ブラインド量子計算と量子計算の検証

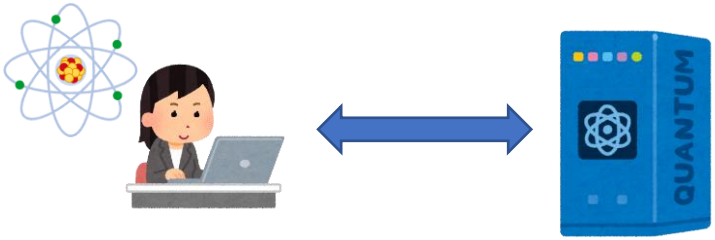
森前智行
（京都大学基礎物理学研究所）

45min

量子暗号

（1）量子鍵配送（QKD)：狭い意味で量子暗号といったらこれを指す。歴史が長く、かなり実用化されている

（2）量子暗号プロトコル：量子を用いて様々な暗号プロトコルを実現する研究。



量子マネー、量子認証、セキュアクラウド量子計算、量子ゼロ知識証明、

（3）耐量子暗号：古典の暗号の量子的攻撃に対する安全性を研究する。

計算能力の向上、重ね合わせ

内容

量子サーバー

通信路
（古典が望ましい）

利用者
（古典が望ましい）

（1）ブラインド量子計算：計算内容をサーバーに秘密にしたい

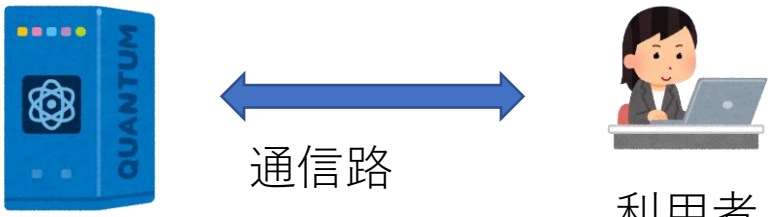
（2）量子計算の検証：計算内容が正しいかチェックしたい

（3）ゼロ知識：計算内容が正しいこと以外の情報は利用者には漏れない

（4）最近の話：Non-interactive ZK(NIZK)、Remote state preparation

ブラインド量子計算

ブラインド量子計算



プロトコルは以下を満たすときブラインドであるという。

Correctness：QPTサーバーがhonestなら、利用者は正しい結果を得る

Privacy: (QPT/unbounded)サーバーが何をしても利用者の入力、出力、プログラムはサーバーに漏れない

Review: Fitzsimons, nature partner journal Quantum Information 2017

ブラインド量子計算

最も理想的な状況

量子サーバー

古典通信路

古典利用者(BPP)

情報理論的安全性

	情報理論的安全性	計算量的安全性
完全古典利用者	Open No-go results [Aaronson et al. 2017, Morimae et al. 2018]	QFHE [Mahadev FOCS2018]
定数個の量子ビットの測定ができる利用者	Zhang arXiv:2004.12621 (Q random oracle)	
Poly(|C|)個の量子ビットの測定・生成ができる利用者	BFK 2009, MF 2014	

No-go results

古典通信

古典利用者(BPP)

可能か？Open problem。No-go resultsが知られている。

もしできたら、Permanentがある小さいサイズの回路で計算できてしまう
[Aaronson et al. arXiv:1704.08482]

もし定数ラウンドでできたら、多項式階層が第三レベルで崩壊してしまう
[Morimae et al. arXiv:1812.03703]

NPハード関数が情報理論的安全に委託できてしまうと多項式階層が第三レベルで崩壊 [Abadi-Feigenbaum-Kilian 1989]

ブラインド量子計算

最も理想的な状況

量子サーバー

古典通信路

古典利用者(BPP)

情報理論的安全性

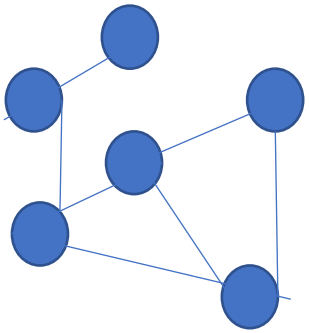
	情報理論的安全性	計算量的安全性
完全古典利用者	Open No-go results [Aaronson et al. 2017, Morimae et al. 2018]	QFHE [Mahadev FOCS2018]
定数個の量子ビットの測定ができる利用者	Zhang, arXiv:2004.12621 (Q random oracle)	
Poly(|C|)個の量子ビットの測定・生成ができる利用者	BFK 2009, MF 2014	

BFKプロトコル

量子ビット生成
能力必要

ランダムに回転した量子
ビットを送る

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



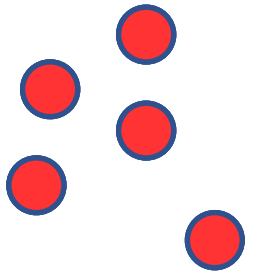
古典メッセージやり取り

グラフ状態作る

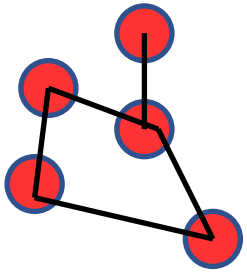
メリット
（１）情報理論的安全性
（２）量子preprocessing＋古典利用者

デメリット
（１）Polyラウンド
（２）証明が複雑

Broadbent-Fitzsimons-Kashefi FOCS2018



サーバーに送る



$\{e^{iZ\theta_j}|+\rangle\}_j$

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

測定角度の指示

$e^{iZ\delta_j}|\pm\rangle$ 基底で測定

$\delta_j = \phi_j - \theta_j$

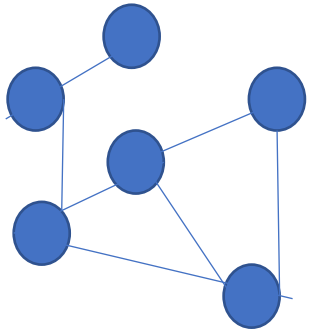
測定結果もらう

サーバーは $\{\phi_j\}_j$ を知ることができない！！

もっとちゃんとした厳密な証明が知りたい方は[Dunjko et al. ASIACRYPTO2014]を参照。

MFプロトコル

量子ビットを送る



グラフ状態作る

メリット
（１）情報理論的安全性(No-signaling)
（２）Singleラウンド
（３）証明が簡単

デメリット
（１）利用者は量子

TM and Fujii Physical Review A 87, 050301 (2013)

まとめ

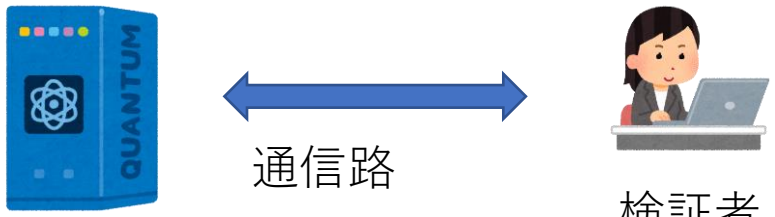
とりのぞける？

1にできる？

	利用者	ラウンド数	安全性
BFK 2009	量子Preprocessing＋古典	poly	情報理論的
MF 2013	量子	1	情報理論的
MahadevのQFHE	古典	2	LWE

量子計算の検証

量子計算の検証



サーバーが正しい量子計算をしているかチェックしたい(皮肉なジレンマ)

任意のBQP問題Lに対し、プロトコルは以下を満たすとき検証（Verification）であるという

Correctness: もし$x \in L$なら、QPT証明者がhonestな時、検証者は確率2/3 以上で受理

Soundness:もし$x \notin L$なら、(QPT/unbounded) な証明者がどんな動作をしても検証者は確率1/3以下で受理

Review: Gheorghiu et al. arXiv:1709.06984

量子計算の検証

最も理想的な状況

量子サーバー

古典通信路

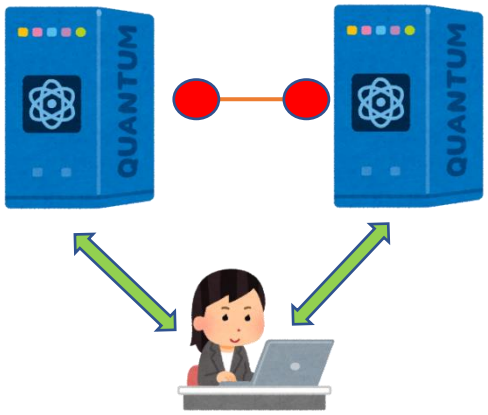
古典検証者(BPP)

情報理論的健全性

BQP⊆IP_BQPか？

	情報理論的健全性	計算量的健全性
完全古典検証者	Open No-go results [Folklore]	Mahadev 2018
多項式個の量子ビットの測定・生成ができる検証者	FK 2014, posthoc 2018	

Multi-prover プロトコル



エンタングルした量子状態を共有しているが、通信はできない証明者

Unger-Reichardt-Vazirani, Nature 2013

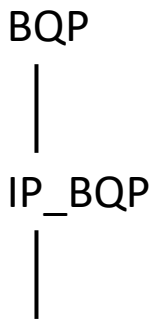
MIP*=RE 2020

No-go results

BQP⊆IP_BQPか？

（１）BQP⊆IP_BQP[const]⊆AM

（２）BQP≠IP_BQP→ BQP≠BPP



量子計算の検証

最も理想的な状況

量子サーバー

古典通信路

古典検証者(BPP)

情報理論的健全性

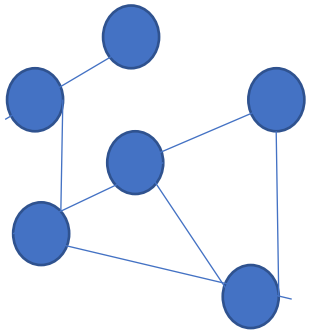
BQP⊆IP_BQPか？

	情報理論的健全性	計算量的健全性
完全古典検証者	Open No-go results [Folklore]	Mahadev 2018
多項式個の量子ビットの測定・生成ができる検証者	FK 2014, posthoc 2018	

FKプロトコル

量子ビット生成
能力必要

ランダムに回転した量子
ビットを送る



古典メッセージやり取り

グラフ状態作る

メリット
（１）情報理論的健全
（２）量子preprocessing+古典検証者

デメリット
（１）Polyラウンド
（２）証明が複雑

Fitzsimons-Kashefi, Physical Review A 96, 012303 (2017)

量子計算の検証

最も理想的な状況

量子サーバー

古典通信路

古典検証者(BPP)

情報理論的健全性

BQP⊆IP_BQPか？

	情報理論的健全性	計算量的健全性
完全古典検証者	Open No-go results [Folklore]	Mahadev 2018
多項式個の量子ビットの測定・生成ができる検証者	FK 2014, posthoc 2018	

Local Hamiltonian問題

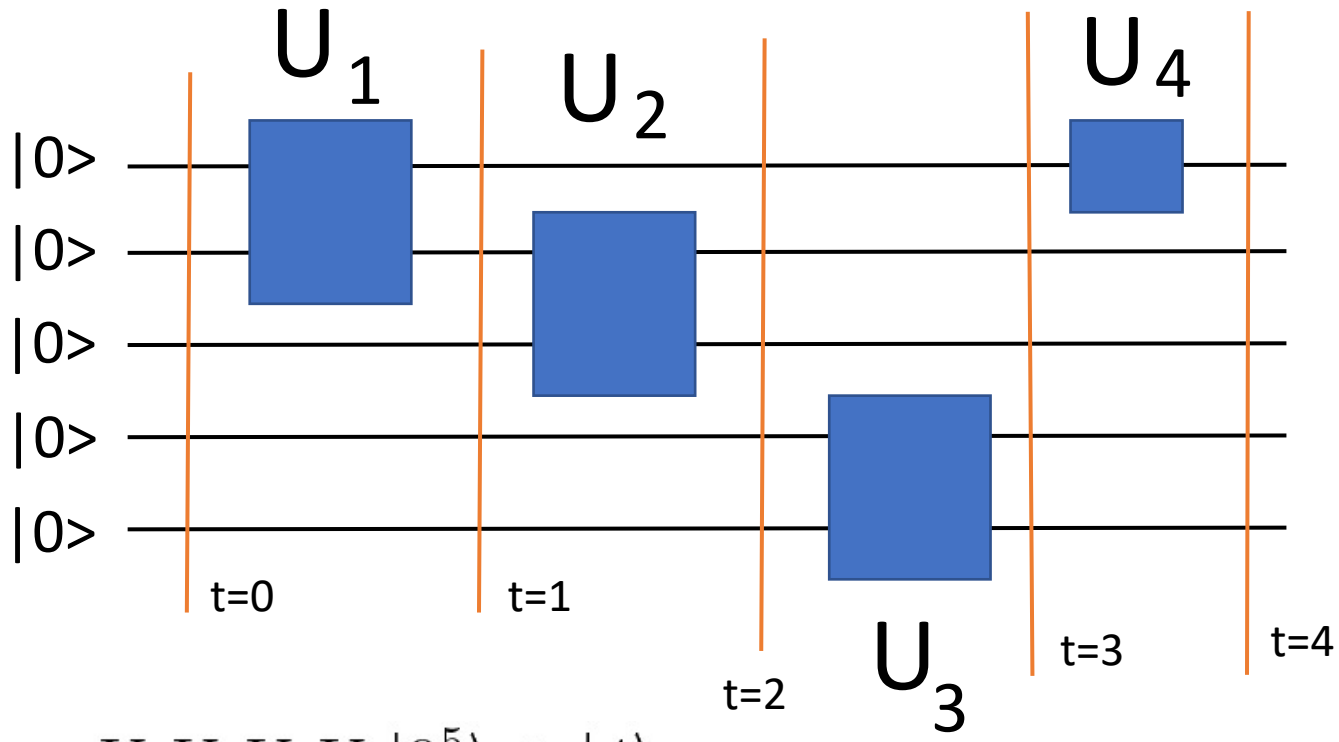
Local Hamiltonian問題：

与えられたエルミート共役行列Hの最小固有値はaより小さいか、bより大きいか？

NP完全問題であるSAT問題の量子版であり、QMA完全（QMAはNPの量子版）

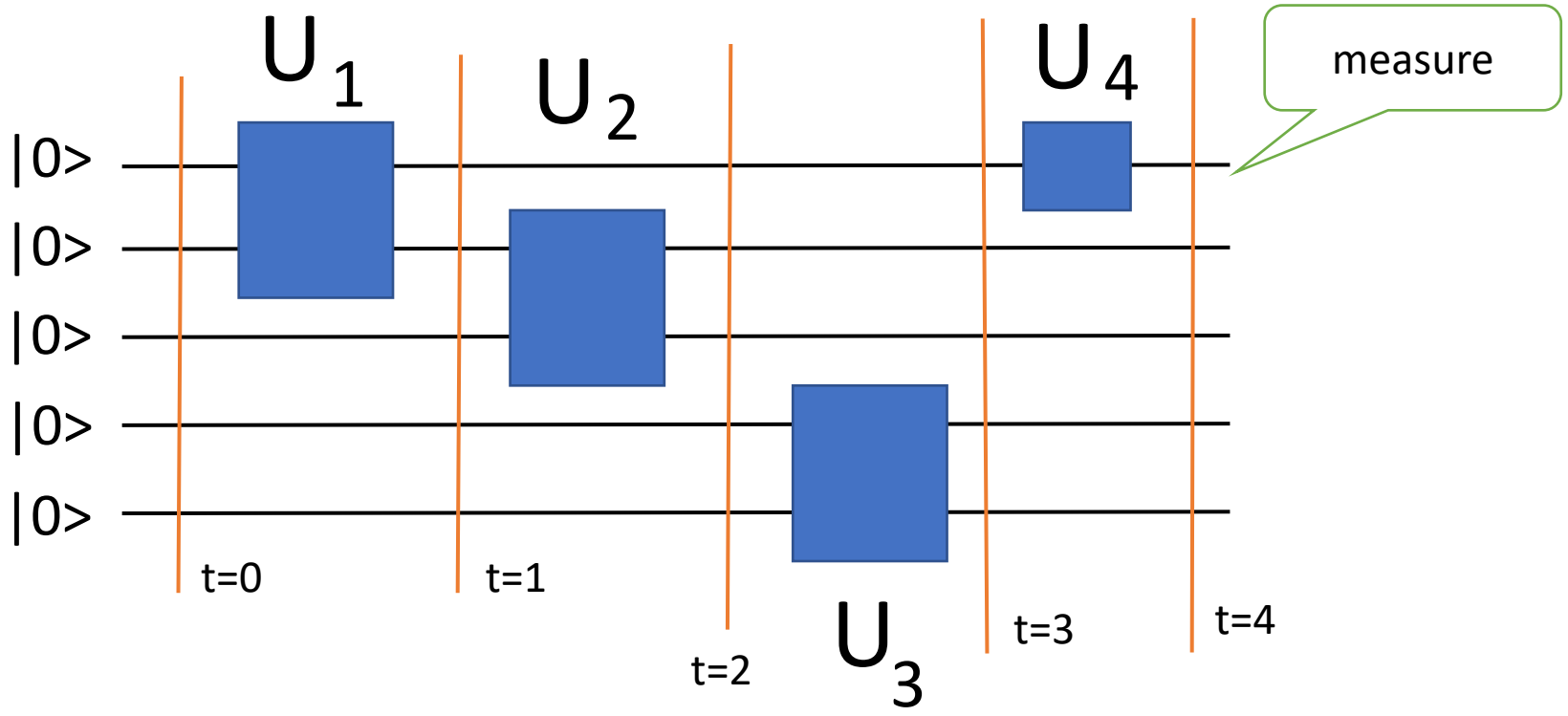
Text book: Vidick-Watrous, quantum proofs, arXiv:1610.01664

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]



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

History state is the ground state of local Hamiltonian!

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

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

Checking whether the initial state is correct

Wrong state-> high energy penalty

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

$$
\begin{aligned}
|\Psi\rangle \quad = \quad & U_4 U_3 U_2 U_1 |0^5\rangle \otimes |4\rangle \\
& + U_3 U_2 U_1 |0^5\rangle \otimes |3\rangle \\
& + U_2 U_1 |0^5\rangle \otimes |2\rangle \\
& + U_1 |0^5\rangle \otimes |1\rangle \\
& + |0^5\rangle \otimes |0\rangle
\end{aligned}
$$

Checking whether propagation is correct

Wrong propagation → high energy penalty

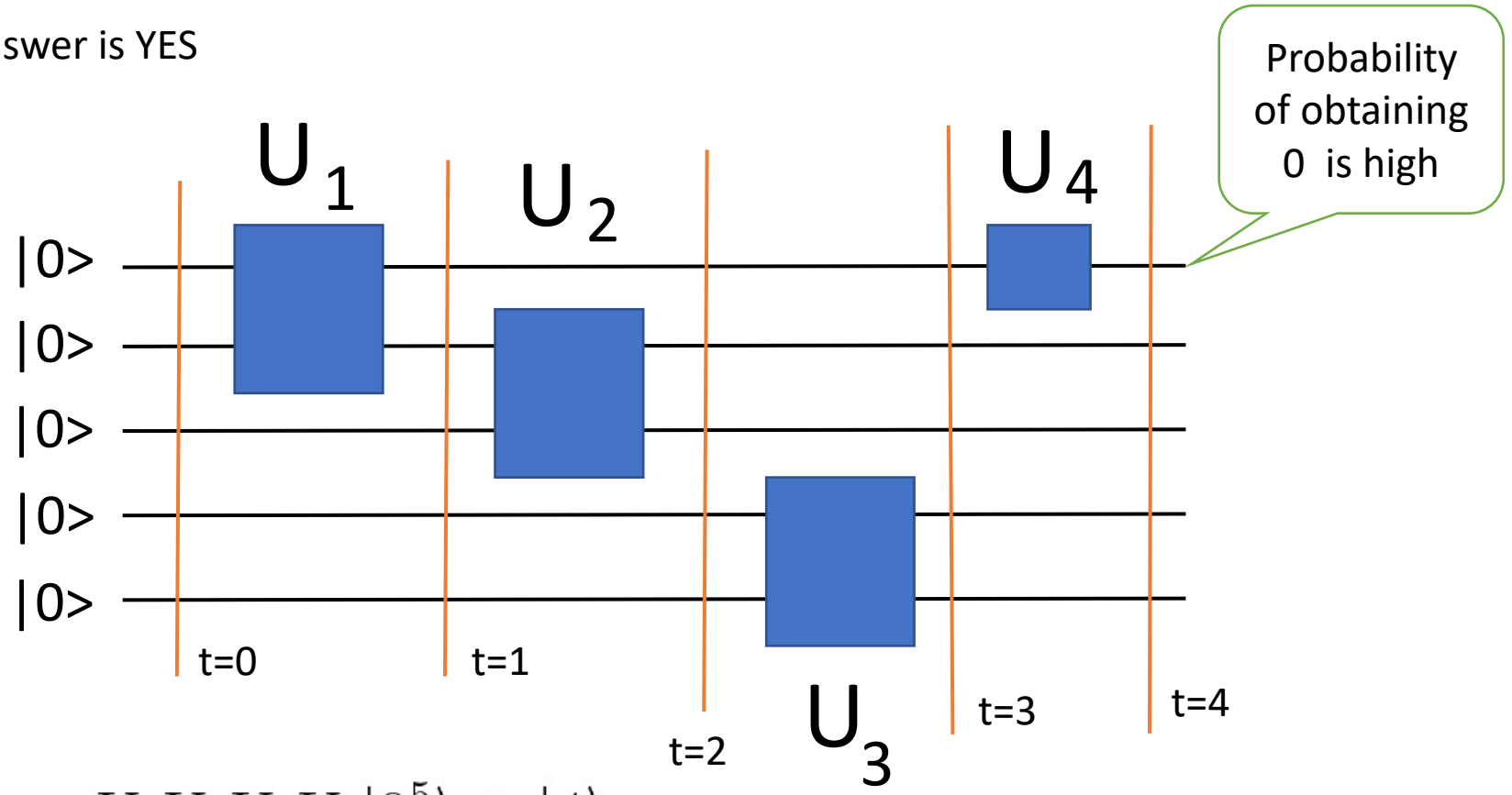
$$H^1_{prop} = I \otimes |1\rangle\langle 1| + I \otimes |2\rangle\langle 2| - U_2 \otimes |2\rangle\langle 1| - U_2^\dagger \otimes |1\rangle\langle 2|$$

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

In summary, the history state is the ground state of

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

If the answer is YES



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

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

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

If the answer is YES, and if the honest server sends the history state

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

Energy is 0

Energy is 0

Energy is almost 0

The total energy is almost 0

If the answer is NO, and if the malicious server sends the state such that

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

The total energy is almost 1 because

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

Energy is almost 0

Energy is almost 0

Energy is almost 1

If the answer is NO, and if the malicious server sends the state such that

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

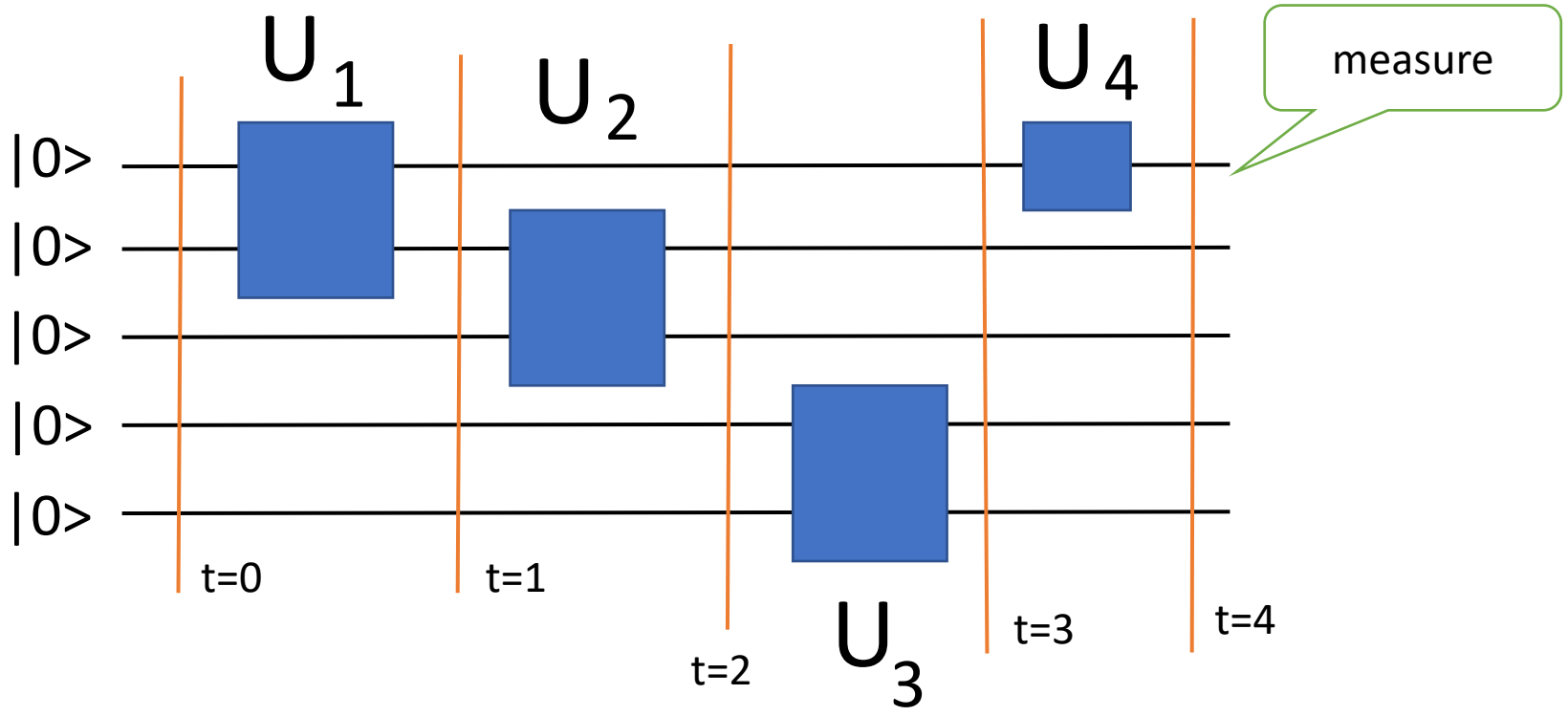
The total energy is large because

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

Energy is large

Energy is large

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

Post hoc verification

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

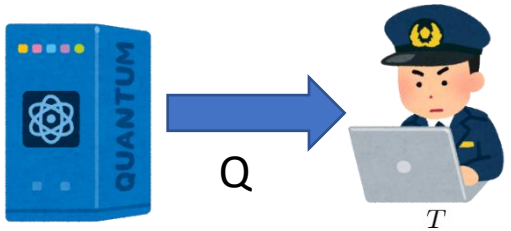
$$|\Psi\rangle = \sum_{t=0}^{T} U_t \ldots U_1 |0^n\rangle \otimes |t\rangle$$

Fitzsimons, Hajdusek, and TM, Physical Review Letters 120, 040501 (2018)

Measurement of energy can be done with single-qubit measurements!
[TM, Nagaj, Schuch, Physical Review A 93, 022326 (2016)]

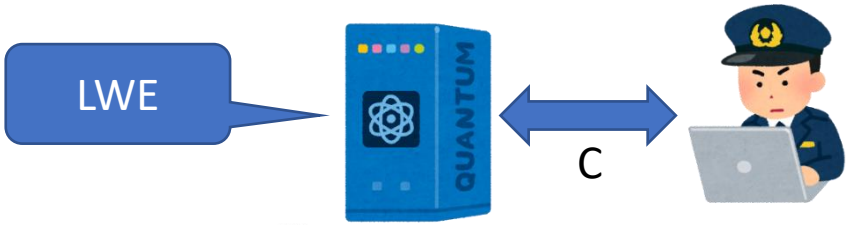
Mahadev

posthoc



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

Classical verification (Mahadev)



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

Mahadev FOCS 2018

まとめ

できた [TM and Yamakawa 2020]

とりのぞける？

1にできる？

	検証者	ラウンド数	健全性
FK 2017	量子Preprocessing＋古典	poly	情報理論的
Posthoc 2018	量子	1	情報理論的
Mahadev 2018	古典	Poly (4, 1)	LWE

ゼロ知識証明

Bit commitment

おまえが明日の昼飯に何を食うかあててやる

紙に書いて第三者に渡せ

Binding:封筒の中身を後で変えれない
Hiding: 封筒の中身を見れない

Zero-knowledge for QMA [Broadbent-Grilo FOCS 2020]

$$\sum_t U_t ... U_0(|w\rangle \otimes |0^k\rangle) \otimes |t\rangle$$

Random local term

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

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, FOCS2019]

Non-interactive proof, RSP

まとめ

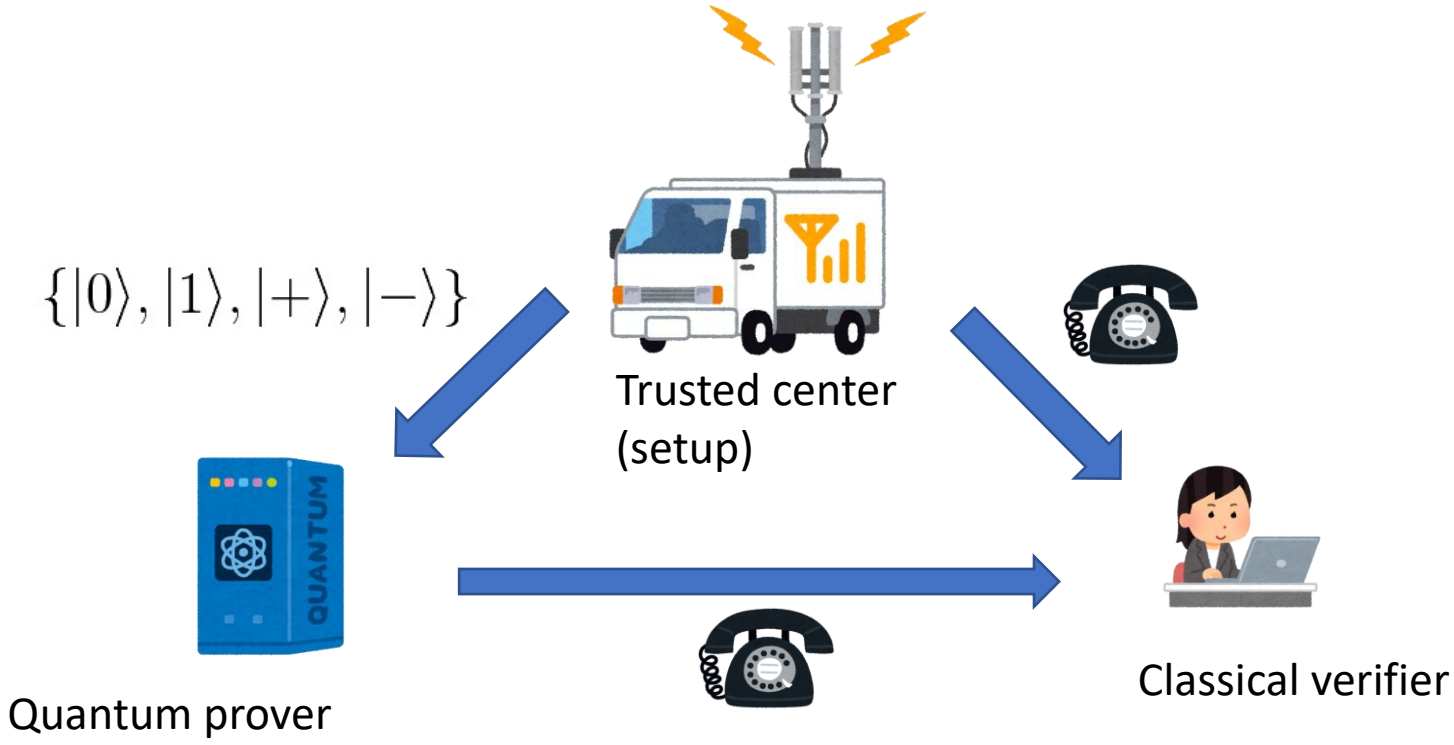
できた [TM and Yamakawa 2020]

とりのぞける？

1にできる？

	検証者	ラウンド数	健全性
FK 2017	量子Preprocessing＋古典	poly	情報理論的
Posthoc 2018	量子	1	情報理論的
Mahadev 2018	古典	Poly (4, 1)	LWE

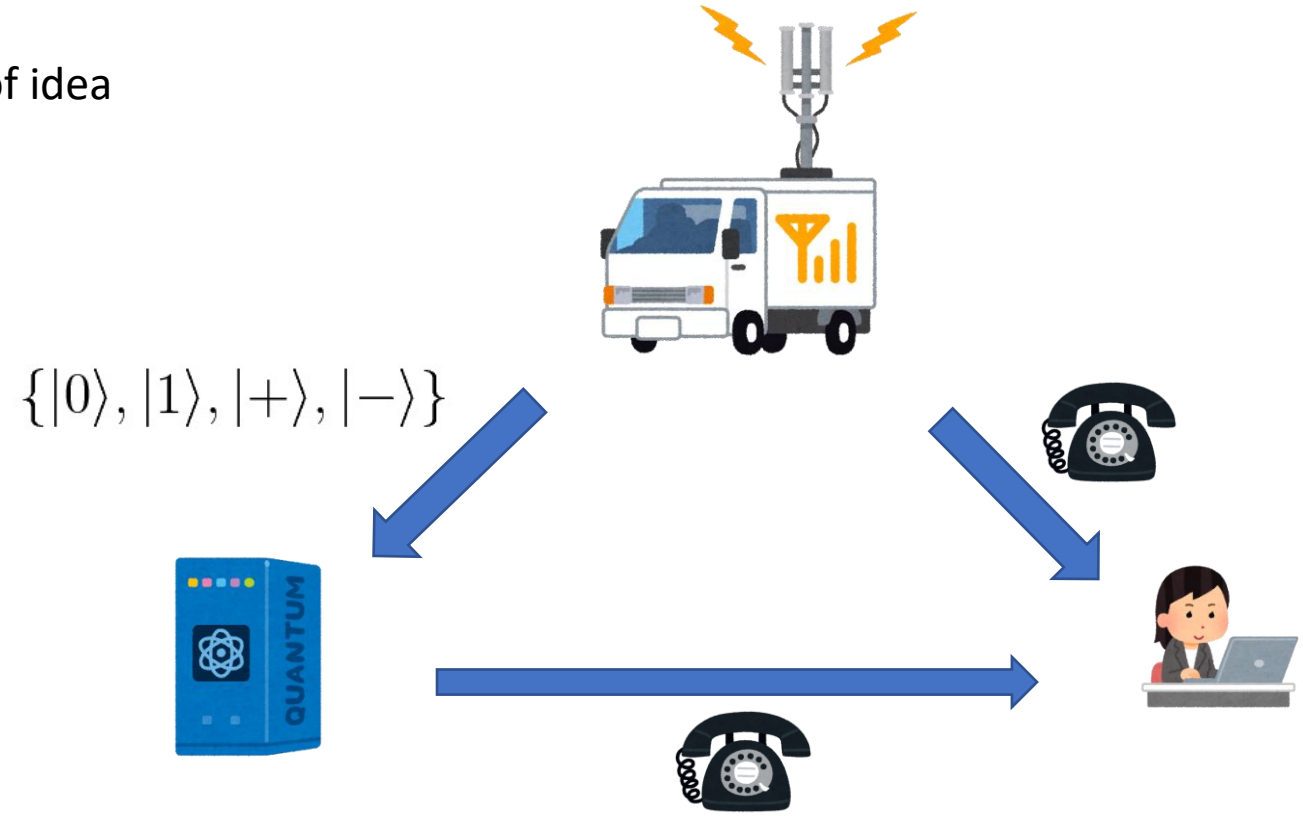
Non-interactive proof



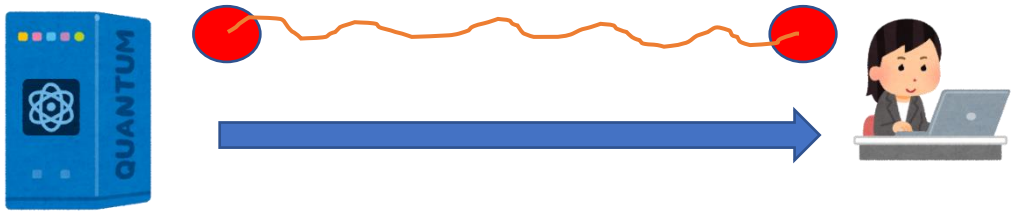
(1) 情報理論的健全性
(2) 完全古典検証者＋Setup

TM and Yamakawa, arXiv:2102.09149

Proof idea



Virtual protocol



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

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

Partial information

Quantum prover

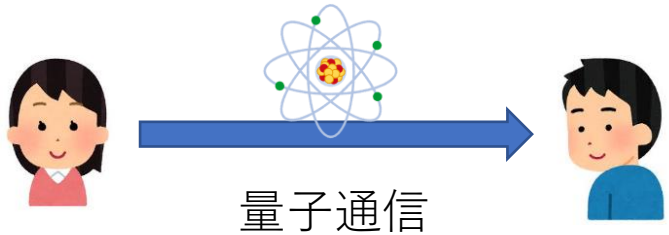
Classical verifier

NIZK with statistical soundness and zero-knowledge

Trusted centerを取り除けないの？

TM and Yamakawa, arXiv:2102.09149

量子暗号プロトコルのキモ



不確定性原理：量子状態は測定すると壊れてしまう

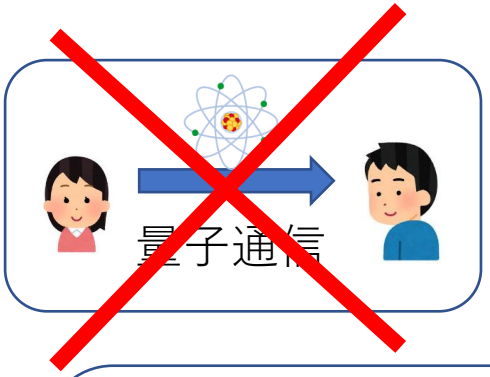
応用：量子鍵配送（盗聴不可能な通信）

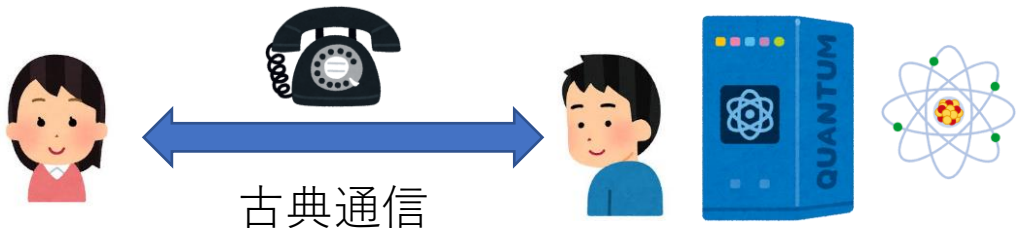
量子状態を送ることにより情報理論的安全性を達成

No-cloning：量子状態は複製できない

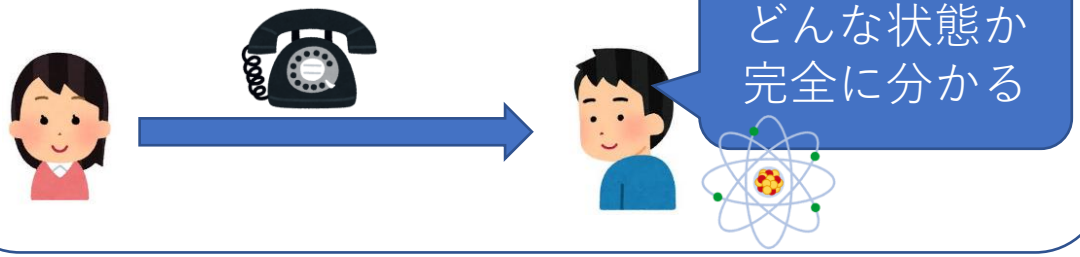
応用：量子マネー

古典通信ではダメそう。。。



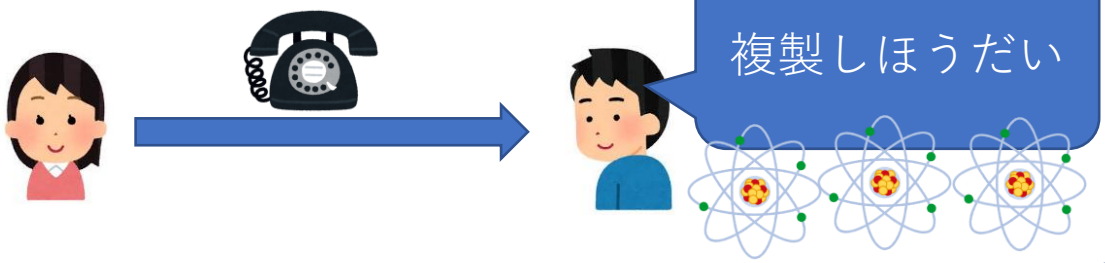


不確定性原理：量子状態は測定すると壊れてしまう



古典通信路
ではダメ！

No-cloning：量子状態は複製できない



Folklore. See also [Berkerski et al. FOCS2018, 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

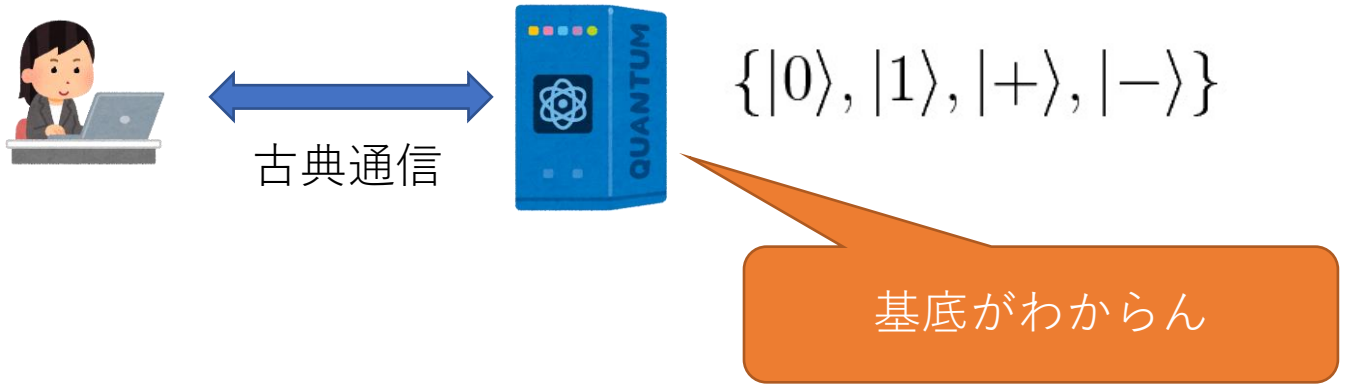
y

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

You cannot clone this state!

古典通信のみでクローンできない量子状態を作らせることができた！

Remote state preparation



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

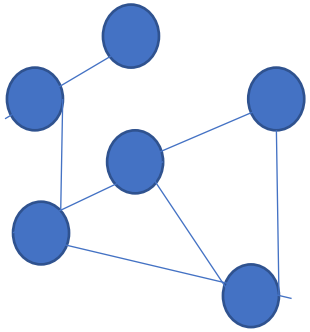
BFKプロトコル＋QFACTORY

ランダムに回転した量子ビットを送る

量子ビット生成能力必要

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

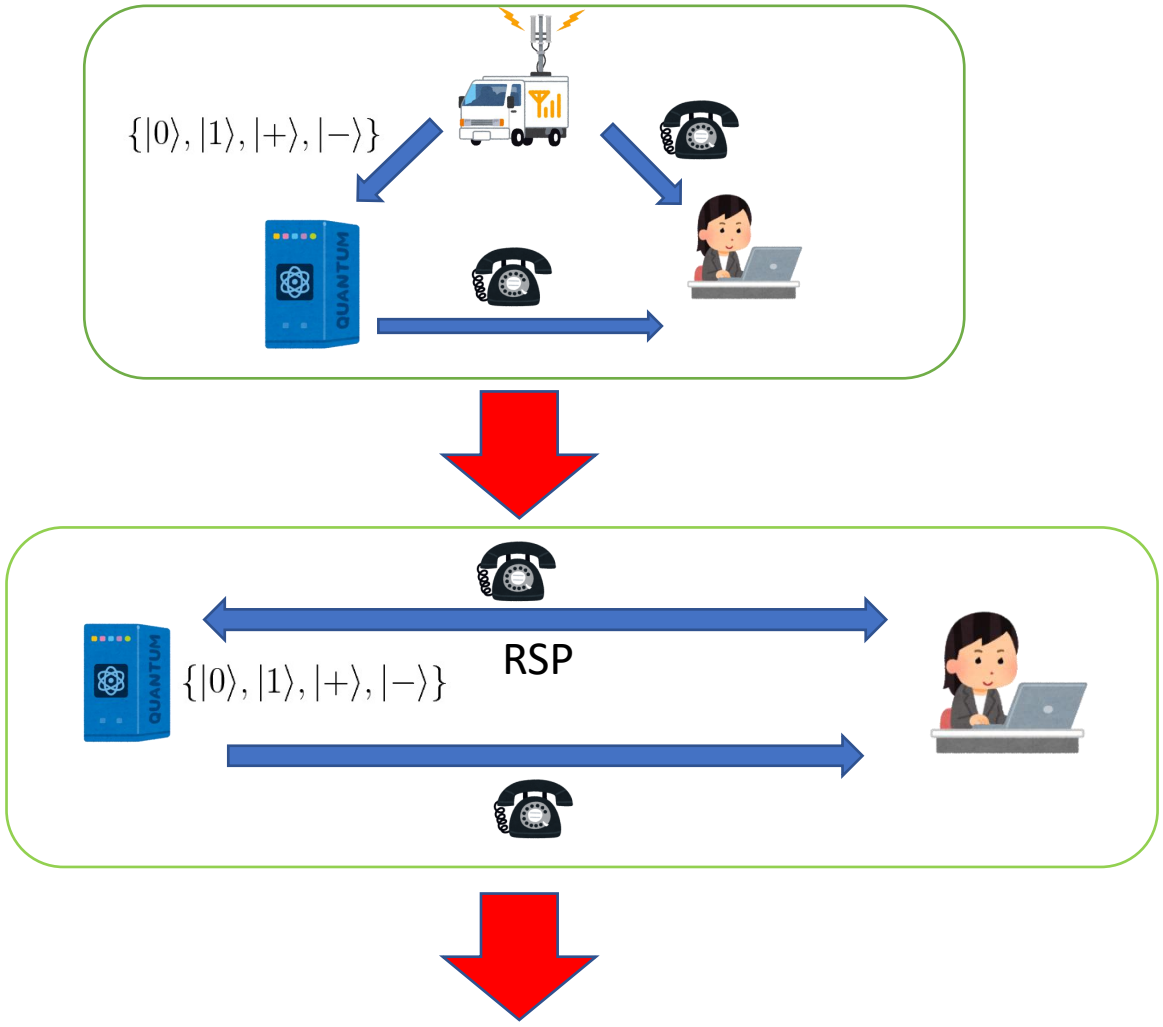
Qfactoryに置き換えられる！



古典メッセージやり取り

グラフ状態作る

Trusted center cannot be removed



$$\mathrm{BQP} \subseteq \mathrm{MA}$$

TM and Takeuchi, arXiv:2008.05033

END