sin(\frac{\pi}{8}) 0\rangle + \cos(\frac{\pi}{8}) 1\rangle\}$

Basis correlations of quantum strategy

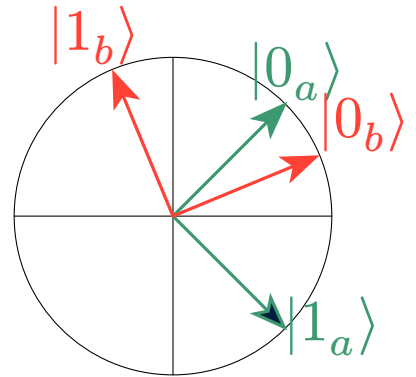
$$x = 0, y = 0$$



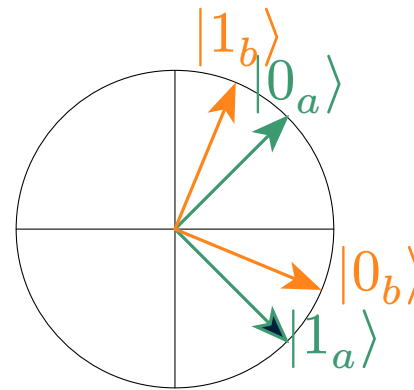
$$x = 0, y = 1$$



$$x = 1, y = 0$$



$$x = 1, y = 1$$

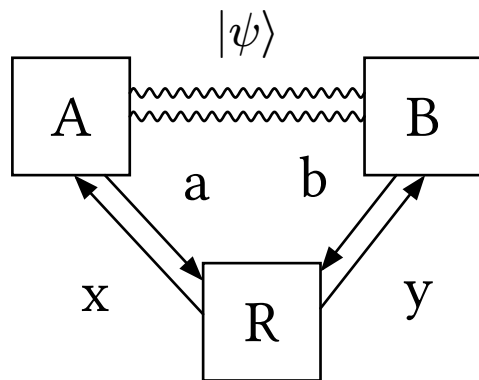


The correct pairs of answers always have a $\cos\left(\frac{\pi}{8}\right)$ angle.

CHSH game - quantum strategies

A and B share an EPR pair $|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

They measure in the following bases:



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

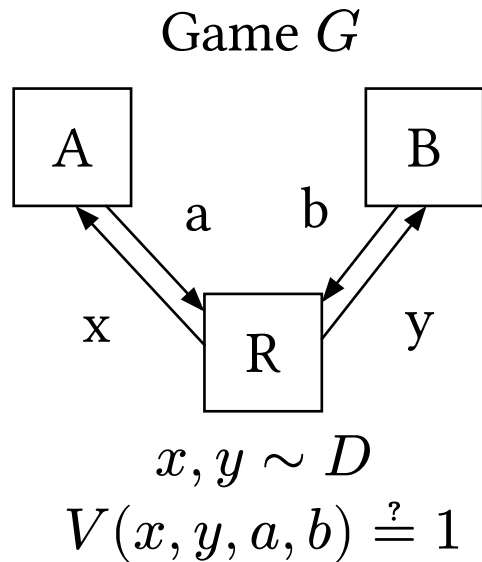
$$x \cdot y \stackrel{?}{=} a \oplus b$$

Input	A's basis	B's basis
0	$\{ 0\rangle, 1\rangle\}$	$\{\cos(\frac{\pi}{8}) 0\rangle + \sin(\frac{\pi}{8}) 1\rangle, \sin(\frac{\pi}{8}) 0\rangle - \cos(\frac{\pi}{8}) 1\rangle\}$
1	$\{ +\rangle, -\rangle\}$	$\{\cos(\frac{\pi}{8}) 0\rangle - \sin(\frac{\pi}{8}) 1\rangle, \sin(\frac{\pi}{8}) 0\rangle + \cos(\frac{\pi}{8}) 1\rangle\}$

A and B win w.p. $\cos^2(\frac{\pi}{8}) \approx 0.85 > \frac{3}{4}$

Theorem. All quantum strategies have acceptance probability $\leq \cos^2(\frac{\pi}{8})$

Non-local game/Bell inequalities



Game G : Arbitrary question distribution D and arbitrary predicate V

Classical value $\omega(G)$: maximum acceptance probability over classical strategies

Quantum value $\omega^*(G)$: maximum acceptance probability over quantum strategies

Non-local game: $\omega^*(G) > \omega(G)$

G is known as a Bell-inequality

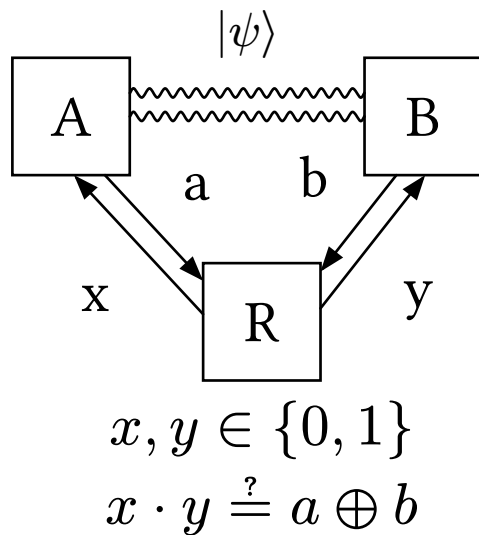
Non-local games gives us an experimental way to prove that the universe is not classical.

CHSH game - rigidity

Textbook strategy: A and B share an EPR pair

$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

They measure in the following bases:



Input	A's basis	B's basis
0	$\{ 0\rangle, 1\rangle\}$	$\{\cos(\frac{\pi}{8}) 0\rangle + \sin(\frac{\pi}{8}) 1\rangle, \sin(\frac{\pi}{8}) 0\rangle - \cos(\frac{\pi}{8}) 1\rangle\}$
1	$\{ +\rangle, -\rangle\}$	$\{\cos(\frac{\pi}{8}) 0\rangle - \sin(\frac{\pi}{8}) 1\rangle, \sin(\frac{\pi}{8}) 0\rangle + \cos(\frac{\pi}{8}) 1\rangle\}$

Theorem. If acceptance probability is $\omega(\text{CHSH}) - \varepsilon$, then strategy is morally close to textbook strategy.

Formal rigidity statement

Theorem. Let

- $(|\text{EPR}\rangle, \{A_x\}, \{B_y\})$ be the textbook strategy for CHSH
- $(|\psi\rangle_{AB}, \{M_x\}, \{N_y\})$ a strategy that wins CHSH w.p. $\geq \cos^2(\frac{\pi}{8}) - \varepsilon$

$$\exists |\text{garb}\rangle_{A'B'} \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}, \quad V_A : \mathcal{H}_A \rightarrow \mathbb{C}^2 \otimes \mathcal{H}_{A'}, \quad V_B : \mathcal{H}_B \rightarrow \mathbb{C}^2 \otimes \mathcal{H}_{B'}$$

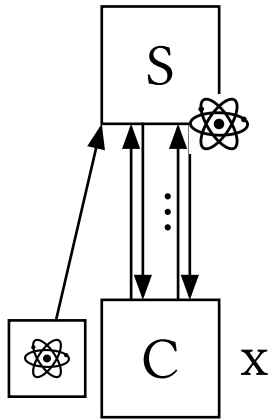
$$|(V_A \otimes V_B)|\psi\rangle_{AB} - |\text{EPR}\rangle_{A''B''} |\text{garb}\rangle_{A'B'}|^2 = O(\sqrt{\varepsilon})$$

$$\mathbb{E}_{x \in \{0,1\}} \left| \left(N_x - V_A^\dagger (A_x \otimes I) V_A \right) \otimes I_B |\psi\rangle \right|^2 = O(\sqrt{\varepsilon}).$$

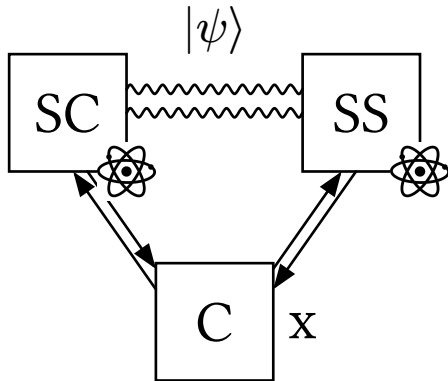
Stronger rigidity theorems

- [MY'98,MIS'12] Self-testing of CHSH - non-perfect quantum strategy
- [WBMS'16] Self-testing of MS - self-tests only 2 EPR pairs
- [C'17,NC'17] Self-testing of parallel repetition of CHSH/MS - closeness decay polynomially
- [NV'18] Self-testing of Pauli Braiding Test - polynomial communication
- [NV'19] Self-testing of Quantum Low-degree test

Recipe from almost classical client to multiple servers



1. Take a protocol with client with very simple quantum operations
2. Consider a two-prover game with SC and SS
 - w.p. $\frac{1}{2}$ SC and SS play a good non-local game
 - w.p. $\frac{1}{2}$ SS runs S and SC to runs C of the original protocol



Proof strategy:

- The questions for SC should be indistinguishable
- The guarantees from self-testing forces SC to be honest
- The guarantees from original protocols gives us security

Instantiating the Recipe

Delegating one-qubit resource states:

- V creates one-qubit resource states, one-time pads them and send them to P
 - Some of these qubits are dummy states to verify the computation
 - The others are *magic states* that enable computation by teleportation
- Very efficient protocols
- Many rounds of interaction to apply corrections

Delegating measurement outcomes (post-hoc verification):

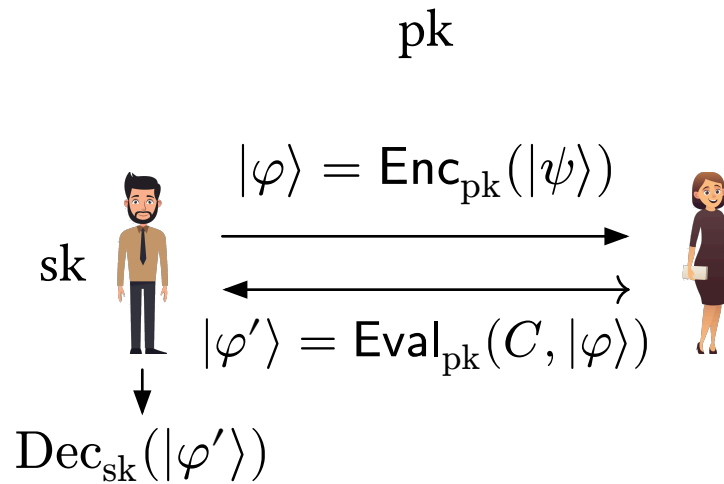
- P creates the history state of the computation
- P sends it to V who only needs to perform simple one qubit measurements
- One message
- Overhead of computation
- No circuit privacy

Known protocols

	Servers	Rounds	Total Resources	Input privacy
RUV 2012	2	$\text{poly}(n)$	g^{8192}	yes
M13	$\text{poly}(n)$	$\text{poly}(n)$	$2^{153} g^{22}$	yes
GKW15	2	$\text{poly}(n)$	g^{2048}	yes
HDF15	$\text{poly}(n)$	$\text{poly}(n)$	$g^4 \log g$	yes
FH15	5	$\text{poly}(n)$	g^3	no
NV18	7	2	g^3	no
CGJV19	2	$O(\text{depth})$	$g \log g$	yes
CGJV19	2	$O(1)$	$g \log g$	no
G19	2	1	g^3	no

Recipe from multiple servers to computational soundness

Quantum FHE

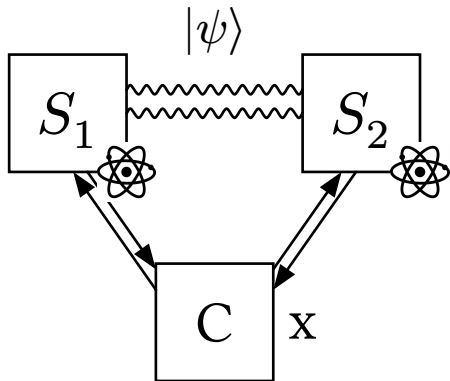


Correctness: $\text{Dec}_{sk}(\text{Eval}_{pk}(\text{Enc}_{pk}(C, |\psi\rangle))) = C|\psi\rangle$

Security: $\forall |\rho\rangle, |\rho'\rangle : \text{Enc}_{pk}(|\rho\rangle) \approx_c \text{Enc}_{pk}(|\rho'\rangle)$

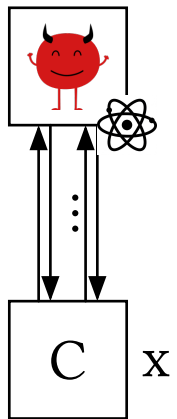
Succinctness: Dec is much simpler than C

Compiled games



Multi-prover game:

1. V sends q_1 to P_1 and q_2 to P_2
2. V gets a_1 from P_1 and a_2 from P_2
3. V checks if $V(q_1, q_2, a_1, a_2) = 1$



Compiled game:

1. V sends $\text{QFHE.Enc}(q_1)$ to P
2. P sends $\text{QFHE.Enc}(a_1)$ to V
3. V sends q_2 to P
4. P sends a_2 to V
5. V checks if $V(q_1, q_2, a_1, a_2) = 1$

Compiled games - known results

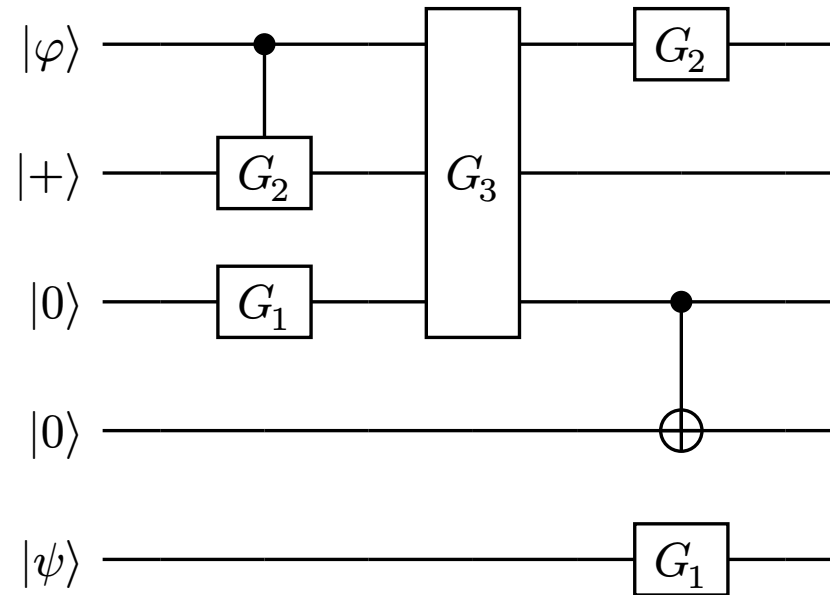
- KLVY'23: The classical value of the compiled game is bounded
- NZ'23,MNZ'24: The quantum value of the parallel repetition of CHSH is bounded
- BVB+'24 The quantum value of XOR games is bounded.
Delegation of quantum computation from compiled games.
- CMM+'24,KMP+'24: The quantum value of all games is bounded by the commuting operator value

Open question: Does the quantum value of the non-local game translates to the compiled game?

A protocol for delegation of quantum computation with almost classical client

Back to quantum circuits

1. Fix a gateset $\mathcal{G} = \{G_1, G_2, \dots\}$ (usually on a constant number of qubits)
2. Fix the number of qubits
3. Compose gates from $\mathcal{G}$ on those qubits
4. Add measurements at the end



How to choose $\mathcal{G}$?

Universal gateset

Definition: $\mathcal{G}$ is an universal gateset for quantum computation if any n -qubit unitary operation can be approximated to arbitrary accuracy using a quantum circuit composed only of gates from $\mathcal{G}$.

Theorem. The gateset

$$\left\{ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, c(X), T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\frac{\pi}{4}) \end{pmatrix} \right\}$$

is universal for quantum computation.

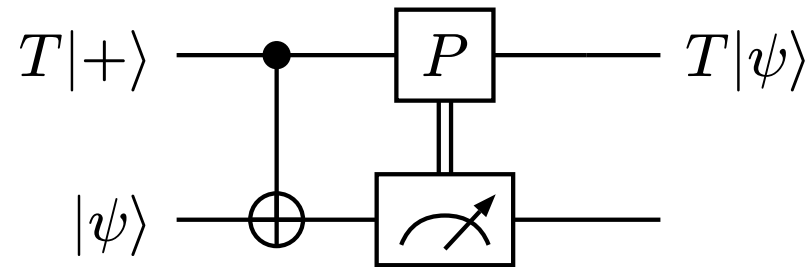
- $X, Z, P, c(X)$ are “simpler” to implement
- T is usually the bottleneck

Magic states and T-gadget

Can we somehow implement T using only $X, Z, P, c(X)$ gates?

NO!

What if we have some help?

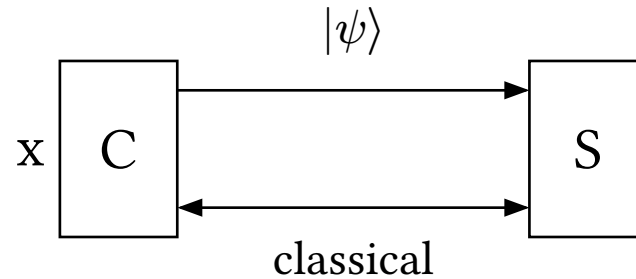


Exercise: Show that the output of the circuit is indeed $T|\psi\rangle$.

If we are given $|T\rangle = T|+\rangle$, then only applying a $c(X)$ and a classically controlled P , we can implement T gates.

Crucial gadget in quantum cryptography

Broadbent delegation scheme



Structure of the protocol:

1. C sends a simple quantum state
2. C and S interact with classical communication

Test rounds: C sends trap states to check if S is honest

Computation rounds: C sends state that makes S perform the computation

Key property: Round types are indistinguishable to the prover

Protocol in more details

1. C sends $X^a Z^b |\psi\rangle$, where $|\psi\rangle$ depends on the round type
2. At the end of the protocol S holds $X^{a'} Z^{b'} |\psi'\rangle$

$$X^a Z^b |\psi\rangle \longrightarrow \boxed{S} \longrightarrow X^{a'} Z^{b'} |\psi'\rangle$$

X-test: $|\psi'\rangle = |\psi\rangle = |0\rangle$

Z-test: $|\psi'\rangle = |\psi\rangle = |+\rangle$

Computation: $|\psi'\rangle = U|\psi\rangle$

C can compute a', b'

Gadgets

C and S interact to run the circuit gate by gate.

Gadget for each $G \in \{X, Z, \text{CNOT}, H, T\}$

$$X^a Z^b |\psi\rangle \text{ --- } \boxed{G} \text{ --- } X^{a'} Z^{b'} |\psi'\rangle$$

X-test: $|\psi'\rangle = |\psi\rangle = |0\rangle$

Z-test: $|\psi'\rangle = |\psi\rangle = |+\rangle$

Computation: $|\psi'\rangle = G|\psi\rangle$

C keeps track of OTP keys at any point

Gadgets - X, Z, CNOT

X and Z

- For computation rounds, C updates the OTP keys
 - X: $(a, b) \leftarrow (a \oplus 1, b)$
 - Z: $(a, b) \leftarrow (a, b \oplus 1)$
- For test rounds, C does nothing

CNOT

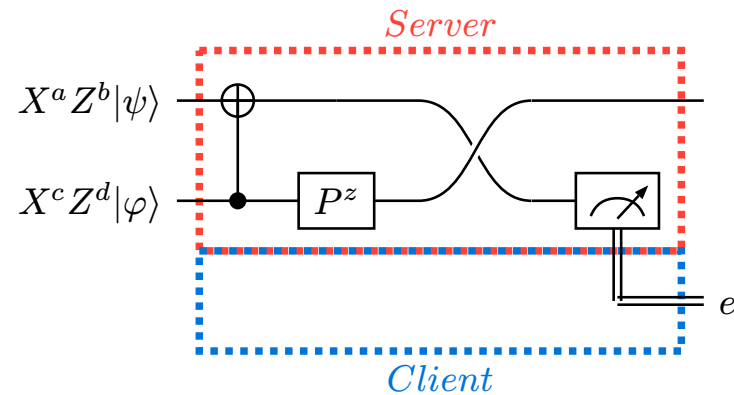
- S applies CNOT:
$$\text{CNOT} \cdot X^a Z^b \otimes X^c Z^d = X^a Z^{b+d} \otimes X^{a+c} Z^d \cdot \text{CNOT}$$
- C updates OTP keys to $(a, b, c, d) \rightarrow (a, b + d, a + c, d)$
- For test rounds $\text{CNOT}|0\rangle|0\rangle = |0\rangle|0\rangle$ and $\text{CNOT}|+\rangle|+\rangle = |+\rangle|+\rangle$

Gadgets - Hadamards

$$H X^a Z^b = X^b Z^a H$$

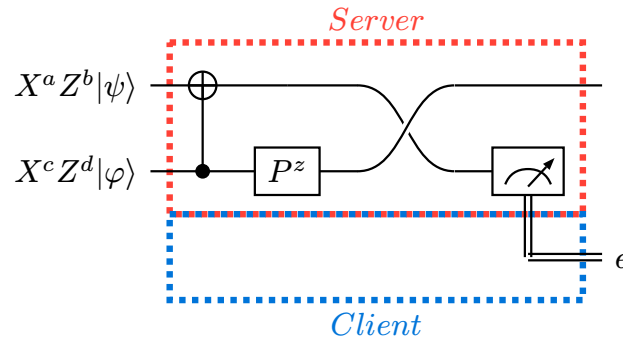
- For computation rounds, S could apply H and C swaps the keys
- Problem with test rounds: $H|0\rangle = |+\rangle$ and $H|+\rangle = |0\rangle$

Gadgets - T



- In computation rounds, C sends $|\varphi\rangle = |T\rangle$ to S
- In test rounds, C sends $|\varphi\rangle = |0\rangle/|+\rangle$ to S
- V sends random z , for each T gate
- P applies CNOT, P^z , measures and send e to the verifier

Update rules for T-gadgets



X-test

- V checks if $a = e$
- $(a', b') \leftarrow (c, 0)$.

Computation round

- $(a', b') \leftarrow (a \oplus c, b \oplus c \oplus (a \oplus e)z)$

Z-test

- $(a', b') \leftarrow (0, b \oplus e \oplus z)$.

Broadbent delegation scheme - Hadamards

- We can use identity $HTTHTTHTTH = H$
- If use T gadget, in test rounds we have $HHHH = I$.
 - X-tests become Z-tests between two physical Hadamards (and vice-versa)
 - Checks done in the T-gadget alternate

Broadbent delegation scheme

Correctness: By construction, if S runs the honest strategy the outcome comes from the right distribution

Security:

1. Move to the entangled version of the protocol $\Rightarrow S$ does the operations before C chose the round-type.
2. If the tests pass, we can characterize the types of attacks that S does
3. Show that these attacks are “benign”

Summary

Protocol for delegation of quantum computation with almost classical client



Protocol for delegation of quantum computation with entangled servers



Protocol for delegation of quantum computation against computationally bounded servers