Universal Blind Quantum Computing (FOCS 2009)

Elham Kashefi

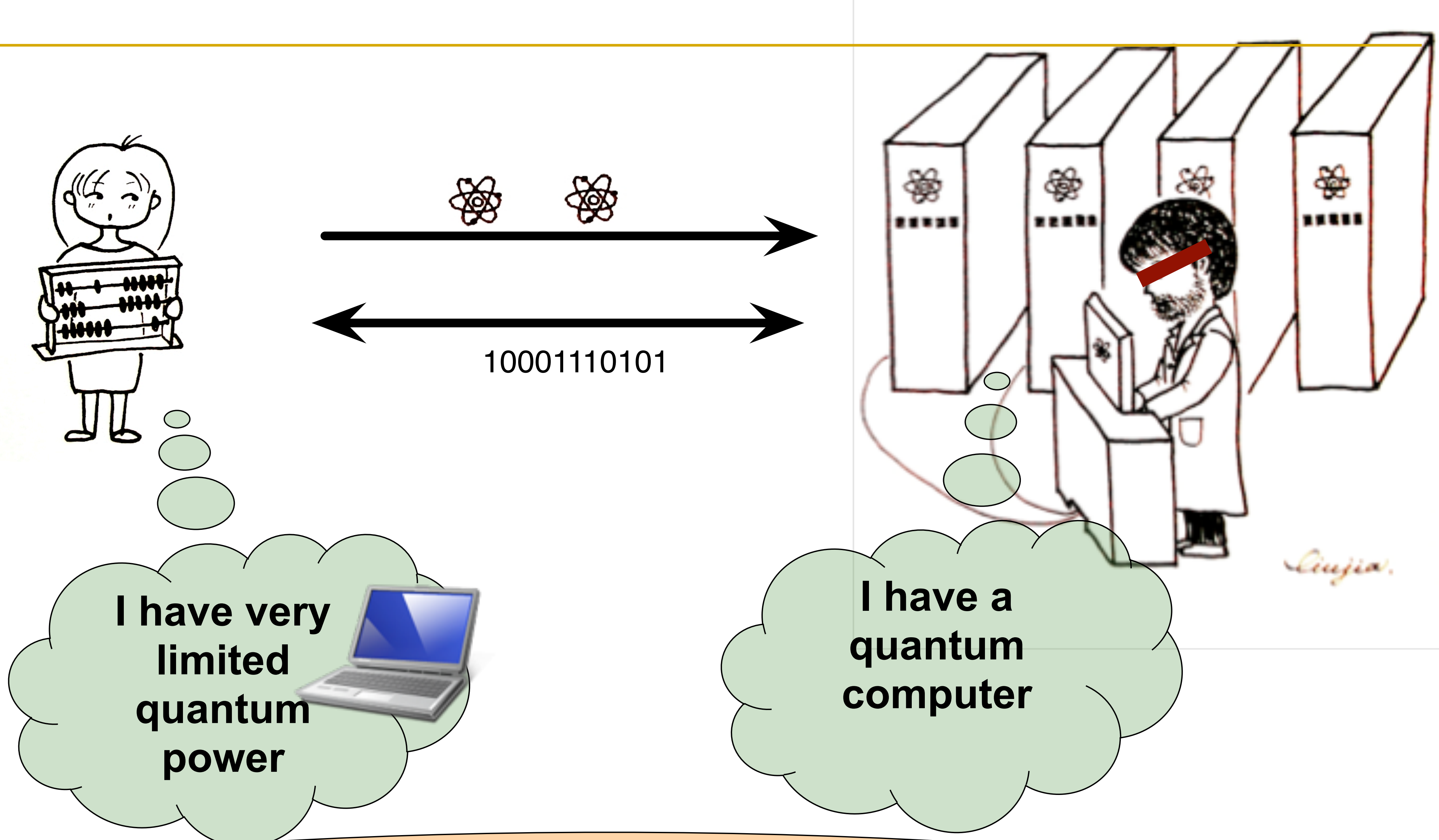
University of Edinburgh

Anne Broadbent

IQC- Waterloo

Joe Fitzsimons

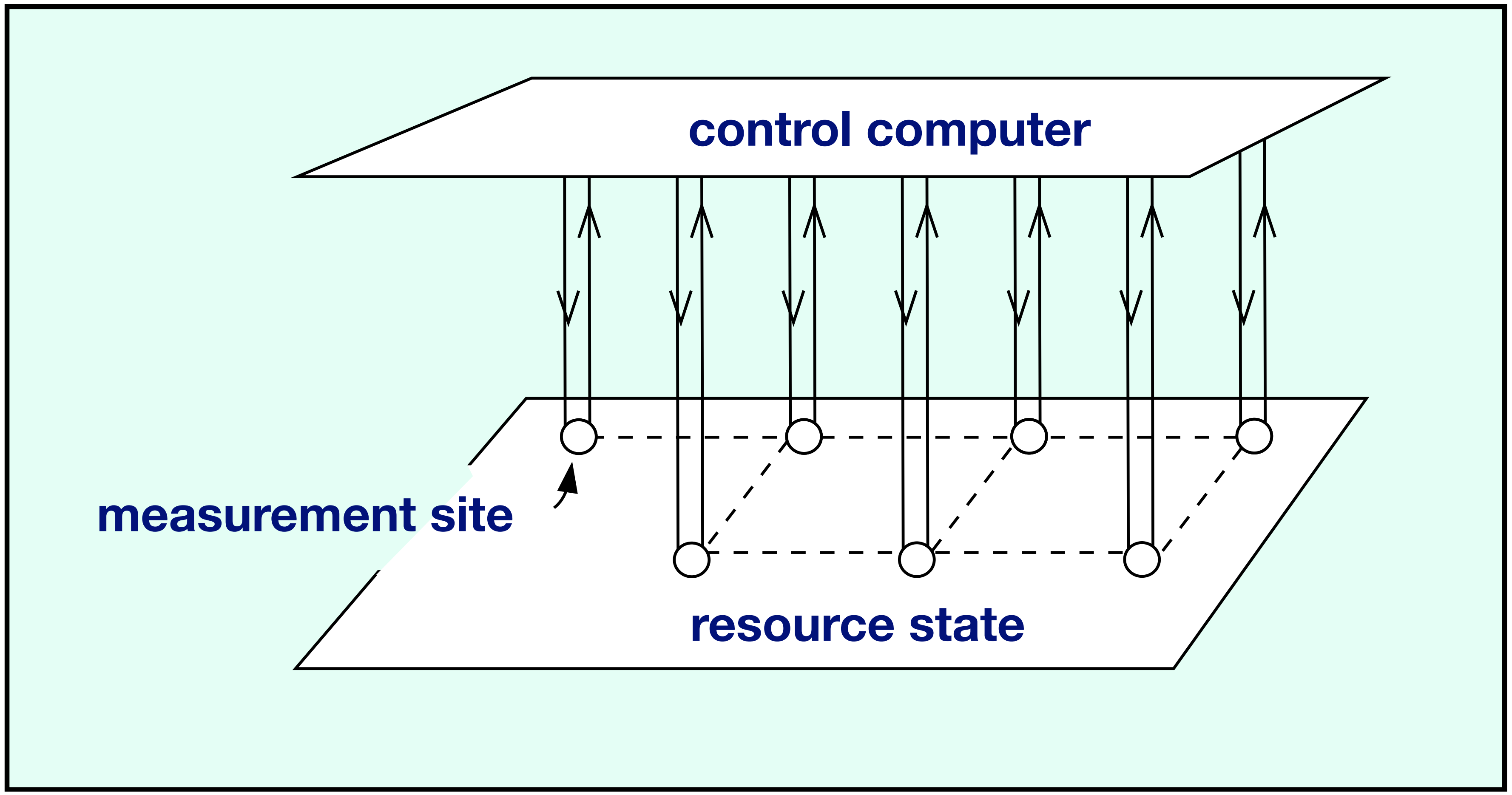
Oxford



perfect privacy &

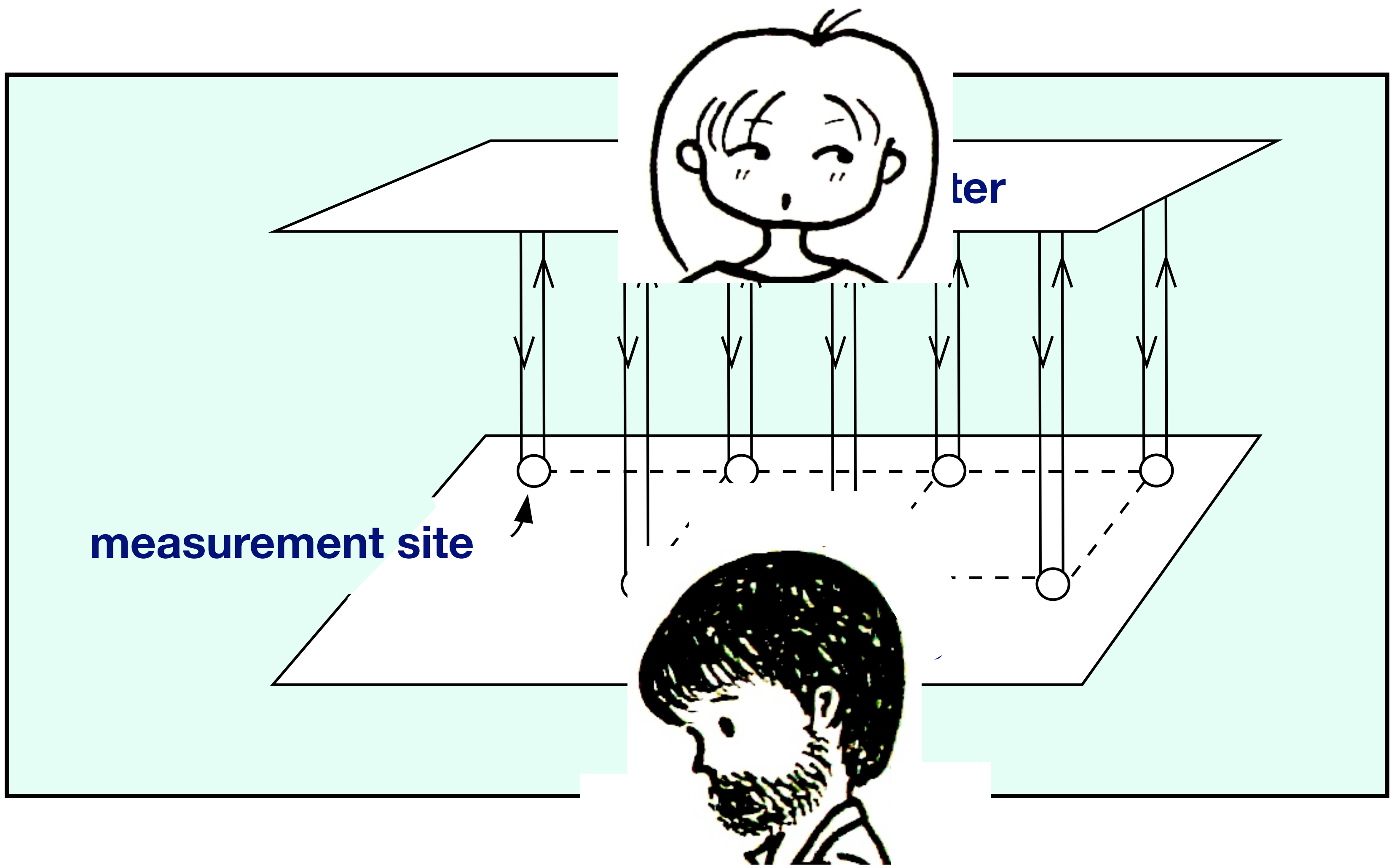
detection of interfering Bob

Key Idea



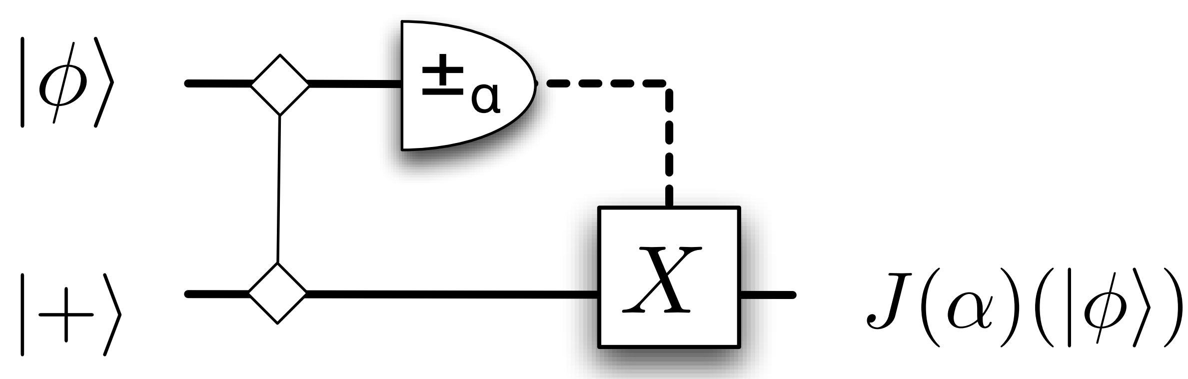
Program is encoded in the classical control computer
Computation Power is encoded in the entanglement

The First MBQC Protocol



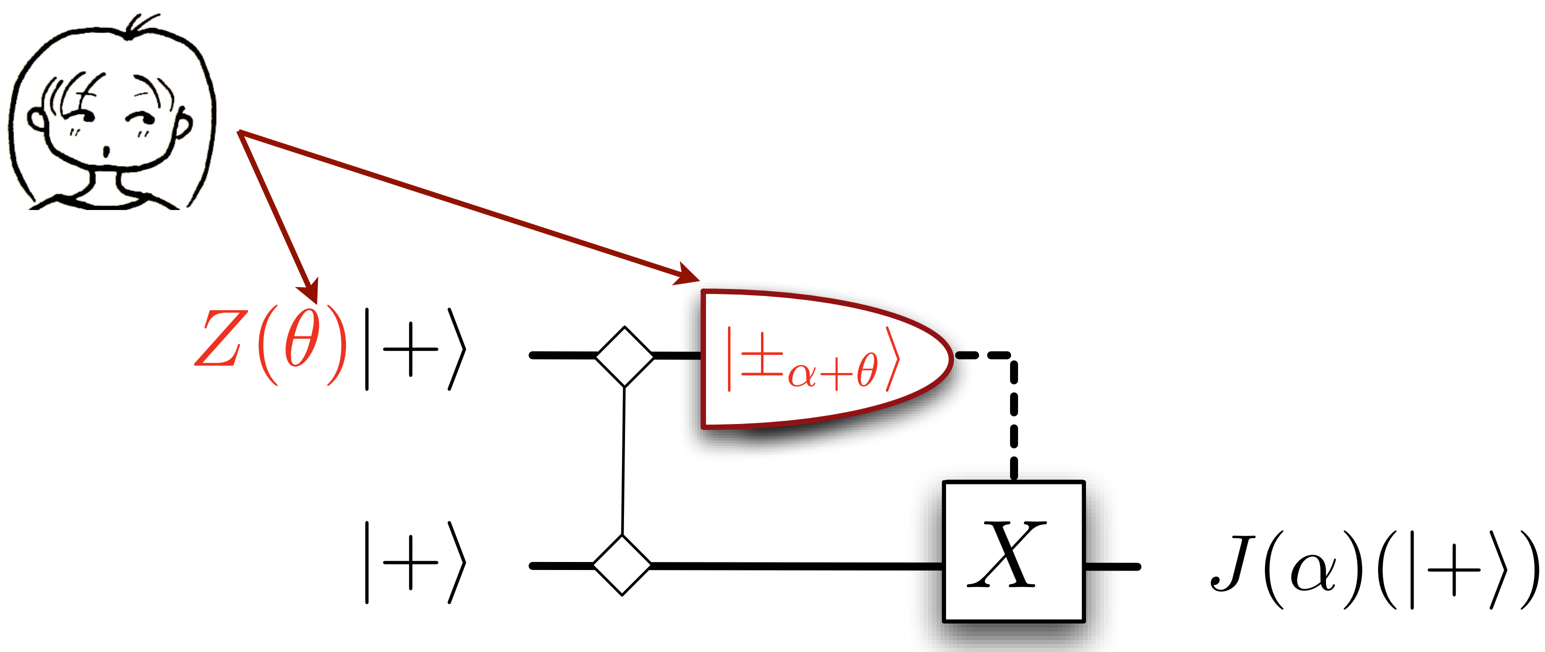
Encoding of the Angles

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



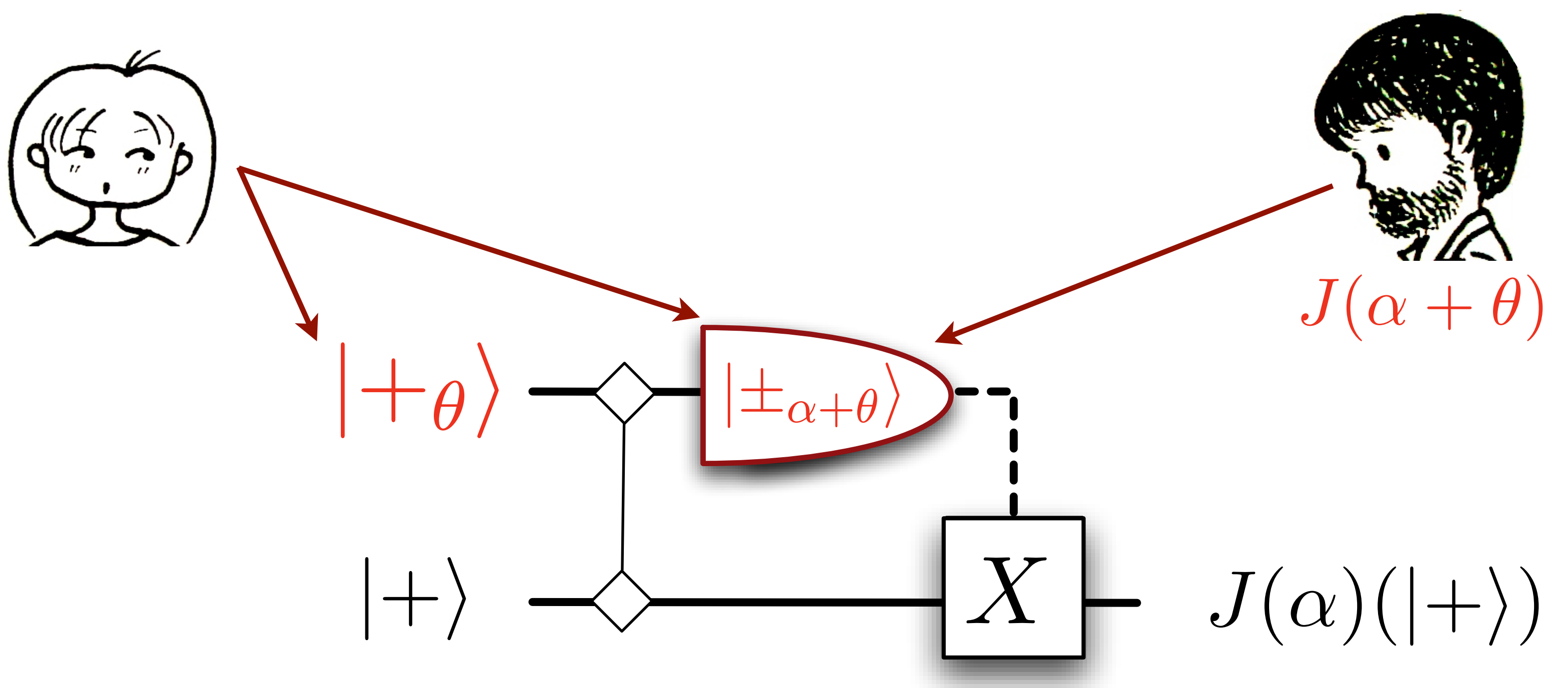
Encoding of the Angles

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



Encoding of the Angles

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

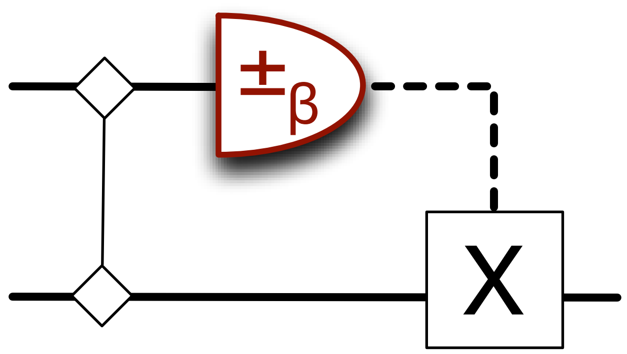


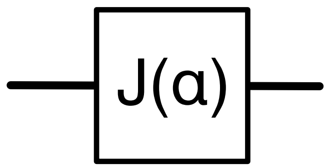
Uncertainty Principle. if θ is chosen uniformly random and independent of α then $(\alpha+\theta)$ is also uniformly random

The Key Elements

- **One-qubit Teleportation**

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



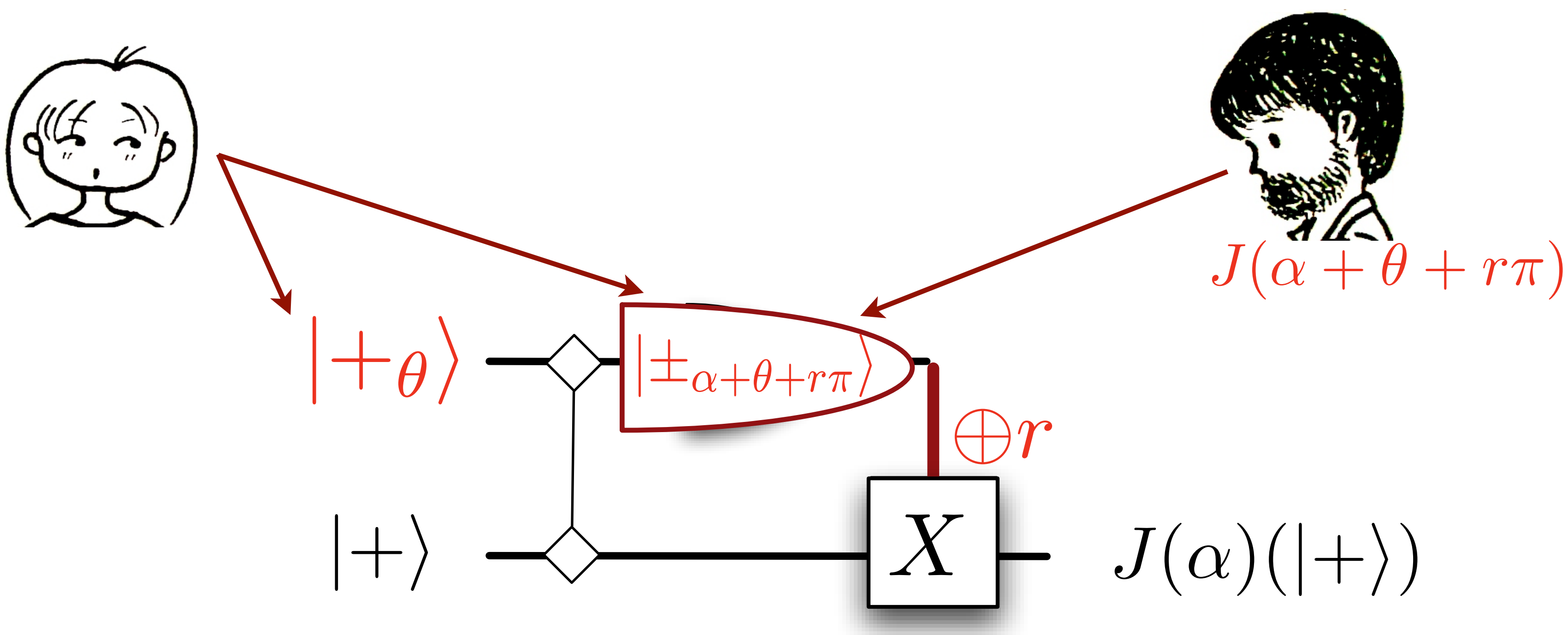


$$\begin{aligned} M^{\alpha}|\phi\rangle &= M^{\alpha} \quad Z(-\theta)Z(\theta) \quad |\phi\rangle \\ &= M^{\alpha-\theta}(Z(\theta)|\phi\rangle) \\ &= M^{\beta}|\psi\rangle \end{aligned}$$

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

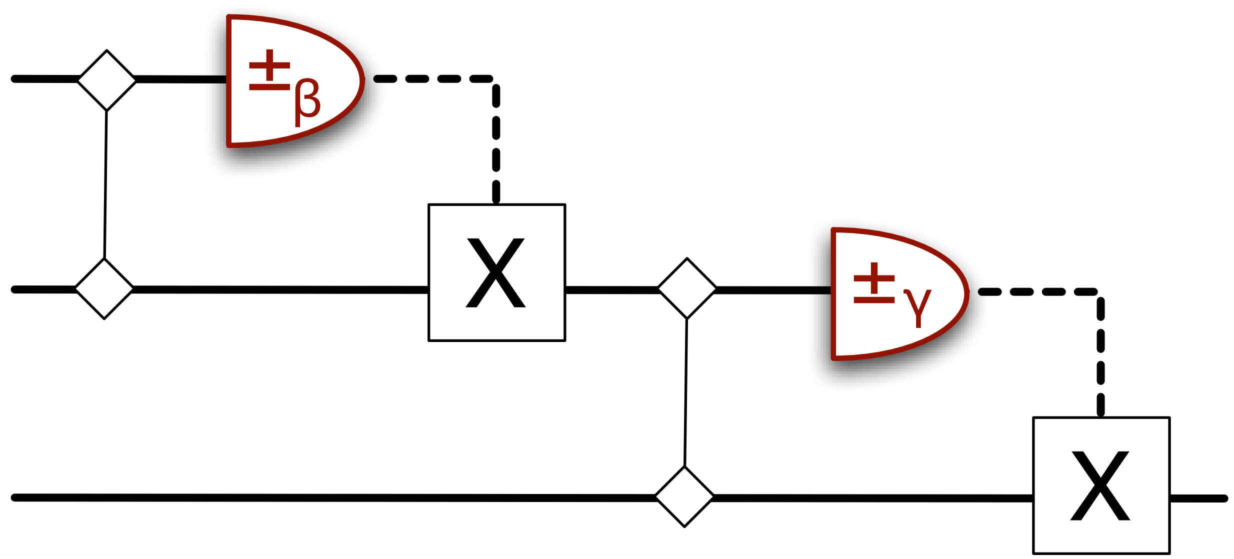
Encoding of the Angles

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



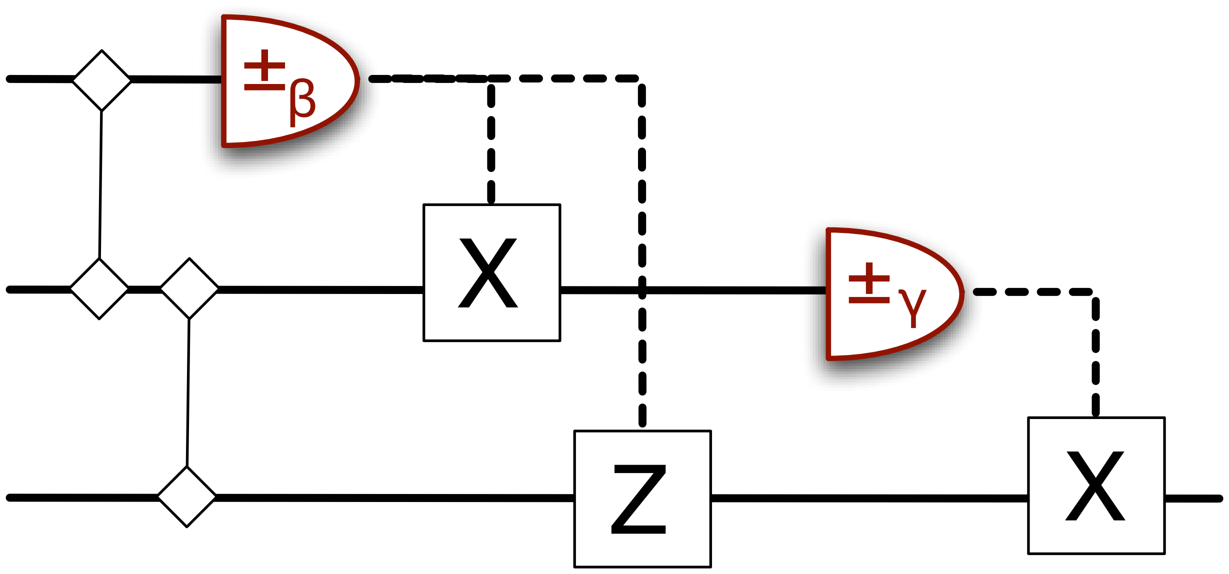
The Key Elements

- **Several one-qubit Teleportations**



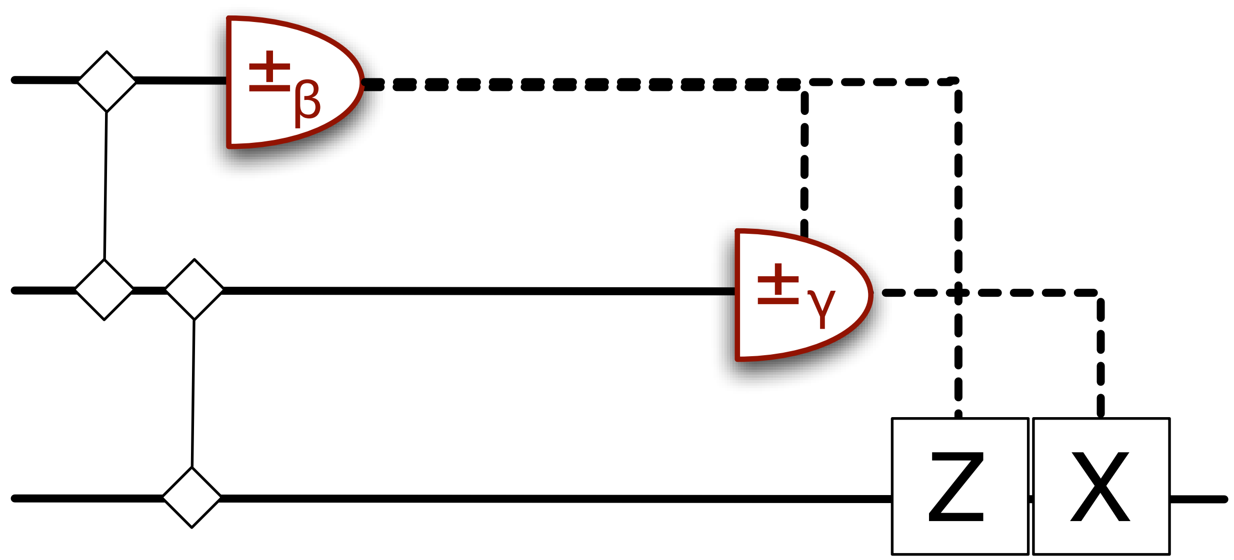
The Key Elements

- **Several one-qubit Teleportations**



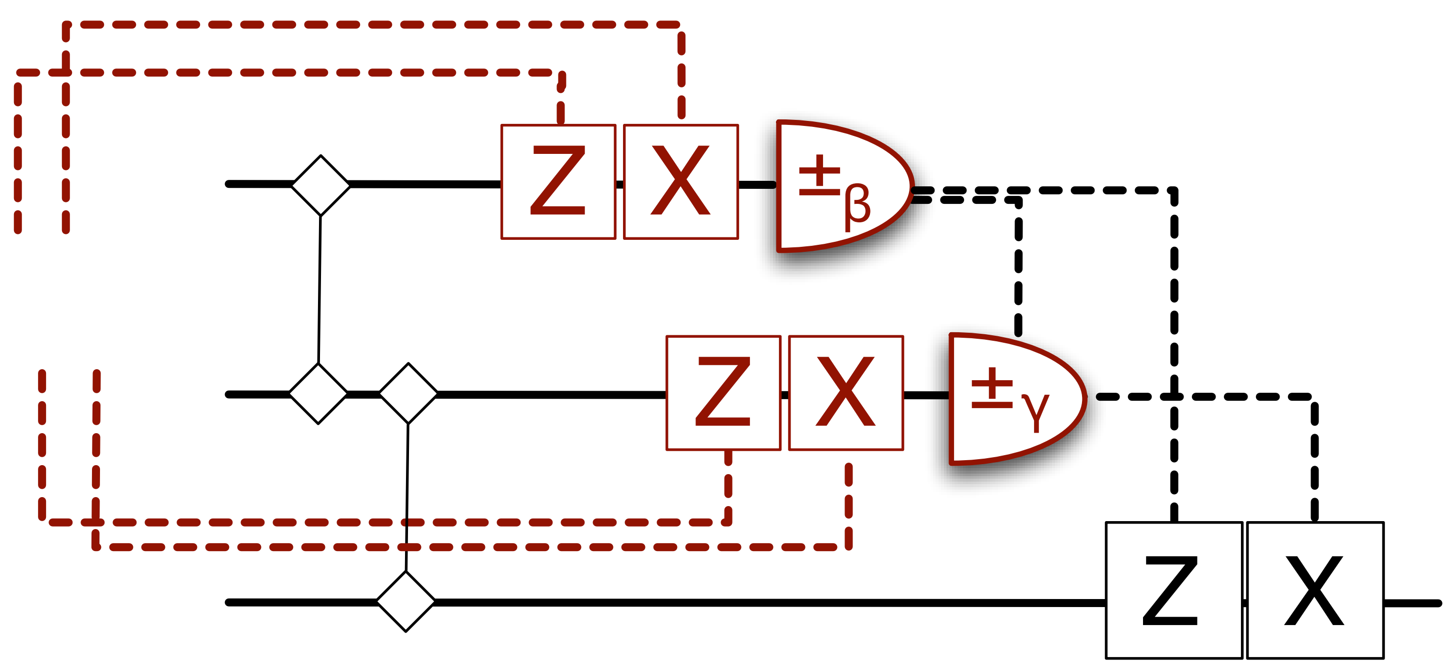
The Key Elements

- **Several one-qubit Teleportations**



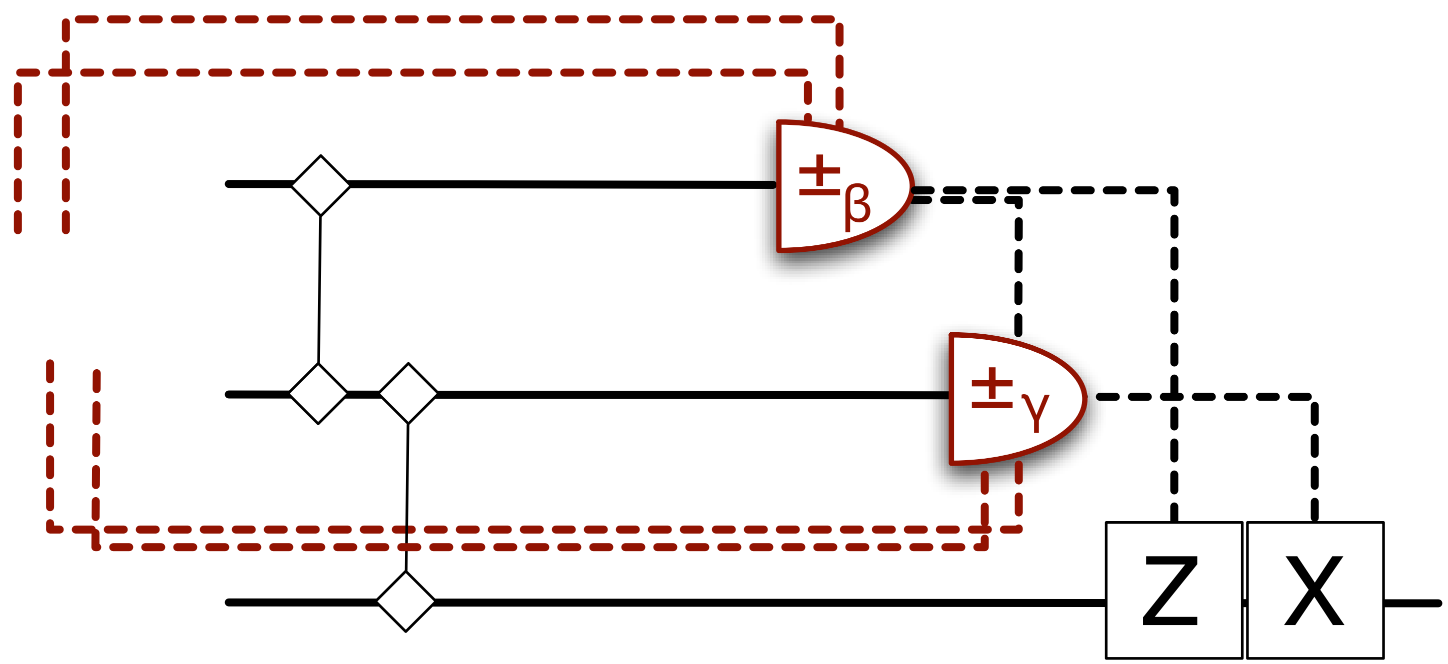
The Key Elements

- **Several one-qubit Teleportations**



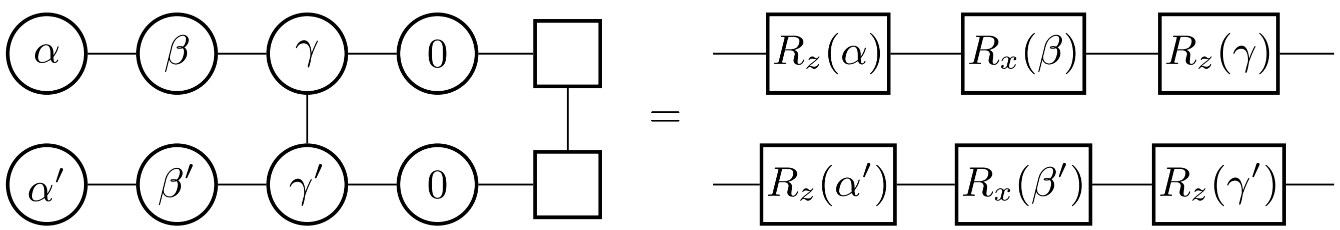
The Key Elements

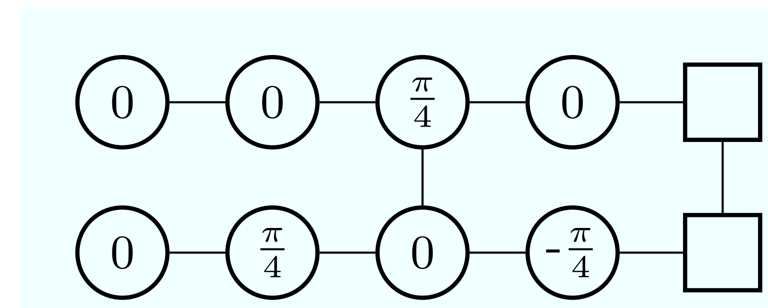
- **Several one-qubit Teleportations**

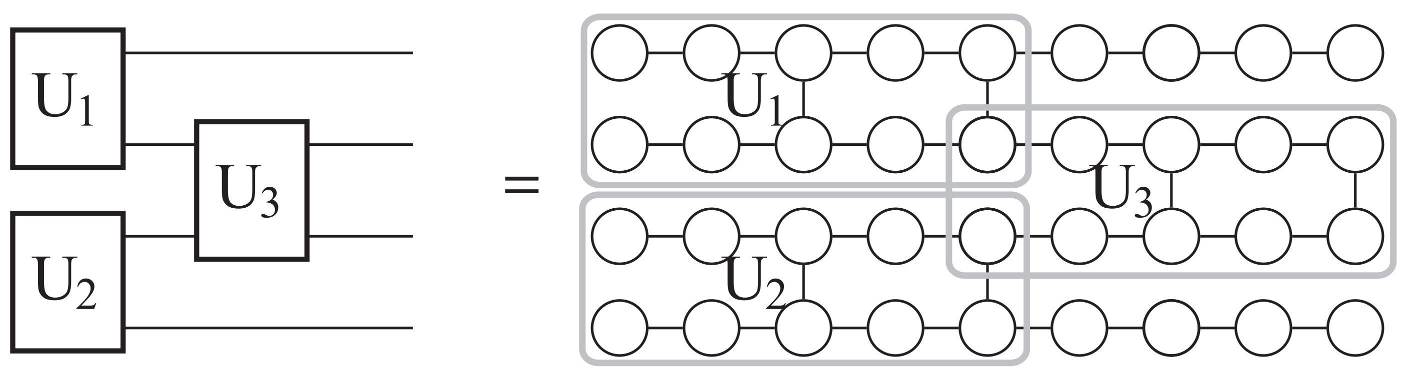


Observation. Classical one-time pad of the angles leads to quantum one-time pad of the states without requiring quantum memory

Universality







Generic Resource. Leaking only the dimension, i.e. upper bound on the input size and the depth

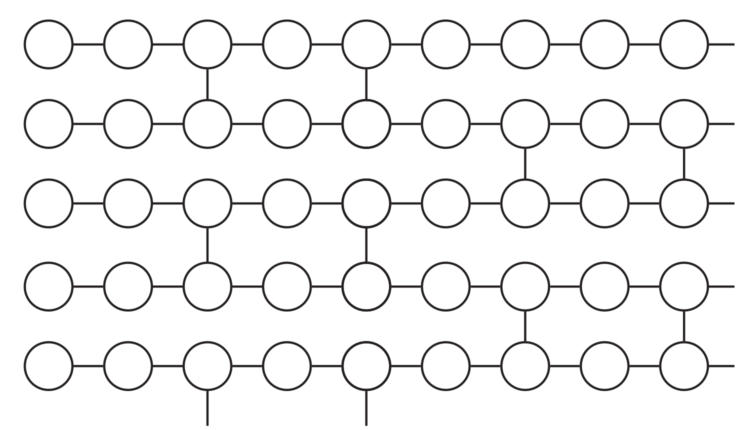
Main Protocol

$$X = (\tilde{U}, \{\phi_{x,y}\})$$

$$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$$

$$\phi'_{x,y} = (-1)^{s^X_{x,y}}\phi_{x,y} + s^Z_{x,y}\pi$$

$$\delta_{x,y}$$



$$r_{x,y} \in_R \{0,1\}$$

$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$

$$\{|+_{\delta_{x,y}}\rangle, |-_{\delta_{x,y}}\rangle\}$$

$$s_{x,y} \in \{0,1\}$$

$$s_{x,y} := s_{x,y} + r_{x,y}$$

Blindness

Protocol P on input $X = (\tilde{U}, \{\phi_{x,y}\})$ leaks at most $L(X)$

➡ The distribution of the classical information obtained by Bob is independent of X

➡ Given the above distribution, the quantum state is fixed and independent of X

Proof (L(X)=m,n)

➡ Independence of Bob's classical information

$$\theta_{x,y} \in_R \{0, \cdots, 7\pi/4\}$$

$$r_{x,y} \in_R \{0, 1\}$$

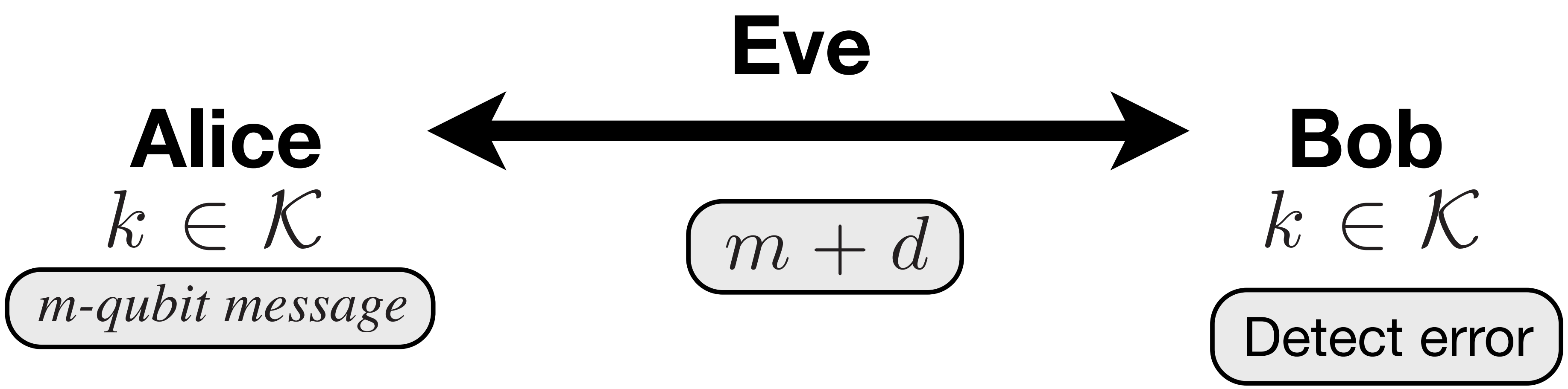
$$\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$$

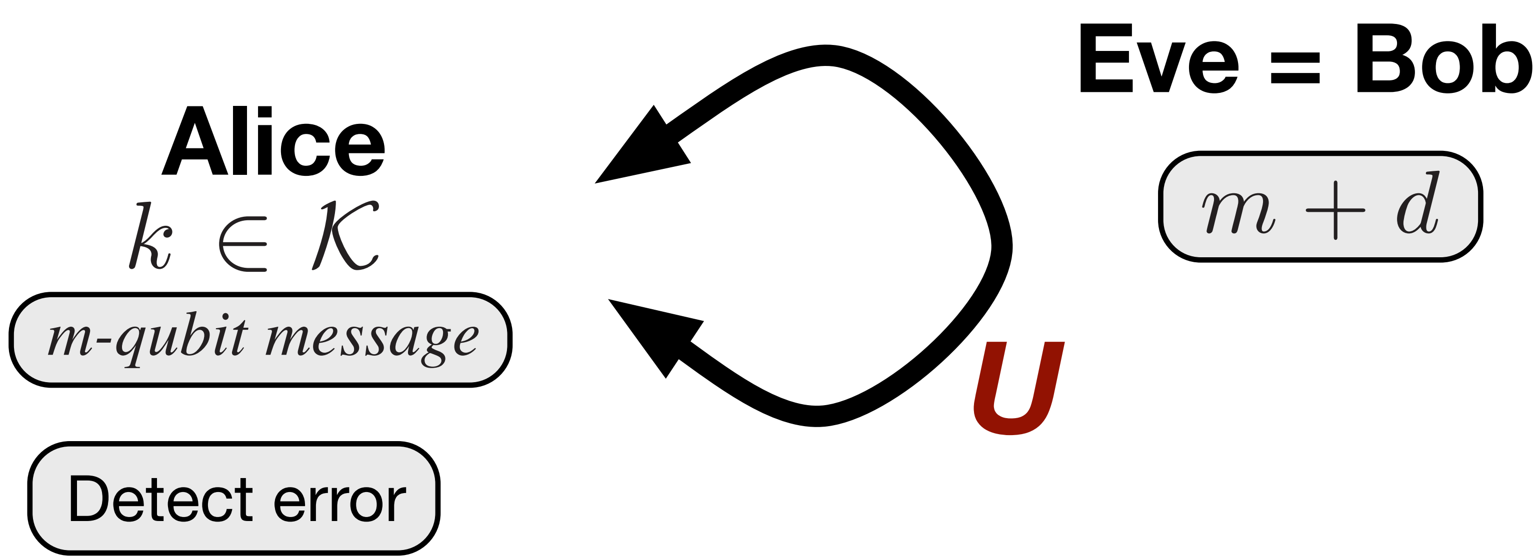
➡ Independence of Bob's quantum information for a fixed δ

1. $r_{x,y} = 0$ so $\delta_{x,y} = \phi'_{x,y} + \theta'_{x,y}$ and $|\psi_{x,y}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\delta_{x,y} - \phi'_{x,y})}|1\rangle)$.

2. $r_{x,y} = 1$ so $\delta_{x,y} = \phi'_{x,y} + \theta'_{x,y} + \pi$ and $|\psi_{x,y}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i(\delta_{x,y} - \phi'_{x,y})}|1\rangle)$.

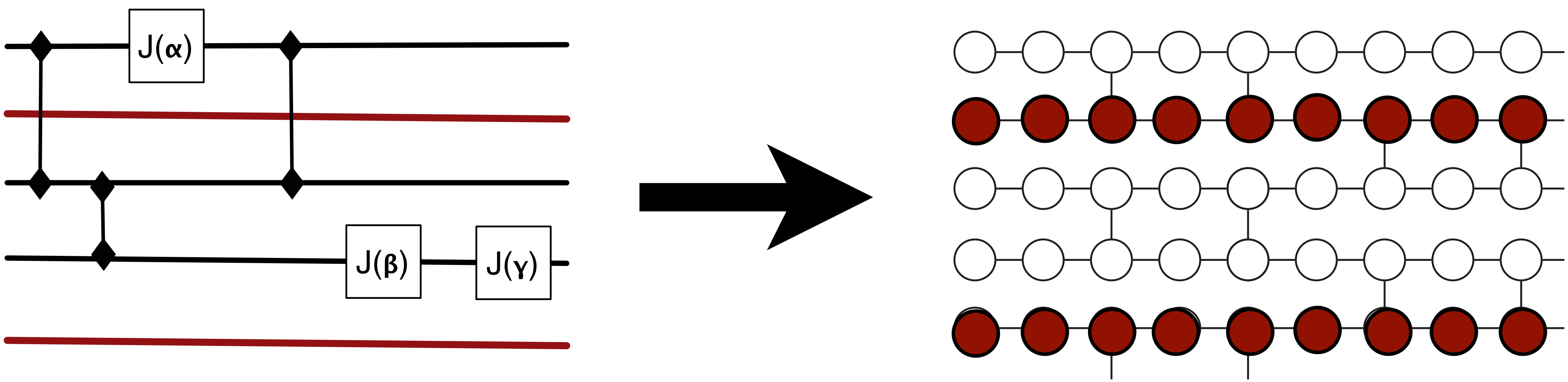
Authentication





Classical Output

She adds *N* random trap wire in $|0\rangle, |1\rangle$



Bob's interference either has no effect on classical output

or he will get caught with probability 1/2

Repeat *s* times, Alice accepts if

all outputs are identical.

Quantum Output and Fault Tolerance

Alice choses a random error correcting code.

[BCGST 02]. A family of codes where

$$\forall\, E_x \in E \; with \; x \neq 0, \#\{k | x \in Q_k^{\perp} - Q_k\} \leq \epsilon(\#\mathcal{K}).$$

Alice should also estimate the error rate.

Random **trap** qubits in eigenstate of *X, Y, Z*

The whole encoded pattern is Blind to Bob

Verification

Vazirani (07)

Can we test the validity of QM in the regime of exponential-dimension Hilbert Space?

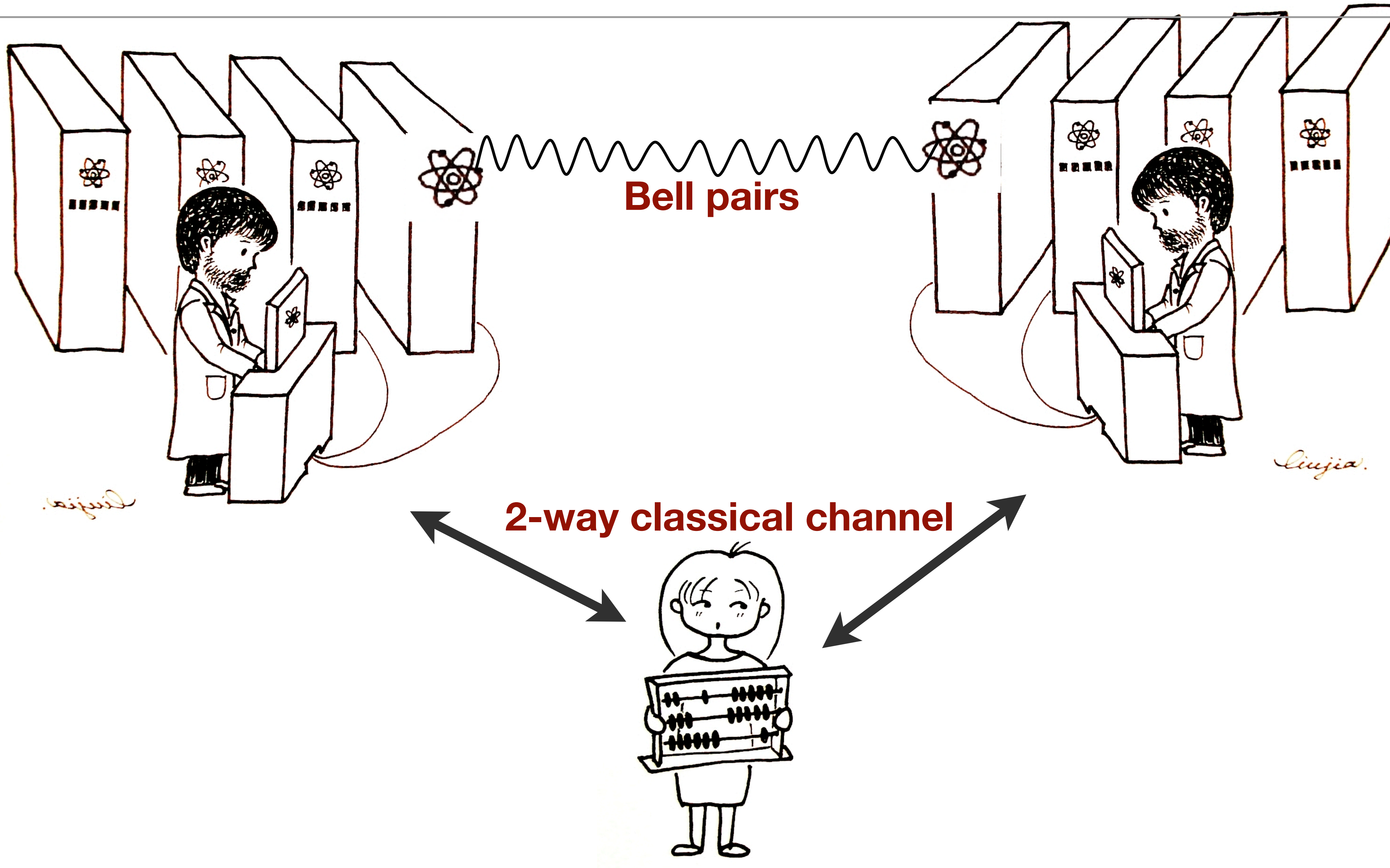
Interactive Proofs

Gottesman (04) - Aaronson **$25** *Challenge (07)*

Does every language in the class BQP admit an interactive protocol where the prover is in BQP and the verifier is in BPP?

Can we classically and efficiently verify quantum devices ?

Interactive Proofs



Classical Computer + 2 Provers + Entanglement = Quantum Computer

Interactive Proofs

Quantum Computer + Multi Interactive Proof =
Classical Computer + Multi Interactive Proof =
NEXP

[Kobayashi, Matsumoto, 2003]

Quantum Computer + Interactive Proof =
Classical Computer + Interactive Proof =
PSPACE

[Jain,Ji,Upadhyay,Watrous 2009]

parallel matrix multiplicative weights update method to a class of semidefinite programs

Entangled Provers

Classical Channel + Entanglement = Quantum Channel

Classical Computer + 2 Provers + Entanglement = Quantum Computer

Quantum Computer + Multi Interactive Proof + Entanglement =
Classical Computer + Multi Interactive Proof + Entanglement =

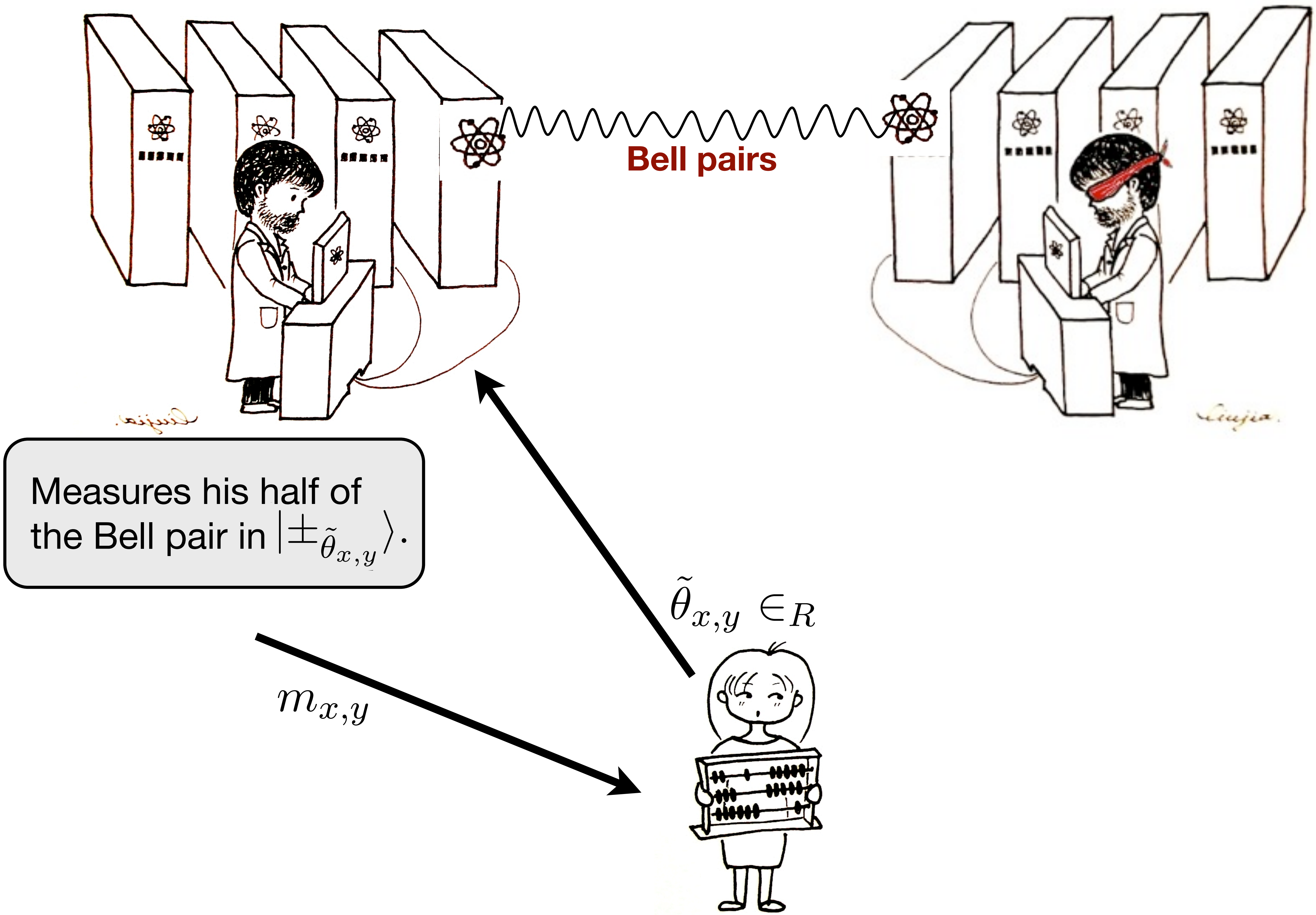
[Broadbent, Fitzsimons, Kashefi 2010]

Speculation

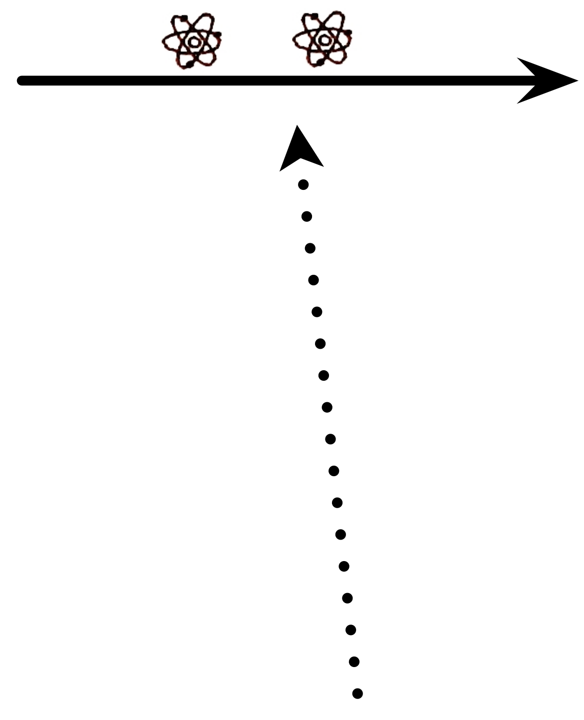
Quantum computing adds no power to the interactive proof system
even with multi provers and entanglement

Entanglement = Quantum memory

Interactive proof

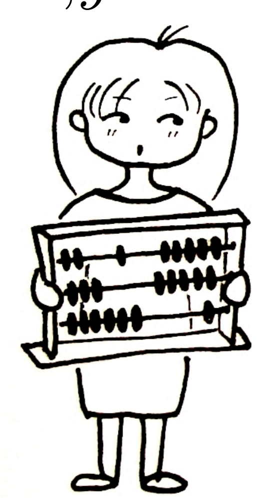


Interactive proof

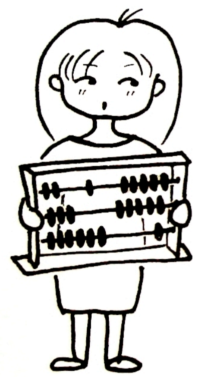


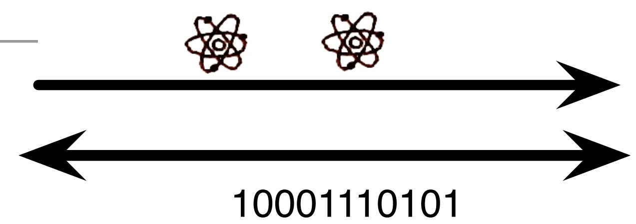
Main Protocol

$\tilde{\theta}_{x,y} \in_R$



Summary





Classical Compute

random single qubit generator

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

$$\theta = 0, \pi/4, 2\pi/4, \ldots, 7\pi/4$$

Detection of malicious Bob

Fault Tolerance

Perfect Privacy