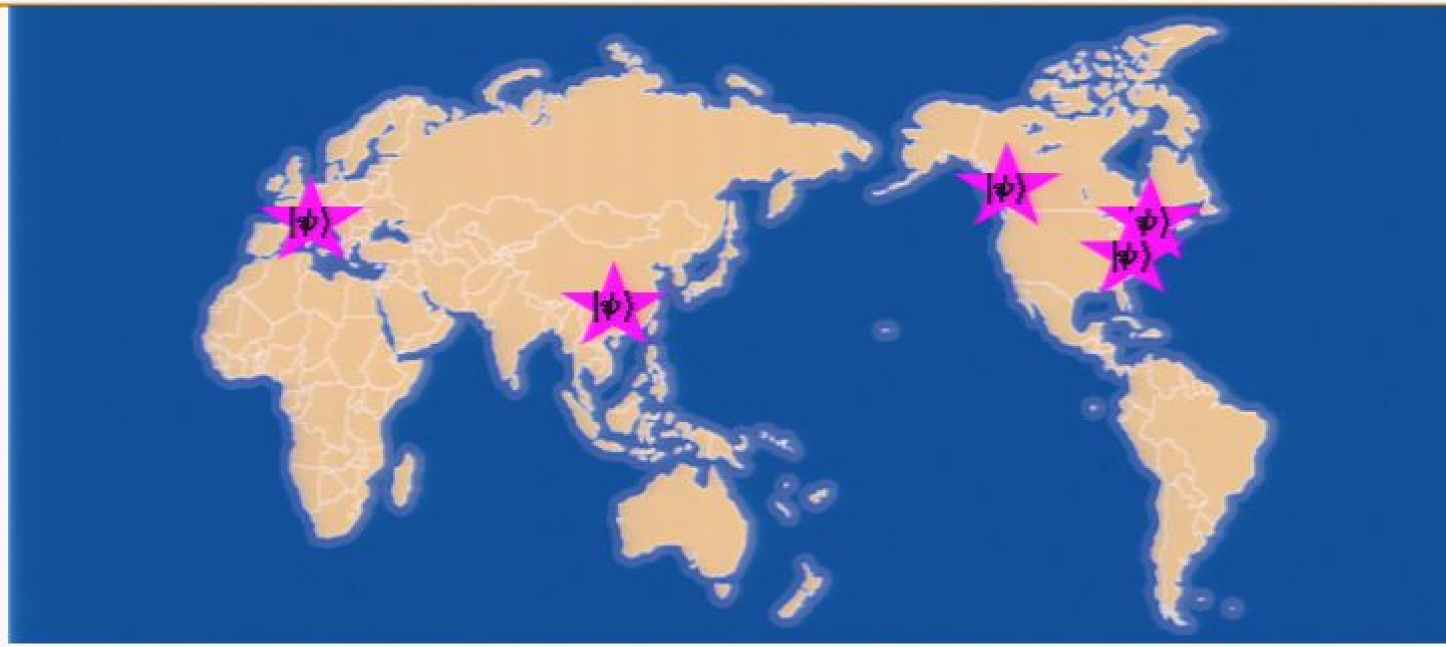
Title: Universal Blind Quantum Computation

Date: May 02, 2008 09:00 AM

URL: http://pirsa.org/08050032

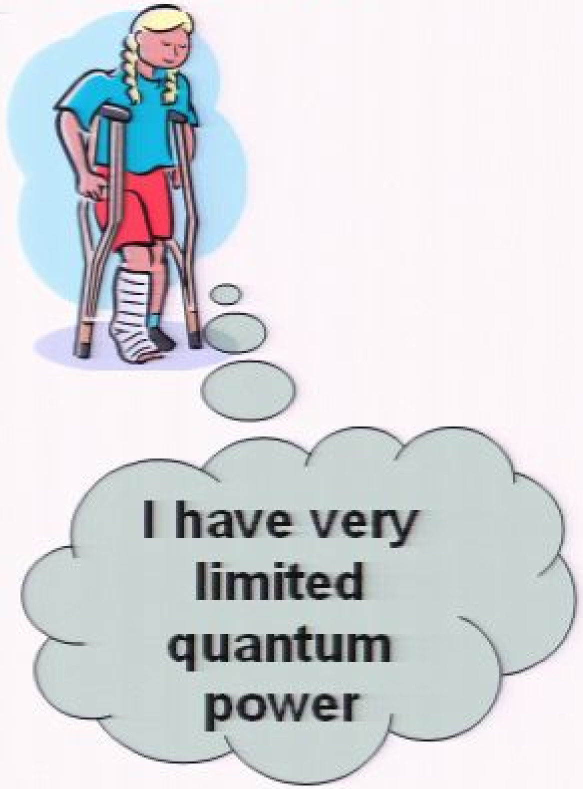
Abstract: I will present a new protocol that was developed entirely in the measurement-based model for quantum computation. Our protocol allows Alice to have Bob carry out a quantum computation for her such that Alice\'s inputs, outputs and computation remain perfectly private, and where Alice does not require any quantum computational power or memory. Alice only needs to be able to prepare single qubits from a finite set and send them to Bob, who has the balance of the required quantum computational resources. Our protocol is interactive: after the initial preparation of quantum states, Alice and Bob use two-way classical communication which enables Alice to drive the computation, giving single-qubit measurement instructions to Bob, depending on previous measurement outcomes. Our protocol is efficient and is presented for the special case of a classical-input, and classical-output; modifications allow the general case of quantum inputs and outputs. We also discuss the use of authentication in order for Alice to detect an uncooperative Bob. Based on joint work with Joseph Fitzsimons and Elham Kashefi

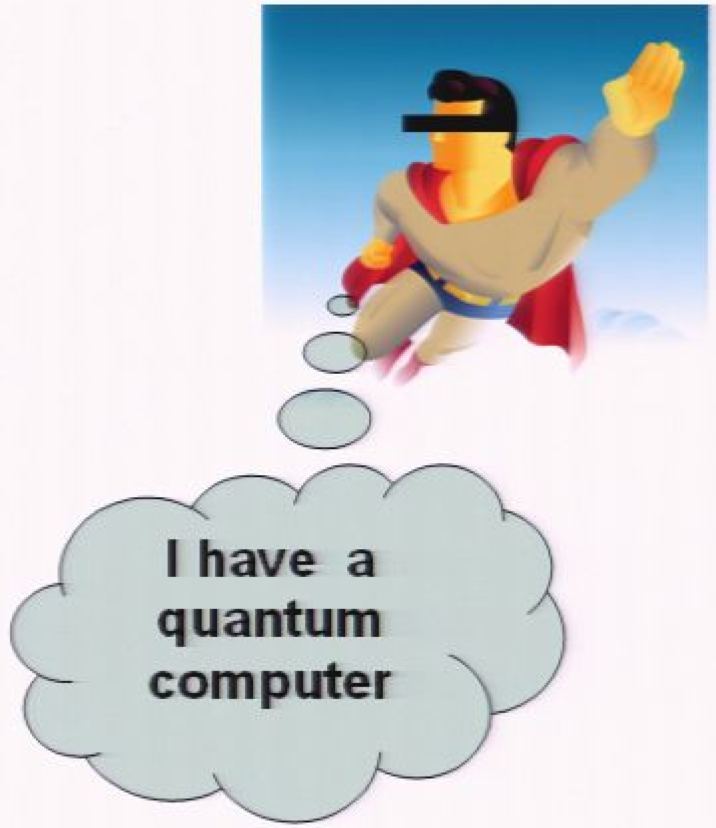
20??



- How can users of quantum computers keep their inputs private?

Applications



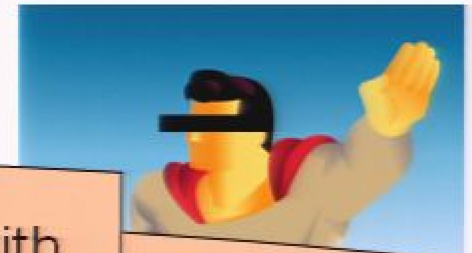


Applications

Applications

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

Applications



We accomplish all of these with information-theoretic privacy & detection of uncooperating Bob

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

Previous 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 has a quantum memory, and can perform Pauli gates

Previous 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 has a quantum memory, and can perform Pauli gates
- Idea: she sends encrypted qubits to Bob who applies a known gate. Alice can decrypt the qubits while preserving the action of the gate. Repeat, cycling through universal set of gates.

Private Quantum Channels

A. Ambainis, M. Mosca, A.Tapp and R. De Wolf (2000);

P.O. Boykin and V. Roychowdhury (2000)

- To encrypt a single qubit, it is sufficient to randomly apply one of the following Pauli operators: {I, X, XZ or Z}.
- To encrypt a single qubit in the x-y plane,

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$$

it is sufficient to randomly apply I or Z.

Previous work-quantum

Blind quantum computation

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

- Publicly-known classical random-verifiable function
- Alice gives Bob multiple inputs, most of which are *decoys*.
- Decoys are verified by Alice. She thus detects a cheating Bob but cannot prevent him from learning about her input.

Previous work-quantum

Blind quantum computation

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

- Publicly-known classical random-verifiable function
- Alice gives Bob multiple inputs, most of which are *decoys*.
- Decoys are verified by Alice. She thus detects a cheating Bob but cannot prevent him from learning about her input.

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

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

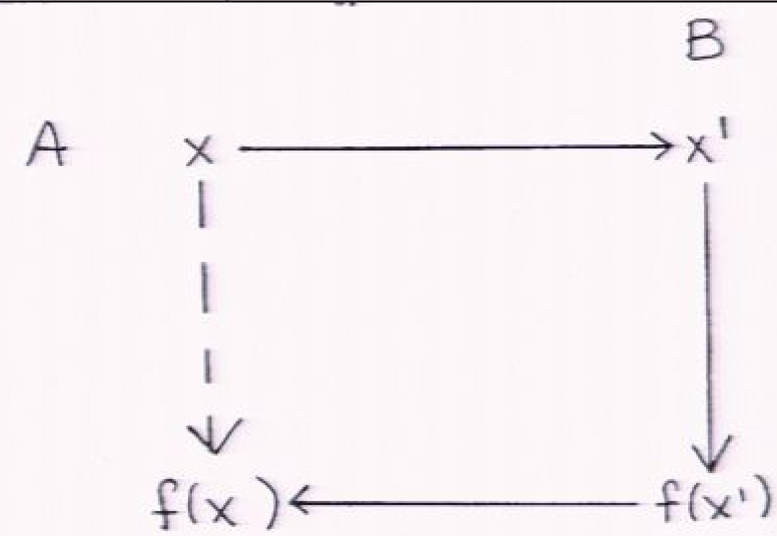


Figure 1. Because the diagram commutes, A learns the value of $f(x)$. A does the inexpensive computations $x \longrightarrow x'$ and $f(x') \longrightarrow f(x)$. B does the expensive computation $x' \longrightarrow f(x')$.

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

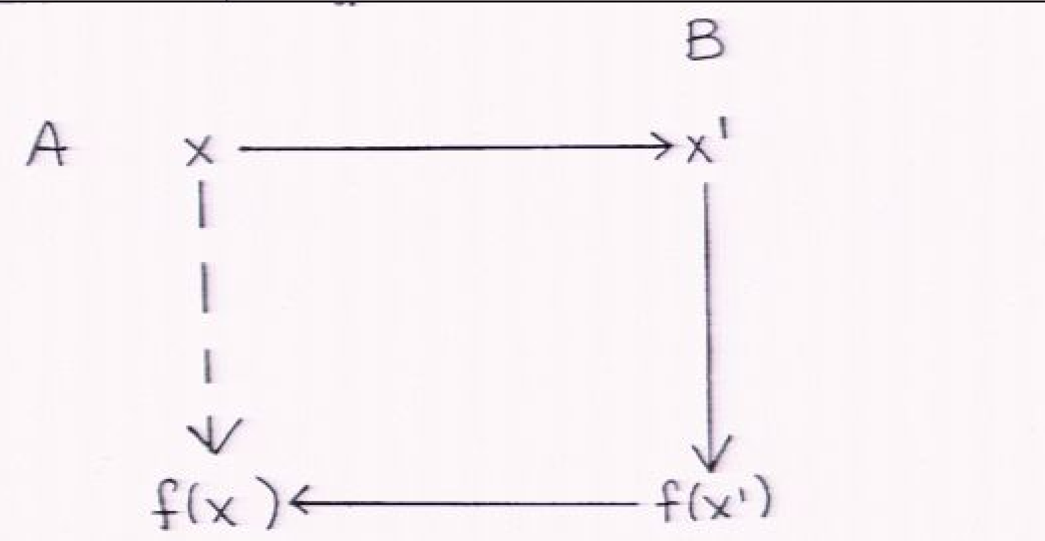


Figure 1. Because the diagram commutes, A learns the value of $f(x)$. A does the inexpensive computations $x \longrightarrow x'$ and $f(x') \longrightarrow f(x)$. B does the expensive computation $x' \longrightarrow f(x')$.

Previous classical work

On Hiding Information from an Oracle*

Martín Abadi†
DEC Systems Research Center
130 Lytton Avenue
Palo Alto, CA 94301

Joan Feigenbaum‡
AT&T Bell Laboratories
600 Mountain Avenue
Murray Hill, NJ 07974

Joe Kilian§
MIT
545 Technology Square
Cambridge, MA 02139

STOC 1987

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

Our contribution

- Works for any polynomial-size circuit, inputs and outputs can be classical or quantum.

Our contribution

- Works for any polynomial-size circuit, inputs and outputs can be classical or quantum.
- Perfect privacy, against a cheating Bob.

Our contribution

- Works for any polynomial-size circuit, inputs and outputs can be classical or quantum.
- Perfect privacy, against a cheating Bob.
- Uncooperative Bob is detected with optimal probability.

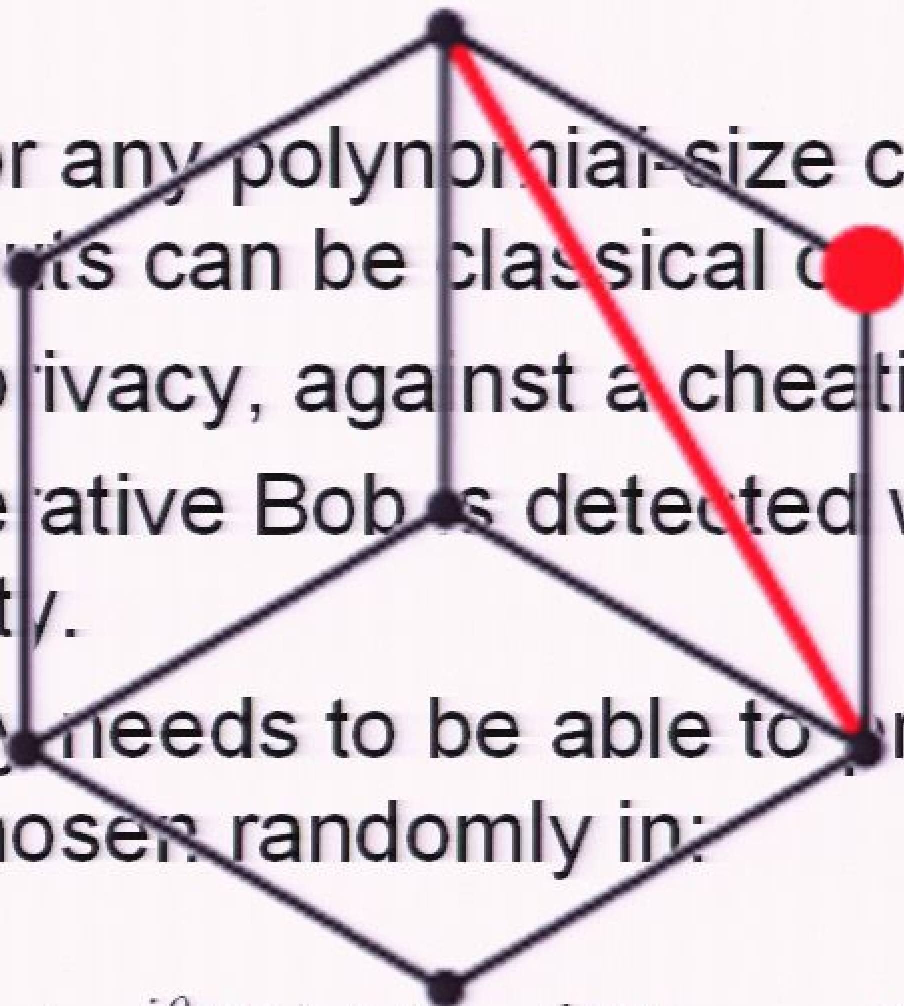
Our contribution

- Works for any polynomial-size circuit, inputs and outputs can be classical or quantum.
- Perfect privacy, against a cheating Bob.
- Uncooperative Bob is detected with optimal probability.
- Alice only needs to be able to prepare single qubits chosen randomly in:

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

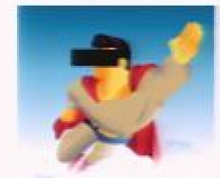
Our contribution

- Works for any polynomial-size circuit, inputs and outputs can be classical or quantum.
- Perfect privacy, against a cheating Bob.
- Uncooperative Bob is detected with optimal probability.
- Alice only needs to be able to prepare single qubits chosen randomly in:

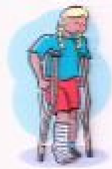


$$\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\frac{n\pi}{8}, n = 0, 1, \ldots, 15\}\}$$

First attempt at blind QC



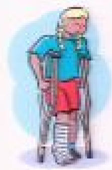
First attempt at blind QC

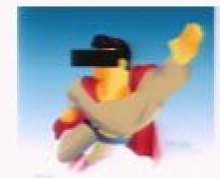


- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

First attempt at blind QC





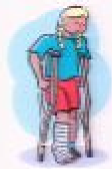
- prepares qubits in state

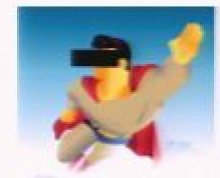
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

→

- entangles according to cluster state

First attempt at blind QC

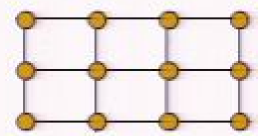




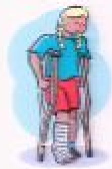
- prepares qubits in state

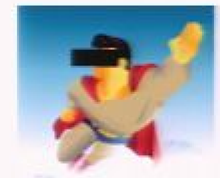
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to cluster state



First attempt at blind QC



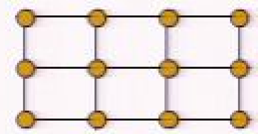


- prepares qubits in state

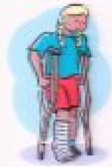
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- chooses σ_z measurements

- entangles according to cluster state



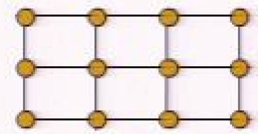
First attempt at blind QC



- prepares qubits in state

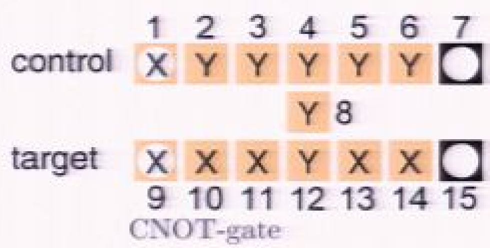
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to cluster state



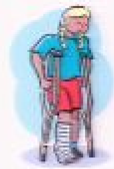
- chooses σ_z measurements

(a)



Raussendorf and Briegel 2001

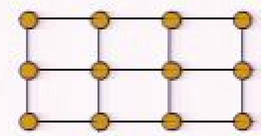
First attempt at blind QC



- prepares qubits in state

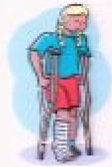
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to cluster state



- chooses σ_z measurements

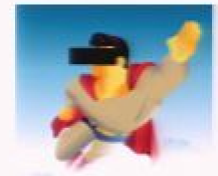
First attempt at blind QC



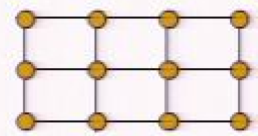
- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- chooses σ_z measurements



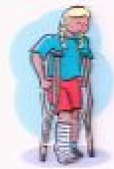
- entangles according to cluster state



- tailors the cluster state

“5”

First attempt at blind QC

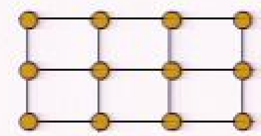


- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

→

- entangles according to cluster state

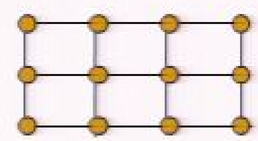


- chooses σ_z measurements

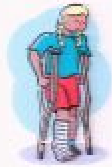
→

- tailors the cluster state

“5”



First attempt at blind QC



- prepares qubits in state

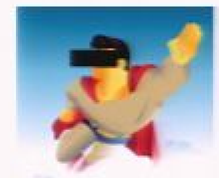
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- chooses σ_z measurements

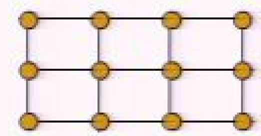
- chooses x-y plane measurement angles, adaptively, layer by layer

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

(s_x and s_z depend on previous measurement outcomes)

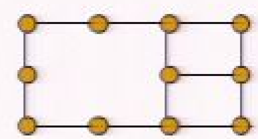


- entangles according to cluster state

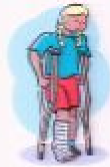


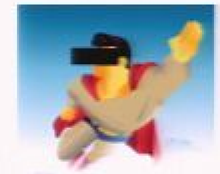
- tailors the cluster state

“5”



First attempt at blind QC



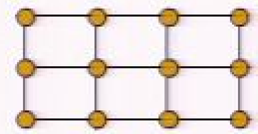


- prepares qubits in state

  $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

  →

- entangles according to cluster state

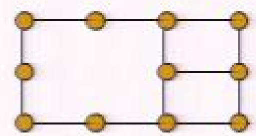


- chooses σ_z measurements

  →

- tailors the cluster state

"5"



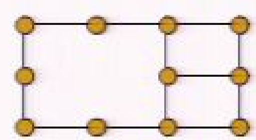
- chooses x-y plane measurement angles, adaptively, layer by layer

  $\phi'_1, \phi'_2, \phi'_3$ →

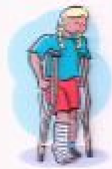
- single-qubit measurements

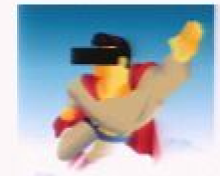
$\phi' = (-1)^{s_x}\phi + \pi s_z$

(s_x and s_z depend on previous measurement outcomes)



First attempt at blind QC

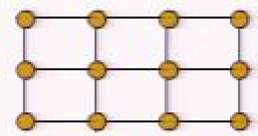




- prepares qubits in state

  $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\longrightarrow$

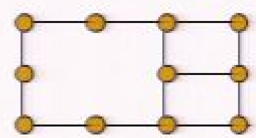
- entangles according to cluster state



- chooses σ_z measurements $\longrightarrow$

- tailors the cluster state

"5"



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

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

  (s_x and s_z depend on previous measurement outcomes)

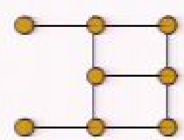
$\xrightarrow{\phi'_1, \phi'_2, \phi'_3}$

$\xleftarrow{m_1, m_2, m_3}$

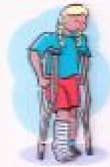
$\xrightarrow{\phi'_4, \phi'_6}$

$\vdots$

- single-qubit measurements



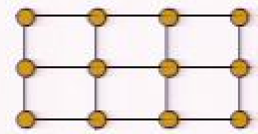
First attempt at blind QC



- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to cluster state

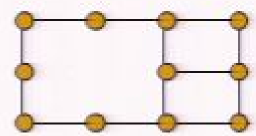


- chooses σ_z measurements

Reveals structure of circuit

- ors the cluster state

"5"



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

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

(s_x and s_z depend on previous measurement outcomes)

$\phi'_1, \phi'_2, \phi'_3$ →

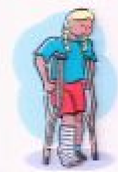
m_1, m_2, m_3 ←

ϕ'_4, ϕ'_6 →

⋮

- single-qubit measurements

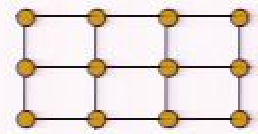
First attempt at blind QC



- prepares qubits in state

  $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

- entangles according to cluster state

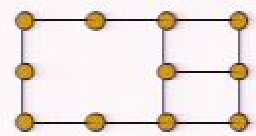


- chooses σ_z measurements

Reveals structure of circuit

- rs the cluster state

"5"



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

  $\phi'_1, \phi'_2, \phi'_3$

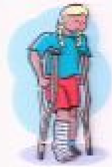
- single-qubit measurements

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

(s_x and s_z depend
previous measureme

Reveals measurement angles

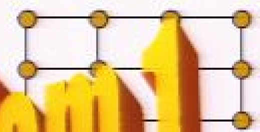
First attempt at blind QC



- prepares qubits in state

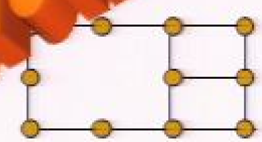
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to cluster state



- chooses σ_z measurements

- ...ster state



Reveals structure of circuit

Problem 1

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

$\phi'_1, \phi'_2, \phi'_3$

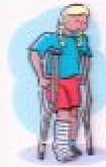
- single-qubit measurements

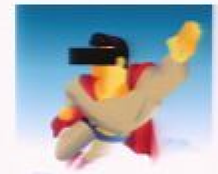
$\phi' = (-1)^{s_x}\phi$ ...

(s_x and s_z depend ... previous measureme...

Reveals measurement angles

First attempt at blind QC

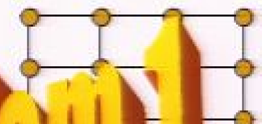




- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to cluster state

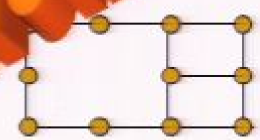


- chooses σ_z measurements

Reveals structure of circuit

Problem 1

- ... ster state



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

$\phi'_1, \phi'_2, \phi'_3$

- single-qubit measurements

$\phi' = (-1)^{s_x}\phi$ ...

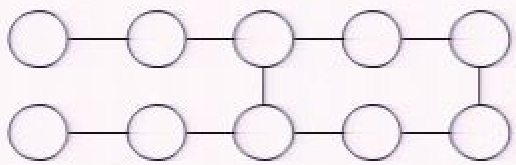
(s_x and s_z depend ... previous measureme...

Reveals measurement angles

Problem 2

Fixing Problem 1

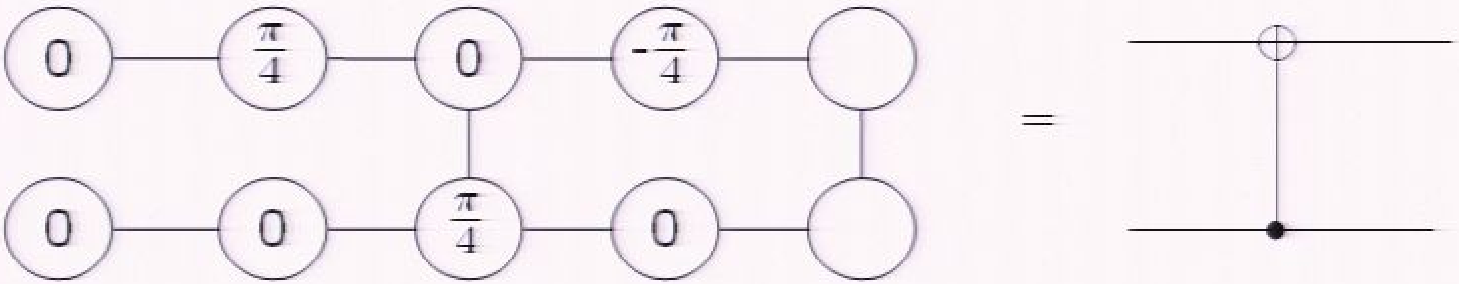
- We want to get rid of σ_z measurements that reveal the structure of underlying circuit
- We'll show that



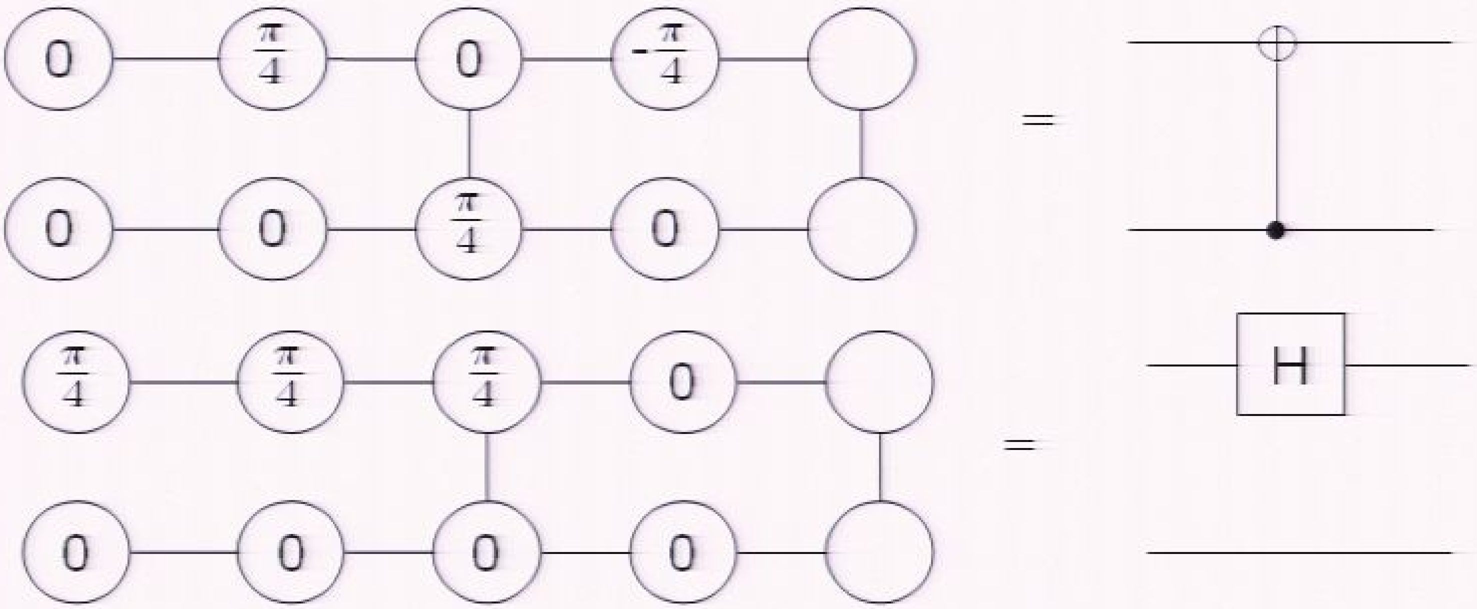
yields universal set of gates:H, pi/8 and CNOT

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

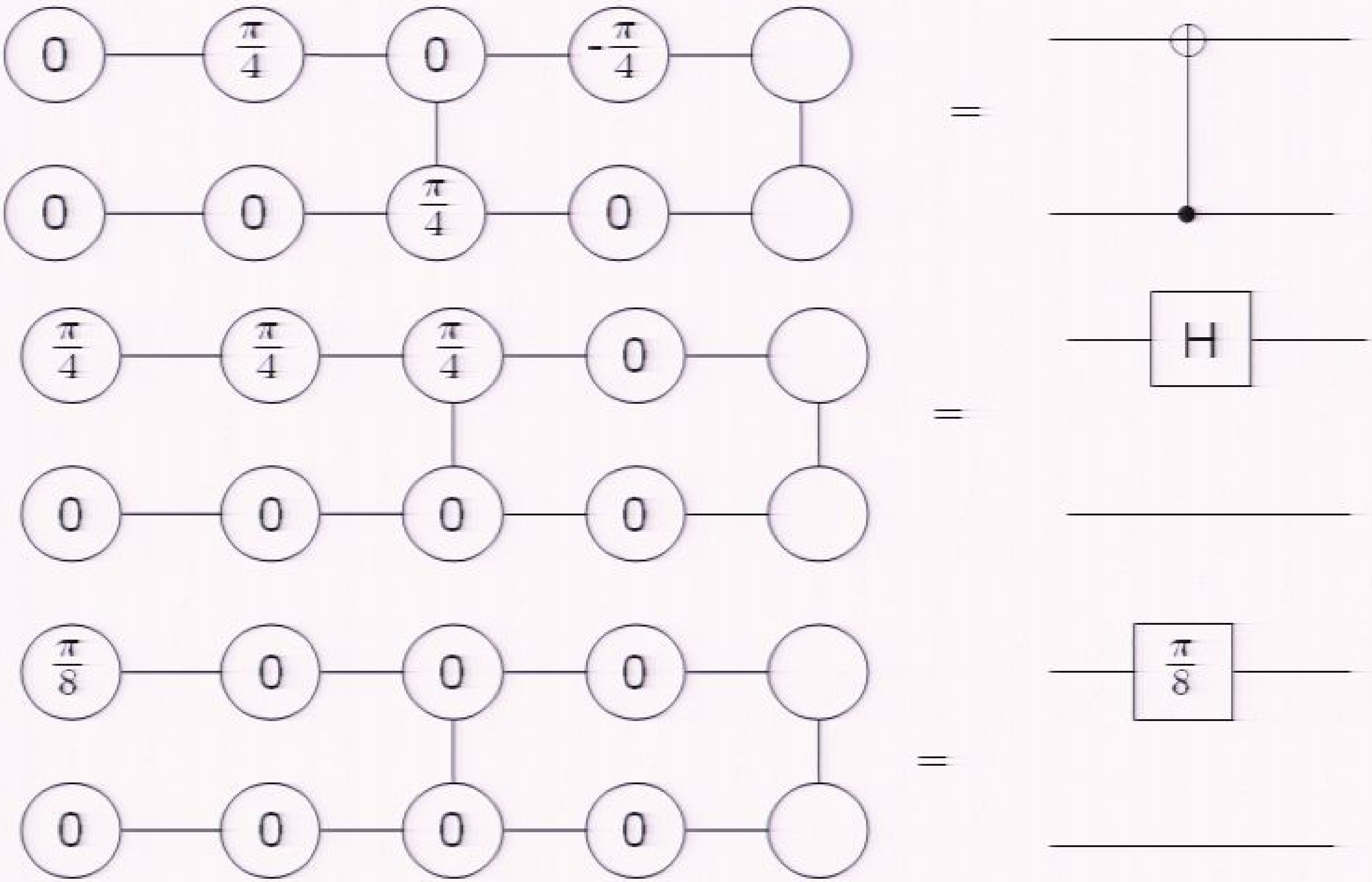
Fixing Problem 1



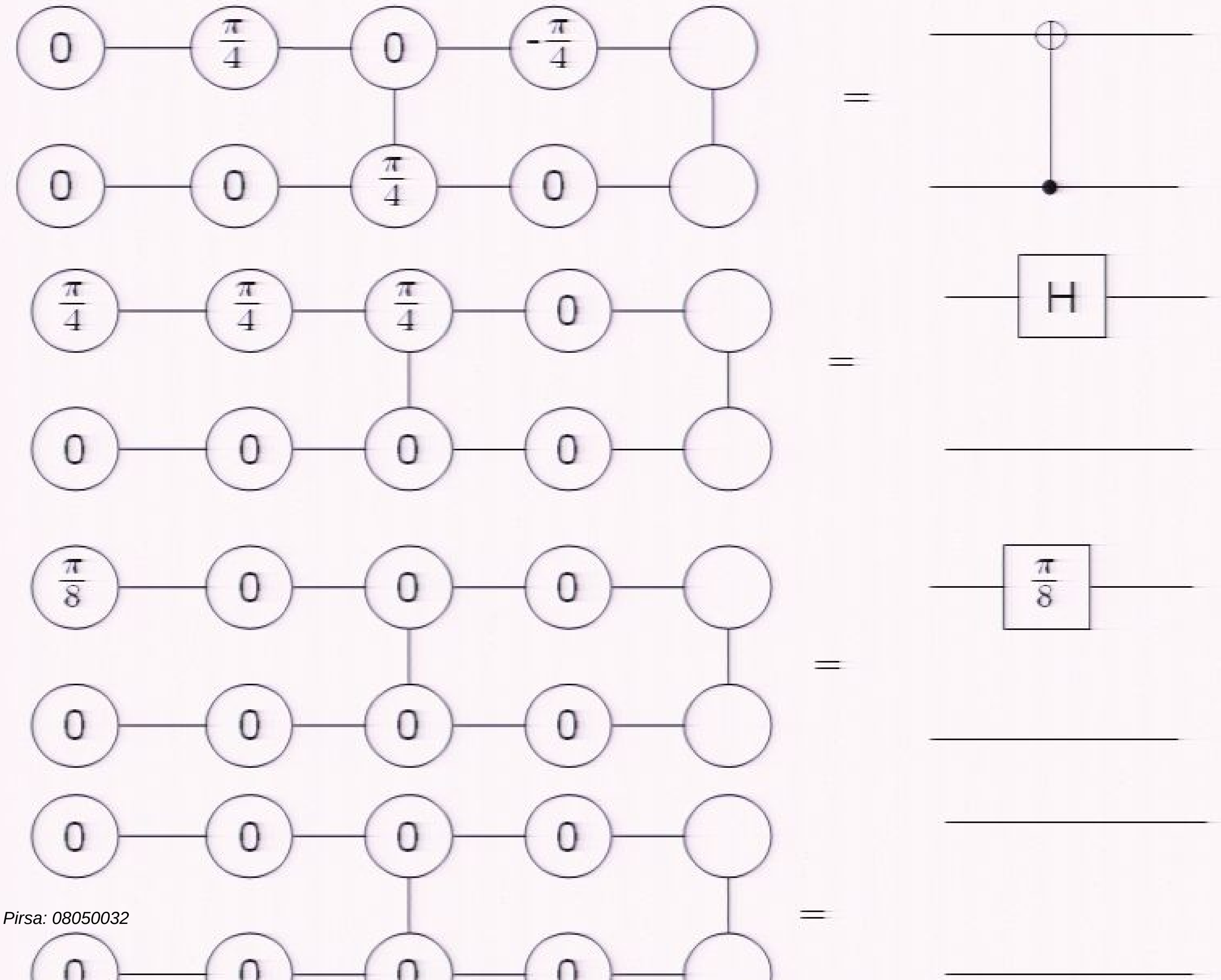
Fixing Problem 1



Fixing Problem 1

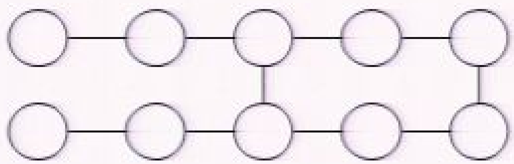


Fixing Problem 1

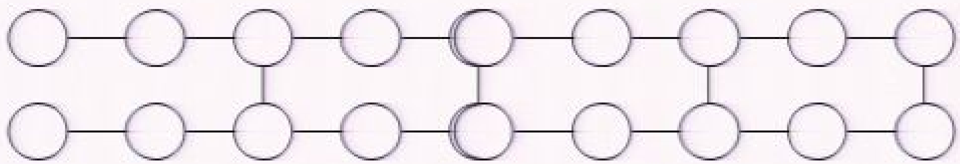


Fixing Problem 1

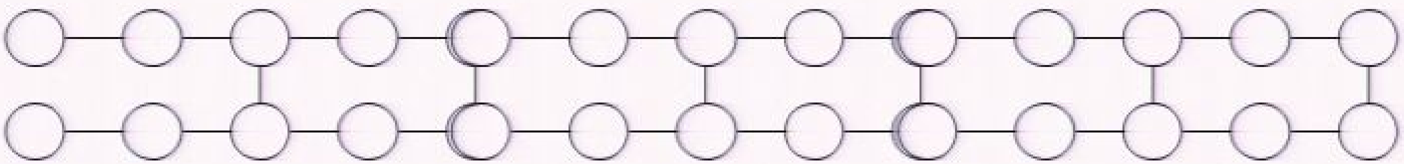
The *brickwork* states



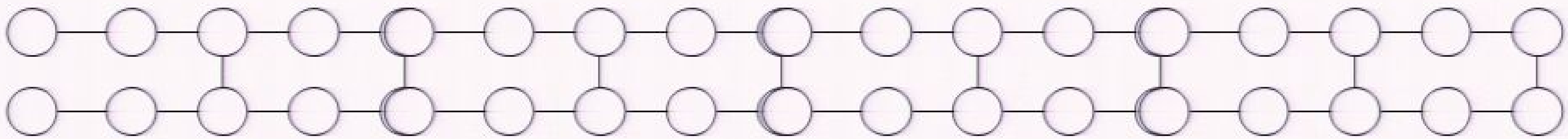
Fixing Problem 1
The *brickwork* states



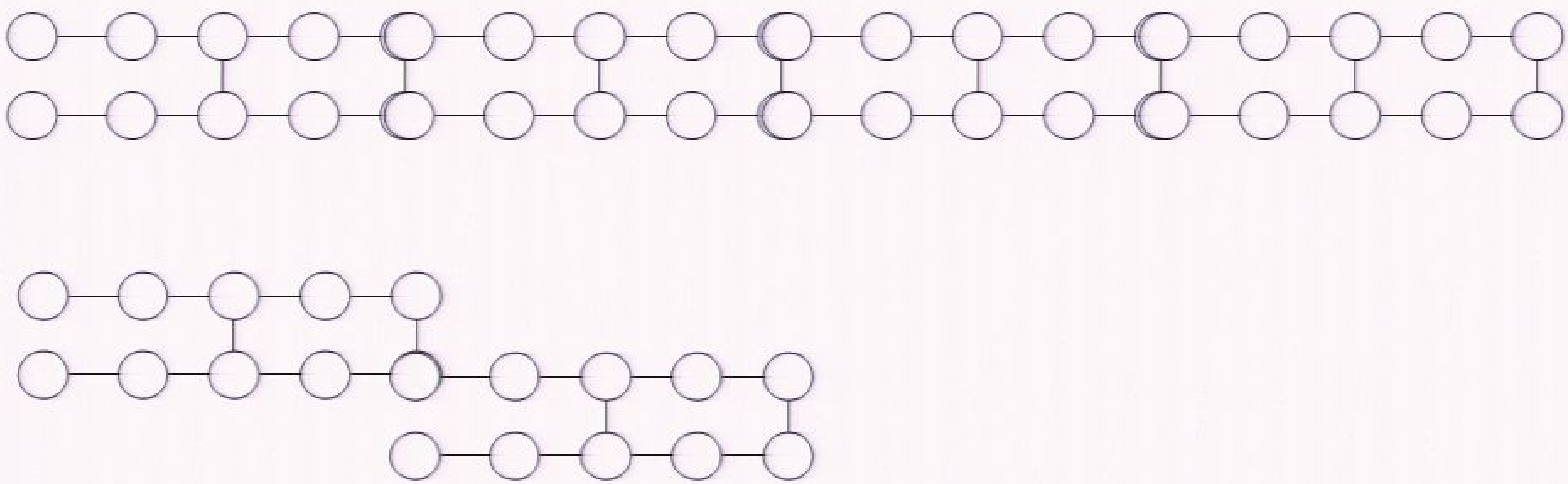
Fixing Problem 1
The *brickwork* states



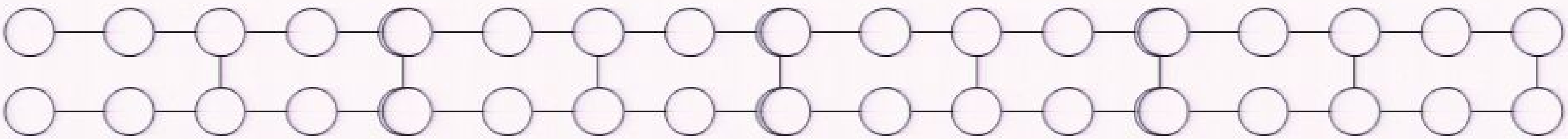
Fixing Problem 1
The *brickwork* states

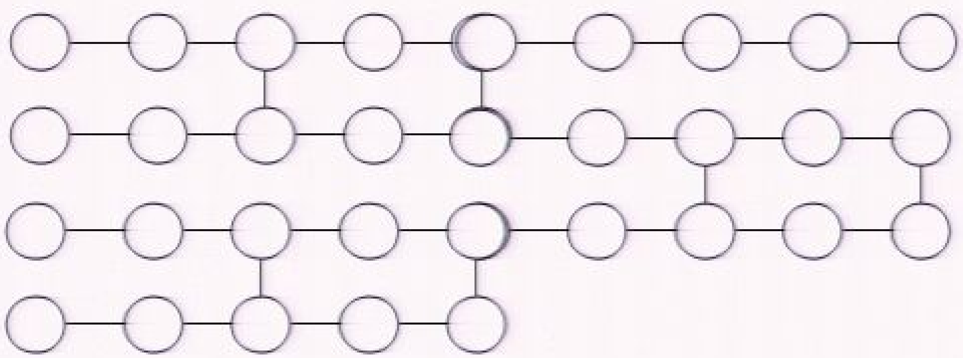


Fixing Problem 1
The *brickwork* states

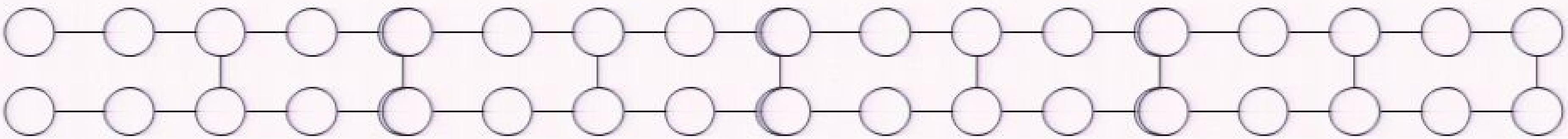


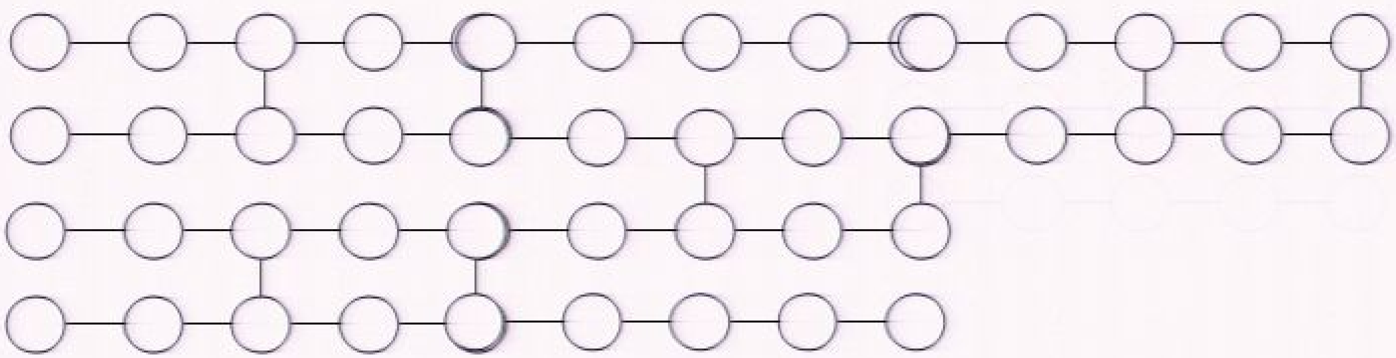
Fixing Problem 1
The *brickwork* states



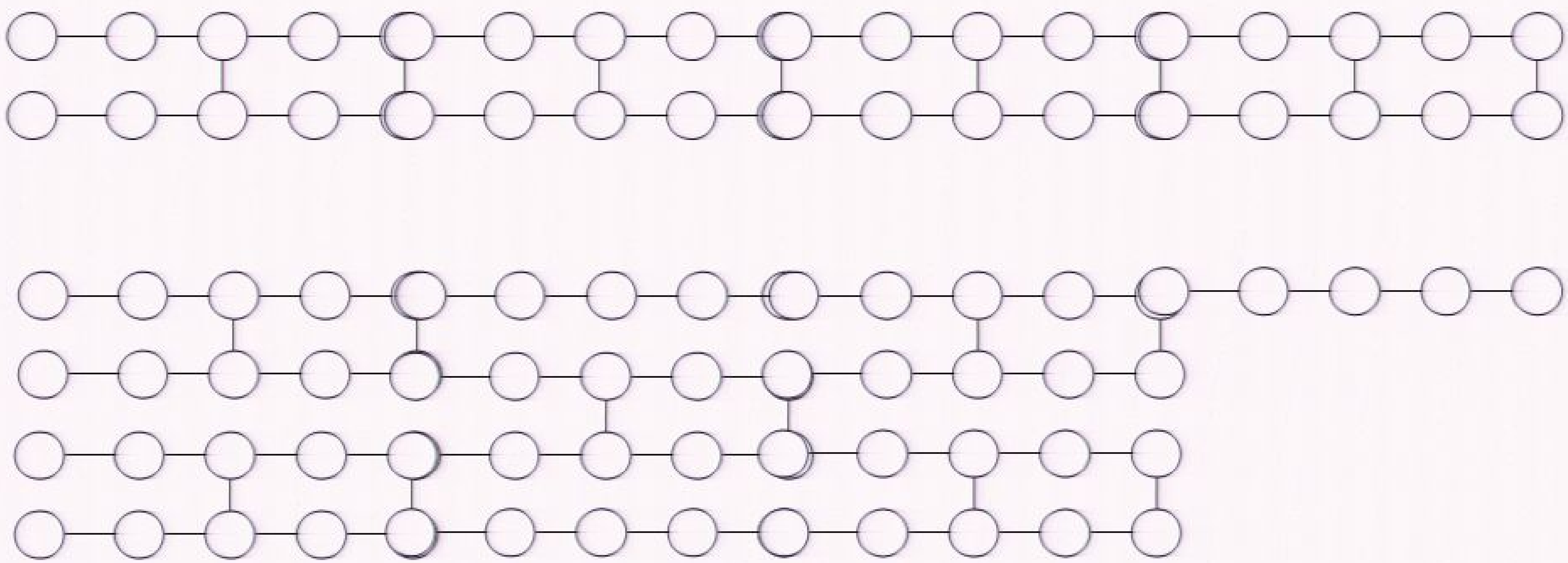


Fixing Problem 1
The *brickwork* states

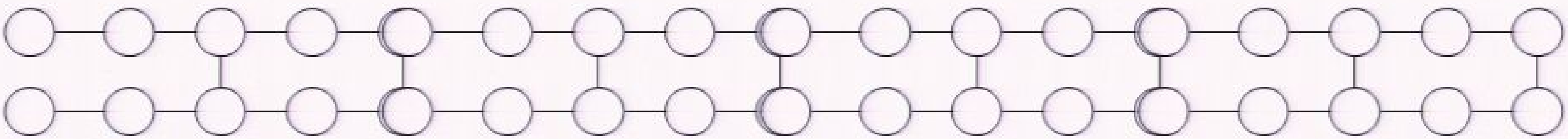


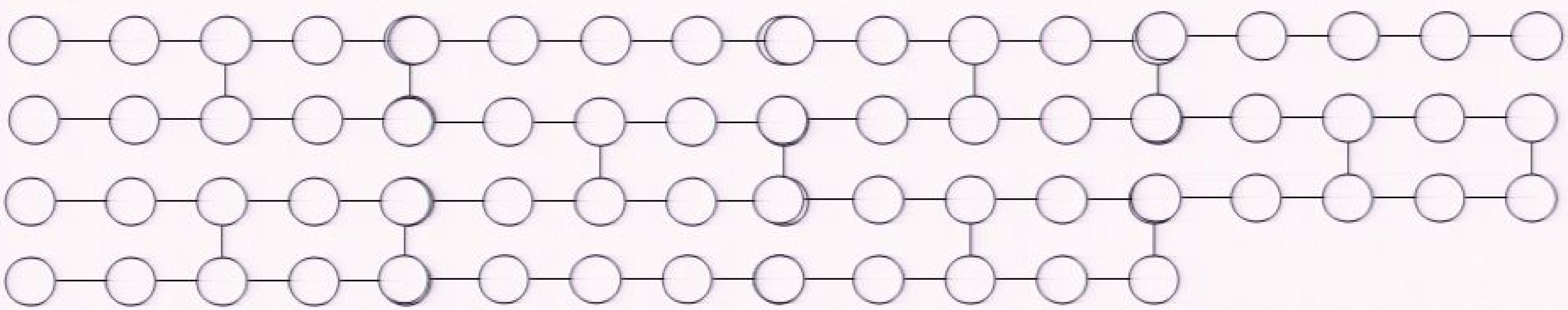


Fixing Problem 1
The *brickwork* states

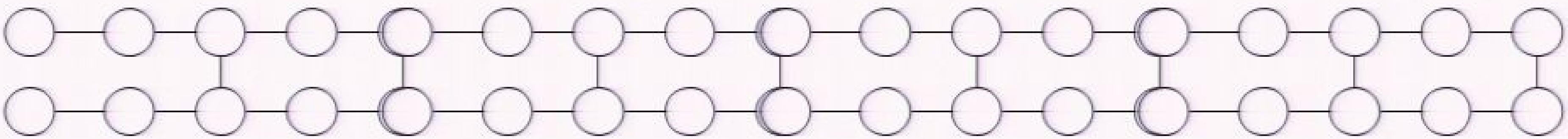


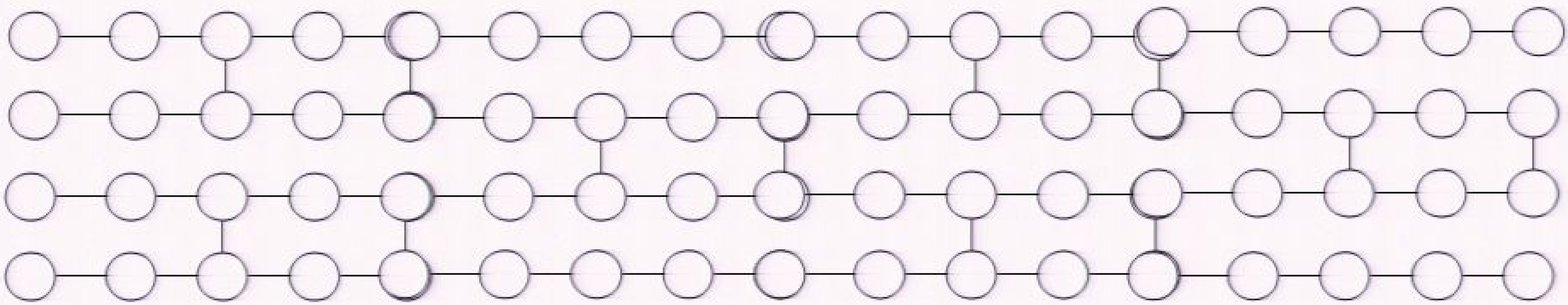
Fixing Problem 1
The *brickwork* states





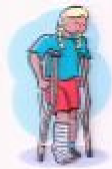
Fixing Problem 1
The *brickwork* states



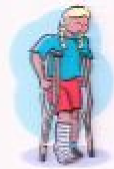


All measurements are in $\{\frac{n\pi}{8}, n = 0, 1, \ldots 7\}$

Second attempt at blind QC



Second attempt at blind QC



- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

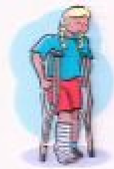
Second attempt at blind QC

- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to **brickwork** state

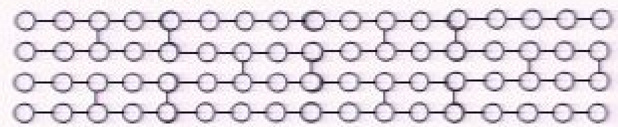
Second attempt at blind QC



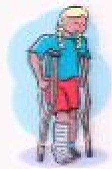
- prepares qubits in state

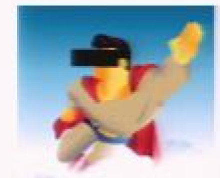
$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to **brickwork** state



Second attempt at blind QC



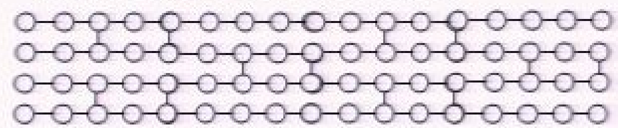


- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

→

- entangles according to **brickwork** state

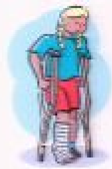


- chooses σ_z measurements

→

- tailors the cluster state

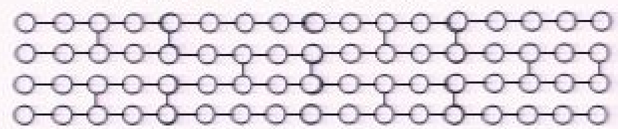
Second attempt at blind QC



- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

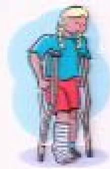
- entangles according to **brickwork** state

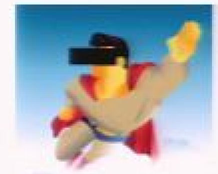


- chooses σ_z measurements

- tailors the cluster state

Second attempt at blind QC

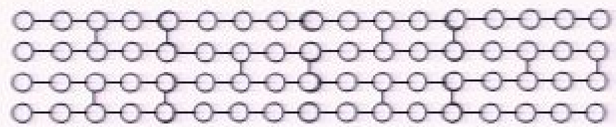




- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to **brickwork** state



- chooses σ_z measurements

- tailors the cluster state

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

$\phi'_1, \phi'_2, \phi'_3$ →

← m_1, m_2, m_3

ϕ'_4, ϕ'_6 →

⋮

- single-qubit measurements

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

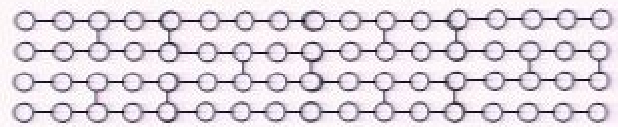
(s_x and s_z depend on previous measurement outcomes)

Second attempt at blind QC

- prepares qubits in state

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- entangles according to **brickwork** state



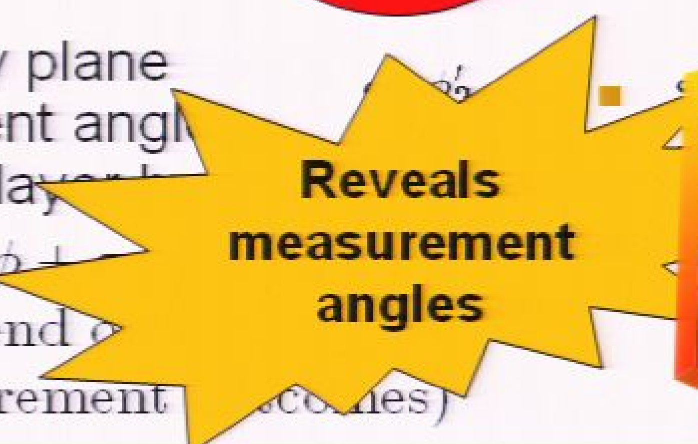
- chooses σ_z measurements

- tailors the cluster state

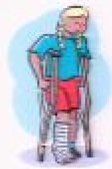
- chooses x-y plane measurement angl… adaptively, la…

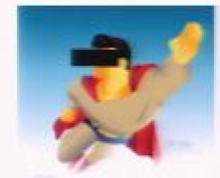
$\phi' = (-1)^{s_x}\phi + \ldots$

(s_x and s_z depend … previous measurement …comes)

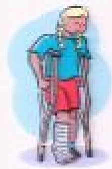


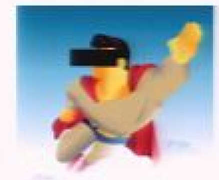
Fixing Problem 2





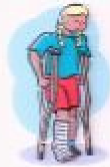
Fixing Problem 2





- prepares qubits randomly chosen in

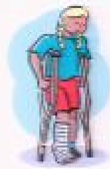
Fixing Problem 2

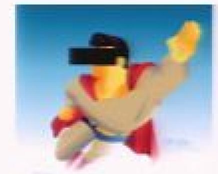


- prepares qubits randomly chosen in

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

Fixing Problem 2



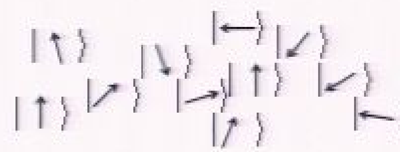


- prepares qubits randomly chosen in

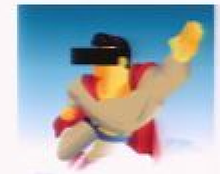
$$\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\frac{n\pi}{8}, n = 0, 1, \ldots, 15\}\}$$

→

- entangles according to **brickwork** state



Fixing Problem 2

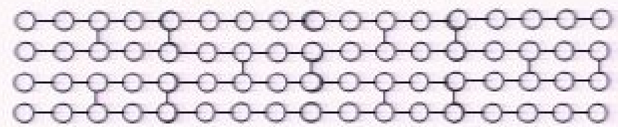


- prepares qubits randomly chosen in

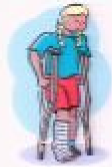
$$\{\tfrac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\tfrac{n\pi}{8}, n = 0, 1, \ldots, 15\}\}$$

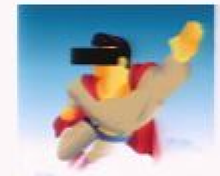
→

- entangles according to **brickwork** state



Fixing Problem 2

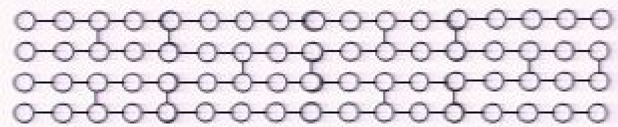




- prepares qubits randomly chosen in $\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\frac{n\pi}{8}, n = 0, 1, \ldots, 15\}\}$

→

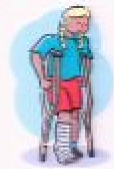
- entangles according to **brickwork** state

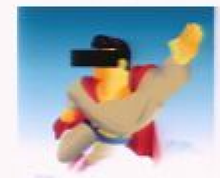


- chooses x-y plane measurement angles, adaptively, layer by layer

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

Fixing Problem 2



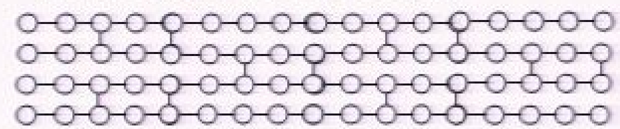


- prepares qubits randomly chosen in

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

→

- entangles according to **brickwork** state



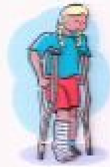
- chooses x-y plane measurement angles, adaptively, layer by layer

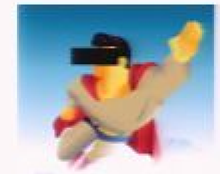
$$\phi' = (-1)^{s_x}\phi + \pi s_z$$

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

r random. r=1 will flip Bob's measurement outcome. Alice can correct this.

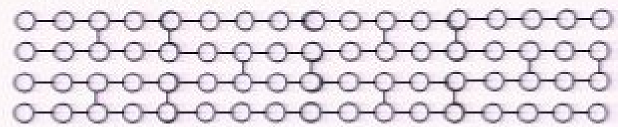
Fixing Problem 2





- prepares qubits randomly chosen in →
  $\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\frac{n\pi}{8}, n = 0, 1, \ldots, 15\}\}$

- entangles according to **brickwork** state

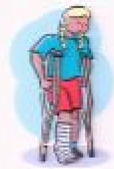


- chooses x-y plane measurement angles, adaptively, layer by layer

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

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

Fixing Problem 2

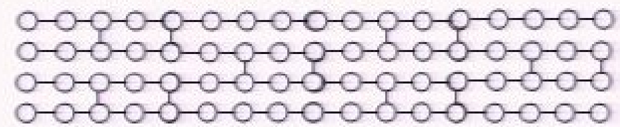


- prepares qubits randomly chosen in

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

→

- entangles according to **brickwork** state



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

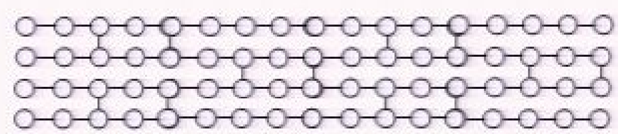
$$\phi' = (-1)^{s_x}\phi + \pi s_z$$

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

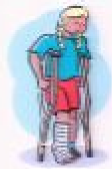
$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ →

- single-qubit measurements in basis

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



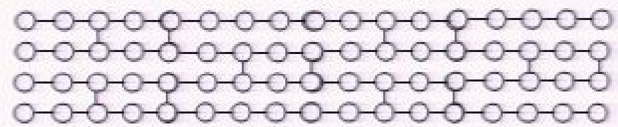
Fixing Problem 2



- prepares qubits randomly chosen in

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

- entangles according to **brickwork** state



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

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

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

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ →

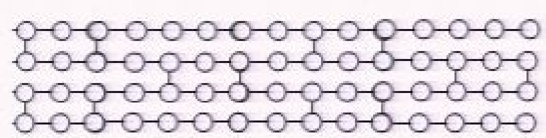
← m_1, m_2, m_3, m_4

$\alpha_5, \alpha_6, \alpha_7, \alpha_8$ →

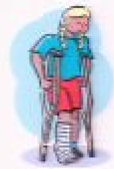
⋮

- single-qubit measurements in basis

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



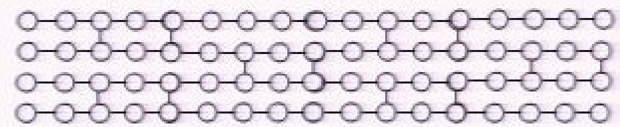
Fixing Problem 2



- prepares qubits randomly chosen in $\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{\frac{n\pi}{8}, n = 0, 1, \ldots, 15\}\}$

$\longrightarrow$

- entangles according to **brickwork** state



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

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

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

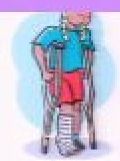
$\alpha_1, \alpha_2, \alpha_3, \alpha_4 \longrightarrow$

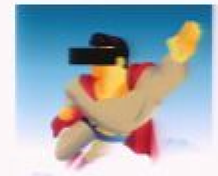
$m_1, m_2, m_3, m_4 \longleftarrow$

$\alpha_5, \alpha_6, \alpha_7, \alpha_8 \longrightarrow$

$\vdots$

- single-qubit measurements in basis $\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle), \{\frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle)$



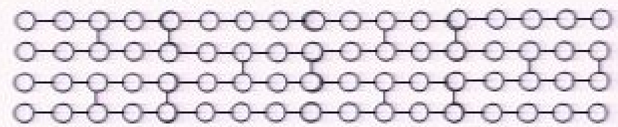


- prepares qubits randomly chosen in

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

→

- entangles according to **brickwork** state



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

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

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

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ →

← m_1, m_2, m_3, m_4

$\alpha_5, \alpha_6, \alpha_7, \alpha_8$ →

⋮

- single-qubit measurements in basis

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

Privacy

Let $\theta = \theta' + k\pi, \theta' \in \{\frac{n\pi}{8}, n = 0, \ldots 7\}$.

Then Alice sends to Bob

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \\
&= \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\theta'+k\pi)}|1\rangle) \\
&= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^k e^{i\theta'}|1\rangle)
\end{aligned}
$$

This forms a private quantum channel with key k and so Bob cannot know θ'.

Privacy

Let $\theta = \theta' + k\pi, \theta' \in \{\frac{n\pi}{8}, n = 0, \ldots 7\}$.

Then Alice sends to Bob

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \\
&= \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\theta'+k\pi)}|1\rangle) \\
&= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^k e^{i\theta'}|1\rangle)
\end{aligned}
$$

This forms a private quantum channel with key k and so Bob cannot know θ'.

Looking at the classical information, that Alice sends Bob:

$$
\begin{aligned}
\alpha &= \phi' + \theta + r\pi \\
&= \phi' + \theta' + (k + r)\pi
\end{aligned}
$$

This forms a classical one-time pad and so ϕ' is unknown to Bob.

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

even if Bob knows s_x and s_z, he still cannot find ϕ.

Quantum input

- Alice applies random Z-rotation to each input qubit, followed by either Pauli-X or I, randomly.
- Alice adds a first layer to her pattern, which undoes the Pauli-X if necessary.
- Remainder of the protocol unchanged.

Privacy

Let $\theta = \theta' + k\pi, \theta' \in \{\frac{n\pi}{8}, n = 0, \dots 7\}$.

Then Alice sends to Bob

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\theta'+k\pi)}|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^k e^{i\theta'}|1\rangle) \end{aligned}$$

This forms a private quantum channel with key k and so Bob cannot know θ'.

Looking at the classical information, that Alice sends Bob:

$$\begin{aligned} \alpha &= \phi' + \theta + r\pi \\ &= \phi' + \theta' + (k+r)\pi \end{aligned}$$

This forms a classical one-time pad and so ϕ' is unknown to Bob.

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

even if Bob knows s_x and s_z, he still cannot find ϕ.

Quantum input

- Alice applies random Z-rotation to each input qubit, followed by either Pauli-X or I, randomly.
- Alice adds a first layer to her pattern, which undoes the Pauli-X if necessary.
- Remainder of the protocol unchanged.

Quantum output

- In Alice's preparation, she does not rotate the qubits of the last layer.
- Run the protocol as usual, except:
  - Bob does not measure the last layer but instead returns the qubits to Alice
  - Alice applies X or Z if necessary to retrieve output. This depends on previous measurement outcomes, which are unknown to Bob.

Authentication

Authentication

For outputs that
<u>can not</u> be easily
verified by Alice

Authentication

For outputs that
can not be easily
verified by Alice

- Alice encodes her input into an appropriate authentication code and suitably modifies her gates so that authentication is preserved
- Uncooperative Bob is detected, except with exponentially small probability.

Conclusion

- Is our protocol optimal for Alice?

Conclusion

- Is our protocol optimal for Alice?
  - one-qubit random preparation is pretty minimal

Conclusion

- Is our protocol optimal for Alice?
  - one-qubit random preparation is pretty minimal
- Assume f is public.
  - Can we get rid of interaction?

Conclusion

- Is our protocol optimal for Alice?
  - one-qubit random preparation is pretty minimal
- Assume f is public.
  - Can we get rid of interaction?
- Other applications of measurement-based quantum computing to distributed tasks

Conclusion

- Is our protocol optimal for Alice?
  - one-qubit random preparation is pretty minimal
- Assume f is public.
  - Can we get rid of interaction?
- Other applications of measurement-based quantum computing to distributed tasks