Measurement-based and Blind quantum computation

Berlin School of
Optical Sciences &
Quantum Technologies

Outline

Measurement based quantum computation

- Instead of *gates*, use *measurements* to drive the computation

Measurement based quantum computation

- Instead of *gates*, use *measurements* to drive the computation
- Only single-qubit measurements needed

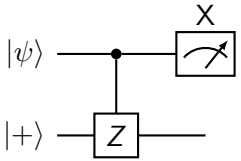
Measurement based quantum computation

- Instead of *gates*, use *measurements* to drive the computation
- Only single-qubit measurements needed
- Uses a *resource* - not just qubits, but (highly) entangled ones

Measurement based quantum computation

- Instead of *gates*, use *measurements* to drive the computation
- Only single-qubit measurements needed
- Uses a *resource* - not just qubits, but (highly) entangled ones
- Equally powerful as gate-based computation

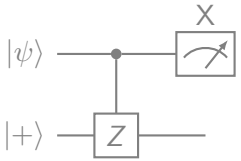
Basics - Teleportation



$m \in \{0, 1\}$

$$|\psi\rangle_t = Z^m H |\psi\rangle$$

Basics - Teleportation

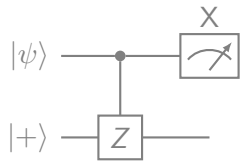


$m \in \{0, 1\}$

$$|\psi\rangle_t = Z^m H |\psi\rangle$$

$X := \{|0\rangle \pm |1\rangle\}$

Basics - Teleportation



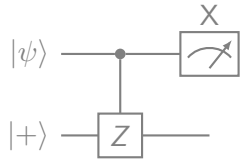
$m \in \{0, 1\}$

$$|\psi\rangle_t = Z^m H |\psi\rangle$$

$X := \{|0\rangle \pm |1\rangle\}$

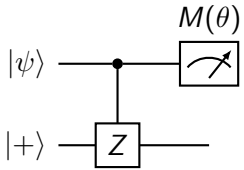
$M(\theta) := \{|0\rangle \pm e^{i\theta} |1\rangle\} = R_z(\theta) \cdot X$

Basics - Teleportation



$m \in \{0, 1\}$

$$|\psi\rangle_t = Z^m H |\psi\rangle$$



$m \in \{0, 1\}$

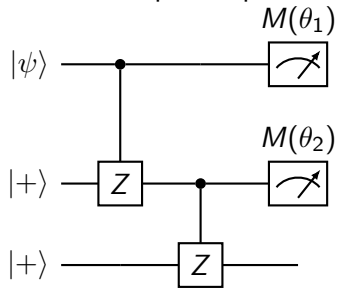
$$|\psi\rangle_t = Z^m H R_z(\theta) |\psi\rangle$$

Combined teleportation

Concatenate multiple teleportations

Combined teleportation

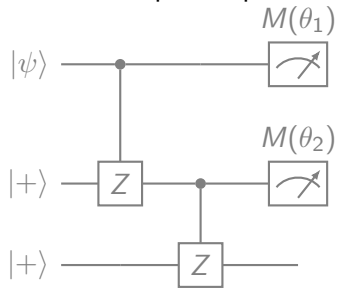
Concatenate multiple teleportations



$$|\psi\rangle_t = HR_z(\theta_2)HR_z(\theta_1)\,|\psi\rangle$$

Combined teleportation

Concatenate multiple teleportations



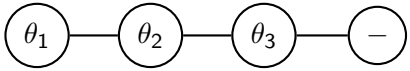
$$|\psi\rangle_t = HR_z(\theta_2)HR_z(\theta_1)\,|\psi\rangle$$

Three times gives us:

$$HR_z(\theta_2)\underbrace{HR_z(\theta_2)H}_{R_x(\theta_2)}R_z(\theta_1)\,|\psi\rangle$$
$$\sim U(\theta_1,\theta_2,\theta_3)\,|\psi\rangle$$

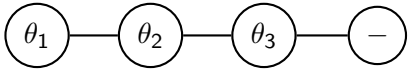
A different way of representing

The cluster state:



A different way of representing

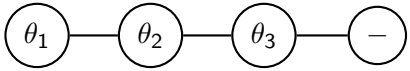
The cluster state:



- Replace the 'input'-$|\psi\rangle$ with $|+\rangle$

A different way of representing

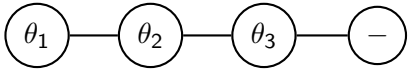
The cluster state:



- Replace the 'input'-$|\psi\rangle$ with $|+\rangle$
- Represent each $|+\rangle$ with a circle ('vertex')

A different way of representing

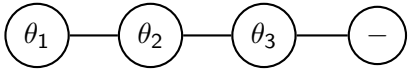
The cluster state:



- Replace the 'input'-$|\psi\rangle$ with $|+\rangle$
- Represent each $|+\rangle$ with a circle ('vertex')
- Represent each CZ with a line ('edge')

A different way of representing

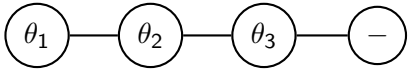
The cluster state:



- Replace the 'input'-$|\psi\rangle$ with $|+\rangle$
- Represent each $|+\rangle$ with a circle ('vertex')
- Represent each CZ with a line ('edge')
- The measurement angles are *inside* the circles

A different way of representing

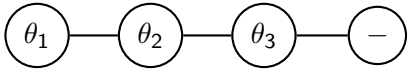
The cluster state:



- Replace the 'input'-$|\psi\rangle$ with $|+\rangle$
- Represent each $|+\rangle$ with a circle ('vertex')
- Represent each CZ with a line ('edge')
- The measurement angles are *inside* the circles
- *All* CZ's can be performed before any measurement

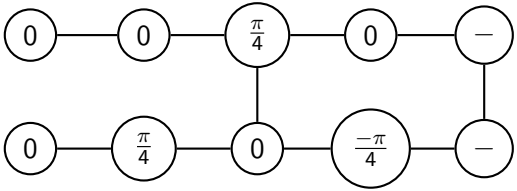
A different way of representing

The cluster state:

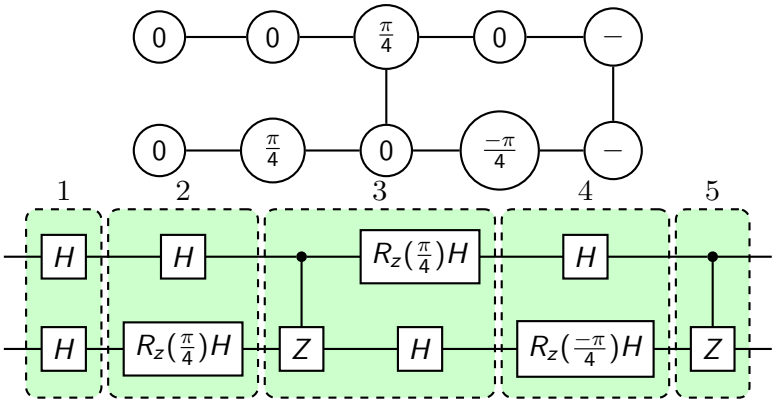


- Replace the 'input'-$|\psi\rangle$ with $|+\rangle$
- Represent each $|+\rangle$ with a circle ('vertex')
- Represent each CZ with a line ('edge')
- The measurement angles are *inside* the circles
- *All* CZ's can be performed before any measurement
- This input 'resource' is the same for all measurement patterns

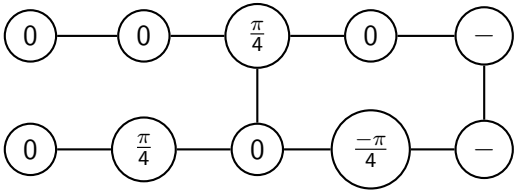
What about 2-qubit gates?



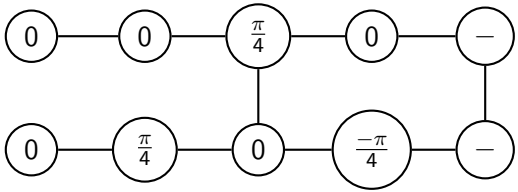
What about 2-qubit gates?

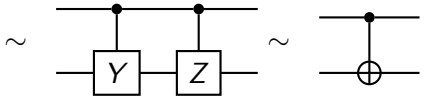


What about 2-qubit gates?

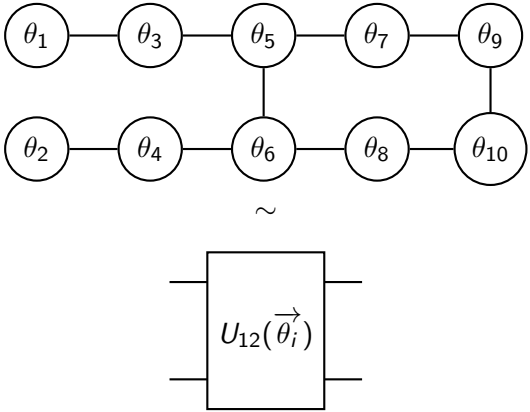


What about 2-qubit gates?

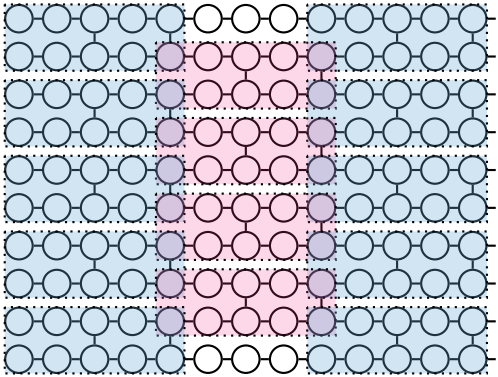




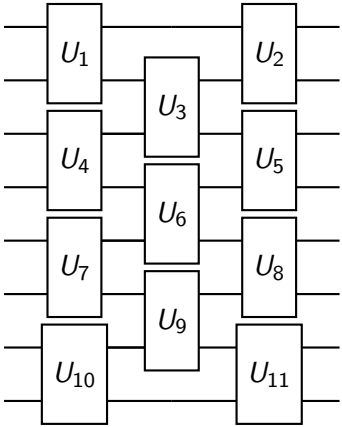
A *Universal* resource: the *brickwork* state



A *Universal* resource: the *brickwork* state



A *Universal* resource: the *brickwork* state



Computational power

- Any single-qubit unitary U with 3(5) measurements layers

Computational power

- Any single-qubit unitary U with 3(5) measurements layers
- CX with 5 measurement layers

Computational power

- Any single-qubit unitary U with 3(5) measurements layers
- CX with 5 measurement layers
- **Universal gateset**

Computational power

- Any single-qubit unitary U with 3(5) measurements layers
- CX with 5 measurement layers
- **Universal gateset**
- n-qubit circuit with gate depth of g gives n rows and $O(g)$ columns

Computational power

- Any single-qubit unitary U with 3(5) measurements layers
- CX with 5 measurement layers
- **Universal gateset**
- n-qubit circuit with gate depth of g gives n rows and $O(g)$ columns
- $BQP \subset$ MBQC (and obviously vice-versa)

All angles?

- Claim: only measurement angles of $\{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$ is enough

All angles?

- Claim: only measurement angles of $\{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$ is enough
- We already saw CX with these angles

All angles?

- Claim: only measurement angles of $\{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$ is enough
- We already saw CX with these angles
- $H, R_z(\frac{\pi}{8})$ are easily performed by single measurement + 0-measurements

All angles?

- Claim: only measurement angles of $\{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$ is enough
- We already saw CX with these angles
- $H, R_z(\frac{\pi}{8})$ are easily performed by single measurement + 0-measurements
- This gives $\{H, T, CX\} :=$ universal gateset

All angles?

- Claim: only measurement angles of $\{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$ is enough
- We already saw CX with these angles
- $H, R_z(\frac{\pi}{8})$ are easily performed by single measurement + 0-measurements
- This gives $\{H, T, CX\} :=$ universal gateset
- Still $O(ng)$ scaling

Recap MBQC

- Perform the computation by single-qubit measurements on resource

Recap MBQC

- Perform the computation by single-qubit measurements on resource
- Resource is 2-dimensional highly-entangled state

Recap MBQC

- Perform the computation by single-qubit measurements on resource
- Resource is 2-dimensional highly-entangled state
- Measurements only in $M(\theta)$ basis $\theta \in \{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$

Recap MBQC

- Perform the computation by single-qubit measurements on resource
- Resource is 2-dimensional highly-entangled state
- Measurements only in $M(\theta)$ basis $\theta \in \{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$
- $n \times g$ circuit simulated with $n \times O(g)$ grid

Recap MBQC

- Perform the computation by single-qubit measurements on resource
- Resource is 2-dimensional highly-entangled state
- Measurements only in $M(\theta)$ basis $\theta \in \{0, \pm\frac{\pi}{4}, \pm\frac{\pi}{2}\}$
- $n \times g$ circuit simulated with $n \times O(g)$ grid
- MBQC and gate-based equally powerful

Blind quantum computation

- Imagine having access to a quantum server

Blind quantum computation

- Imagine having access to a quantum server
- **Very** limited quantum resources locally

Blind quantum computation

- Imagine having access to a quantum server
- **Very** limited quantum resources locally
- Paranoid-dial to 11

Blind quantum computation

- Imagine having access to a quantum server
- **Very** limited quantum resources locally
- Paranoid-dial to 11
  - No leakage about **input** of computation

Blind quantum computation

- Imagine having access to a quantum server
- **Very** limited quantum resources locally
- Paranoid-dial to 11
  - No leakage about **input** of computation
  - No leakage about **type** of computation

Blind quantum computation

- Imagine having access to a quantum server
- **Very** limited quantum resources locally
- Paranoid-dial to 11
  - No leakage about **input** of computation
  - No leakage about **type** of computation
- Verifiable (no tricks from the server!)

Multiple protocols

- Two protocols:

Multiple protocols

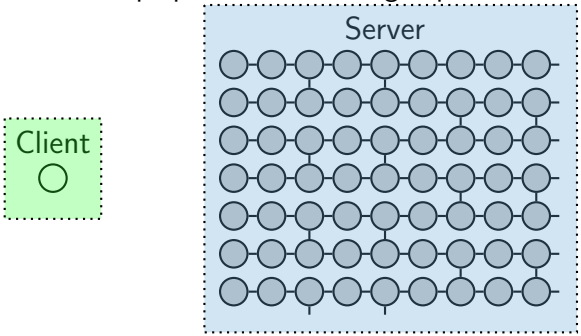
- Two protocols:
  - Client state preparation by Broadbent et al.

Multiple protocols

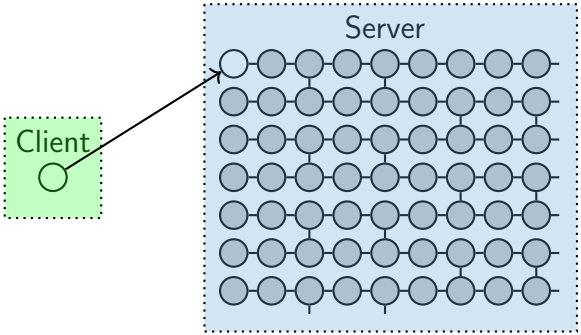
- Two protocols:
  - Client state preparation by Broadbent et al.
  - Client state measurement by Morimae et al.

First protocol[1]

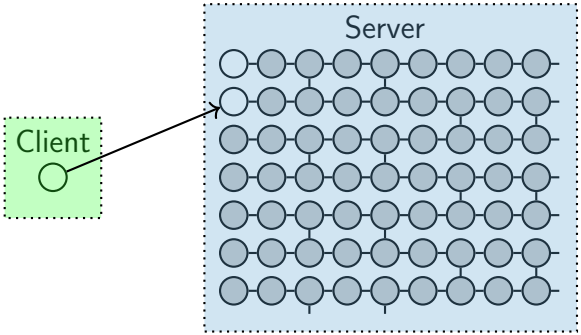
Client can prepare and send single qubits



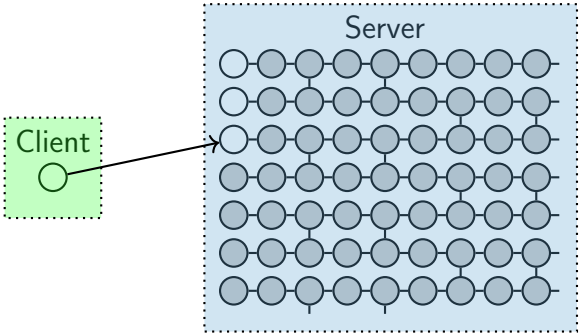
First protocol



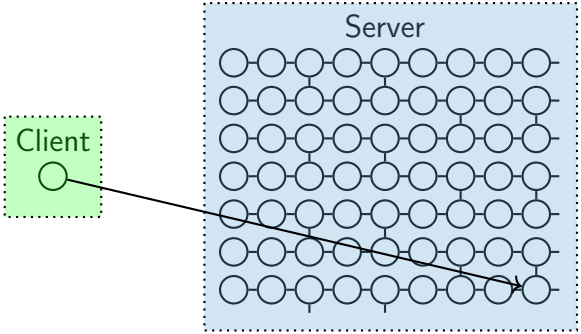
First protocol



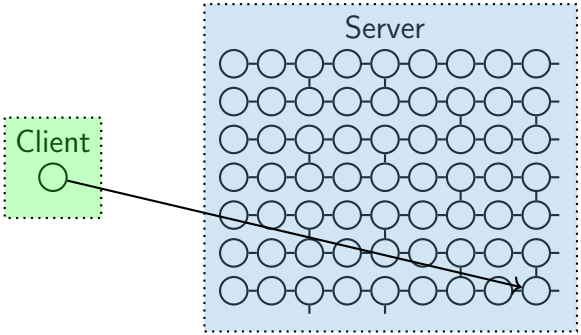
First protocol



First protocol

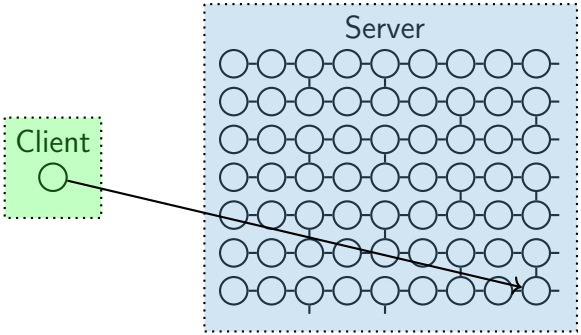


First protocol



Prepare qubits $|0\rangle + e^{i\phi}|1\rangle$ for random $\phi \in \frac{\pi}{8}\{0, 1, 2 \ldots, 7\}$

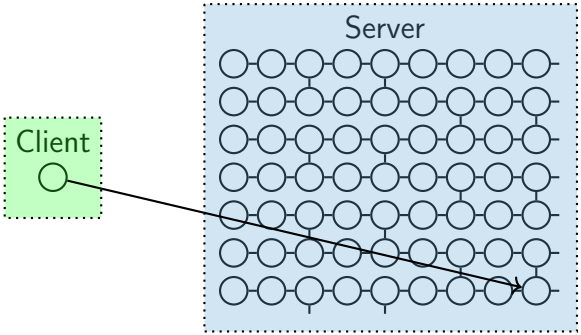
First protocol



Prepare qubits $|0\rangle + e^{i\phi}|1\rangle$ for random $\phi \in \frac{\pi}{8}\{0, 1, 2 \ldots, 7\}$

ϕ **unknown to server**

First protocol



Prepare qubits $|0\rangle + e^{i\phi}|1\rangle$ for random $\phi \in \frac{\pi}{8}\{0, 1, 2 \ldots, 7\}$

ϕ unknown to server

Hide the measurement angles

Protocol

For every node i, with intended measurement angle θ_i:

- Client sends qubit $|\phi_i\rangle = |0\rangle + e^{i\phi_i}|1\rangle = R_z(\phi_i)|+\rangle$
- Client picks random $r_i \in \{0, 1\}$
- Client tells server to measure with angle $\hat{\theta}_i = \theta_i + \phi_i + r_i\pi$

Measuring $|\phi_i\rangle$ with angle $\hat{\theta}_i \hat{=}$ measuring $|+\rangle$ with angle $\theta_i + r_i\pi$

- Server sends measurement outcome $m_i \in \{0, 1\}$
- Client computes output $o_i = m_i$ or $o_i = 1 - m_i$

Security

- Server wants:

  Classic information: n, g, $\{\theta_i\}$, $\{o_i\}$

- Server receives:

  Classic information: n, g, $\{\hat{\theta}_i\}$, $\{m_i\}$
  Quantum information: $\{|\phi_i\rangle\} = |0\rangle + e^{i\phi_i}|1\rangle$

  - Classic leakage:

    $\hat{\theta}_i$, θ_i are uncorrelated due to random ϕ_i
    $\{m_i\}$, $\{o_i\}$ are uncorrelated due to random r_i
    No leakage but n, g

  - Quantum leakage:

    $\{|\phi_i\rangle\} = |0\rangle + (-1)^{r_i} e^{i(\hat{\theta}_i - \theta_i)}|1\rangle$
    Trace away r_i: maximally mixed state
    No leakage whatsoever

Recap first protocol

- Can only prepare and send qubits

Recap first protocol

- Can only prepare and send qubits
- Hide the measurement angle by pre-rotating qubit to $|0\rangle + e^{i\phi}|1\rangle$ before sending

Recap first protocol

- Can only prepare and send qubits
- Hide the measurement angle by pre-rotating qubit to $|0\rangle + e^{i\phi}|1\rangle$ before sending
- Server only knows to measure under uncorrelated angle $\hat{\theta}$

Recap first protocol

- Can only prepare and send qubits
- Hide the measurement angle by pre-rotating qubit to $|0\rangle + e^{i\phi}|1\rangle$ before sending
- Server only knows to measure under uncorrelated angle $\hat{\theta}$
- Extra flip $r\pi$ of measurement angle to hide outcomes

Recap first protocol

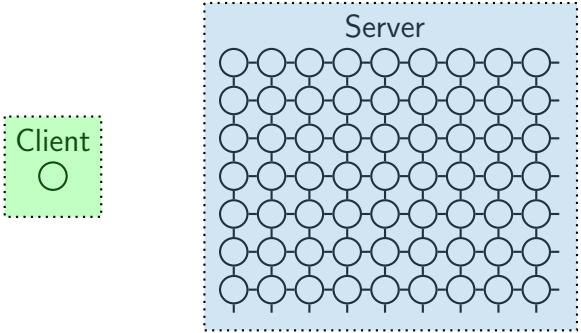
- Can only prepare and send qubits
- Hide the measurement angle by pre-rotating qubit to $|0\rangle + e^{i\phi}|1\rangle$ before sending
- Server only knows to measure under uncorrelated angle $\hat{\theta}$
- Extra flip $r\pi$ of measurement angle to hide outcomes
- Classical and quantum information of server completely uncorrelated

Recap first protocol

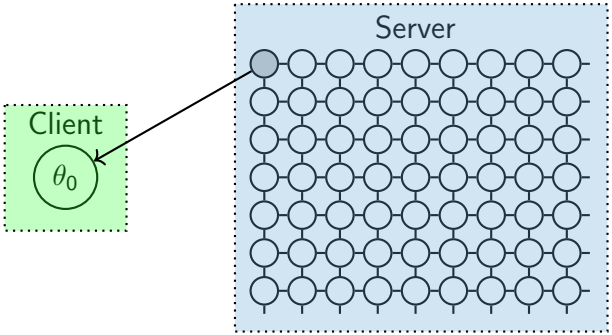
- Can only prepare and send qubits
- Hide the measurement angle by pre-rotating qubit to $|0\rangle + e^{i\phi}|1\rangle$ before sending
- Server only knows to measure under uncorrelated angle $\hat{\theta}$
- Extra flip $r\pi$ of measurement angle to hide outcomes
- Classical and quantum information of server completely uncorrelated

Second protocol #1.a[1]

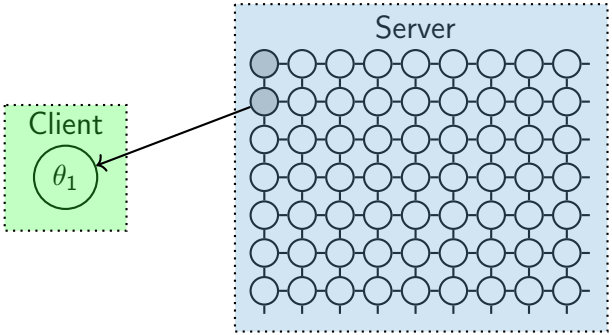
Client can receive and measure single qubits



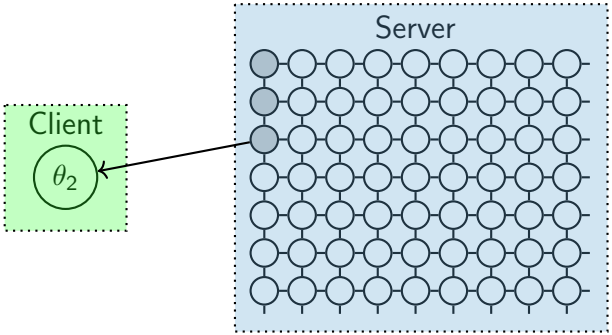
Second protocol #1.*a*



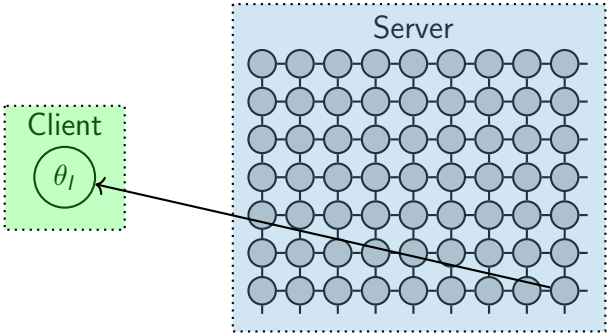
Second protocol #1.*a*



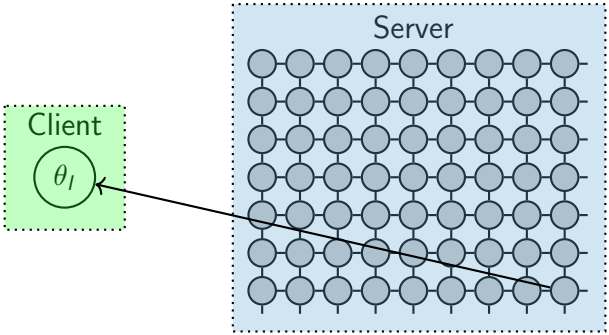
Second protocol #1.*a*



Second protocol #1.*a*

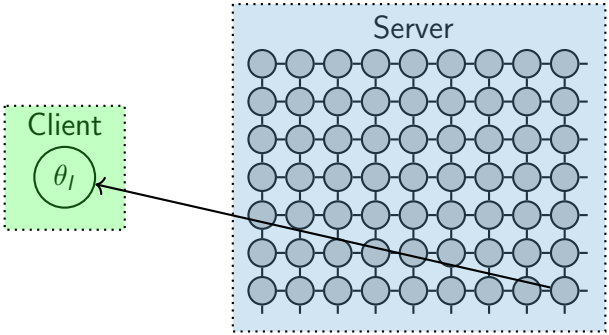


Second protocol #1.*a*



No signalling from client to server!

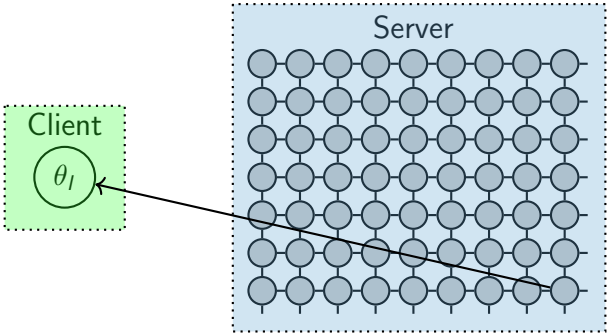
Second protocol #1.*a*



No signalling from client to server!

Inherently secure based on 'bigger then quantum' principles

Second protocol #1.*a*



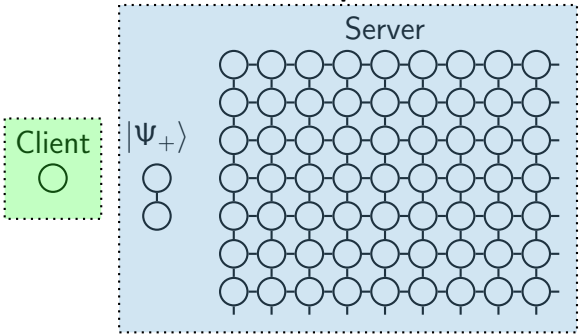
No signalling from client to server!

Inherently secure based on 'bigger then quantum' principles

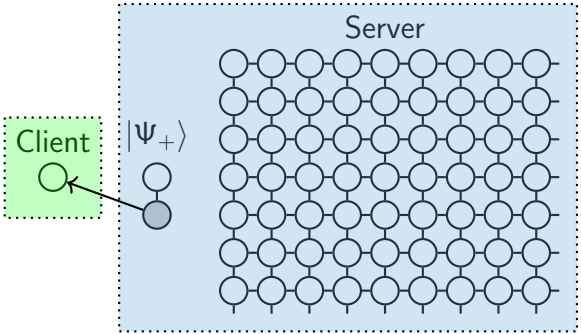
Very prone to photon loss

Second protocol #1.*b*

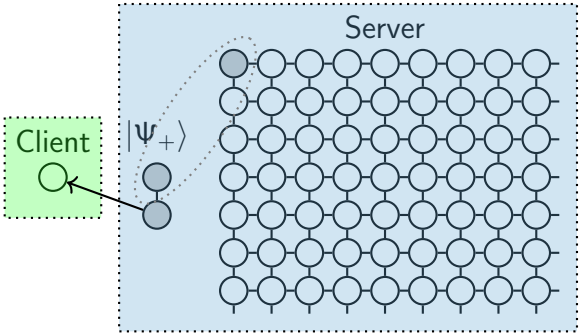
Client can receive, measure single qubits
and store them for short periods in time



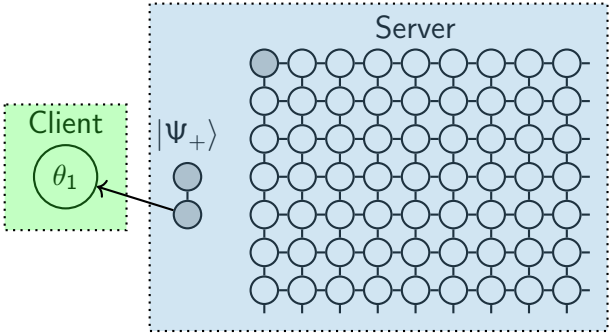
Second protocol #1.*b*



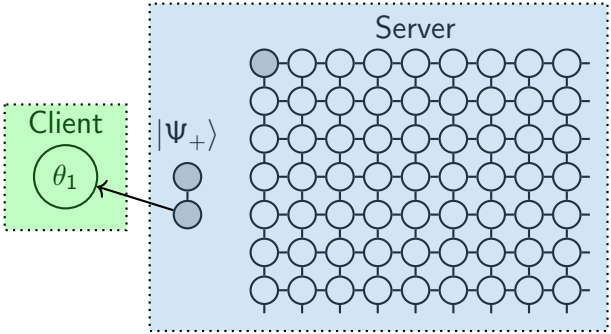
Second protocol #1.*b*



Second protocol #1.*b*

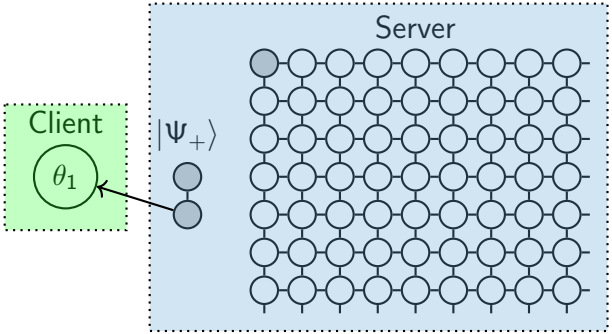


Second protocol #1.*b*



Now there is signalling...

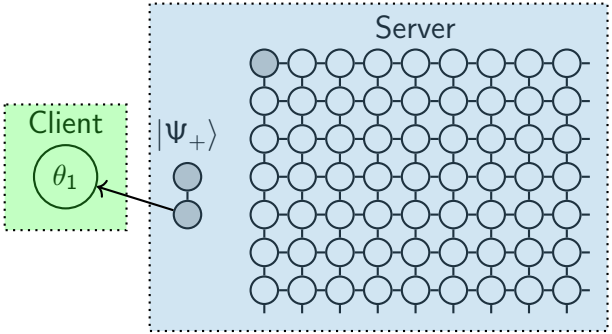
Second protocol #1.*b*



Now there is signalling...

Inherently secure based on ~~'bigger then~~ quantum' principles

Second protocol #1.*b*



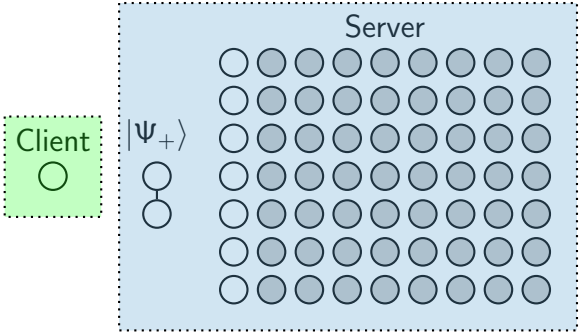
Now there is signalling...

Inherently secure based on '~~bigger then~~ quantum' principles

Qubit storage not a nice aspect...

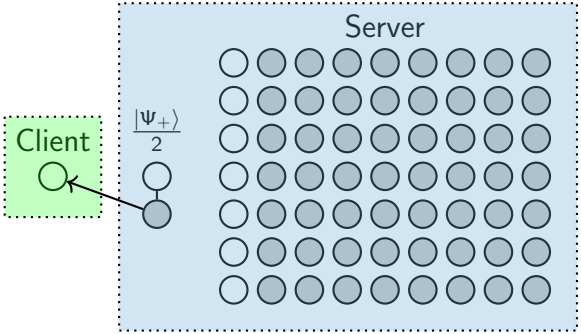
Second protocol #2

Client can receive, measure single qubits



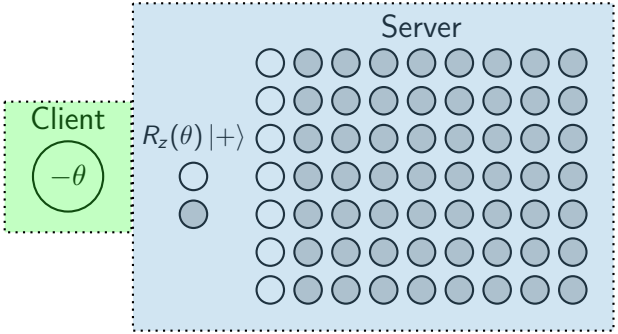
Create a Bell pair

Second protocol #2



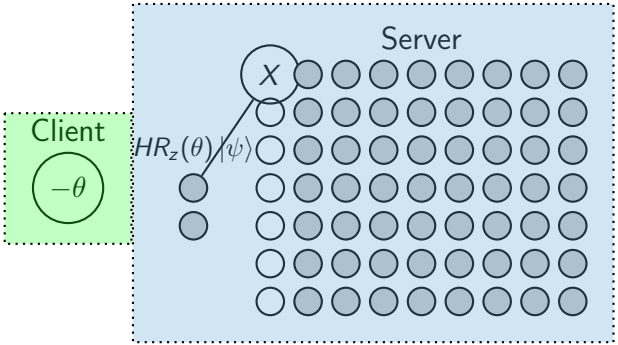
Client receives half

Second protocol #2



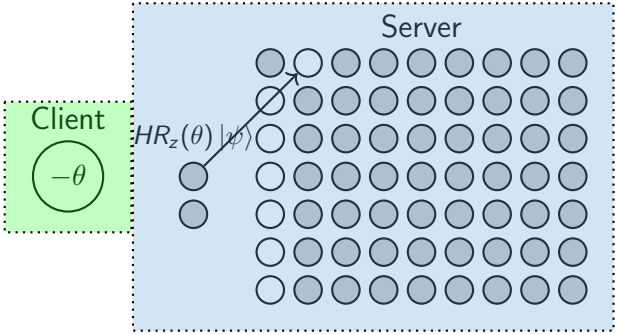
Client measures in $-\theta$ basis, other half becomes $R_z(\theta)\,|+\rangle$

Second protocol #2



Entangle with node $|\psi\rangle$, measure node in X, get $HR_z(\theta)|\psi\rangle$

Second protocol #2



Send $HR_z(\theta)\,|\psi\rangle$ to its 'right' place in the chain

Security

Version #1.*a* is 'obviously' secure

Security

Version #1.*a* is 'obviously' secure

Version #1.*b* is still secure by quantum mechanics

Security

Version #1.*a* is 'obviously' secure

Version #1.*b* is still secure by quantum mechanics

Version #2 is secure by the same argument

Recap

- Can only receive and measure qubits (and maybe store them for short time)

Recap

- Can only receive and measure qubits (and maybe store them for short time)
- Easiest: just have the server send the qubits over

Recap

- Can only receive and measure qubits (and maybe store them for short time)
- Easiest: just have the server send the qubits over
- Harder 1: receive Bell pair half and measure there after server teleports

Recap

- Can only receive and measure qubits (and maybe store them for short time)
- Easiest: just have the server send the qubits over
- Harder 1: receive Bell pair half and measure there after server teleports
- Harder 2: receive Bell pair half and teleport computation angle to server

Recap

- Can only receive and measure qubits (and maybe store them for short time)
- Easiest: just have the server send the qubits over
- Harder 1: receive Bell pair half and measure there after server teleports
- Harder 2: receive Bell pair half and teleport computation angle to server
- Security by no-signaling, or 'just' quantum mechanics

Recap

- Can only receive and measure qubits (and maybe store them for short time)
- Easiest: just have the server send the qubits over
- Harder 1: receive Bell pair half and measure there after server teleports
- Harder 2: receive Bell pair half and teleport computation angle to server
- Security by no-signaling, or 'just' quantum mechanics

Research questions

- Are the two protocols actually equivalent?

Research questions

- Are the two protocols actually equivalent?
- Make use of *abstract cryptography*

Research questions

- Are the two protocols actually equivalent?
- Make use of *abstract cryptography*
- Fabian Kruger is working on this

Research questions

- Are the two protocols actually equivalent?
- Make use of *abstract cryptography*
- Fabian Kruger is working on this
- Other questions about i.e. verifiability

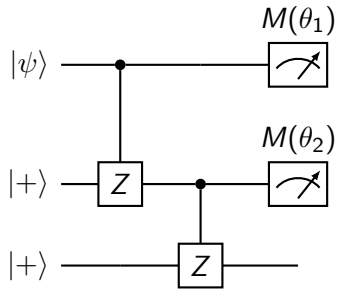
Thanks for the attention!

Backup - What about -1 outcomes?

Multiple teleportations with -1 outcomes

Backup - What about -1 outcomes?

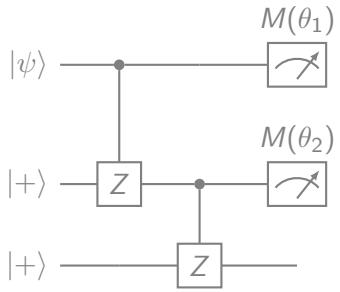
Multiple teleportations with -1 outcomes



$$|\psi\rangle_t = Z^{m_2} H R_z(\theta_2) Z^{m_1} H R_z(\theta_1) |\psi\rangle$$

Backup - What about -1 outcomes?

Multiple teleportations with -1 outcomes

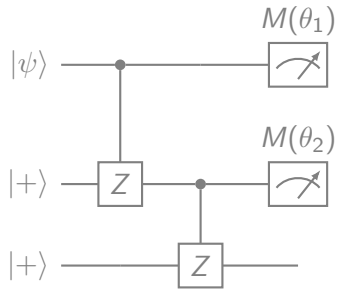


$$|\psi\rangle_t = Z^{m_2} H R_z(\theta_2) Z^{m_1} H R_z(\theta_1) |\psi\rangle$$

Pull the Z^m Paulis through consecutive H's and $R_z(\theta)$'s

Backup - What about -1 outcomes?

Multiple teleportations with -1 outcomes



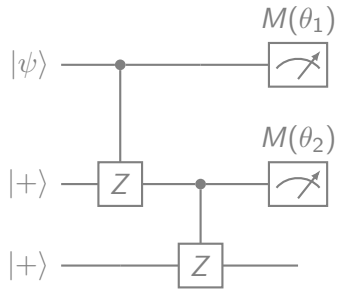
$$|\psi\rangle_t = Z^{m_2} H R_z(\theta_2) Z^{m_1} H R_z(\theta_1) |\psi\rangle$$

Pull the Z^m Paulis through consecutive H's and $R_z(\theta)$'s

But: $HZ = XH$ and $R_z(\theta)X = XR_z(-\theta)$

Backup - What about -1 outcomes?

Multiple teleportations with -1 outcomes



$$|\psi\rangle_t = Z^{m_2} H R_z(\theta_2) Z^{m_1} H R_z(\theta_1) |\psi\rangle$$

Pull the Z^m Paulis through consecutive H's and $R_z(\theta)$'s

But: $HZ = XH$ and $R_z(\theta)X = XR_z(-\theta)$

Paulis can be pulled through, but **measurement angles become dependend of previous outcomes**

Backup - How to verify?

- The server can do anything it wants
- It can try and trick us by:
  - Measuring in a different basis
  - Returning different results
  - Sending wrong qubits

Backup - How to verify?

- The server can do anything it wants
- It can try and trick us by:
  - Measuring in a different basis
  - Returning different results
  - Sending wrong qubits
- Put in sub-computations of which you know the outcome

Backup - How to verify?

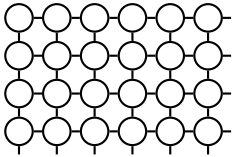
- The server can do anything it wants
- It can try and trick us by:
  - Measuring in a different basis
  - Returning different results
  - Sending wrong qubits
- Put in sub-computations of which you know the outcome
- Measure a logical qubit every now and then

Backup - How to verify?

- The server can do anything it wants
- It can try and trick us by:
  - Measuring in a different basis
  - Returning different results
  - Sending wrong qubits
- Put in sub-computations of which you know the outcome
- Measure a logical qubit every now and then
- Measure stabilizers of the resource every now and then

Backup - Different kinds of resources

- We saw the *brickwork* state



- Originally introduced was the *cluster* state
- With θ- and Z-measurements
- Only in 2017 it was shown[1] that one doesn't need Z-measurements for universality
- Many other resources possible

[1] Mantri et al. - Sci Rep 7, 42861 (2017)

Backup - A note on the two-qubit unitary