# Local Hamiltonian and verification of quantum computing

Tomoyuki Morimae
（YITP, Kyoto University）

45min

# Outline

- Local Hamiltonian problem
- Verification of quantum computing

# k-Local Hamiltonian problem

Given a, b, and

$$H = \sum_i H_i$$

k-body

decide

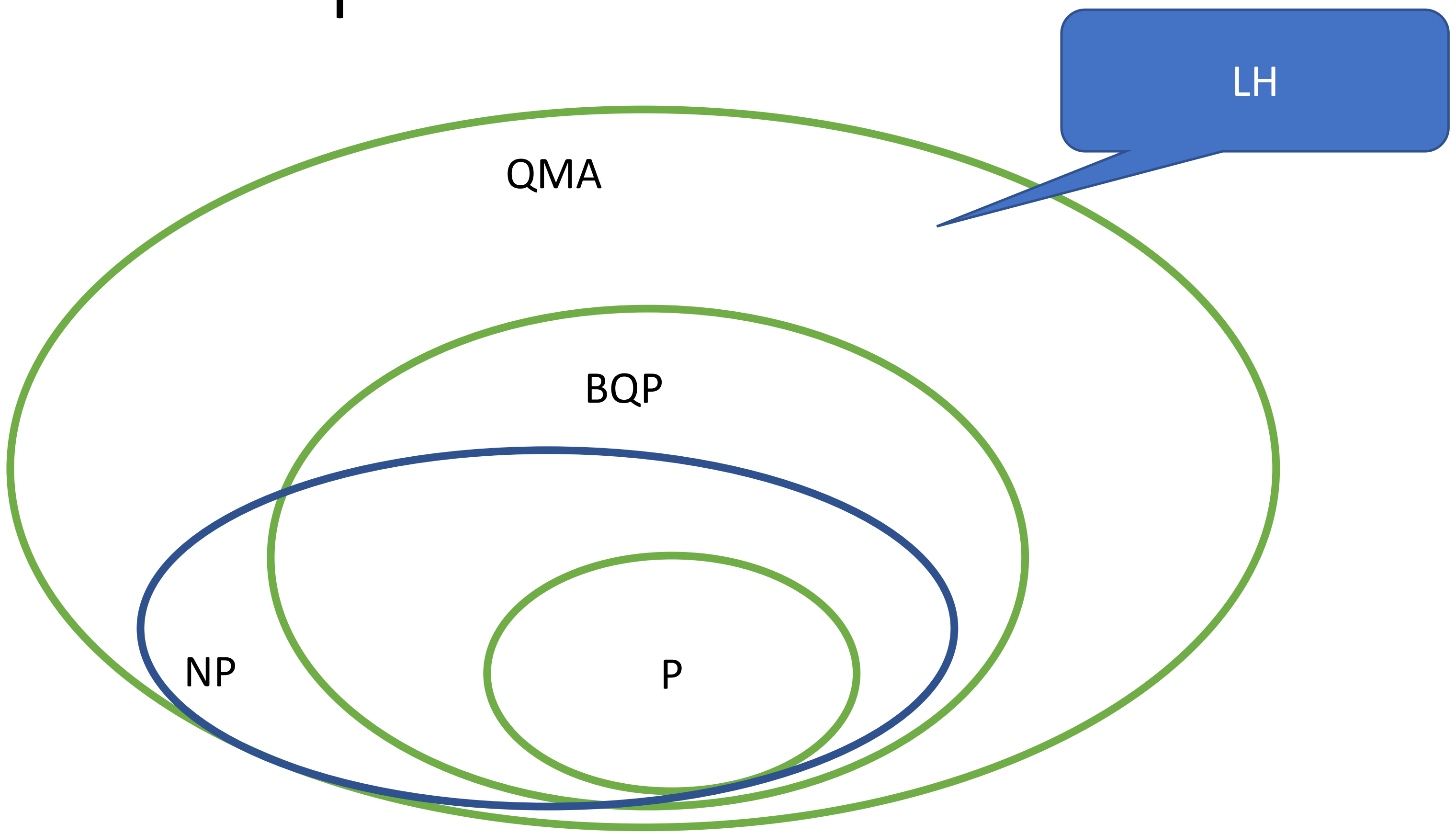
YES: $E_0 < \mathrm{a}$

NO: $E_0 > \mathrm{b}$

2-local XZ-Hamiltonian problem is QMA-complete

$$H = \sum_{i,j} \alpha_{i,j}(X_i X_j + Z_i Z_j)$$

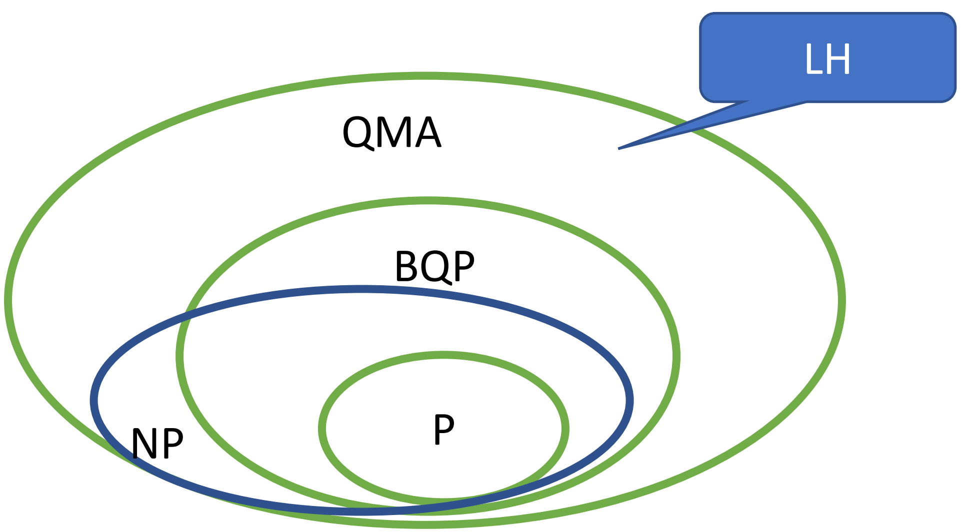
# QMA-complete




Local Hamiltonian problem is the hardest problem in QMA

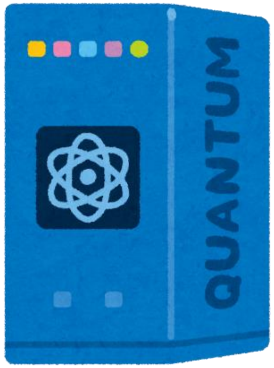
# P(BPP)

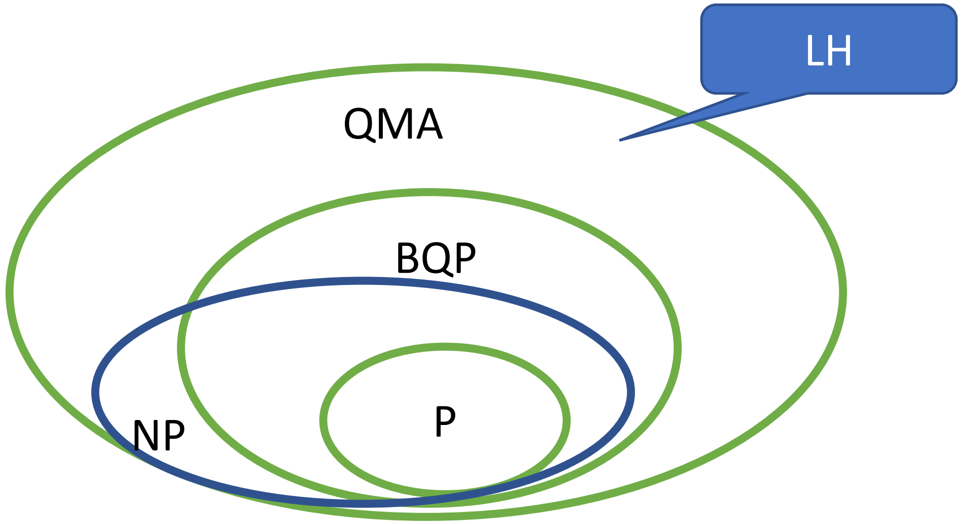
Problems that can be efficiently solved with classical computer



# BQP

Problems that can be efficiently solved with quantum computer



# NP(MA)

Problems that can be efficiently verified with classical hint

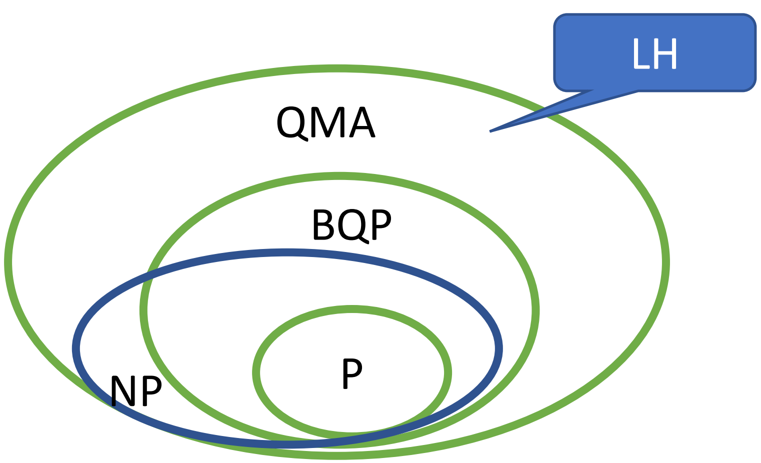
Witness

A problem is in MA if and only if

P(BPP)

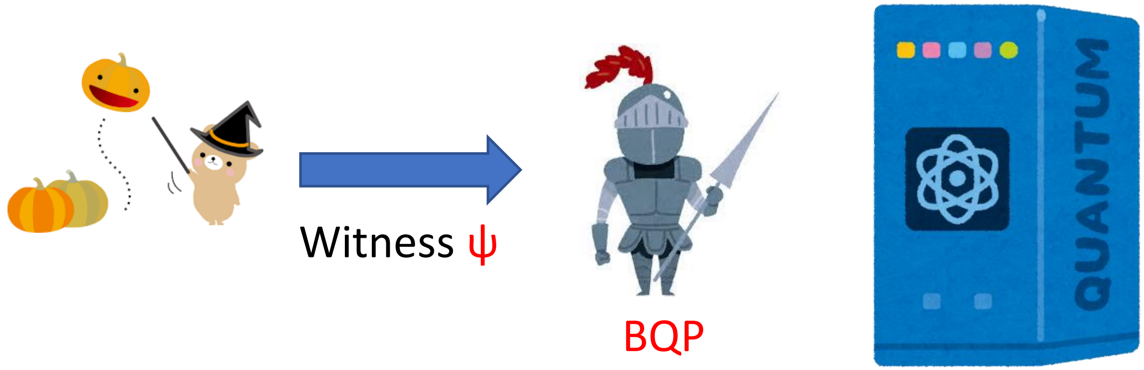
For yes instance, there exists a witness s.t. the verifier accepts with high probability

For no instance, for any witness, the verifier accepts with small probability



# QMA

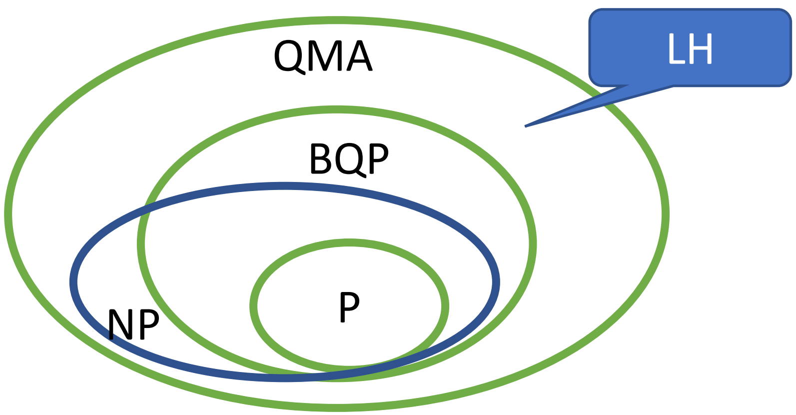
Problems that can be efficiently verified with quantum hint



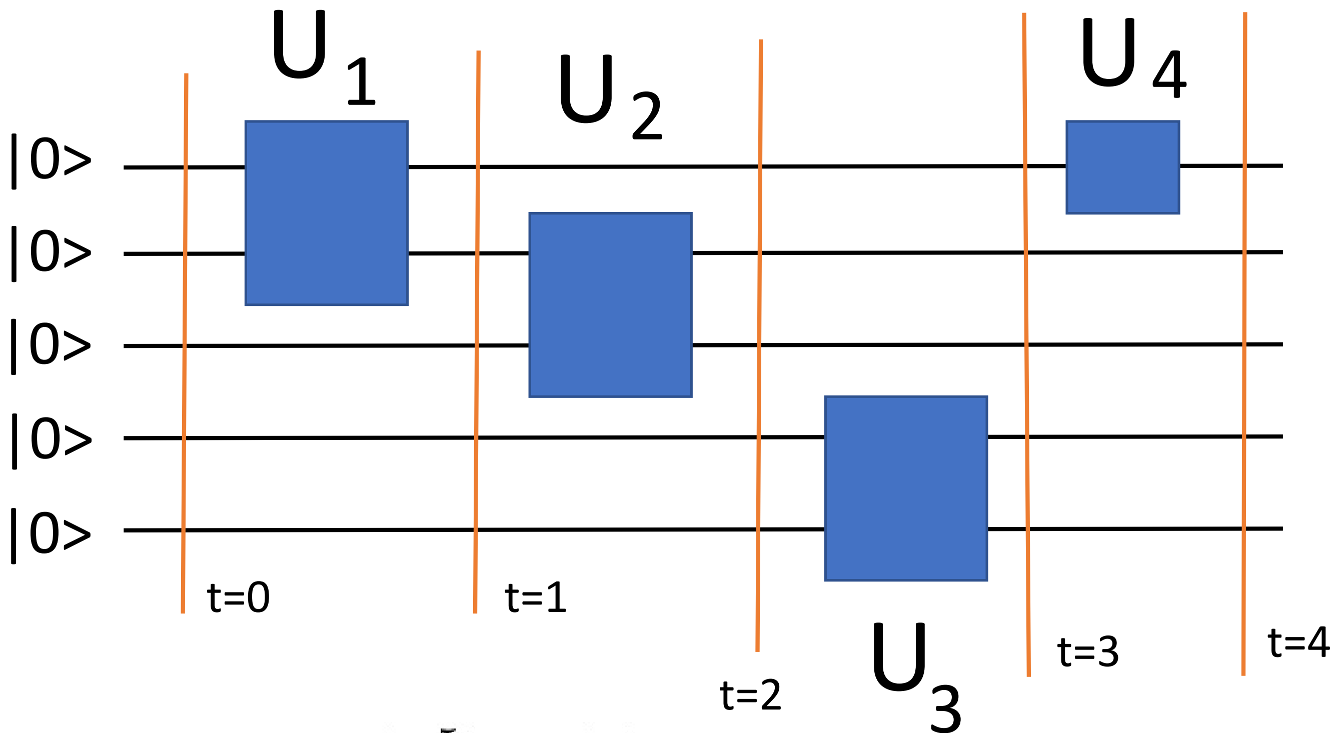

A problem is in QMA if and only if

For yes instance, there exists a witness s.t. the verifier accepts with high probability

For no instance, for any witness, the verifier accepts with small probability



# Feynmann-Kitaev construction




$$
\begin{aligned}
|\Psi\rangle \quad = \quad & U_4U_3U_2U_1|0^5\rangle \otimes |4\rangle \\
& + U_3U_2U_1|0^5\rangle \otimes |3\rangle \\
& + U_2U_1|0^5\rangle \otimes |2\rangle \\
& + U_1|0^5\rangle \otimes |1\rangle \\
& + |0^5\rangle \otimes |0\rangle
\end{aligned}
$$

Such state is called history state
[Feynmann and Kitaev]

# History state is the ground state of local Hamiltonian!

$$
\begin{aligned}
|\Psi\rangle \quad = \quad & U_4U_3U_2U_1|0^5\rangle \otimes |4\rangle \\
& +U_3U_2U_1|0^5\rangle \otimes |3\rangle \\
& +U_2U_1|0^5\rangle \otimes |2\rangle \\
& +U_1|0^5\rangle \otimes |1\rangle \\
& +|0^5\rangle \otimes |0\rangle
\end{aligned}
$$

$$H_{init} = (I - |0^5\rangle\langle 0^5|) \otimes |0\rangle\langle 0|$$

Checking whether the initial state is correct

Wrong state-> high energy penalty

$$H_{init}|\Psi\rangle = 0$$

$$
\begin{aligned}
|\Psi\rangle \quad = \quad & U_4U_3U_2U_1|0^5\rangle \otimes |4\rangle \\
& + U_3U_2U_1|0^5\rangle \otimes |3\rangle \\
& + U_2U_1|0^5\rangle \otimes |2\rangle \\
& + U_1|0^5\rangle \otimes |1\rangle \\
& + |0^5\rangle \otimes |0\rangle
\end{aligned}
$$

Checking whether propagation is correct

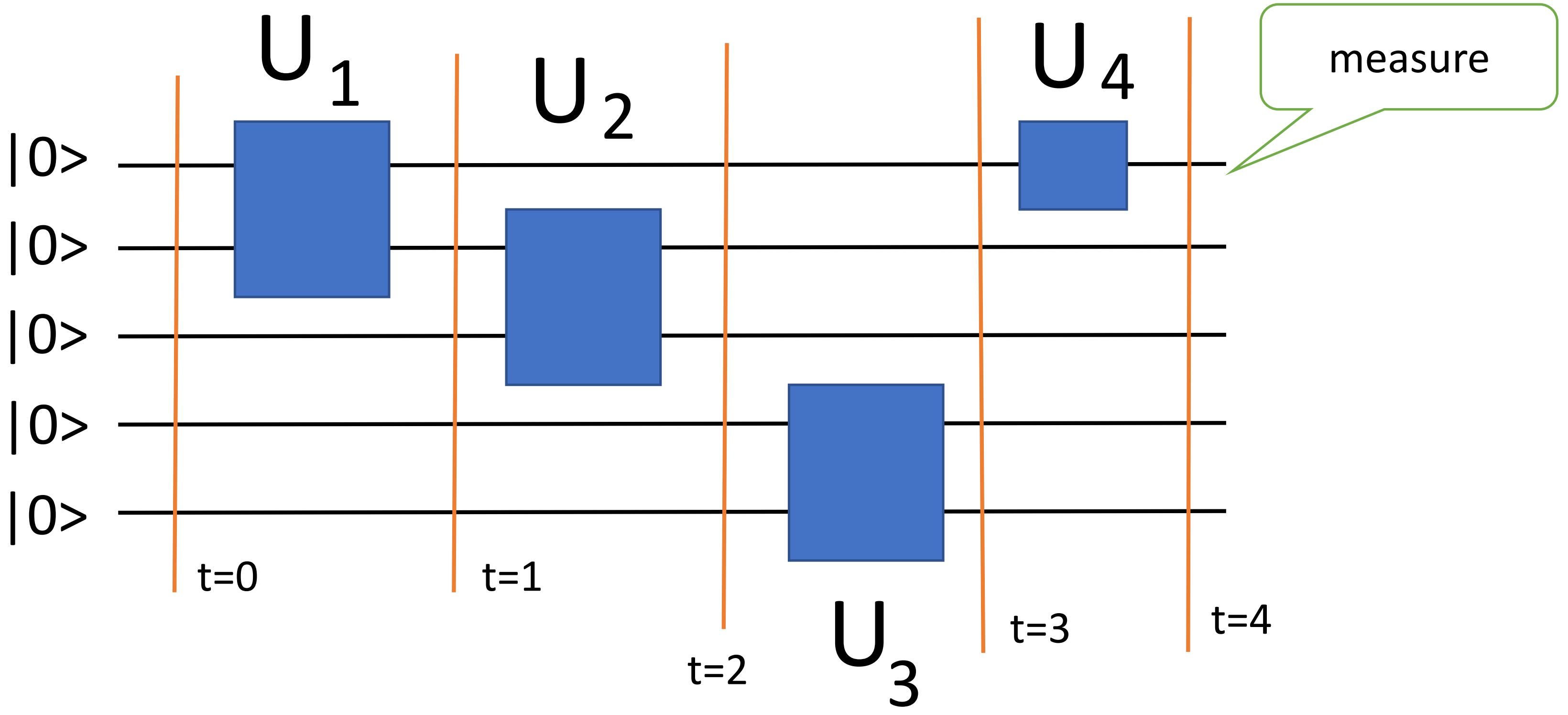
Wrong propagation → high energy penalty

$$H^1_{prop} = I \otimes |1\rangle\langle 1| + I \otimes |2\rangle\langle 2| - U_2 \otimes |2\rangle\langle 1| - U_2^\dagger \otimes |1\rangle\langle 2|$$

$$H^1_{prop}|\Psi\rangle = 0$$

In summary, the history state is the ground state of

$$H_{init} + \sum_{t=0}^{4} H^t_{prop}$$

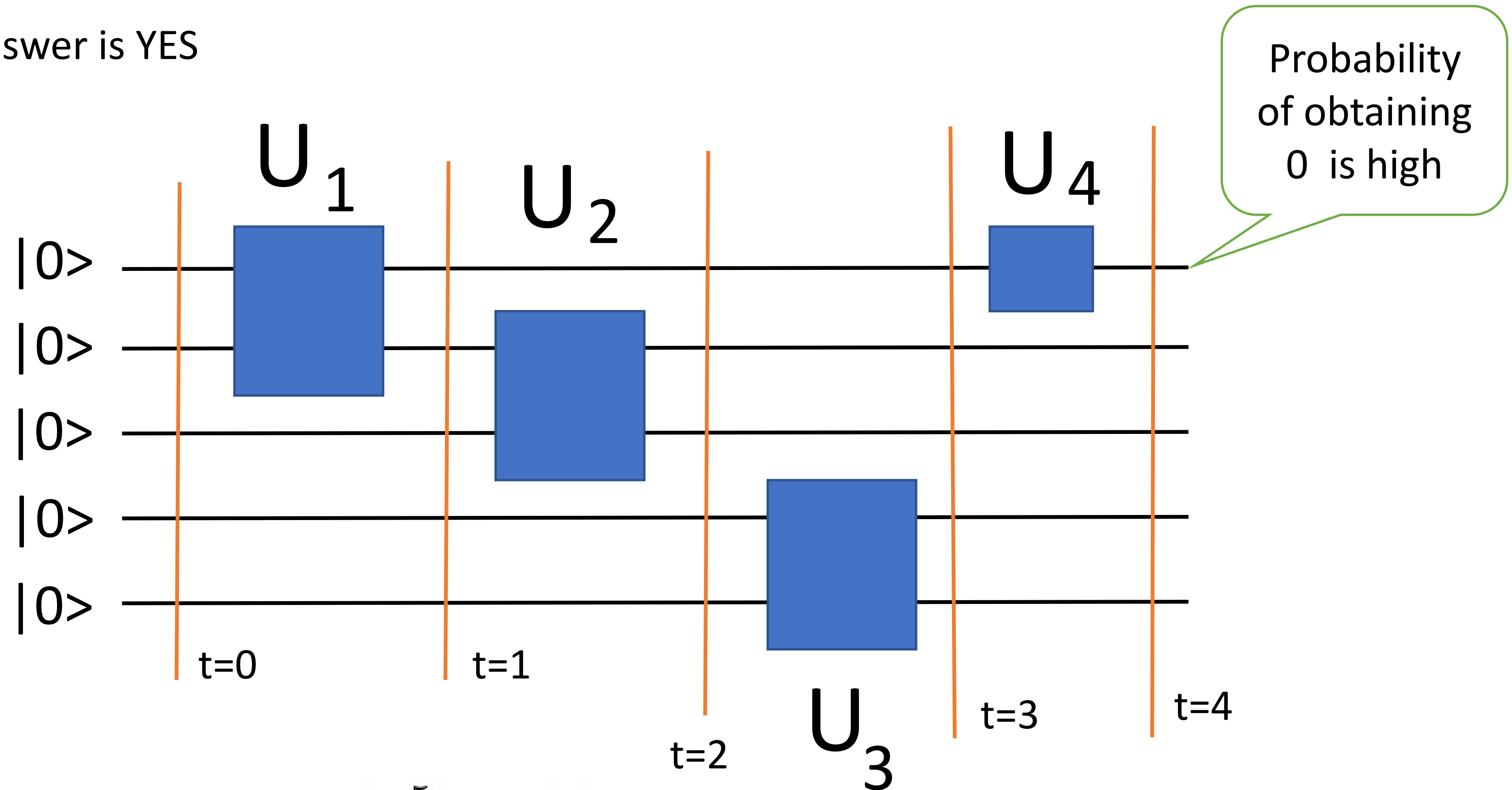



Theorem:

If the output is 0, then the history state is the almost-0 ground state of a local Hamiltonian

If the output is 1, the ground energy is high

If the answer is YES




$$
\begin{aligned}
|\Psi\rangle \;=\; & U_4U_3U_2U_1|0^5\rangle \otimes |4\rangle \\
& +U_3U_2U_1|0^5\rangle \otimes |3\rangle \\
& +U_2U_1|0^5\rangle \otimes |2\rangle \\
& +U_1|0^5\rangle \otimes |1\rangle \\
& +|0^5\rangle \otimes |0\rangle
\end{aligned}
$$

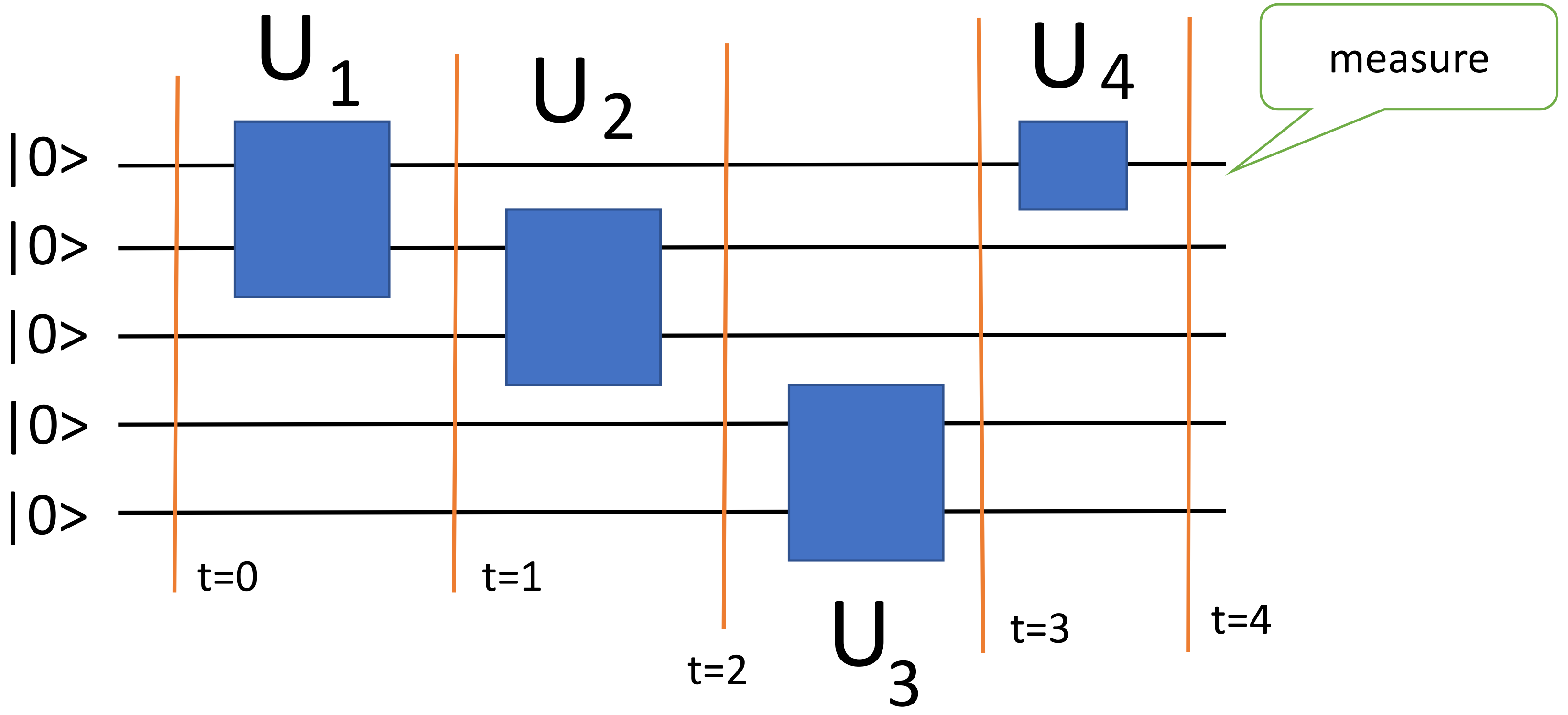
$$H_{out}|\Psi\rangle \simeq 0$$

$$H_{out} = (|1\rangle\langle 1| \otimes I^4) \otimes |4\rangle\langle 4|$$

If the answer is YES, the history state satisfies

$$H = \underbrace{H_{init}}_{\text{Energy is 0}} + \underbrace{H_{prop}}_{\text{Energy is 0}} + \underbrace{H_{out}}_{\text{Energy is almost 0}}$$

The total energy is almost 0




Theorem:

If the output is 0, then the history state is the almost-0 ground state of a local Hamiltonian

If the output is 1, the ground energy is high

If the answer is NO, for any state such that

$$(H_{init} + H_{prop})|\psi\rangle \simeq 0$$

The total energy is almost 1 because

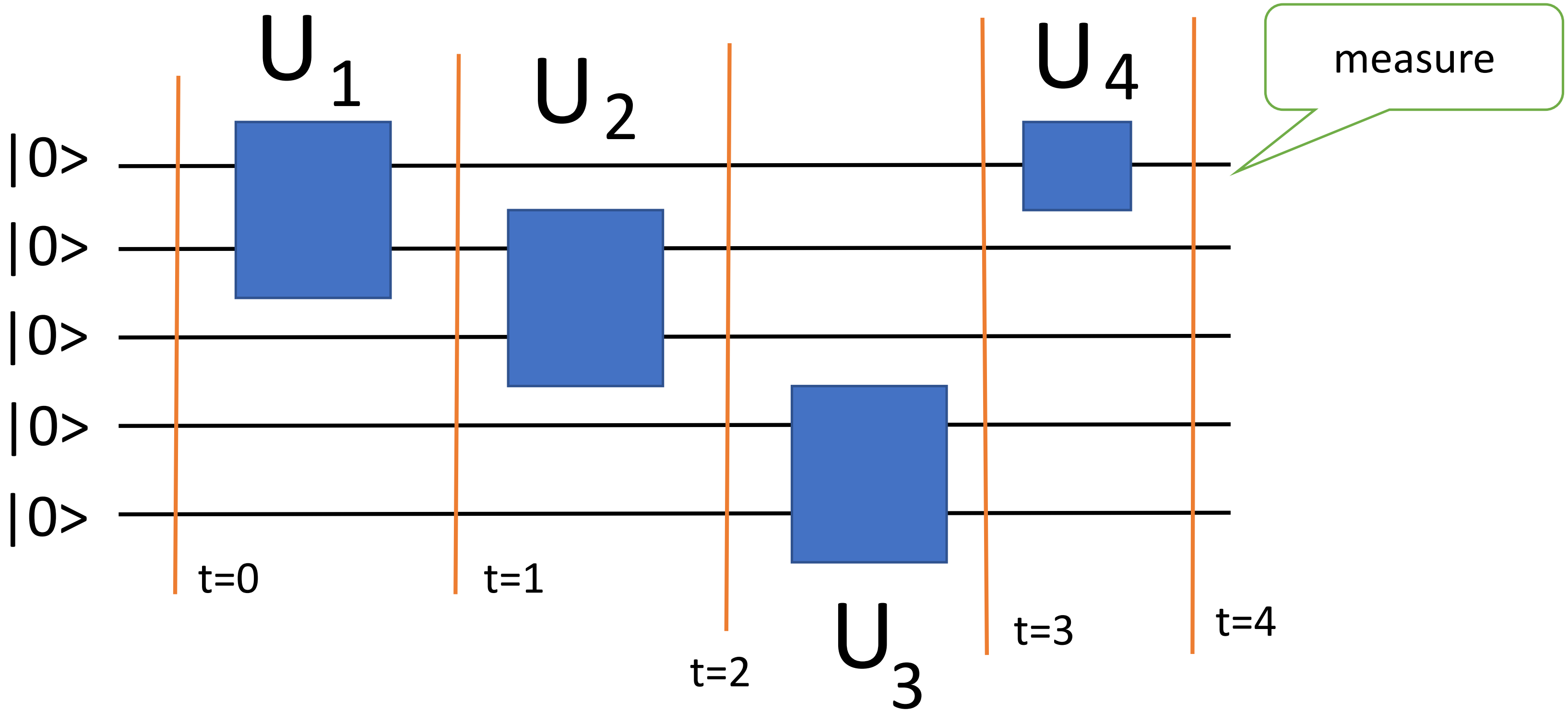
$$H = \underbrace{H_{init}}_{\text{Energy is almost 0}} + \underbrace{H_{prop}}_{\text{Energy is almost 0}} + \underbrace{H_{out}}_{\text{Energy is almost 1}}$$

If the answer is NO, for any state such that

$$H_{out}|\psi\rangle \simeq 0$$

The total energy is large because

$$H = \underbrace{H_{init}}_{\text{Energy is large}} + \underbrace{H_{prop}}_{\text{Energy is large}} + \underbrace{H_{out}}_{\text{Energy is almost 0}}$$




Theorem:

If the output is 0, then the history state is the almost-0 ground state of a local Hamiltonian

If the output is 1, the ground energy is high

$$H = H_{init} + H_{prop} + H_{out}$$

$$H_{out} = (|1\rangle\langle 1| \otimes I^4) \otimes |4\rangle\langle 4|$$

To encode time, logT qubits are necessary

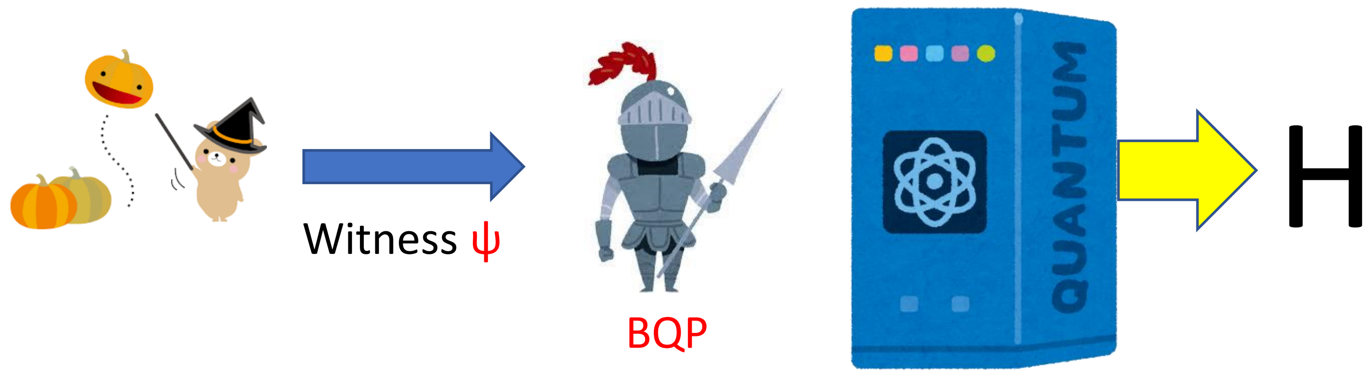
H is log-local, but by using the perturbation technique,

$$H = \sum_{i,j} \alpha_{i,j}(X_i X_j + Z_i Z_j)$$

We finally have 2-local XZ Hamiltonian!

# QMA

Problems that can be efficiently solved with ``quantum hint”



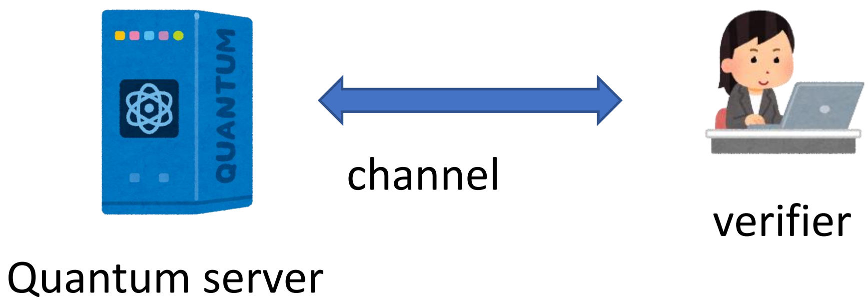

A problem is in QMA if and only if

For yes instance, there exists a witness s.t. the verifier accepts with high probability

For no instance, for any witness, the verifier accepts with small probability

# Application to verification of quantum computing

# Verification of quantum computing

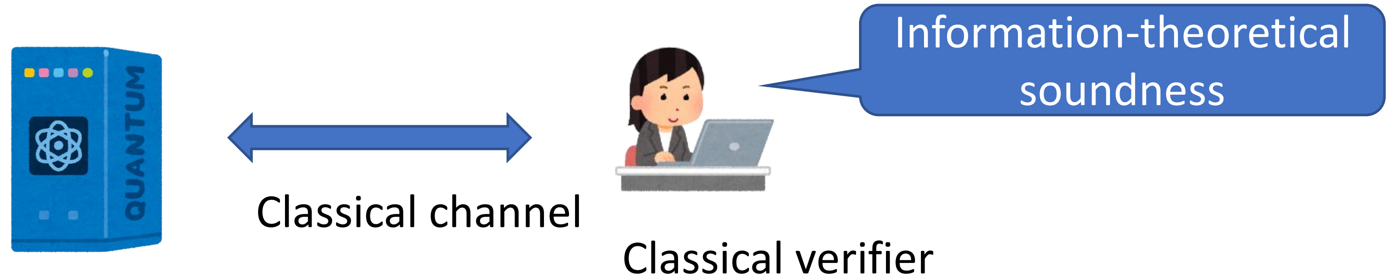



Can the classical verifier check the correctness of quantum computing?

（１） Security of cloud quantum computing

（２） Experimental realizations of quantum devices

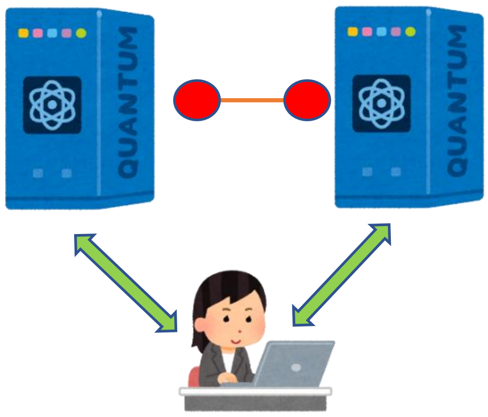
（３） Quantum interactive proof system




| | Information-theoretical soundness | Computational soundness |
|---|---|---|
| Classical verifier | Open | Mahadev protocol |
| Verifier who can measure/generate single-qubit states | FK protocol, posthoc protocol | |

Review: Gheorghiu et al. arXiv:1709.06984

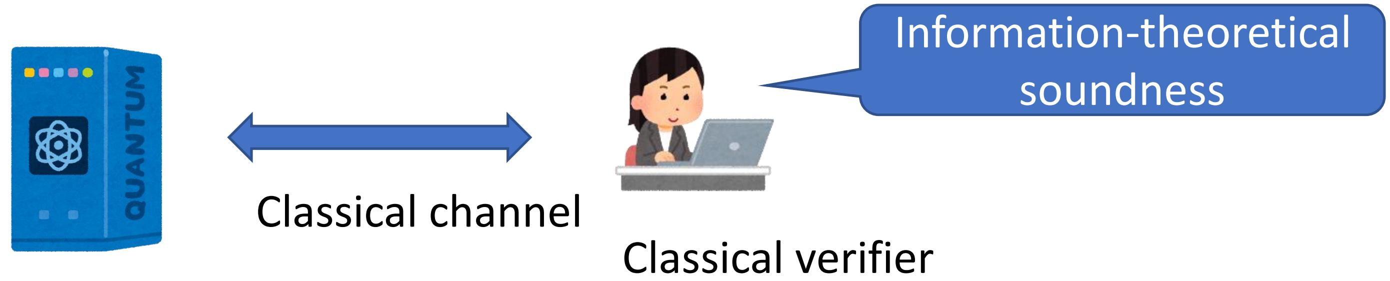
# Multi-prover setting




Provers who share entanglement but cannot communicate

Unger-Reichardt-Vazirani 2013

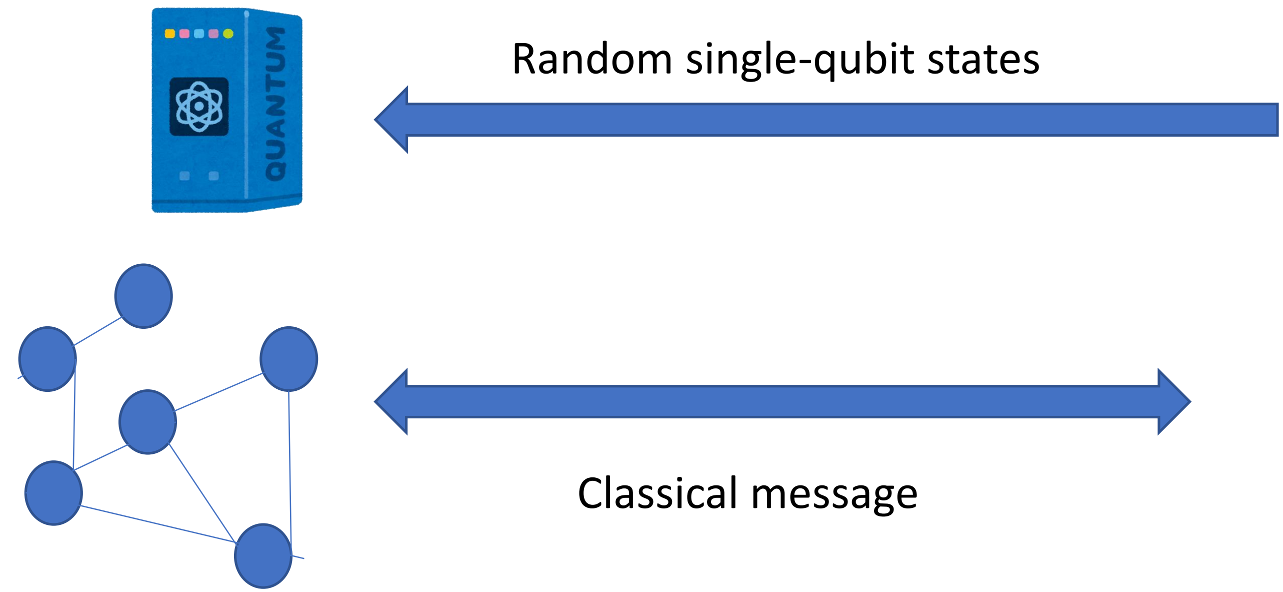
MIP*=RE [Ji, Natarajan, Vidick, Wright, Yuen 2020]




| | Information-theoretical soundness | Computational soundness |
|---|---|---|
| Classical verifier | Open | Mahadev protocol |
| Verifier who can measure/generate single-qubit states | FK protocol, posthoc protocol | |

Review: Gheorghiu et al. arXiv:1709.06984

# FK protocol

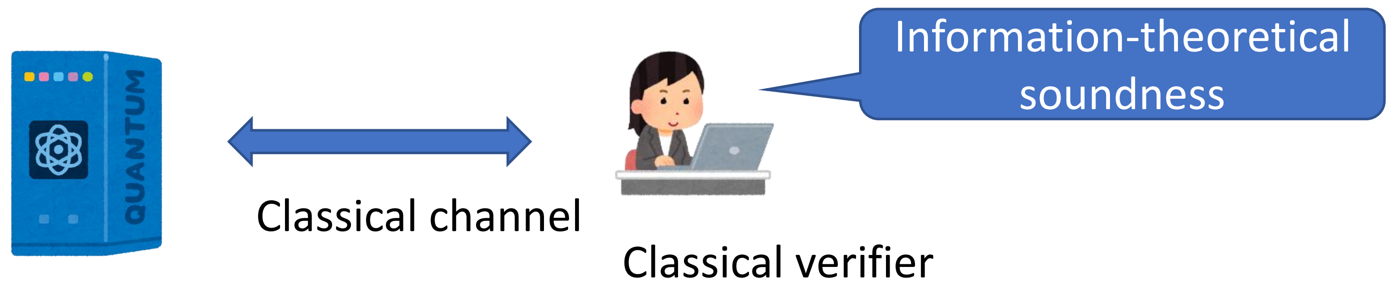




Graph state

Pro
（１） Information-theoretical soundness
（２） off-line quantum communication

Con
（１） Poly round
（２） Proof is complicated

Fitzsimons-Kashefi 2017

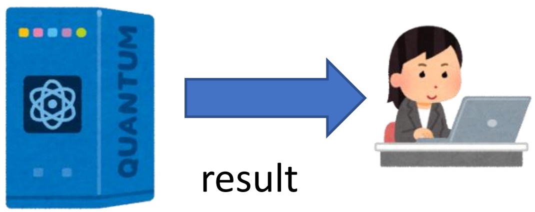



| | **Information-theoretical soundness** | **Computational soundness** |
|---|---|---|
| Classical verifier | Open | Mahadev protocol |
| Verifier who can measure/generate single-qubit states | FK protocol, posthoc protocol | |

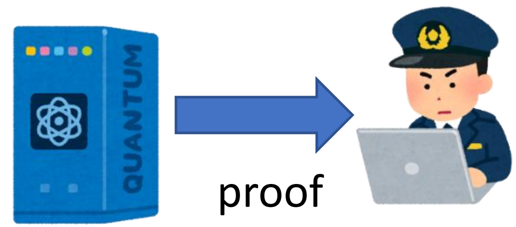
Review: Gheorghiu et al. arXiv:1709.06984

# Post hoc verification

Fitzsimons, Hajdusek, and TM, PRL 2018




10 years later..



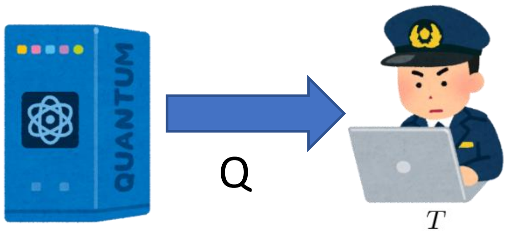

Correctness of QC can be checked in the post hoc way!

$$|\Psi\rangle = \sum_{t=0}^{T} U_t ... U_1 |0^n\rangle \otimes |t\rangle$$

Measurement of energy can be done with single-qubit measurements!
[TM, Nagaj, Schuch, PRA2016]

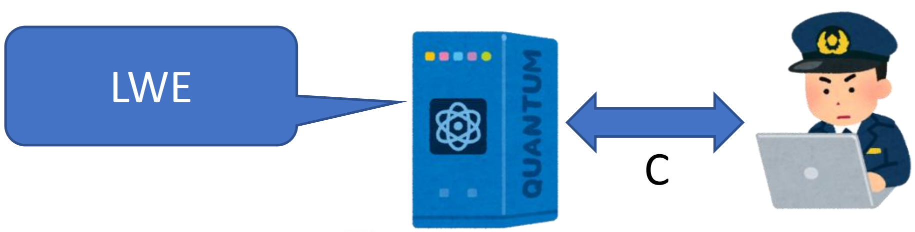
# Mahadev

Posthoc verification




$$|\Psi\rangle = \sum_{t=0}^{T} U_t \ldots U_1 |0^n\rangle \otimes |t\rangle$$

Classical verification (Mahadev 2018)




$$|\Psi\rangle = \sum_{t=0}^{T} U_t \ldots U_1 |0^n\rangle \otimes |t\rangle$$

Zero-knowledge (Broadbent, Grilo 2020)


$$|\Psi\rangle = \sum_{t=0}^{T} U_t \ldots U_1 |0^n\rangle \otimes |t\rangle$$

$$H = \sum_{i=1}^{m} H_i$$

Random local term

Open the commitment

Computationally hiding
Unconditionally binding

Computational ZK proof

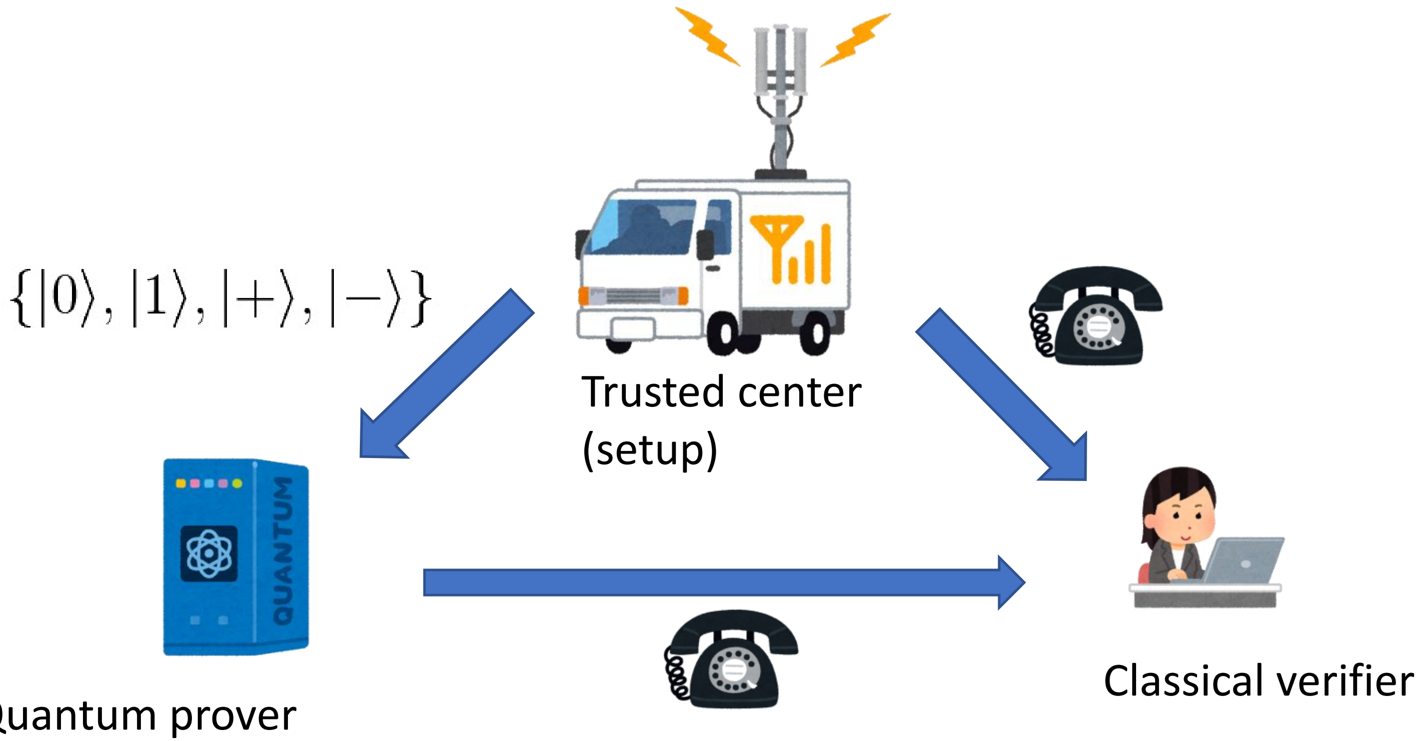
Computationally binding
Unconditionally hiding

Statistical ZK argument

Local simulatability: local system of encoded history state is classically computable [Grilo-Yuen-Solfstra 2019]

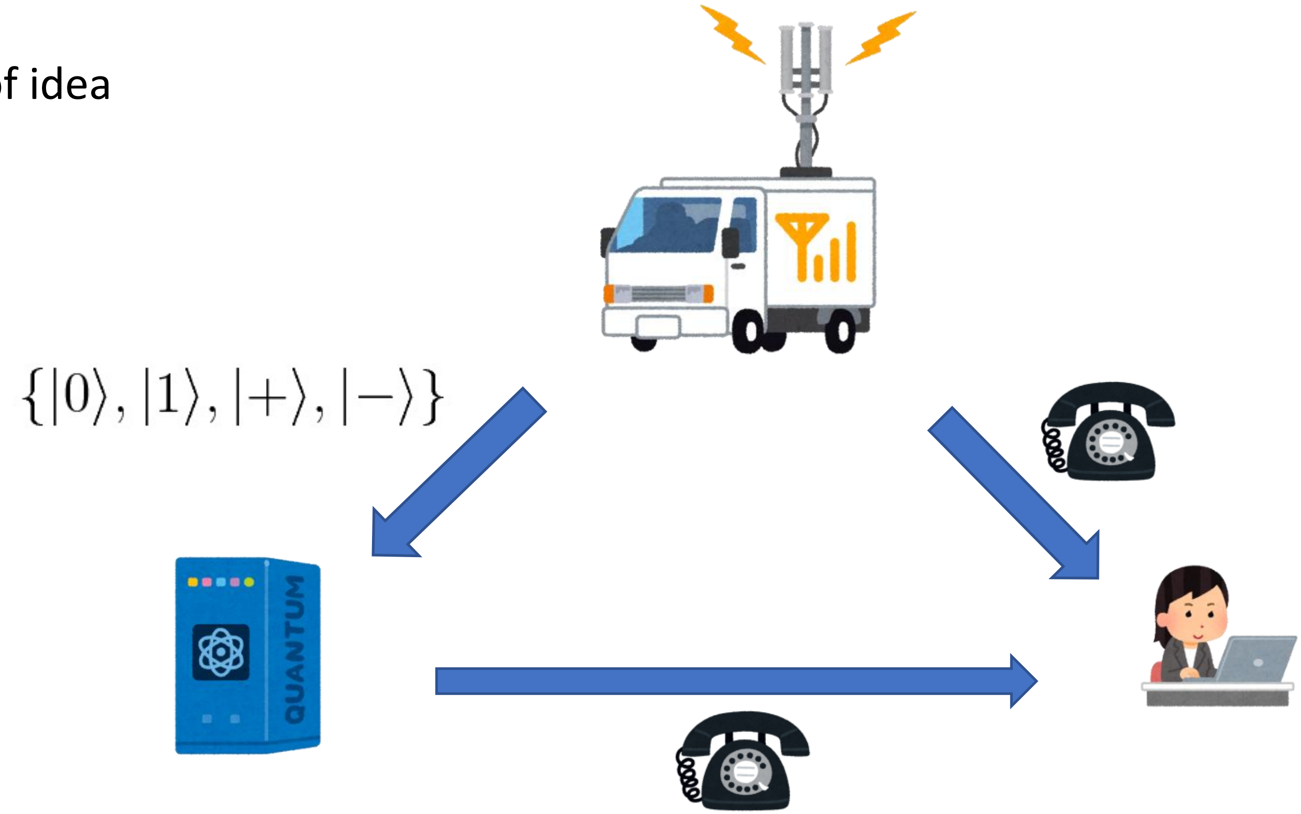
# Non-interactive proof

TM, arXiv:2003.10712

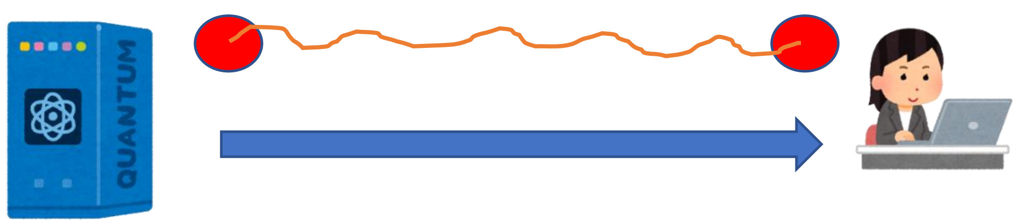



(1) Information theoretical soundness
(2) Classical verifier

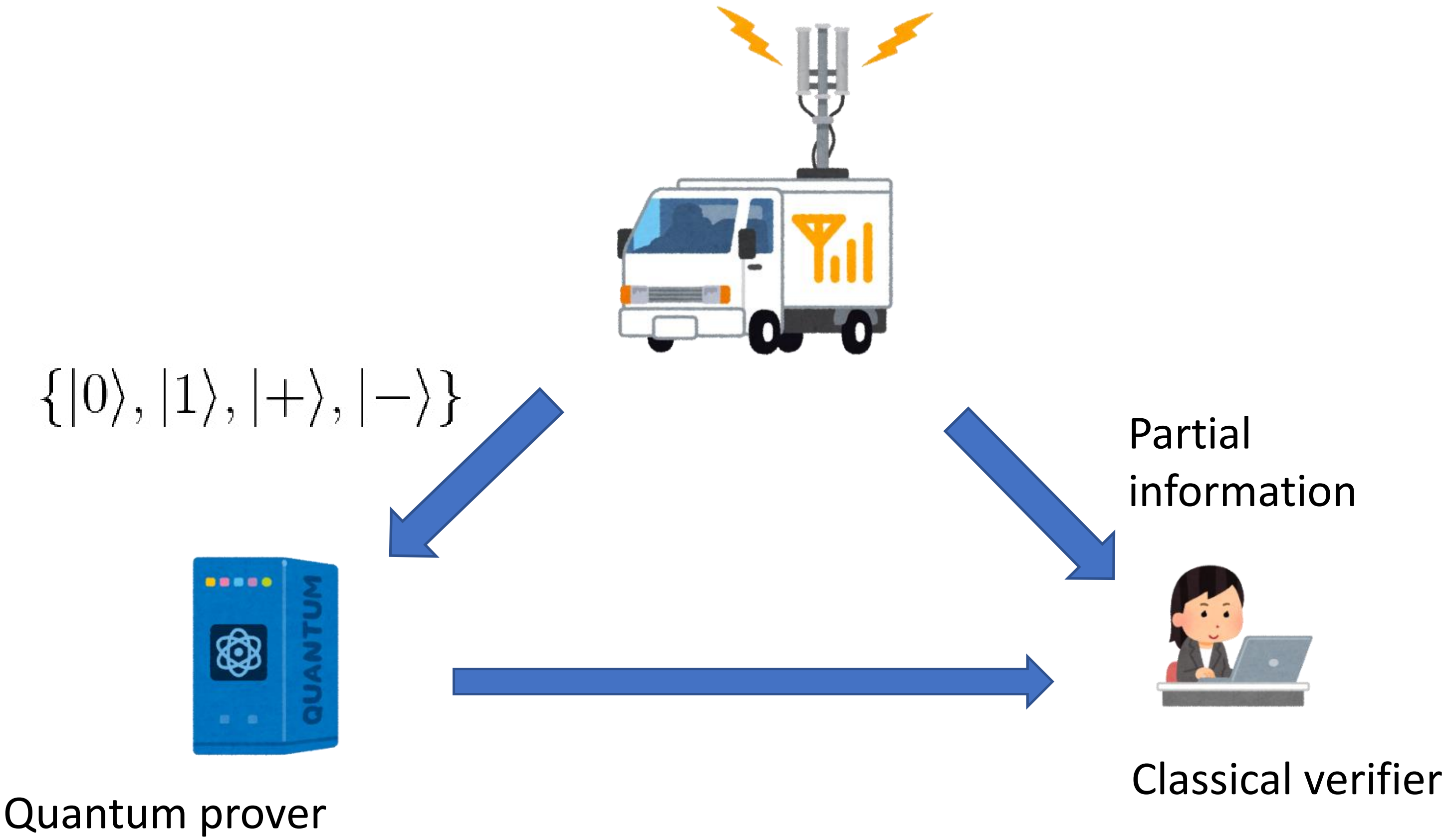
Proof idea




Virtual protocol



$$|\Psi\rangle = \sum_{t=0}^{T} U_t \ldots U_1 |0^n\rangle \otimes |t\rangle$$

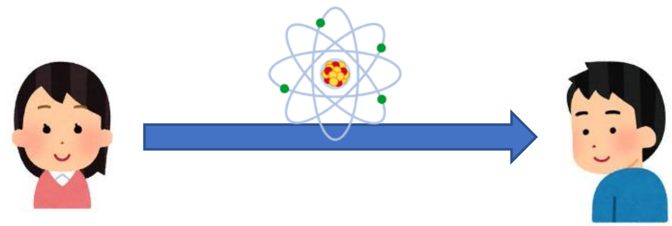



Statistical zero-knowledge proof!

Trusted center can be removed?

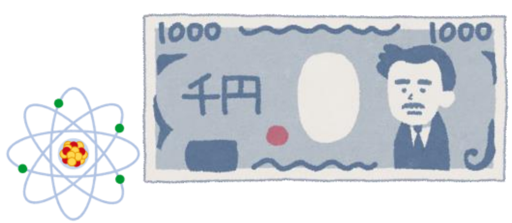
TM and Yamakawa, arXiv:2102.09149

# Sending quantum state is essential

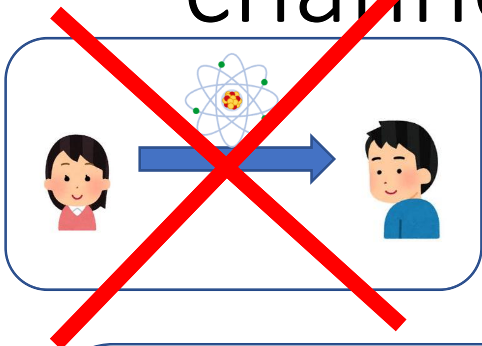


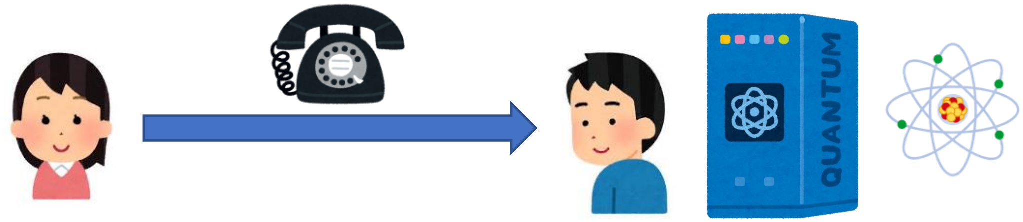
Uncertainty relation: QKD

No-cloning：Q money

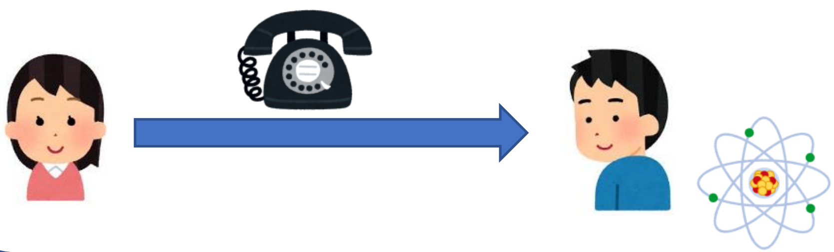


# Cannot be replaced with classical channel...

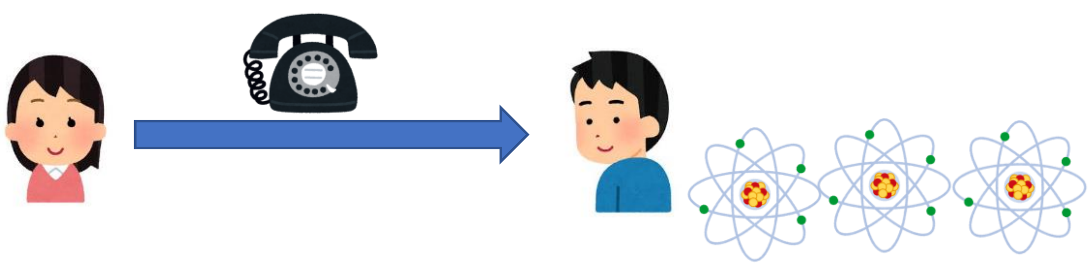





No uncertainty...



Cloning is possible...

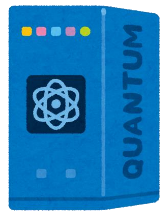


Folklore [See also Brakerski et al. , Mahadev FOCS2018]

f: 2-to-1 and claw-free

Finding $x_0, x_1$ $s.t.$ $f(x_0) = f(x_1)$ is difficult

f




$$\sum_x |x\rangle \otimes |0^m\rangle \rightarrow \sum_x |x\rangle \otimes |f(x)\rangle$$

measure

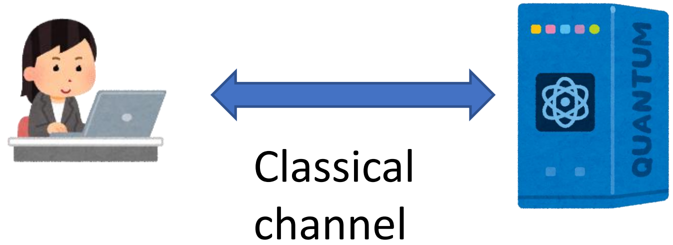
y

$$(|x_0\rangle + |x_1\rangle) \otimes |y\rangle$$

You cannot clone this state!

Unclonable state can be remotely generated with only classical channel!

# Remote state preparation

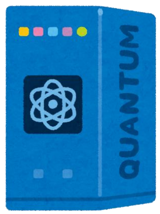



$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$

Blind RSP (Qfactory) [Cojocaru et al. 2019 ]

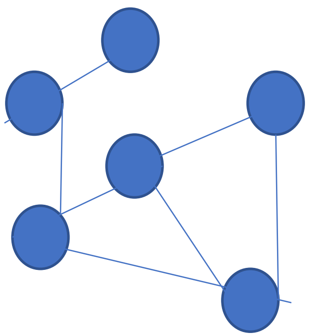
Verifiable RPS [Andru-Vidick 2019]

# FK protocol + RSP



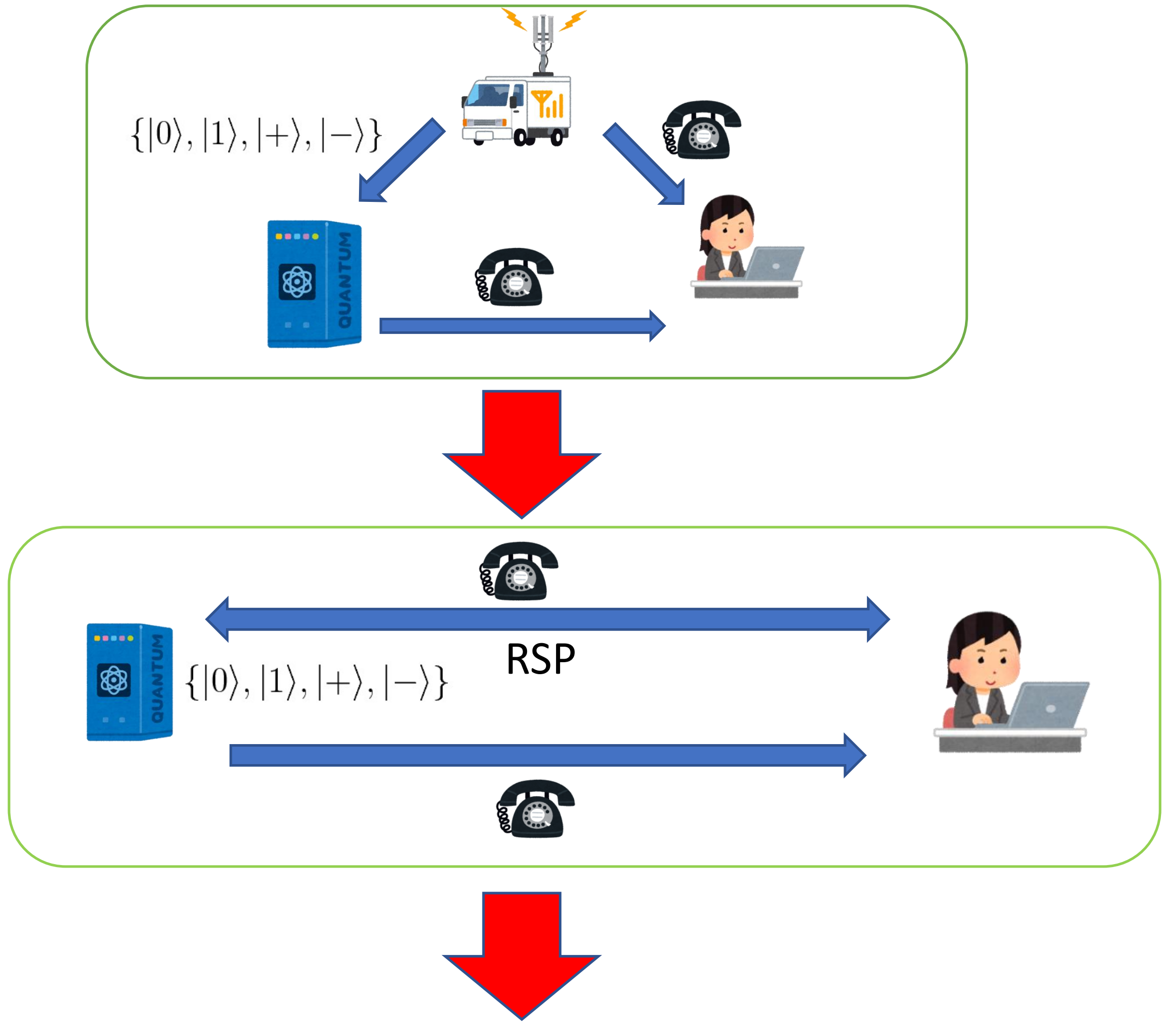

$e^{i\theta Z}|+\rangle$

RSP!



Classical communication

# Trusted center cannot be removed




# BQP $\subseteq$ MA

TM and Takeuchi, 2020

END