

---

# Universal Blind Quantum Computation

---

Anne Broadbent (Institute for Quantum Computing,  
University of Waterloo)

with

Joseph Fitzsimons (University of Oxford)

Elham Kashefi (Grenoble & Edinburgh)

China Theory Week  
September 2008

# Quantum Computers

- Quantum Computer: operates on quantum states

- Qubits  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$   
 $\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$       $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  and  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

- Evolution: unitary operators  $UU^\dagger = I$

- Computations given as quantum circuits. Universal set of gates:

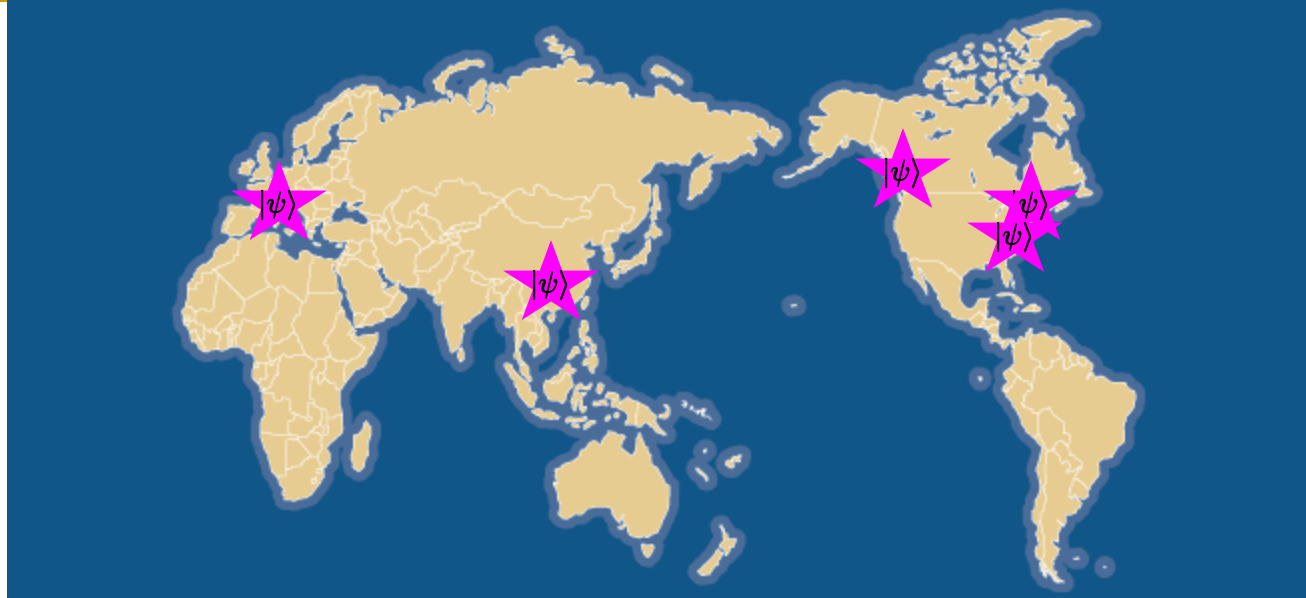
$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pi/8 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}, \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

- Reading output: measurement

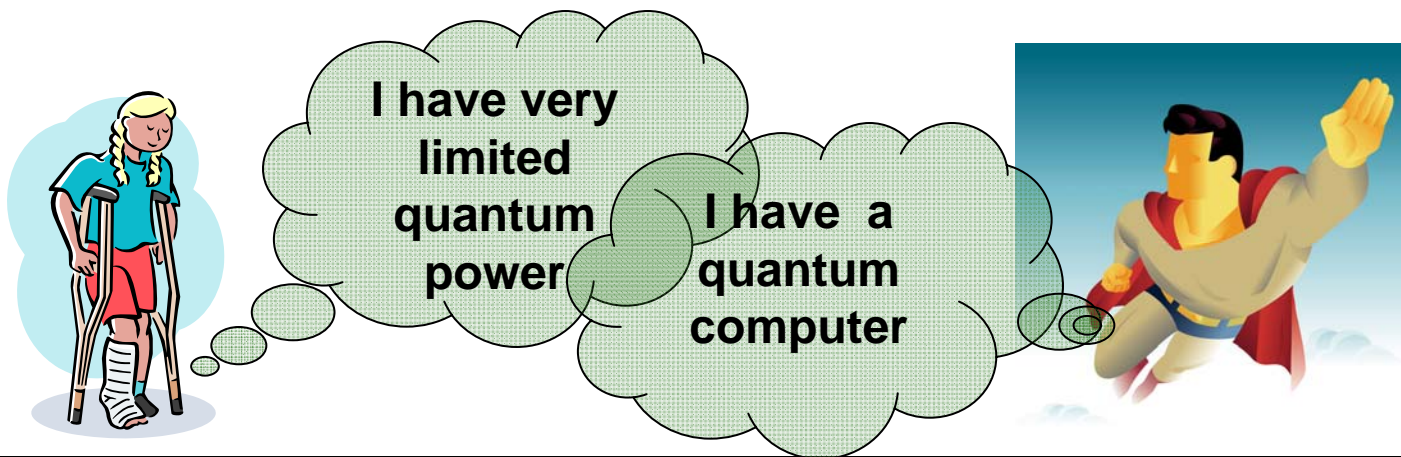
$$\alpha|0\rangle + \beta|1\rangle \begin{cases} 0 \text{ with probability } |\alpha|^2 \\ 1 \text{ with probability } |\beta|^2 \end{cases}$$

- Quantum computers can factor in polynomial time: Shor's algorithm

20??



- In the future, users of quantum computers will probably have access to a handful of central machines.
- How can users keep their inputs private?



| inputs - outputs                       | Application   |
|--|---|
| Classical-classical<br>(in <b>NP</b> ) | factoring using Shor's algorithm  |
| Classical-Classical<br>(other)         | <b>BQP</b> -complete problem such as approximation of the Jones polynomial. |
| Classical-Quantum                      | Quantum state preparation   |
| Quantum-Classical                      | <b>QMA</b> : Alice is a quantum verifier in an interactive proof            |
| Quantum-Quantum                        | <b>QIP</b> : Alice is a verifier in a multi-round quantum interactive proof |

# Previous classical work

## Encrypting Problem Instances

Or ... , Can You Take Advantage of Someone  
Without Having to Trust Him?

Joan Feigenbaum\*

Computer Science Department  
Stanford University  
Stanford, CA 94305

CRYPTO 85

$f$  is *encryptable* if it fits in the diagram and  $x'$  does not reveal anything about  $x$

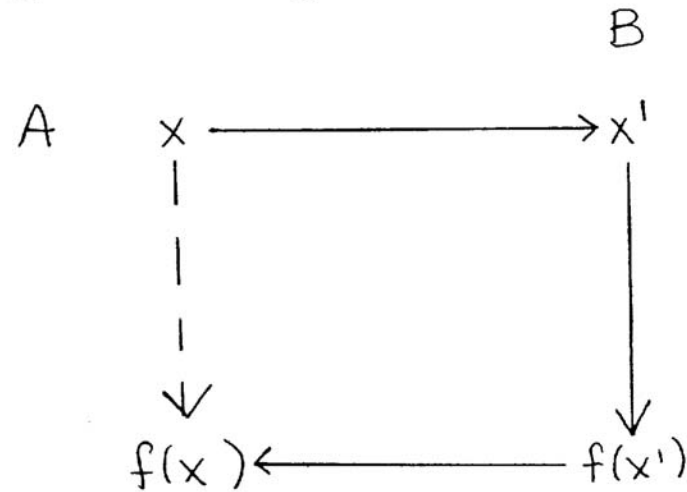


Figure 1. Because the diagram commutes, A learns the value of  $f(x)$ . A does the inexpensive computations  $x \rightarrow x'$  and  $f(x') \rightarrow f(x)$ . B does the expensive computation  $x' \rightarrow f(x')$ .

# Previous classical work

## On Hiding Information from an Oracle\*

|                             |                              |
|-----------------------------|------------------------------|
| Martín Abadi <sup>†</sup>   | Joan Feigenbaum <sup>‡</sup> |
| DEC Systems Research Center | AT&T Bell Laboratories       |
| 130 Lytton Avenue           | 600 Mountain Avenue          |
| Palo Alto, CA 94301         | Murray Hill, NJ 07974        |
| Joe Kilian <sup>§</sup>     |                              |
| MIT                         |                              |
| 545 Technology Square       |                              |
| Cambridge, MA 02139         | STOC 1987                    |

- Impossibility result: No NP-hard function is encryptable (even allowing errors and polynomial interaction) unless the polynomial hierarchy collapses at the third level.

---

# Previous quantum work

MIT-CTP #3211

## Secure assisted quantum computation

Andrew M. Childs\*  
*Center for Theoretical Physics  
Massachusetts Institute of Technology  
Cambridge, MA 02139, USA  
(7 November 2001)*

- Alice must have a quantum memory and must be able to apply certain one-qubit gates.

## Blind quantum computation

Pablo Arrighi<sup>1,\*</sup> and Louis Salvail<sup>2,†</sup>  
<sup>1</sup>*Laboratoire Leibniz, Institut d'Informatique et de Mathématiques Appliquées de Grenoble (IMAG),  
CNRS UMR 5522, 46 Avenue Félix Viallet, 38031 Grenoble Cedex, France.*  
<sup>2</sup>*BRICS, Department of Computer Science, University of Aarhus,  
Building 540, Ny Munkegade, Aarhus C-8000, Denmark.*

- Applies only to a restricted class of publicly known classical functions.

---

# Our contribution

- Works for any polynomial-size quantum circuit; inputs and outputs can be classical or quantum.
- Perfect privacy, no matter what Bob does.
- Uncooperative Bob is detected with optimal probability.
- Alice only needs to be able to prepare single qubits chosen randomly in:

$$\left\{ \frac{1}{\sqrt{2}} (|0\rangle + e^{i\theta} |1\rangle) \mid \theta \in \left\{ \frac{n\pi}{8}, n = 0, 1, \dots, 15 \right\} \right\}$$

---

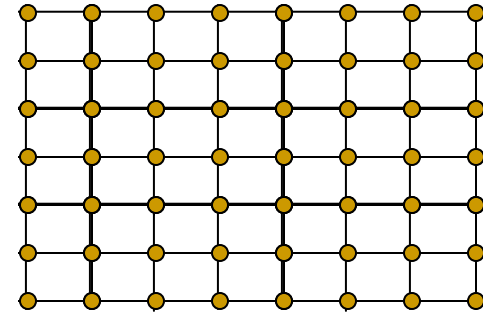
---

# A new paradigm for quantum computing

## Measurement Based quantum computing (MBQC)

Raussendorf and Briegel, 2001

1. Start with *cluster state*
2. Perform  $\sigma_z$  measurements, depending on underlying circuit
3. Perform x-y plane measurements adaptively, layer by layer



---

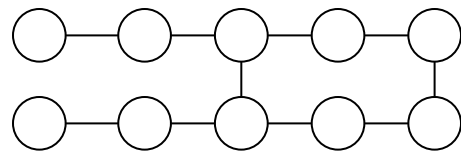
# Main idea of protocol

- Perform a distributed version of MBQC:
  - Alice prepares the qubits.
  - Bob does two-qubit gates and measurements.
  - Alice drives the computation by providing measurement angles.
- Add privacy:
  - Get rid of  $\sigma_z$  measurements
  - Encrypt the measurement angles

---

# Getting rid of $\sigma_z$ measurements

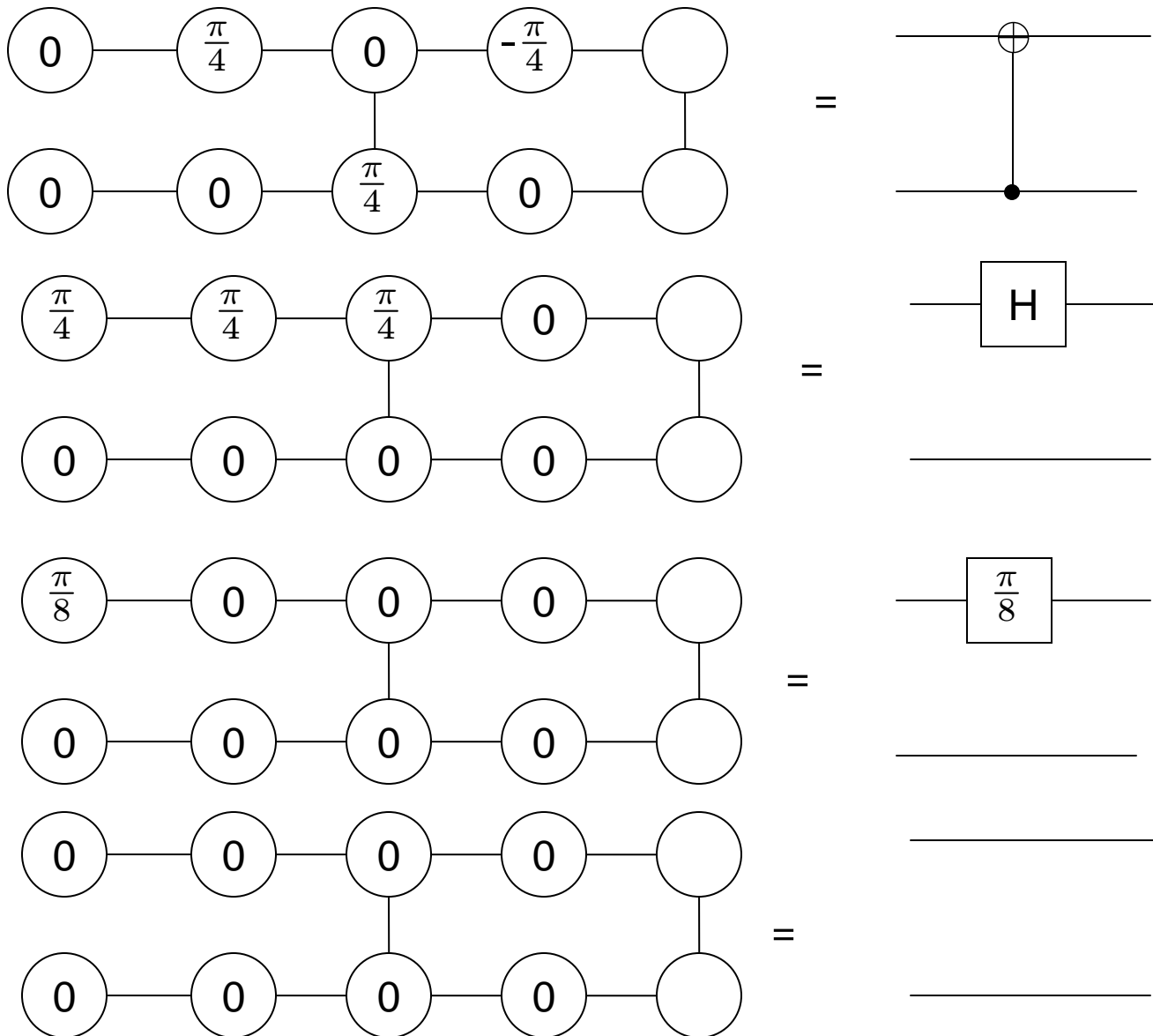
- We want to get rid of  $\sigma_z$  measurements that reveal the structure of underlying circuit
- We'll show that



yields universal set of gates.

- Tiling the 2-qubit gate enables us to handle multiple inputs

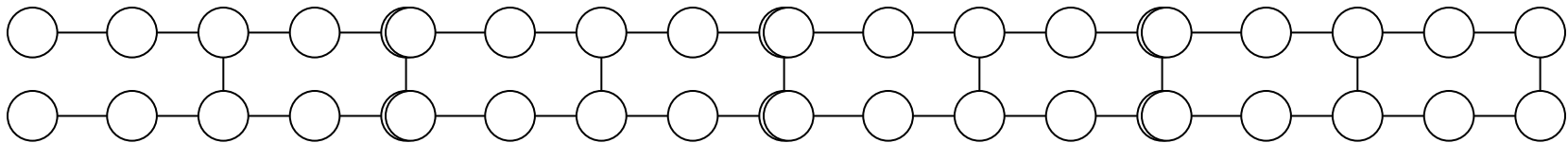
# Getting rid of $\sigma_z$ measurements



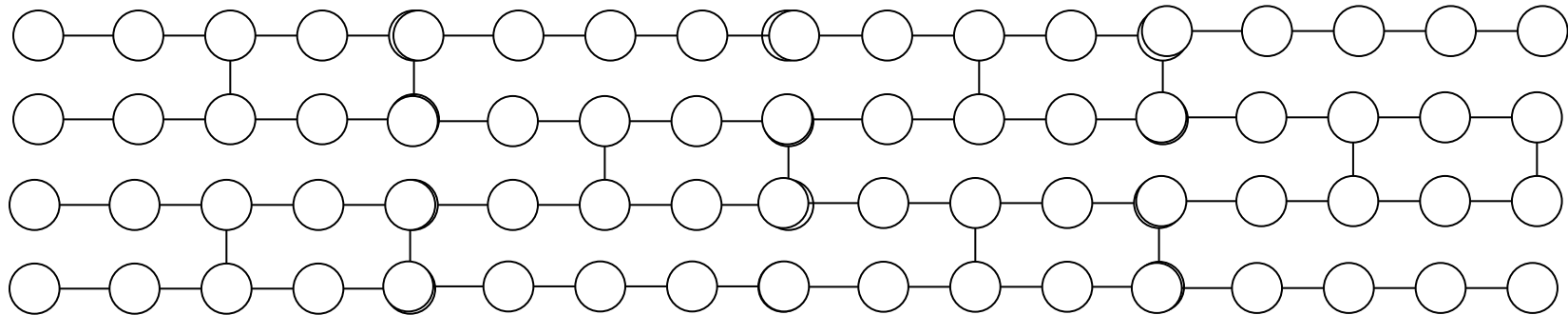
# Getting rid of $\sigma_z$ measurements

## The *brickwork* states

2-qubit circuit



4-qubit circuit



$n$ -qubit circuit...

All measurements are in  $\{\frac{n\pi}{8}, n = 0, 1, \dots, 7\}$

---

# Encrypting the measurement angles

- $Z(\alpha)$  -rotation:  $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\theta+\alpha)}|1\rangle)$
- Applying  $Z(\alpha)$  to a qubit and measuring in  $\alpha + \beta$  basis: result is as if no rotation was applied.
- Ctrl-Z gates commute with Z-rotations.

# Blind Quantum Computation Protocol

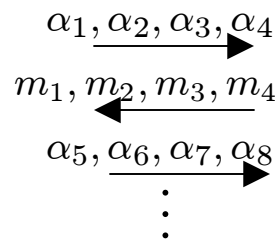


- prepares qubits randomly chosen in  $\left\{ \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \left\{ \frac{n\pi}{8}, n = 0, 1, \dots, 15 \right\} \right\}$ 
  - $|\uparrow\rangle \quad |\downarrow\rangle \quad |\leftarrow\rangle \quad |\searrow\rangle$
  - $|\uparrow\rangle \quad |\rightarrow\rangle \quad |\leftarrow\rangle \quad |\leftarrow\rangle$
  - $|\nearrow\rangle \quad |\uparrow\rangle \quad |\uparrow\rangle \quad |\rightarrow\rangle$

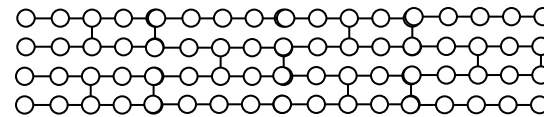
- chooses x-y plane measurement angles, adaptively, layer by layer

$$\phi' = (-1)^{s_x} \phi + \pi s_z$$

$$\alpha = \phi' + \theta + \pi r$$

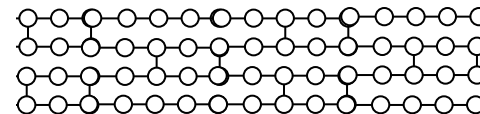


- entangles according to **brickwork state**



- single-qubit measurements in basis

$$\left\{ \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle) \right\}$$



# Privacy

- Universality of the brickwork state guarantees that graph state does not reveal anything on the underlying computation.
- The only thing that Alice needs to hide is the angles:
- Fix a single qubit. Bob sees  $\alpha$ . Because  $\theta$  and  $r$  are chosen uniformly at random, from Bob's point of view, with equal probability, one of the following two has occurred:
  1.  $r = 0$  so  $\alpha = \phi' + \theta$  and  $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\alpha - \phi')}|1\rangle)$ .
  2.  $r = 1$  so  $\alpha = \phi' + \theta + \pi$  and  $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i(\alpha - \phi')}|1\rangle)$ .
- For any choice of  $\phi'$ , the density matrix for this system is totally mixed, hence Bob can't distinguish between Alice's different choices of measurement angles.

---

# Extensions

- We have extended our protocol to allow:
  - quantum inputs
  - quantum outputs
  - detection of uncooperative Bob

---

# Conclusion

- Is our protocol optimal for Alice?
  - one-qubit random preparation is pretty minimal
- Find other applications of measurement-based quantum computing to distributed tasks