Measurement-based Quantum Computation

Elham Kashefi

University of Edinburgh

Quantum Information Processing

A cross-disciplinary field of great importance from both fundamental and technological perspectives.

It has changed our perspective on the foundation of

Information Theory, Computation and Physics.

Birth of QIP

It is possible to perform computation both
logically and thermodynamically reversible.

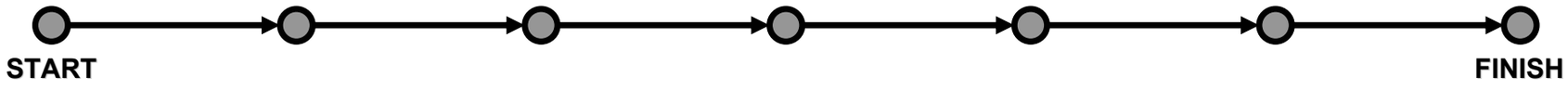
Quantum physics is also reversible, as the reverse-time
evolution specified by the unitary operator always exists.

Quantum Mechanics in a nutshell

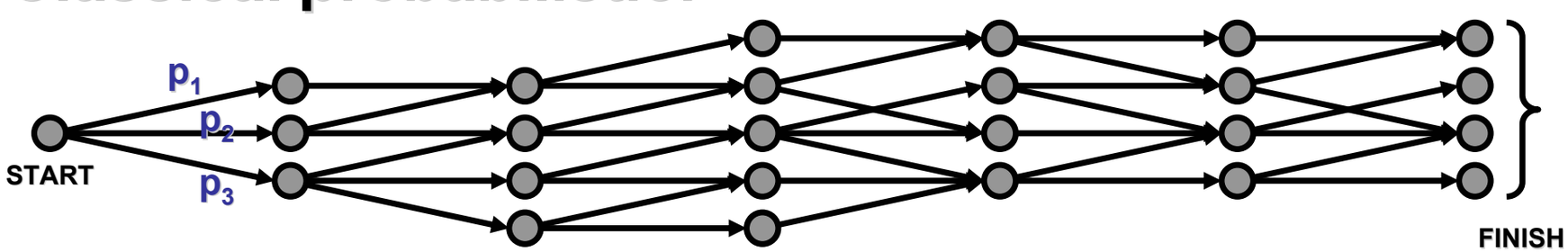
- **Data:** Unit vector in a Hilbert space (**qubit**)
- **Processing:** Unitary transformation
- **Result:** Projective measurement
- **Composite System:** Tensor product

Quantum Transition Systems

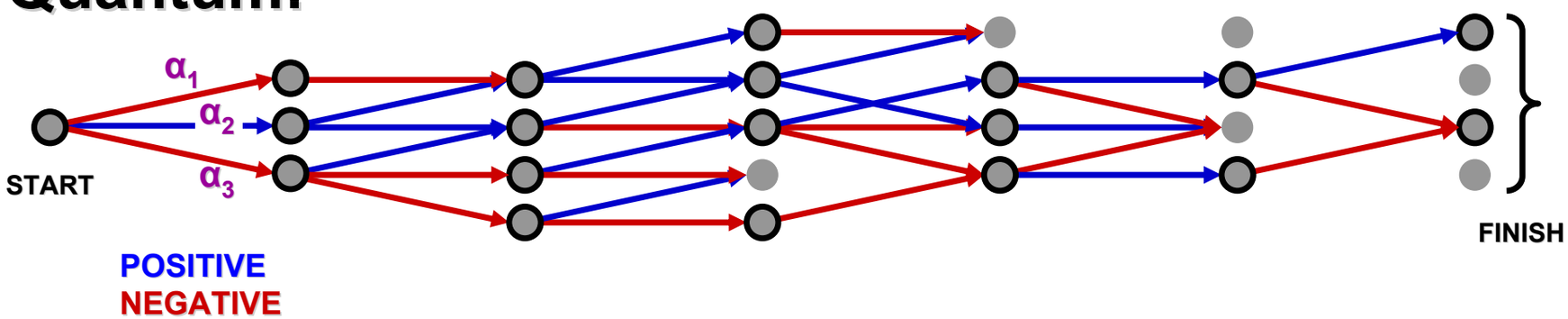
Classical deterministic:



Classical probabilistic:

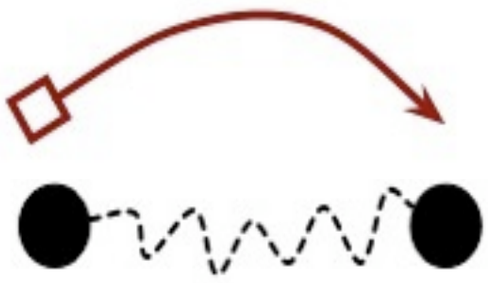


Quantum:



Entanglement

Non-local Correlation



Fundamental Feature of Quantum Mechanics

- ➡ Computation
- ➡ Information
- ➡ Cryptography

Models of QC

Quantum Circuit Model
Quantum Cellular Automata
Quantum Turing Machine

Measurement-based QC
Adiabatic QC
Topological QC

Quantum Categorical Framework
Quantum Processes Calculus
Quantum Programming Languages

An end-to-end Story

- Physics - Ising Hamiltonian, one-way QC

  Raussendorf and Briegel Phys. Rev. Lett. 2000

- Formal Methods - Measurement Calculus

  Danos, Kashefi, Panangaden JACM 2007

- Parallelism and Determinism

  Broadbent, Browne, Danos, Kashefi, Mhalla, Perdrix,
  Phys. Rev. A. 2006, TCS 2007, New. J. Physics 2008, TQC 2009

- Protocol Design - Universal Blind QC

  Broadbent, Fitzsimons, Kashefi FOCS 2009

- Implementation - Foundation of Quantum Mechanics

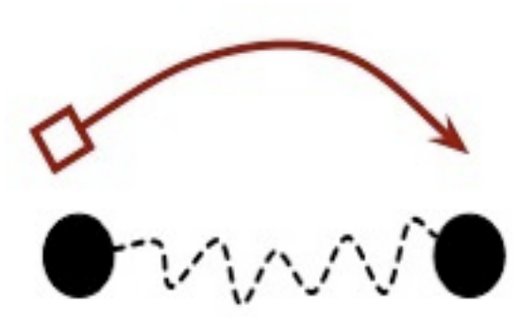
  Bartz, Kashefi, Broadbent, Fitzsimons, Zeilinger, Walther, Science 2012

Measurement-based QC

Measurements play a central role.

Scalable implementation

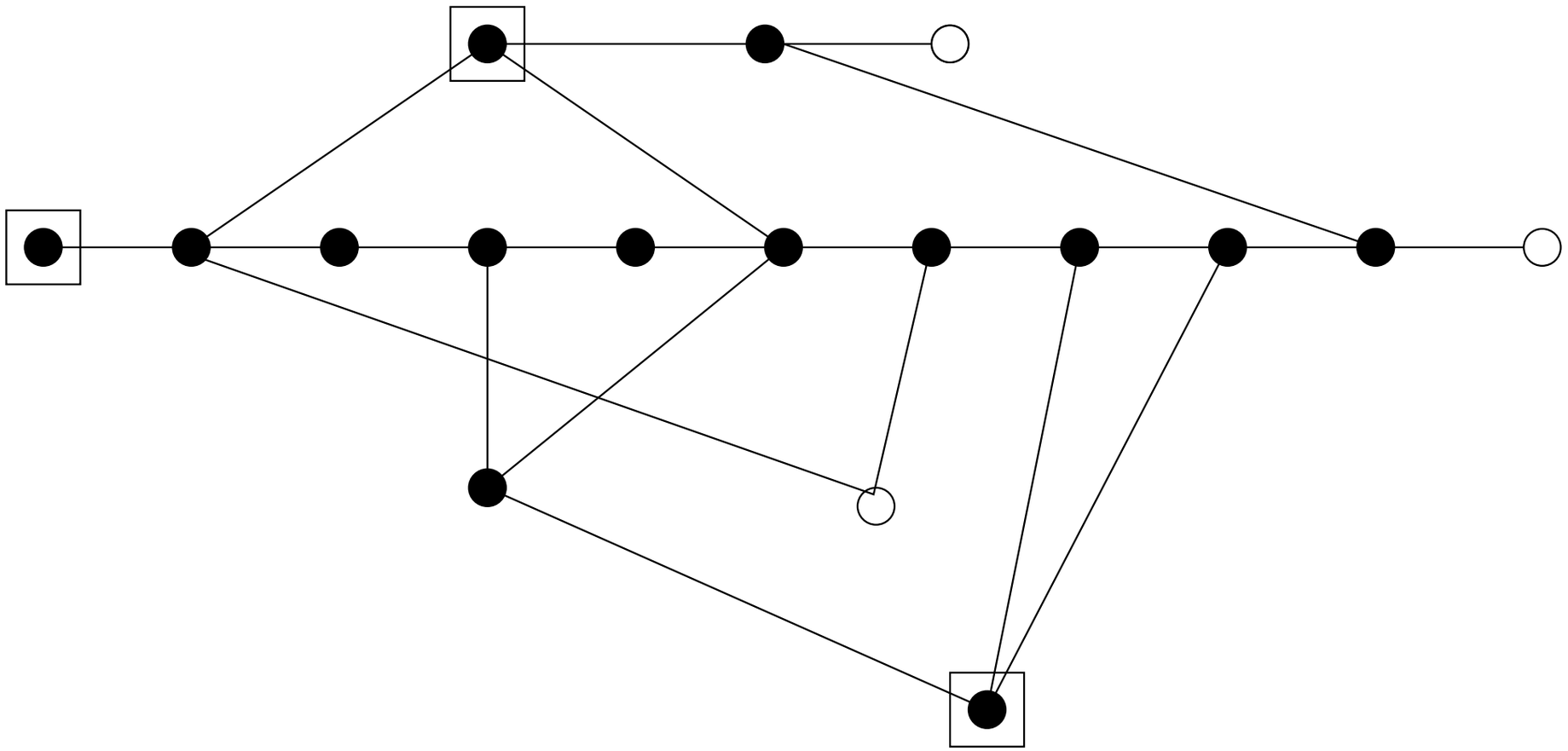
Clear separation between classical and quantum parts of computation



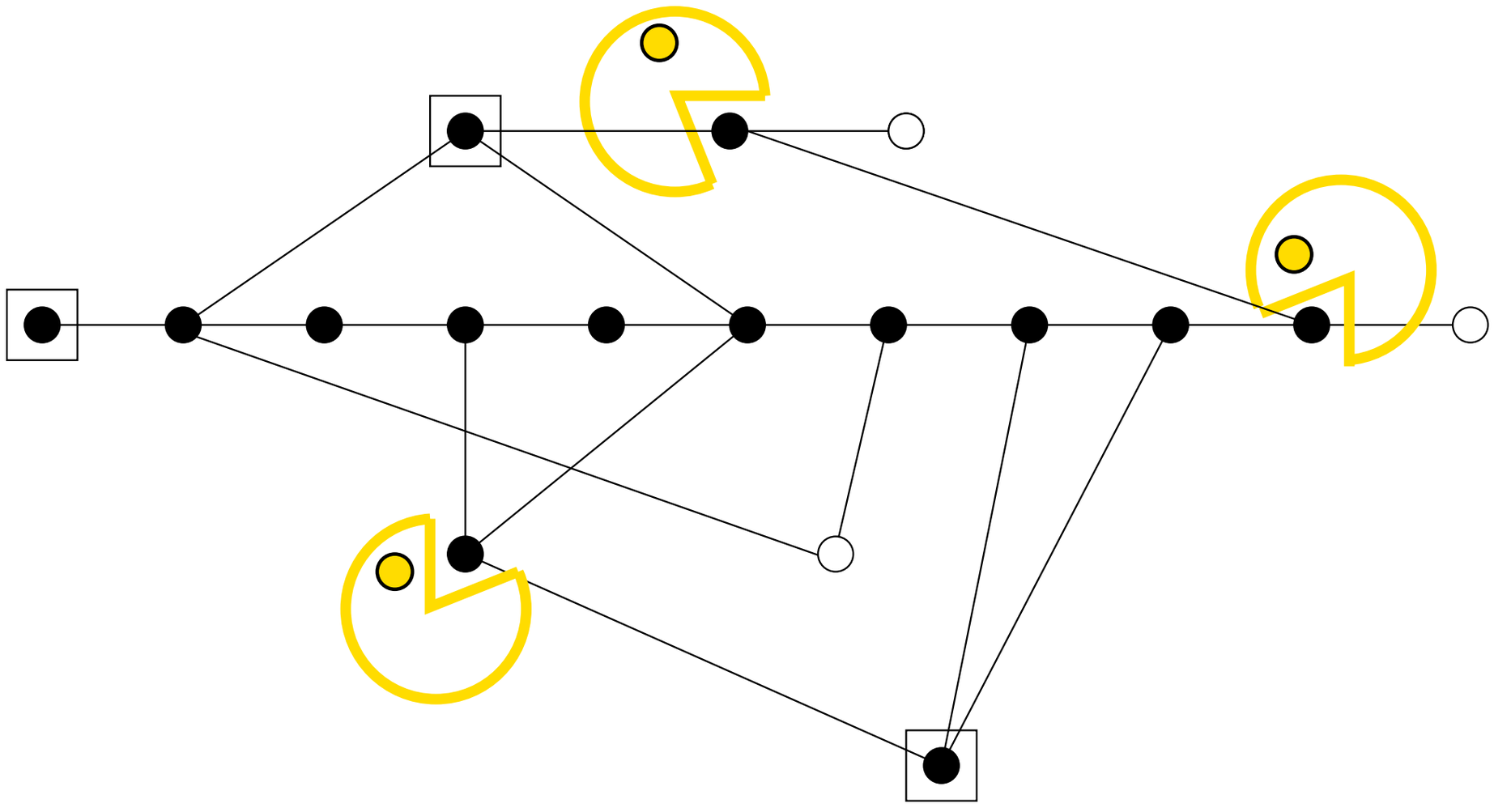
Entanglement

Clear separation between creation and consumption of resources

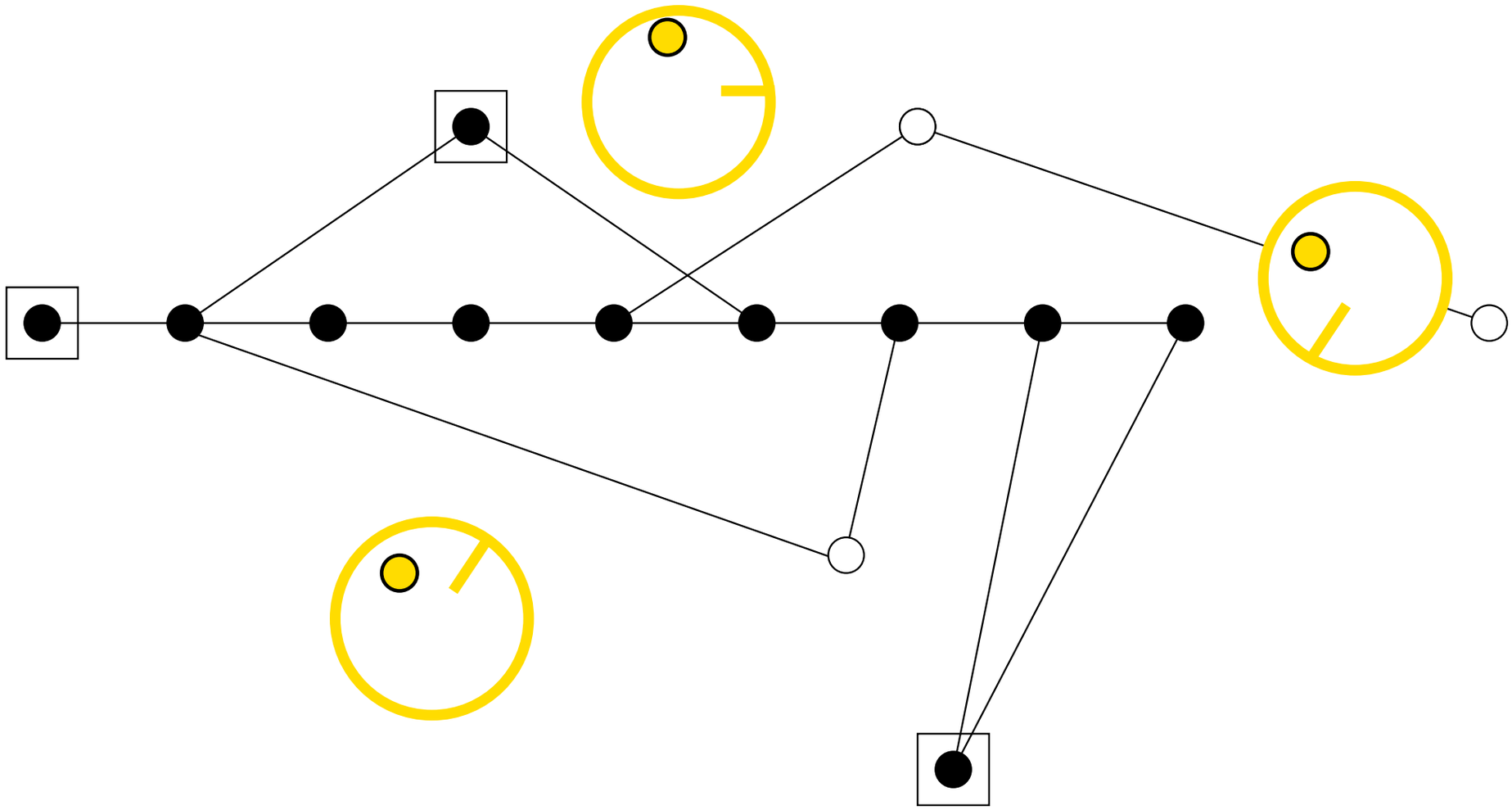
Quantum Pacman



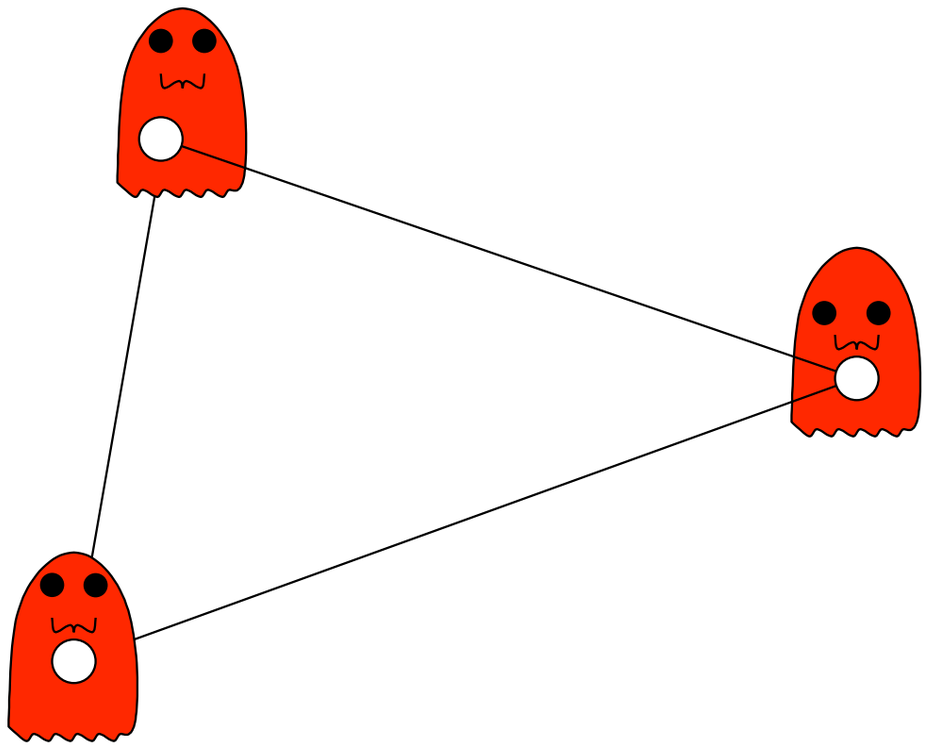
Quantum Pacman



Quantum Pacman



Quantum Pacman



Basic Commands

- **New qubits,** to prepare the auxiliary qubits: N
- **Entanglements,** to build the quantum channel: E
- **Measurements,** to propagate(manipulate) qubits: M
- **Corrections,** to make the computation deterministic: C

2-state System $\mathbb{C}^2$

The canonical basis, $(1,0)$, $(0,1)$, also called the computational basis, is usually denoted $|0\rangle$, $|1\rangle$. It is orthonormal by definition of $\langle x, y\rangle_{\mathbb{C}^2}$.

$$|\pm\rangle := \tfrac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \qquad |\pm_\alpha\rangle := \tfrac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$$

The *preparation* map N_i^α is defined to be:

$$|+_\alpha\rangle \otimes \_ : \mathfrak{H}_n \to \mathbb{C}^2 \otimes \mathfrak{H}_n$$

Maps over $\mathbb{C}^2$

Pauli Spin Matrices

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Other Single qubit gates

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P(\alpha) := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

$$P(\alpha)^\star = P(-\alpha)$$

The two qubit state $\mathbb{C}^2 \otimes \mathbb{C}^2$

Canonical basis

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

Bases need not be made of decomposable elements, they can consists of entangled states.

Graph basis

$$\begin{aligned}
\mathcal{G}_{00} &= \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\
\mathcal{G}_{01} &= \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle) \\
\mathcal{G}_{10} &= \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle) \\
\mathcal{G}_{11} &= \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)
\end{aligned}$$

Maps on $\mathbb{C}^2 \otimes \mathbb{C}^2$

- In general if $f : A \longrightarrow B$ and $g : A' \longrightarrow B'$, one defines $f \otimes g : A \otimes A' \longrightarrow B \otimes B' : \psi \otimes \phi \mapsto f(\psi) \otimes g(\phi)$.

- Or given $f : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$, one defines $\wedge f$ (read controlled-f) a new map on $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$\begin{aligned} \wedge f|0\rangle|\psi\rangle &:= |0\rangle|\psi\rangle \\ \wedge f|1\rangle|\psi\rangle &:= |1\rangle f(|\psi\rangle) \end{aligned}$$

Entangling Map

$$\wedge Z(|+\rangle \otimes |+\rangle) = \mathcal{G}_{00}$$

Pauli and Clifford

Define the *Pauli group* over A as the closure of $\{X_i, Z_i \mid 1 \leq i \leq n\}$ under composition and $\otimes$. These are all local maps (corrections).

Define the *Clifford group* over A as the normalizer of the Pauli group, that is to say the set of unitaries f over A such that for all g in the Pauli group, fgf^{-1} is also in the Pauli group.

Entangling Map is in Clifford

$$\wedge Z_{ij} X_i = X_i Z_j \wedge Z_{ij}$$
$$\wedge Z_{ij} Z_i = Z_i \wedge Z_{ij}$$

Projective Measurement on $\mathfrak{H}_n$

A complete measurement is given by an orthonormal basis

$$\mathcal{B} = \{\psi_a\}$$

which defines a decomposition into orthogonal 1-dimensional subspaces

$$\mathfrak{H}_n = \oplus_a E_a$$

Define $|\psi_a\rangle\langle\psi_a| : \mathfrak{H}_n \to E_a$ to be projection to E_a

Outcome

$$M^{\mathcal{B}} : \mathfrak{H}_n \to \oplus_a E_a : |\phi\rangle \mapsto \oplus_a \langle\psi_a, \phi\rangle |\psi_a\rangle$$

Probability

Destructive Measurement

Given a complete measurement over A, as $\mathcal{A} = \{\psi_a\}$, one can extend it to an incomplete measurement on $A \otimes B$, with components given by $|\psi_a\rangle\langle\psi_a| : A \otimes B \to B$.

1-qubit destructive measurement

M^α associated to $\{|+_\alpha\rangle\}$

Unitary Action

If U maps orthonormal basis $\mathcal{B}$ to $\mathcal{A}$ then

$$M^{\mathcal{A}} \;=\; U M^{\mathcal{B}} U^{\dagger}$$

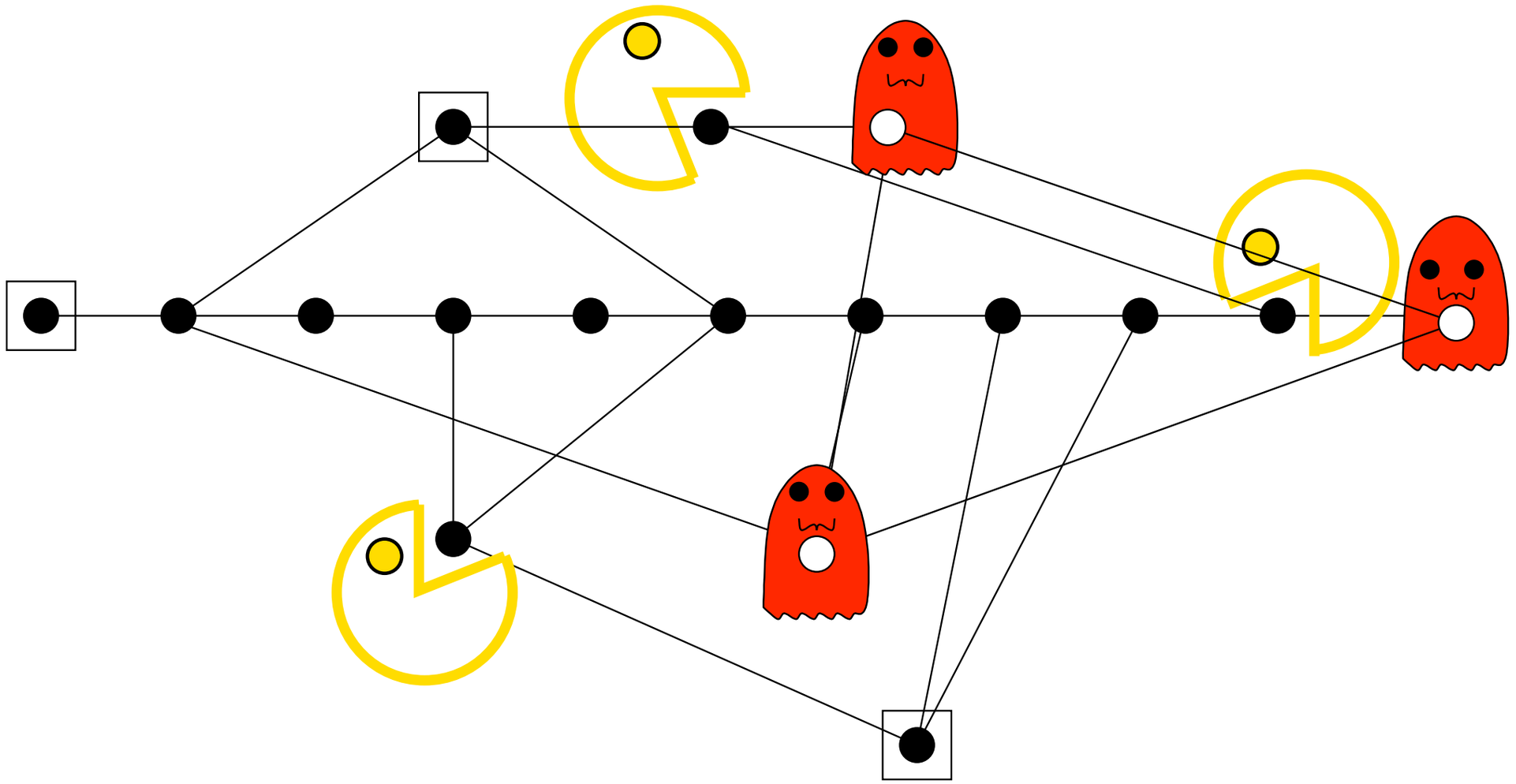
- X-action:

$$X|+_{\alpha}\rangle = |+_{-\alpha}\rangle$$
$$X|-_{\alpha}\rangle = -|-_{-\alpha}\rangle$$

- Z-action:

$$Z|+_{\alpha}\rangle = |+_{\alpha+\pi}\rangle$$
$$Z|-_{\alpha}\rangle = |-_{\alpha+\pi}\rangle$$

Quantum Pacman



A formal language

- N_i prepares qubit in $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$

- M_i^α projects qubit onto basis states $|\pm_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ \pm e^{i\alpha}\end{pmatrix}$
  (measurement outcome is $s_i = 0, 1$)

- E_{ij} creates entanglement $\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}$

- Local Pauli corrections $X_i = \begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Z_i = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$

- **Feed forward:** measurements and corrections commands are allowed to depend on previous measurements outcomes.

$$C_i^s \qquad [M_i^\alpha]^s = M_i^{(-1)^s\alpha} \qquad {}_s[M_i^\alpha] = M_i^{\alpha+s\pi}$$

Dependent Commands

The measurement outcome $s_i \in \mathbb{Z}_2$:
— 0 refers to the $\langle +_\alpha |$ projection,
— 1 refers to the $\langle -_\alpha |$ projection.

measurements and corrections may be parameterised by signal $\sum_i s_i$

- $[M_i^\alpha]^s = M_i^{(-1)^s \alpha} = M_i^\alpha X_i^s$
- ${}_t[M_i^\alpha] = M_i^{t\pi+\alpha} = M_i^\alpha Z_i^s$

with $X^0 = Z^0 = I$, $X^1 = X$, $Z^1 = Z$.

$$ {}_t[M_i^\alpha]^s \;=\; M_i^{t\pi+(-1)^s\alpha} $$

Patterns of Computation

$$(V, I, O, A_n \ldots A_1)$$

$$\mathfrak{H} := (\{1,2\}, \{1\}, \{2\}, X_2^{s1} M_1^0 E_{12} N_2^0)$$

Sequential or Parallel Composition

$$X_3^{s2} M_2^0 E_{23} \quad X_2^{s1} M_1^0 E_{12}$$

Definiteness Conditions

no command depends on outcomes not yet measured

no command acts on a qubit already measured

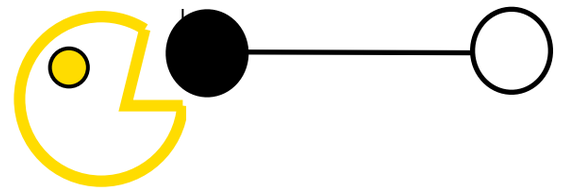
a qubit i is measured if and only if i is not an output

Example

$$\mathfrak{H} := (\{1,2\},\{1\},\{2\},X_2^{s1}M_1^0E_{12}N_2^0)$$

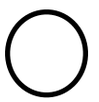
Starting with the **input state** $(a|0\rangle + b|1\rangle)|+\rangle$

$(a|0\rangle + b|1\rangle)|+\rangle \xrightarrow{E_{12}} \frac{1}{\sqrt{2}}(a|00\rangle + a|01\rangle + b|10\rangle - b|11\rangle)$

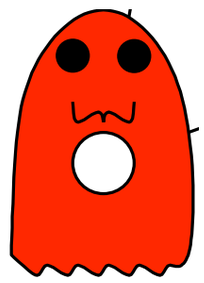


H

$$\xrightarrow{M_1^0} \begin{cases} \frac{1}{2}((a+b)|0\rangle + (a-b)|1\rangle) & s_1 = 0 \\ \frac{1}{2}((a-b)|0\rangle + (a+b)|1\rangle) & s_1 = 1 \end{cases}$$



$$\xrightarrow{X_2^{s1}} \frac{1}{2}((a+b)|0\rangle + (a-b)|1\rangle)$$



State Space

$$\mathcal{S} \;:=\; \cup_{V,W} \mathfrak{H}_V \times \mathbb{Z}_2^W$$

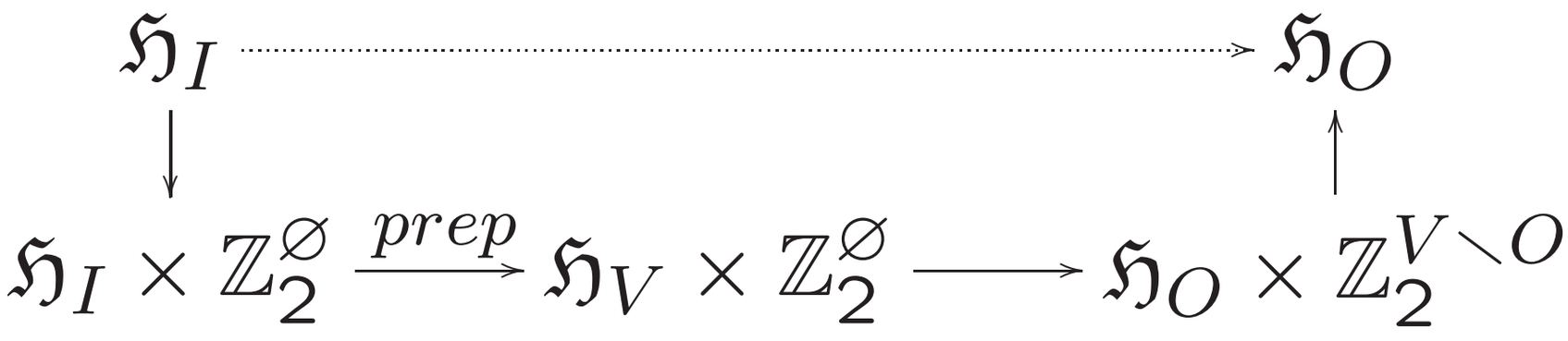
In other words a computation state is a pair q, Γ, where q is a quantum state and Γ is a map from some W to the outcome space $\mathbb{Z}_2$. We call this classical component Γ an *outcome map* and denote by $\varnothing$ the unique map in $\mathbb{Z}_2^{\varnothing}$.

Operational Semantics

$$
\begin{array}{lll}
q, \Gamma & \xrightarrow{N_i^{\alpha}} & q \otimes |{+}\alpha\rangle_i, \Gamma \\
q, \Gamma & \xrightarrow{E_{ij}} & \wedge Z_{ij} q, \Gamma \\
q, \Gamma & \xrightarrow{X_i^s} & X_i^{s_\Gamma} q, \Gamma \\
q, \Gamma & \xrightarrow{Z_i^s} & Z_i^{s_\Gamma} q, \Gamma \\
q, \Gamma & \xrightarrow{{}_t[M_i^{\alpha}]^s} & \langle {+}\alpha_\Gamma|_i q, \Gamma[0/i] \\
q, \Gamma & \xrightarrow{{}_t[M_i^{\alpha}]^s} & \langle {-}\alpha_\Gamma|_i q, \Gamma[1/i]
\end{array}
$$

where $\alpha_\Gamma = (-1)^{s_\Gamma}\alpha + t_\Gamma \pi$.

Denotational Semantics

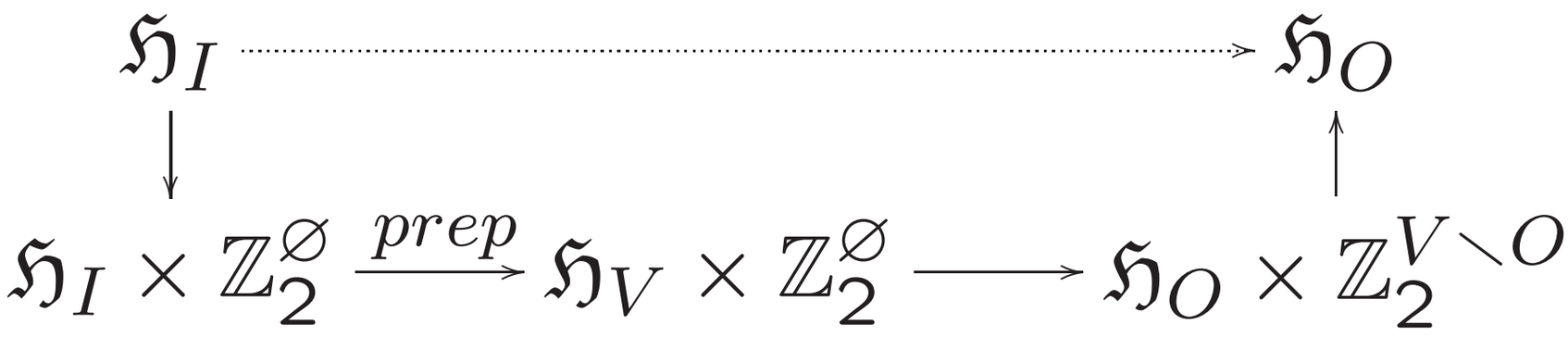


Let $A_{\mathbf{s}} = C_{\mathbf{s}} \Pi_{\mathbf{s}} U$ be a branch map, the pattern realises the cptp-map

$$T(\rho) := \sum_{\mathbf{s}} A_{\mathbf{s}} \rho A_{\mathbf{s}}^{\dagger}$$

Density operator : A probability distribution over quantum states

Denotational Semantics



A pattern is strongly deterministic if all the branch maps are equal.

Theorem. A strongly determinist pattern realises a unitary embedding.

Universal Gates

$$\wedge Z \;:=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

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

$$U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$$

$$\begin{array}{lcl} P(\alpha) & = & J(0)J(\alpha) \\ H & = & J(0) \\ H^i & = & J(\frac{\pi}{2}) \end{array}$$

Generating Patterns

$$\wedge Z \;:=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$\wedge \mathfrak{Z} \;:=\; E_{12}$$

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

$$\mathfrak{J}(\alpha) \;:=\; X_2^{s1} M_1^{-\alpha} E_{12}$$

Example (ctrl-U)

$$U \;=\; e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$$

$$\wedge U_{12} \;=\; J_1^0 J_1^{\alpha'} J_2^0 J_2^{\beta+\pi} J_2^{-\frac{\gamma}{2}} J_2^{-\frac{\pi}{2}} J_2^0 \wedge Z_{12} J_2^{\frac{\pi}{2}} J_2^{\frac{\gamma}{2}} J_2^{\frac{-\pi-\delta-\beta}{2}} J_2^0 \wedge Z_{12} J_2^{\frac{-\beta+\delta-\pi}{2}}$$

$$\alpha' \;=\; \alpha + \tfrac{\beta+\gamma+\delta}{2}$$

Example (ctrl-U)

Wild Pattern

$$X_C^{s_B} M_B^0 E_{BC} X_B^{s_A} M_A^{-\alpha'} E_{AB} X_k^{s_j} M_j^0 E_{jk} X_j^{s_i} M_i^{-\beta-\pi} E_{ij}$$
$$X_i^{s_h} M_h^{\frac{\gamma}{2}} E_{hi} X_h^{s_g} M_g^{\frac{\pi}{2}} E_{gh} X_g^{s_f} M_f^0 E_{fg} E_{Af} X_f^{s_e} M_e^{-\frac{\pi}{2}} E_{ef}$$
$$X_e^{s_d} M_d^{-\frac{\gamma}{2}} E_{de} X_d^{s_c} M_c^{\frac{\pi+\delta+\beta}{2}} E_{cd} X_c^{s_b} M_b^0 E_{bc} E_{Ab} X_b^{s_a} M_a^{\frac{\beta-\delta+\pi}{2}} E_{ab}$$

Standard Pattern

$$Z_k^{s_i+s_g+s_e+s_c+s_a} X_k^{s_j+s_h+s_f+s_d+s_b} X_C^{s_B} Z_C^{s_A+s_e+s_c}$$
$$M_B^0 M_A^{-\alpha'} M_j^0 [M_i^{\beta-\pi}]^{s_h+s_f+s_d+s_b} [M_h^{-\frac{\gamma}{2}}]^{s_g+s_e+s_c+s_a} [M_g^{\frac{\pi}{2}}]^{s_f+s_d+s_b}$$
$$M_f^0 [M_e^{-\frac{\pi}{2}}]^{s_d+s_b} [M_d^{\frac{\gamma}{2}}]^{s_c+s_a} [M_c^{\frac{\pi-\delta-\beta}{2}}]^{s_b} M_b^0 M_a^{\frac{-\beta+\delta+\pi}{2}}$$
$$E_{BC} E_{AB} E_{jk} E_{ij} E_{hi} E_{gh} E_{fg} E_{Af} E_{ef} E_{de} E_{cd} E_{bc} E_{ab} E_{Ab}$$

Measurement Calculus

Pushing entanglement to the beginning

$$
\begin{array}{rcl}
E_{ij} X_i^s & = & X_i^s Z_j^s E_{ij} \\
E_{ij} X_j^s & = & X_j^s Z_i^s E_{ij} \\
E_{ij} Z_i^s & = & Z_i^s E_{ij} \\
E_{ij} Z_j^s & = & Z_j^s E_{ij}
\end{array}
$$

Pushing correction to the end

$$
\begin{array}{rcl}
{}^t[M_i^\alpha]^s X_i^r & = & {}^t[M_i^\alpha]^{s+r} \\
{}^t[M_i^\alpha]^s Z_i^r & = & {}^{t+r}[M_i^\alpha]^s
\end{array}
$$

Theorem. The re-writing system is confluent and terminating.

Theorem. An MQC model admits a standardisation procedure iff the ***E*** operator is normaliser of all the ***C*** operators.

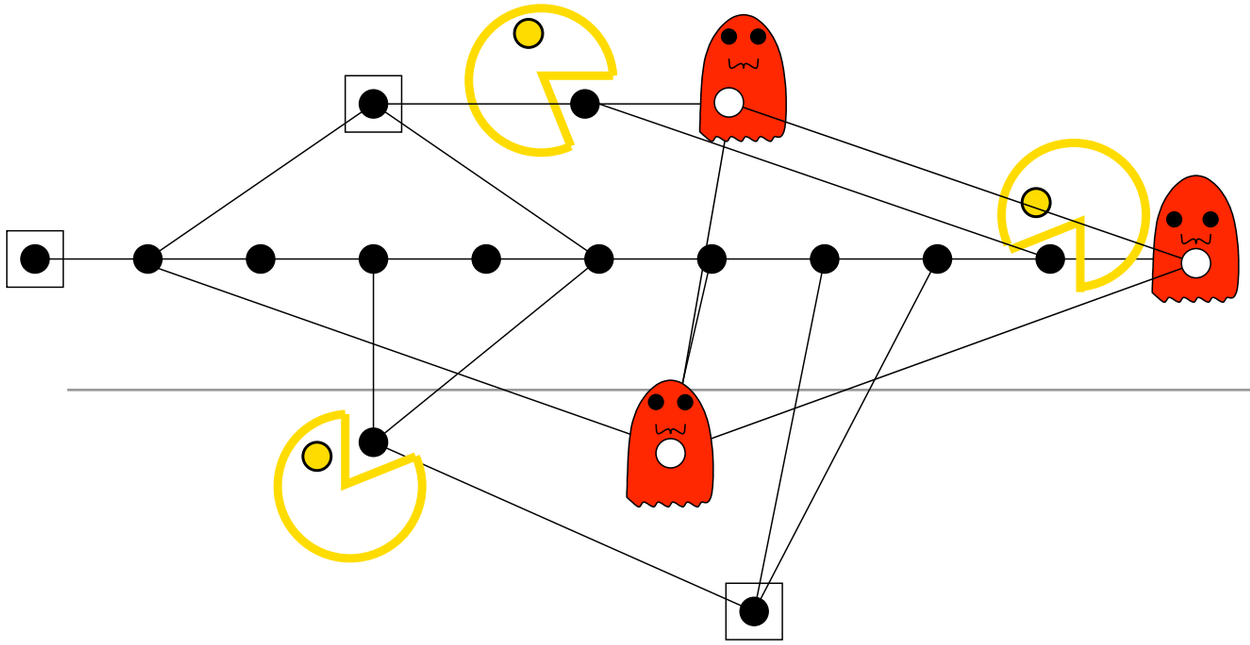
Algorithm

$$\boxed{U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)}$$

$$\mathfrak{J}(0)(4,5)\mathfrak{J}(\alpha)(3,4)\mathfrak{J}(\beta)(2,3)\mathfrak{J}(\gamma)(1,2) \quad =$$

$$\begin{aligned}
&X_5^{s_4} M_4^0 E_{45} X_4^{s_3} M_3^\alpha E_{34} X_3^{s_2} M_2^\beta E_{23} X_2^{s_1} M_1^\gamma E_{12} && \Rightarrow_{EX} \\
&X_5^{s_4} M_4^0 E_{45} X_4^{s_3} M_3^\alpha E_{34} X_3^{s_2} M_2^\beta X_2^{s_1} Z_3^{s_1} M_1^\gamma E_{123} && \Rightarrow_{MX} \\
&X_5^{s_4} M_4^0 E_{45} X_4^{s_3} M_3^\alpha E_{34} X_3^{s_2} Z_{s_1}^3 [M_2^\beta]^{s_1} M_1^\gamma E_{123} && \Rightarrow_{EXZ} \\
&X_5^{s_4} M_4^0 E_{45} X_4^{s_3} M_3^\alpha X_3^{s_2} Z_{s_1}^3 Z_4^{s_2} [M_2^\beta]^{s_1} M_1^\gamma E_{1234} && \Rightarrow_{MXZ} \\
&X_5^{s_4} M_4^0 E_{45} X_4^{s_3} Z_4^{s_2}{}_{s_1} [M_3^\alpha]^{s_2} [M_2^\beta]^{s_1} M_1^\gamma E_{1234} && \Rightarrow_{EXZ} \\
&X_5^{s_4} M_4^0 X_4^{s_3} Z_4^{s_2} Z_5^{s_3}{}_{s_1} [M_3^\alpha]^{s_2} [M_2^\beta]^{s_1} M_1^\gamma E_{12345} && \Rightarrow_{MXZ}
\end{aligned}$$

Worst Case Complexity: $O(N^5)$ where N is the number of qubits in the given pattern



✓ Compositional
✓ Universal
✓ Standardisation *EMCN*

Why Standardisation

Strong tool for proving pattern properties

Revealing Parallel Structure

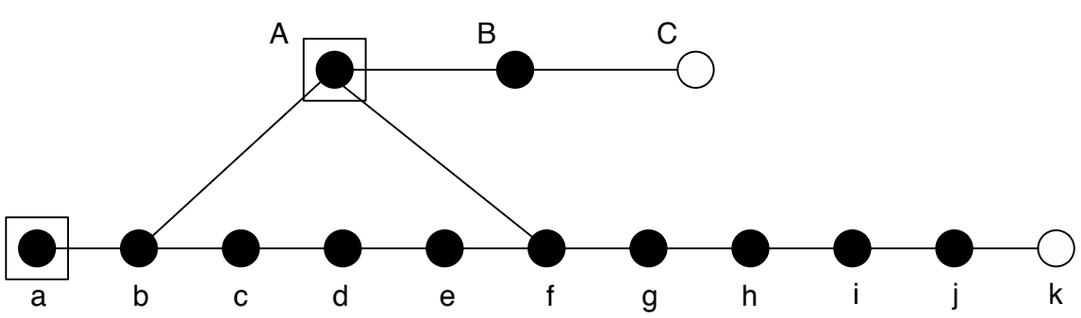
Characterisation of Determinism

Pattern Synthesis

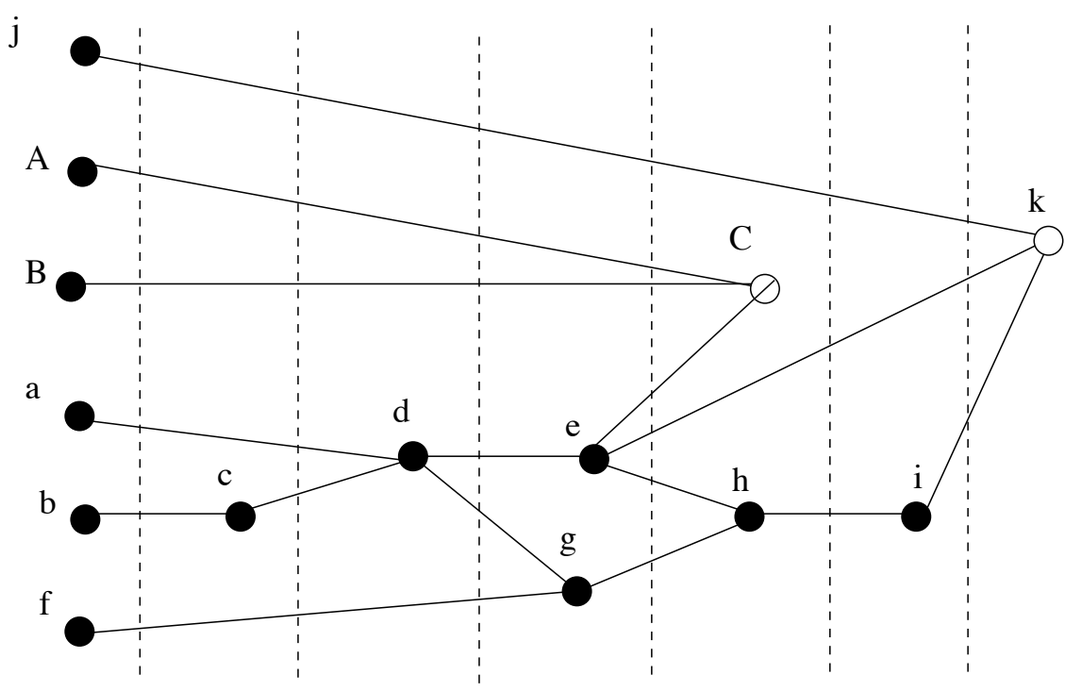
Protocol Design

The Key Feature of MBQC

A clean separation between Classical and Quantum Control



Entanglement Graph



Execution Graph

No dependency Theorems

Pauli Measurements

Theorem. A unitary map is in Clifford iff $\exists$ a pattern implementing it with measurement angles 0 and $\frac{\pi}{2}$

Theorem. If pattern *P* with no dependent commands implements unitary U, then U is in Clifford

Gottesman Knill Theorem

Efficient representation in terms of Pauli Operators

If the states of computation are restricted to the stabiliser states
and the operation over them to the Clifford group then
the corresponding quantum computation
can be efficiently simulated using Classical Computing

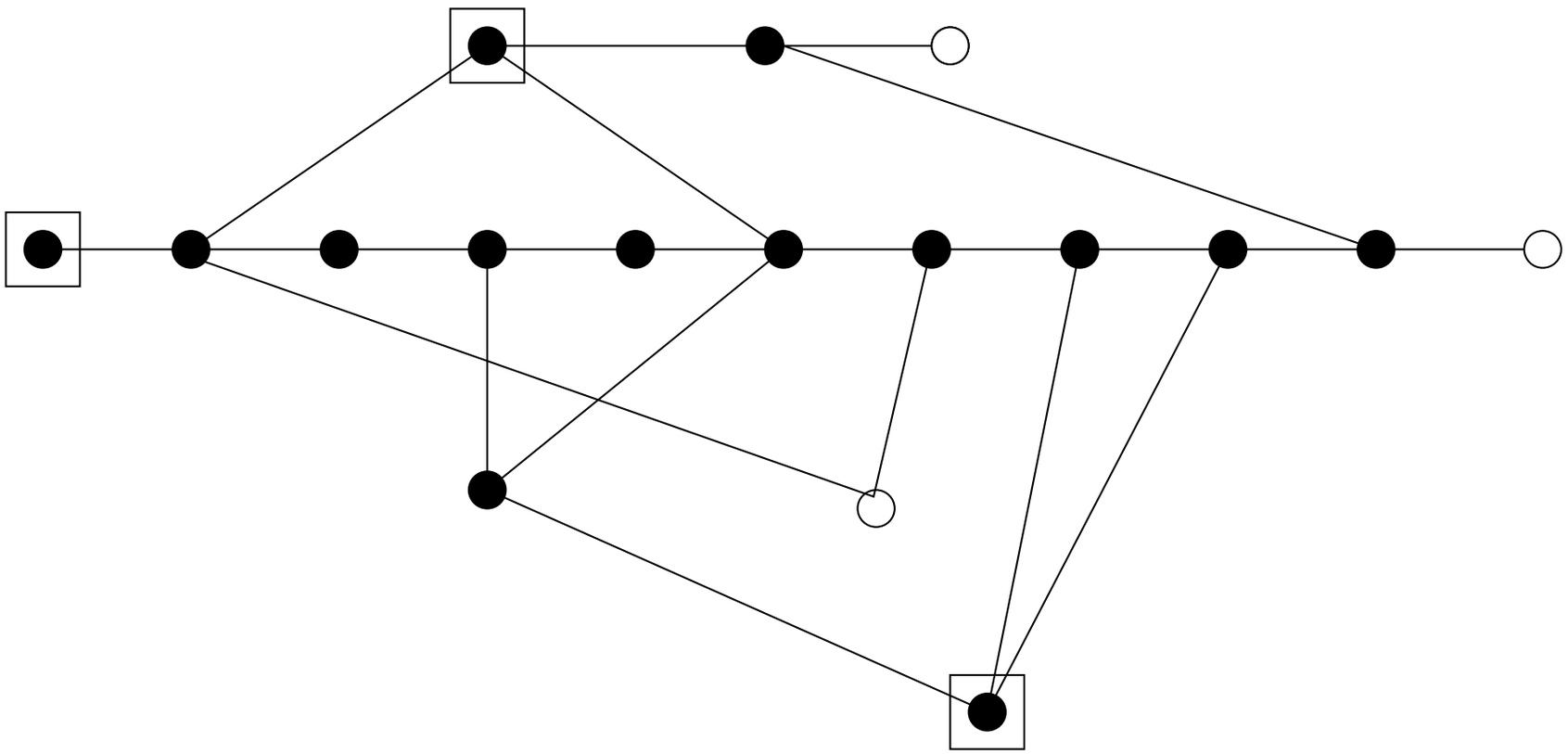
Preserves the efficient representation

Graph State as Stabiliser States

Graph Stabilisers:

$$K_i := X_i(\prod_{j \in N_G(i)} Z_j)$$

$$K_i E_G N_{I^c} = E_G N_{I^c}$$

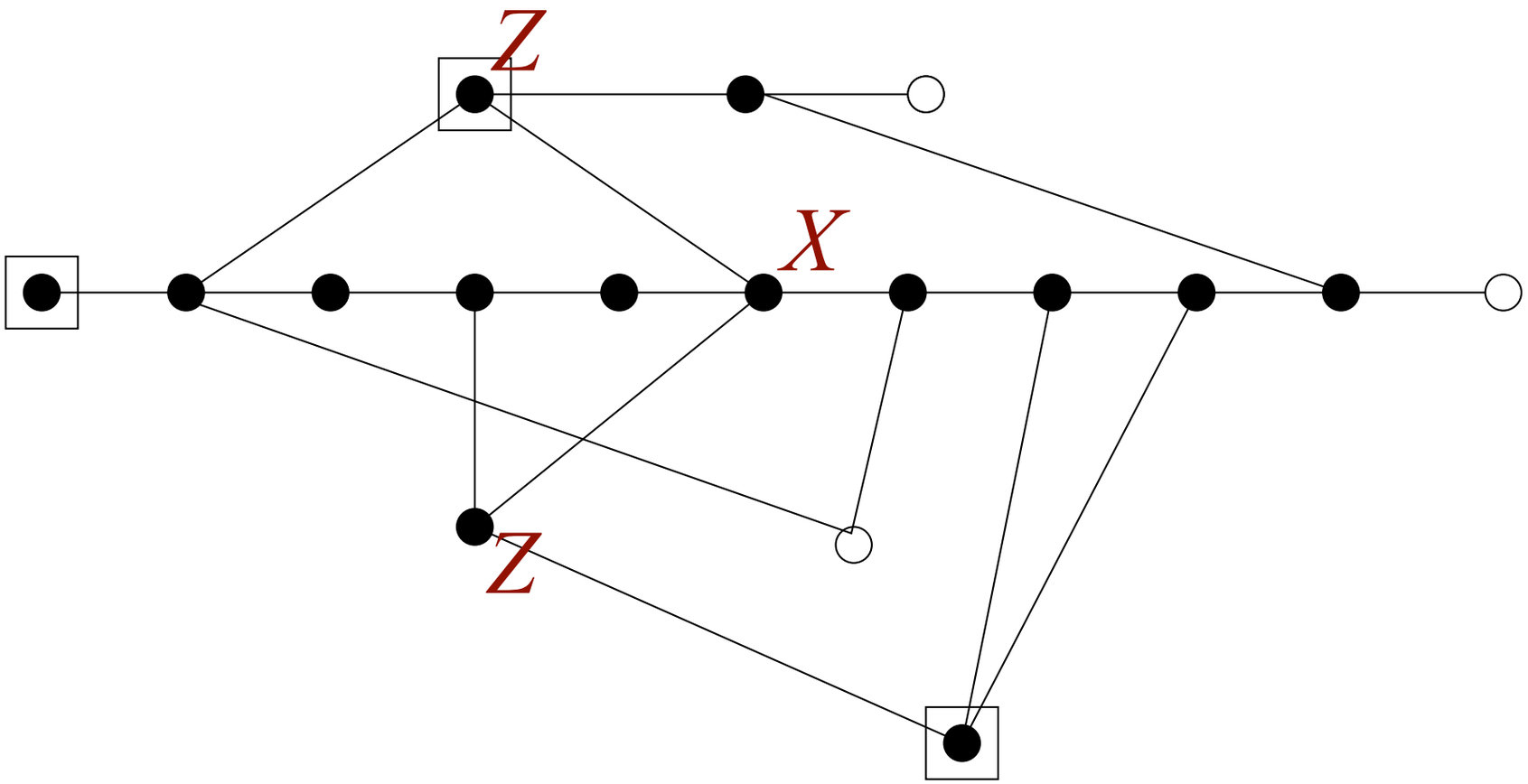


Graph State as Stabiliser States

Graph Stabilisers:

$$K_i := X_i(\prod_{j \in N_G(i)} Z_j)$$

$$K_i E_G N_{I^c} = E_G N_{I^c}$$

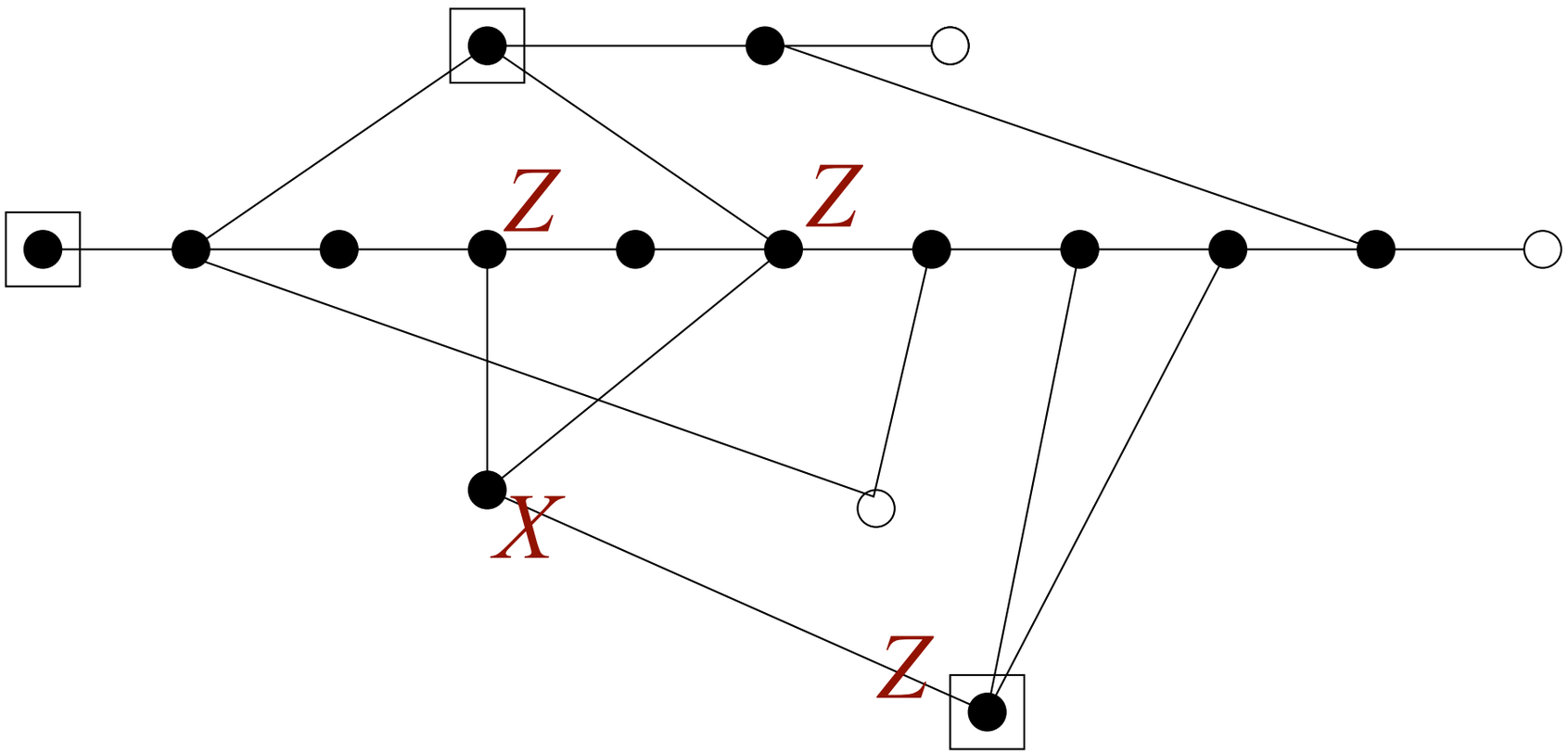


Graph State as Stabiliser States

Graph Stabilisers:

$$K_i := X_i(\prod_{j \in N_G(i)} Z_j)$$

$$K_i E_G N_{I^c} = E_G N_{I^c}$$

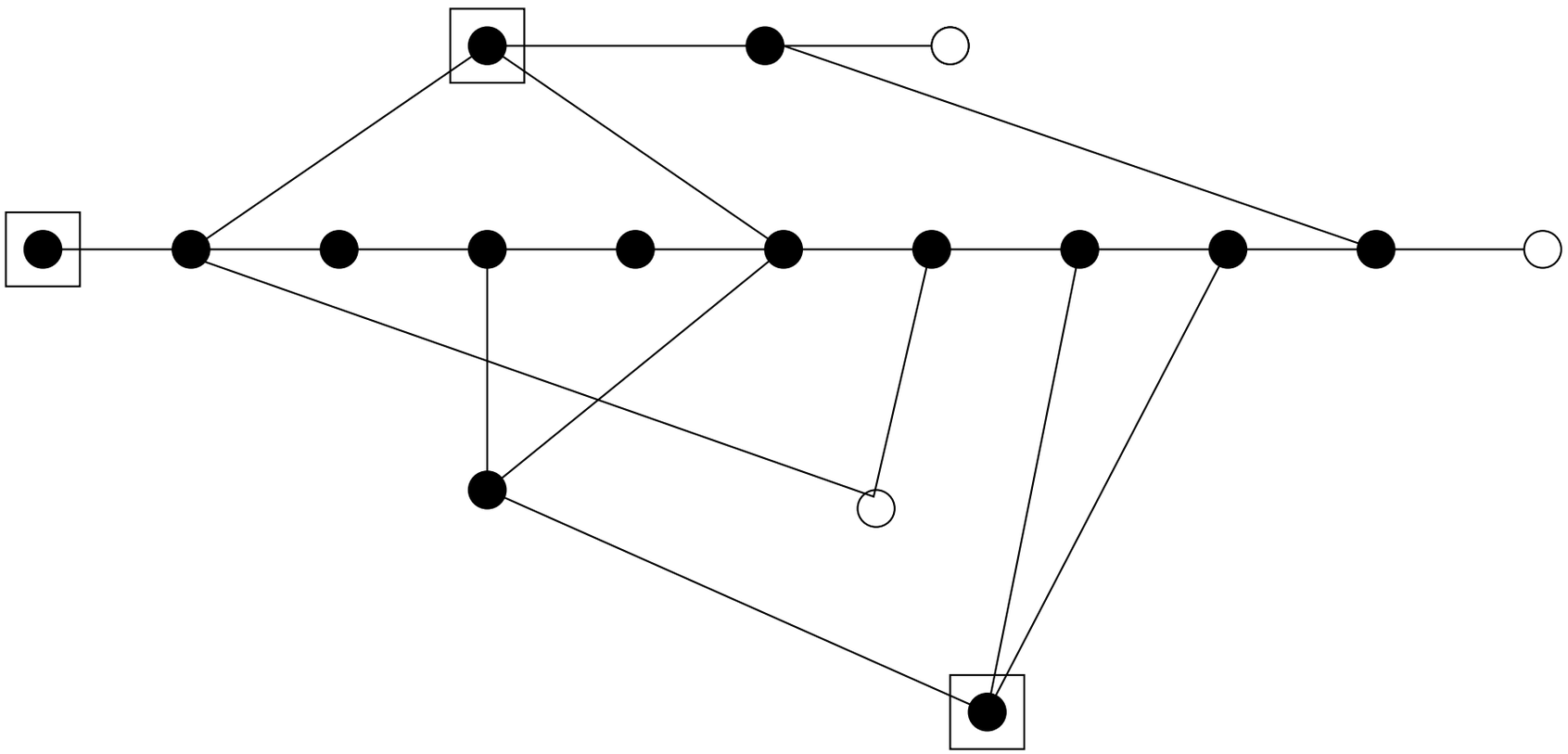


Graph State as Stabiliser States

Graph Stabilisers:

$$K_i := X_i(\prod_{j \in N_G(i)} Z_j)$$

$$K_i E_G N_{I^c} = E_G N_{I^c}$$



Classical Simulation

Corollary. Any MBQC pattern with only Pauli measurements can be efficiently simulated using Classical Computing.

Quantum Pattern

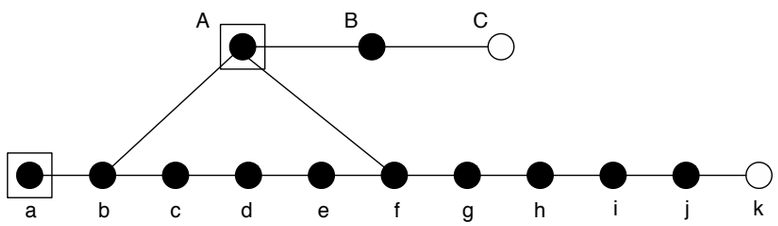
Fixing Angles

Classical Pattern

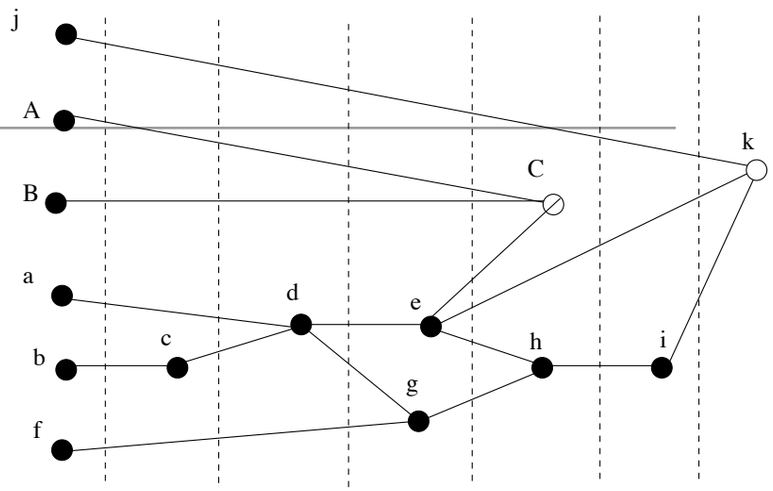
Model checking for a class of quantum protocols using PRISM

S. J. Gay, R. Nagarajan and N. Papanikolaou.

Parallelisation



Entanglement Graph



Execution Graph

Signal Shifting

$$
\begin{aligned}
{}^{t}[M_i^{\alpha}]^{s} &\Rightarrow S_i^{t}[M_i^{\alpha}]^{s} \\
X_j^{s} S_i^{t} &\Rightarrow S_i^{t} X_j^{s[t+s_i/s_i]} \\
Z_j^{s} S_i^{t} &\Rightarrow S_i^{t} Z_j^{s[t+s_i/s_i]} \\
{}^{t}[M_j^{\alpha}]^{s} S_i^{r} &\Rightarrow S_i^{r}\, {}^{t[r+s_i/s_i]}[M_j^{\alpha}]^{s[r+s_i/s_i]} \\
S_i^{s} S_j^{t} &\Rightarrow S_j^{t} S_i^{s[t+s_j/s_j]}
\end{aligned}
$$

Reducing Depth

Depth of a pattern is the length of the longest feed-forward chain

Standardisation and Signal Shifting reduce depth.

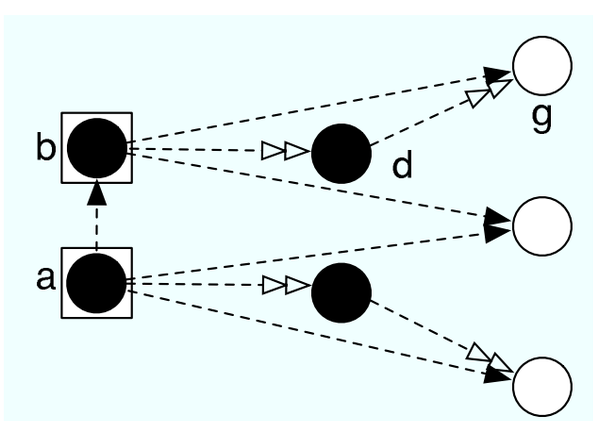
$$Z_g^{s_b} X_g^{s_d} Z_f^{s_b} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b} [M_c^{\gamma}]^{s_a}{}_{s_a}[M_b^{\beta}] M_a^{\alpha} E_G$$

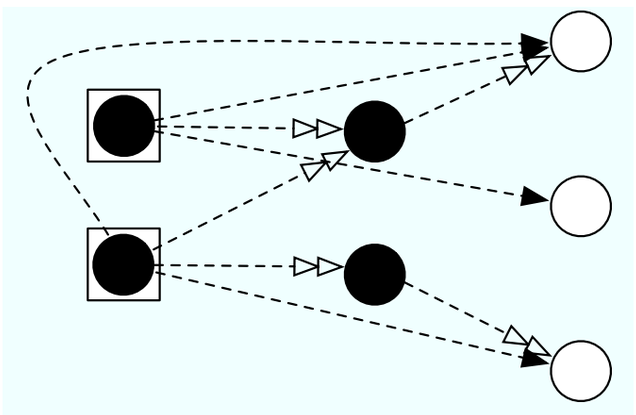
$$\Rightarrow \quad Z_g^{s_b} X_g^{s_d} Z_f^{s_b} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b} S_b^{s_a} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G$$

$$\Rightarrow \quad Z_g^{s_b} X_g^{s_d} Z_f^{s_b} S_b^{s_a} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b + s_a} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G$$

$$\Rightarrow \quad Z_g^{s_b} S_b^{s_a} X_g^{s_d} Z_f^{s_b + s_a} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b + s_a} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G$$

$$\Rightarrow \quad Z_g^{s_b + s_a} X_g^{s_d} Z_f^{s_b} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b + s_a} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G$$





Depth Complexity

All the models for QC are equivalent in computational power.

Theorem. There exists a logarithmic separation in depth complexity between MBQC and circuit model.

Parity function: MQC needs 1 quantum layer and $O(\log n)$ classical layers whereas in the circuit model the quantum depth is $\Omega(\log n)$

A. Broadbent and E. Kashefi, TCS 07

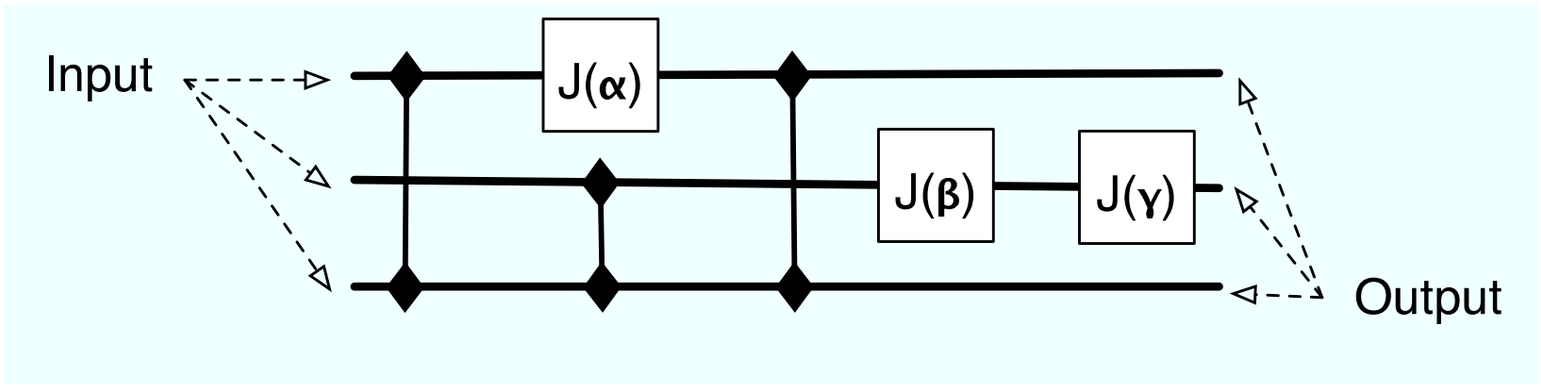
Depth Complexity

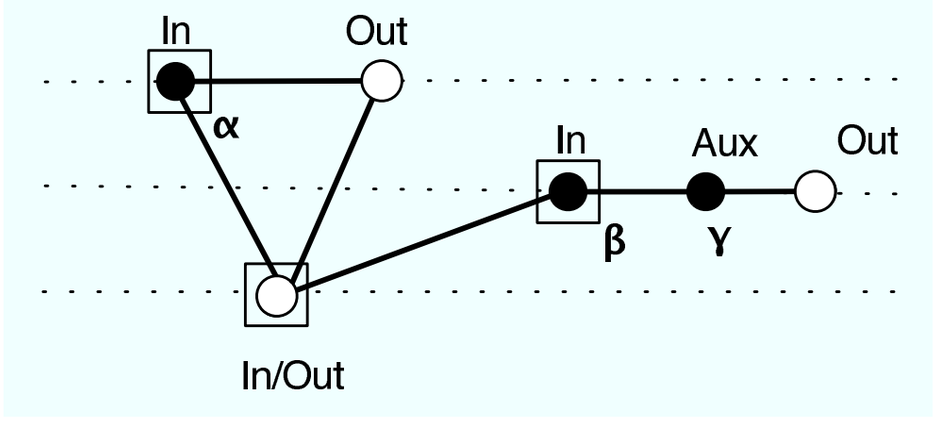
Theorem. MBQC has the same parallel computational power as quantum circuits with unbounded fan-out.

D. Browne, E. Kashefi, S. Perdrix TQC 07

Automated Parallelising Scheme

Theorem. Forward and backward translation between circuit model and MQC can only decrease the depth.



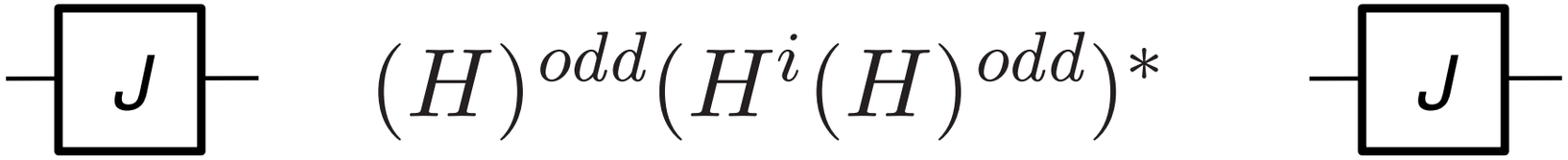


Characterisation

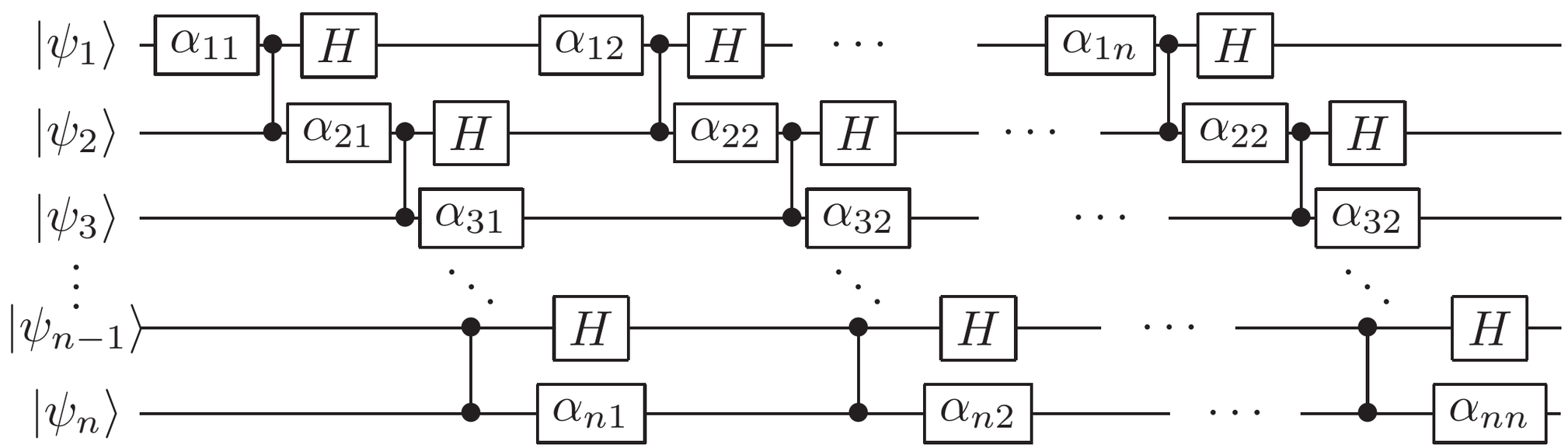
Theorem. A pattern has depth $d+2$ if and only if on any influencing path we obtain $P^* N^{i \leq d} P^*$ after applying the following rewriting rule:

$$N\, P_1^*\, \alpha_1\beta_1\, P_2^*\, \alpha_2\beta_2\, \cdots\, P_k^*\, N \begin{cases} NN & if \quad \forall P_i^* \neq X(XY)^* \\ N & otherwise \end{cases}$$

The Magical Clifford Sequence



Example



Can be parallelised to a pattern with depth 2

Determinism

A pattern is deterministic if all the branches are the same.

How to obtain global determinism via local controls

A necessary and sufficient condition for determinism
based on geometry of entanglement

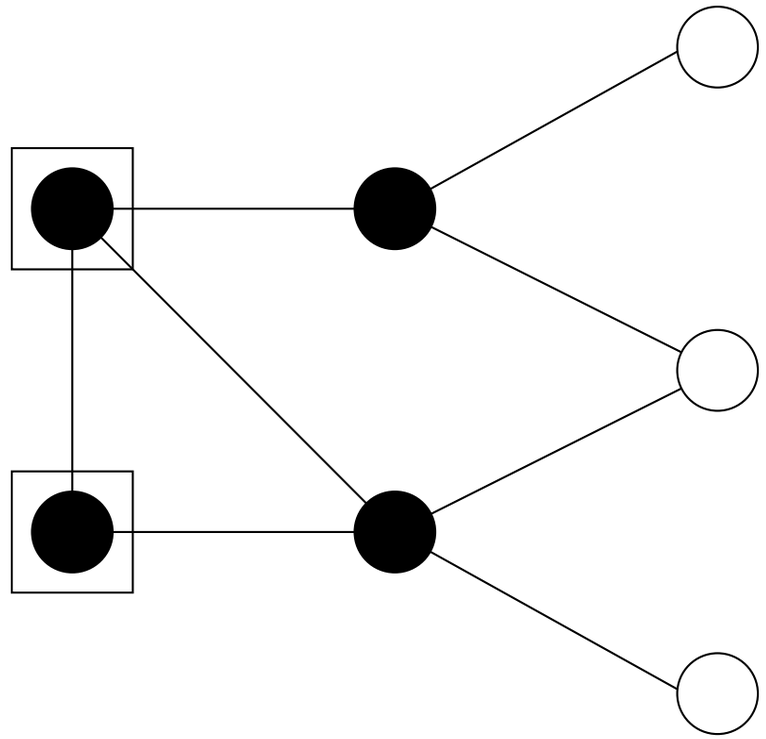
Flow

Definition. An entanglement graph (G, I, O) has flow if there exists a map $f : O^c \to I^c$ and a partial order $\preceq$ over qubits

- (i) $x \sim f(x)$
- (ii) $x \preceq f(x)$
- (iii) for all $y \sim f(x)$, we have $x \preceq y$

V. Danos and E. Kashefi Phys. Rev. A 07

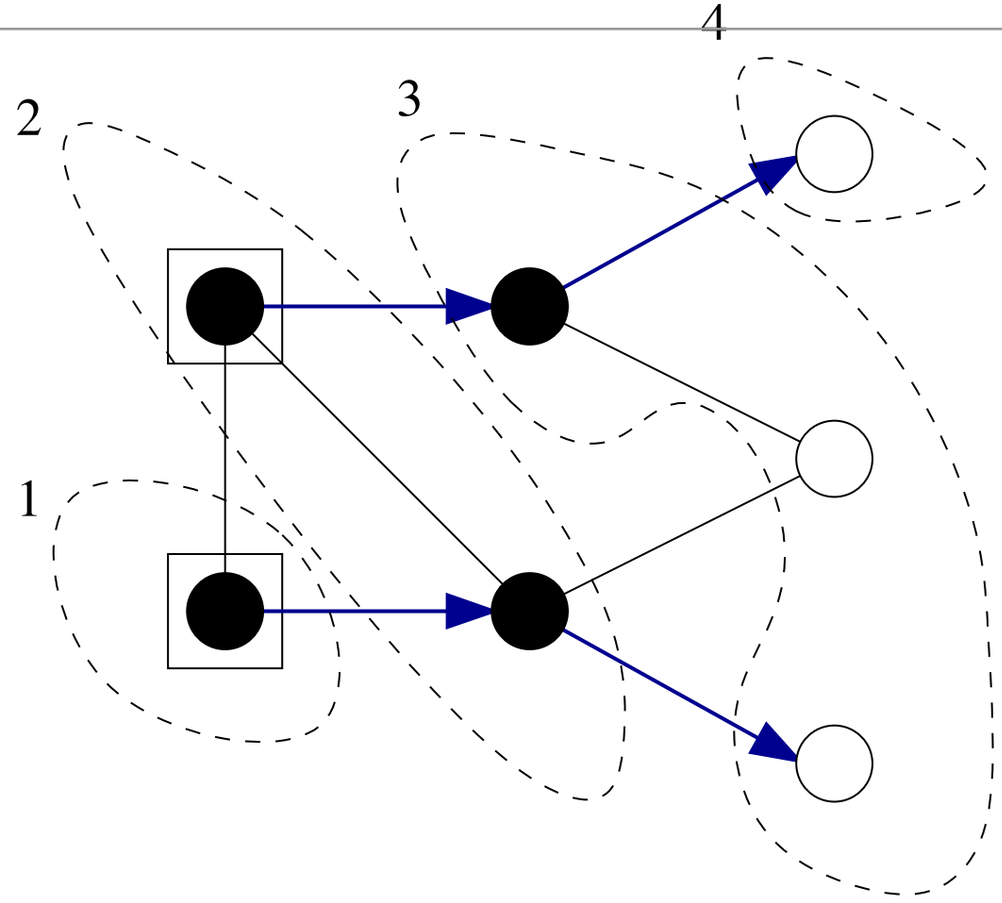
Flow



Find

- a qubits to qubits assignment
- a matching partial order

Flow

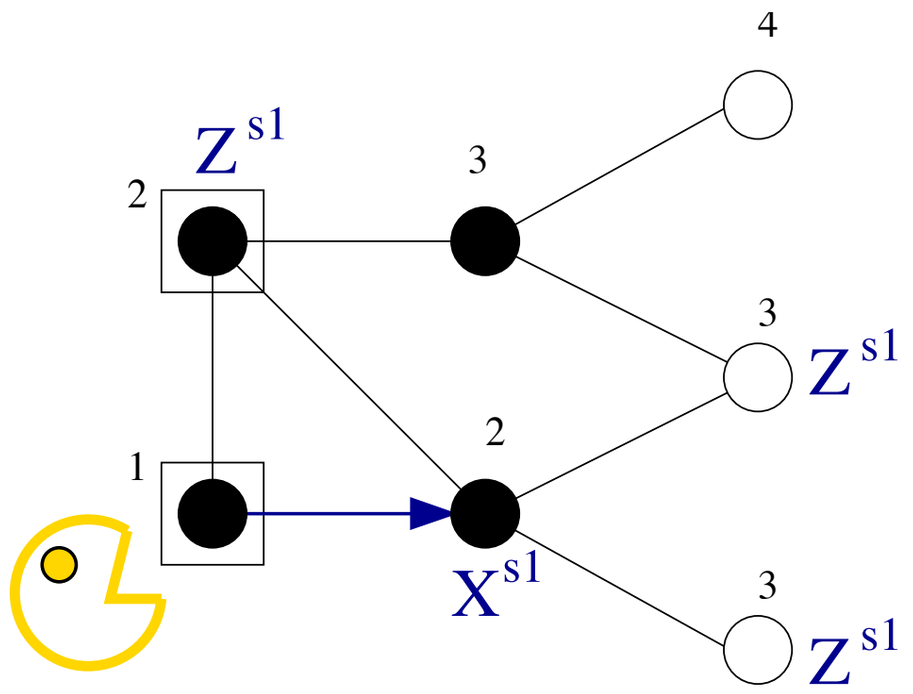


Find

- a qubits to qubits assignment
- a matching partial order

Constructive Determinism

Theorem. A pattern is uniformly and step-wise deterministic iff its graph has a flow.



$$\prod_{i \in O^c} (X_{f(i)}^{s_i} \prod_{k \in N_G(f(i)) \setminus \{i\}} Z_k^{s_i} M_i^{\alpha_i}) E_G$$

Pattern Design

Given a Unitary map we have to find

** Entanglement graph, $G(V, I, O)$

** Angles of measurements, $\{\alpha_i\}$

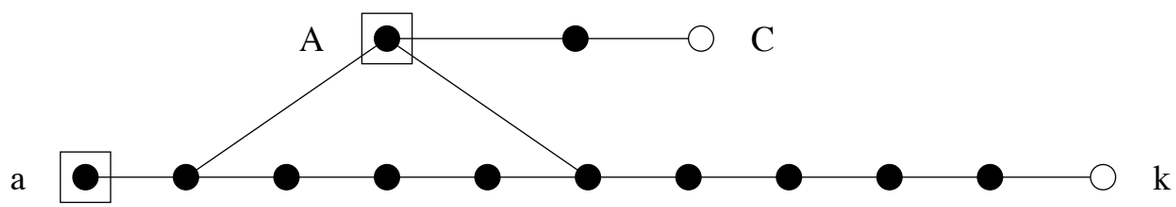
** Dependency structure

$$Z_k^{s_i+s_g+s_e+s_c+s_a} X_k^{s_j+s_h+s_f+s_d+s_b} X_C^{s_B} Z_C^{s_A+s_e+s_c}$$

$$M_B^0 M_A^{-\alpha'} M_j^0 [M_i^{\beta-\pi}]^{s_h+s_f+s_d+s_b} [M_h^{-\frac{\gamma}{2}}]^{s_g+s_e+s_c+s_a} [M_g^{\frac{\pi}{2}}]^{s_f+s_d+s_b}$$

$$M_f^0 [M_e^{-\frac{\pi}{2}}]^{s_d+s_b} [M_d^{\frac{\gamma}{2}}]^{s_c+s_a} [M_c^{\frac{\pi-\delta-\beta}{2}}]^{s_b} M_b^0 M_a^{\frac{-\beta+\delta+\pi}{2}}$$

$$E_{BC} E_{AB} E_{jk} E_{ij} E_{hi} E_{gh} E_{fg} E_{Af} E_{ef} E_{de} E_{cd} E_{bc} E_{ab} E_{Ab}$$



Indirect Way

- Start with a circuit implementing U
- Translates each gate with the corresponding pattern
- Use measurements calculus algorithm to obtain the standard form

Direct Way

- Given *U* find *G* and $\{\alpha_i\}$ *(Phase Map Decomposition)*

- From the geometry of *G* obtain the feed-forward structure *(Flow Condition)*

- *If failed then back track*

Phase Map Decomposition

Theorem. Every Unitary on ***n*** qubits can be decomposed as:

$$U = R_O \circ D_V \circ P_{I^c}$$

Preparation map, $P_{I^c} : \mathcal{H}_I \to \mathcal{H}_V$ where $|x\rangle \mapsto |x\rangle \otimes |+\cdots+\rangle_{I^c}$

Restriction map, $R_O : \mathcal{H}_V \to \mathcal{H}_O$ where $|x\rangle \mapsto |x\rangle|_O$

Example

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

$$J_\alpha = R_{12\to 2} D_{12\to 12} P_{1\to 12}$$

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & -e^{i\alpha} \end{pmatrix} \cdot 2^{-1/2} \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{aligned} J_\alpha &= R_1(Z_1^\alpha \wedge Z_{12}) P_2 \\ &= \langle +_\alpha |_1 \wedge Z_{12}) P_2 \end{aligned} \longrightarrow X_2^{s_1} M_1^\alpha E_{12} N_2$$

An algorithm to generate all such decompositions

- *Input*: for sets V, I, and O and $n = |I^c|$:

  ** a unitary U on $\mathcal{H}_I$;
  ** complex numbers $\{ x_{pq}^{(i)} \}_{i=1}^{2^{n-|I|}}$ satisfying Equations:

$$u = \sum_{i<2^{n-|I|}} x^{(i)}$$

$$2^{n/2}|x^{(i)}| = 1$$

  ** a permutation σ over $\{1, \cdots, 2^{n-|I|}\}$.

- *Output*: diagonal elements $\{d_{kk}\}_{k=1}^{2^{|V|}}$, such that $d_{kk} = \sqrt{2^n}\, x_{pq}^{(i)}$, where:

  ** the binary representation of p agrees with that of k after restriction to O;
  ** $q \equiv k \bmod 2^{|I|}$;
  ** $i = \sigma(\lfloor k/2^{|I|} \rfloor)$.

An algorithm to obtain the graph and the angles

- *Input*: A phase map decomposition for U
- *Output*: either (i) A graph G on V and $\{\alpha_j\}_{j\in O^c}$, or (ii) no matching graph exists.

1. For $j \in \{1, \cdots, |O^c|\}$, consider the $|V|$-bit string $\mathbf{z}_j$ that only has a 1 at position j, and set α such that $e^{-i\alpha_j} = d_{\mathbf{z}_j\mathbf{z}_j}$.

2. For all j, k, consider the $|V|$-bit string $\mathbf{z}_{jk}$ having a 1 only at positions j and k. Check whether $d_{\mathbf{z}_{jk}\mathbf{z}_{jk}} = \pm e^{-i(\alpha_j+\alpha_k)}$ (the angles for the corresponding qubit in O is taken to be 0).
   — (i) if YES and the sign is -1, return E_{jk} as an edge in G.
   — (ii) if NO, no matching graph exists.

So we get:

A pattern with projections

$$\langle +_\alpha|_1 \wedge Z_{12})P_2$$

We need to replace ***projections*** with ***measurements*** and still obtain determinism

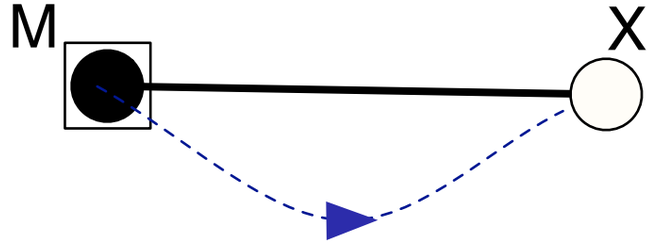
From Projection to Measurement

$$P_i^{|+\alpha\rangle} =$$

From Projection to Measurement

$$P_i^{|+\alpha\rangle} = M_i^{\alpha} Z_i^{s_i}$$

Anachronical Correction



$$P_i^{|+\alpha\rangle} E_{ij} = M_i^{\alpha} \; X_j^{s_i} \; E_{ij} \; X_j^{s_i}$$

From Noise to Determinism

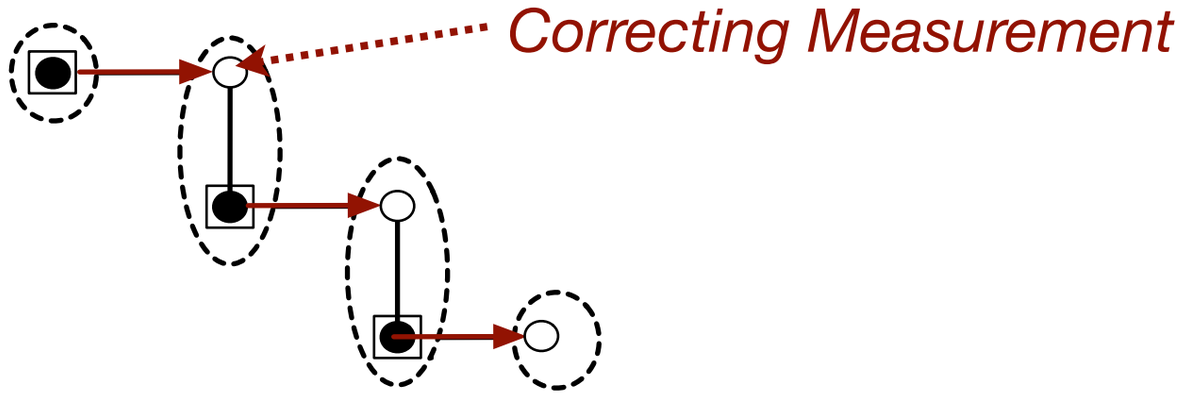
A pattern is **deterministic** if all the branches are the same.

A necessary condition for determinism
based on **geometry** of entanglement is given by flow

Flow

Definition. An entanglement graph (G, I, O) has flow if there exists a map $f : O^c \to I^c$ and a partial order $\preceq$ over qubits

- (i) $x \sim f(x)$
- (ii) $x \preceq f(x)$
- (iii) for all $y \sim f(x)$, we have $x \preceq y$



Flow

Theorem. A pattern with flow is uniformly and strongly deterministic.

Patterns with flow  Unitary embedding

Summary

Static structure/Entanglement

Understand ↓ **Analyse** ↓ **Control**

Quantum Computation

Parallelism, Determinism, Decomposition

Future Directions - *Specific tools for MBQC*

Algorithmic Design

Direct synthesis of unitaries as patterns

Complexity Analysis

Parallelisation scheme and characterisation of low depth patterns

Security Protocols

Commitment and hiding by exploring the geometry of interaction

Model Checking and Formal Verification

To detect security leaks in protocols

Experimental Blind Quantum Computing

Experimental Blind Quantum Computing

Stefanie Barz
Vienna

Elham Kashefi,
Edinburgh

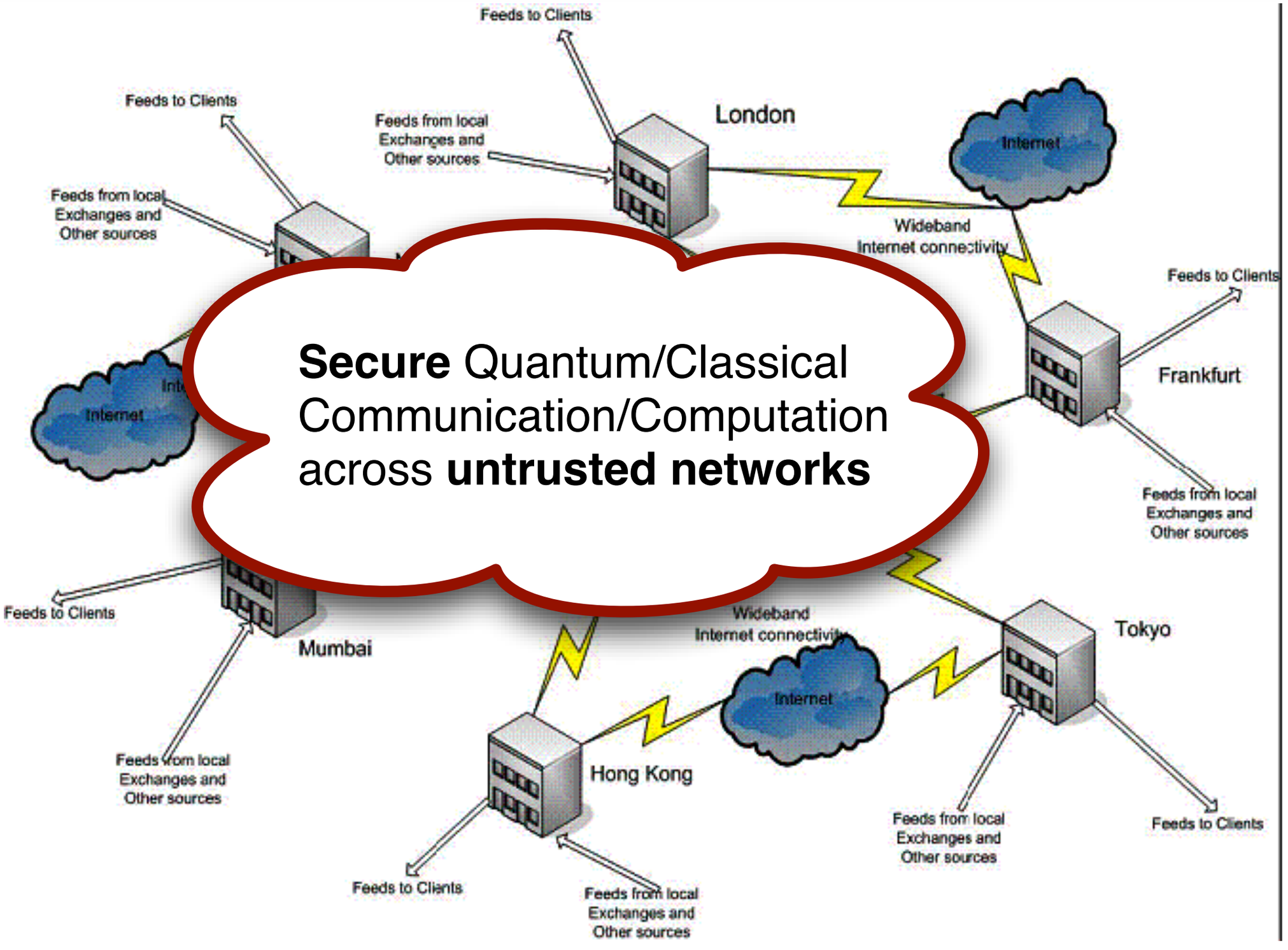
Anne Broadbent
Waterloo

Philip Walther,
Vienna

Anton Zeilinger,
Vienna

Joe Fitzsimons,
Singapore

Cloud Computing



Homomorphic Encryption

Rivest 78: Processing encrypted data without decrypting it first

- Voting system
- Collision-resistance hash function
- Private information retrieval

➡ There are several efficient, partially homomorphic crypto-systems

(RSA: for multiplication)

Gentry 09: A Lattice-based cryptosystem that is fully homomorphic but **inefficient** and only **computationally secure**

Broadbent Fitzsimons Kashefi 09: A quantum based fully homomorphic **unconditionally** secure cryptosystem with **verification**

Related Works

- 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

- Andrew Childs - *Secure assisted QC*

  ➡ Alice needs quantum memory, state preparation and Pauli gates

  ➡ The unitary function is public

  ➡ In general dishonest Bob cannot be detected

- Aharonov, Ben-Or and Eban - *Interactive Prove for QC*

  ➡ Alice has a constant-size quantum computer

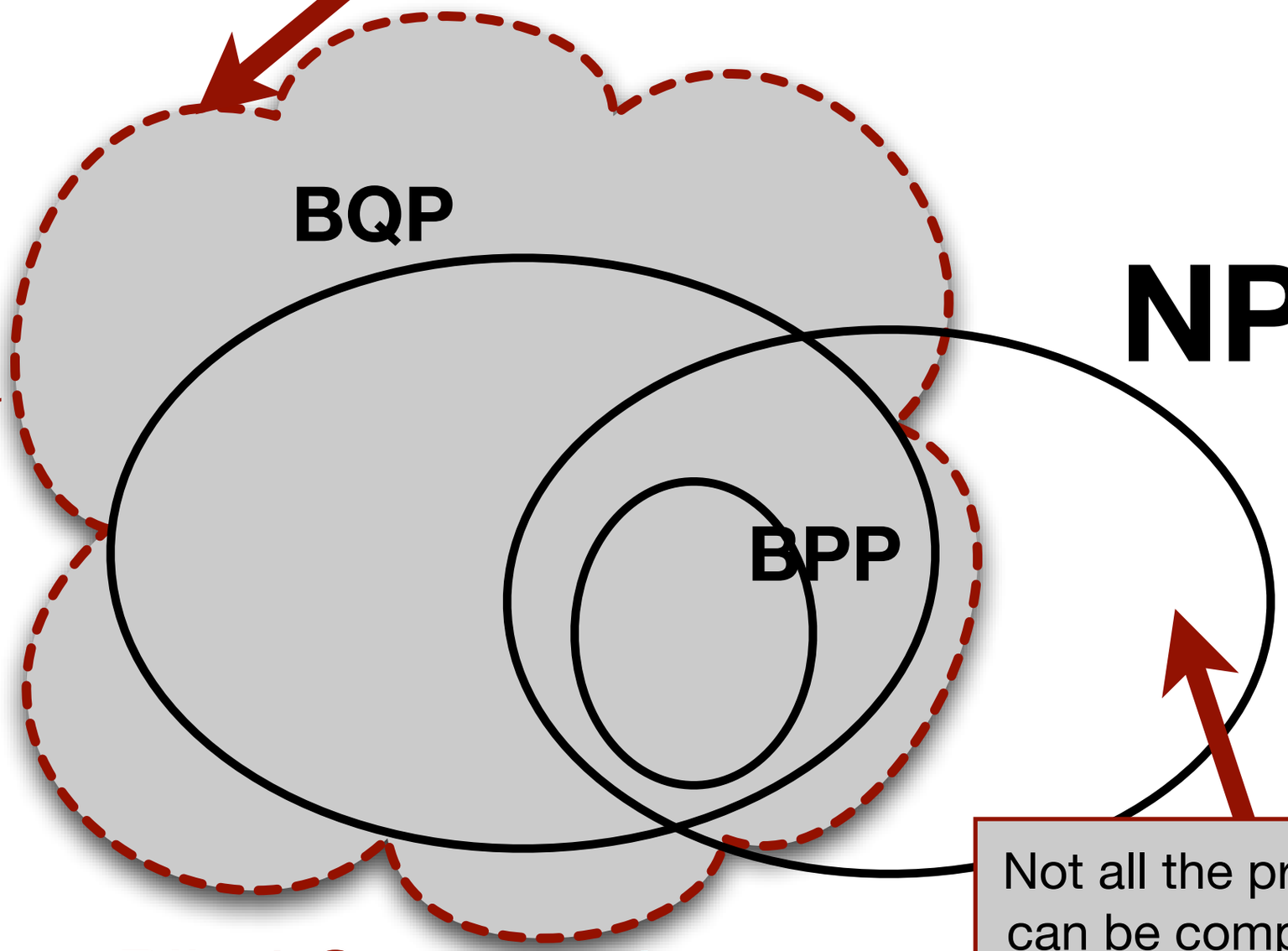
Big Picture

Still requires 2^n parameters for a classical computer to simulate it

How do we verify the Solution ?

Can we verify it with a classical Computer ?

YES

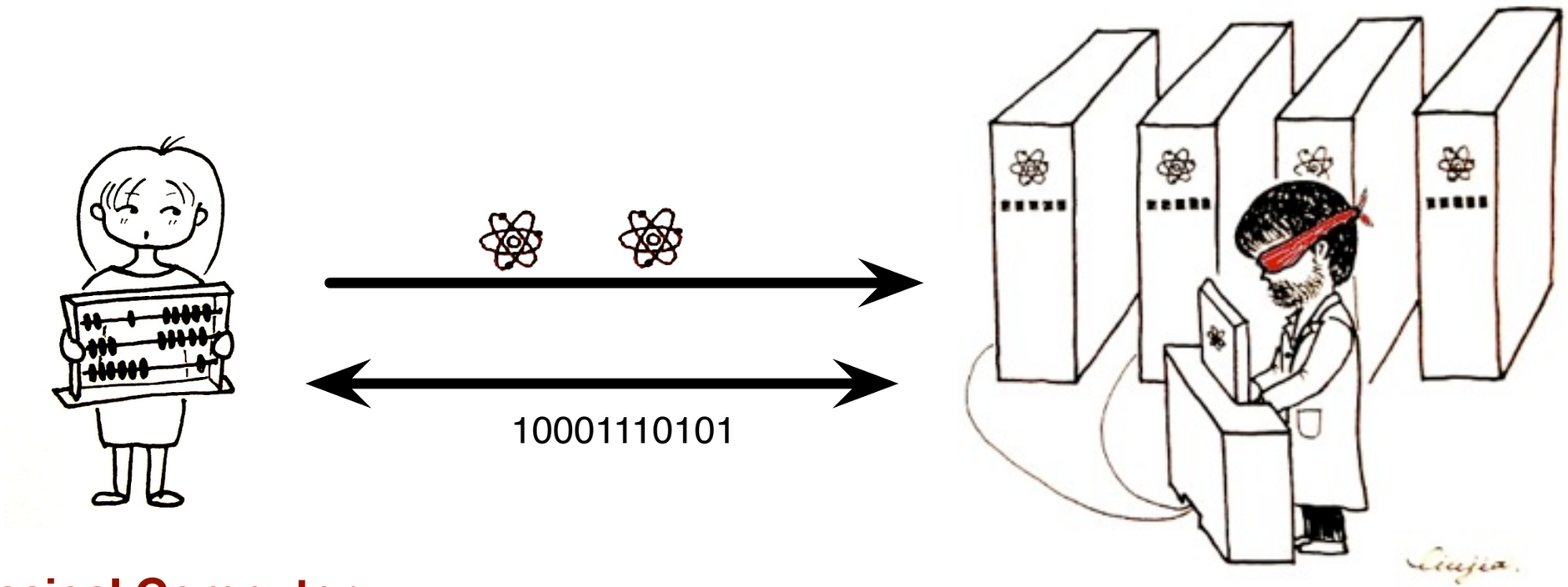


Blind Computation with **BPP*** Alice

Not all the problem in NP can be computed blindly with a BPP Alice

- Abadi, Feigenbaum and Kilian

Universal Blind QC Protocol



Classical Computer

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

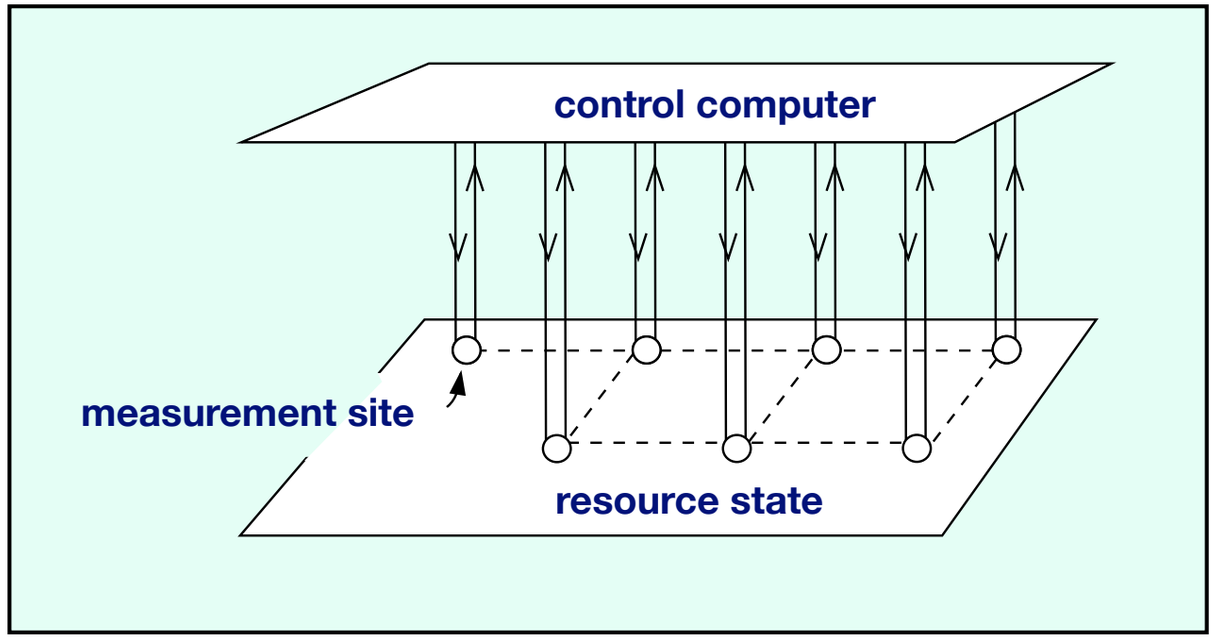
Our Technique

Measurement-based Quantum Computing

[Raussendorf, Briegel, 2001]

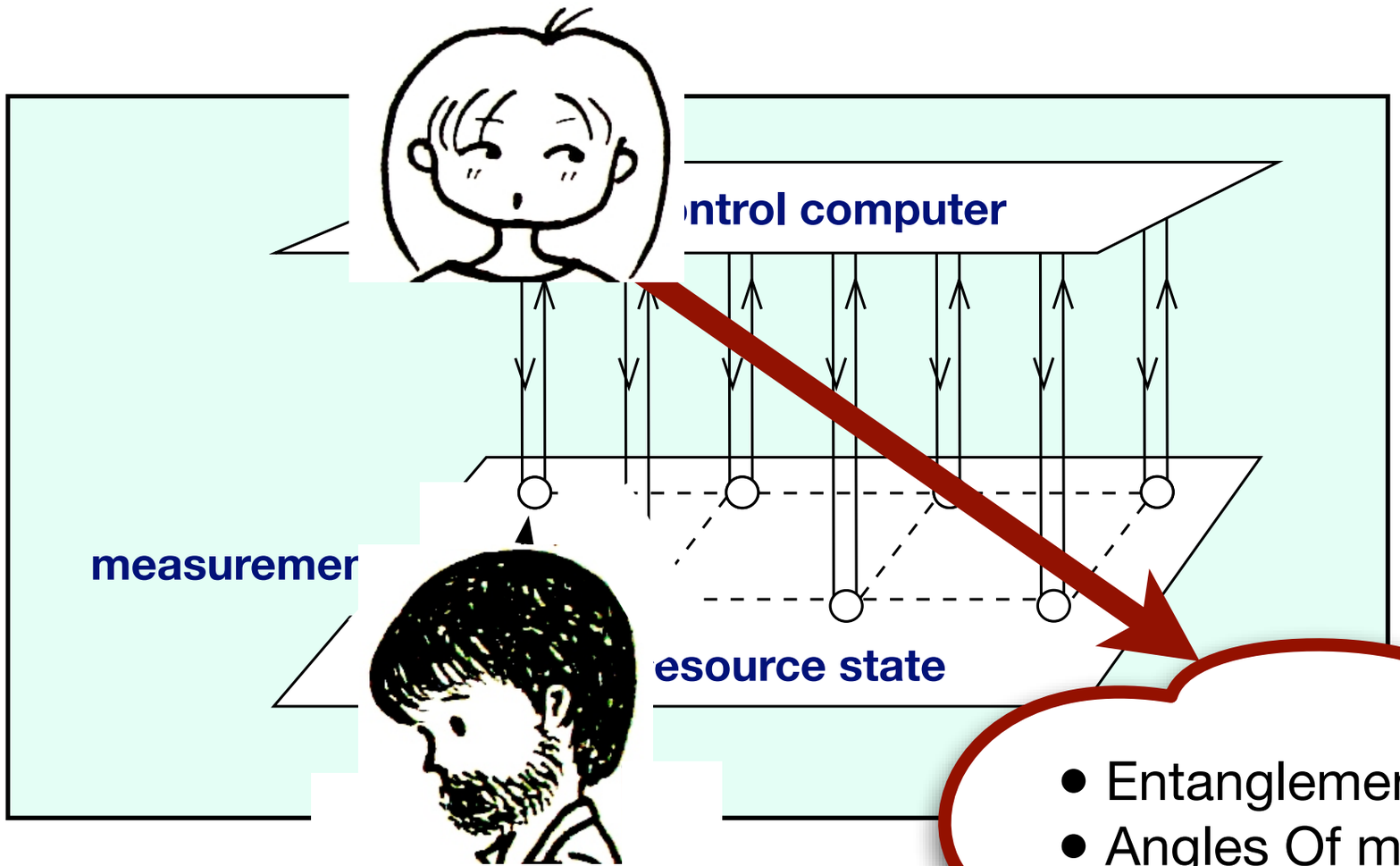
Measurement Calculus

[Danos, Kashefi, Panangaden 2007]



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

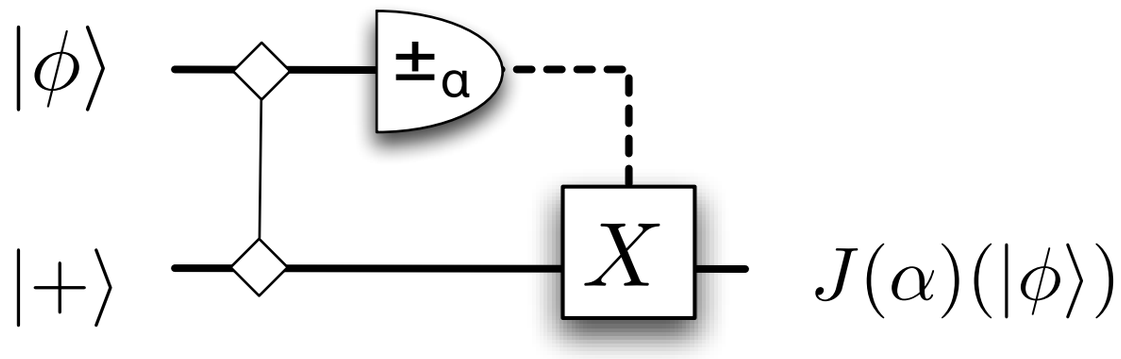
The First MBQC Protocol



- Entanglement Resource
- Angles Of measurements
- Results of Measurements
- Dependencies

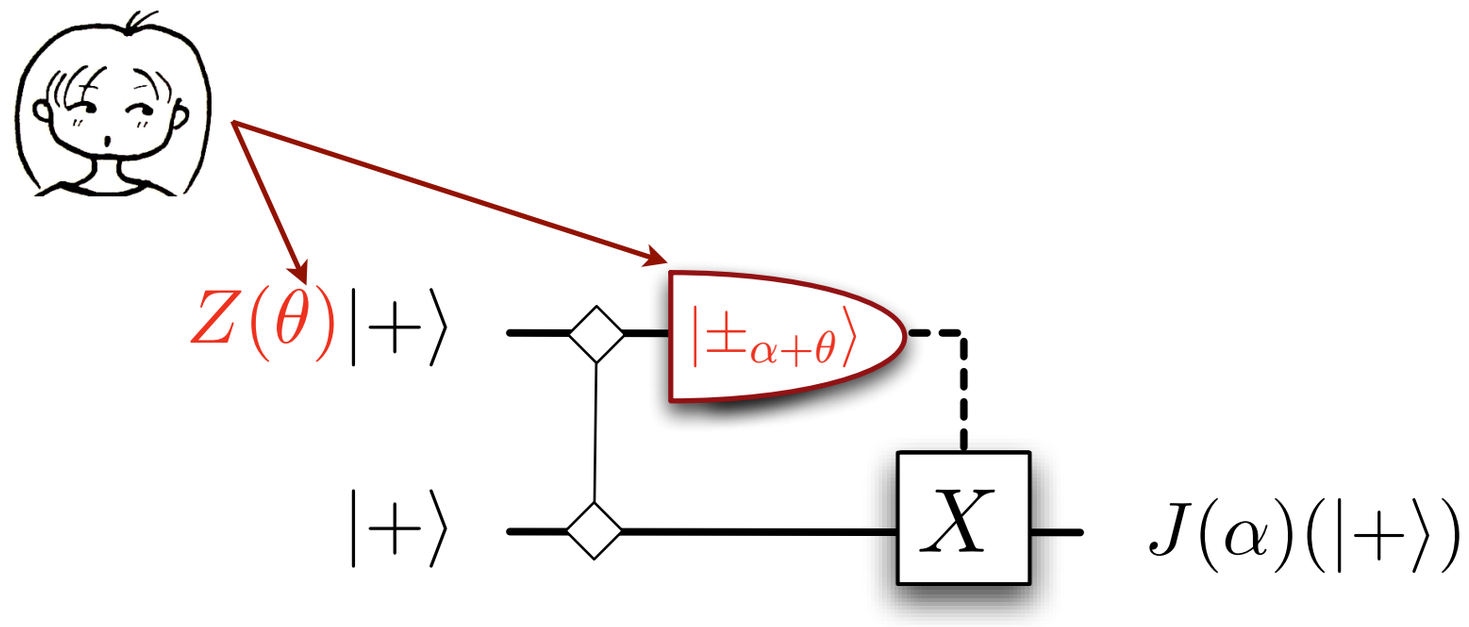
Encoding of the Angles

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



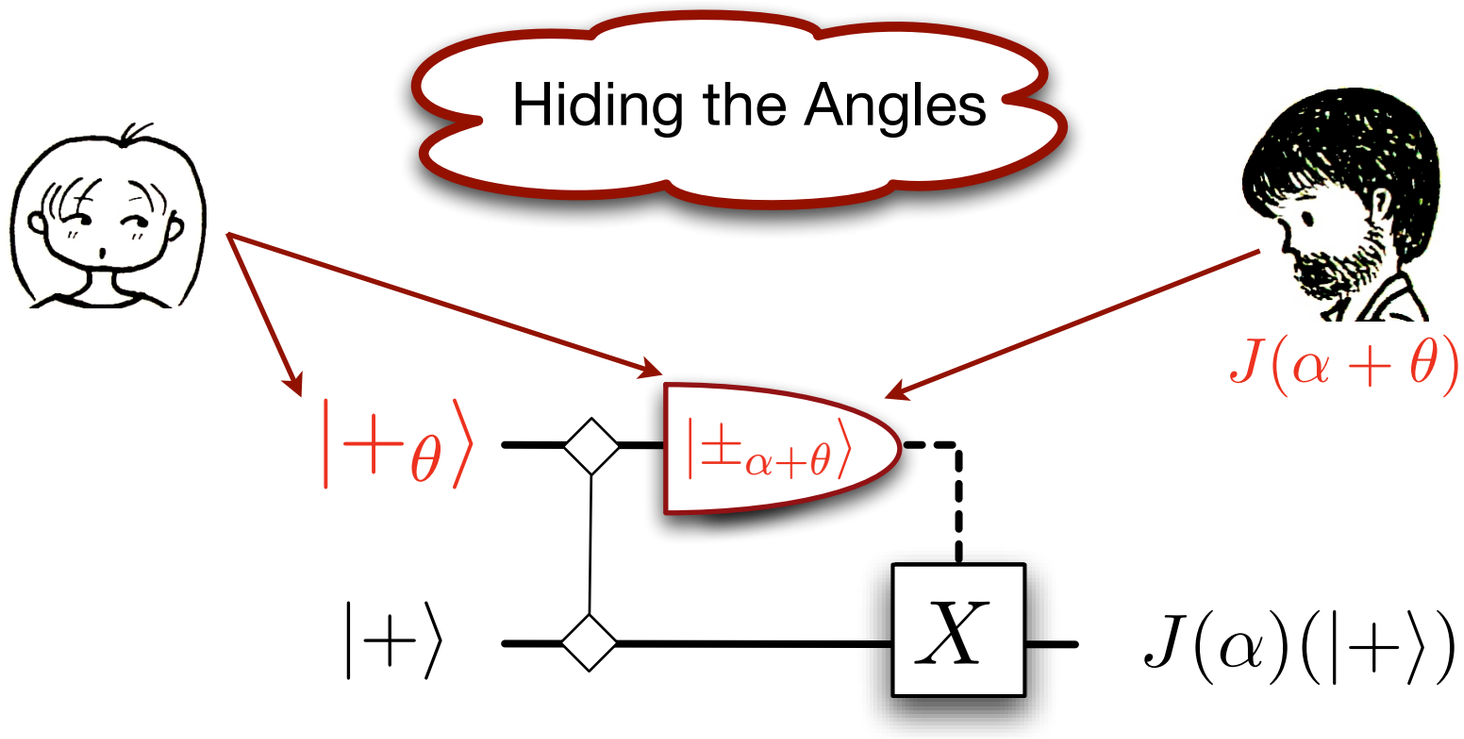
Encoding of the Angles

- **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

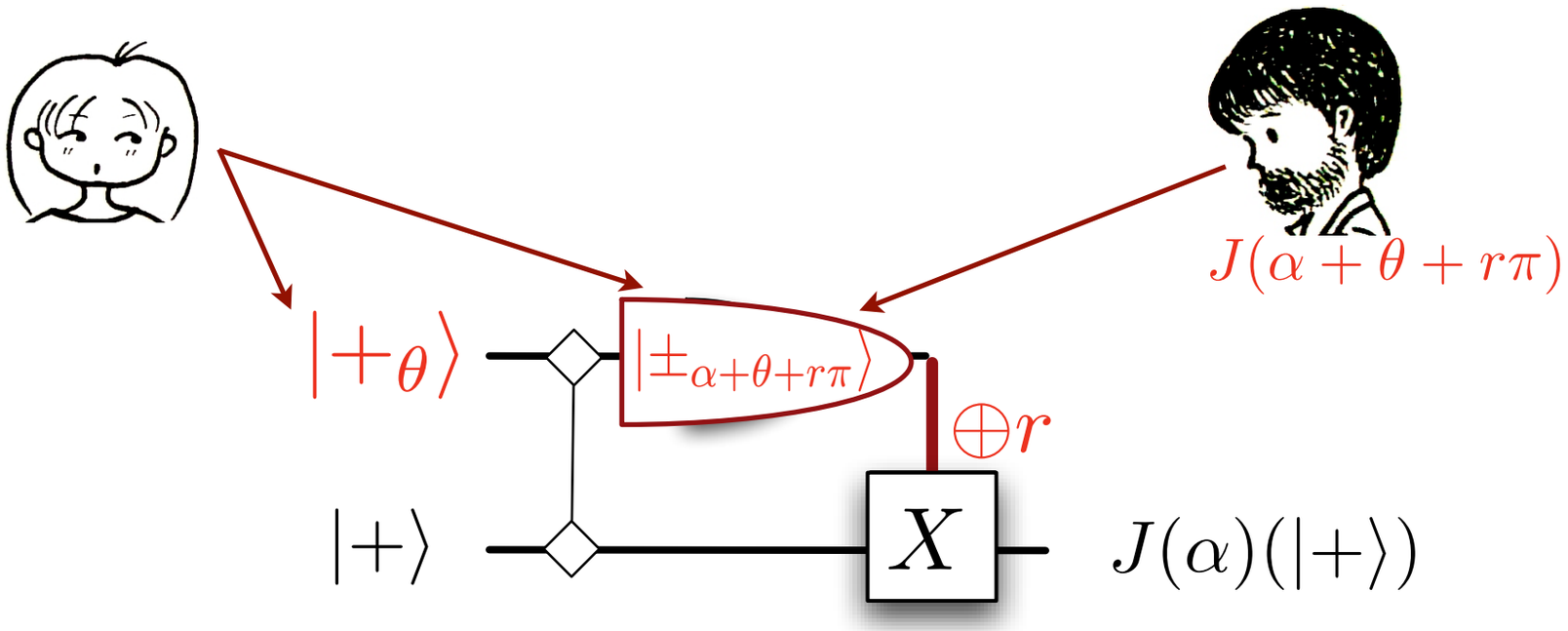
- **One-qubit Teleportation** $\quad J(\alpha) \;:=\; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$



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

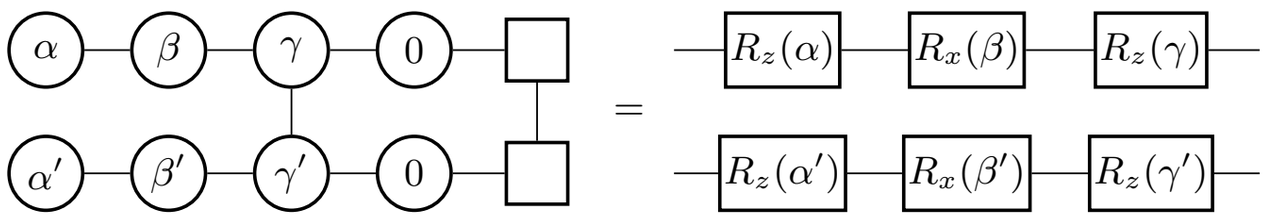
Encoding of the Angles

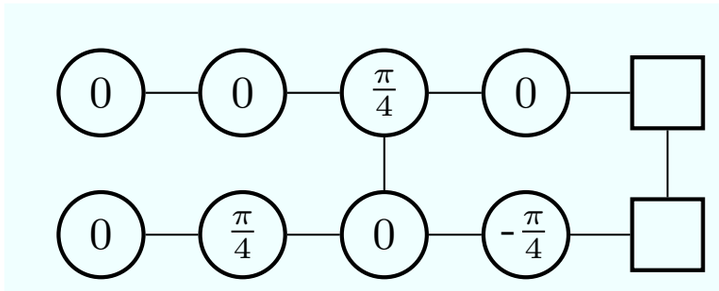
- **One-qubit Teleportation** $J(\alpha) := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$

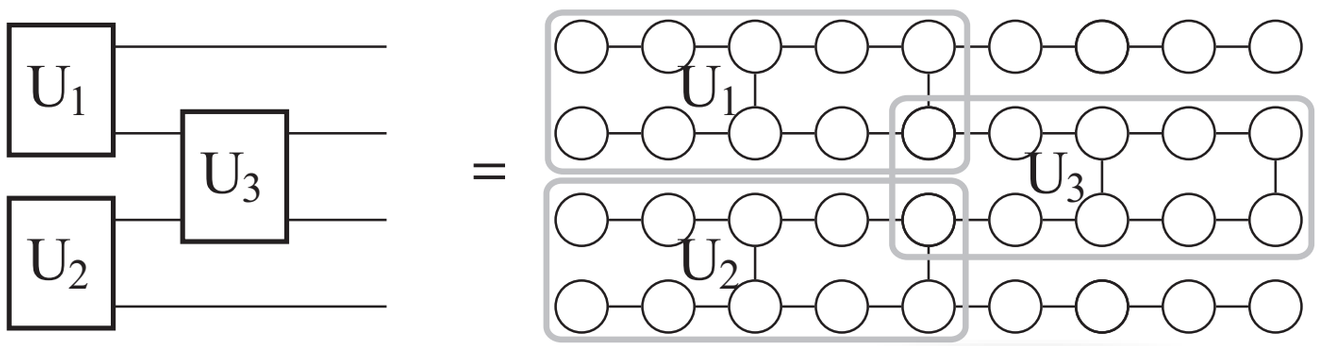


Hiding the measurement result

Universality



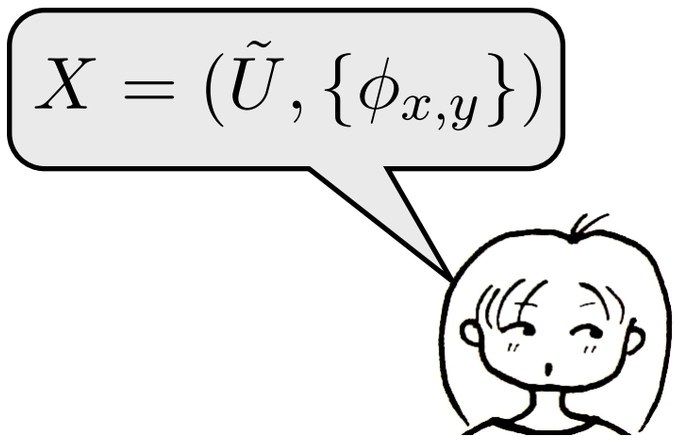




Hiding the entanglement resource

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

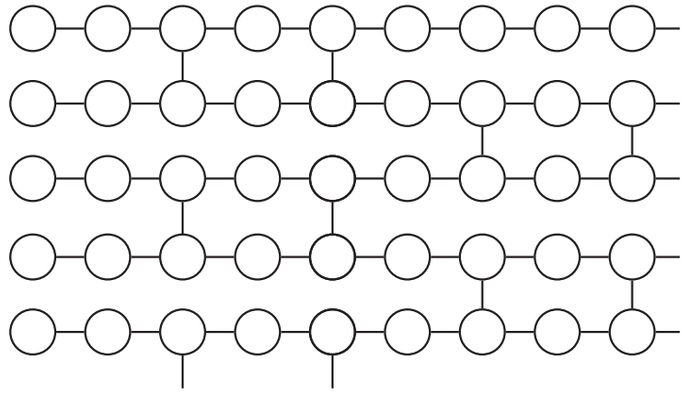
Main Protocol



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

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

$\delta_{x,y}$



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

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

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

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

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

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

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

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

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

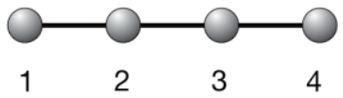
➡ Independence of Bob's quantum information for a fixed δ

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

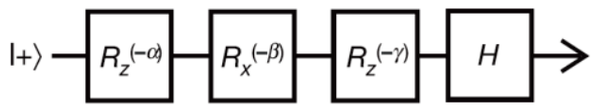
2. $r_{x,y} = 1$ so $\delta_{x,y} = \phi'_{x,y} + \theta'_{x,y} + \pi$ and $|\psi_{x,y}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i(\delta_{x,y} - \phi'_{x,y})}|1\rangle)$.

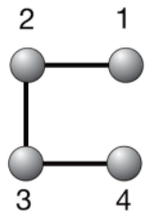
Real Bob

Univ.-Ass. Dr. Philip Walther
Photonic Quantum Computation & Quantum Simulation

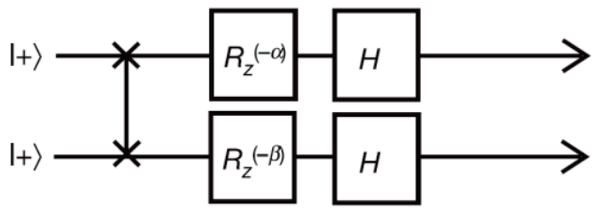


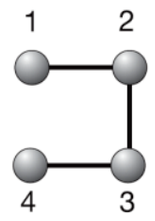
Linear$^{(4)}$ cluster



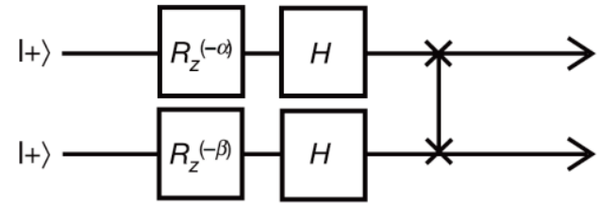


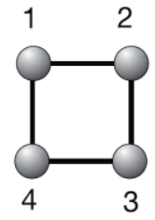
Horseshoe$^{(4)}$ cluster



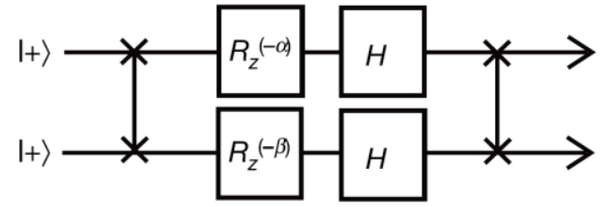


Horseshoe$^{(4)}$ cluster
(rotated180°)

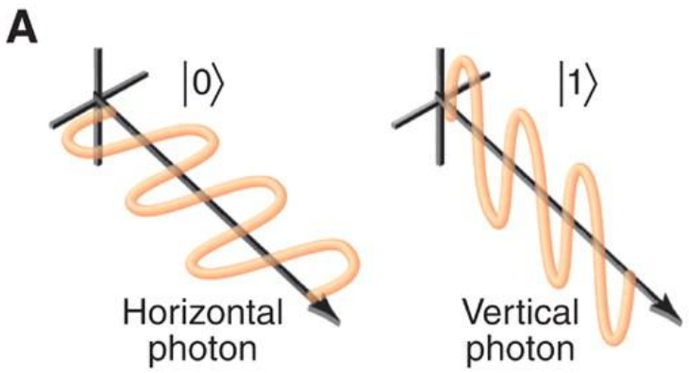




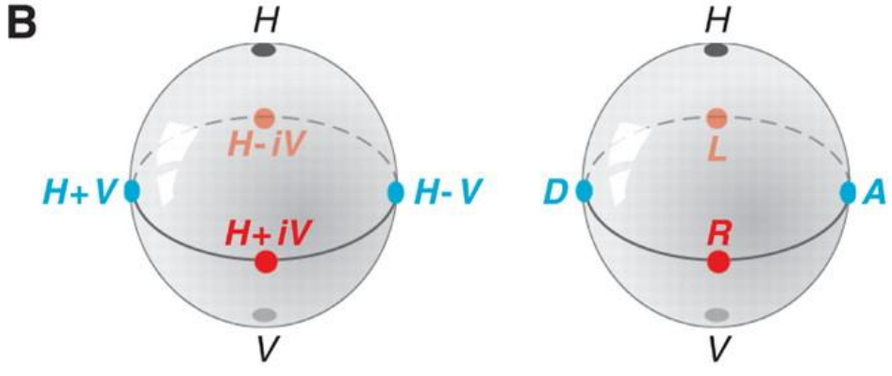
Box$^{(4)}$ cluster

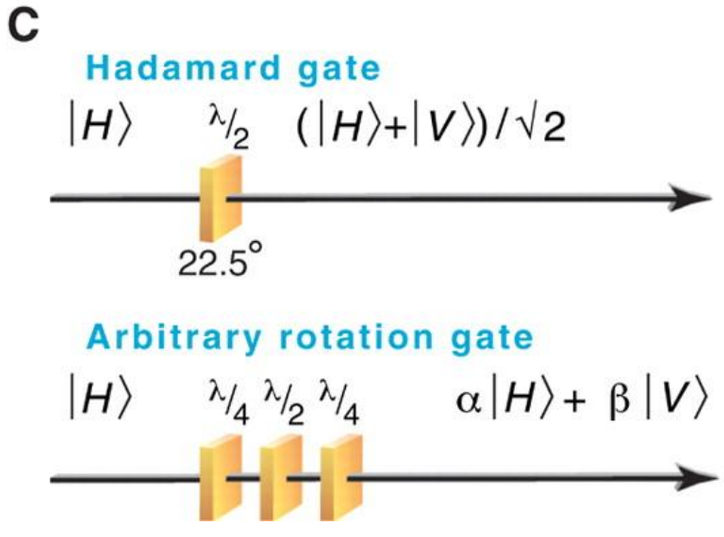


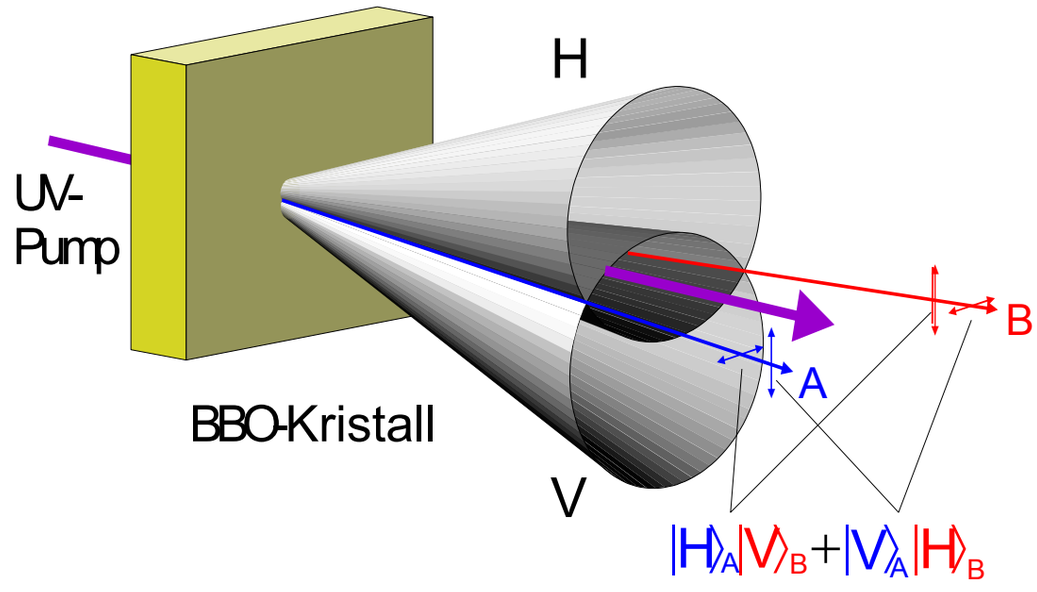
Photonic ToolBox for QC



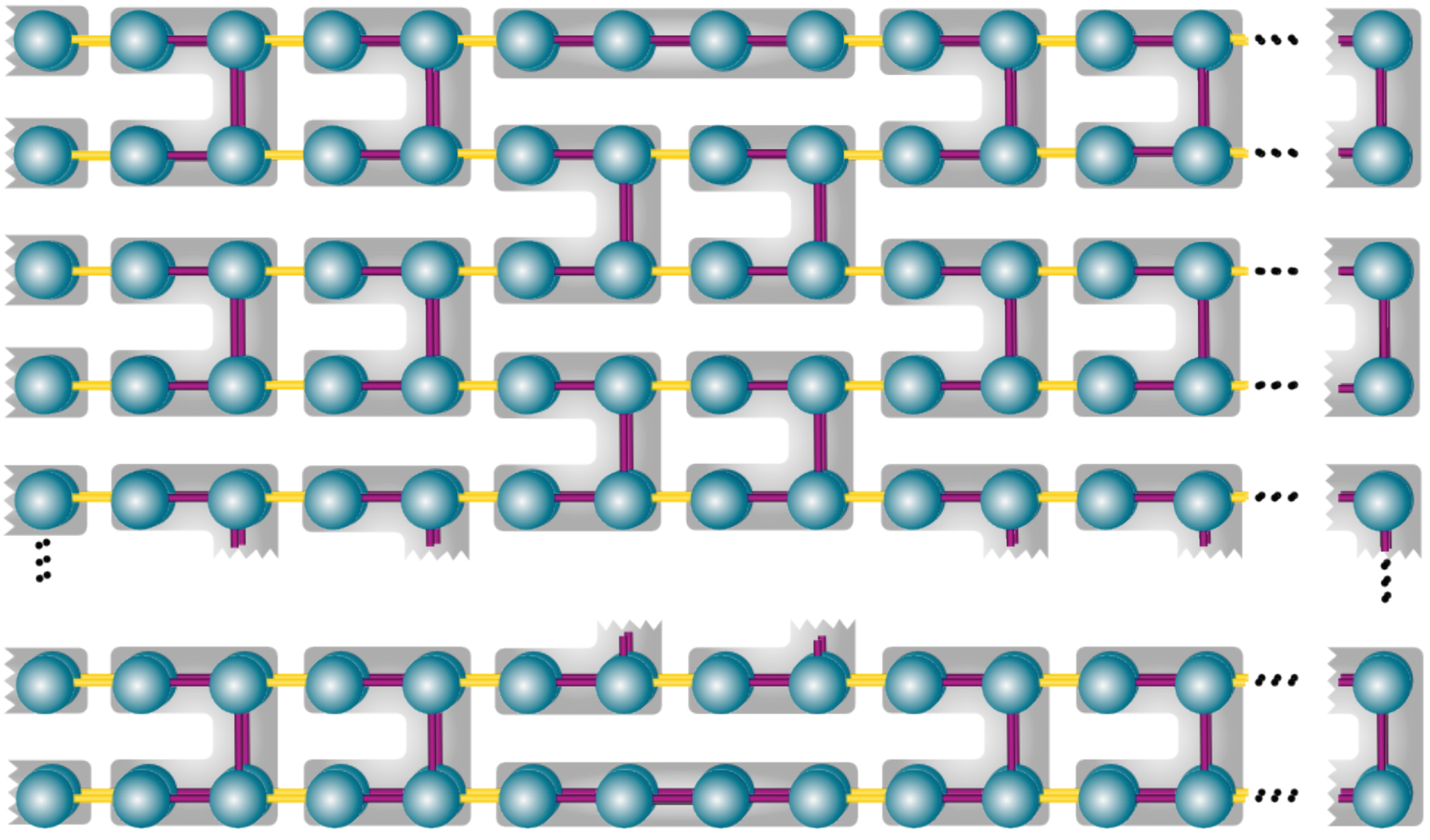
Spontaneous Parametric Down-Conversion



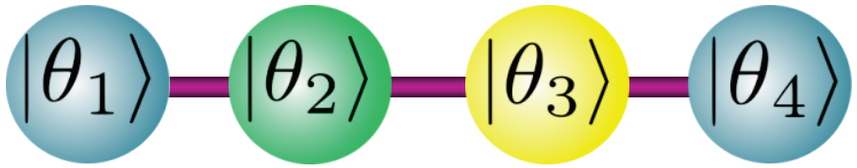




Implementation = Think Small



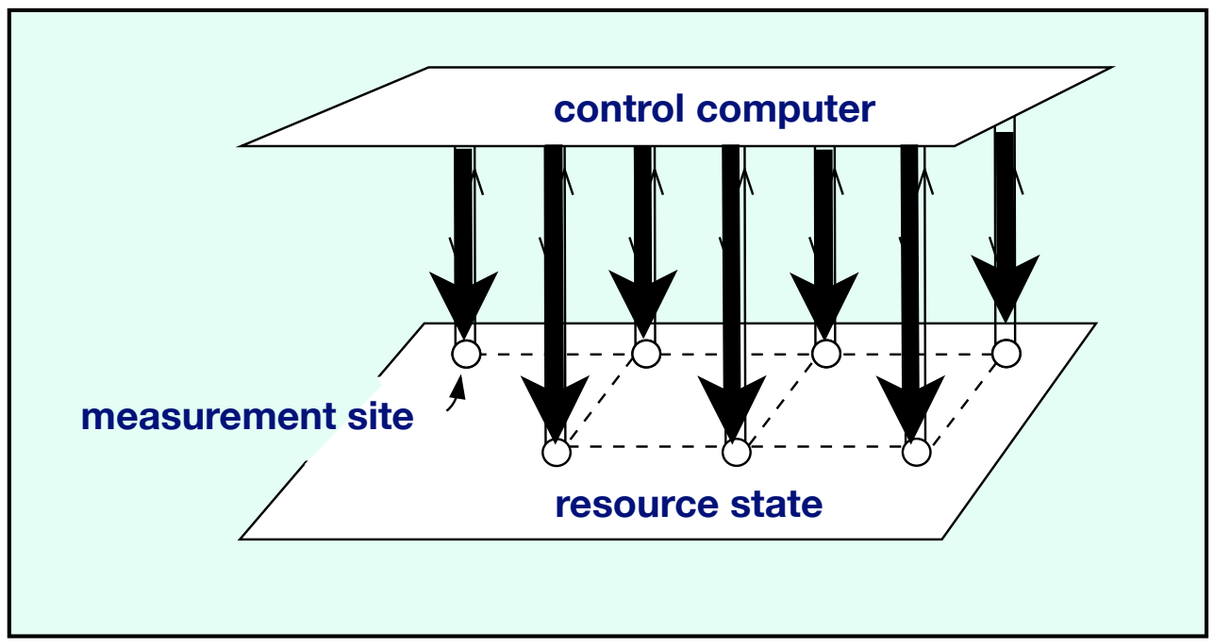
Implementation = Ask Minimum



$$\theta_1 = \theta_4 = 0$$

random single qubit generator → *random bell pair generator*

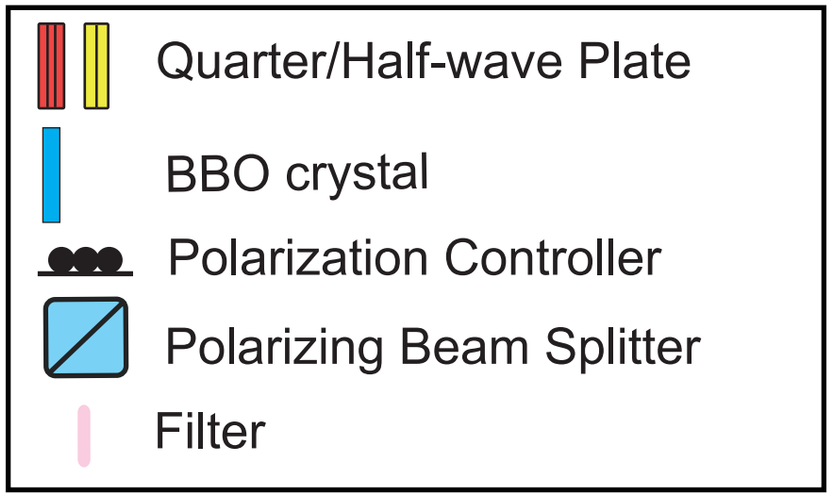
No Feed-Forward

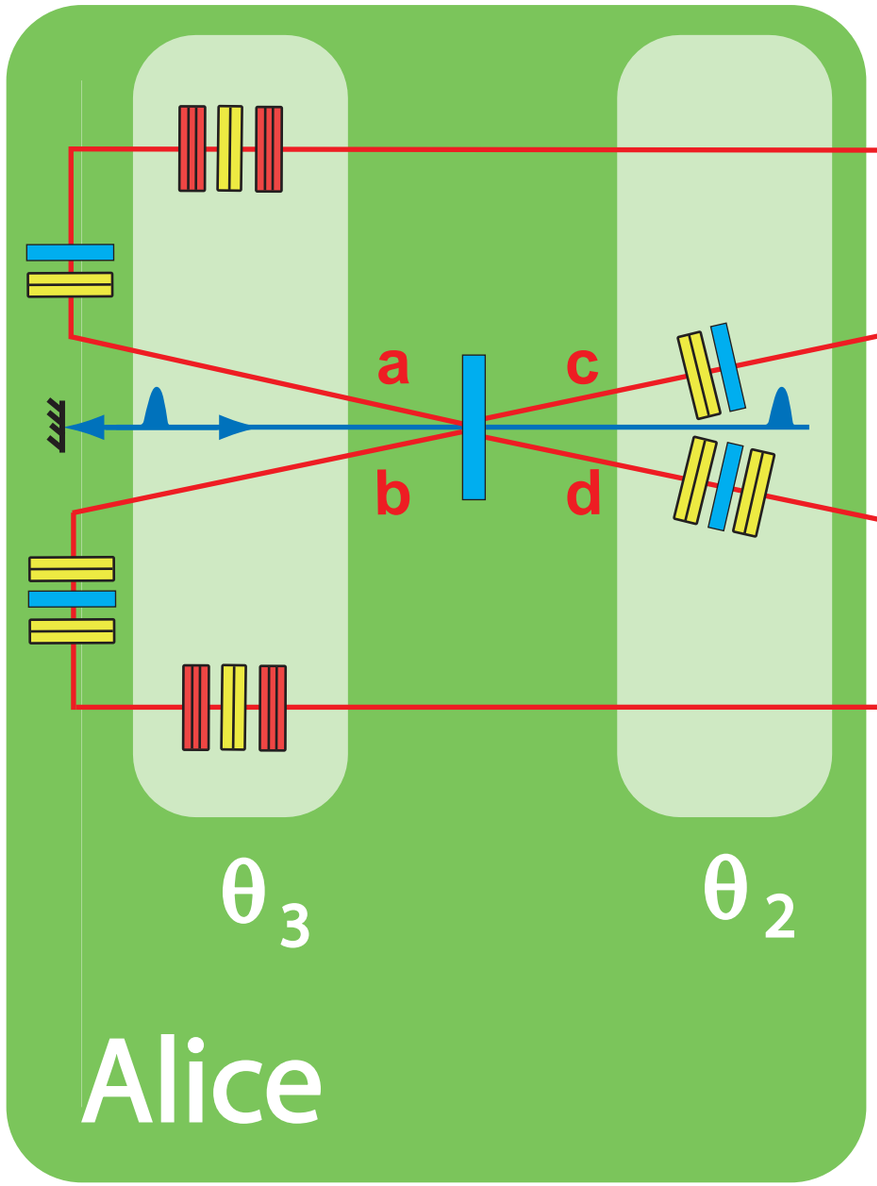


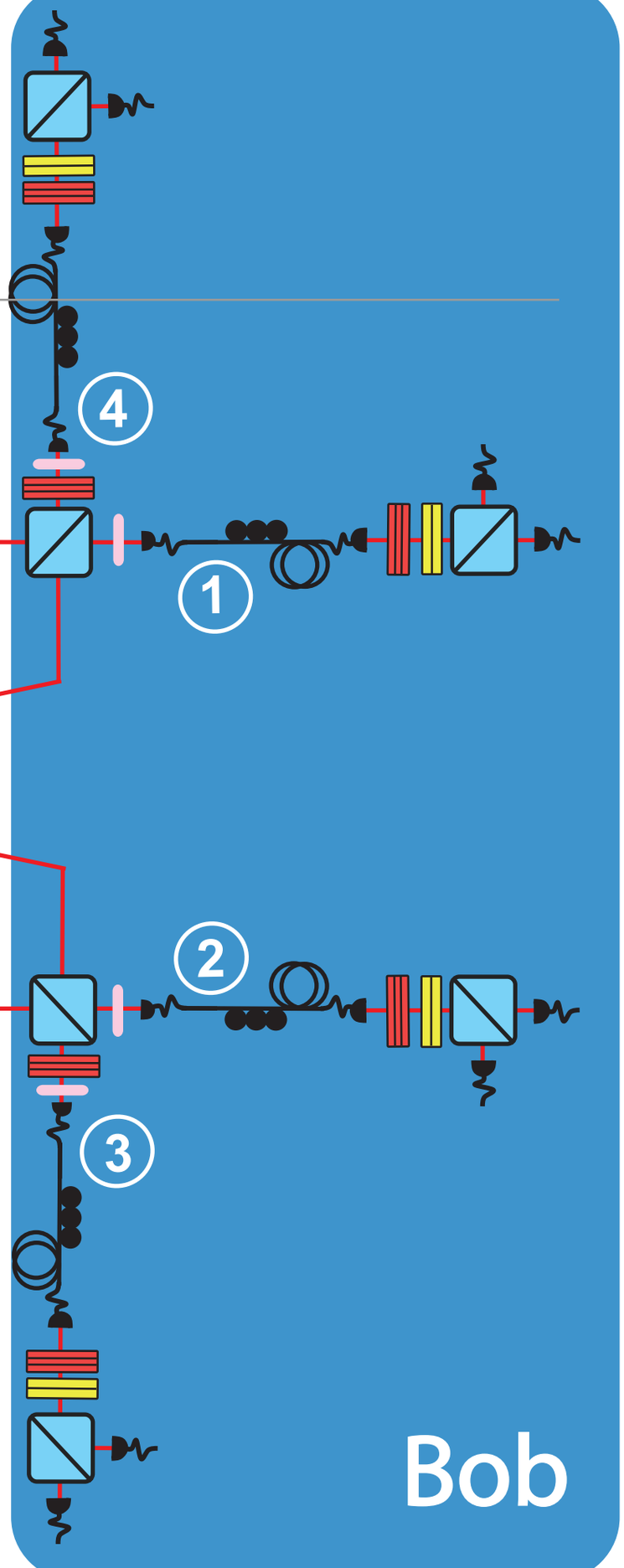
Theory = Justify Implementation

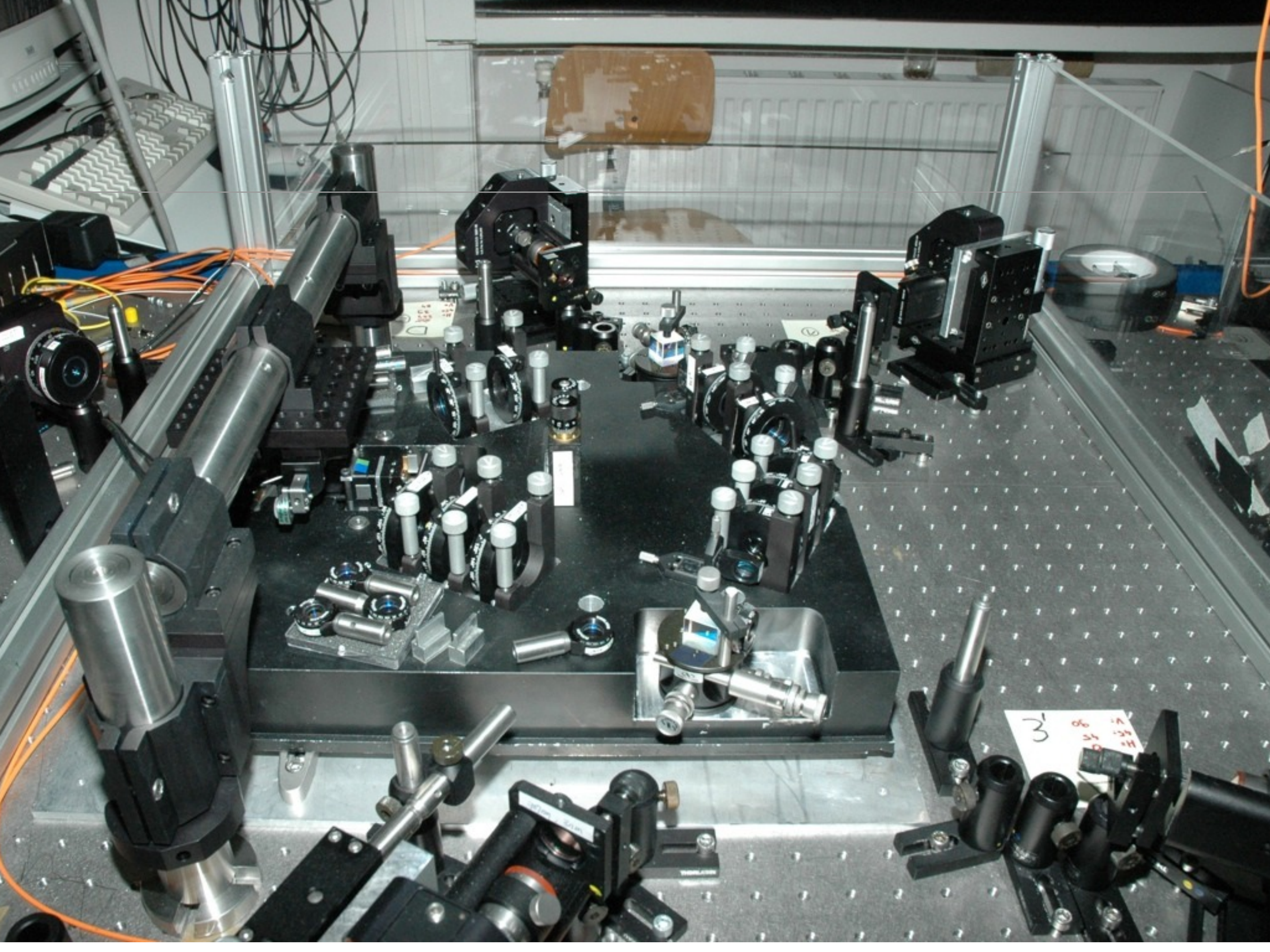
Theorem. The post-selected partially rotated Blind QC protocol is still blind.

Experimental Set-up









Experimental Set-up

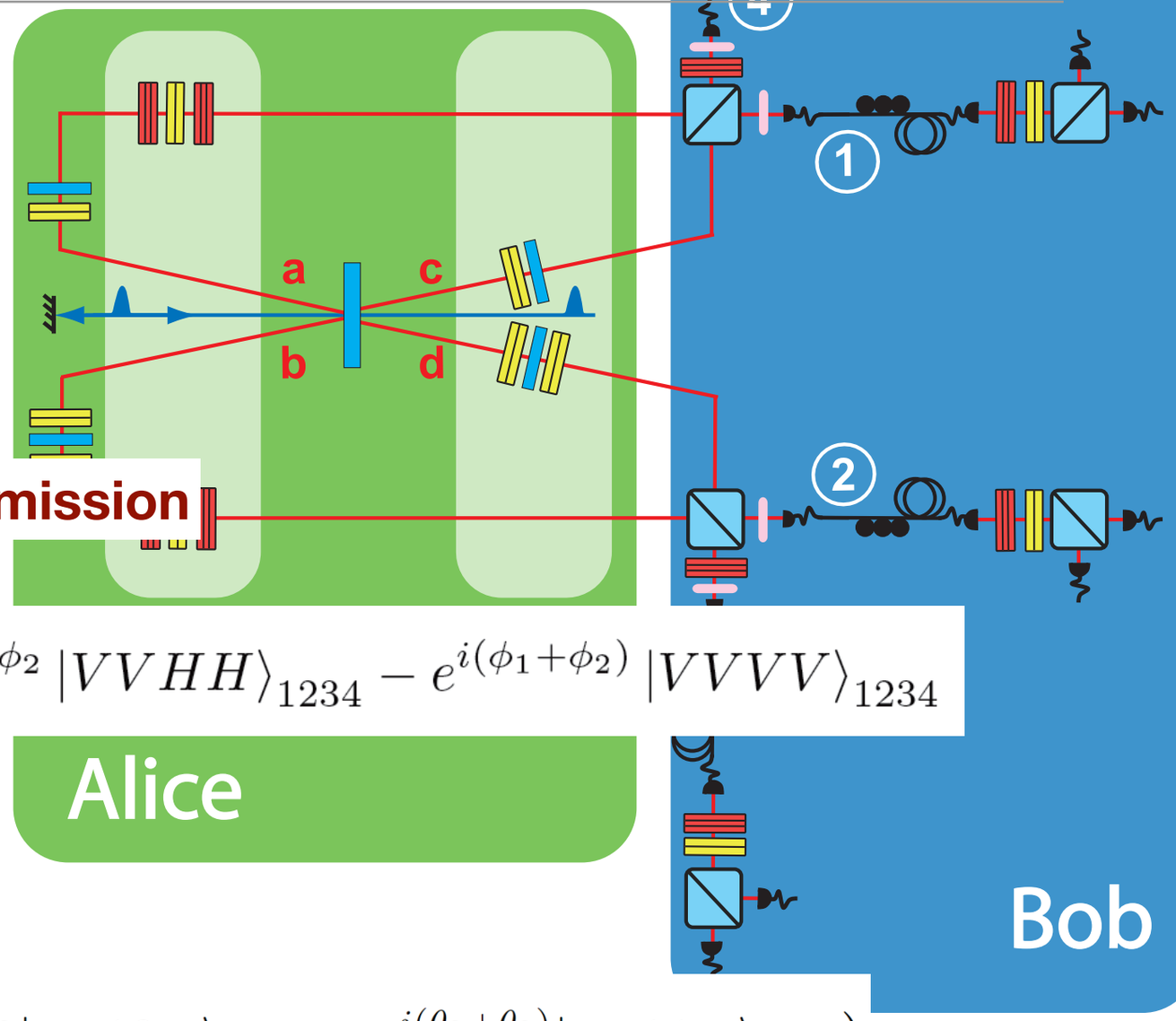
$$\left|\tilde{\phi}^{-}\right\rangle_{ab} = \frac{1}{\sqrt{2}}(|HH\rangle_{ab} - e^{i\phi_1}|VV\rangle_{ab})$$

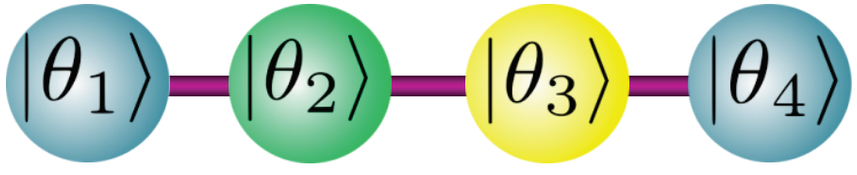
Post-selection 4-photons emission

$$|\mathrm{Lab}\rangle = |HHHH\rangle_{1234} + e^{i\phi_1}|HHVV\rangle_{1234} + e^{i\phi_2}|VVHH\rangle_{1234} - e^{i(\phi_1+\phi_2)}|VVVV\rangle_{1234}$$

Local Unitary

$$|\Phi^{\hat{\theta}}\rangle = \frac{1}{2}\left(|+00+\rangle_{1234} + e^{i\theta_3}|+01-\rangle_{1234} + e^{i\theta_2}|-10+\rangle_{1234} - e^{i(\theta_2+\theta_3)}|-11-\rangle_{1234}\right)$$

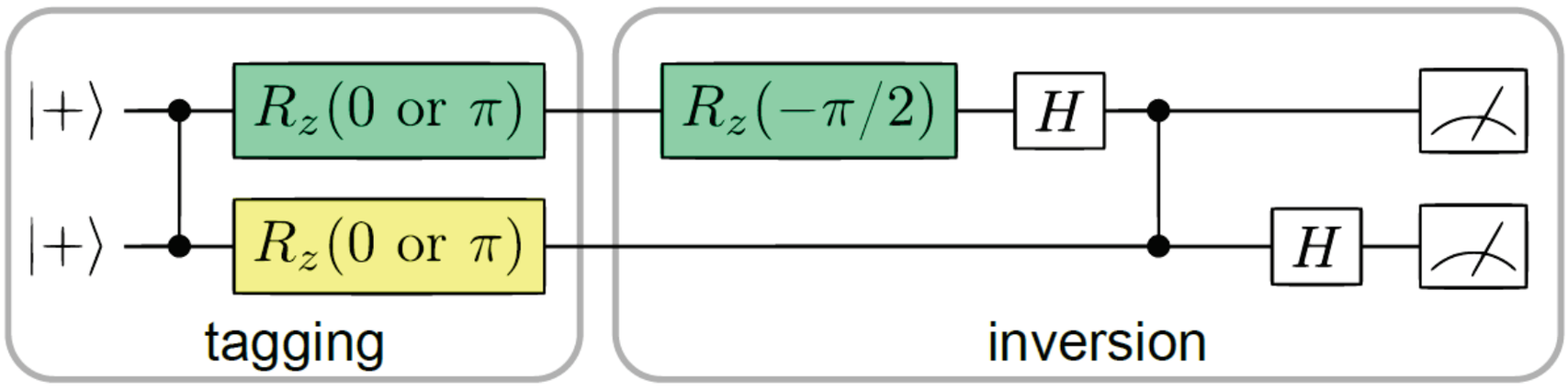




Blind Grover Algorithm

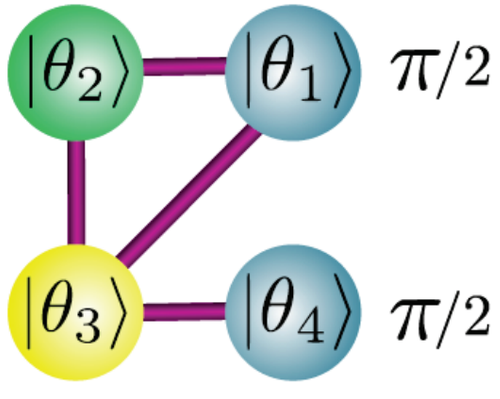
Given a function $f : \{0,1\}^n \rightarrow \{0,1\}$

Find an x such that $f(x) = 1$



$\delta_2 - \theta_2 - \pi r_2 \in \{\pm\pi/2\}$

$\delta_3 - \theta_3 - \pi r_3 \in \{0,\ \pi\}$

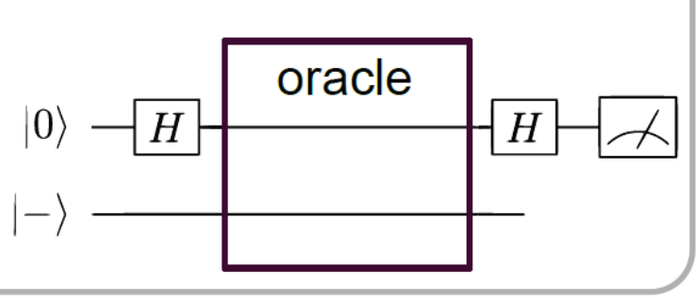


Blind Duetsch Algorithm

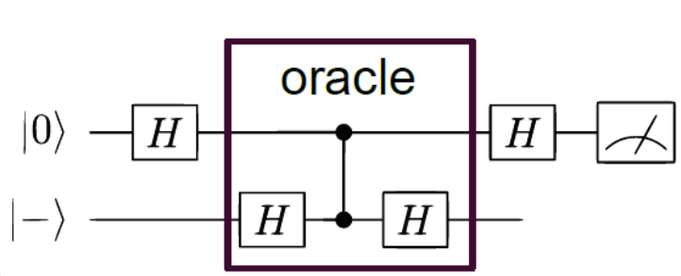
$$f : \{0,1\}^n \rightarrow \{0,1\}$$

Determine if function is constant or balanced

$f(0) = f(1) = 0$



$f(0) = 0, f(1) = 1$



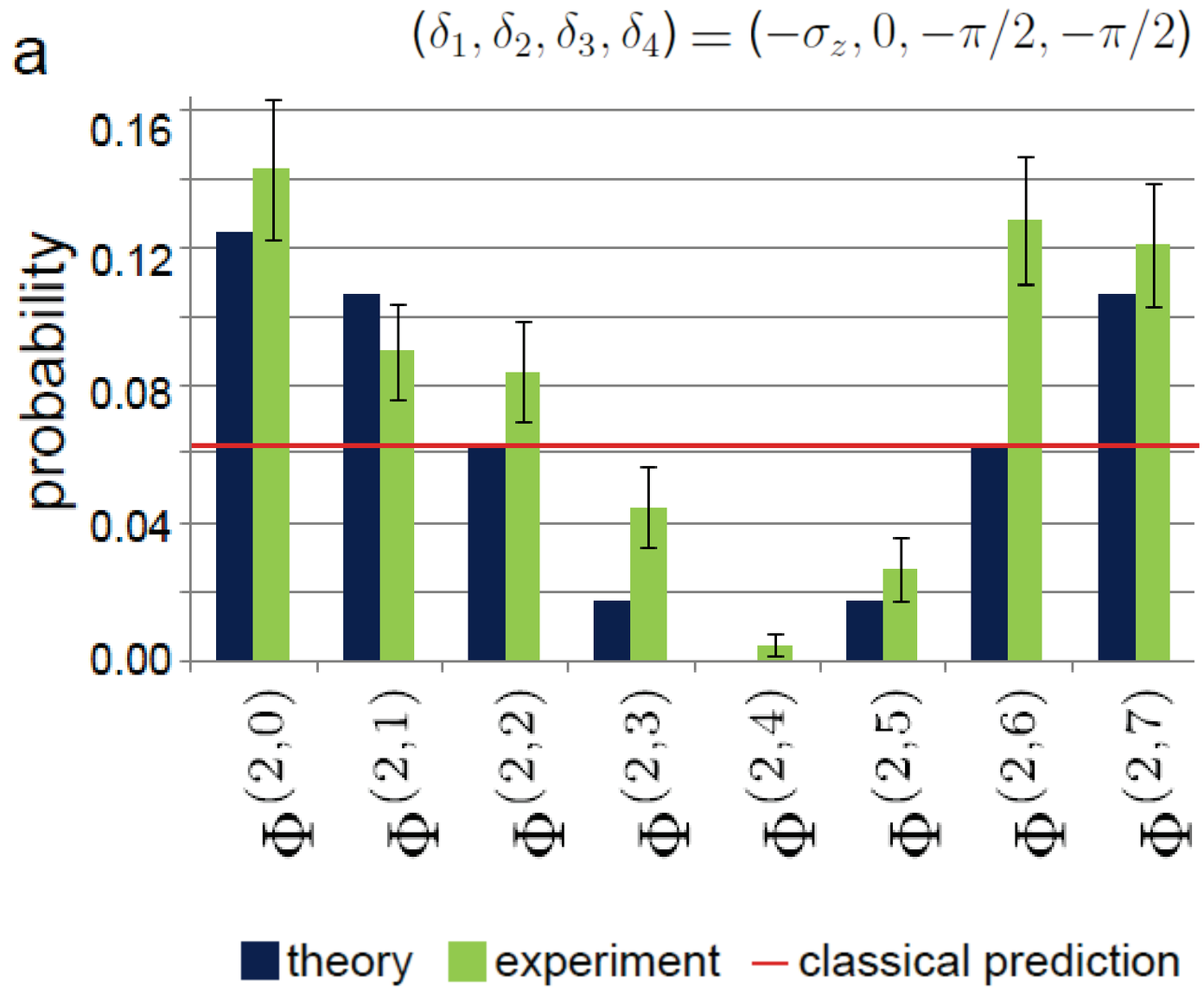
$\delta_3 - \theta_3 - \pi r_3 \in \{\pi,\ 0\}$ $|\theta_3\rangle$ $|\theta_4\rangle$ readout σ_z

π $|\theta_1\rangle$ $|\theta_2\rangle$ $\delta_2 - \theta_2 - \pi r_2 \in \{-\sigma_z,\ 0\}$

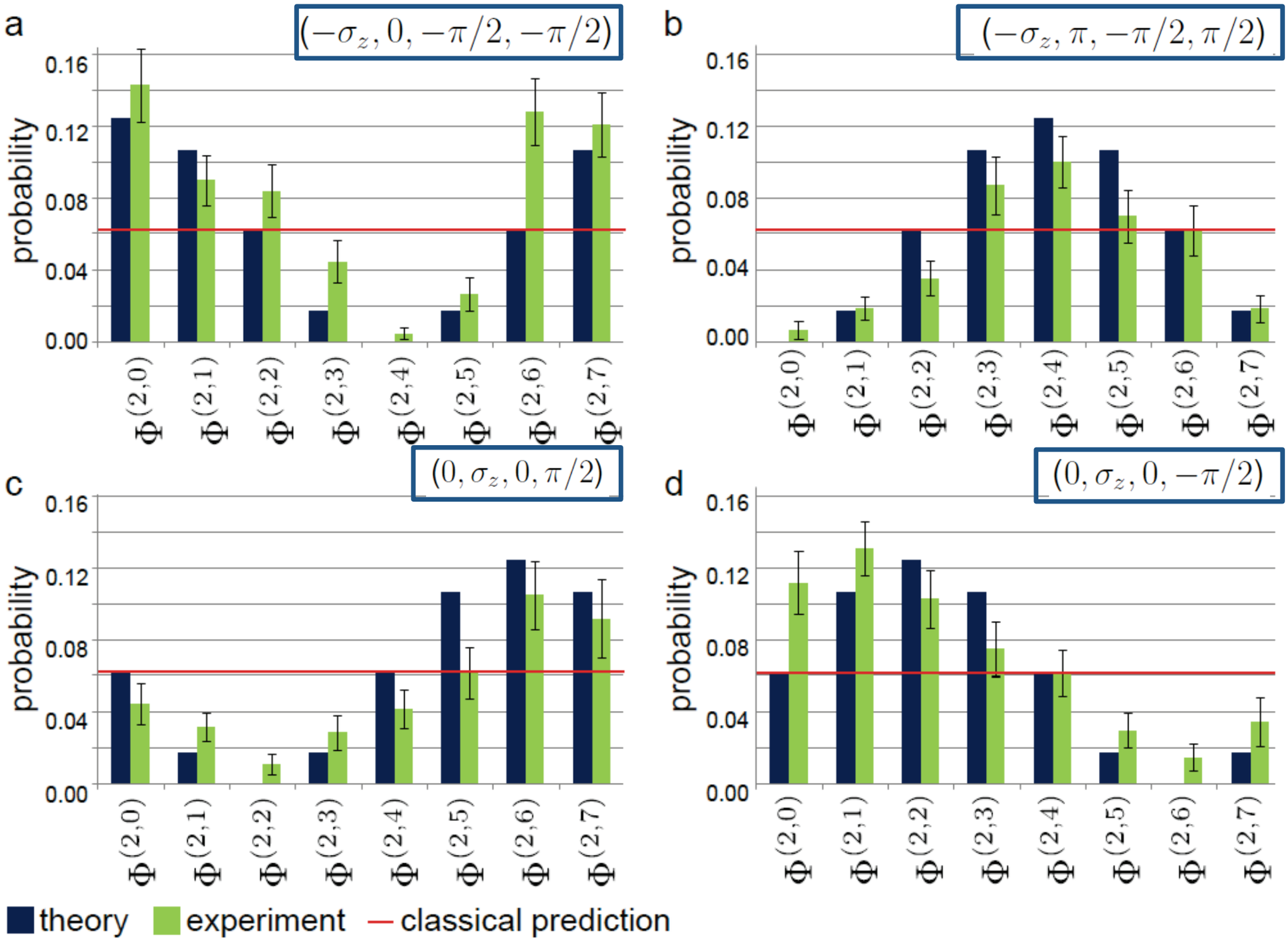
Testing the quantum server

Client can find out if the server possesses any quantum technology

- Measurement of the probability distributions for a fixed measurement setting
- Comparison with the theoretical expectations



Testing the quantum server



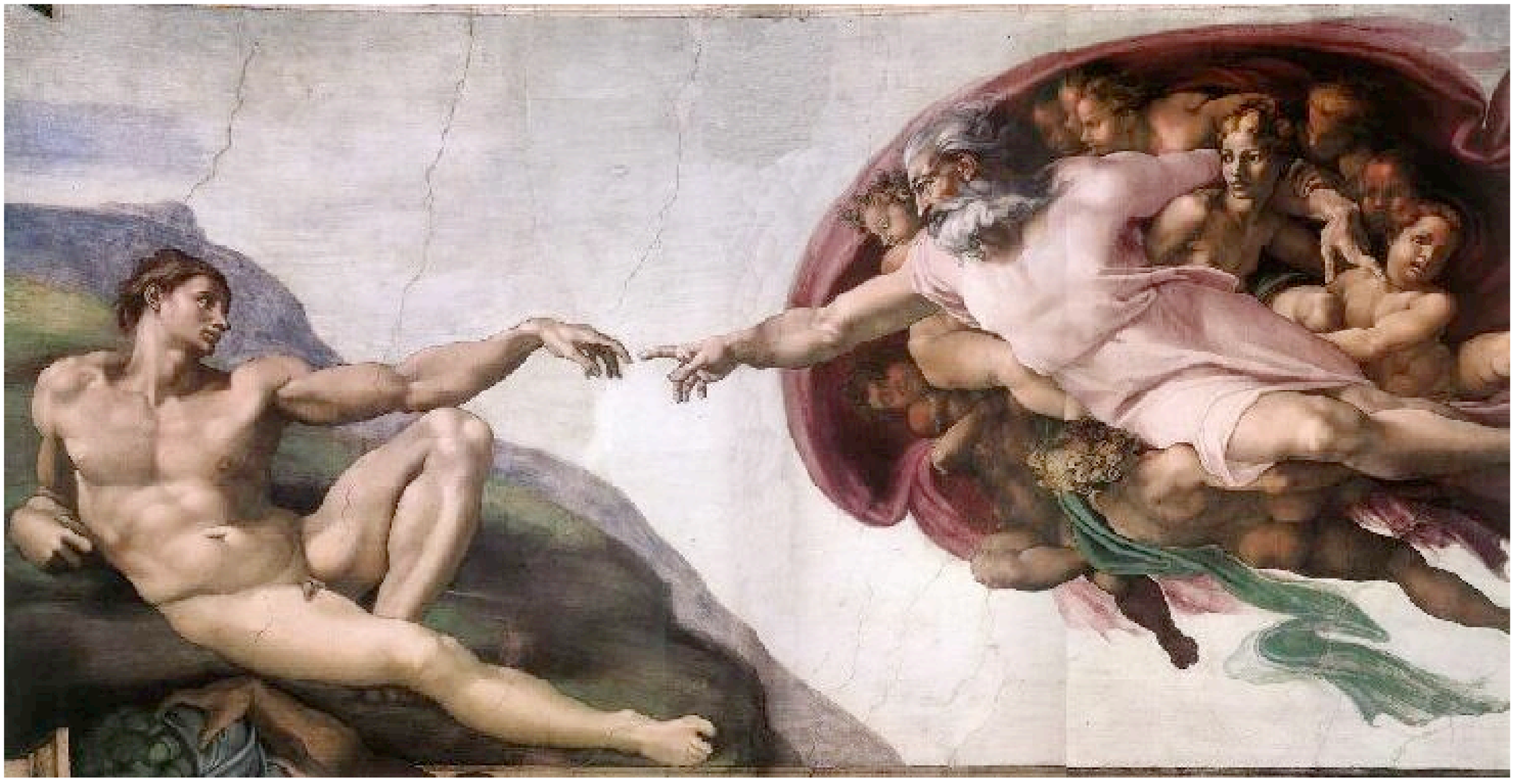
Real Stuff

Vazirani (07)

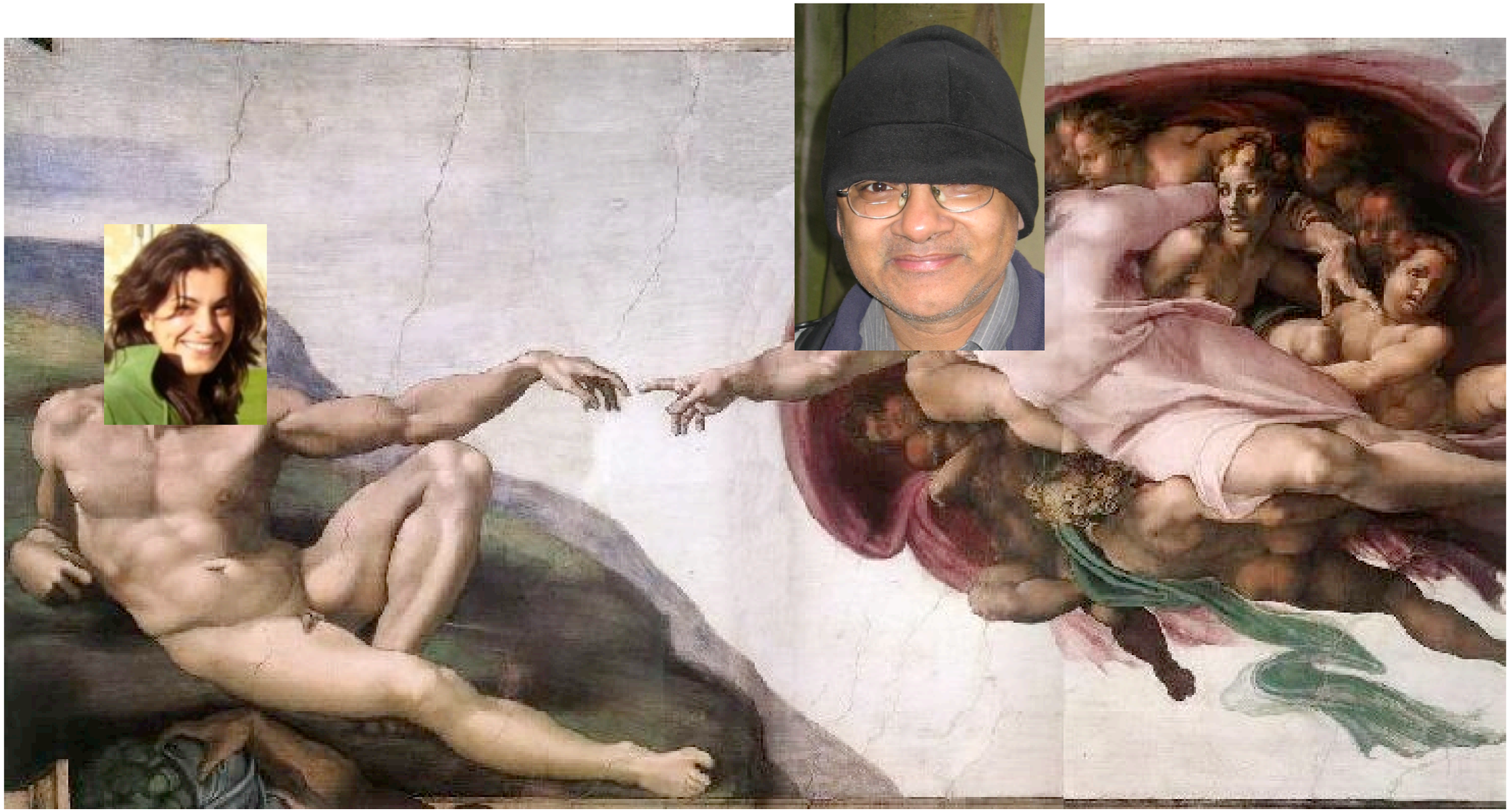
Can we test the validity of QM in the regime of exponential-dimension Hilbert Space?

Interactive Proofs

What can a computationally unbounded entity prove to a mere mortal (BPP)?



Asking help without trusting



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 =

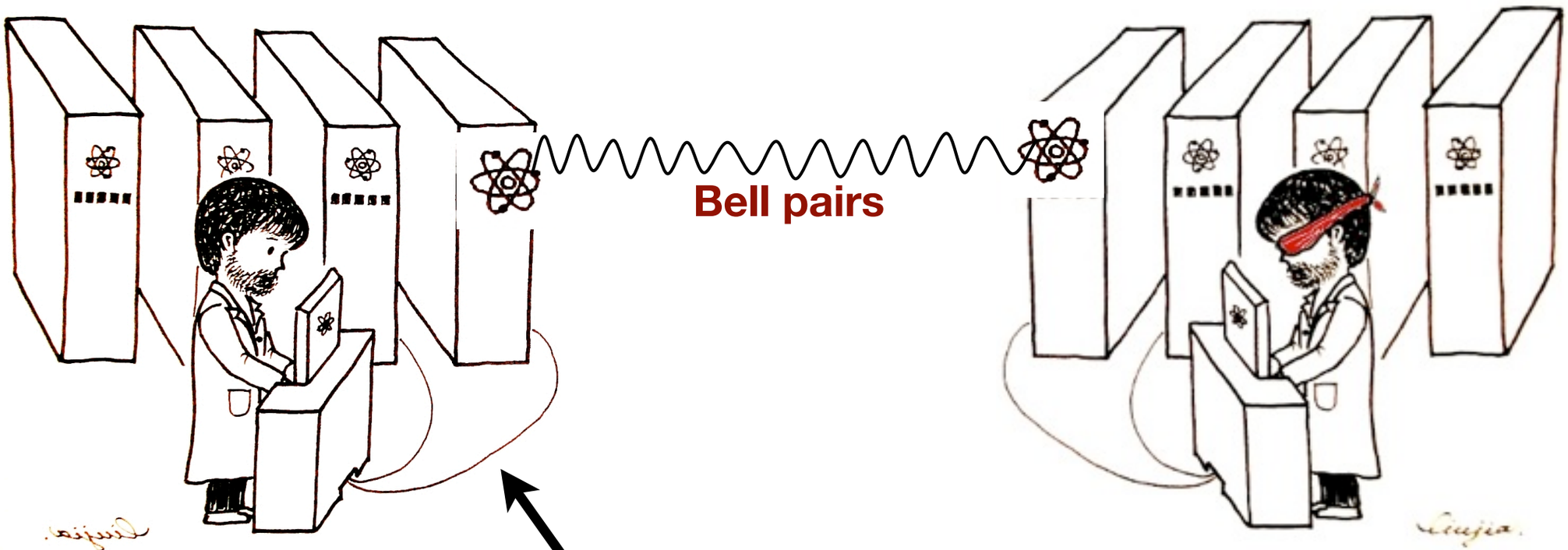
[Broadbent, Fitzsimons, Kashefi 2010]

Speculation

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

Entanglement = Quantum memory

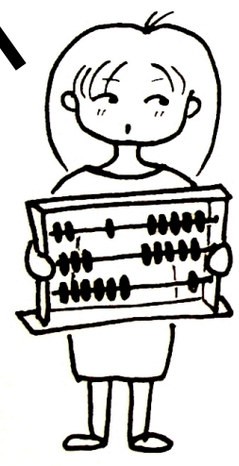
Interactive proof



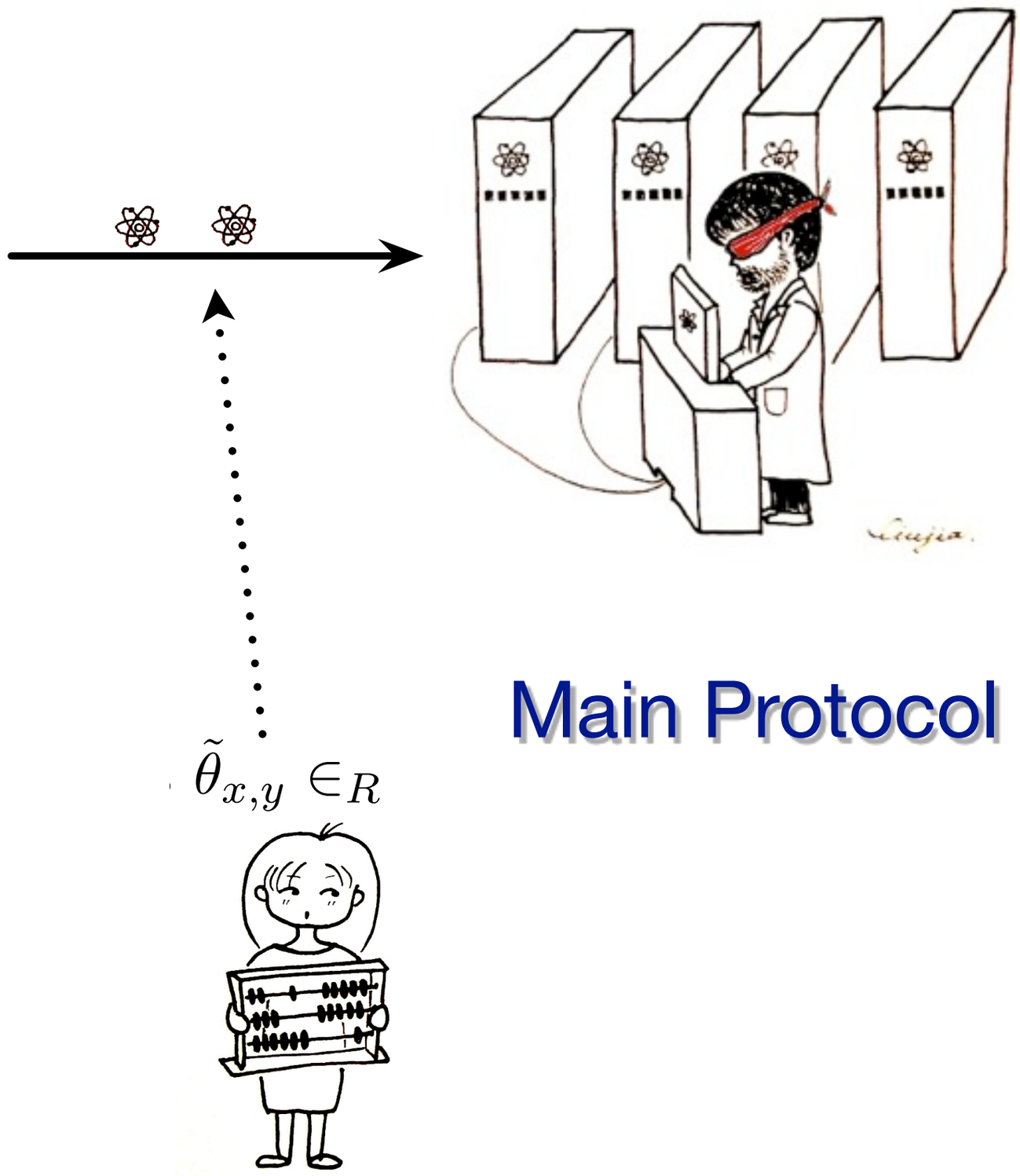
Measures his half of the Bell pair in $|\pm_{\tilde{\theta}_{x,y}}\rangle$.

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

$m_{x,y}$



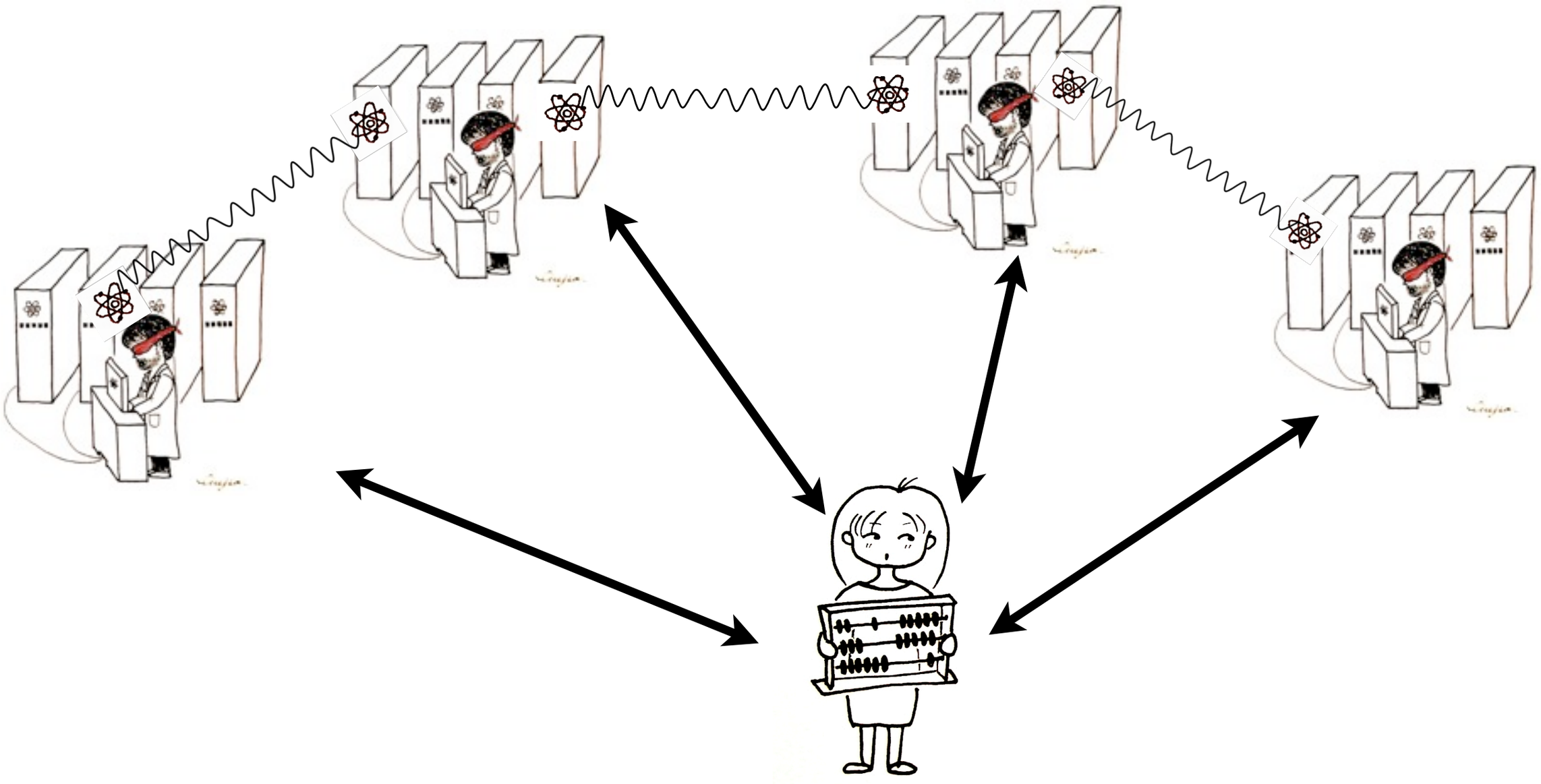
Interactive proof



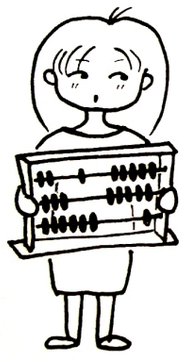
Main Protocol

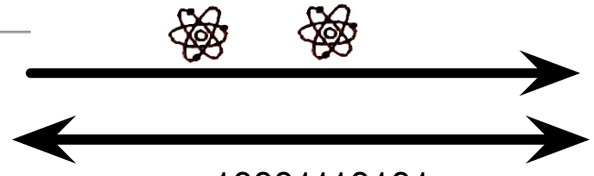
QMIP = MIP*

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.



Summary





Classical Compute

random single qubit generator

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

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

Detection of malicious Bob

Fault Tolerance

Perfect Privacy