Universal Blind Quantum Computing

Elham Kashefi
Laboratoire d'Informatique de Grenoble

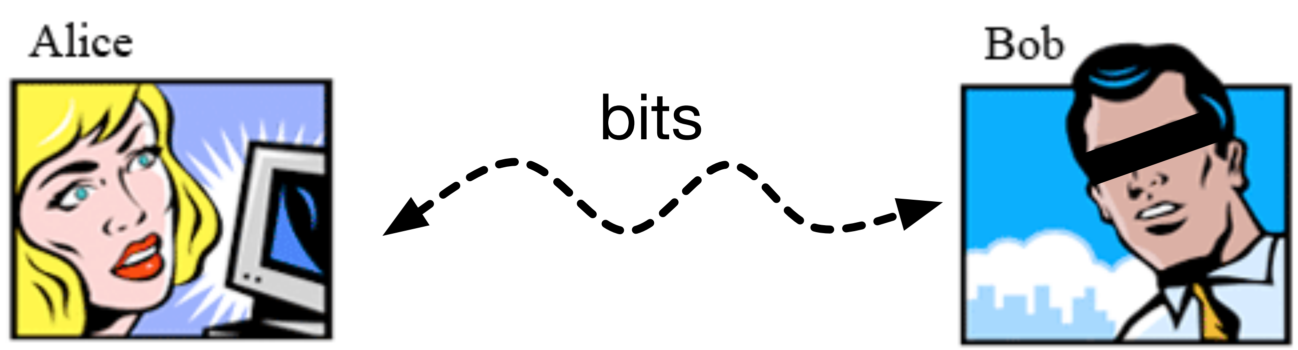
Joint work with

Anne Broadbent
Montreal

Joe Fitzsimons
Oxford

Classical Blind Computing

- Fundamentally asymmetric unlike the secure two-party communication



secret x power to compute f

- Client-Server relation with mistrusted server
- Testing Procedures
- Hiding Data

Classical Blind Computing

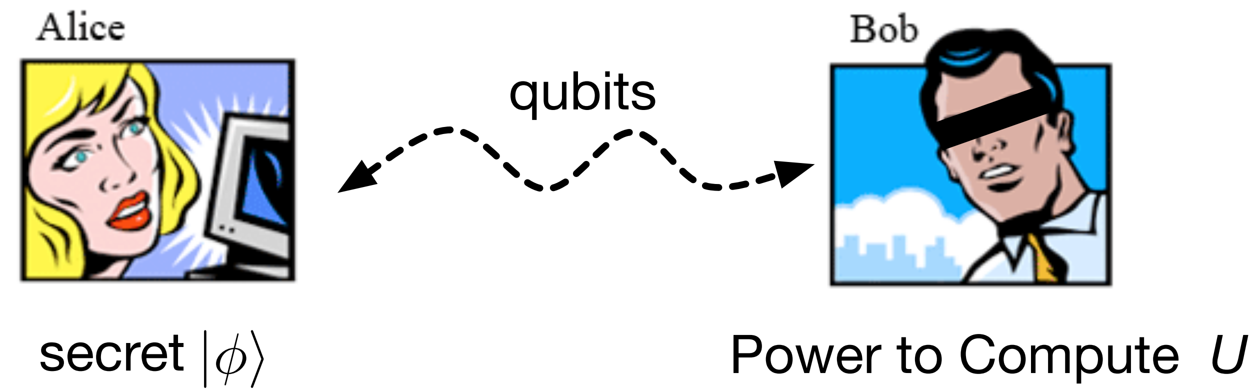
- Feigenbaum

  ➡ Computing with encrypted date for some function f

- Abadi, Feigenbaum and Kilian

  ➡ No NP-hard function has an efficient blind computing protocol

Quantum Blind Computing



- Andrew Childs - *Secure assisted QC*
  - ➡ Alice needs quantum memory, state preparation and Pauli gates
  - ➡ The unitary function is public
  - ➡ Dishonest Bob cannot be detected

- Arrighi and Salvail- *Blind QC for a restricted set of classical functions*
  - ➡ Alice needs quantum memory, state preparation and measurement
  - ➡ The classical function is public
  - ➡ Polynomial security against individual attacks

Our Result

- ➡ **Minimal Resources:** Alice needs only single qubit state preparation
- ➡ **Pure Blindness:** Bob will never learn either the data or the program
- ➡ **Universality:** Works for all classical and quantum functions
- ➡ **Security:** Against any individual or coherent attacks
- ➡ **Efficiency:** Polynomial in the size of the circuit implementing U or f
- ➡ **Detection:** Exponentially small probability of not detecting a deceptive Bob

The Key Elements

- **One-time pad**

$$message = data \oplus key$$

- **Quantum one-time pad**

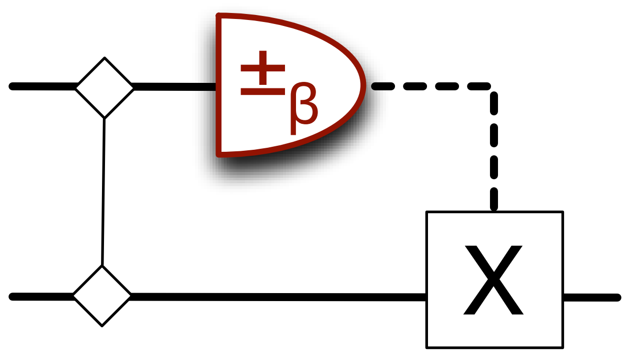
$$\frac{1}{4}\sum_{j,k=0}^{1} Z^k X^j |\psi\rangle\langle\psi| X^j Z^k = \frac{I}{2}$$

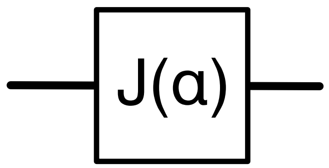
Quantum one-time pad is secure against any general attacks

The Key Elements

- **One-qubit Teleportation**

$$J(\alpha) \ := \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$



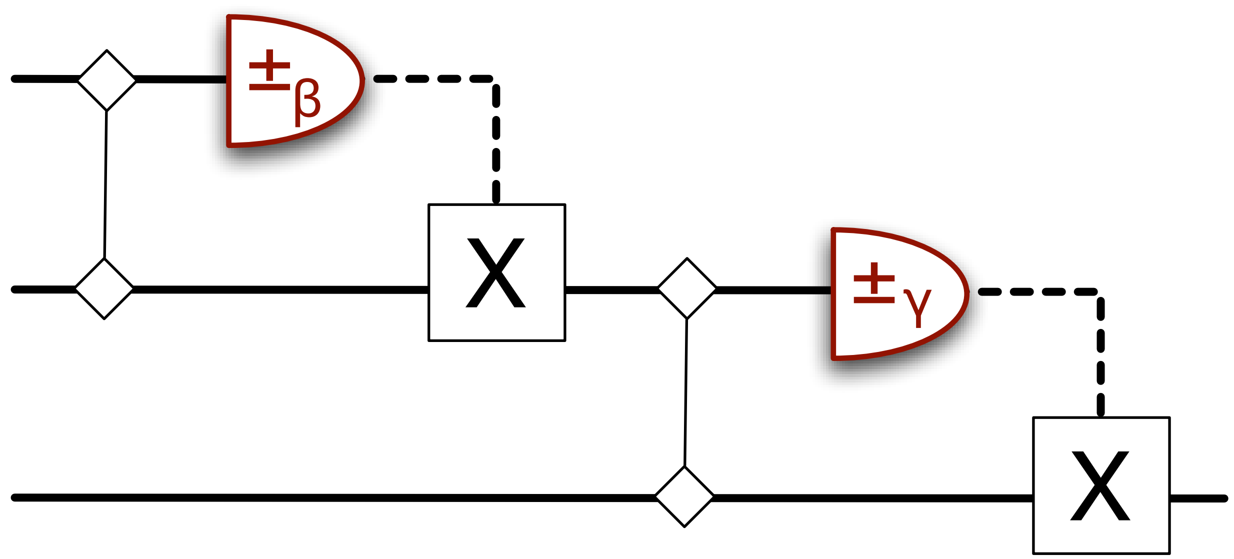


$$\begin{aligned} M^{\alpha}|\phi\rangle &= M^{\alpha} \quad Z(-\theta)Z(\theta) \quad |\phi\rangle \\ &= M^{\alpha-\theta}(Z(\theta)|\phi\rangle) \\ &= M^{\beta}|\psi\rangle \end{aligned}$$

Observation. One-time pad of the quantum state leads to one-time pad of the angle

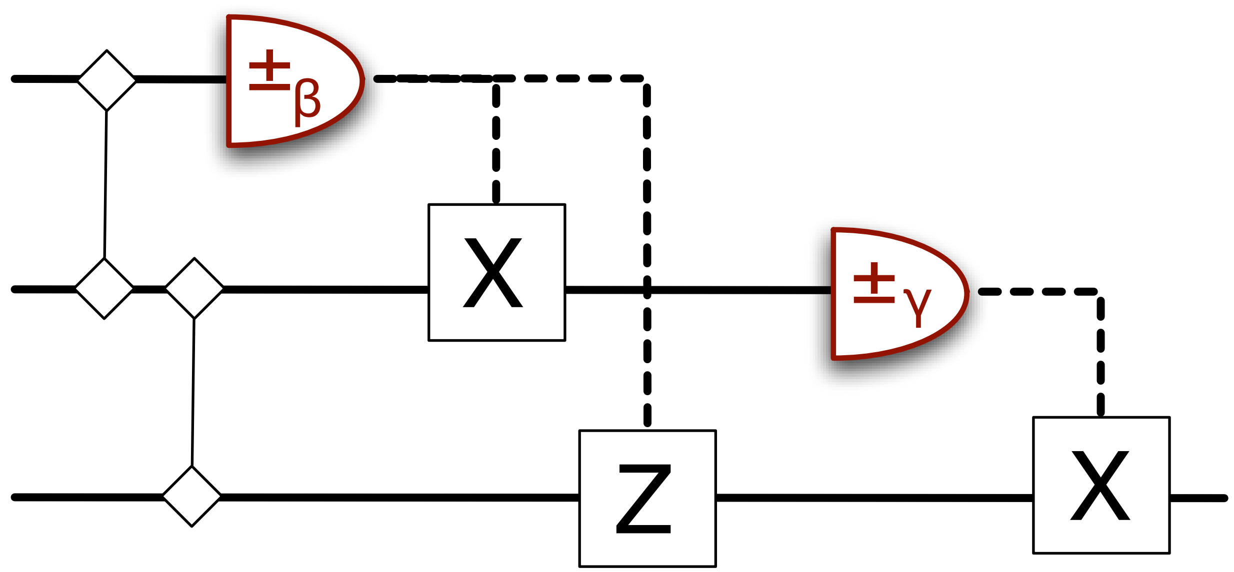
The Key Elements

- **Several one-qubit Teleportations**



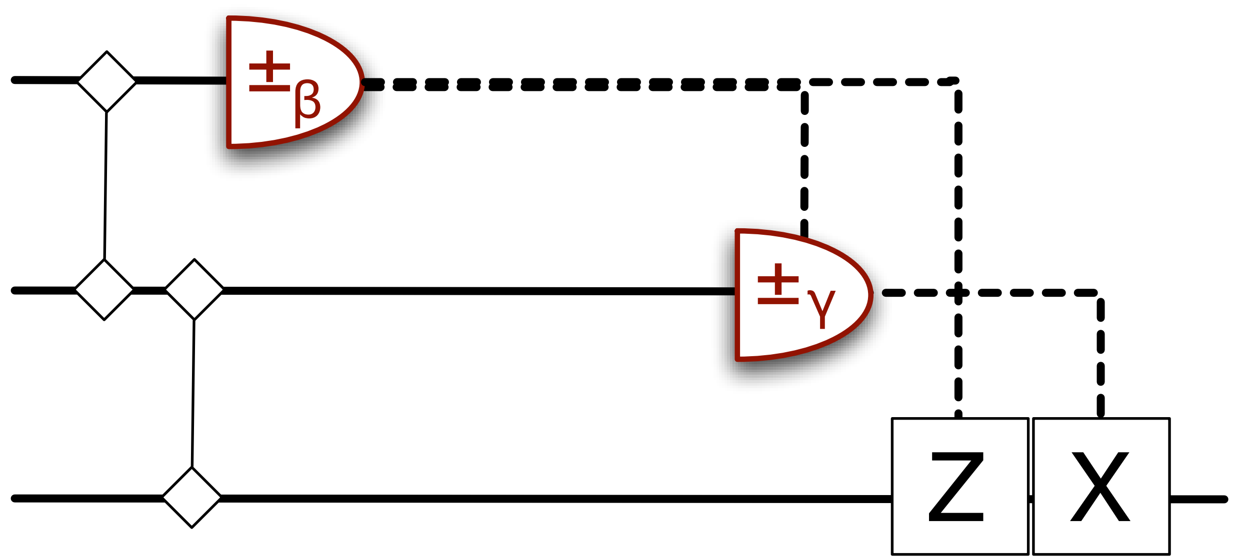
The Key Elements

- **Several one-qubit Teleportations**



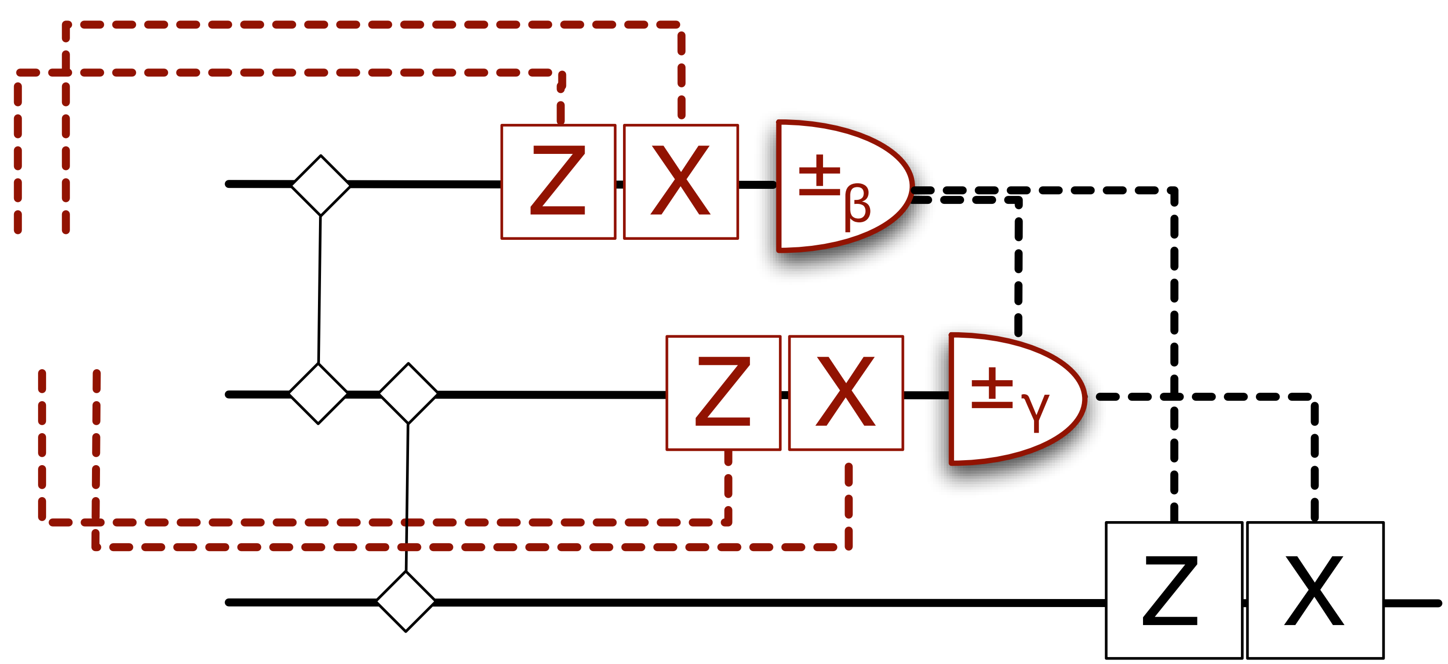
The Key Elements

- **Several one-qubit Teleportations**



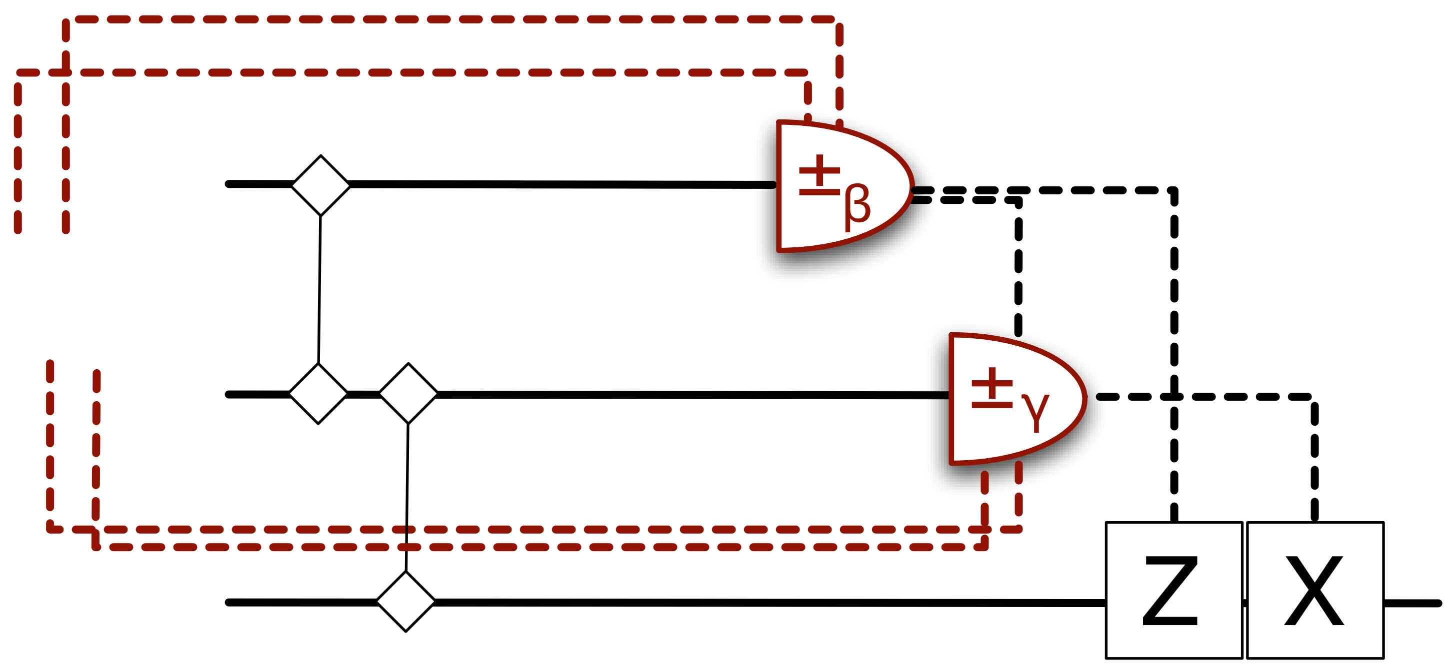
The Key Elements

- **Several one-qubit Teleportations**



The Key Elements

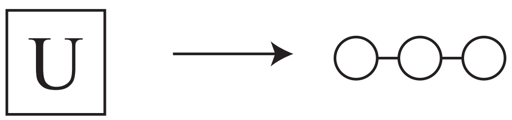
- **Several one-qubit Teleportations**

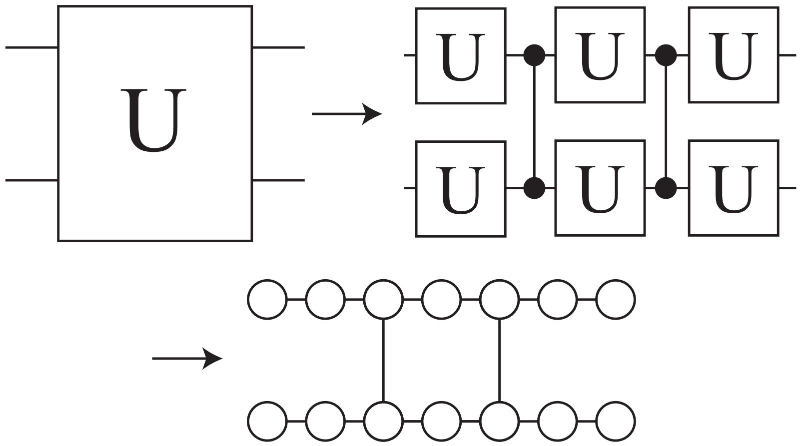


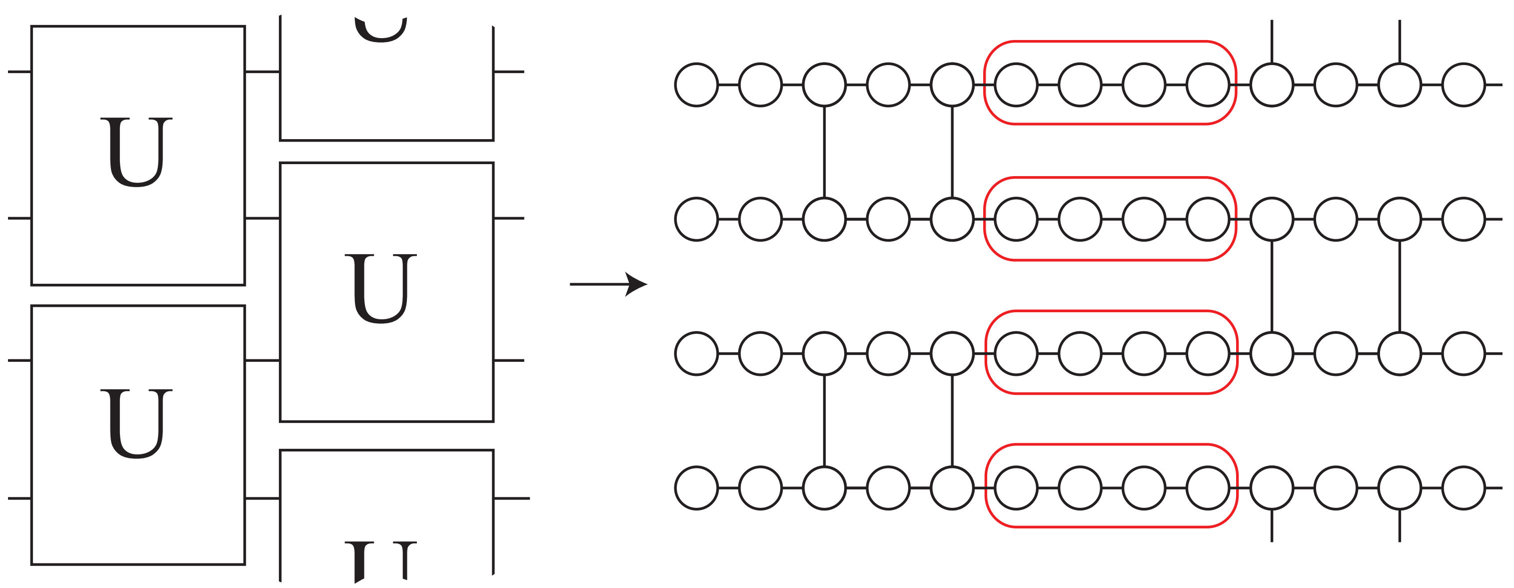
Observation. Classical one-time pad of the angles leads to quantum one-time pad of the states without requiring quantum memory

The Key Elements

- **Universality**

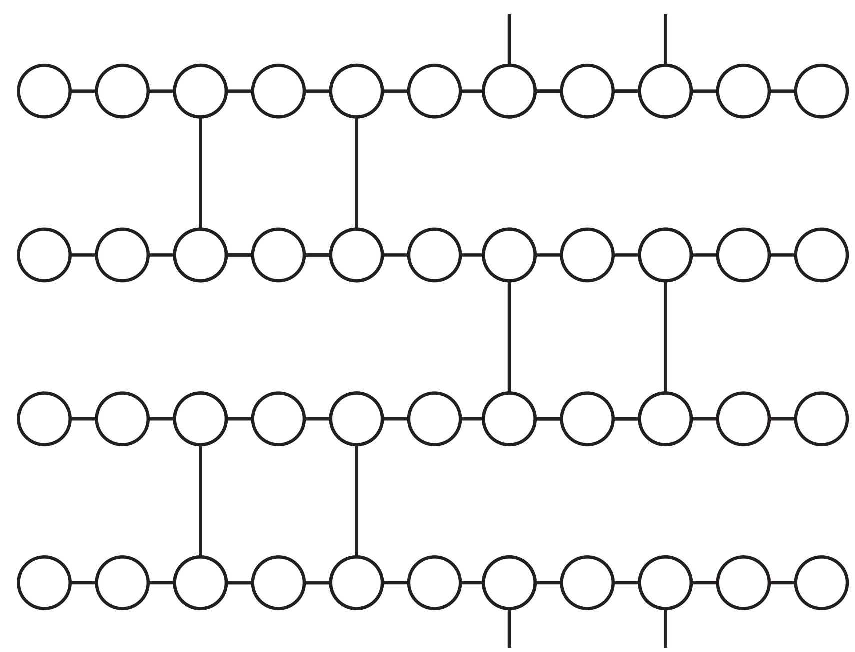






The Key Elements

- **Universality**



Observation. The true entangled structure is hidden to Bob

The Universal BQC Protocol

Alice Preparation Step

Alice

Bob

$$q_{x,y} = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta_{x,y}}|1\rangle\right)$$

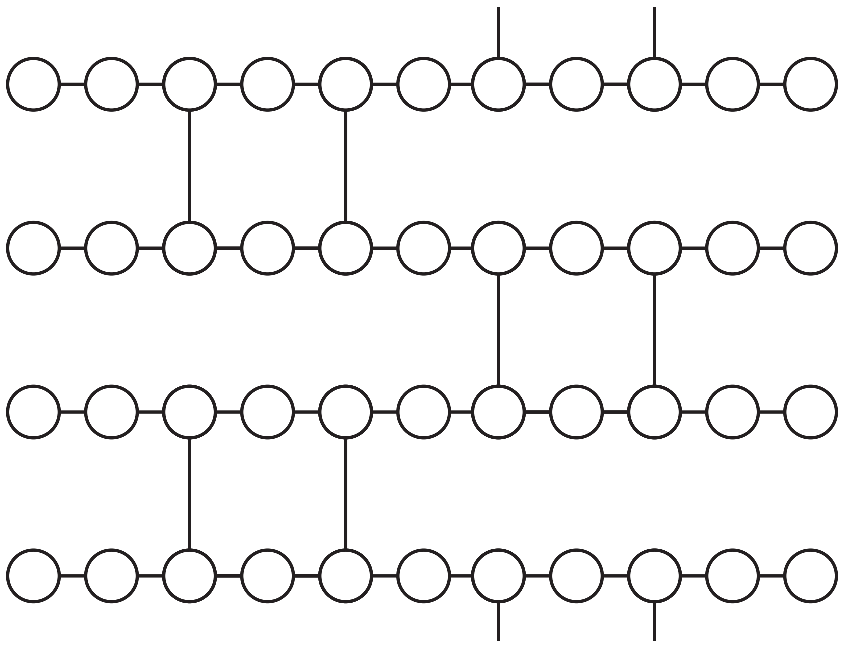
$\theta_{x,y}$ *chosen at random*

Repeat for $N = n \times d$ times for $1 \leq x \leq n \text{ and } 1 \leq y \leq d,$

where *n* is an upper bound of number of logical qubits and *d* of computation depth

The Universal BQC Protocol

Bob Preparation Step



The Universal BQC Protocol

Angles one-time pad

Alice

Bob

For all the left most qubits

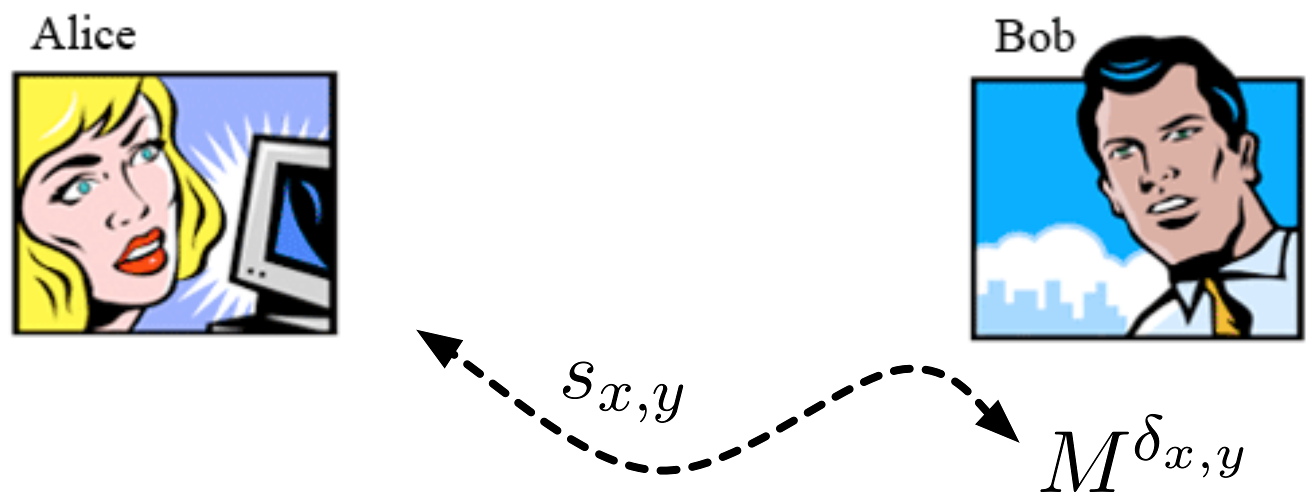
$$\delta_{x,y} = \phi_{x,y} - \theta_{x,y} + \frac{\pi}{2} r_{x,y}$$

$\phi_{x,y}$ *real angle including the Pauli corrections*

$r_{x,y}$ *chosen at random*

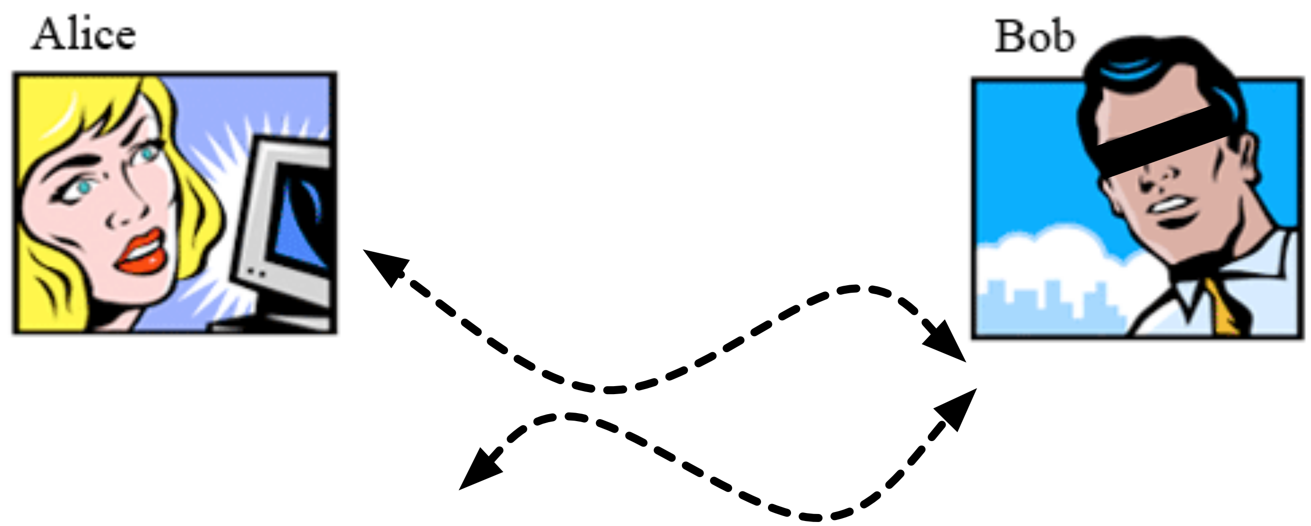
The Universal BQC Protocol

Bob Measurement



The Universal BQC Protocol

Classical Function

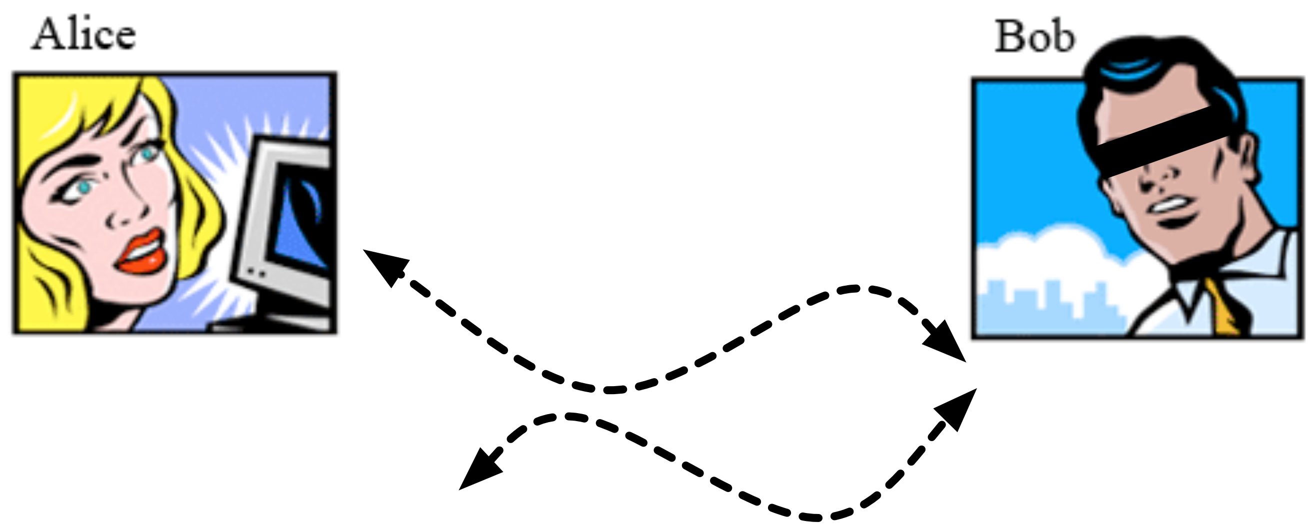


Repeat until all qubits are measured

$$\boxed{R_x = s_{x,d} - r_{x,d-1} - b_{x,d}}$$

The Universal BQC Protocol

Quantum Input and Output



Repeat until all non-output qubits are measured

$$|\psi_O\rangle = \prod_{x,d} \; Z_{x,d}\left(s_{x,d}, r_{x,d-1}, b_{x,d}, \theta_{x,y}\right)$$

Correctness

Theorem. Assume Bob follows the protocol honestly, then the outcome is correct.

Proof. Bob is simply implementing a measurement pattern

Universality of MBQC

Rewrite rules of Measurement Calculus

Privacy of Computation

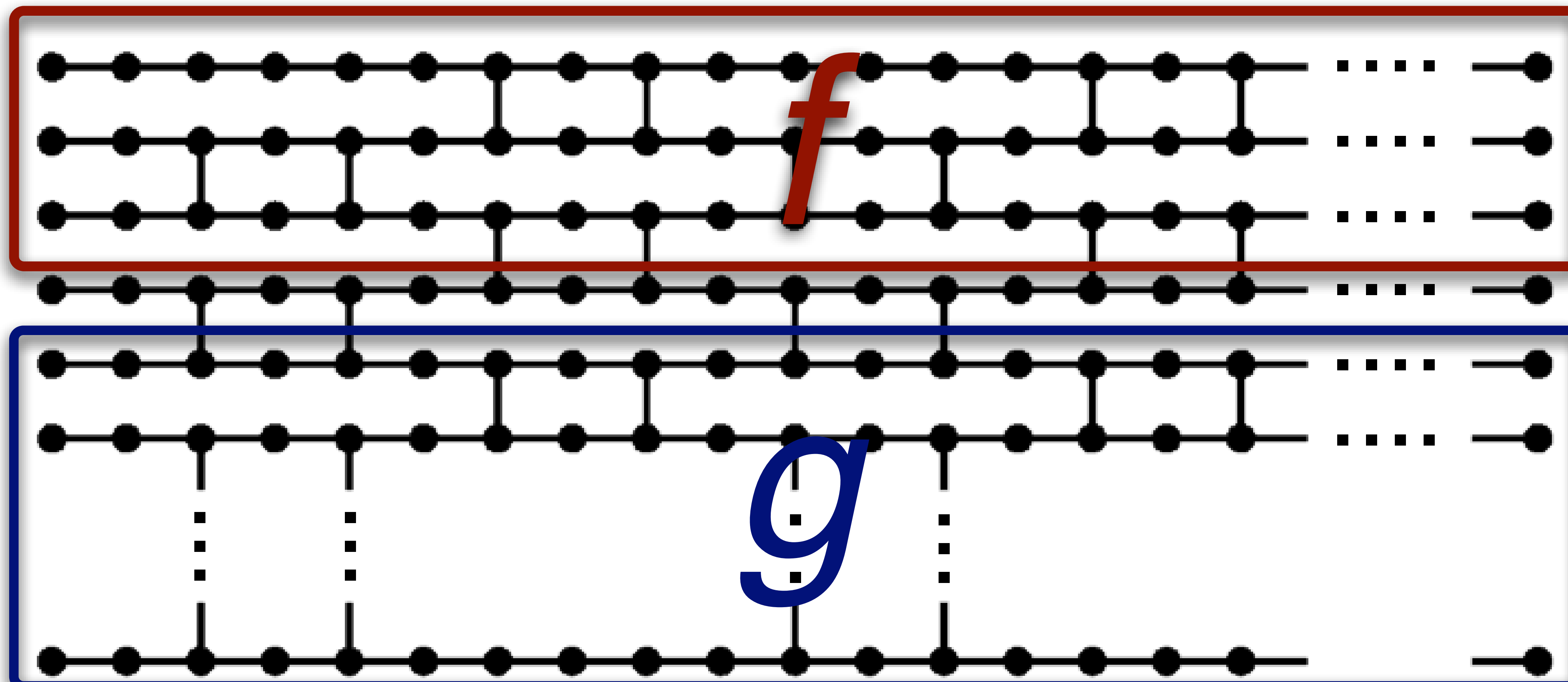
Theorem. No matter what Bob does he will never learn Alice's data or program.

Proof. In *preparation* stage the quantum one-time pad of the qubits conceals the preparation angles (Q1time-pad $\longrightarrow$ C1time-pad)

In *computation* stage the classical one-time pad of each measurements angles conceals the quantum data (C1time-pad $\longrightarrow$ Q1time-pad)

Detection

Alice adds traps (easily verifiable functions) to her real computation



Alice detects a cheating Bob with probability of $1/Poly(N)$

Detection via Quantum Authentication

Taking advantage of PURE blindness of Bob !

Alice

Bob

A random error-correcting codes

Encoding N logical qubits with N+K qubits

Computation on the encoded qubits

Can not guess an undetectable error

Theorem. The probability of not detecting deceptive Bob decreases exponentially in the size of the encoding

Future Work

- ➡ The proper security definition for quantum blind computing
- ➡ Connection to the complexity hierarchy
- ➡ Other applications of distributive structures of MBQC