How Do I Know If You Have A Quantum Computer

Information Theoretically Secure Hypothesis Test for Temporally Unstructured Quantum Computing

Daniel Mills[1], Anna Pappa[12], Theodoros Kapourniotis[13], and Elham Kashefi[14]

[1]School of Informatics, The University of Edinburgh

[2]Department of Physics, University College London

[3]Department of Physics, University of Warwick

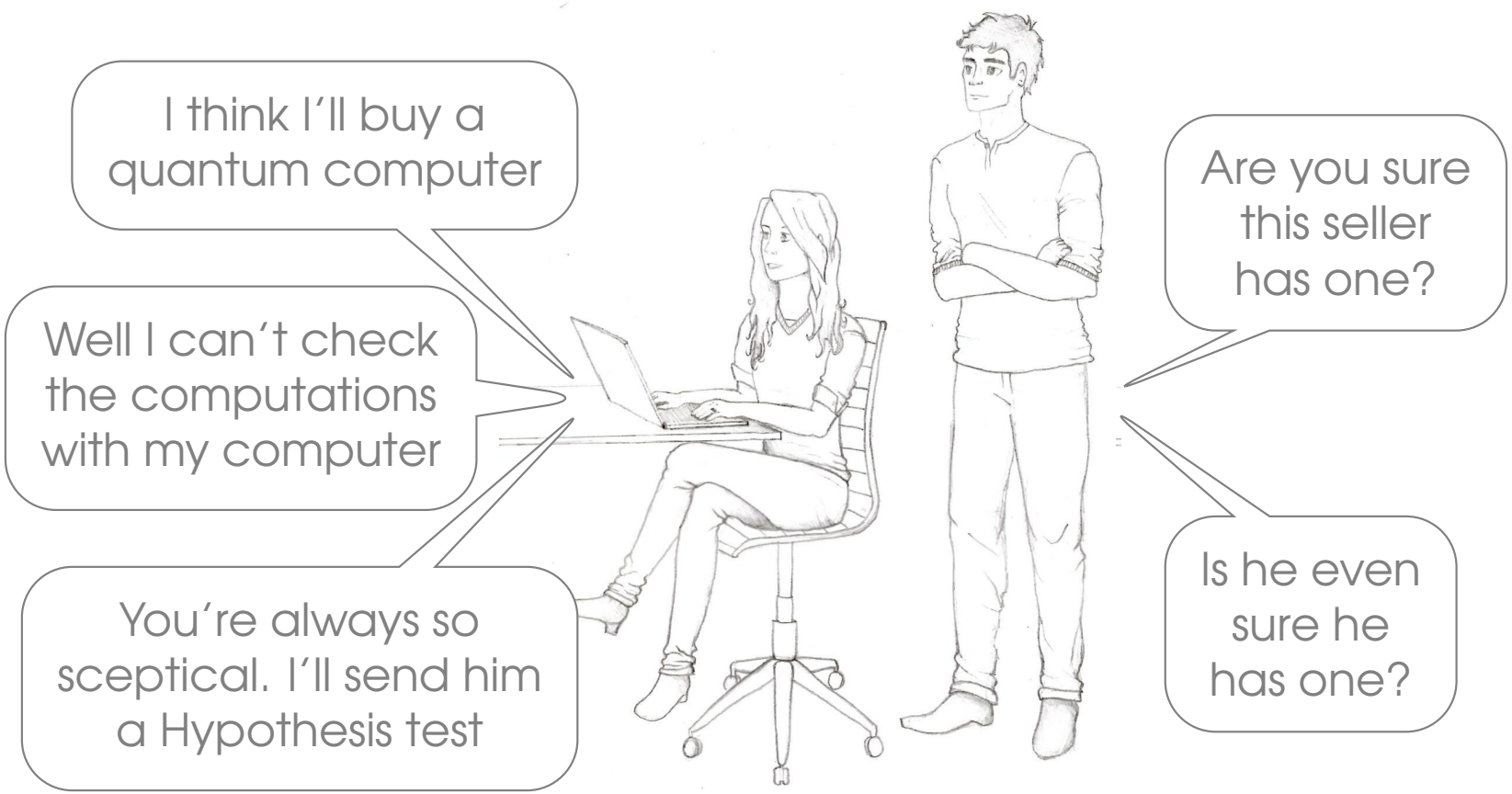
[4]LIP6, CNRS, Pierre et Marie Curie University

Quantum Simulation Models Workshop, June 12, 2017

This Presentation

This Presentation

Introduction



Introduction

A well designed *Hypothesis test* should allow:

Introduction

A well designed *Hypothesis test* should allow:

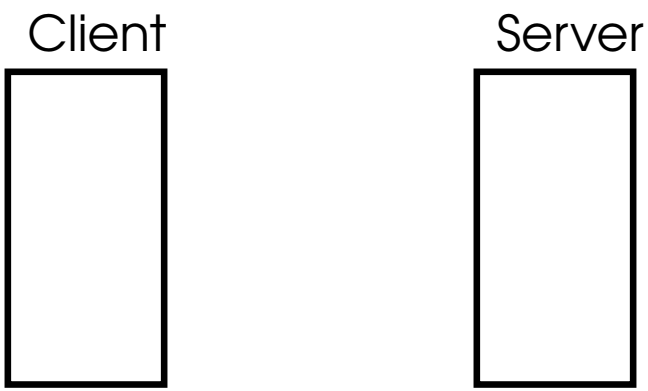
- A Client to ensure a malicious Server is capable of quantum computations.

Introduction

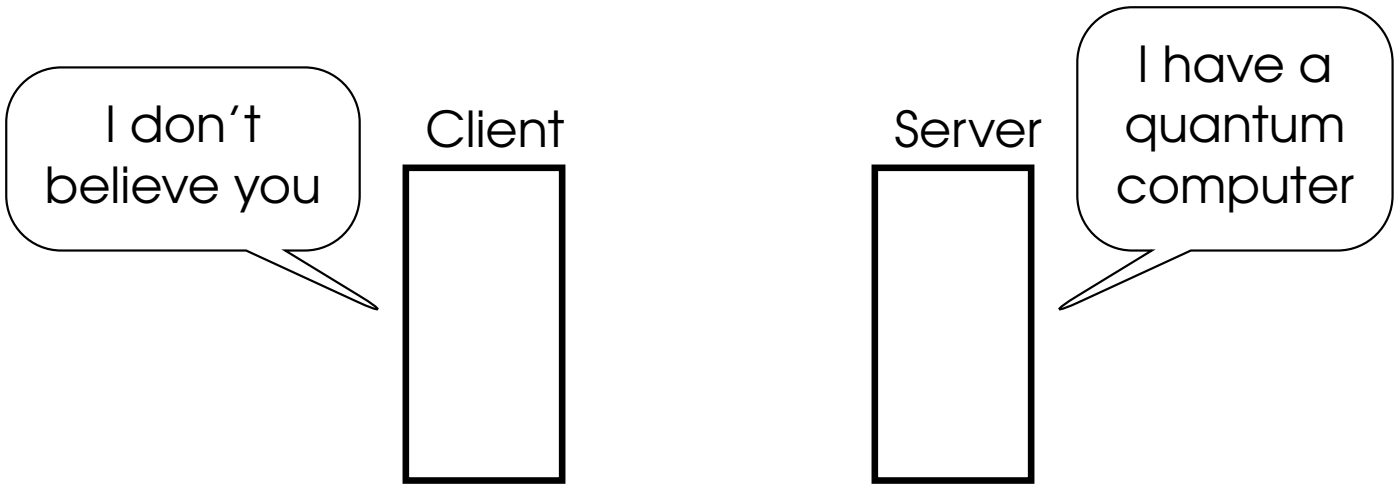
A well designed *Hypothesis test* should allow:

- A Client to ensure a malicious Server is capable of quantum computations.
- An engineer to check their machine is capable of quantum computations.

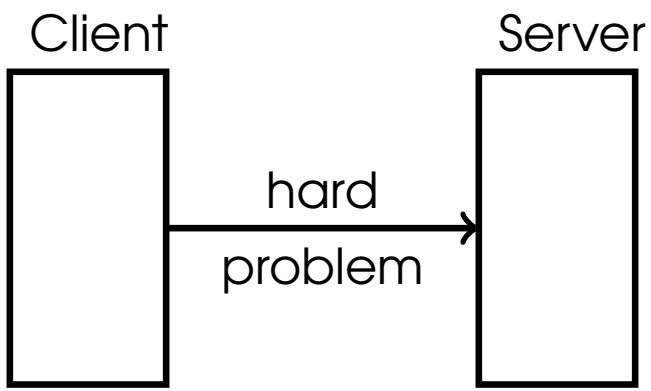
A Proposal



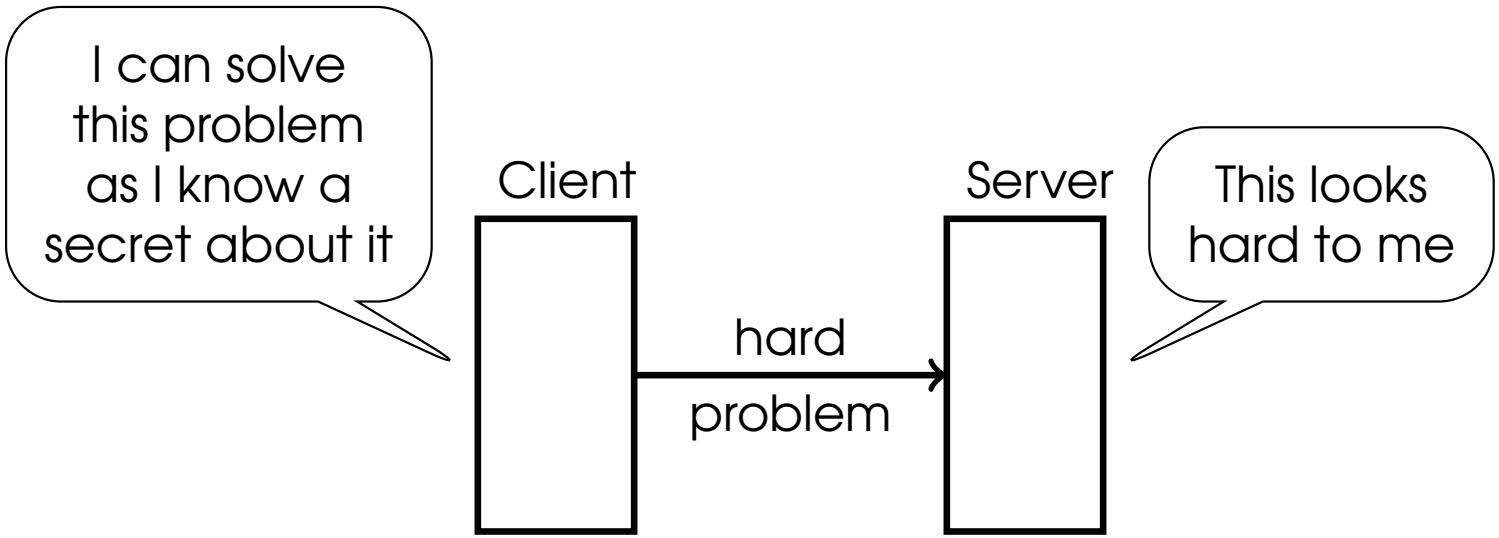
A Proposal



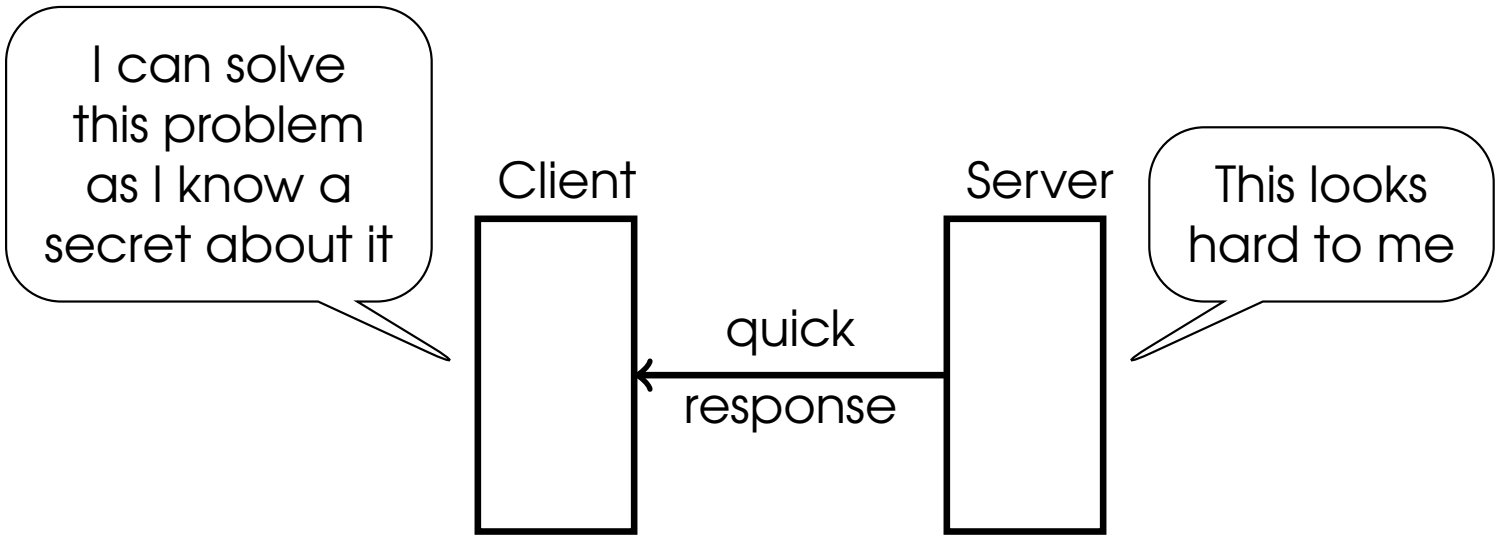
A Proposal



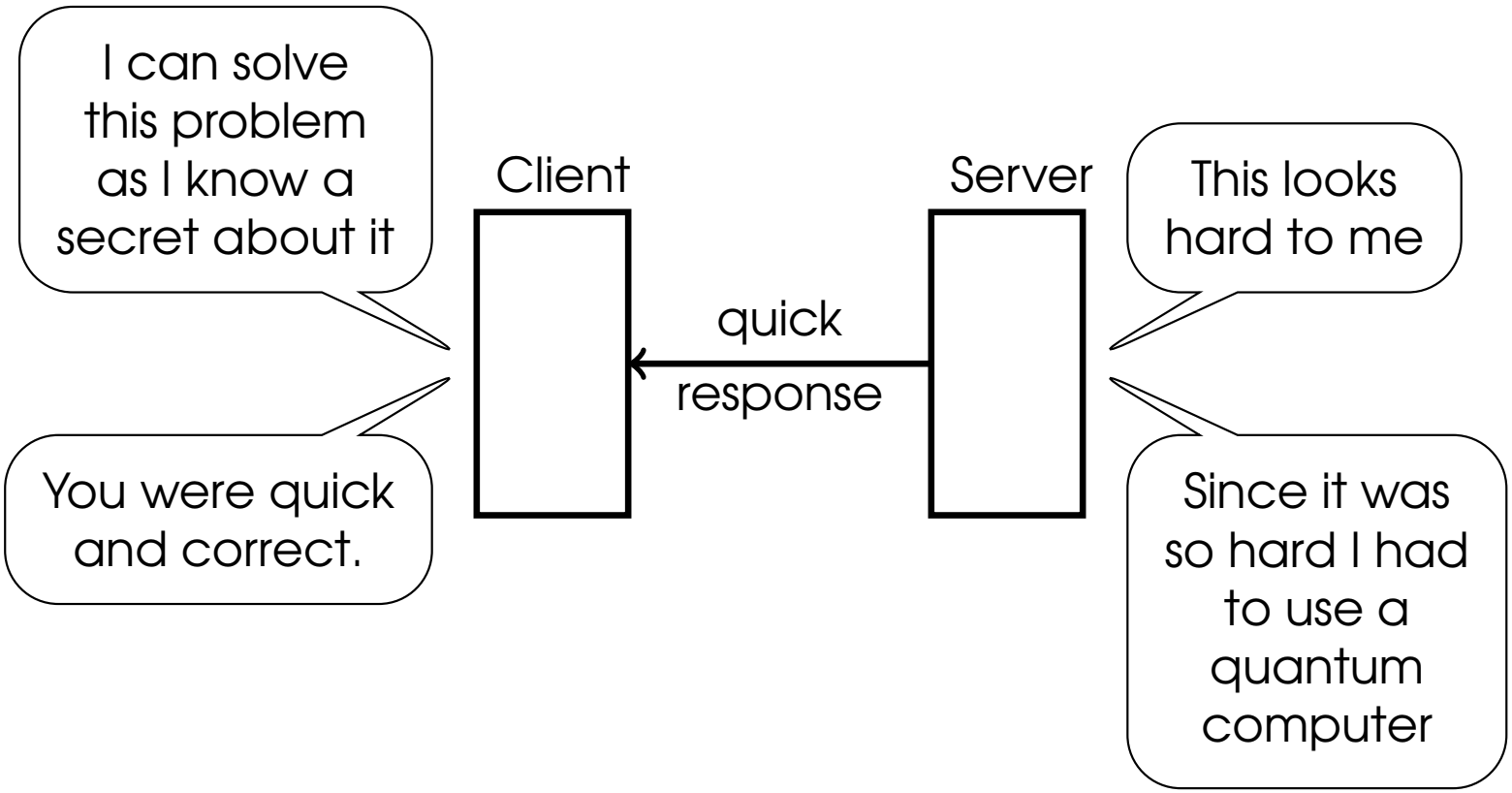
A Proposal


I can solve this problem as I know a secret about it
Client
hard problem
Server
This looks hard to me

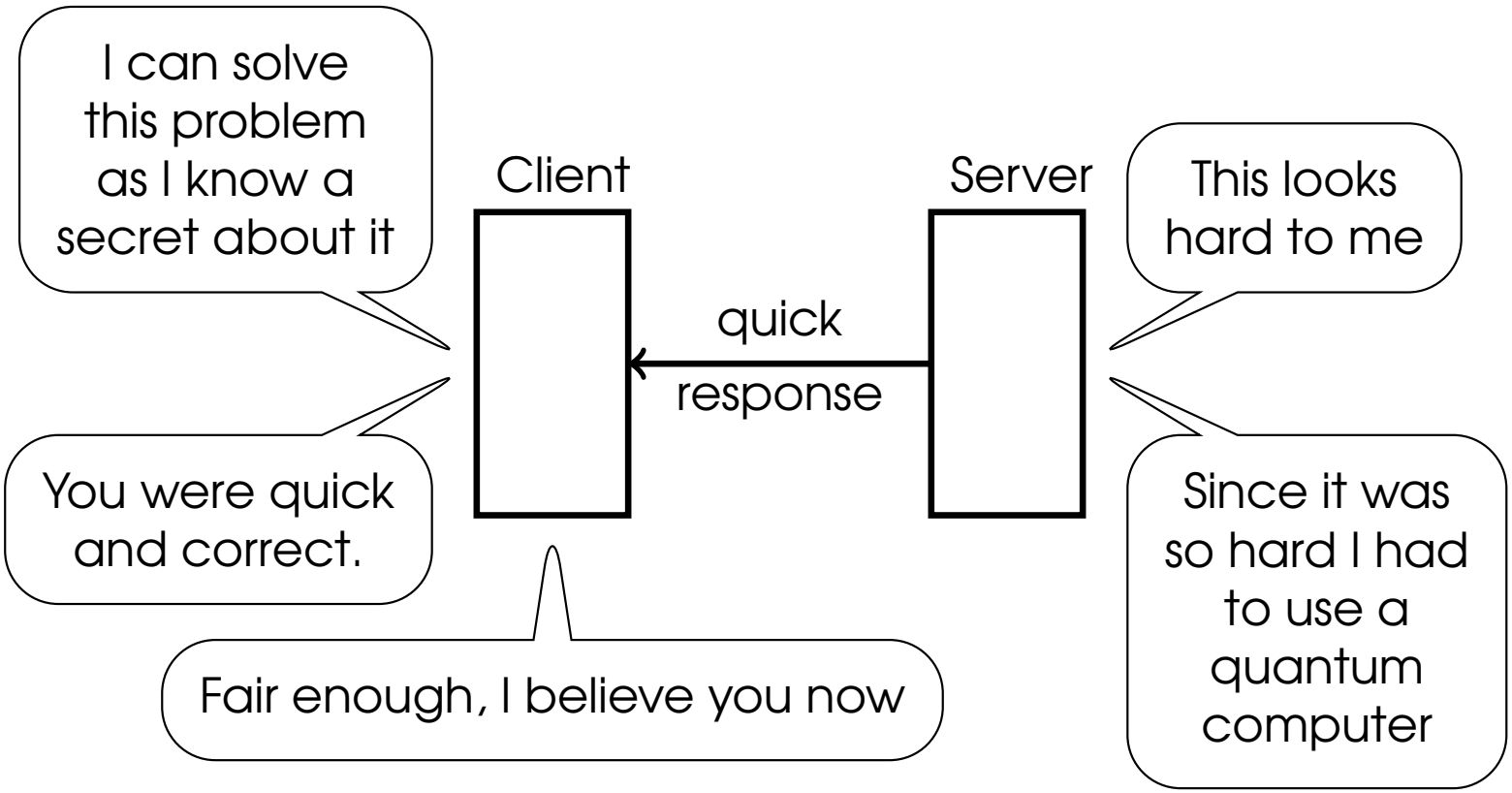
A Proposal


I can solve this problem as I know a secret about it
Client
Server
This looks hard to me
quick
response

A Proposal


I can solve this problem as I know a secret about it
Client
Server
This looks hard to me
quick
response
You were quick and correct.
Since it was so hard I had to use a quantum computer

A Proposal


I can solve this problem as I know a secret about it
Client
Server
This looks hard to me
quick
response
You were quick and correct.
Fair enough, I believe you now
Since it was so hard I had to use a quantum computer

A Proposal

So three conditions for a successful hypothesis test might be:

A Proposal

So three conditions for a successful hypothesis test might be:

- The Server must complete a hard IQP computations
  - This means it is an IQP machine

A Proposal

So three conditions for a successful hypothesis test might be:

- The Server must complete a hard IQP computations
  - This means it is an IQP machine
- The Client knows a secret allowing them to check the outcome
  - Must be sure that this does not add structure to the problem which the Server can use

A Proposal

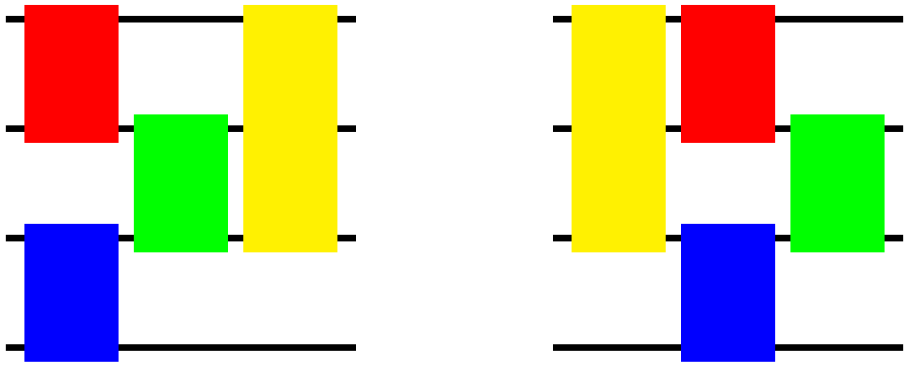
So three conditions for a successful hypothesis test might be:

- The Server must complete a hard IQP computations
  - This means it is an IQP machine
- The Client knows a secret allowing them to check the outcome
  - Must be sure that this does not add structure to the problem which the Server can use
- The Server hides the secret something

This Presentation

The Instantaneous Quantum Polytime Machine (SB)

Commuting gates:



In particular:

$$\exp\left\{ i\theta \bigotimes_{i:q_i=1} X_i \right\}$$

where $q \in \{0,1\}^{n_p}$, $\theta \in [0, 2\pi]$.

The Instantaneous quantum Polytime Machine (SB)

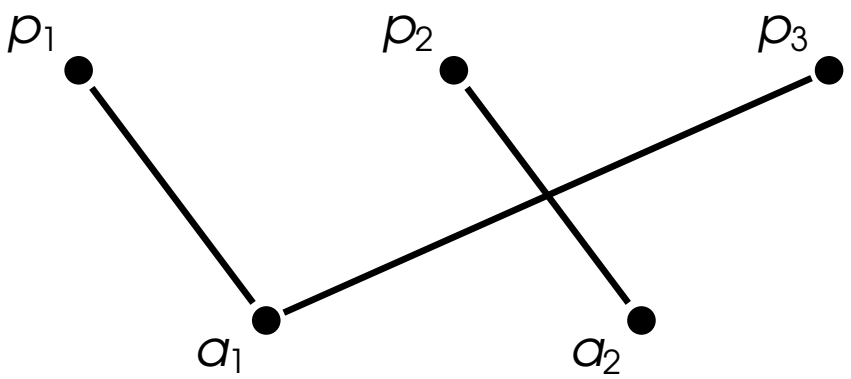
$$\exp\left\{ i\theta \bigotimes_{i:q_i=1} X_i \right\}$$

An IQP program may consist of many of these gates, and so many different q. Hence we may represent the whole computation by, for example:

$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

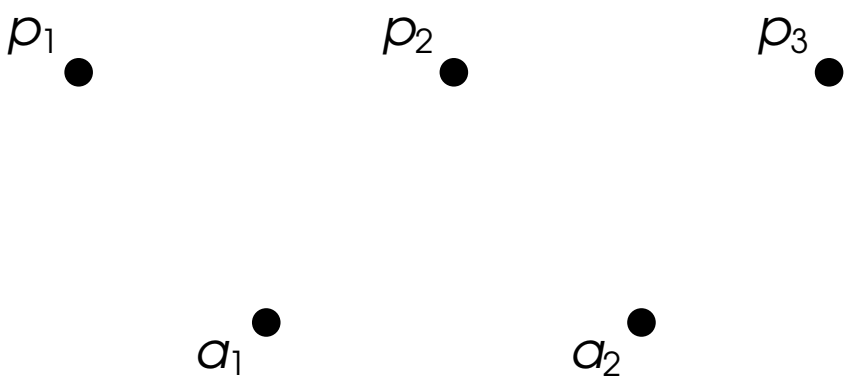
where, in this case, we have two gates defined by $q = (101)$ and $q = (010)$.
The input is $|0^{n_p}\rangle$ and the output is the resulting state measured in the computational basis.

IQP in MBQC



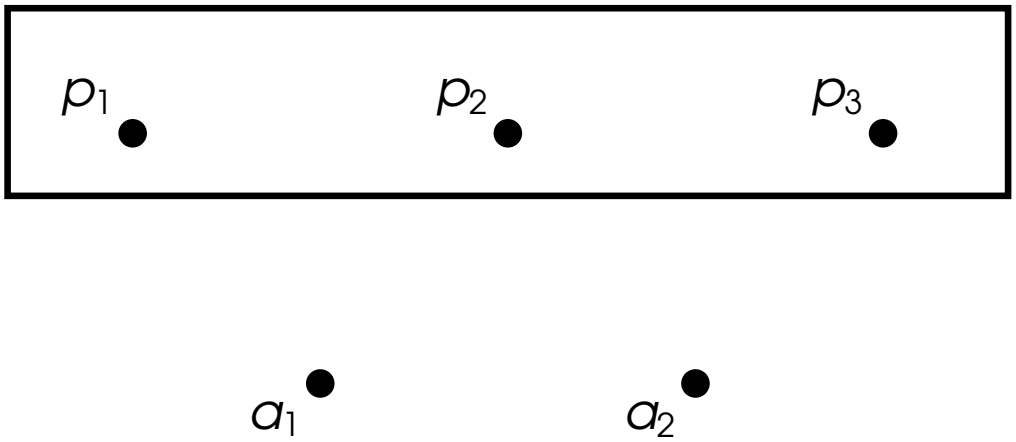
$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

IQP in MBQC



$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

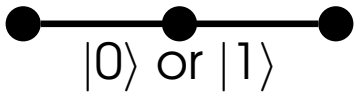
IQP in MBQC



$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

This Presentation

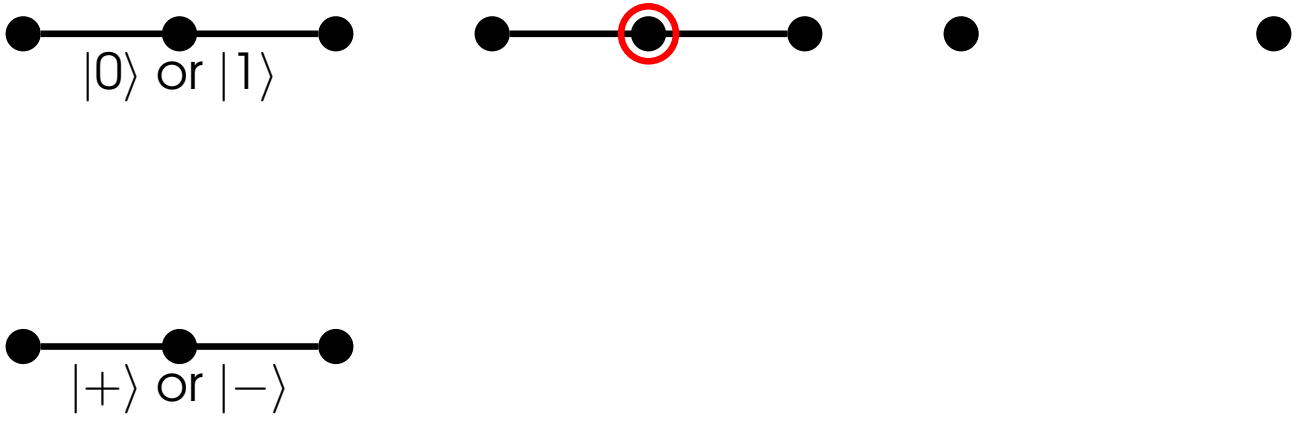
Bridge and Break (FK)



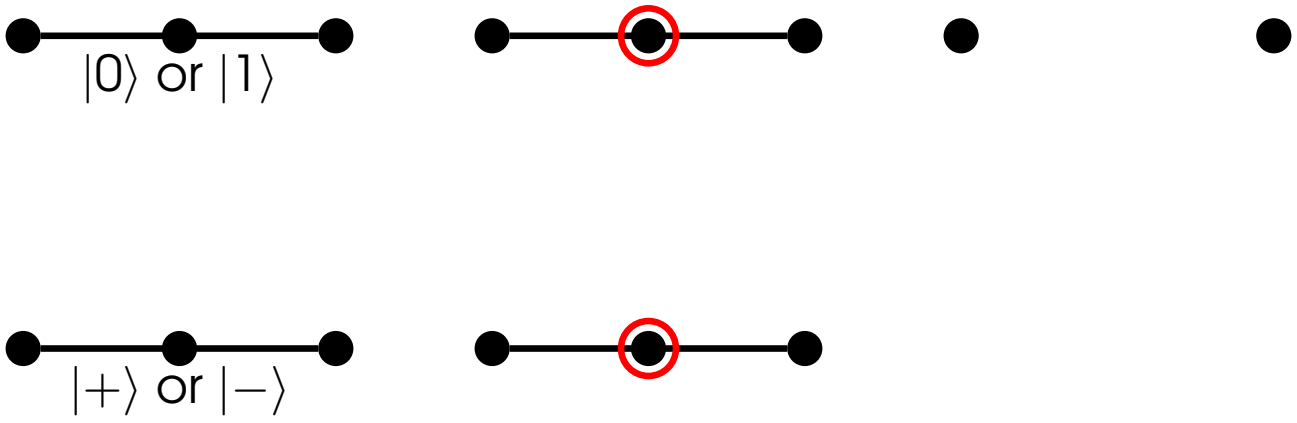
Bridge and Break (FK)

Bridge and Break (FK)

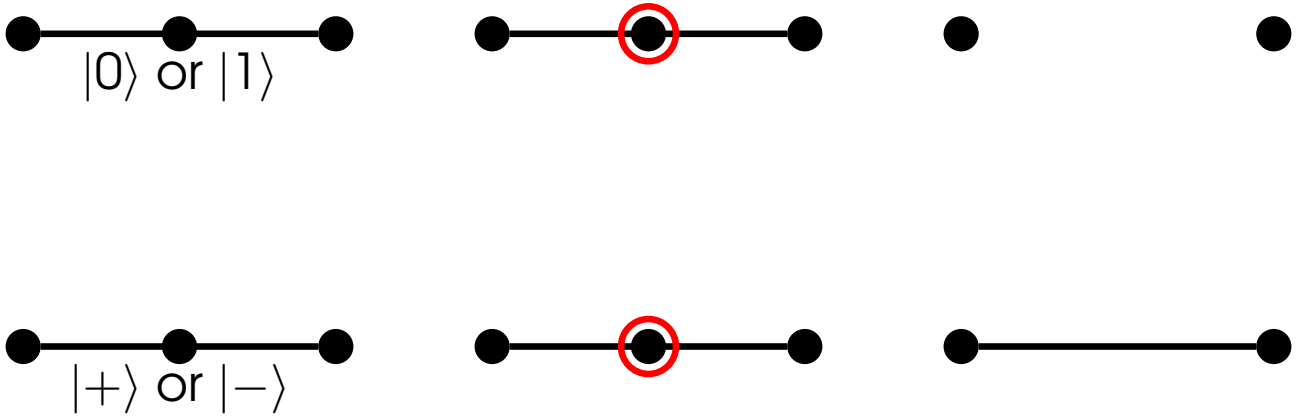
Bridge and Break (FK)



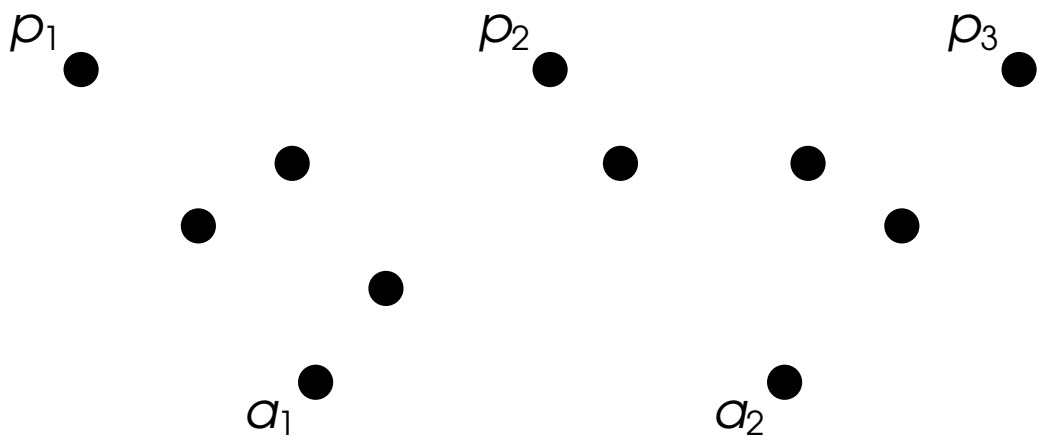
Bridge and Break (FK)



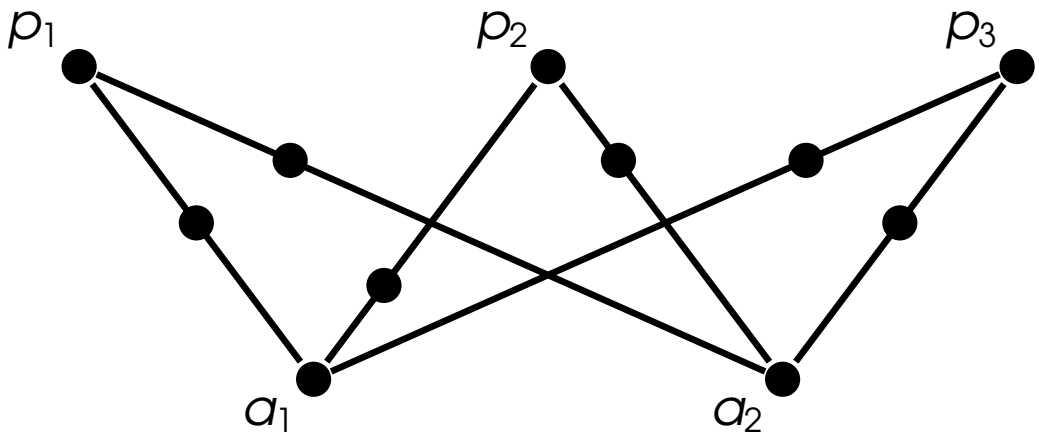
Bridge and Break (FK)



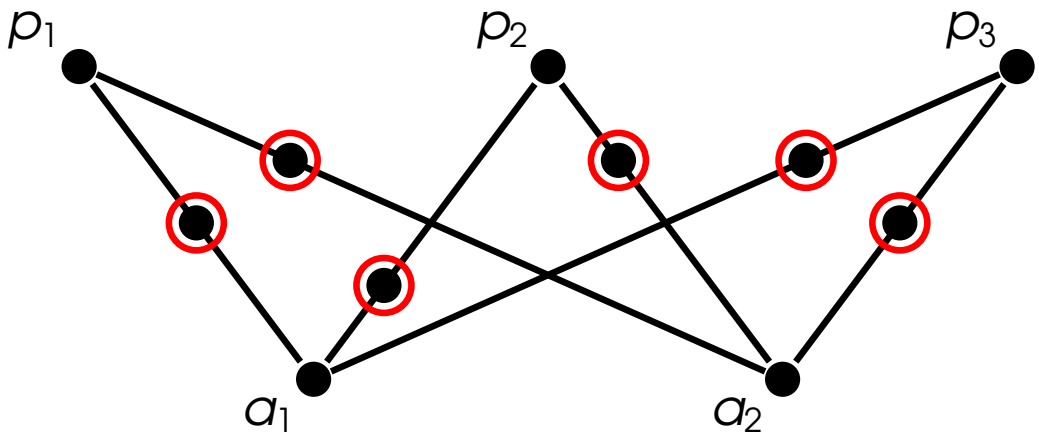
IQP By Bridge and Break



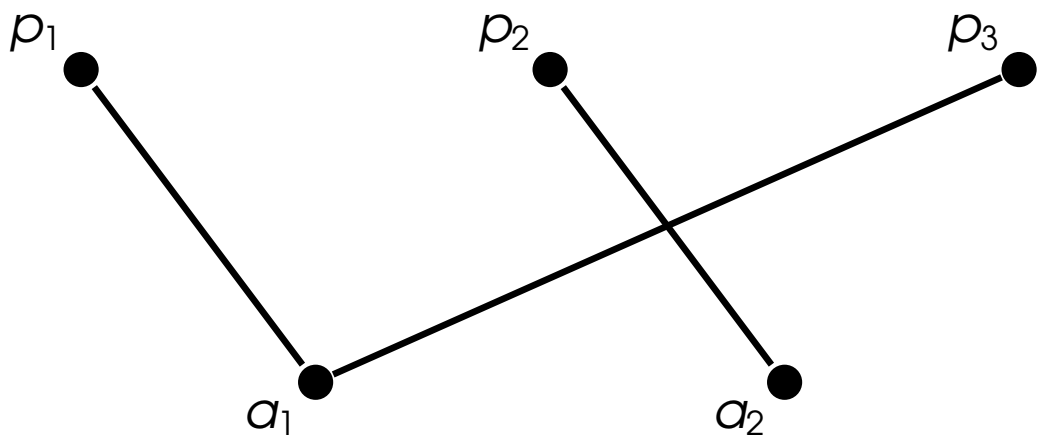
IQP By Bridge and Break



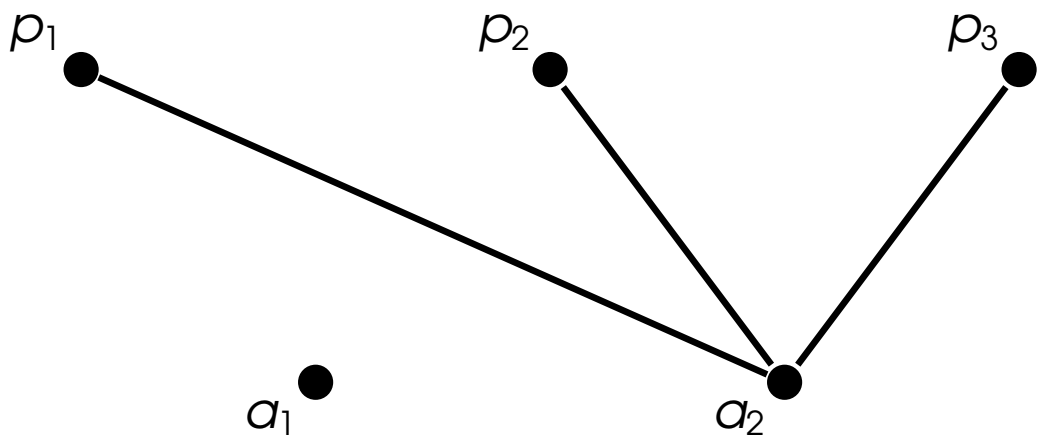
IQP By Bridge and Break



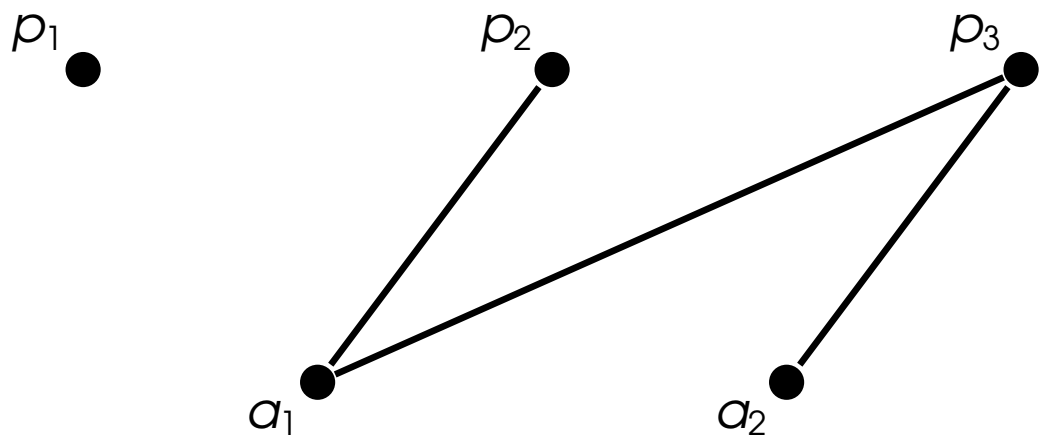
IQP By Bridge and Break



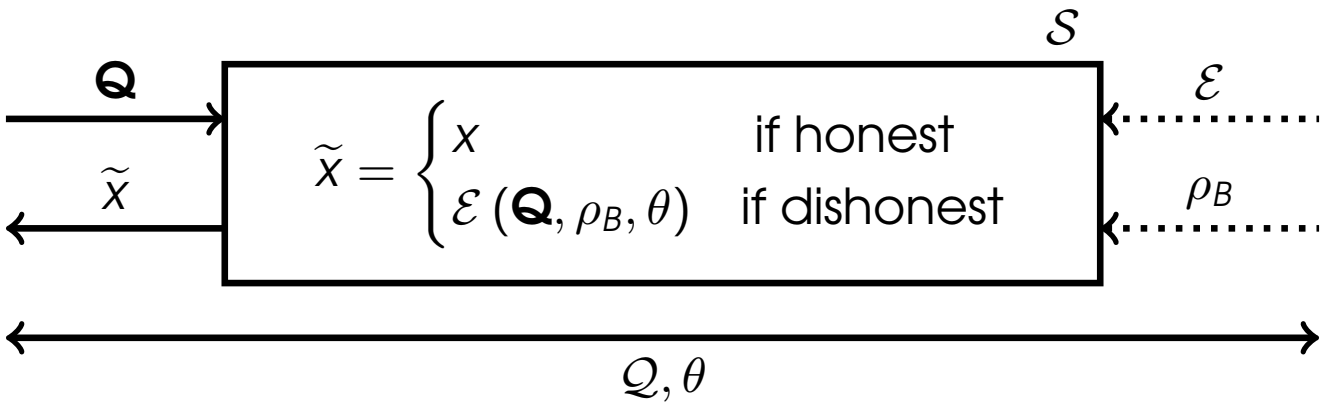
IQP By Bridge and Break



IQP By Bridge and Break



Blind IQP Ideal Resource (V)



This Presentation

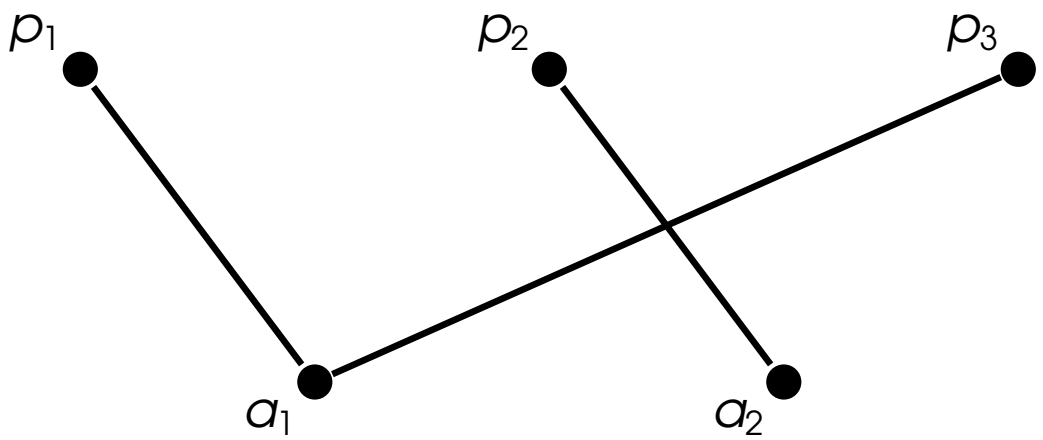
Hypothesis Test

Bias of a random variable, $X \in \{0,1\}^{n_p}$, in a direction $s \in \{0,1\}^{n_p}$.

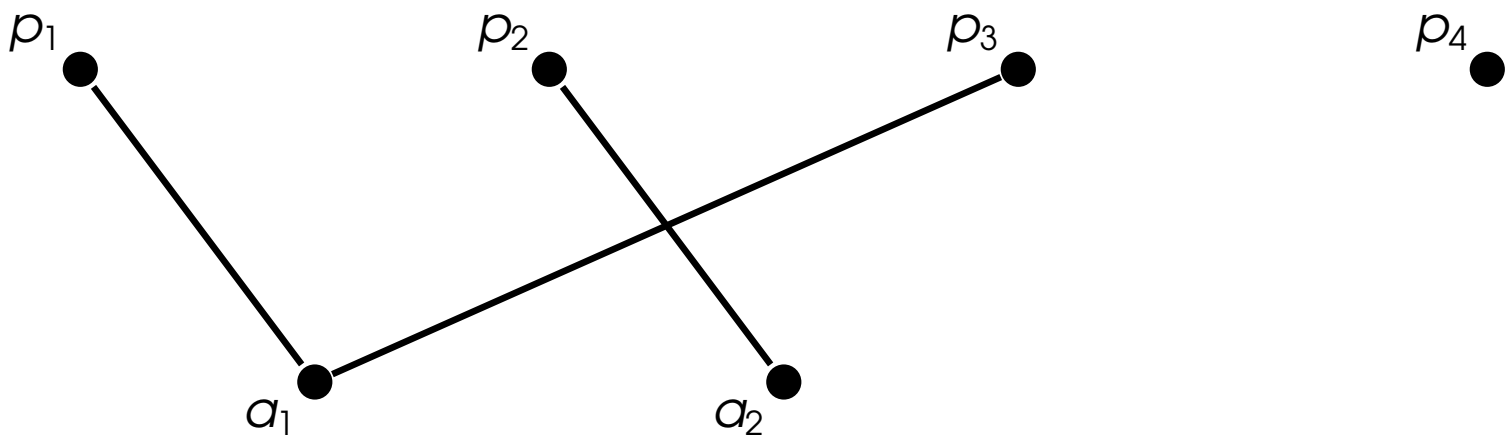
$$\mathbb{P}\left(X \cdot s^T = 0\right)$$

Can be easily calculated, for some IQP computations, if one knows s.

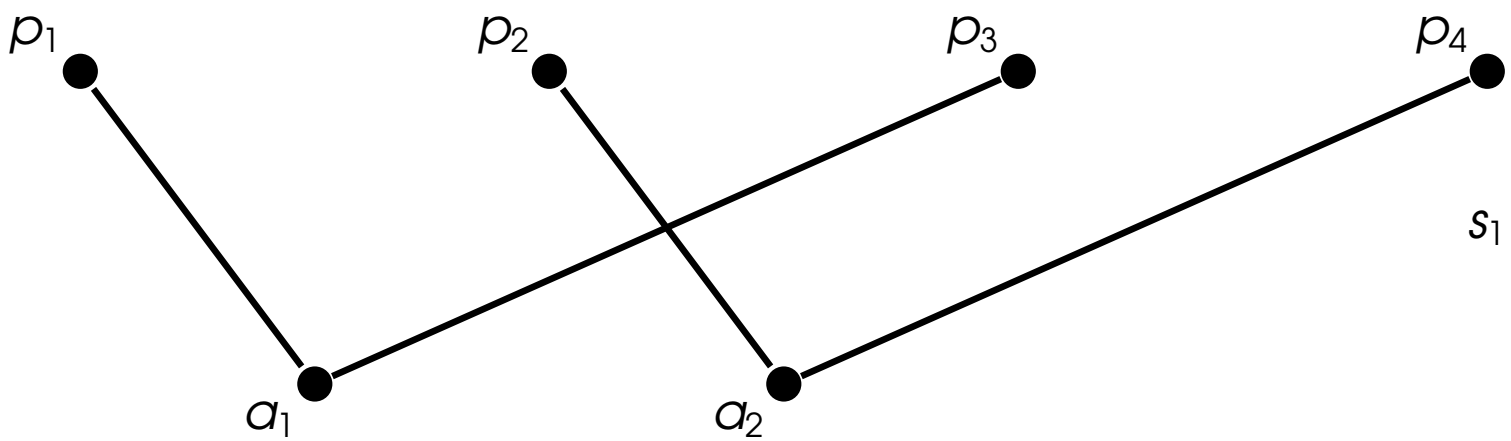
Hypothesis Test



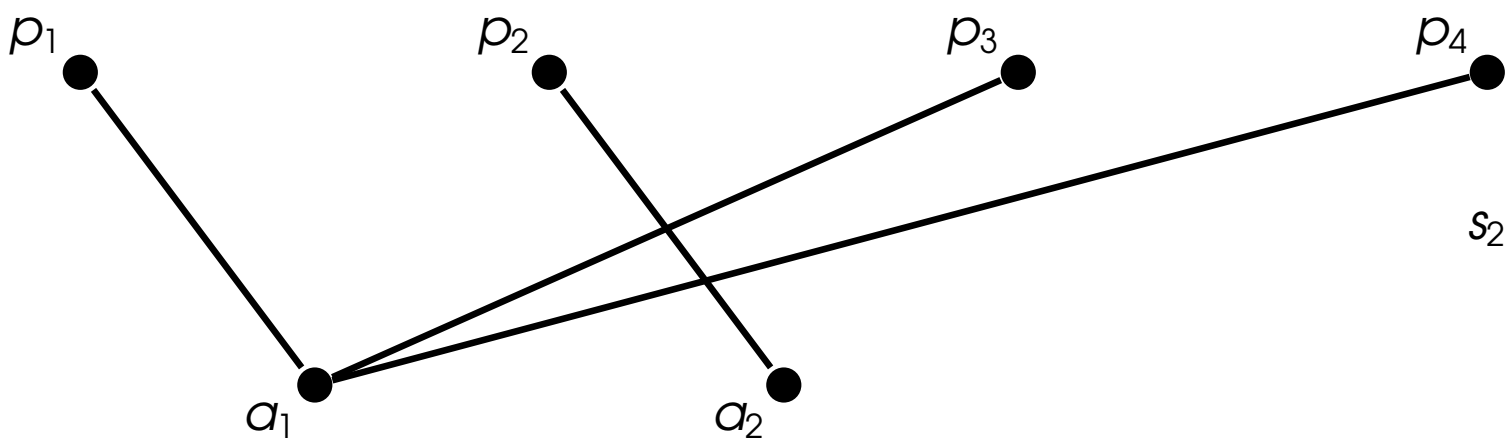
Hypothesis Test



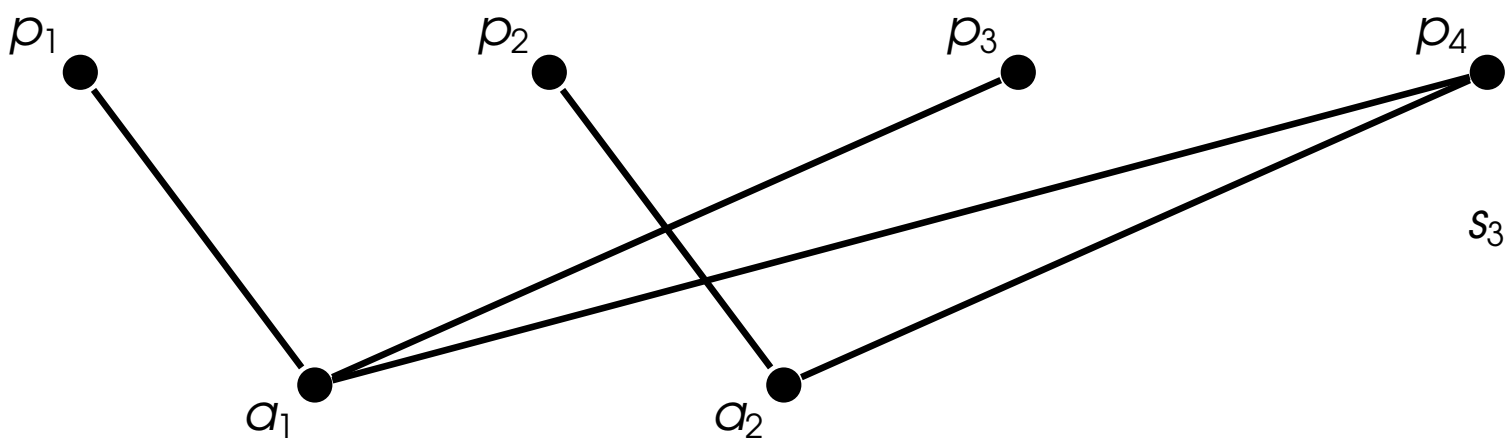
Hypothesis Test



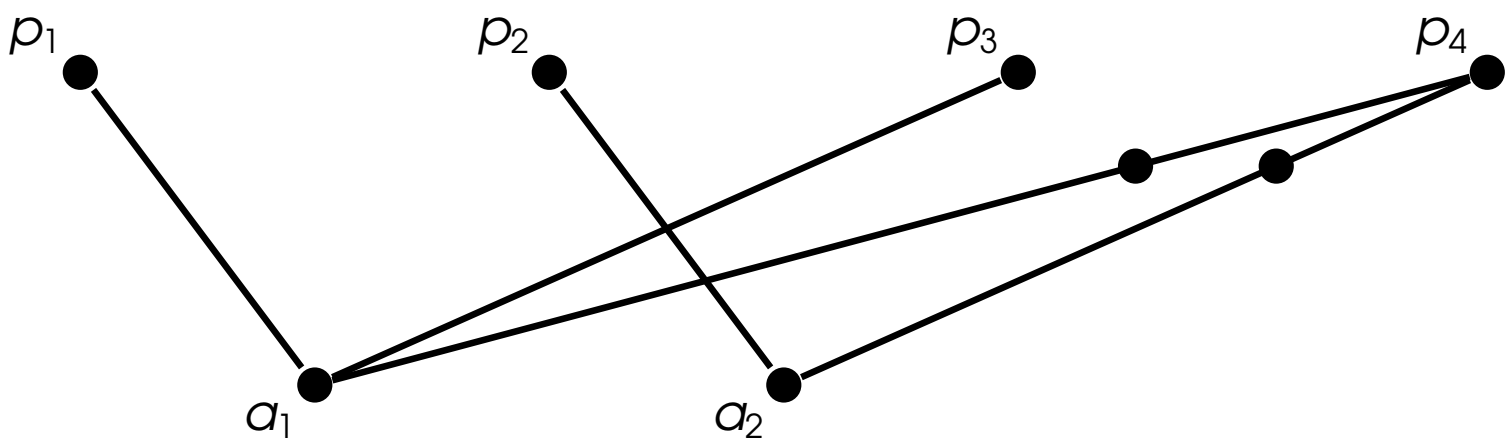
Hypothesis Test



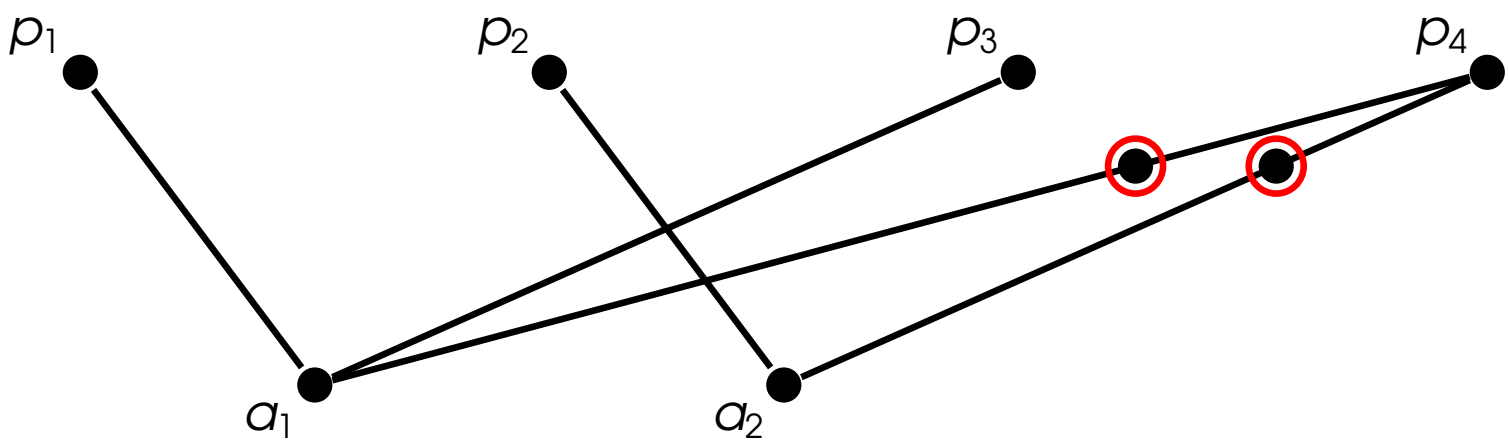
Hypothesis Test



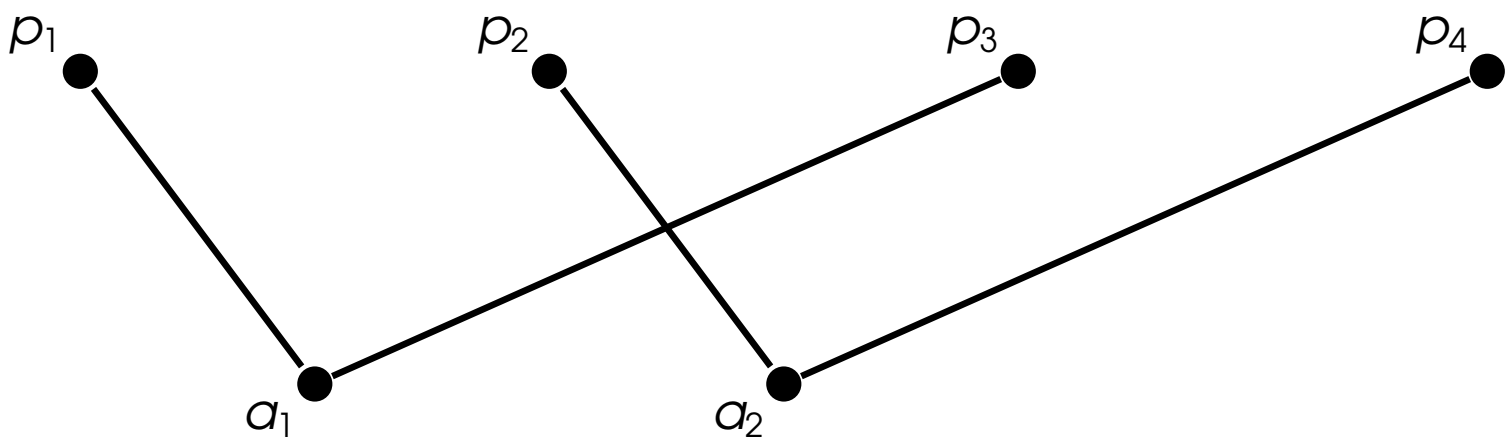
Hypothesis Test

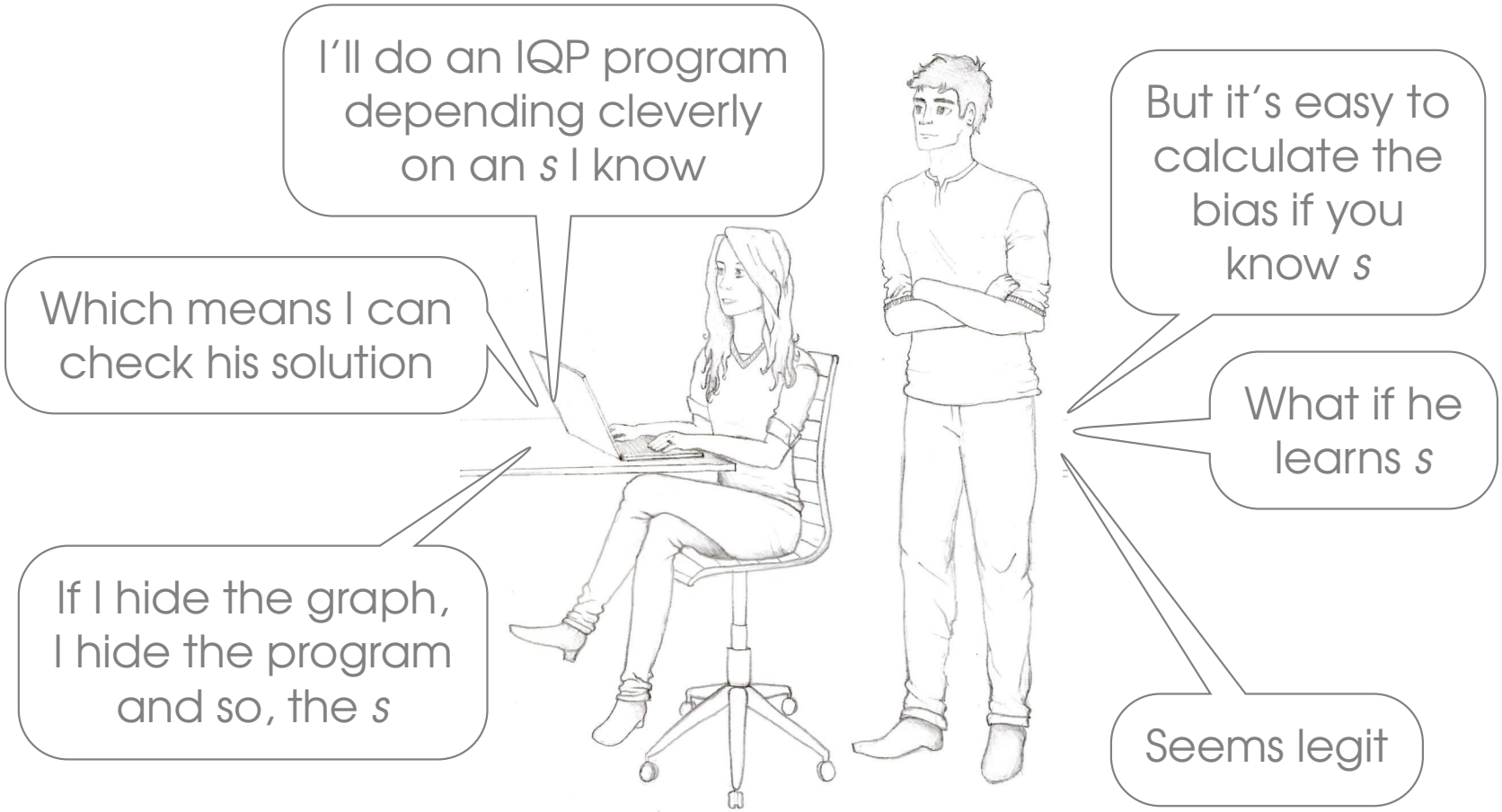


Hypothesis Test



Hypothesis Test




I'll do an IQP program depending cleverly on an s I know
But it's easy to calculate the bias if you know s
Which means I can check his solution
What if he learns s
If I hide the graph, I hide the program and so, the s
Seems legit

Three conditions for a successful hypothesis test:

- The Server must complete a hard IQP computations
  - Computation bias is calculated for is hard
- The Client knows a secret allowing them to check the outcome
  - The Client knows the direction s
- The Server hides the secret something
  - Using blind IQP


Thank you for listening
Any questions?

Bibliography

(FK) - Joseph F. Fitzsimons and Elham Kashefi, *Unconditionally Verifiable Blind Quantum Computation*, arXiv preprint arXiv:1203.5217 (2012).
(SB) - Dan Shepherd and Michael J. Bremner, *Temporally Unstructured Quantum Computation*, Proc. R. Soc. A 465, 1413–1439 (2009).
(V) - Dunjko, Vedran, et al, *Composable security of delegated quantum computation*, International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg (2014).

Thanks to:

EPSRC
Engineering and Physical Sciences Research Council

EPSRC Centre for Doctoral Training in Pervasive Parallelism

THE UNIVERSITY of EDINBURGH informatics