# Blind Quantum Computation

Charles Herder

December 12, 2012

# Table of contents

# Blind Computation

## Client

1. Circuit description $D_C$ and input $|\psi\rangle_n$
2. Send $D_C$ and $|\psi\rangle_n$ to Server.
3. Receive output $C|\psi\rangle_n$.

## Server

1. Receive encoded $D_C$ and $|\psi\rangle_n$.
2. Perform computation
3. Return $C|\psi\rangle_n$.

Server doesn't know:

- Input, Output, or Intermediate states ($|\psi\rangle_n$)
- What computation is performed ($C$)

# Random Local Paulis

**Claim:**

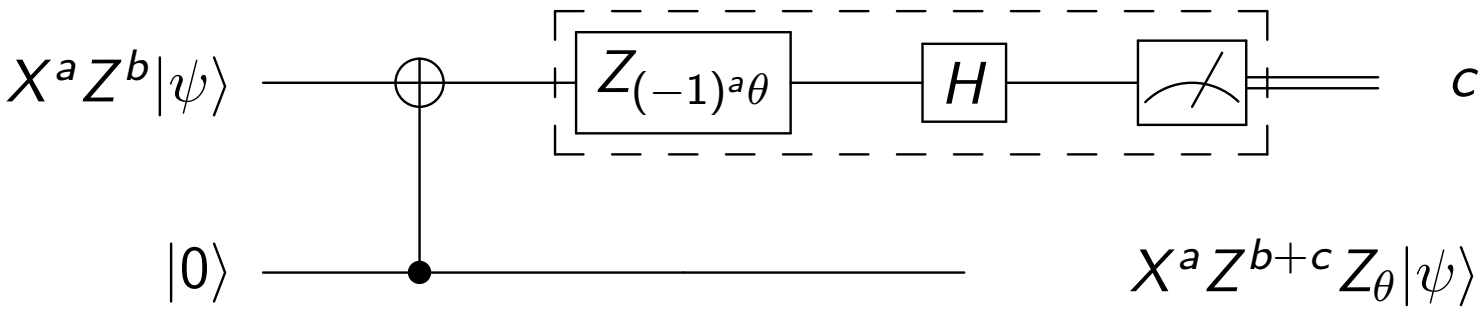
For random $a, b \in 0, 1$, $X^a Z^b |\psi\rangle$ is indiscernable from the completely mixed state.

**Idea:** (Ahornov, Ben-Orr, Eban, 2008)
Use the above to "Encrypt" a quantum state.

**Problem:**
Hard to compute on an encrypted state.

# MBQC - Blindness

**Key Recognition:** MBQC already deals with Random Local Pauli matrices!

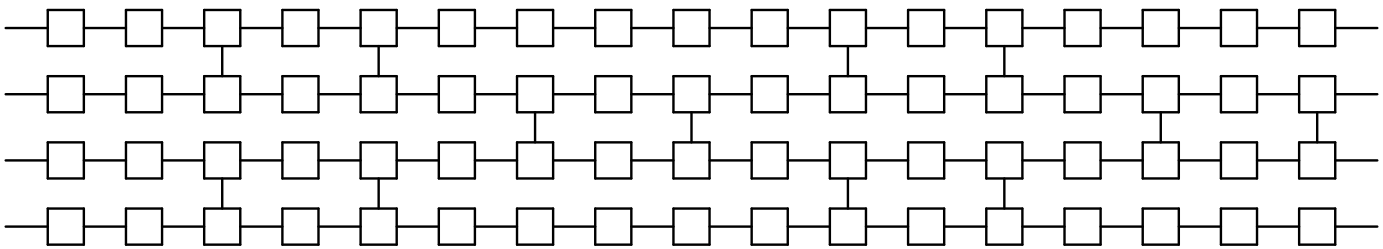



**Intuition:**

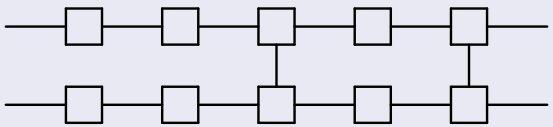
- Client knows $a$, $b$. Server does not.
- Rotations are basic operation - $X$ and $Z$ commute easily

# MBQC - Blindness Pt 2

**Problem:**
"Shape" of the computation reveals where qubits are interacting!
**Solution:** "Brickwork State"

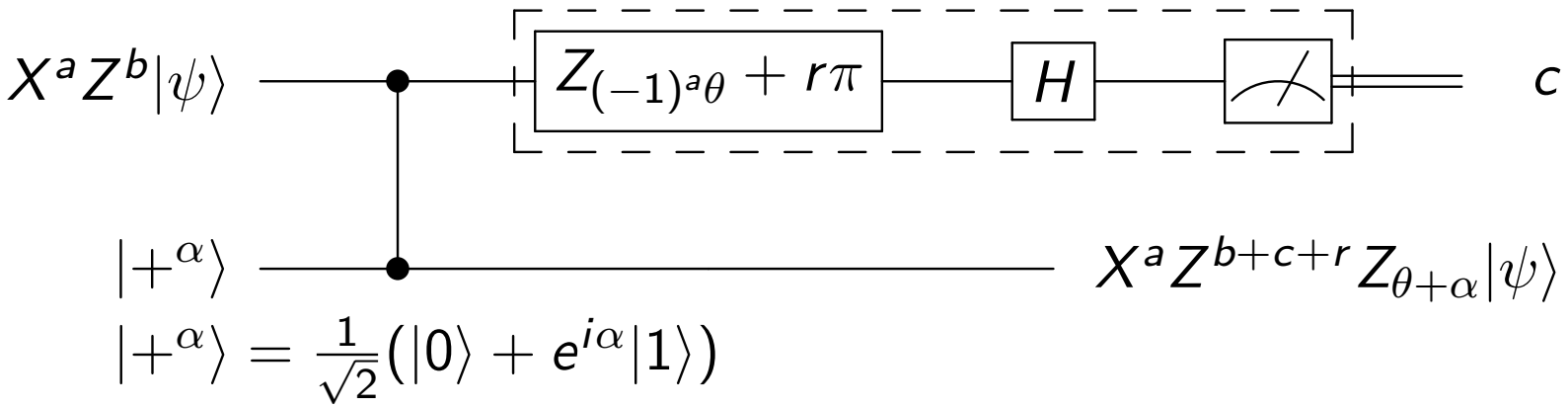


## "Universal Unit Cell"



# MBQC - Blindness Pt. 3

**Problem:** Hiding operations from server.




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

**Intuition:**

- The client knows $\alpha$, server does not.
- $\alpha$ decorrelates server info from performed operation.

# Blind MBQC - Putting it together

Protocol:

1. Client prepares input with randomized Pauli operators for each qubit.
2. Client prepares all brickwork qubits with random phase.
3. Client sends all qubits to server.
4. Server performs brickwork state entanglement.
5. For each qubit:
   1. Client calculates measurement basis. Sends to server
   2. Server measures, sends to Client.
   3. Client updates Pauli matrices based on result.

# Sufficient Properties for Blindness

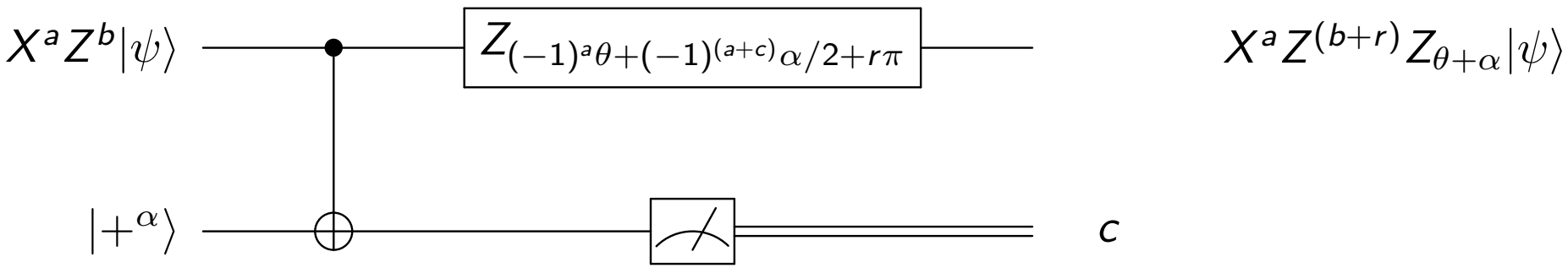
## Properties Sufficient for Blindness

- "Universal Unit Cell"
- Pauli-encrypted quantum state
- Hidden operations using random phase

**Key Recognition:** *Not unique to MBQC*
Idea: Use Phase Kickback instead of Quantum Teleportation!

# Ancilla-Driven Blind Quantum Computation

New rotation circuit:




Data *stays* on the first qubit - follows circuit model.