Basics of quantum computing and some recent results

Tomoyuki Morimae
(YITP Kyoto University)
50+10 min

YUKAWA INSTITUTE FOR THEORETICAL PHYSICS

Outline

1. Basics of quantum computing
circuit model, classically simulatable/unsimulatable, quantum supremacy (15min)

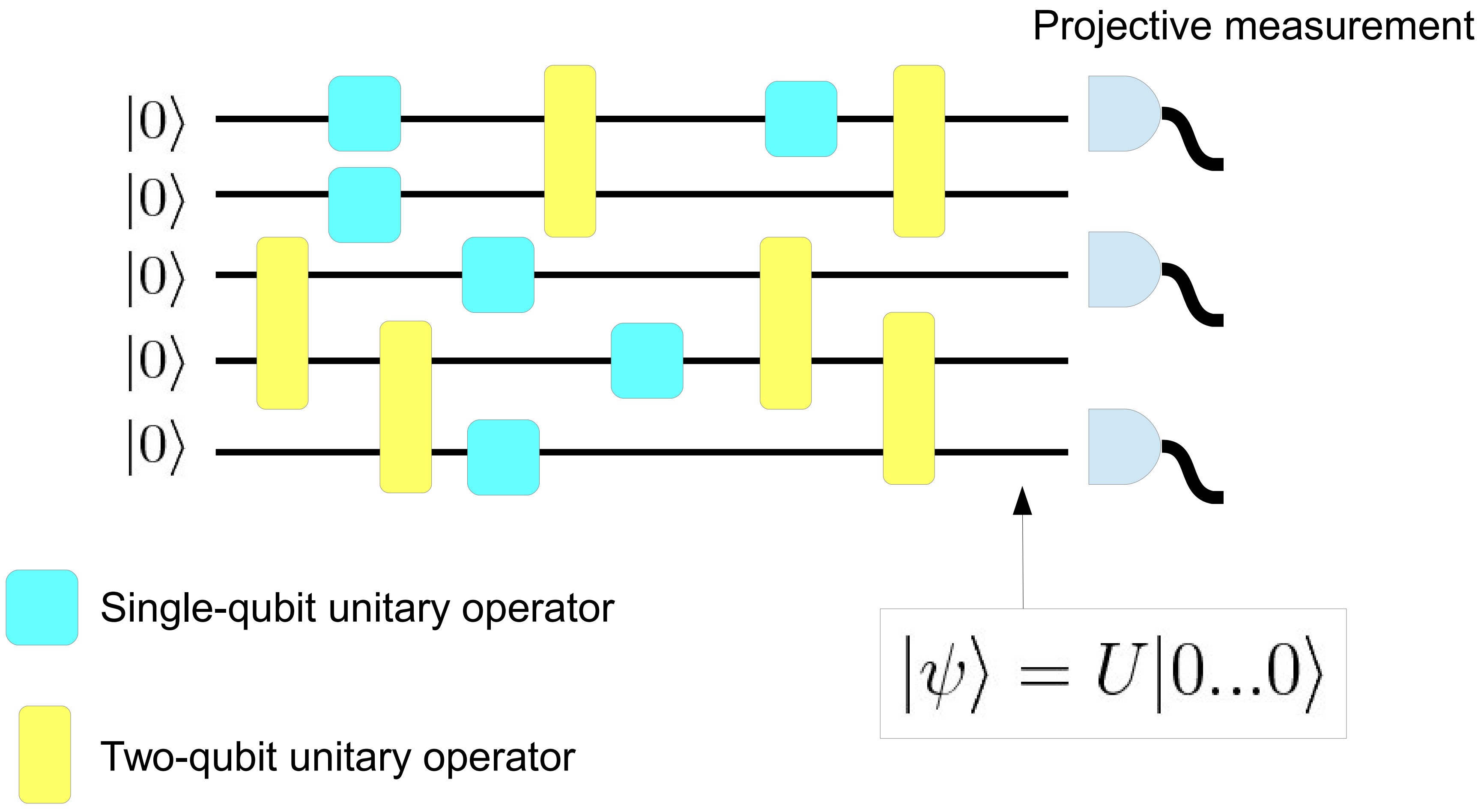
2. Measurement-based quantum computing
Tensor-network and quantum computing (15min)

3. Quantum interactive proof system, verification of quantum computing, blind quantum computing (20min)

4. Question (10min)

Basics of Quantum Computing

Circuit model

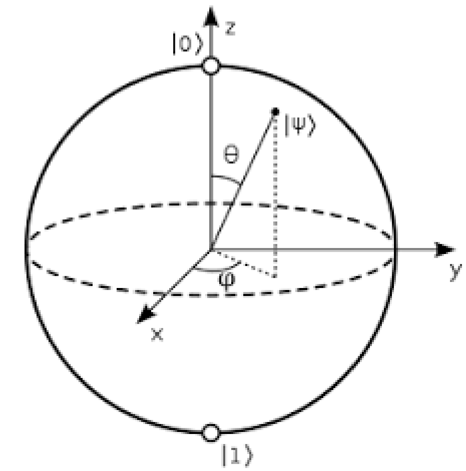


Universal gates

X-rotation + Z-rotation is single-qubit universal

$$e^{i\theta X}, e^{i\phi Z} \qquad e^{i\theta Z}, H$$

Hadamard H → basis changing



Single-qubit universal + any entangling two-qubit gate is n-qubit universal

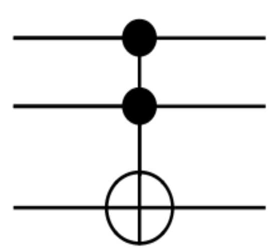
$$e^{i\theta Z_i \otimes Z_j}$$

$$CX = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

Hadamard + Toffoli = universal

Toffoli is classically universal
→ Hadamard has the quantum power



Important question

Which quantum circuits are classically simulatable? Which are not?

Simulatable 1: Clifford circuits

$H, diag(1,i), CZ$	Clifford gates

Quantum circuit that consists of only Clifford gates is classically simulatable
= Gottesman-Knill theorem

Clifford circuits can generate highly-entangled states...

GHZ state $|0^n\rangle + |1^n\rangle$

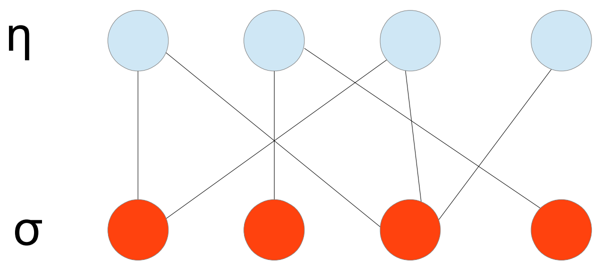
Graph state

States for QEC

Having strong entanglement is not enough for quantum speed up

Simulatable 2: Neural-network representation

$$|\psi\rangle = \sum_{\sigma} \psi(\sigma)|\sigma\rangle$$



$$\psi(\sigma) = \sum_{\eta} \frac{e^{-\beta H(\sigma,\eta)}}{Z}$$

Carleo and Troyer, Science 2017

Simulatable 3: Match gate circuit

Valiant 2001

$$e^{iH}, H = H_1 + H_2 + H_3$$
$$H_1 = \alpha_1 Z \otimes I + \beta_1 I \otimes Z$$
$$H_2 = \alpha_2 X \otimes X + \beta_2 Y \otimes Y$$
$$H_3 = \alpha_3 X \otimes Y + \beta_3 Y \otimes X$$

Jordan-Wigner transform

$$c_{2k-1} = Z_1 ... Z_{k-1} X_k I_{k+1} ... I_n$$
$$c_{2k} = Z_1 ... Z_{k-1} Y_k I_{k+1} ... I_n$$

Majonara fermion

$$H = \sum_{k,l} h_{k,l} c_k c_l$$

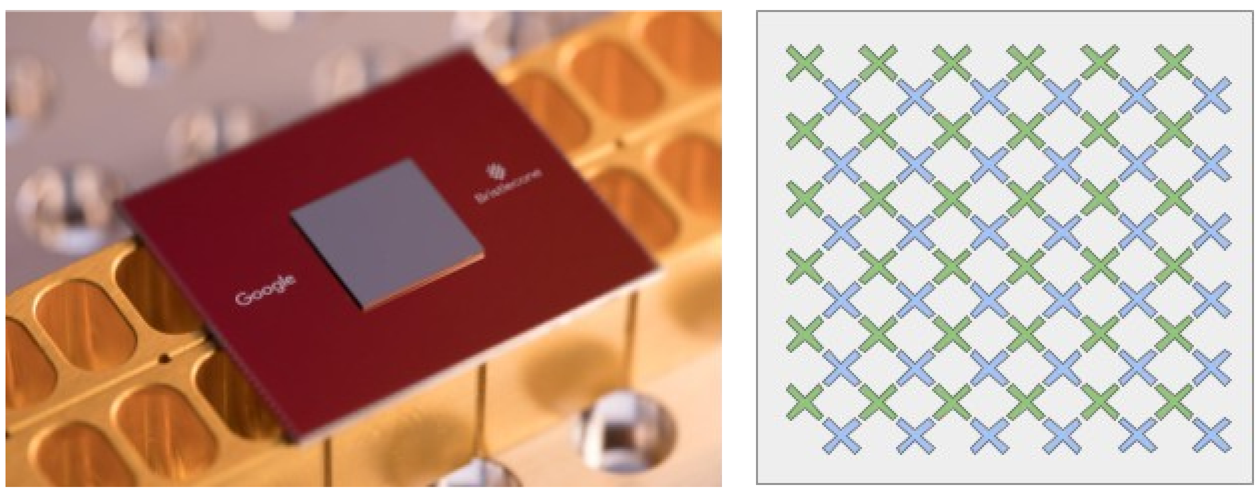
Quadratic form of Fermions → solvable!

We have seen several quantum circuits are classically simulatable.

Next question: which circuits are NOT classically simulatable?

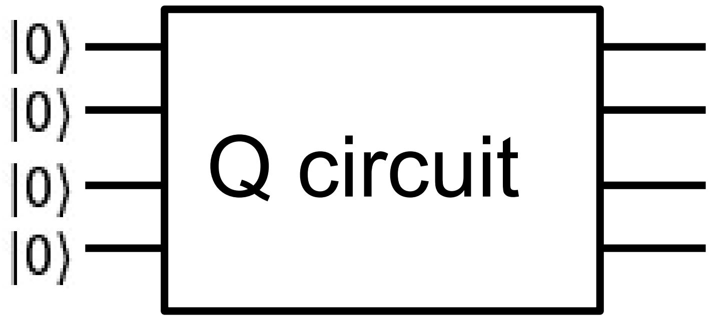
Universal QC → classically not simulatable
→ even non-universal weak QCs are faster than classical computing?

→ Important for quantum supremacy

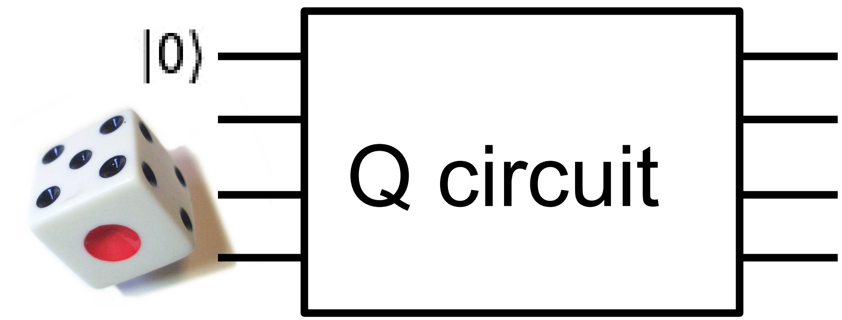


Google 72qubit quantum computer (this March APS)

One clean qubit model



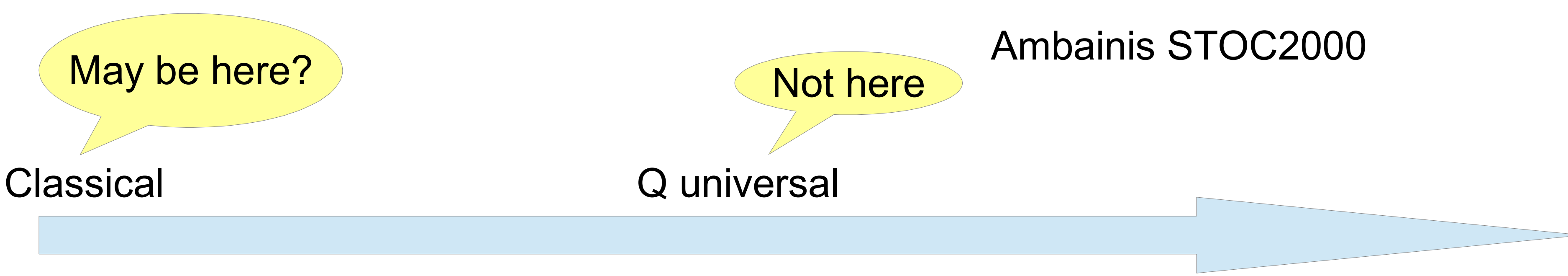
Usual QC



One clean qubit model

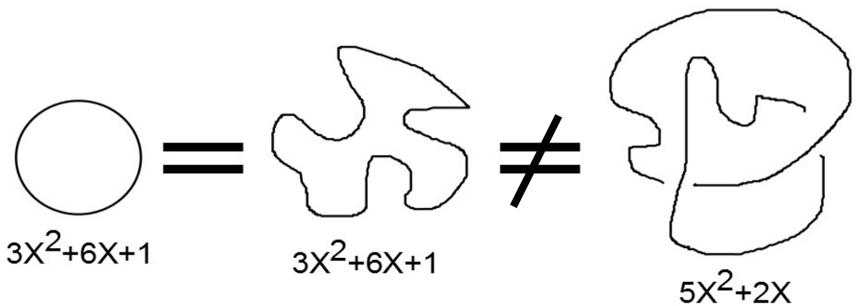
Model for NMR QC
Knill and Laflamme PRL1998

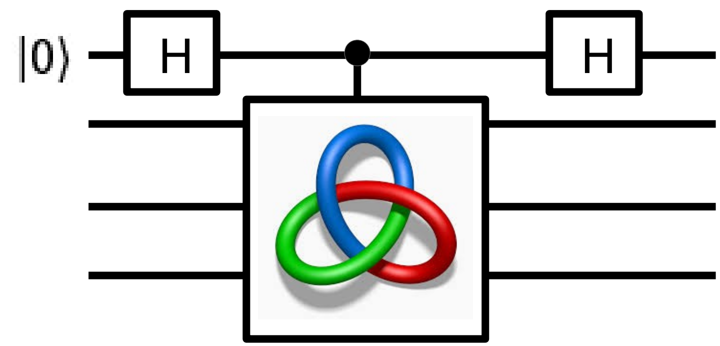
Ambainis STOC2000

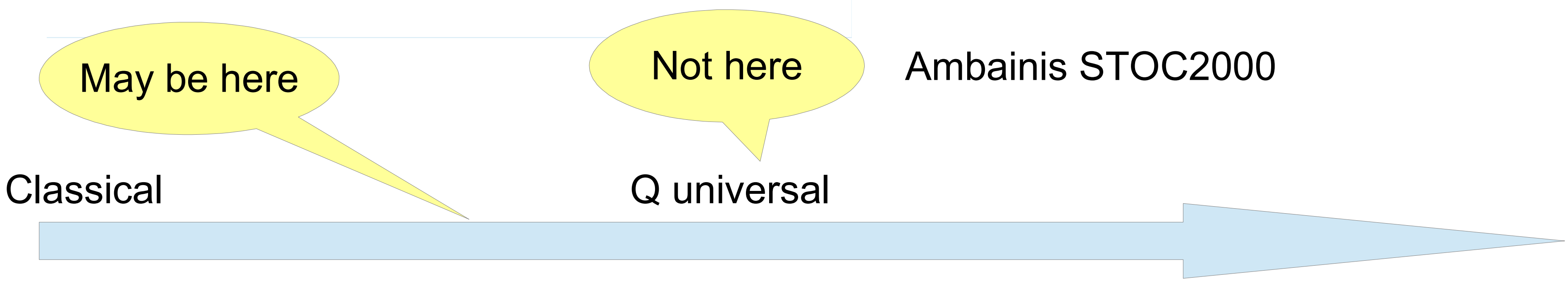


Ex: Jones polynomial

Classical: no efficient algorithm is known
One clean qubit model: poly-time algorithm (Shor and Jordan, QIC 2008)







Ambainis STOC2000

Not persuading:

A classical fast algorithm may be found in a future

c.f. Factoring: it can be in BPP since it is not believed to be NP-complete

Hardness of classically simulating one clean qubit model

If one clean qubit is classically simulated then PH collapses
[TM, Fujii, and Fitzsimons, PRL 112, 130502 (2014); TM, PRA(R)2017]

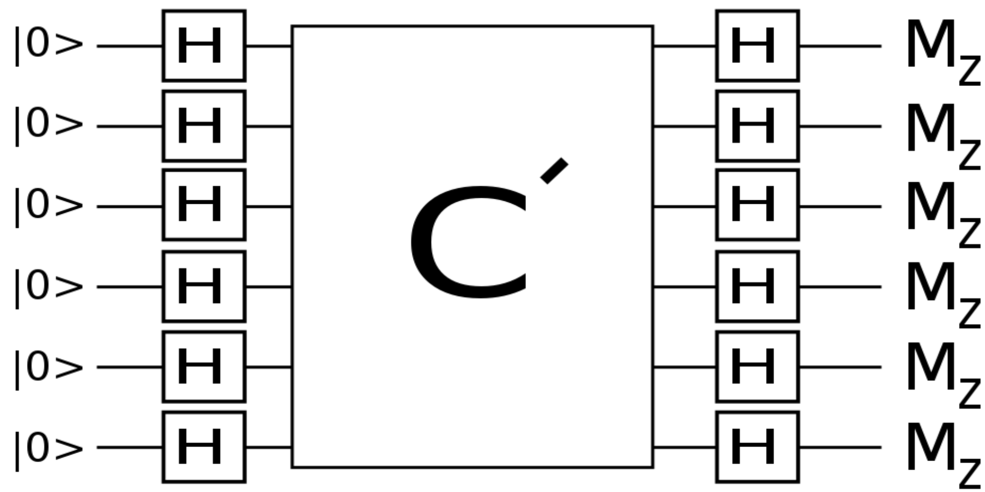
Polynomial hierarchy

$$\mathrm{P} \subset \mathrm{NP} \subset \mathrm{NP}^{\mathrm{NP}} \subset \mathrm{NP}^{\mathrm{NP}^{\mathrm{NP}}} \subset \ldots$$

Collapse of PH is not believed to happen

→ one-clean qubit model cannot be simulated classically

IQP(Instantaneous Quantum Polytime)



C' : Z-diagonal gate, such as Z、CZ、CCZ、exp(iZΘ)

IQP is closely related to Ising partition function [Fujii and TM, NJP2016]

IQP is not universal, but its classical simulation leads to the collapse of PH
[Bremner, et. al. Proc. Roy. Soc. 2010]

Summary

1. Some circuits are classically simulatable

Clifford circuits
Neural network states
Match gate circuits

→ Efficient numerical algorithm for cond-mat and stat phys?

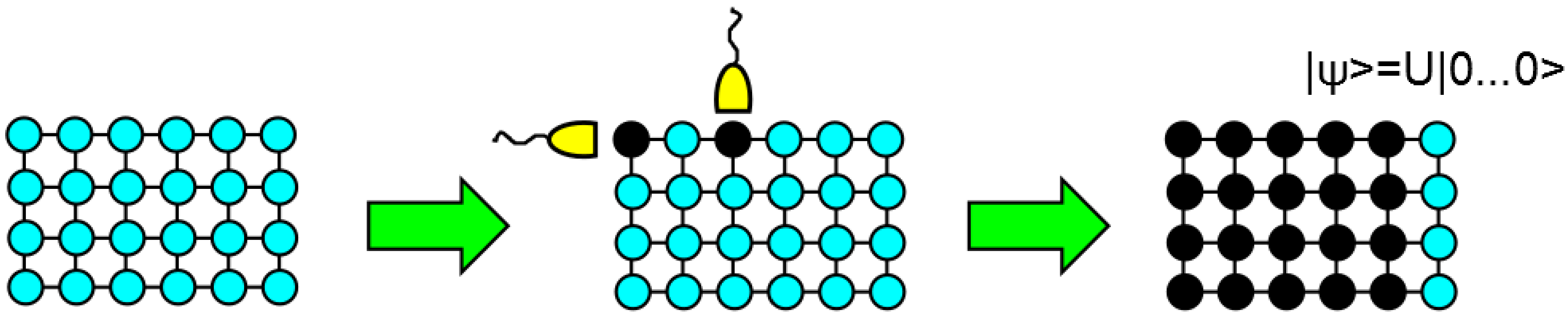
2. Some circuits exhibit quantum supremacy

→ Near-term realization of QC
→ Foundation of quantum physics: clarifies the boarder between Q and C

Measurement-based quantum computing

Measurement-based quantum computing

(Raussendorf and Briegel, PRL 2001)



Generate a many-qubit state

Measure each qubit

The state is generated!

|ψ> is generated → quantum computing is done!

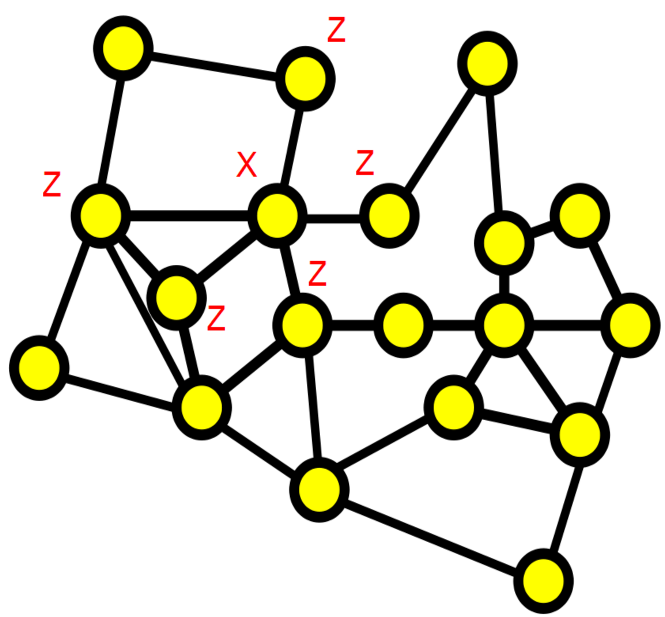
Why we can generate it? → intuitive idea: disturbance

The initial state is indepent of |ψ> → existance of universal resource state

Cluster state (graph state)

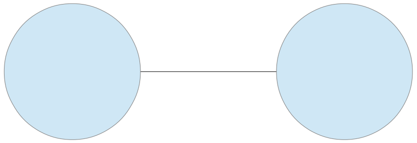
Definition 1: CZ|++...+>

Definition 2: Stabilized by commuting $K_i = X_i \bigotimes_{j \in N_i} Z_j$

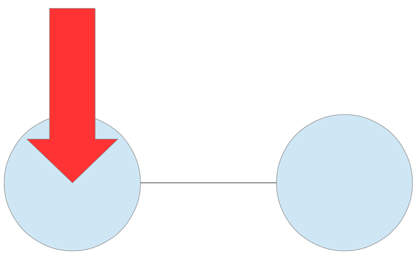


[Raussendorf and Briegel, PRL 2001]

How MBQC work



$$CZ(|+\rangle|+\rangle) = CZ(|0\rangle|+\rangle + |1\rangle|+\rangle) = |0\rangle|+\rangle + |1\rangle|-\rangle$$

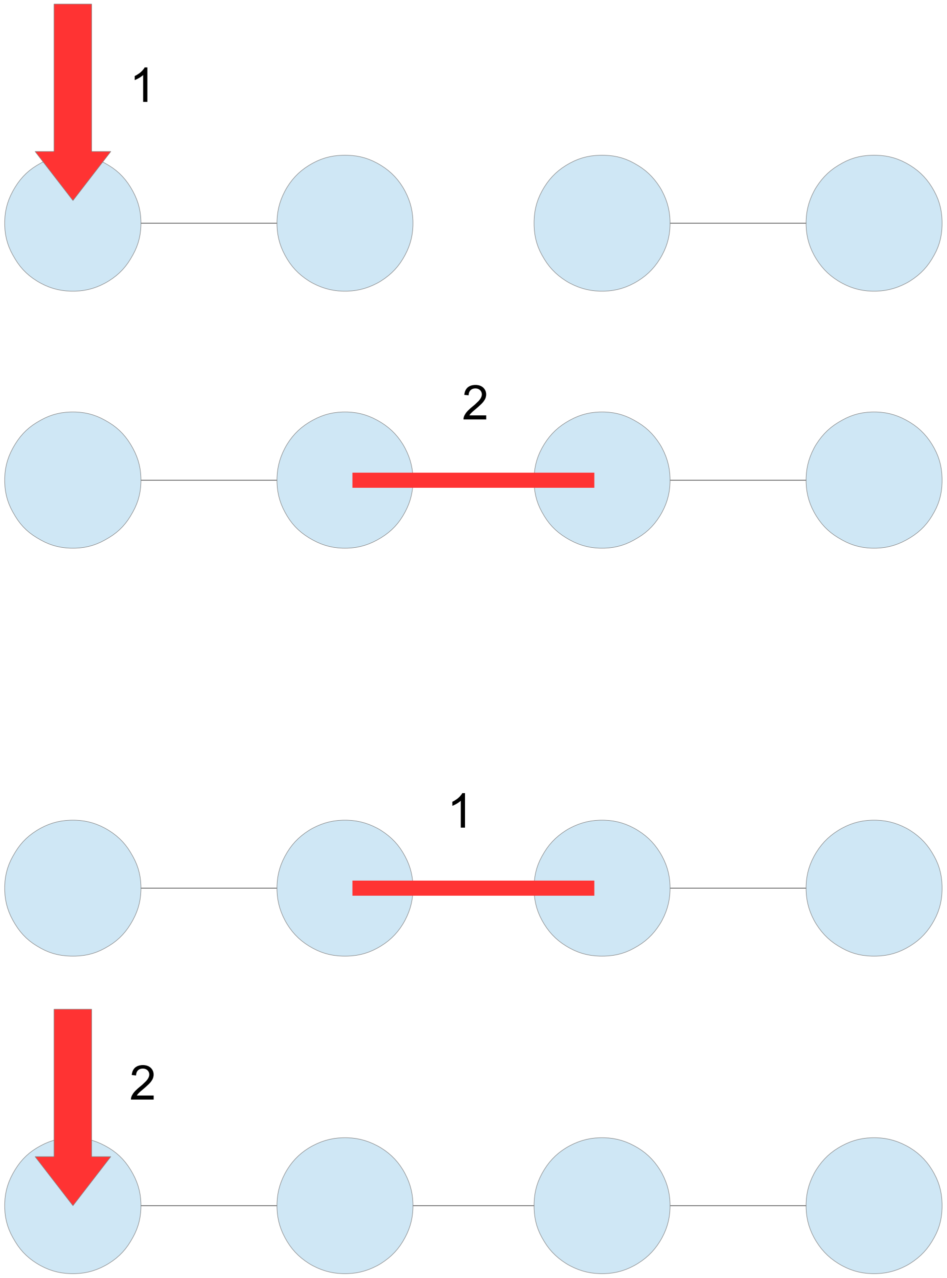


$$|0\rangle \pm e^{-i\theta}|1\rangle$$

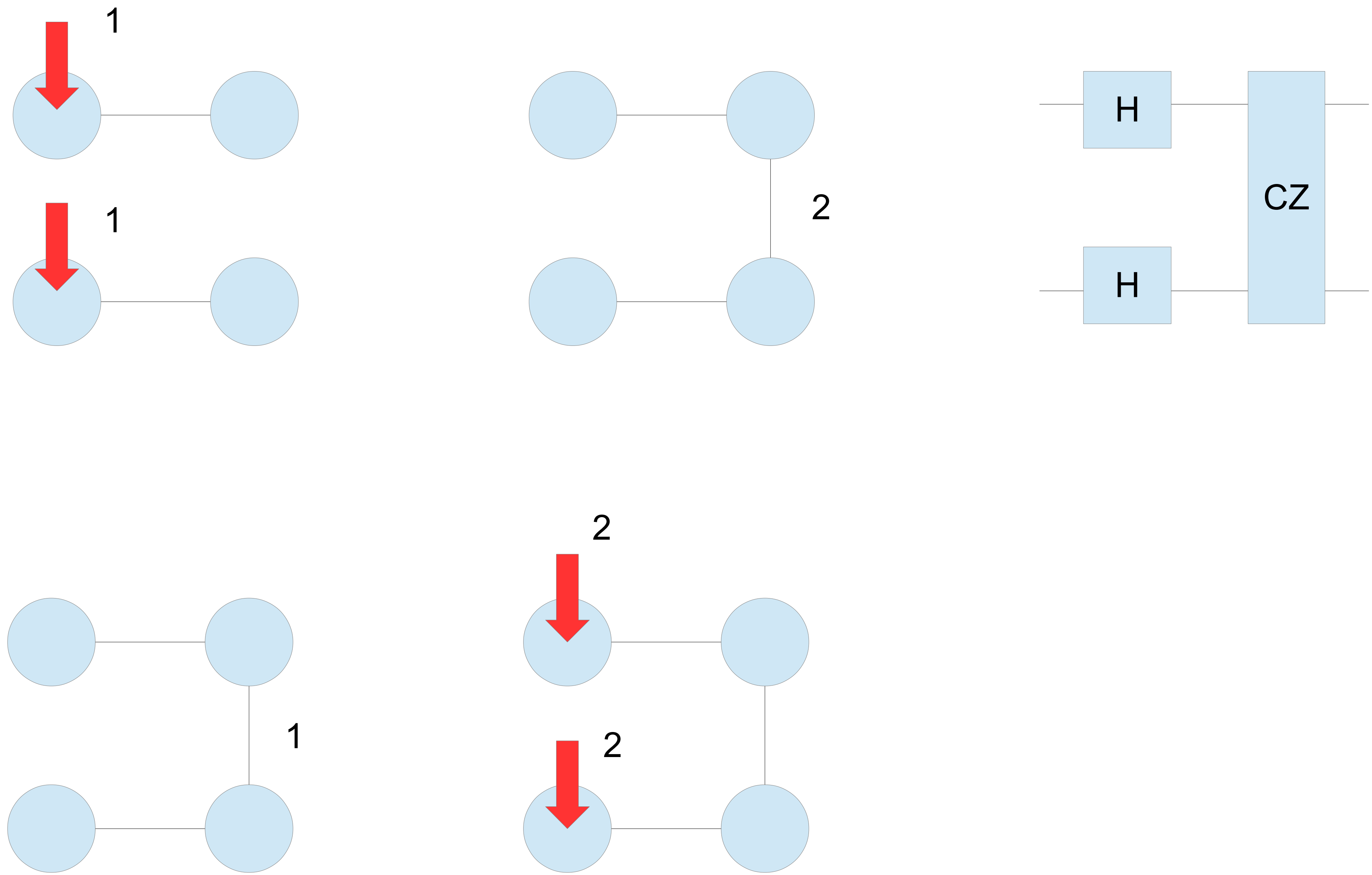
$$|0\rangle|+\rangle + |1\rangle|-\rangle \rightarrow |+\rangle \pm e^{i\theta}|-\rangle = He^{i\theta Z/2}|+\rangle$$

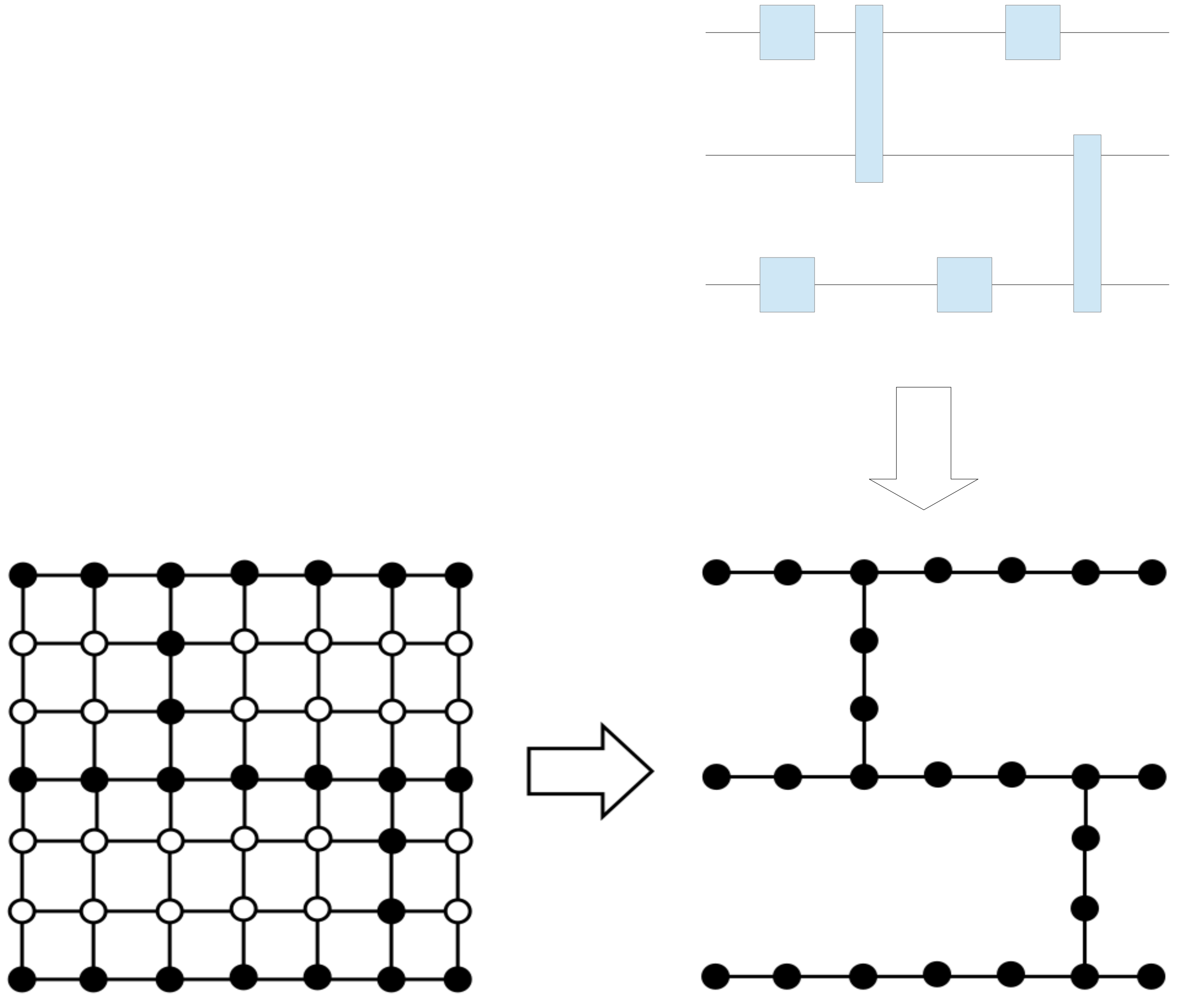
$J(\theta) \equiv He^{i\theta Z}$ is universal

$$J(0)J(\theta) = e^{i\theta Z}, J(\theta)J(0) = e^{i\theta X}$$



One-dimensional cluster state is single qubit unviersal

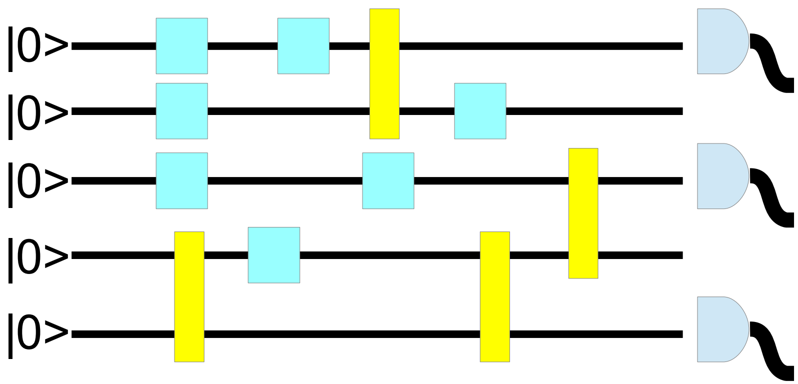

1
1
2
H
H
CZ
1
2
2

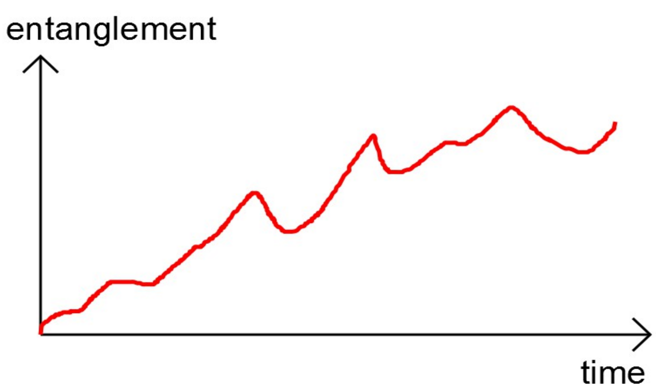


2D-square graph state is universal

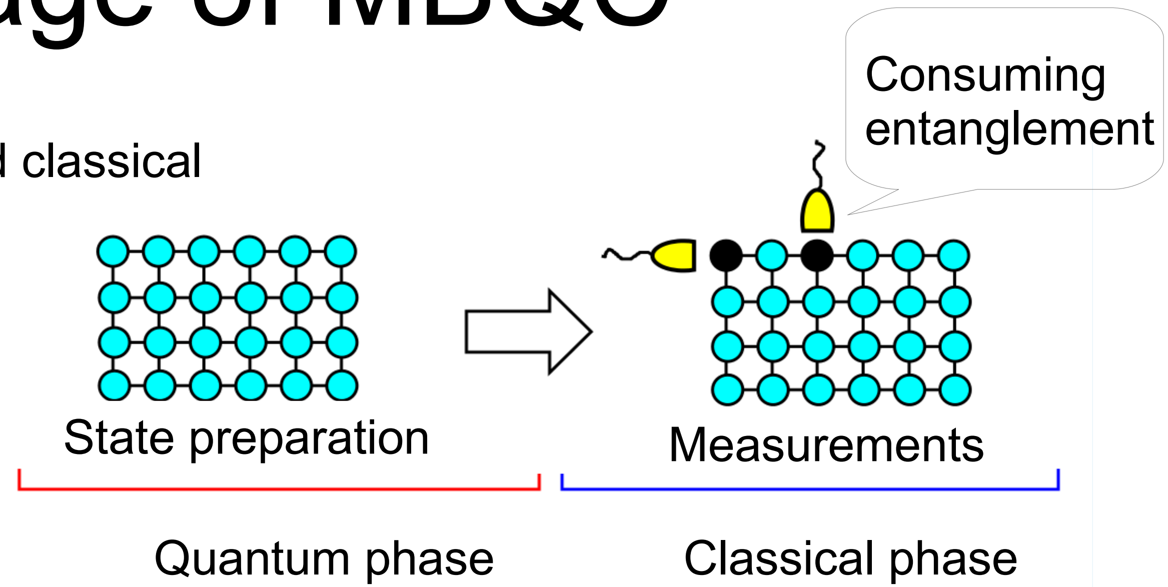
Advantage of MBQC

Clear separation between quantum and classical

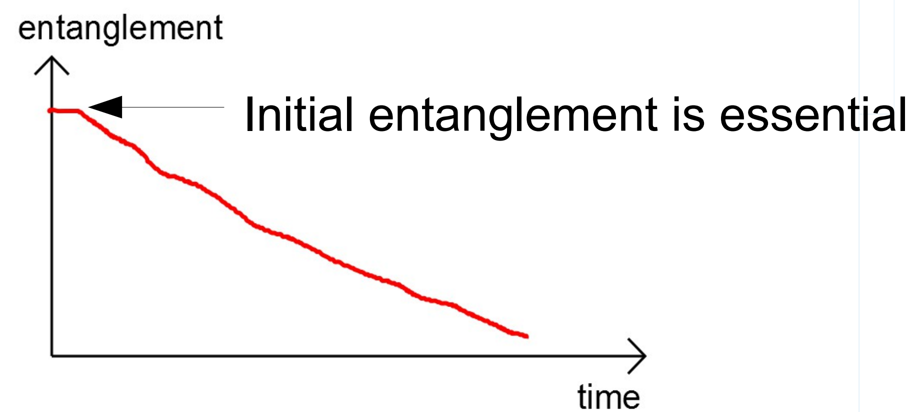




Which entanglement is essential?



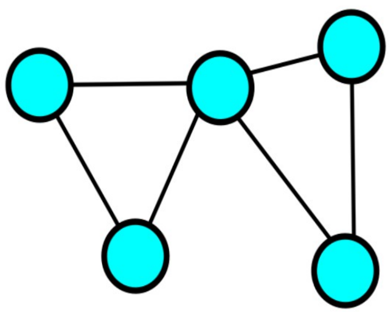
Classical vs quantum is clear!



MBQC and Ising partition function

An interesting relation between MBQC and Ising partition function

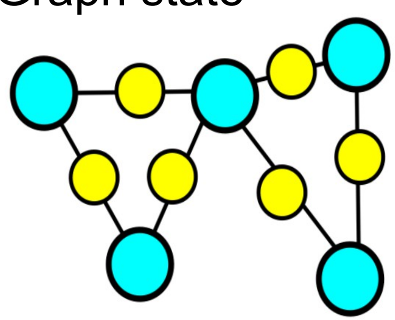
Classical Ising model



$$H = J \sum_{<i,j>} \sigma_i^z \sigma_j^z + \sum_j h_j \sigma_j^z$$

$$Z_\beta = |\langle \phi | C \rangle|^2$$

Graph state



$$|\phi\rangle = \bigotimes_{j=1}^{n} |\phi_j(\beta, J, h_j)\rangle$$

Classical statistical physics

Solvable, NP-hard....

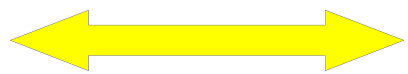
Quantum computing

Classically simulatable, universal....

(Bravyi and Raussendorf, PRA 2007)
(Nest, et. al. PRL 2007)
(Fujii and TM, NJP2016)

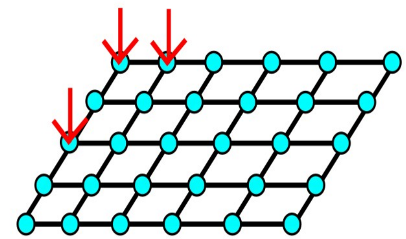
Quantum subroutine

Another interpretation of measurement-based QC



Subroutine

Measurement



Classical computer
（only XOR gate）

Quantum many-body system
（resource state）

Classical XOR + graph state = quantum universal

XOR＋GHZ＝classical universal [Anders and Browne, PRL2009]

XOR gate

0 0 → 0
0 1 → 1
1 0 → 1
1 1 → 0

Tensor network and measurement-based quantum computing

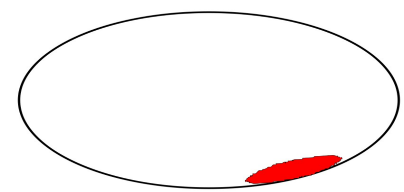
Matrix-product state

N-qubit state

$$|\psi\rangle = \sum_{z_1=0}^{1} \cdots \sum_{z_N=0}^{1} c(z_1,\ldots,z_N)|z_1 \ldots z_N\rangle$$

Exponentially many parameters have to be specified → numerical simulation is hard

Only small corner of the huge Hilbert space is of interest



Matrix-product state

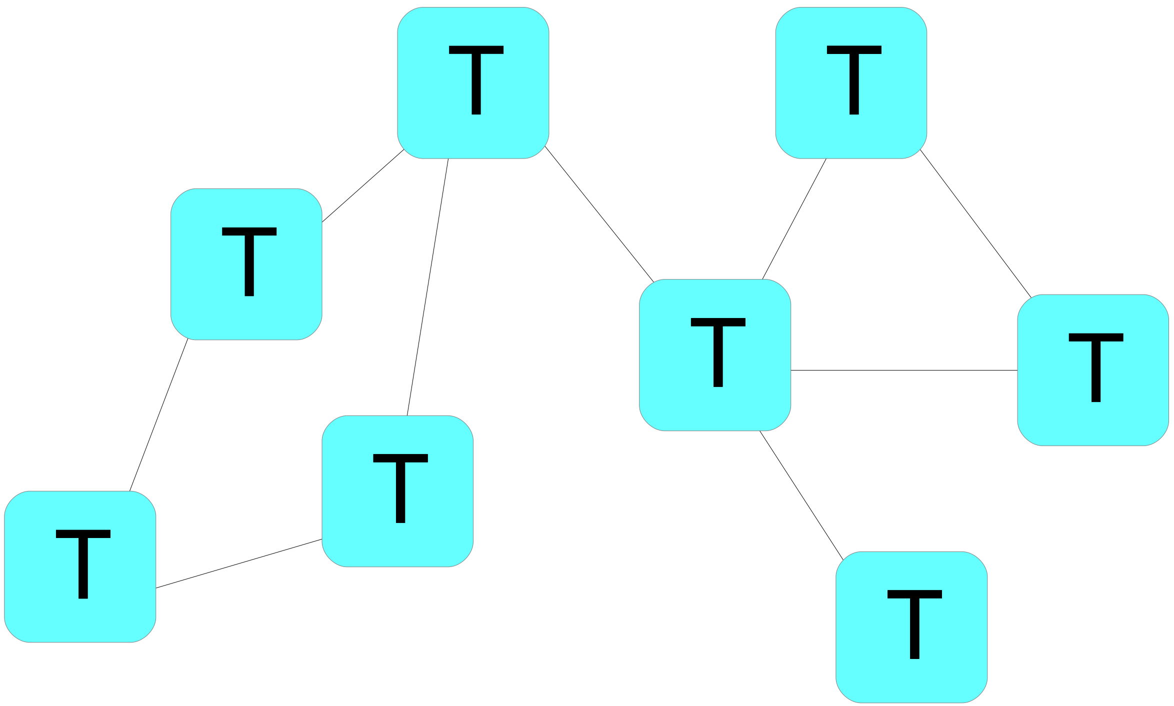
$$|\psi\rangle = \sum_{z_1=0}^{1} \cdots \sum_{z_N=0}^{1} \langle L|A[z_N]\ldots A[z_1]|R\rangle|z_1 \ldots z_N\rangle$$

A is a D-dim matrix, |L> and |R> are D-dim vector

By specifying A, |L>, and |R>, we can specify the state!

Tensor-network state

Generalization of MPS to higher dimension



$$\sum_{z_1=0}^{1} \cdots \sum_{z_N=0}^{1} C(T[z_N] \ldots T[z_1]) |z_1 \ldots z_N\rangle$$

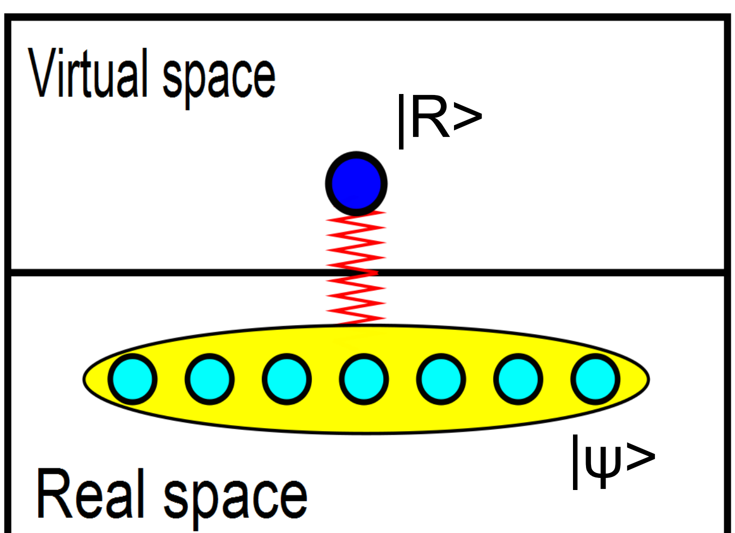
Contraction of tensors

$$|\psi\rangle = \sum_{z_1=0}^{1} \cdots \sum_{z_N=0}^{1} \langle L|A[z_N]\ldots A[z_1]|R\rangle |z_1\ldots z_N\rangle$$

$$|\eta\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$\sum_{z_2=0}^{1} \cdots \sum_{z_N=0}^{1} \langle L|A[z_N]\ldots A[z_2]A[\theta,\phi]|R\rangle |\eta\rangle \otimes |z_2\ldots z_N\rangle$$

$$A[\theta,\phi] = \cos\frac{\theta}{2}A[0] + e^{-i\phi}\sin\frac{\theta}{2}A[1]$$



Simulating QC in the virtual space!

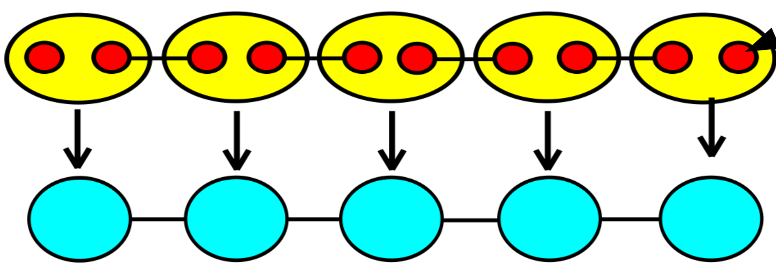
(Gross and Eisert, PRL 2007)
(TM, PRA 2012)

Edge state

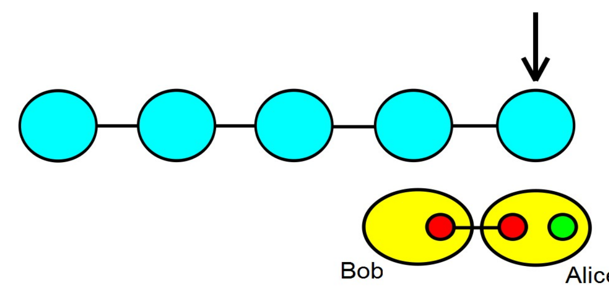
Virtual space corresponds to the edge state

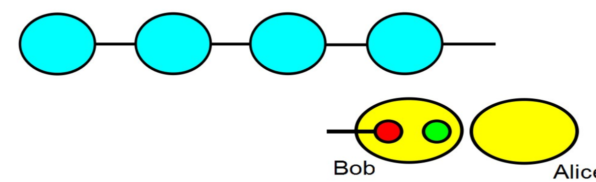
$$|\psi\rangle = \sum_{z_1=0}^{1} \cdots \sum_{z_N=0}^{1} \langle L|A[z_N]\ldots A[z_1]|R\rangle |z_1 \ldots z_N\rangle$$

AKLT



Edge state





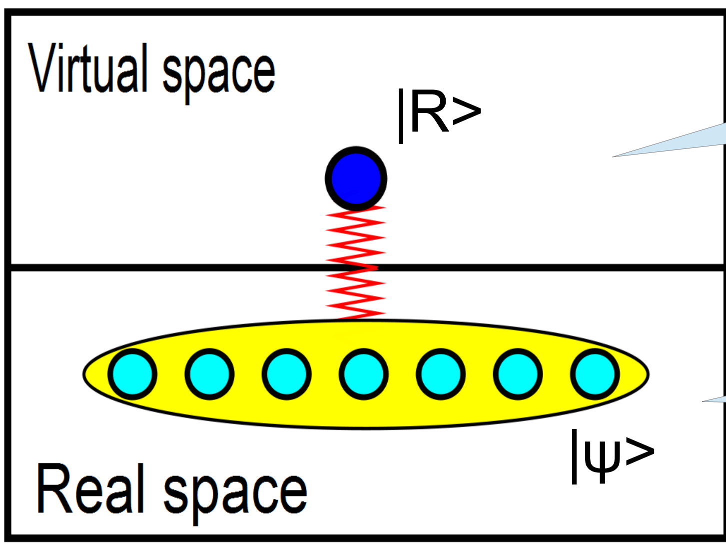
Edge state is the register of QC!

New resource states for MBQC:

AKLT (Brennen, et. al. PRL 2008)
VBS, PEPS (Verstraete, et. al. PRA(R) 2004; Fujii and TM PRA(R) 2012)
Haldane phase (Bartlett, et. al. PRL 2010)
String-net condensate (TM, PRA 2011)

Recent interest

How physical properties affect the structure of virtual space?
Is it useful for QC?



Some structure in Hilbert space
→ useful/useless for QC

Some physical properties:
Topological order, SPT, etc.

Some symmetry-protected topological order

→ $A = U \otimes B_{junk}$ Else, PRL 2012

Summary

- Tensor network representation/MPS
- MBQC and tensor network (virtual space)
- Edge state interpretation
- Relation between physical properties and virtual space structure

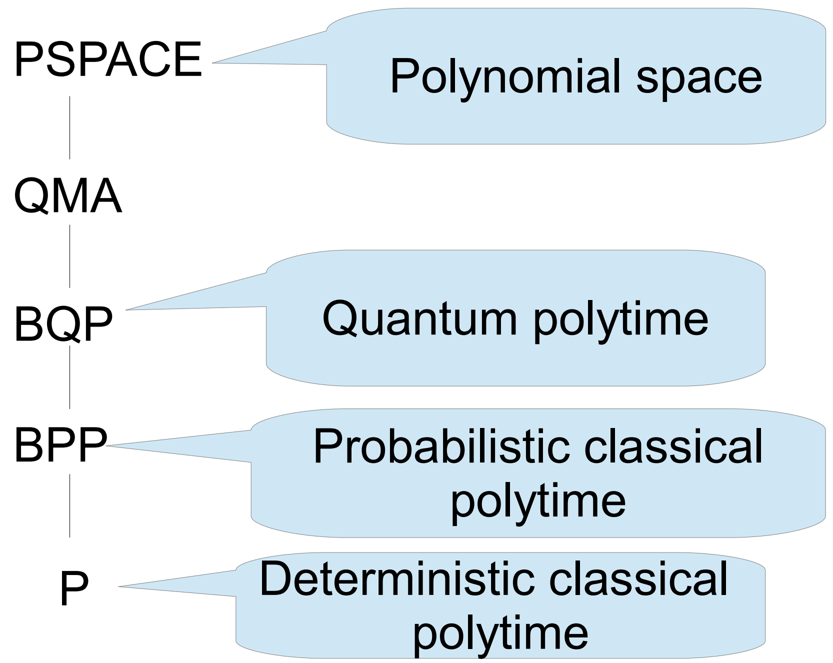
Quantum interactive proof system and its applications

Quantum computational complexity

Computational complexity: how much resource (time, space, entanglement, etc.) you need to solve a problem?

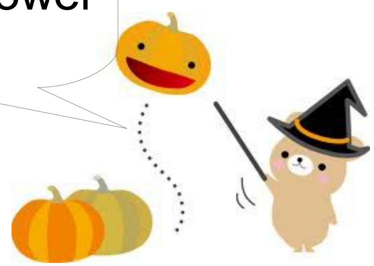
Decision problem: answerable with YES or NO

For example,
what is 1+1=? (it is not decision problem)
Is 1+1 larger than 3? (it is)

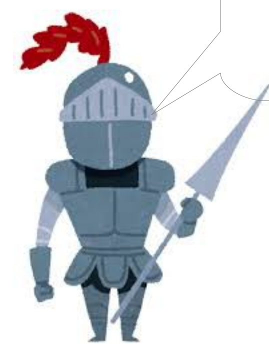


QMA(Quantum Merlin-Arthur)

Unbounded computational power



Merlin
Prover



BQP

Arthur
Verifier

Quantum state
（witness）

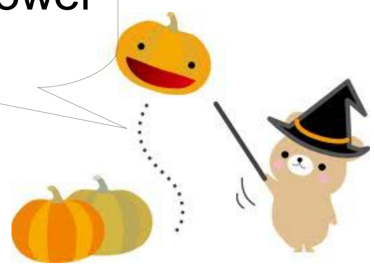
Kitaev, Knill, Watrous

A problem is QMA if and only if

If yes then there exists a quantum state such that Arthur accepts with high probability
If no then for any state Arthur accepts with small probability

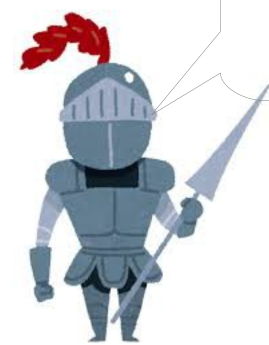
QIP(Quantum Interactive proof)

Unbounded
computational power



Merlin
Prover

BQP



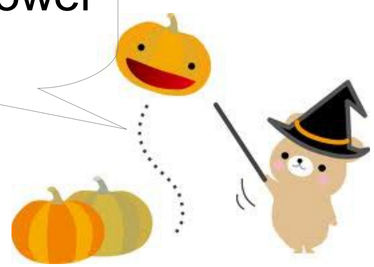
Arthur
Verifier

Quantum state
（witness）

QIP=IP=PSPACE
Watrous

QZK(Quantum Zero Knowledge)

Unbounded computational power



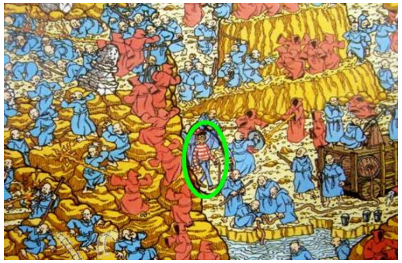
Merlin
Prover

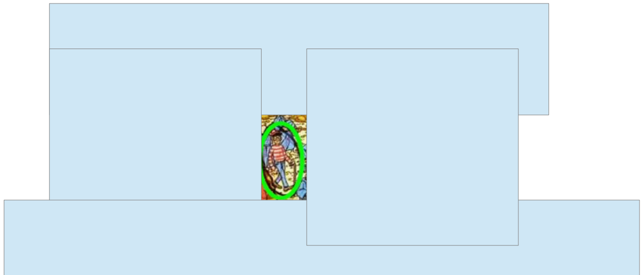
BQP

Arthur
Verifier

Quantum state (witness)

Where's Waldo?





Zero knowledge: no information is leaked to Arthur

Local Hamiltonian problem

$$H = \sum_j H_j$$

H_j = local Hamiltonian acting on 2 qubits

Yes: The ground energy of H is smaller than a

No: The ground energy of H is larger than b

Here, a-b>1/poly

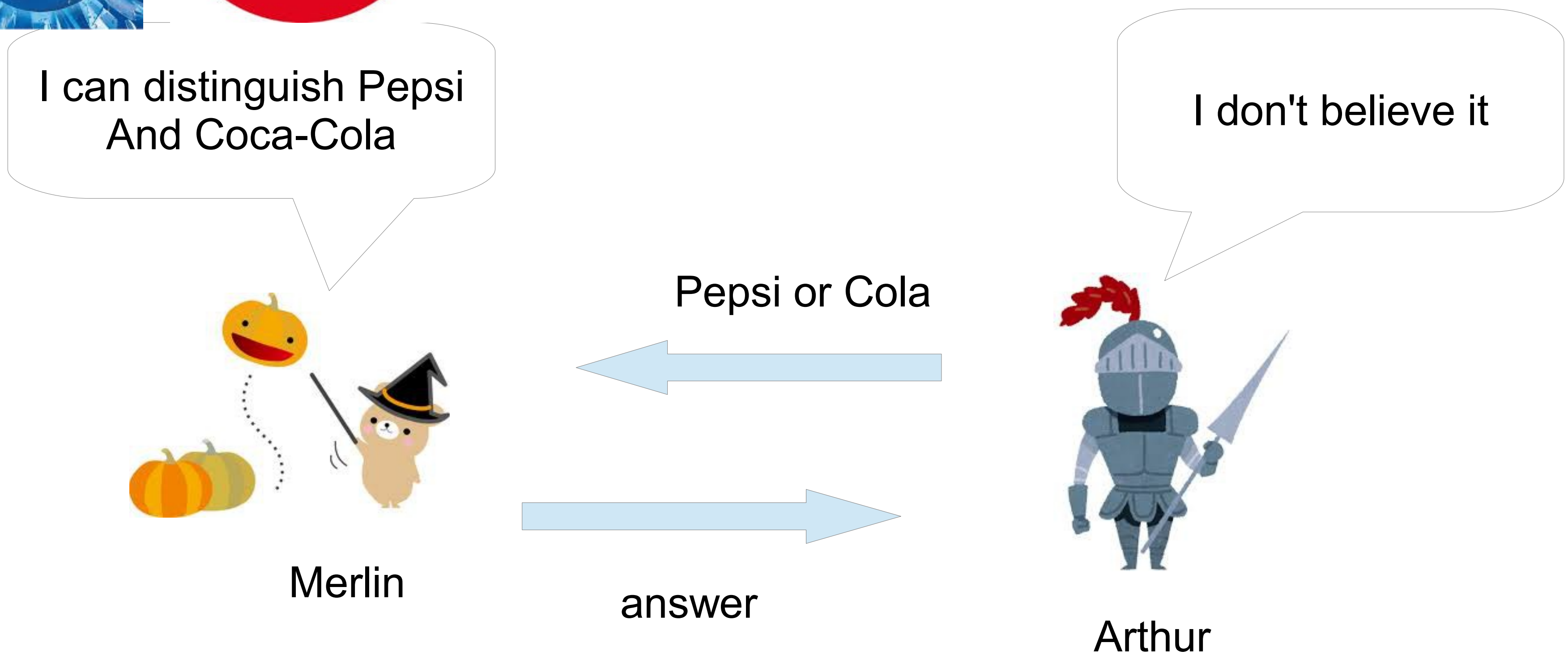
Local Hamiltonian problem is QMA-complete

Kitaev, Kempe, Regev,
Review by Aharonov arXiv:0210077

Even quantum computing cannot calculate the ground energy of Hamiltonians

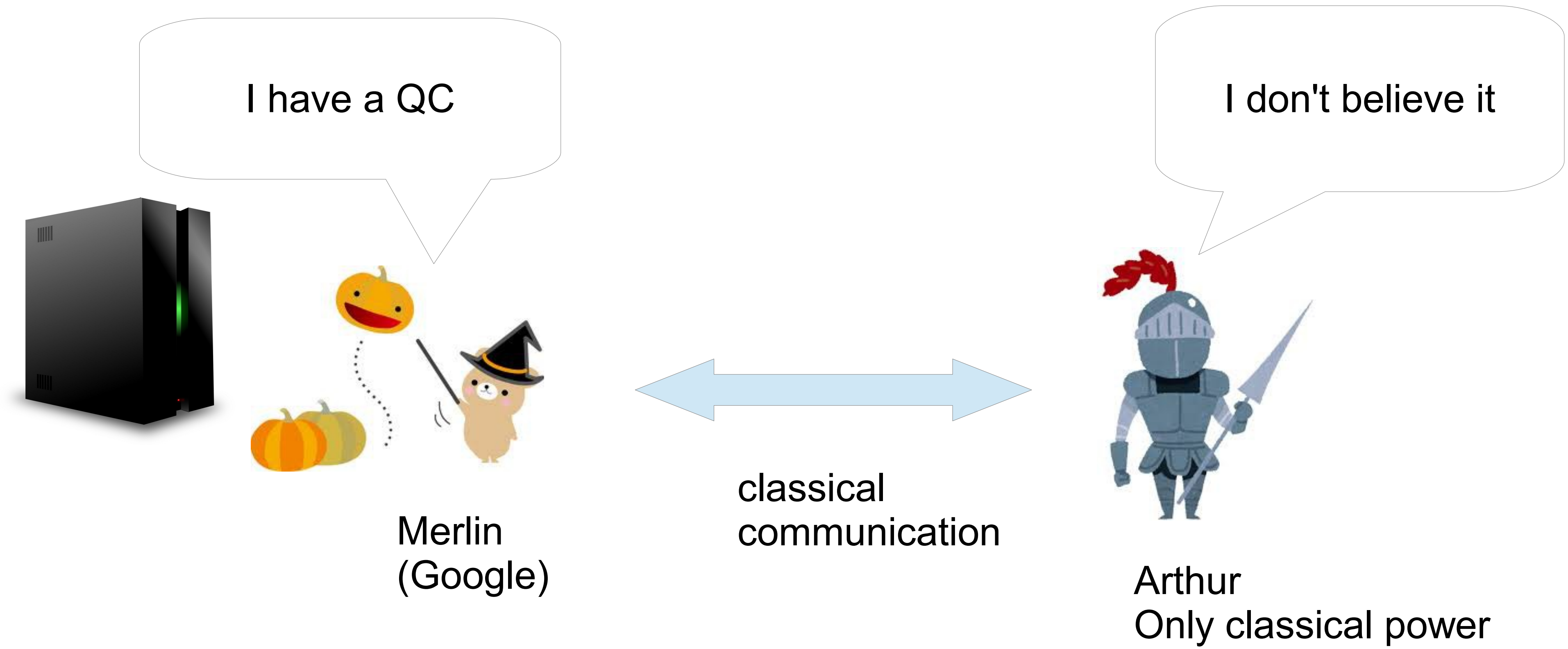
Verification of QC

Example



If Merlin answers correctly every time, Arthur is persuaded.

How about it?

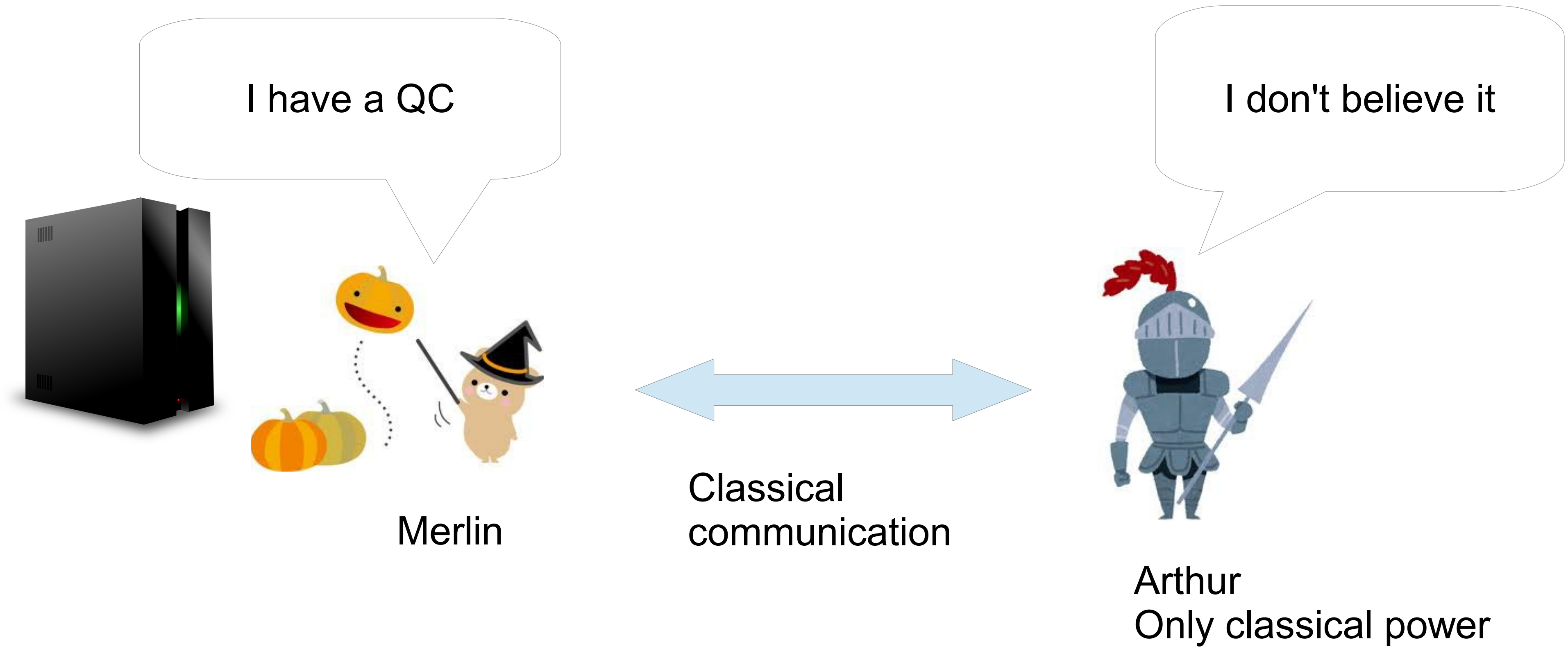


Can Arthur verify it?

Long-standing open problem in computer science!

Practically important: Can we verify Google?

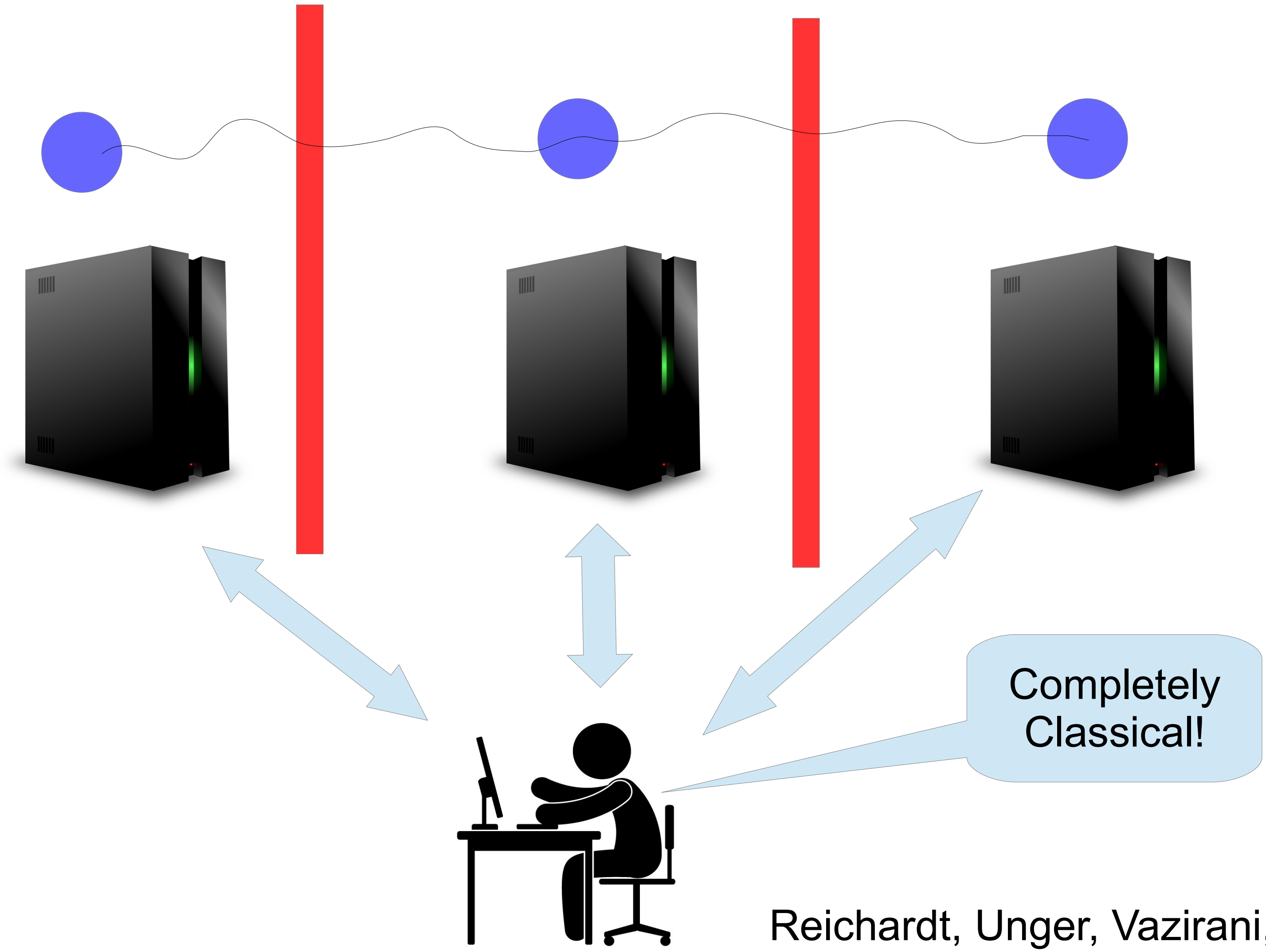
Partial solutions



Partial solutions

1. multi provers
2. verifier can generate single qubits
3. verifier can measure single qubits

More than two servers

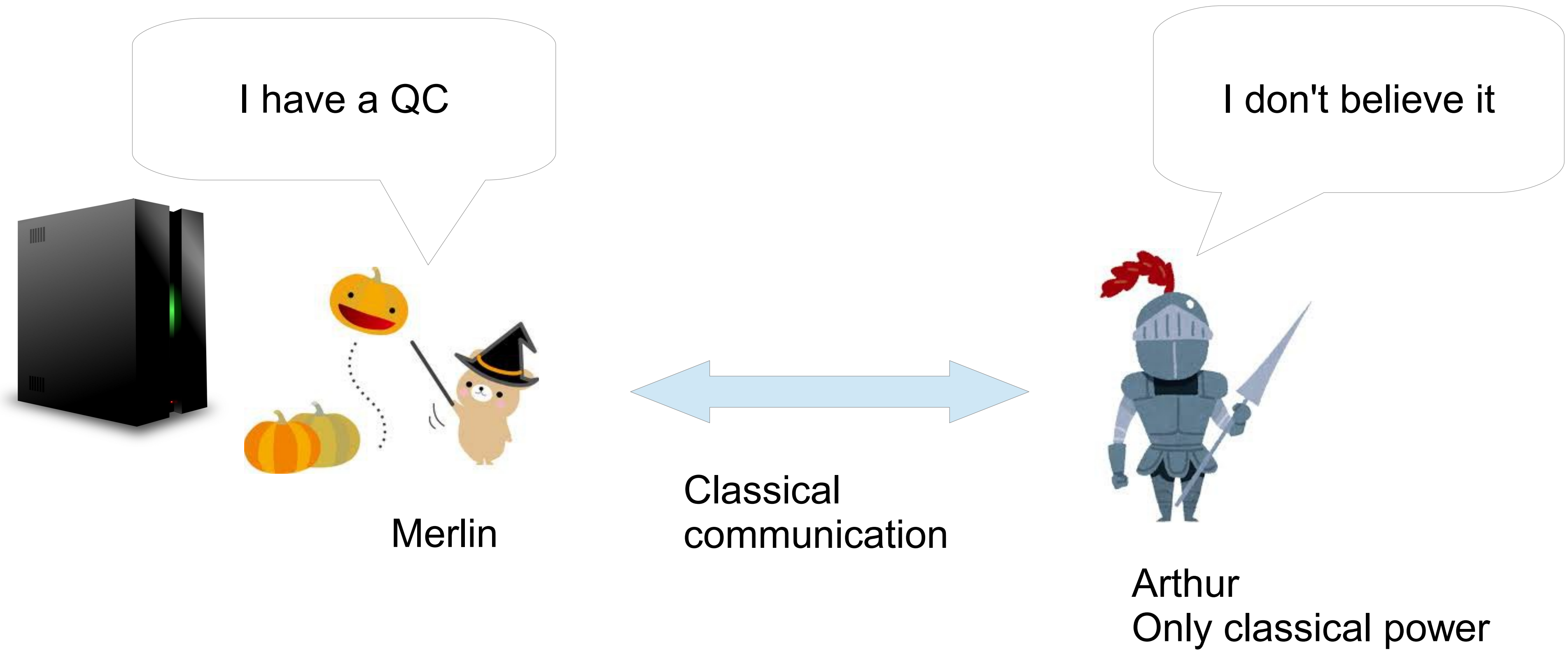


Reichardt, Unger, Vazirani, Nature 2013
McKague Theory of Computing 2016
Zi, STOC16

Experiment: Jian-Wei Pan, PRL2017

Non-communicating provers cannot cheat!

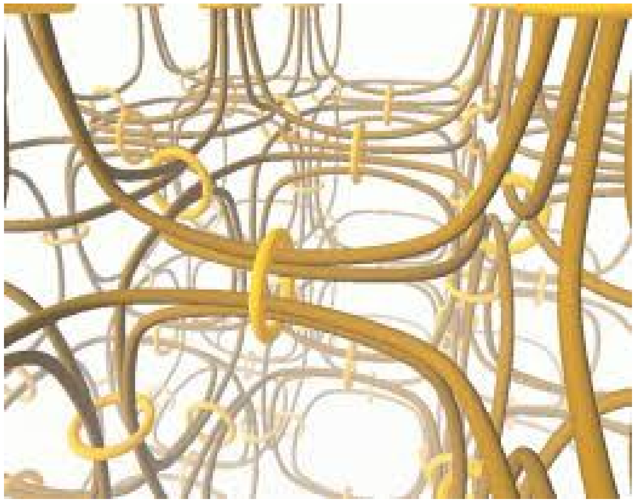
Partial solutions



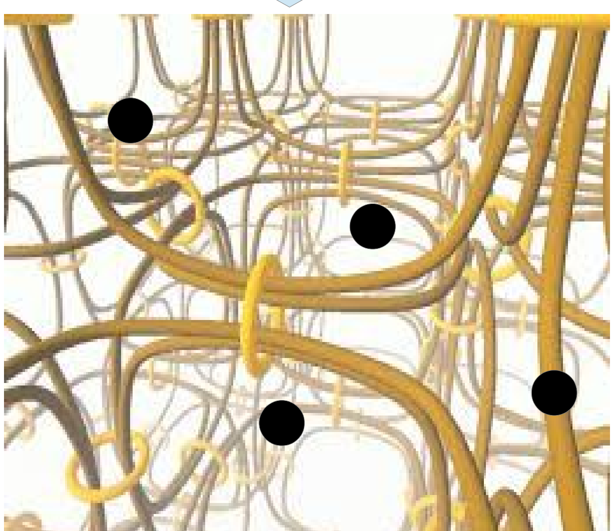
Partial solutions

1. multi provers
2. verifier can generate single qubits
3. verifier can measure single qubits

Trap technique (FK protocol)



Hiding traps



Fitzsimons and Kashefi, arXiv 2012
TM, Phys. Rev. A (R) 2014

news & views

QUANTUM COMPUTATION

Honesty test

Alice does not have a quantum computer so she delegates a computation to Bob, who does own one. But how can Alice check whether the computation that Bob performs for her is correct? An experiment with photonic qubits demonstrates such a verification protocol.

Tomoyuki Morimae

Access to first-generation quantum computers will most probably come as a cloud service because only few organizations, such as governments or big companies, will own such expensive and high-maintenance machines. How can client's privacy be protected in cloud quantum computing? How can clients test the correctness of the results output by the quantum server even though they do not have a quantum computer of their own? Writing in *Nature Physics*, Stefanie Barz and colleagues[1] answer these questions with a photonic qubit experiment.

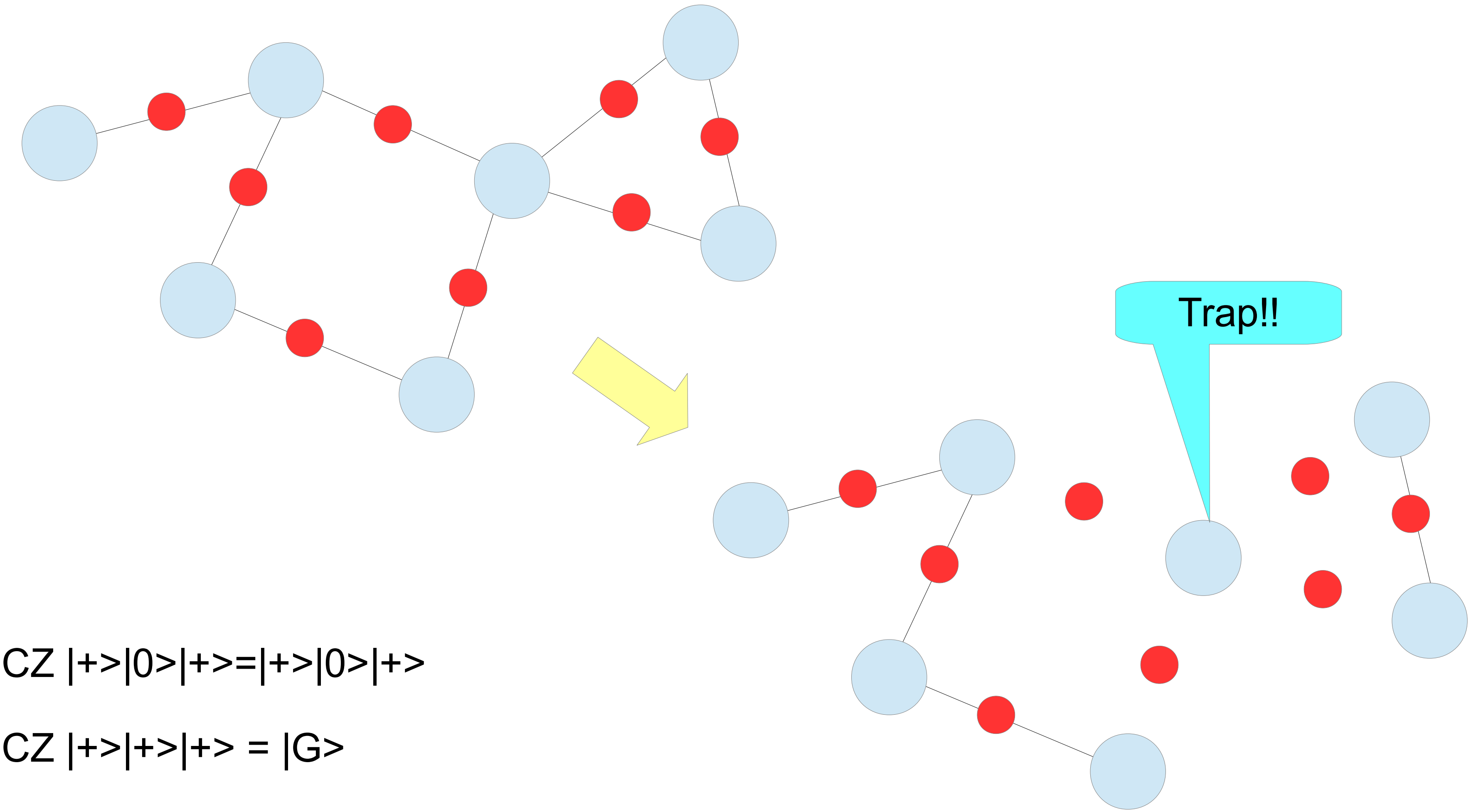
When you shop online, you do not want to reveal to a third party your private information, such as what you bought, your credit card number, your home address and so on. Alternatively, imagine that a pharmaceutical company uses a time-sharing service of a super-computer to run their molecular dynamics simulations. The pharmaceutical company wants to make sure that the data and the program — which are top secret in the industry — cannot be read by others. In short, securing

ILLUSTRATION FROM LEWIS CARROLL'S THROUGH THE LOOKING-GLASS, AND WHAT ALICE FOUND THERE

Experiment by Vienna group
Barz et al. Nature Phys. 2013
TM, Nature Phys. N&V 2013

Hiding traps

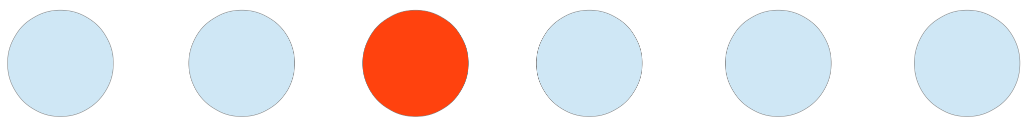
Fitzsimons and Kashefi, PRA 2017



CZ CZ |+>|0>|+>=|+>|0>|+>

CZ CZ |+>|+>|+> = |G>

Quantum error correcting code



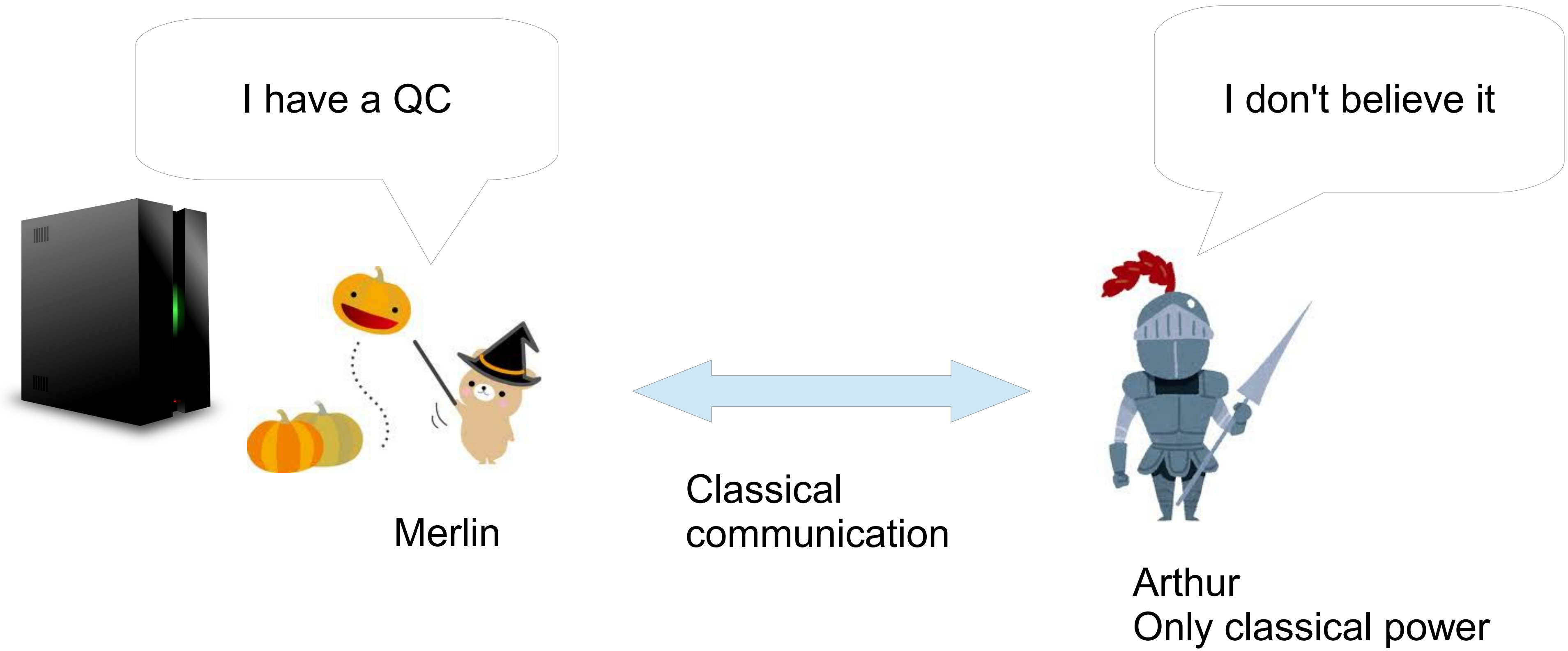
Probability being detected＝1/N

Encoding registers with QEC

Few qubit error → corrected

To change the logical state, more than d qubits must be changed
→ probability that Bob can change state without touching any trap = 2^{-d}

Partial solutions

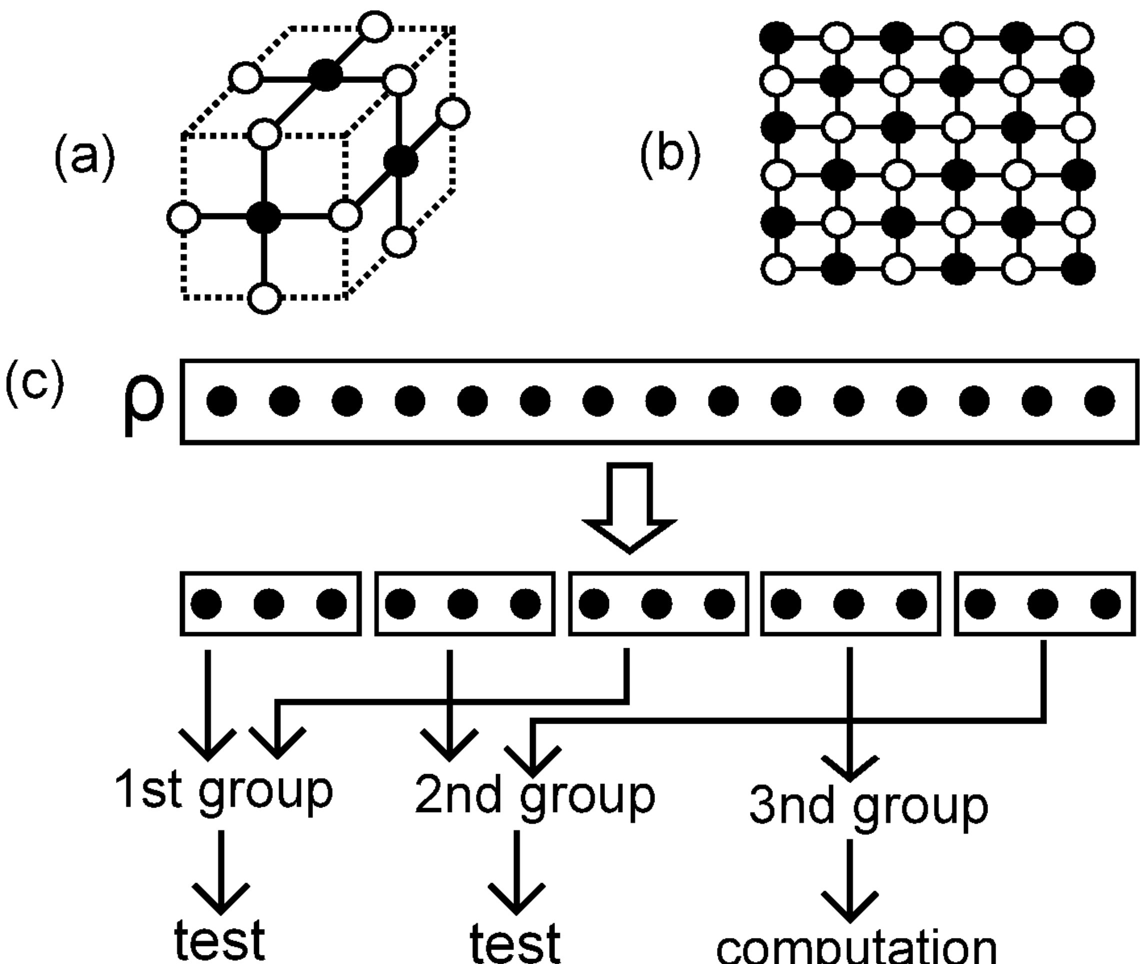


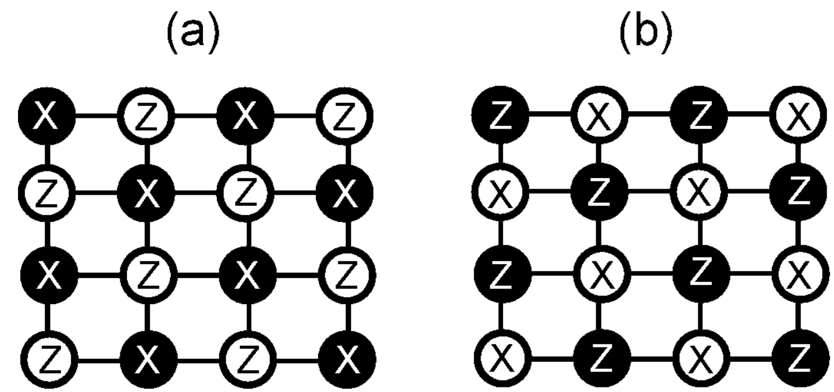
Partial solutions

1. multi provers
2. verifier can generate single qubits
3. verifier can measure single qubits

Verification with stabilizer testing

Hayashi and TM, PRL 2015





If the test passes, the resultant state satisfies (k is # of samples)

$$\langle G|\sigma|G\rangle \geq 1-\frac{1}{poly(k)}$$

Experiment by Vienna group
Greganti et al. NJP2016

Verification of Q supremacy

I have a QC

I don't believe it

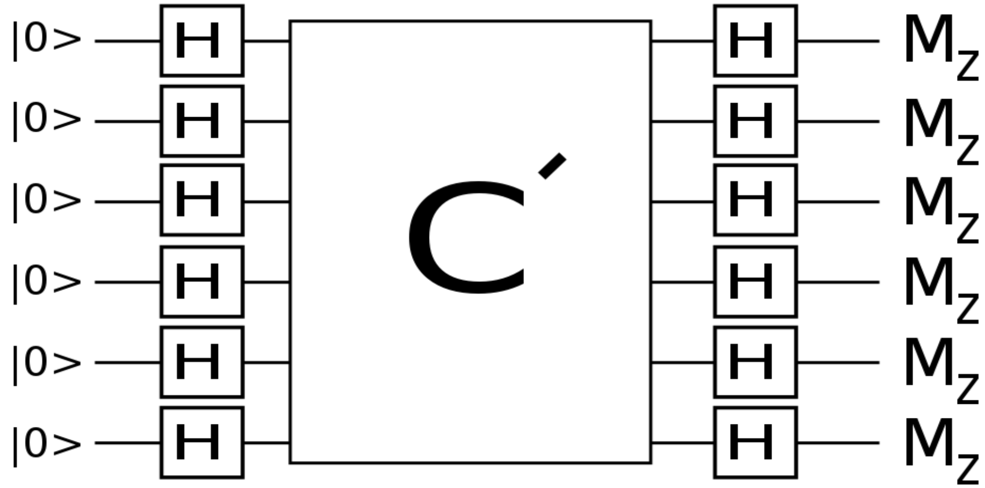
Merlin
(Google)

Classical
communication

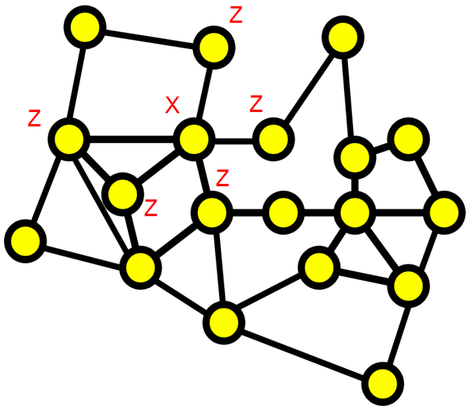
Arthur
Only classical power
(User)

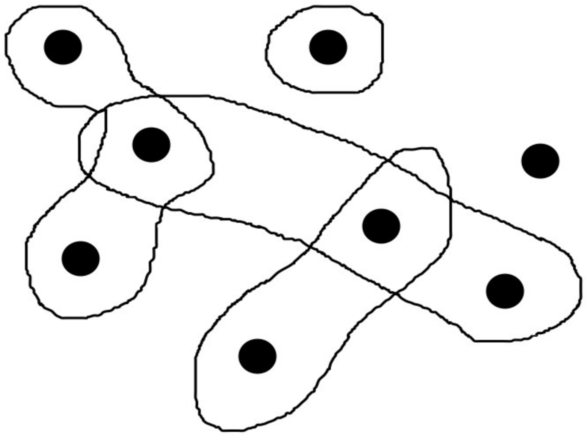
Can Arthur verify Q supremacy?

IQP(Instantaneous Quantum Polytime)



Output state of IQP is hypergraph state!





Verification of hypergraph state

Generalized stabilizer state!

$$|\psi\rangle = U|0^n\rangle$$

$$g_i \equiv U Z_i U^\dagger = \sum_i c_i \sigma_i$$

Z_i = diag(1,-1)

If the test passes

Given state

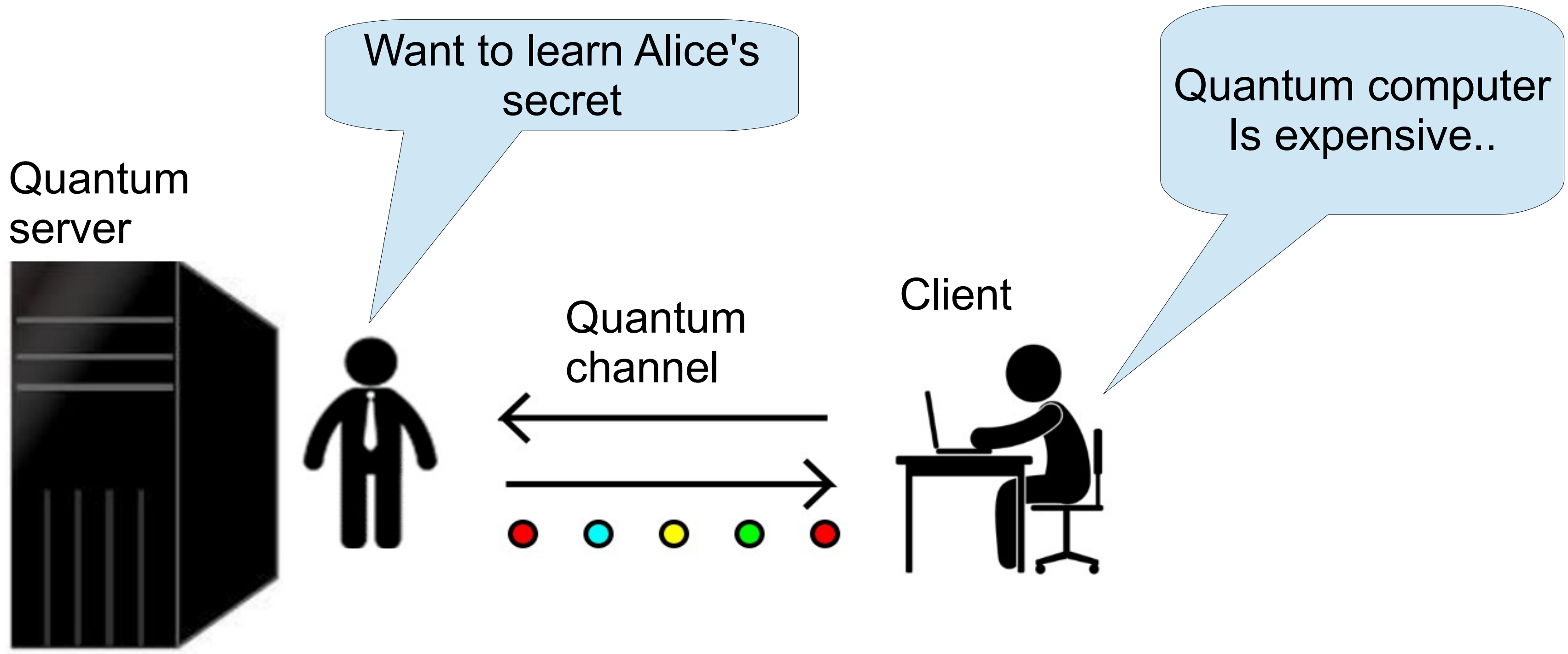
Ideal state

$$\|\rho - \rho_{IQP}\|_1 \leq \frac{1}{poly}$$

TM, Takeuchi, Hayashi, PRA2017
Takeuchi and TM, arXiv:1709.07575

Blind quantum computing

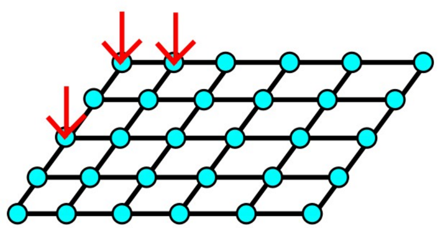
Blind quantum computing

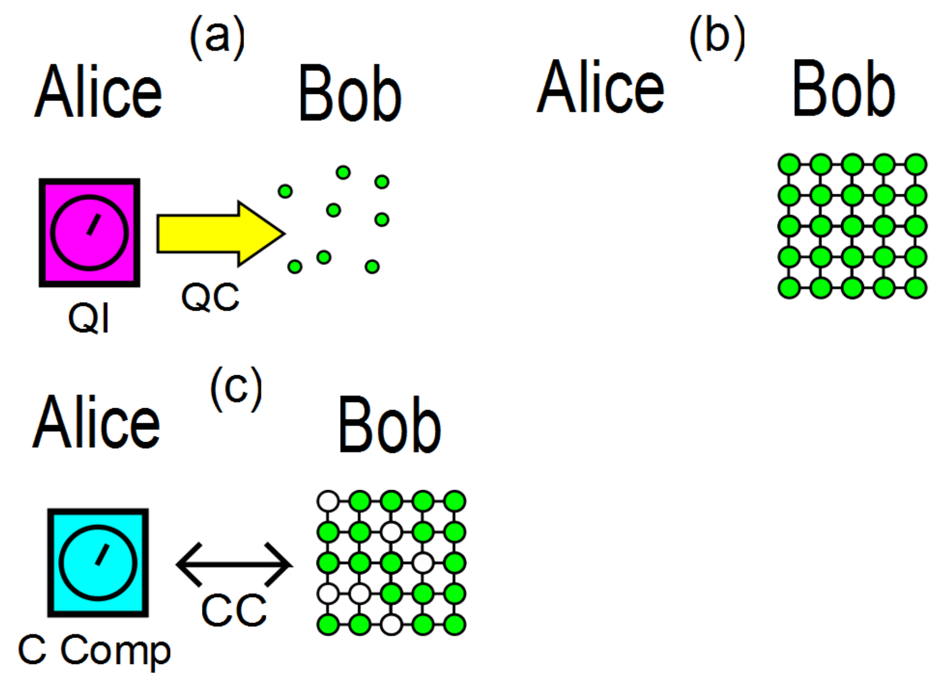


Can Alice delegate her quantum computing while protecting her privacy?

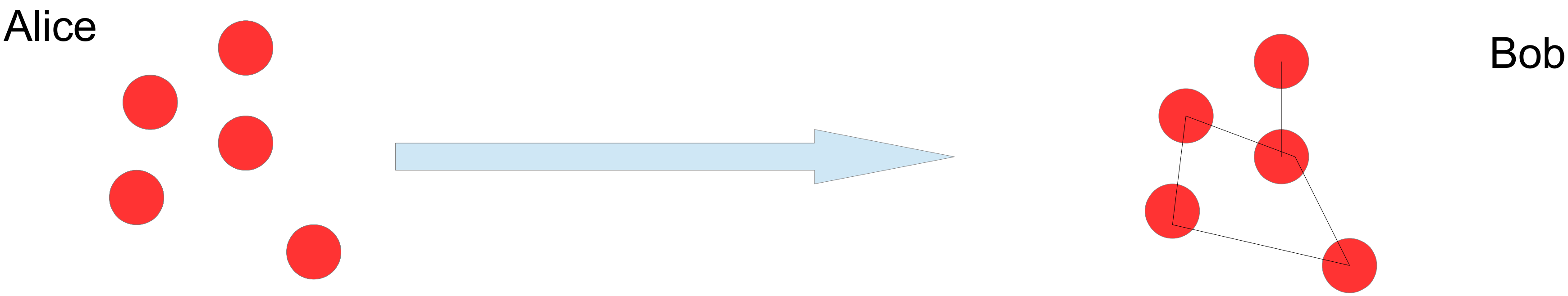
BFK protocol

cluster MBQC is used





[Broadbent, Fitzsimons, Kashefi, FOCS 2009]



$$\{e^{iZ\theta_j}|+\rangle\}_j \qquad CZ(\otimes_{j=1}^{N} e^{iZ\theta_j}|+\rangle) = (\otimes_{j=1}^{N} e^{iZ\theta_j})|G\rangle$$

$$e^{iZ\delta_j}|\pm\rangle$$ measurement

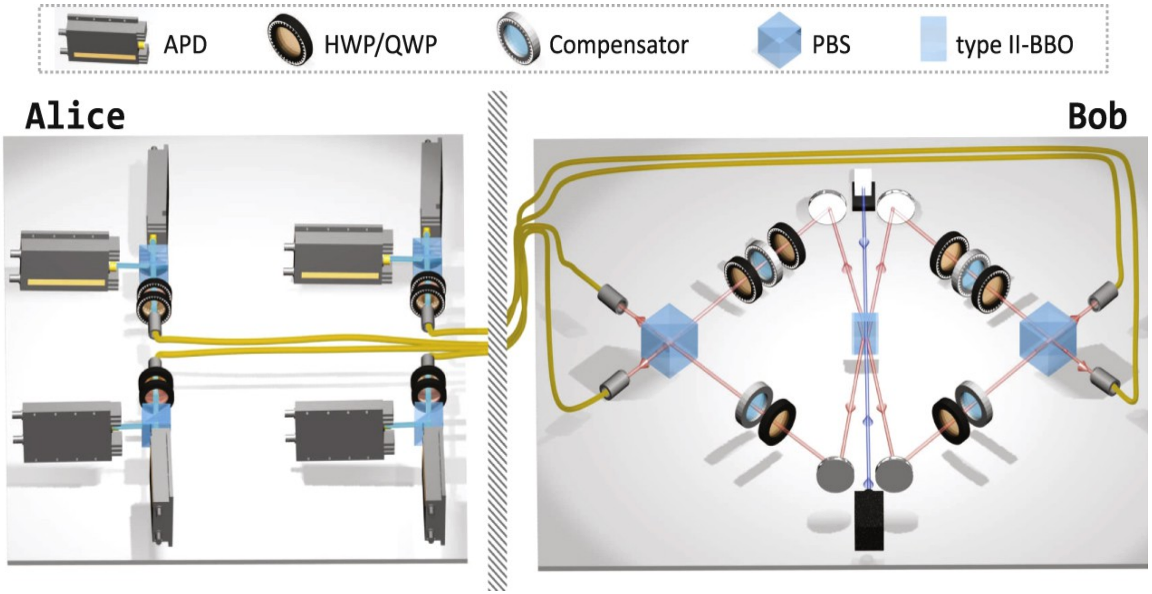
$$\delta_j = \phi_j - \theta_j$$

Measurement result

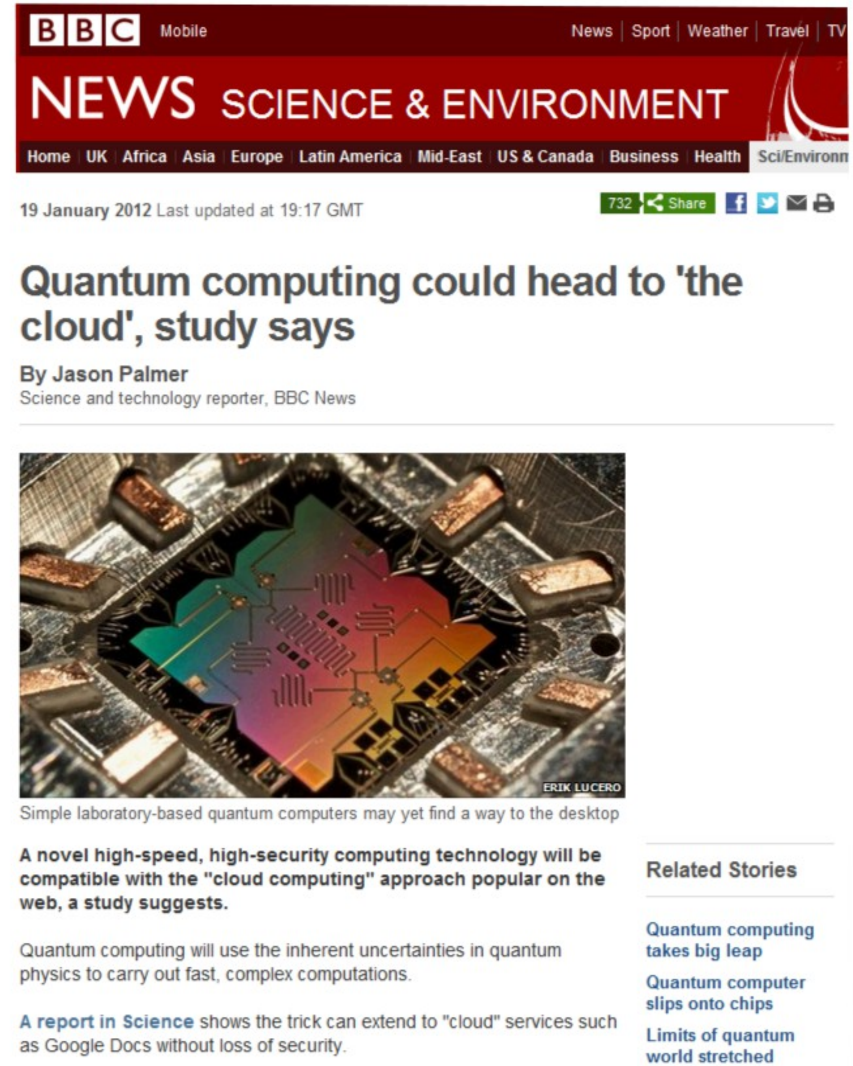
Bob cannot learn $\{\phi_j\}_j$

More rigorous proof: Dunjko et al. ASIACRYPTO2014

Experiment



Photonic qubits (Vienna group)
Barz et al., Science 2012



BBC Mobile News | Sport | Weather | Travel | TV

NEWS SCIENCE & ENVIRONMENT

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environm

19 January 2012 Last updated at 19:17 GMT

732 Share

Quantum computing could head to 'the cloud', study says

By Jason Palmer
Science and technology reporter, BBC News

ERIK LUCERO

Simple laboratory-based quantum computers may yet find a way to the desktop

A novel high-speed, high-security computing technology will be compatible with the "cloud computing" approach popular on the web, a study suggests.

Quantum computing will use the inherent uncertainties in quantum physics to carry out fast, complex computations.

A report in Science shows the trick can extend to "cloud" services such as Google Docs without loss of security.

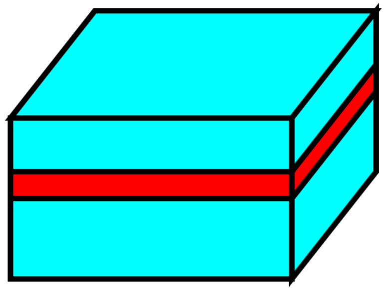
Related Stories

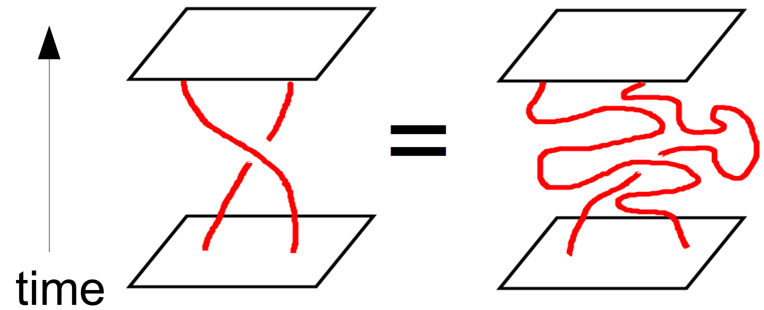
Quantum computing takes big leap
Quantum computer slips onto chips
Limits of quantum world stretched

Topological QC

Physics

Quasi-particle in a 2D electron system: anyon

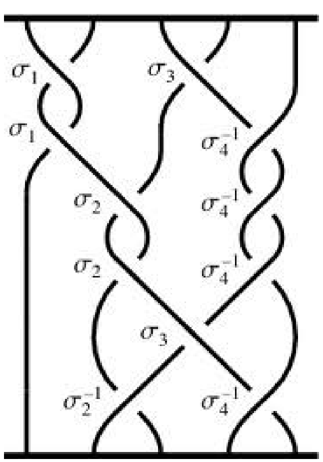


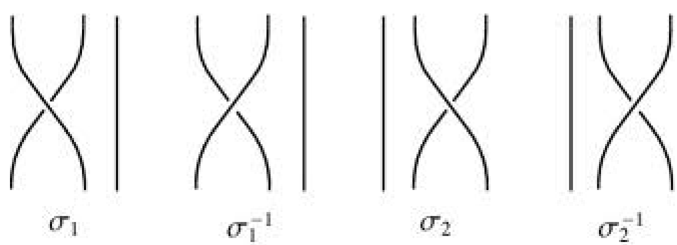


Topological equivalence

Mathematics

Unitary representation of braid group → quantum gate

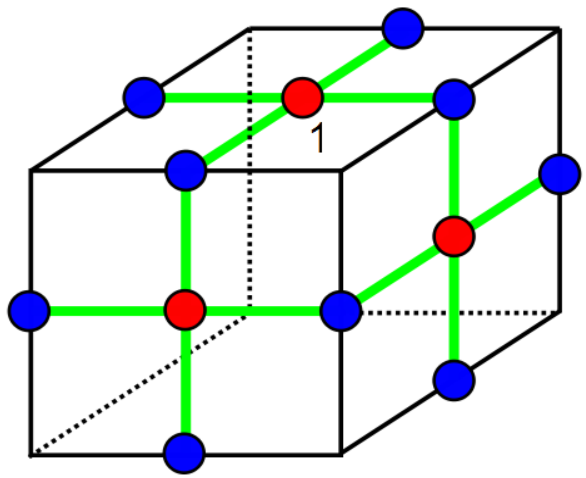




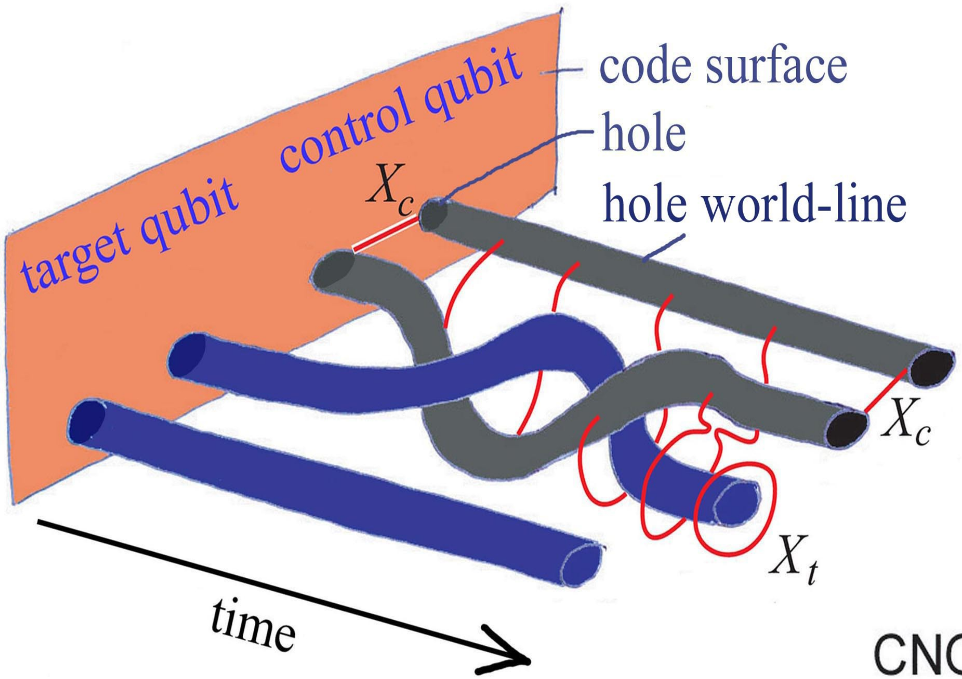
Different representation → Difference anyons
Ising anyon → realistic, but non-universal
Fibonattic anyon → not yet found, but universal

Simulation of topological QC

Simulate topological QC on measurement-based model



(a)

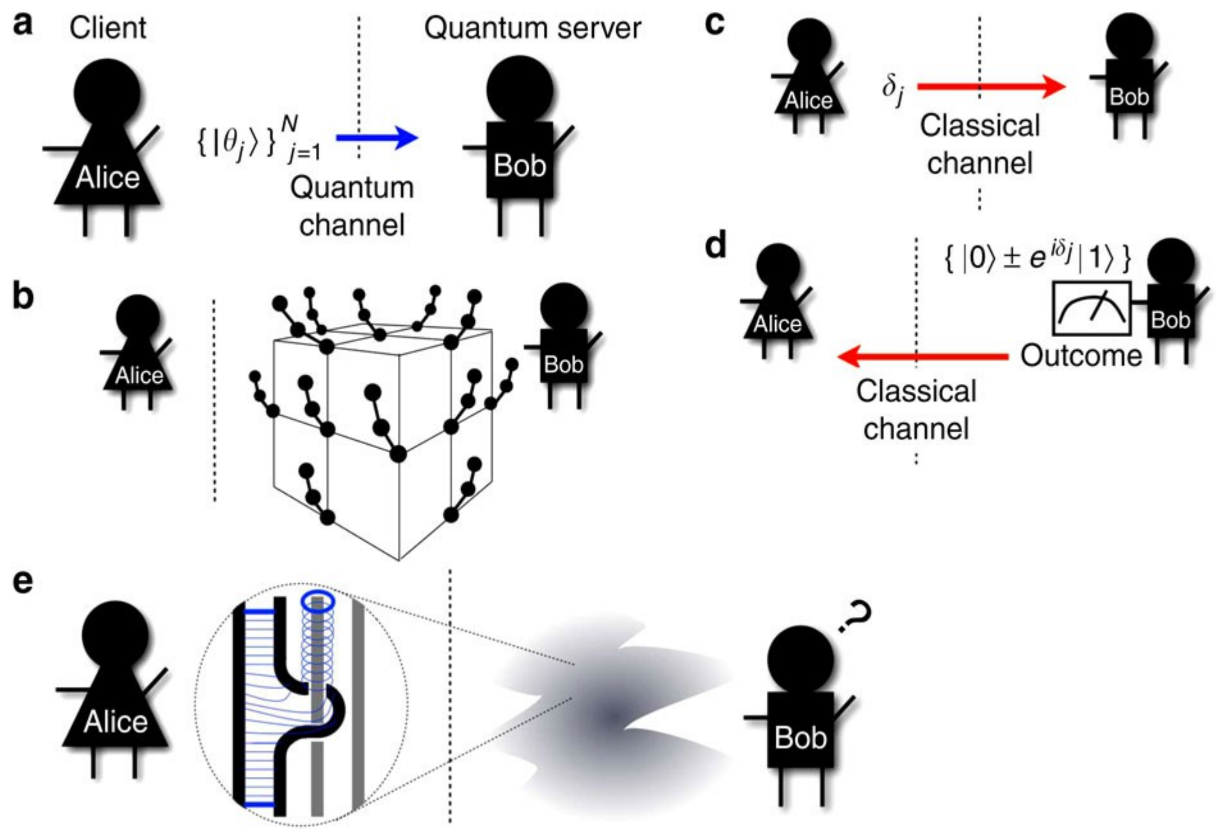


CNOT-gate

(Raussendorf et al, Physical Review Letters 2007)

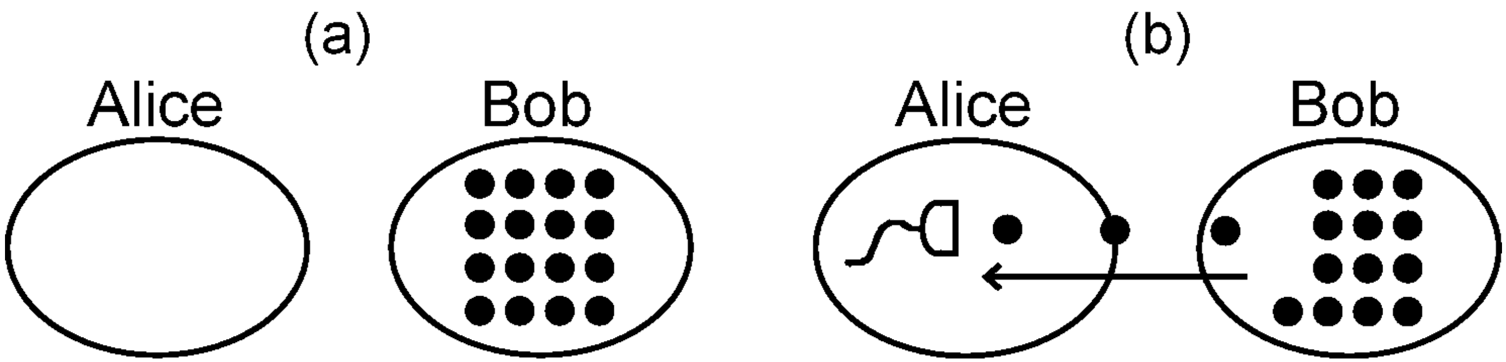
Topological blind QC

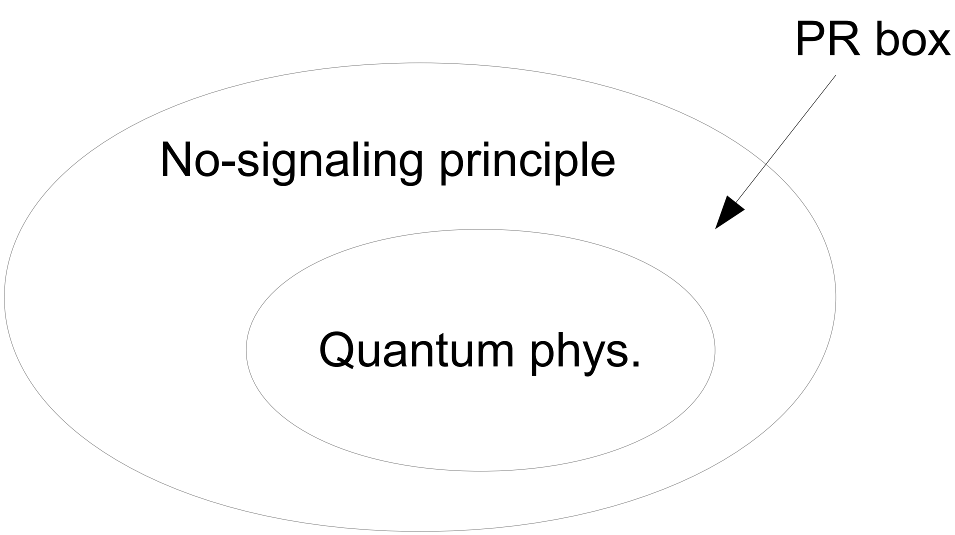
Topological QC with a nice error threshold



TM and Fujii, Nature Communications 2012

Measurement-only blind QC





Advantage:

Measurement is easier (optics, etc.)
Simple
No-signaling security
Device independence security

TM and Fujii, PRA(R) 2012

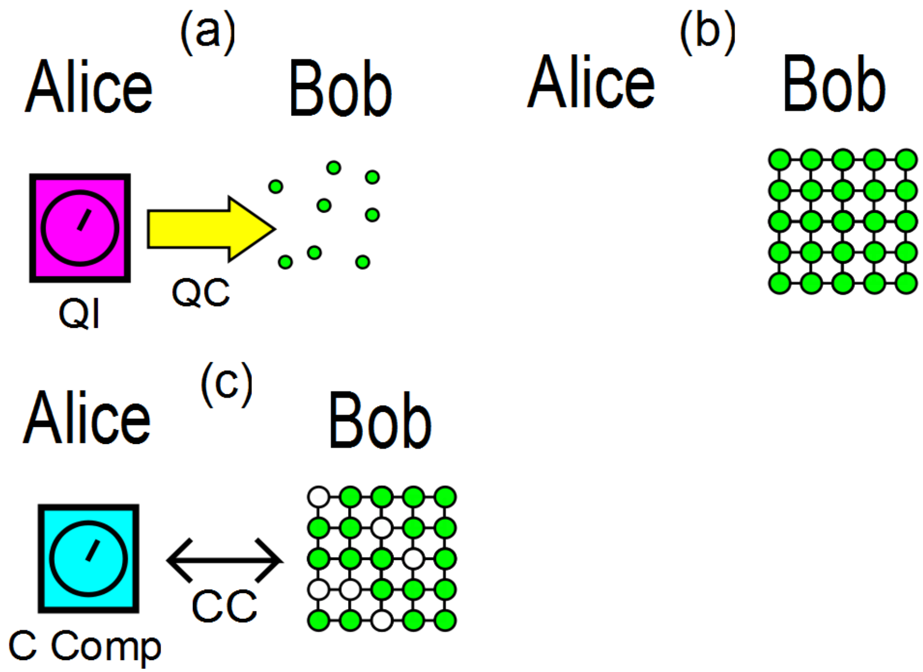
Summary

- Quantum Interactive proof system (QMA, QIP, QZK)
- Verification of QC
- Verification of Q supremacy
- Blind QC

END

Problems of the BFK protocol

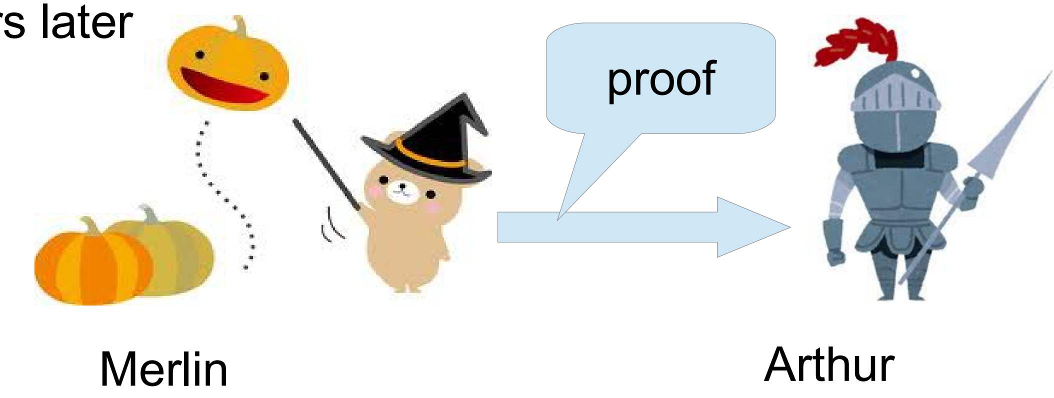
1. Generating single qubit is not easy
2. Fault-tolerant?
3. Security proof is complicated



Post hoc verification

Post hoc verification

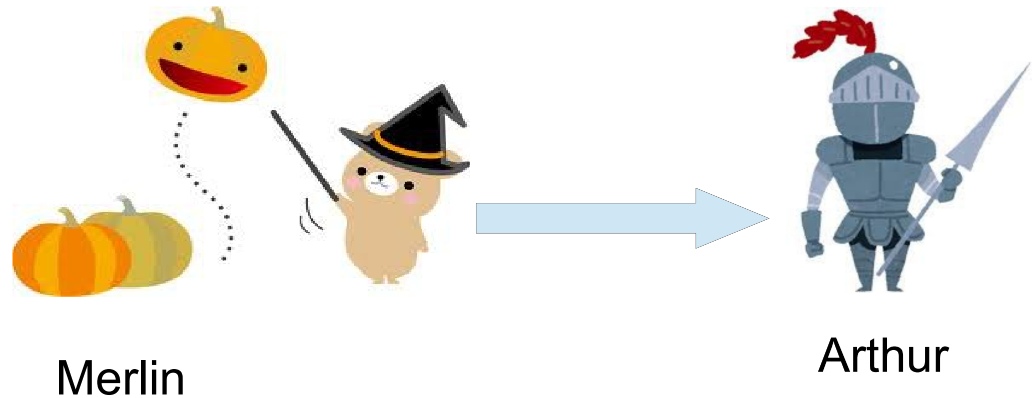
10years later



Fitzsimons, Hajdusek, TM, Phys. Rev. Lett. 2018

$$\sum_{t=0}^{T}(V_t \ldots V_1 V_0|\psi\rangle \otimes |0\rangle) \otimes |t\rangle$$

Post hoc verification



BQP is in QMA
QMA can be verified with single-qubit measurements [TM, Nagaj, Schuch, PRA2016]

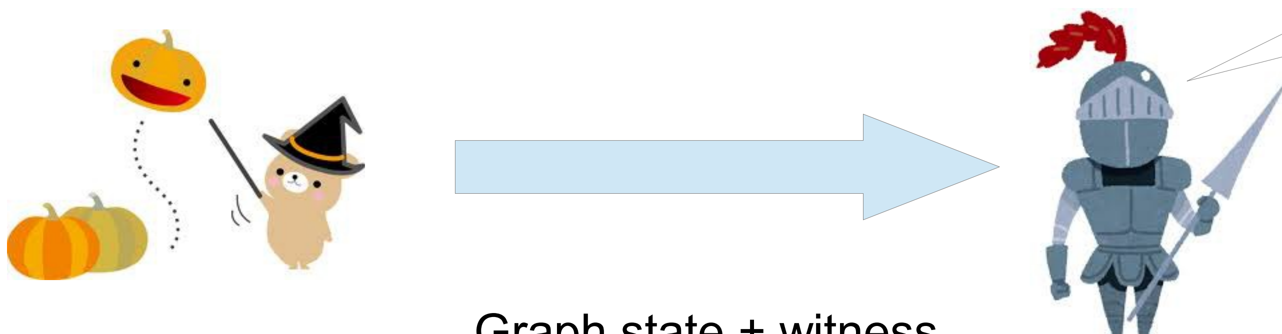
Summary

- QMA (higher than BQP)
- Verification of QC
- Blind QC

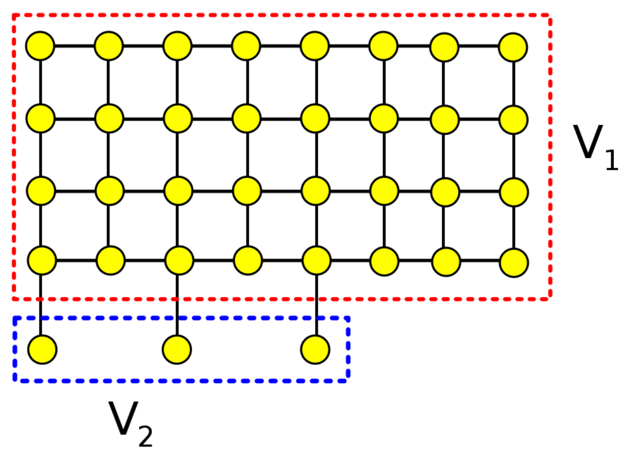
QMA for single-qubit measurement verifier

TM, Nagaj, Schuch, PRA 2016

Check stabilizers, or
Doing MBQC

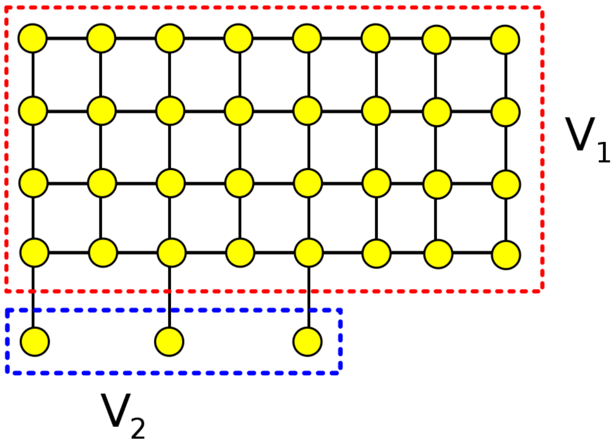


Graph state + witness



Correct graph state
→ by the soundness,
rejection probability is high

Wrong state
→ Stabilizer check rejects it



$$s_k = \prod_{j=1}^{N} g_j$$

$$p_{pass} = \frac{1}{2^n} \sum_k \mathrm{Tr}\left(\frac{I + s_k}{2}\rho\right)$$

By using gentle measurement lemma, $\|\rho - \Lambda\rho\Lambda\|_1 \leq 2\sqrt{1 - Tr(\Lambda\rho)}$

If $p_{pass} \geq 1 - \epsilon$ $\quad \frac{1}{2}\|\rho - CZ(|G\rangle \otimes |\phi\rangle)\|_1 \leq \sqrt{2\epsilon}$

$$p_{acc} = qp_{comp} + (1-q)p_{test}$$

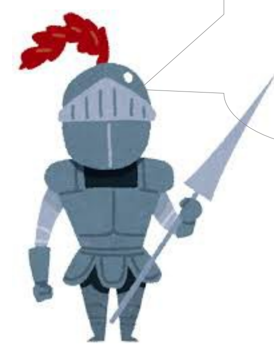
if $p_{test} \geq 1 - \epsilon$ then $p_{acc} \leq q(2^{-r} + \sqrt{2\epsilon}) + (1-q)$

if $p_{test} < 1 - \epsilon$ then $p_{acc} \leq q + (1-q)(1-\epsilon)$

QMA for Clifford Arthur

TM, Hayashi, Nishimura, Fujii, QIC 2015

Magic states + witness



Clifford gates: H, CNOT, S=(1,i) → Classically simulatable（Gottesman-Knill）

Magic state: $\sin\frac{\pi}{8}|0\rangle+\cos\frac{\pi}{8}|1\rangle$ → universal