Why physicists and computer scientists should remain partners

Elham Kashefi

University of Edinburgh

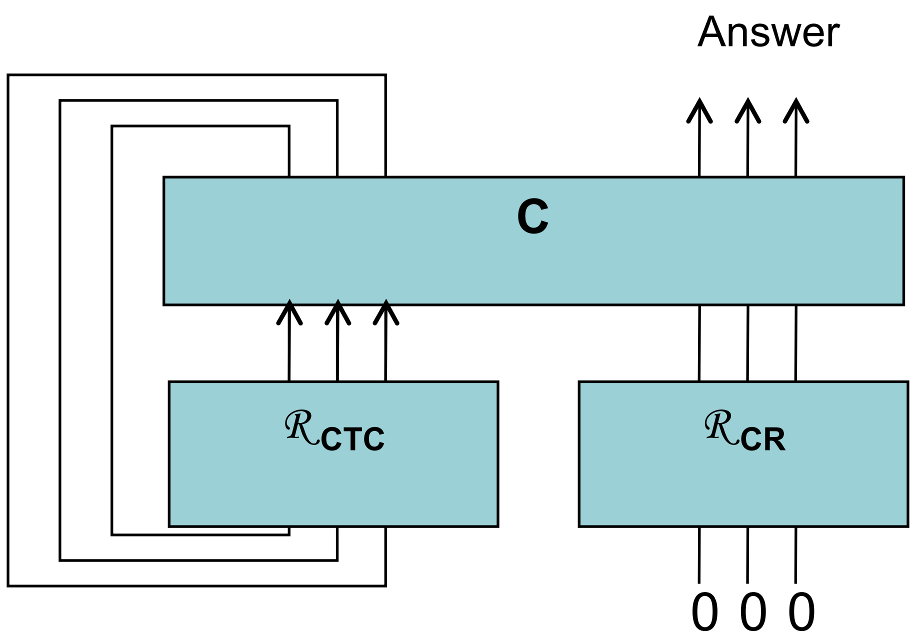
Quantum Informatics

- A Computational Revolution
- Influenced Foundational Research
- Greatest Fun Ever

Hamming is Wrong !

... By important I mean **guaranteed** a Nobel Prize and any sum of money you want to mention. We didn't work on **(1) time travel, (2) teleportation**, and (3) antigravity. They are not important problems because we do not have an attack. It's not the **consequence** that makes a problem important, it is that you have a reasonable attack."

Time Travel



"causal consistency"
A fixed-point of some evolution operator

Quantum Computer + Closed Timelike Loop =
Classical Computer + Closed Timelike Loop =
PSPACE

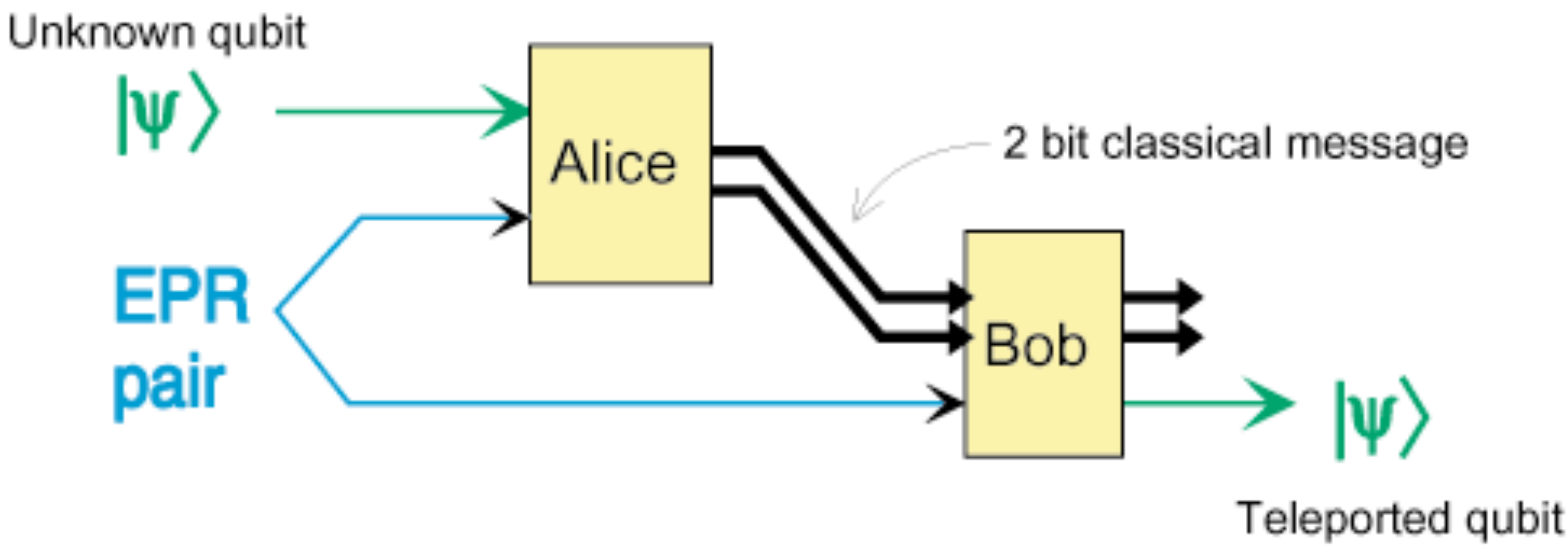
[Aaronson.Watrous 2008]

Quantum Computers + Postselected Measurements = NP

[Aaronson.Watrous 2005]

PP is closed under intersection

Teleportation



Classical Channel + Entanglement = Quantum Channel

Hamming is Right !

... He who works with the door open gets all kinds of **interruptions**, but he also occasionally gets clues as to what the **world** is and what might be important.

The Answer

... “How do I do this one so I’ll be on top of it? How do I obey Newton’s rule? He said, ‘If I have seen further than others, it is because I’ve stood on the shoulders of giants.’ These days we stand on each other’s feet!

Quantum Love

Distinctive features of QI

- Superposition Principle
- Imperfect Distinguishability
- No-Cloning
- No-Deleting
- Non-local Correlation
- ....

Old days ...

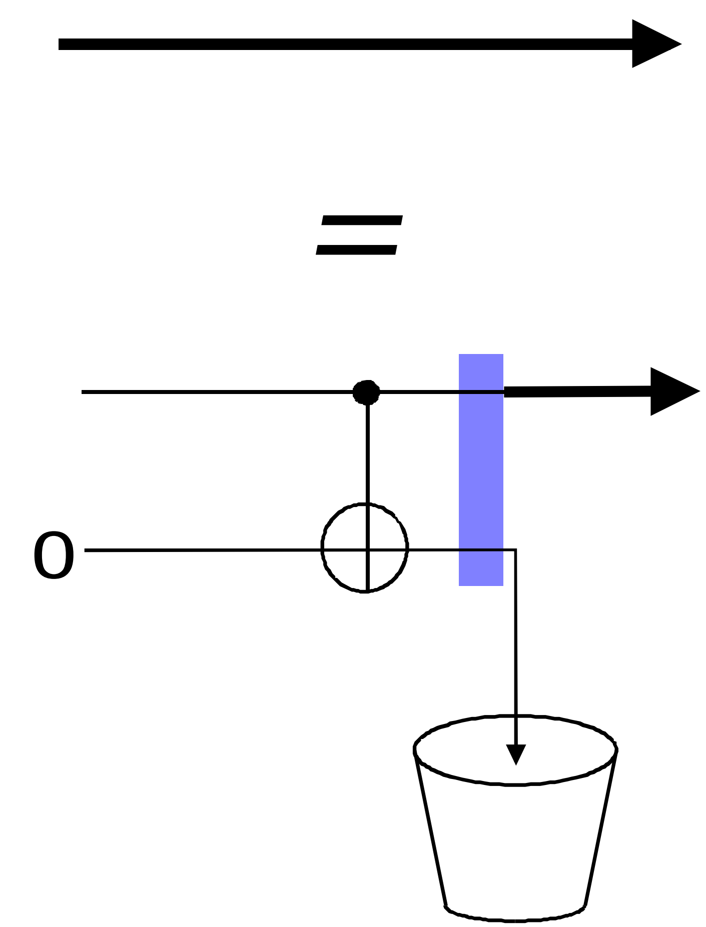
Information and Computation Theory was developed by considering bits and logic gates abstractly, **ignoring** the nature of the information carriers and the mechanisms of their interaction.

Our information society is built on the success of this abstraction

Nowadays ...

The correct arena for making this abstraction is quantum, not classical

A classical wire is a quantum channel that conducts 0 and 1 faithfully, but randomises superpositions of 0 and 1.



This slide is taken from Charlie Bennett’s talk.

Charlie Bennett

Quantum Information is like the information in a **dream**. You know that it was there, but you don't know what it was until you tell someone about it.

Classical computation is Quantum computation **handicapped** by having an eavesdropper on all its wires. You can't really get anything done if someone is always looking over your back.

Nowadays ...

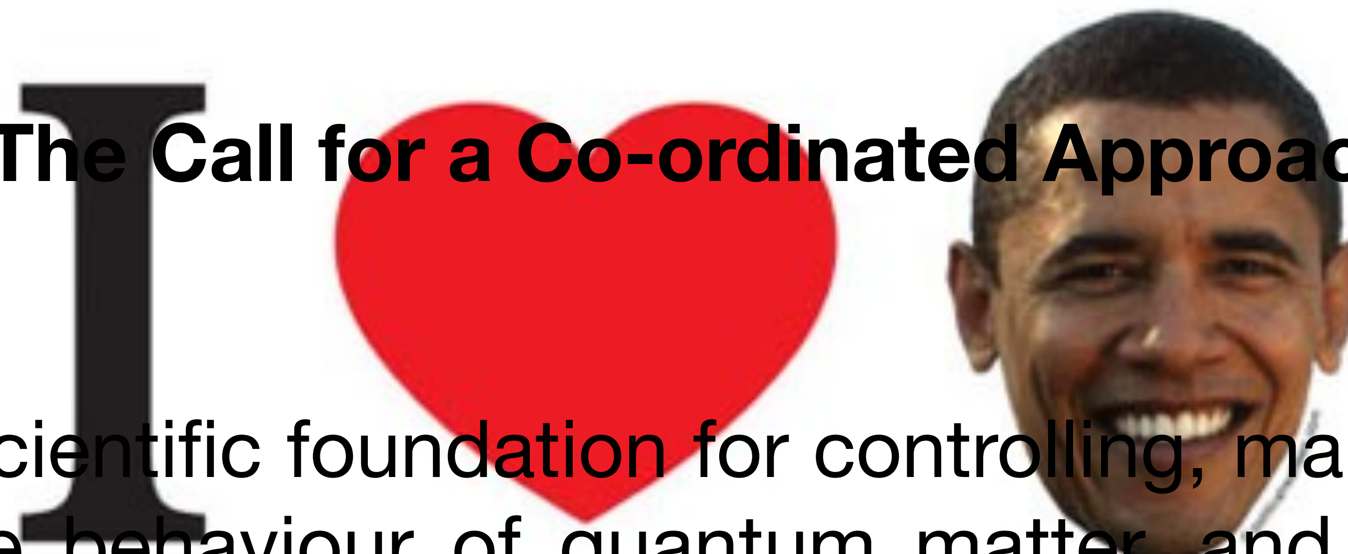
Recasting the classical theory in this way yields

- Dramatic speedups of some classically hard computations
- New kinds of communication and measurement
- New encryption techniques and breaking of some old ones
- New Classical Simulation Techniques

...

- An exciting area of basic science

A Federal Vision for Quantum Information Science



The Call for a Co-ordinated Approach

To create a scientific foundation for controlling, manipulating, and exploiting the behaviour of quantum matter, and for identifying the physical, mathematical, and computational capabilities and limitations of quantum information processing systems in order to build a knowledge base for this 21st century technology.

Quantum Computing

- The true power of a general purpose quantum computer?
- Problems that can be computed efficiently?
- What does it teach us about nature?
- What error correction schemes can be developed to allow quantum computer free of errors?

Decoherence

- What are the weak interactions that destroy QI?
- Are there fundamental limits on the control and read-out of QI in quantum systems that are also interacting with an environment?
- What constructs, such as decoherence-free subspaces and topological methods, can be employed to manage or avoid decoherence?

Non-Locality

- Are there fundamental limits to how large an entangled system can become?
- How can we best quantify "multi-partite" entanglement?
- How does one characterise a highly entangled state or at least verify that it is the state one intended to create?
- What is the power of distributed entanglement and what unique capabilities does this provide?

Complex Quantum System

- Are there exotic new states of matter that emerge from collective quantum systems?
- What are they useful for?
- How robust are they to environmental interactions?
- Does collective quantum phenomena limit the complexity of computing devices we can build?

Conclusion

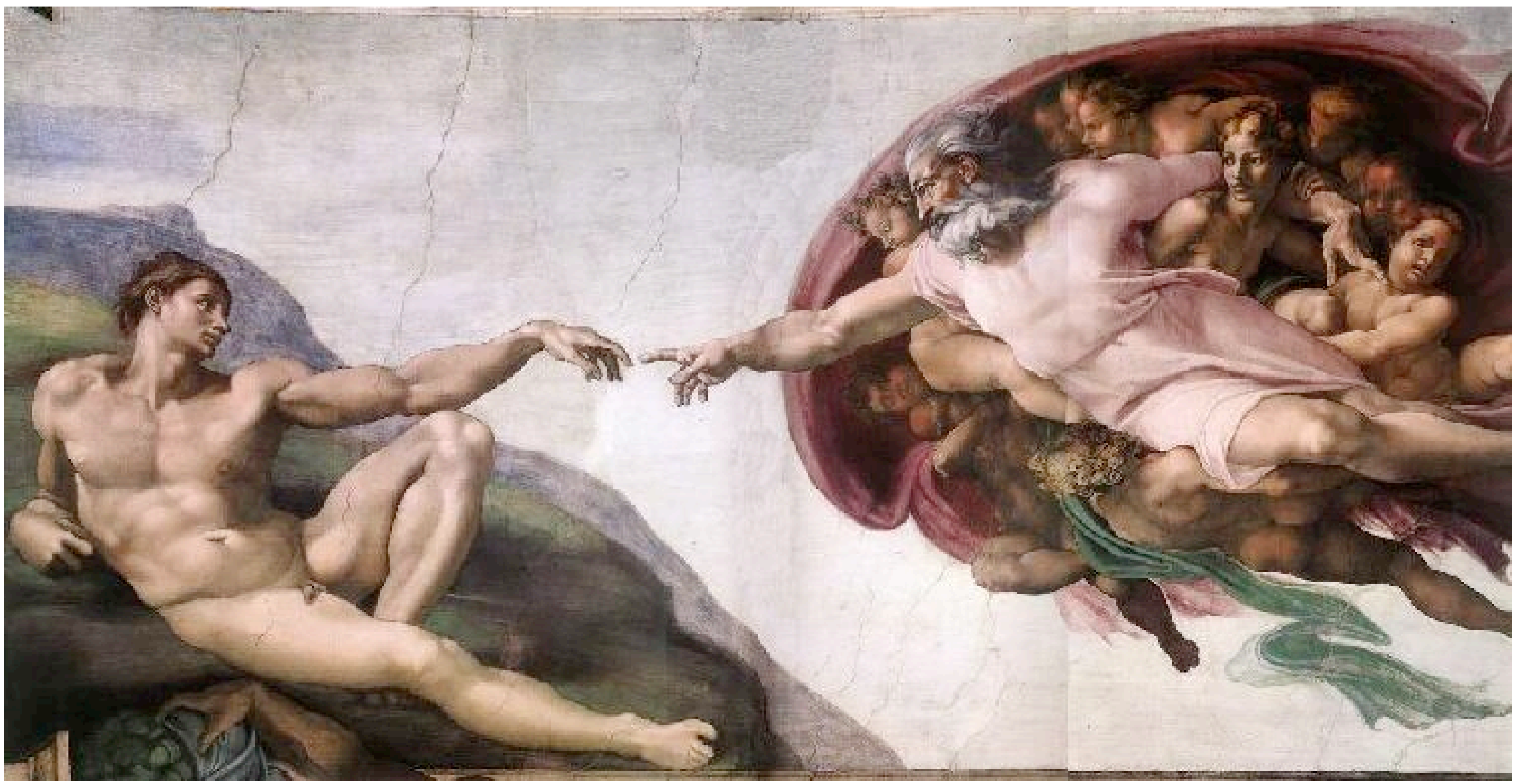
- *19th: Thermodynamics and Classical mechanics*
- *20th: Quantum mechanics lasers, transistors, computers but constrained by semi-classical approximations*

The impact of QIS is not yet known,
nor is the schedule on which working systems might be available.

QI phenomena are at an early pre-application stage, but possess a novelty and a richness that suggests the likelihood of unanticipated impact

Interactive Proofs

What can a computationally unbounded entity prove to a mere mortal*?



*BPP computation

A Quantum Supervisor

What can a computationally unbounded entity prove to a mere mortal*?

*BPP computation

Verification

Vazirani (07)

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

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?

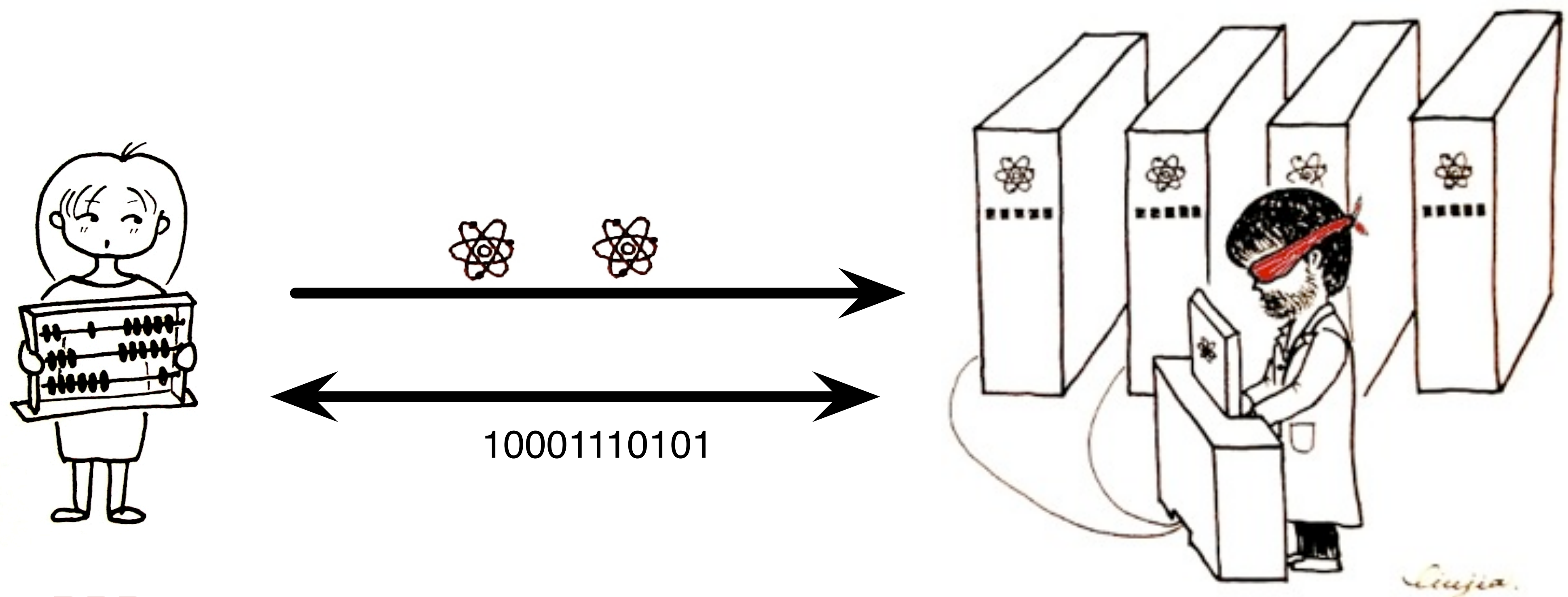
Cryptographic Scenario

How will a user interface with a quantum server?

- *Classical Client*
- *Perfect Privacy with Authentication*

Universal Blind QC Protocol

[Broadbent, Fitzsimons, Kashefi, 2009]



BPP

random single qubit generator

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

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

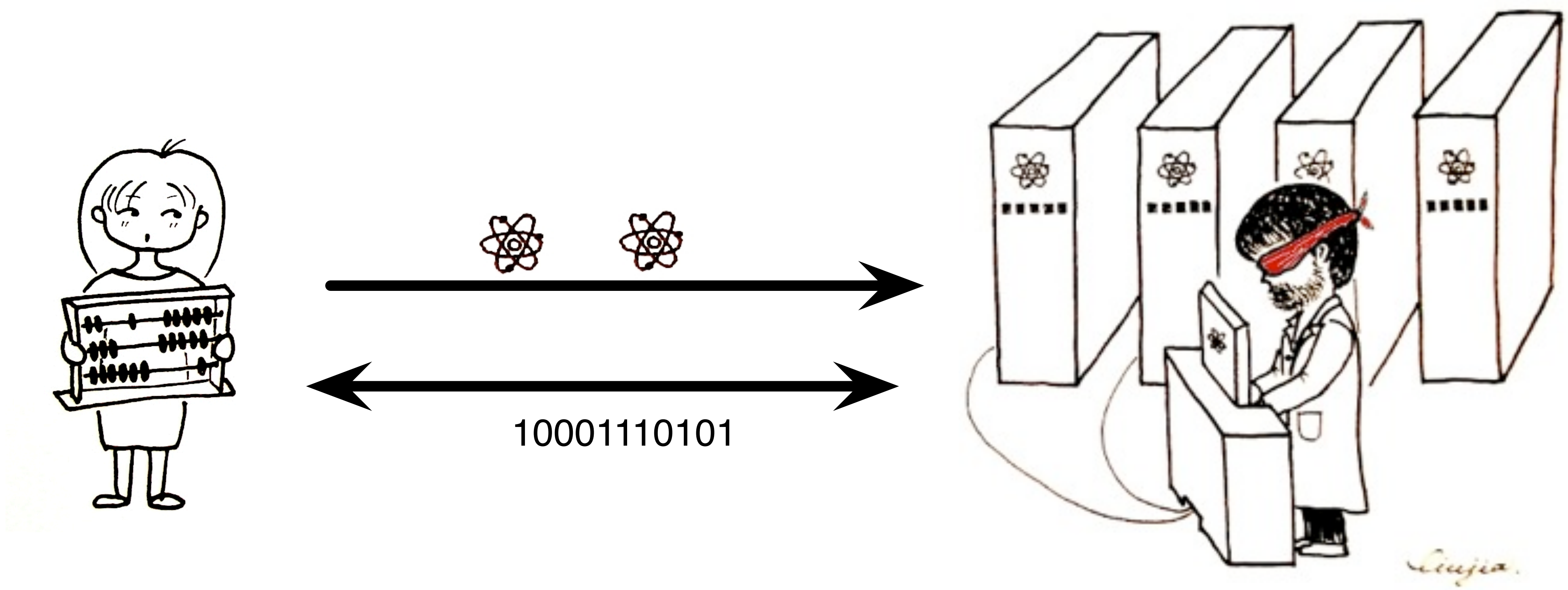
Perfect Privacy

- Detection of malicious Bob

- Fault Tolerance

Applications

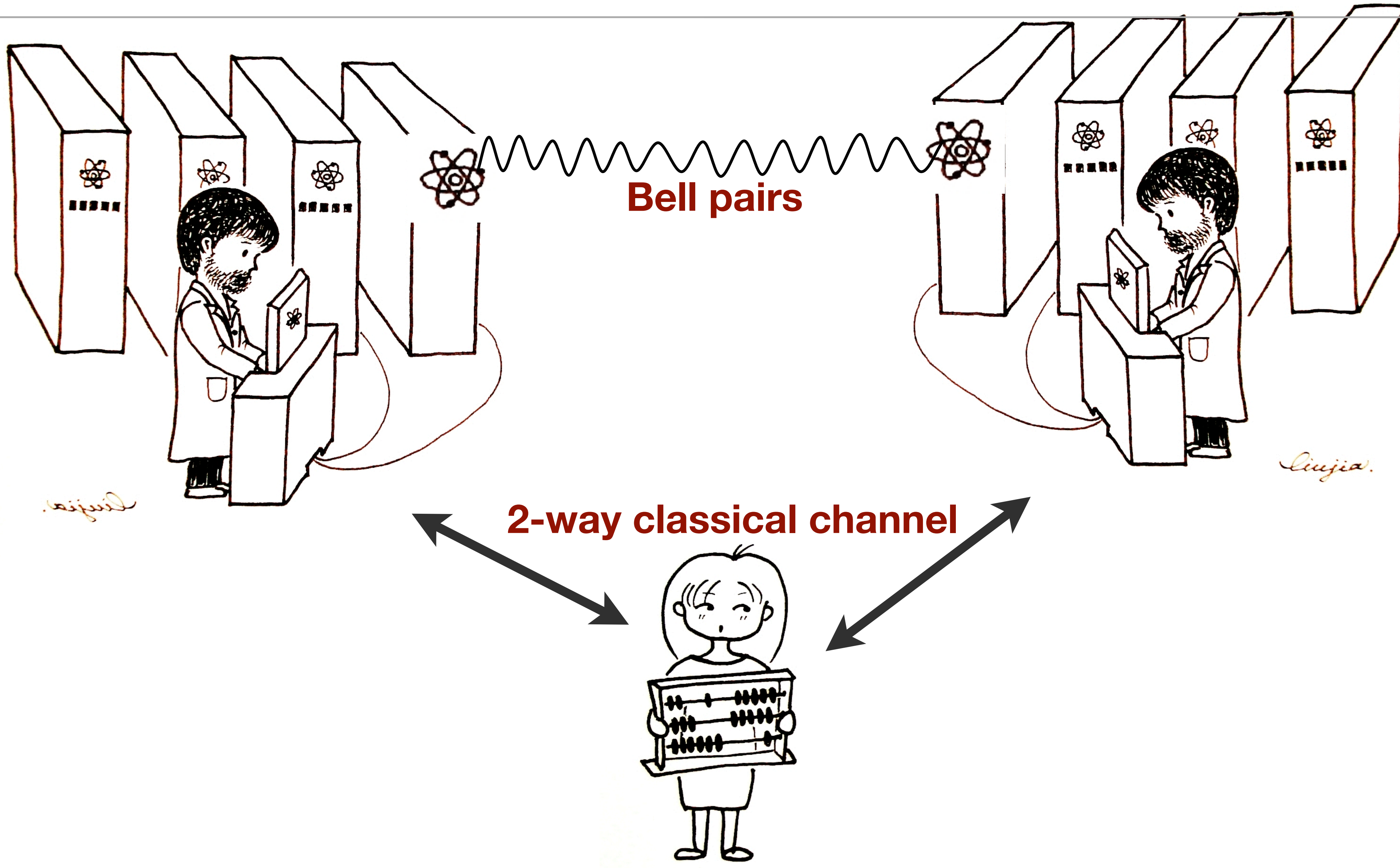
Factoring, Jones Polynomial (BQP-complete), State Preparation



Quantum Money

[Mosca, Stebila 2009]

Interactive Proofs



Classical Computer + 2 Provers + Entanglement = Quantum Computer

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]

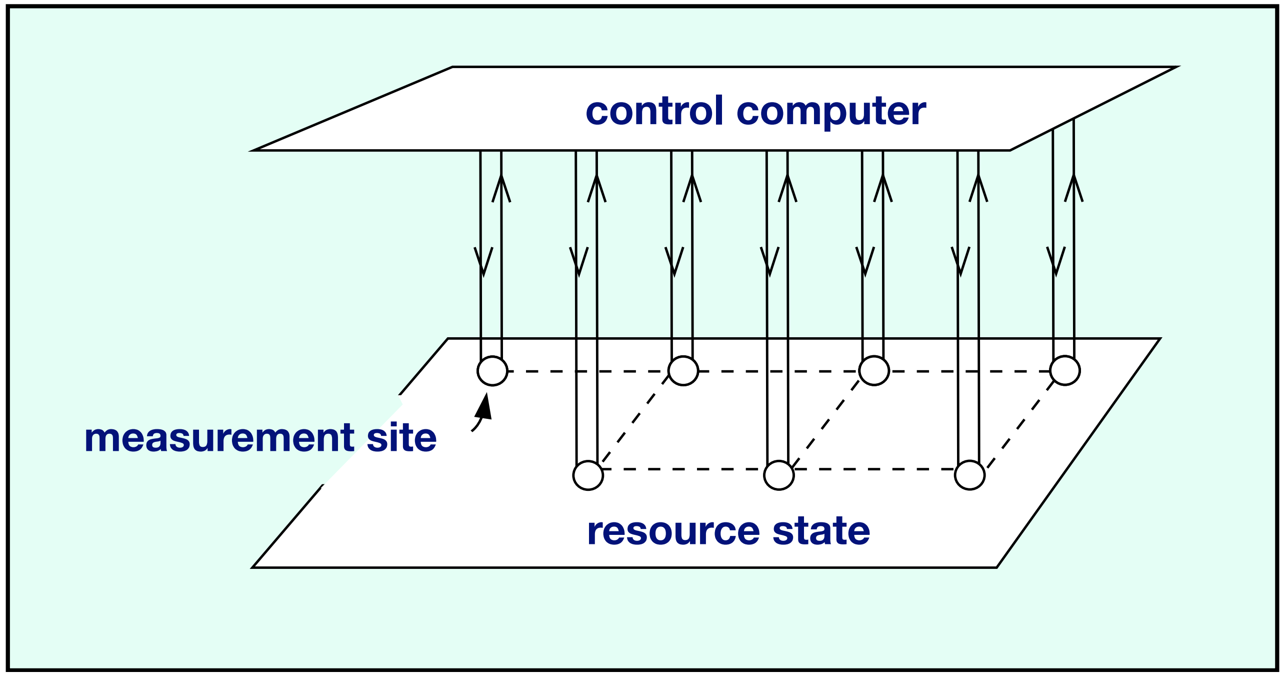
A Formal Method Approach

Measurement-based Quantum Computing

[Raussendorf, Briegel, 2001]

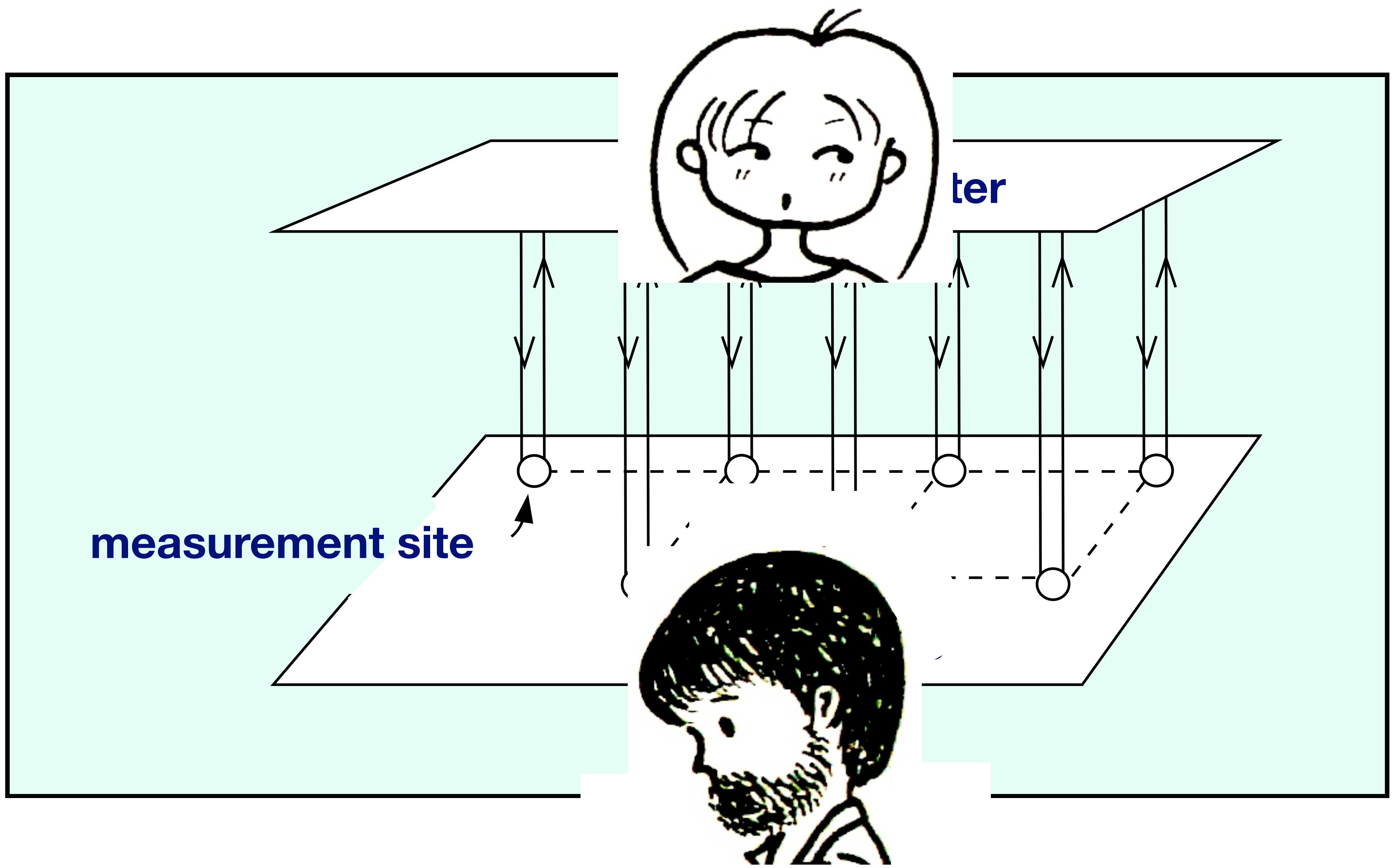
Measurement Calculus

[Danos, Kashefi, Panangaden 2007]



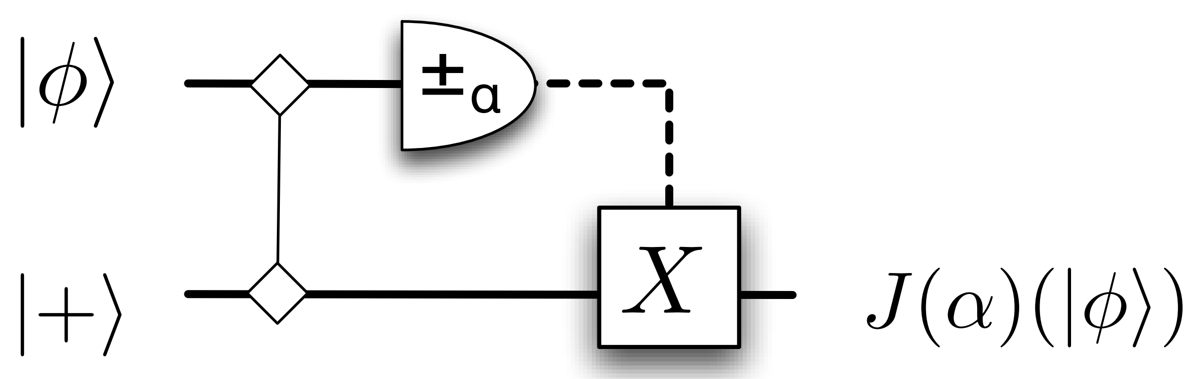
Program is encoded in the classical control computer
Computation Power is encoded in the entanglement

The First MBQC Protocol

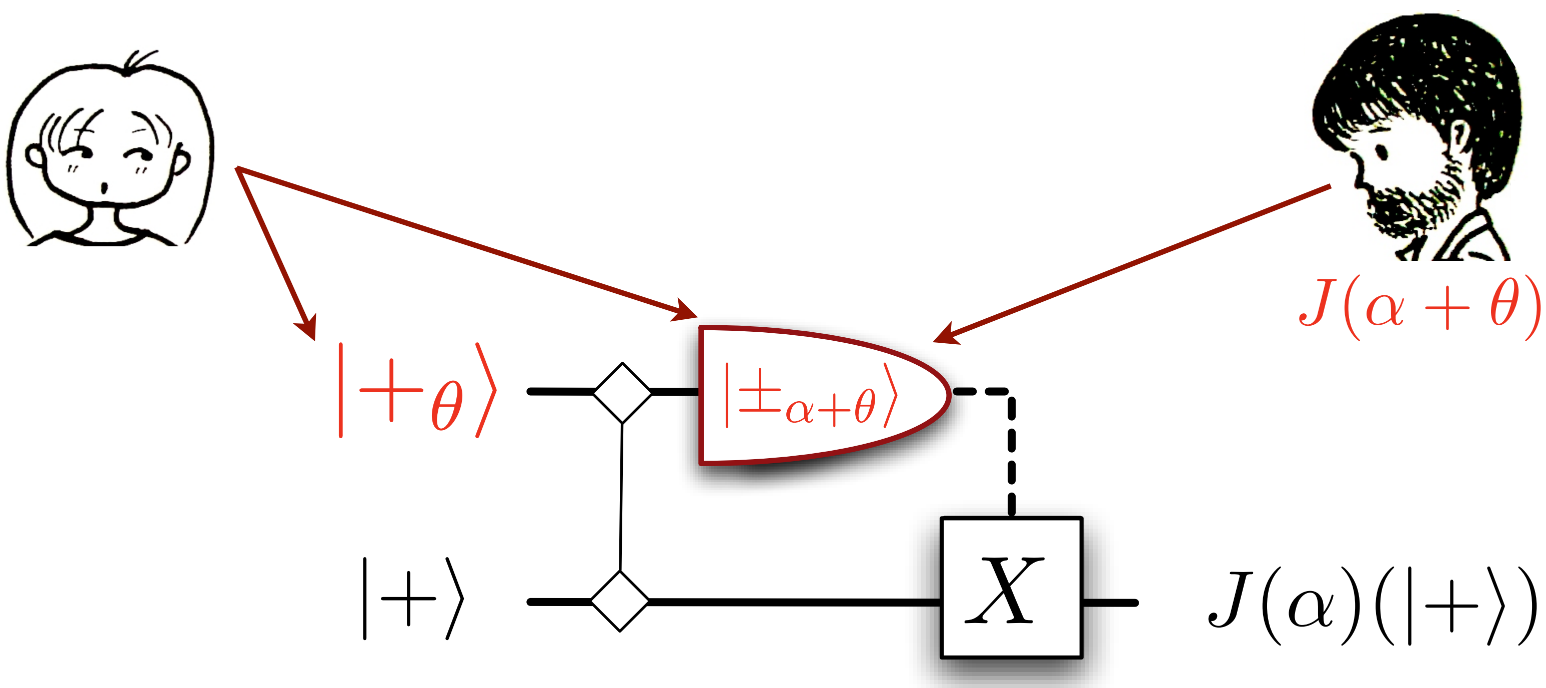


Teleportation Again

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



Uncertainty Principle



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

Main Protocol

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

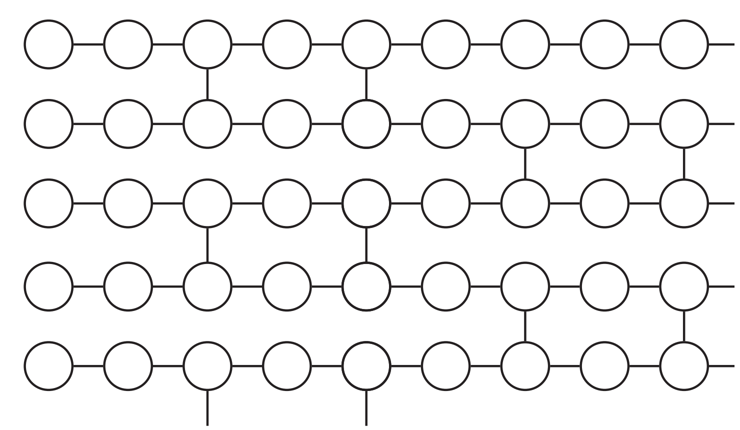
$|\psi_{x,y}\rangle \in_R \{|+_\theta\rangle\}$

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

$\delta_{x,y}$

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

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

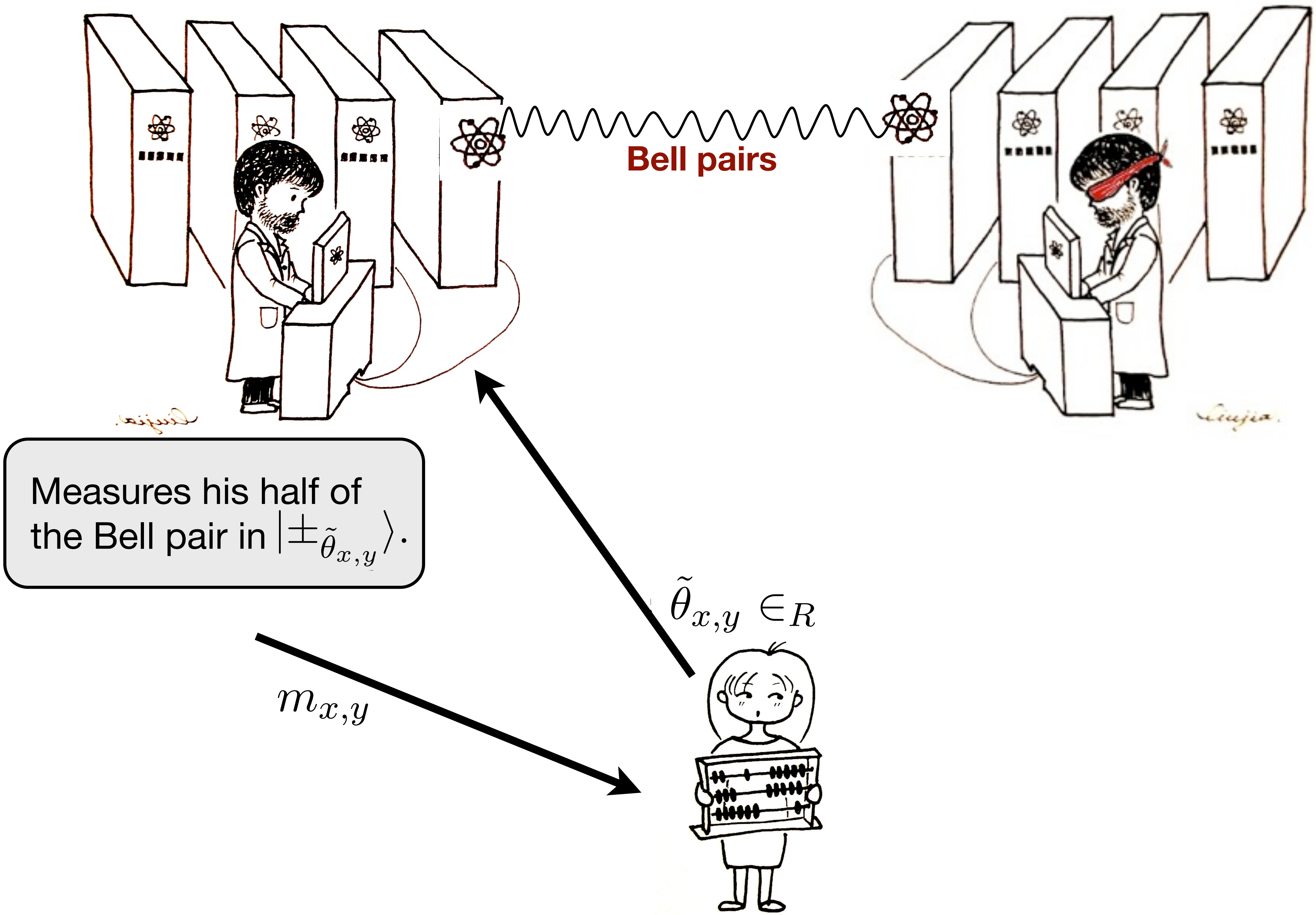


$\{|+_{\delta_{x,y}}\rangle, |-_{\delta_{x,y}}\rangle\}$

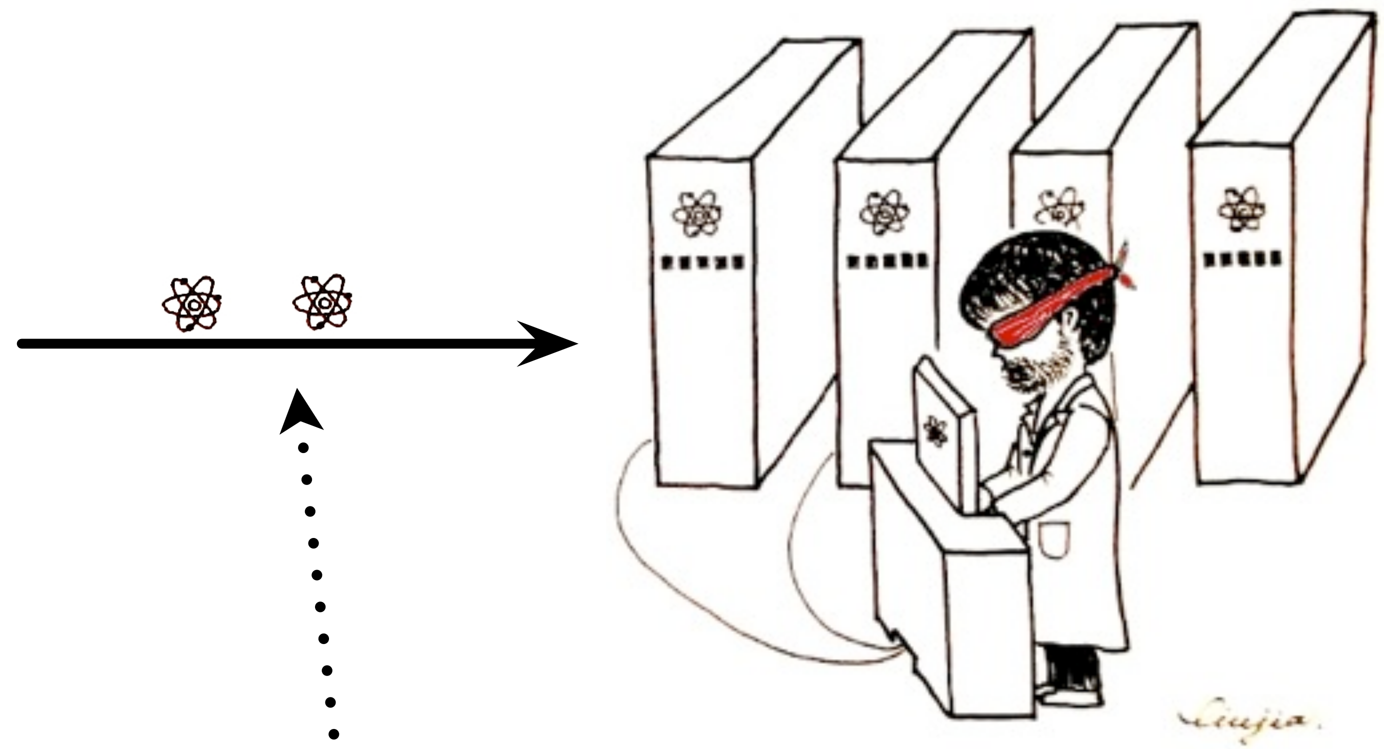
$s_{x,y} \in \{0,1\}$

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

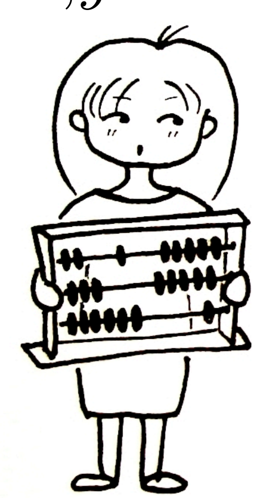
Interactive proof



Interactive proof



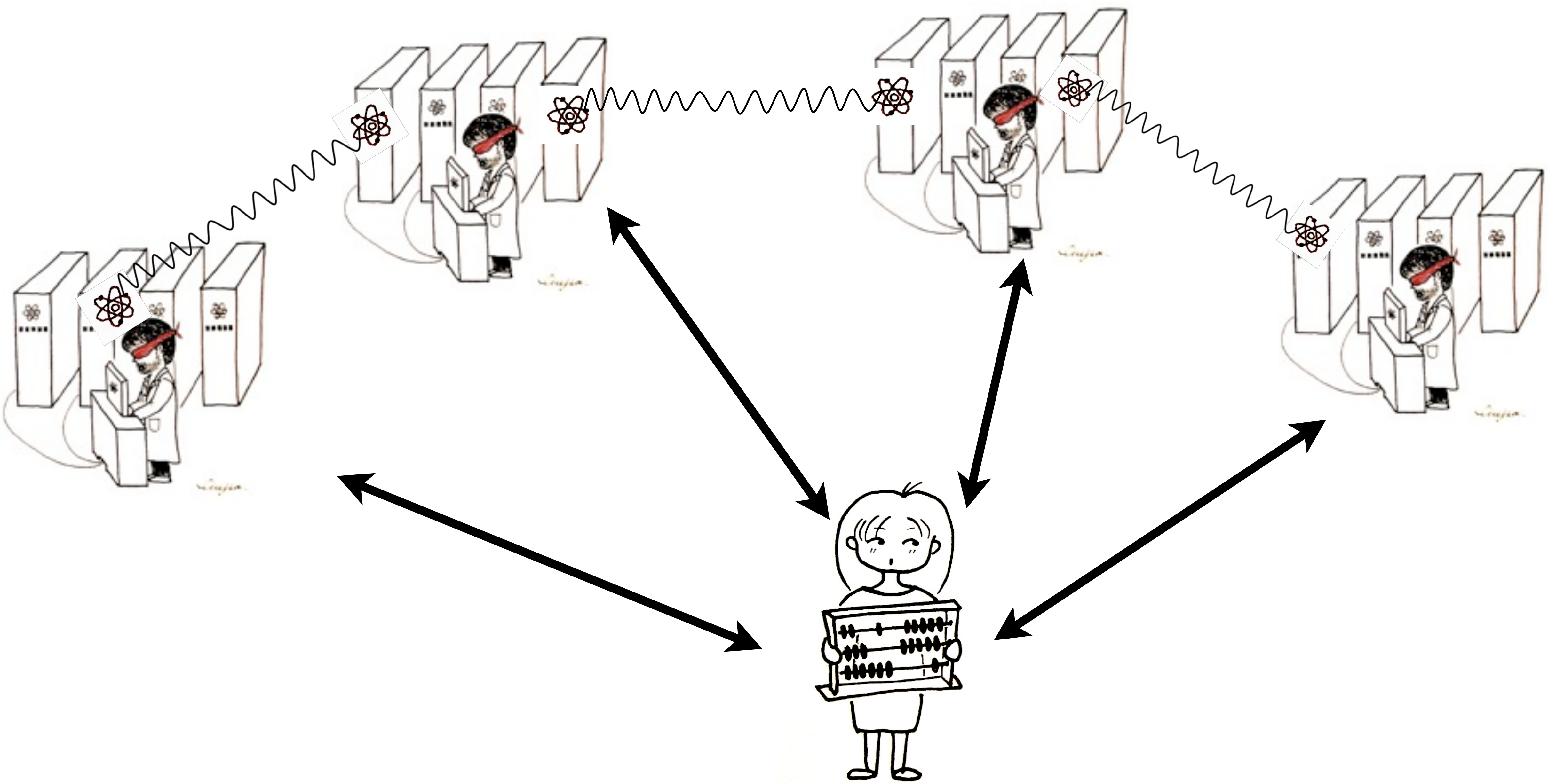
$\tilde{\theta}_{x,y} \in_R$



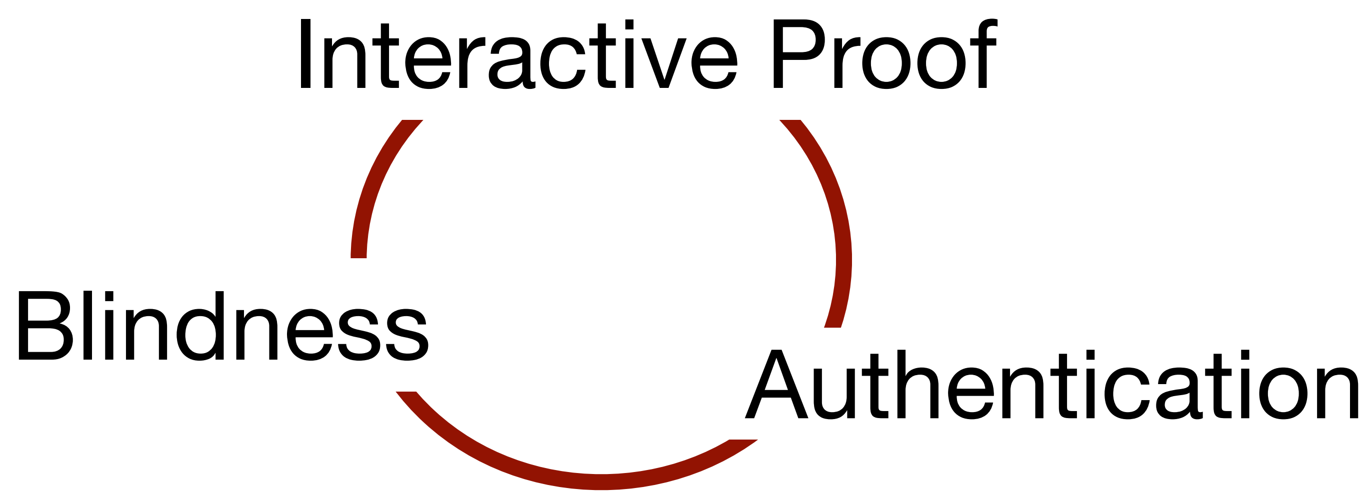
Main Protocol

QMIP = MIP *

We design an interactive protocol with only classical communication that replaces a turn for the verifier in a given quantum interactive proof system the new protocol requires only classical resources for the verifier.



What Next ?



The remaining \$10 ?

$$\mathbf{BQP} \overset{?}{=} \mathbf{IP}^{BQP}$$

Making Alice weaker ?

Quantum Money

The uncertainty principle and no-cloning made quantum money one of the original interests of QI

[Wiesner, 1969]

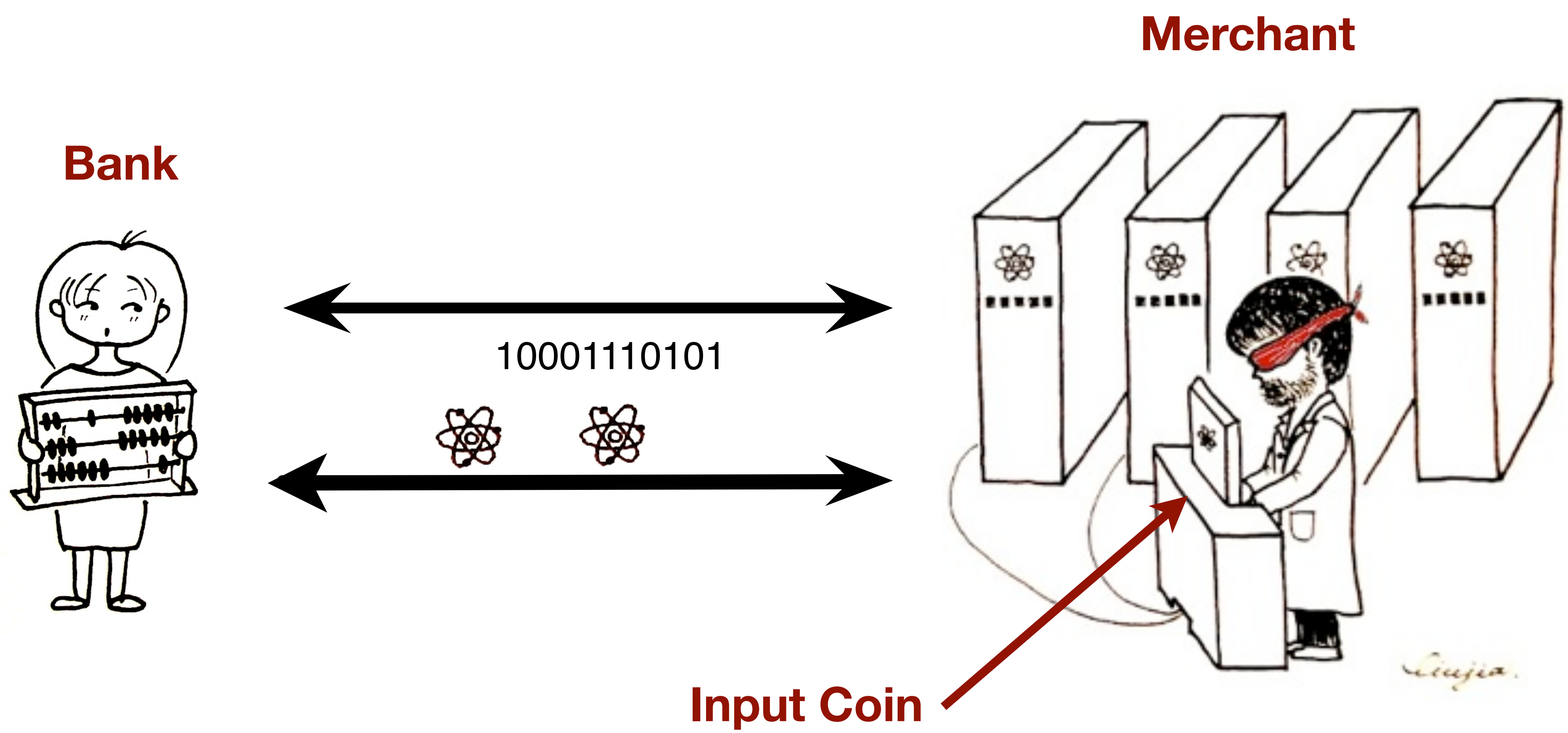
Ordinary serial number + few hundreds photons

Locally verifiable, unforgable, and anonymous

Public-key Quantum Money. *[Lutomirski, et.al., 2009]*

Quantum Coins. *[Mosca, Stebila, 2009]*

Blind Quantum Coin



Question: Can we do this without any final Q communication?

An interactive protocol for quantum circuit obfuscation

What does my mum think about all of these ?

Mum: I'm struggling to learn about internet and now you are telling me without knowing teleportation I cannot even shop!