Flow Ambiguity: A Path Towards Classically Driven Blind Quantum Computation

Atul Mantri

September 6, 2017

Singapore University of Technology and Design (SUTD) and
Centre for Quantum Technologies (CQT), Singapore

Joint work with

Tommaso Demarie
SUTD & CQT

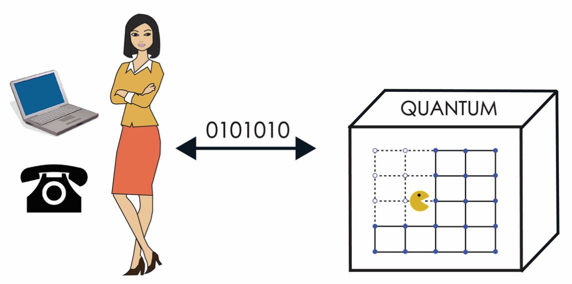
Nicolas Menicucci
RMIT University

Joseph Fitzsimons
SUTD & CQT

Problem Statement and Prior Work

Delegated computation

Imagine a scenario where large scale quantum computer becomes available BUT only at a few locations around the globe, however anyone can access it over the internet!



Security

What about integrity and privacy of the client's computation?

Blind quantum computation

Blind quantum computation[1]- allows a client, with weak computational power, to delegate a computation to a remote (powerful) quantum server. These protocols come mainly in two flavors:

- (*Blindness*) privacy of client's computation is preserved.
- (*Verification*) integrity of the desired computation is maintained.

[1]For more information see review article: npj Quantum Information 3, Article number: 23 (2017)

Previous works

Protocol	client's power	No. of server
BFK[2]	single qubit preparation device	1
MF[3]	measurement apparatus	1
RUV[4]	completely classical	2

A common feature among all these known protocols is that either the client requires a small quantum device on their side or there must exist at least two non-communicating quantum servers.

[2] Universal blind quantum computation. FOCS'09. 50th Annual IEEE Symposium (pp. 517-526).
[3] PRA 87(5), 050301
[4] Nature, 496(7446), 456-460. (servers are entangled but noncommunicating)

Problem statement

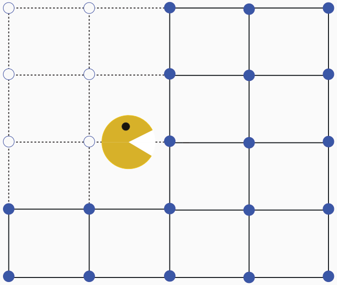
Classically Driven Blind Quantum Computation

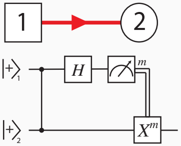
Is it possible for a completely classical client to delegate a quantum computation to a single remote quantum server while keeping the information about computation hidden?

Preliminaries

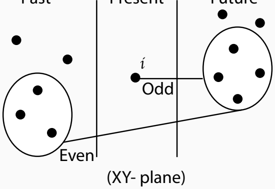
Measurement-based quantum computation

MBQC





1-bit teleportation



gflow

Our contribution

Blind computing protocol with a completely classical client

Task

Alice's target computation is given by $\Delta_A = \{\rho_I, U_A, \mathcal{M}\}$, where ρ_I[5] is the n-qubit input state, U_A is the unitary embedding that maps ρ_I to the output state $\rho_O = U_A \rho_I U_A^{\dagger}$, and $\mathcal{M}$ is the final set of measurement on the output state to get the classical output.

We propose an interactive protocol to perform this task which we call *classically driven blind quantum computation*.

[5] We take input states that can be efficiently described classically.

Classically driven blind quantum computing

Protocol steps are as follows:

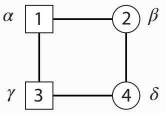
- **State preparation**: Bob prepares the graph state $|\mathcal{G}\rangle_{n\times m}$.
- **Measurements**: For $i = 1, \ldots, N$, repeat:
  1. Alice picks a bit $r_i \in_R \{0,1\}$ uniformly at random. Then, using r_i, $\boldsymbol{s}^x$, $\boldsymbol{s}^z$, she computes the angle α'_i, where

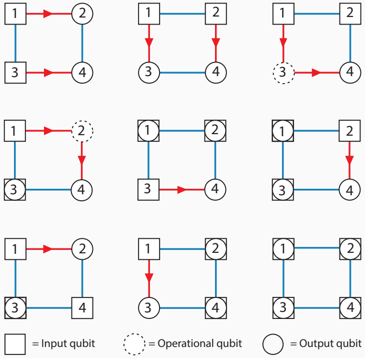
  $$\boldsymbol{\alpha}' = (-1)^{\boldsymbol{s}^x}\boldsymbol{\alpha} + (\boldsymbol{s}^z + \boldsymbol{r})\pi \mod 2\pi,$$

  2. Alice transmits α'_i to Bob.
  3. Bob measures the ith qubit in the basis $\{|\pm_{\alpha'_i}\rangle\}$ and transmits the measurement outcome $b'_i \in \{0,1\}$ to Alice.
  4. Alice records $b_i = b'_i \oplus r_i$ in $\mathbf{b}$ and then updates the dependency sets $(\boldsymbol{s}^x, \boldsymbol{s}^z)$. If $i \in O$, then she also records b_i in $\mathbf{p}^C_{\mathcal{B}}$
- **Post Processing**: Alice performs final (classical) operations on the set of output qubits by calculating $\mathbf{p} = \mathbf{p}^C_{\mathcal{B}} \oplus \mathbf{s}^z_O$, where $\mathbf{s}^z_O$ is used to represent the final set of Z corrections .

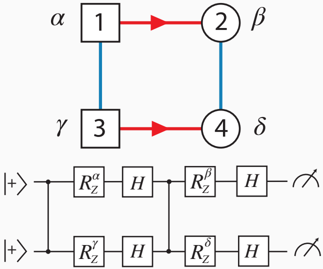
Example: 2×2 cluster state

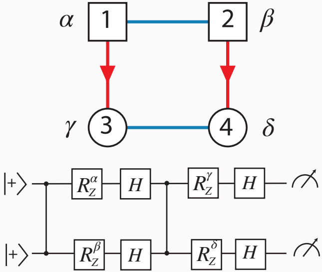
To demonstrate this we take a simple example of 2×2 cluster state $G(I, O)_{(2\times 2)}$. The figure shows 9 possible open graphs compatible with all the flow conditions.





Flow - circuit mapping





In general different flows correspond to different computations.

Security

- Description of Alice's computation - $\Delta_A^{\mathrm{MBQC}} := (G_{n\times m}, \boldsymbol{\alpha}, f)$
- Information Bob receives $:= (\boldsymbol{b'}, \boldsymbol{\alpha'})$

Aim (Formal)

$$H(A, F|B', A') = ?$$

We observe the following relation:

$$H(A, F|B', A') \geq H(F) - N + H(B', A'|A, F)$$

Therefore, our task reduces to calculate:

1. $H(B', A'|A, F)$
2. $H(F)$

1. Conditional entropy: $H(B', A'|A, F)$

Claim

$H(B', A'|A, F) \geq N$ regardless of Bob's strategy.

Outline of the proof:

- Construct full joint probability distribution for all the variables in the protocol - $\Pr(b', \alpha', \alpha, f, b, r)$
- Use dependencies between different variables to calculate the full joint probability.
- Marginalizing over B and using the joint probability distribution $\Pr(b', \alpha', \alpha, f, r)$ to compute $\Pr(b', \alpha'|\alpha, f)$

This in turn gives a lower bound on the conditional entropy

$$H(A, F|B', A') \geq H(F) = \log_2 N_F$$

Side result

$I(B', A'; A, F) \leq H(A')$

2. Flow counting argument: H_F

Theorem

$$\#\mathcal{G}(I,O)_{n,m} = F_{2\min(n,m)+1}^{|n-m|} \prod_{\mu=2}^{\min(n,m)} F_{2\mu}^2.$$

where F_i is the ith Fibonacci number.

Upon simplification: $\#\mathcal{G}(I,O)_{n,m} = 2^{2N\log_2\phi + O(N^\epsilon)}$ for $\epsilon < 1$, $N = nm$, and $m = \text{poly}(n)$

Combining $N_F \geq \#\mathcal{G}(I,O)_{n,m}$ with the previous result, we get $\log_2 N_F \geq \log_2 \#\mathcal{G}(I,O)_{n,m} \approx 1.388N$.

Final Result

$$H(A,F|B',A') \geq 1.388N$$

Conclusion and Future Directions

To sum up

- We explore the possibility of classically driven blind quantum computation.

- This is shown by observing that multiple non-equivalent computations in the MBQC model can yield the same transcript of measurement angles and results, even when the resource state and order of measurements are fixed.

- We also show that, in a single run of the protocol, the amount of information obtained by the server about client's computation is bounded.

Open problems

- Is it possible to exploit this novel cryptographic tool, flow ambiguity, to achieve *universal* classically driven blind quantum computation?

- More importantly, can such a technique be used as a building block for *verification* of quantum computers by completely *classical client* or in other words to prove if $\mathrm{BQP} = \mathrm{IP}_{BQP}$?

Thank you for your attention!

Paper reference: Phys. Rev. X 7, 031004 (2017).