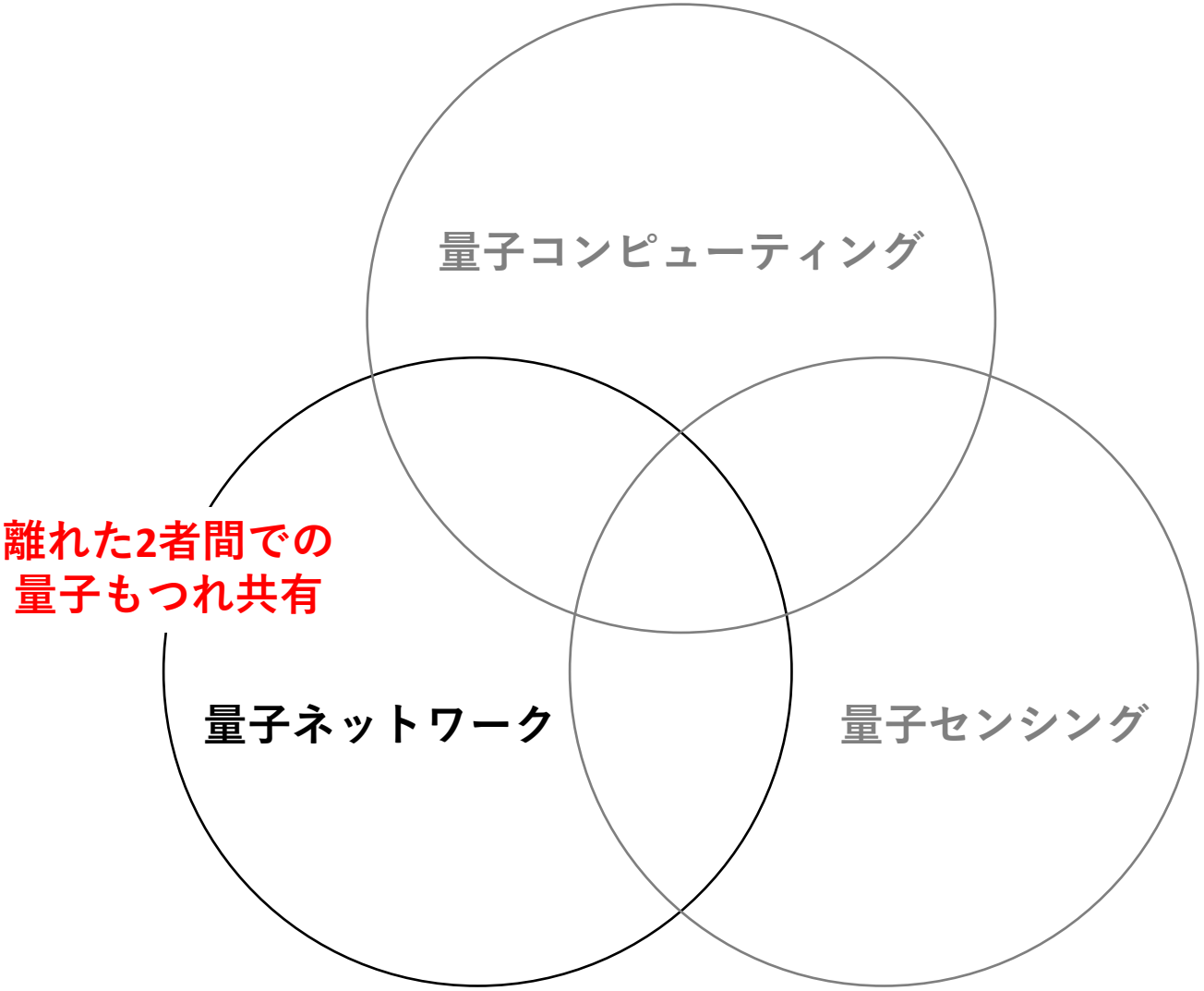
量子ネットワーク

阿部 英介
理化学研究所 創発物性科学研究センター

応用物理特別講義A
2020年度春学期後半 金曜4限@~~14-202~~オンライン講義

量子技術



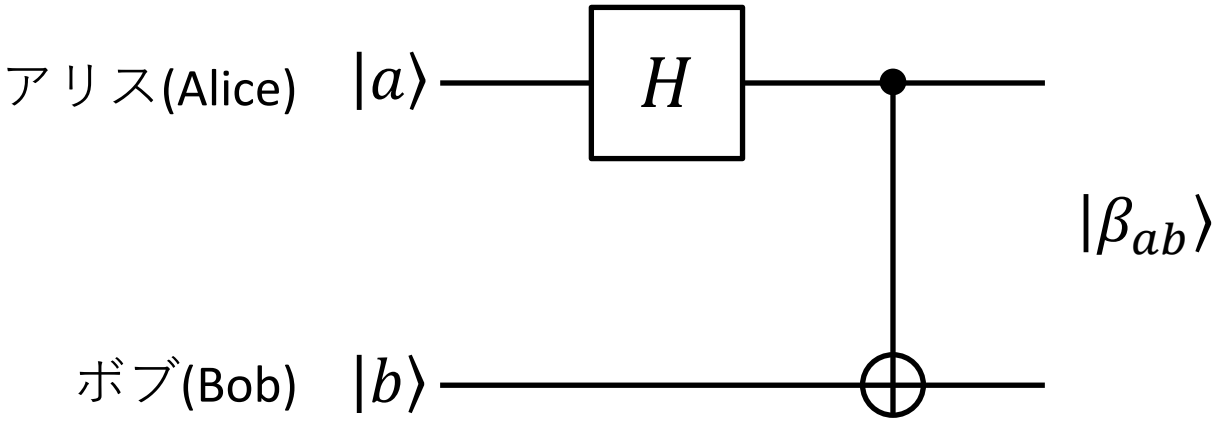
講義内容

- **量子もつれとベルの不等式**
- **量子テレポーテーション**
- **量子鍵配送**

講義内容

- **量子もつれとベルの不等式**
- **量子テレポーテーション**
- **量子鍵配送**

ベル状態



John Bell
(1928–1990)

(from Wikipedia)

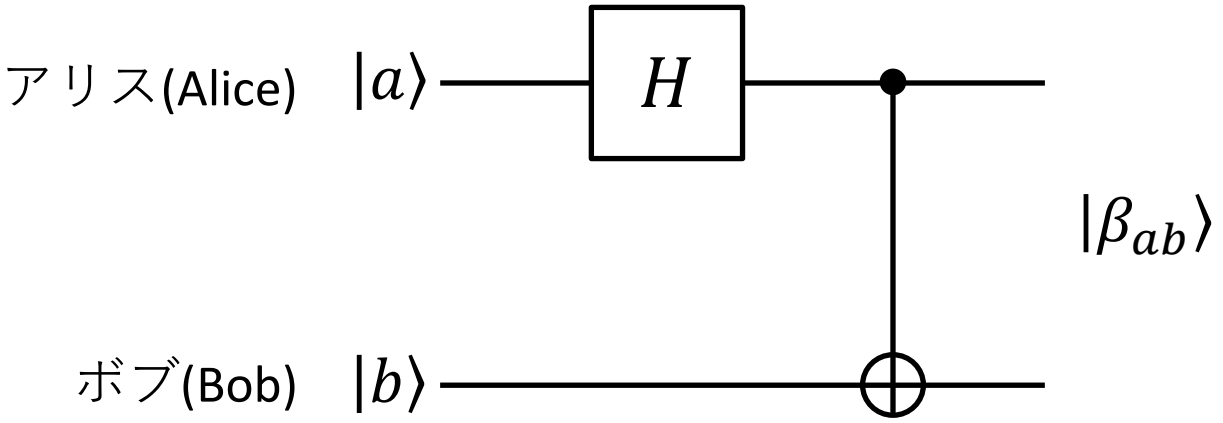
$$|0\rangle|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|0\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$$

$$|1\rangle|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|0\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$$

$$|0\rangle|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|1\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$$

$$|1\rangle|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|1\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$$

ベル状態



John Bell
(1928–1990)

(from Wikipedia)

$$|0\rangle|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|0\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$$

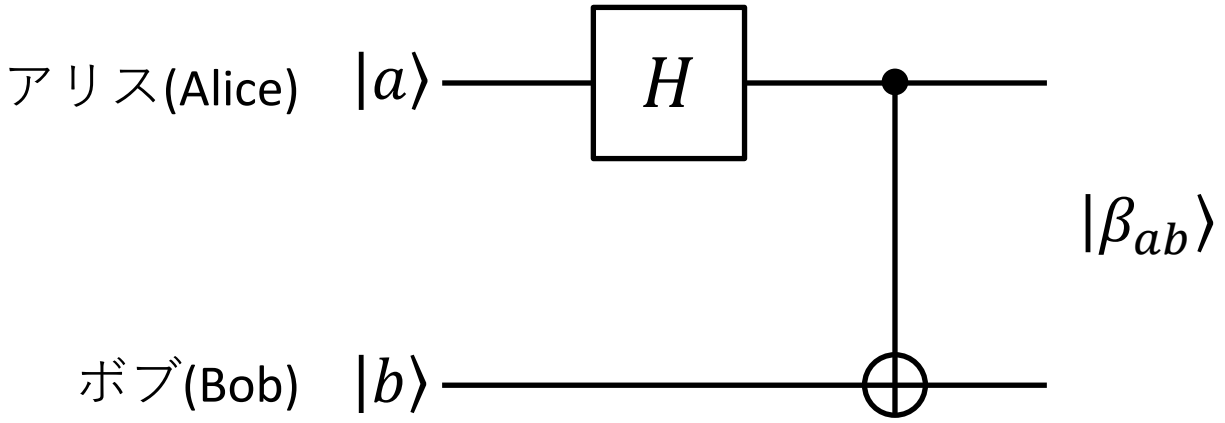
$$|1\rangle|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|0\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$$

$$|0\rangle|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|1\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$$

$$|1\rangle|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)|1\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$$

計算基底 **ベル基底**

ベル状態



John Bell
(1928–1990)

(from Wikipedia)

$$|ab\rangle \xleftrightarrow{H} \frac{|0b\rangle + (-1)^a|1b\rangle}{\sqrt{2}} \xleftrightarrow{\text{CNOT}} \frac{|0b\rangle + (-1)^a|1\bar{b}\rangle}{\sqrt{2}} = |\beta_{ab}\rangle$$

$$|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$|\beta_{01}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$$
$$|\beta_{10}\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$$
$$|\beta_{11}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$$

量子もつれ

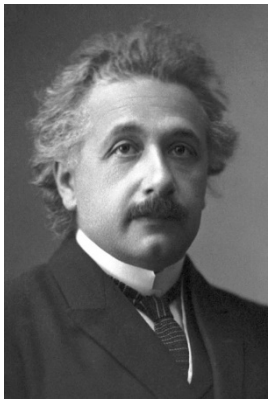
(Entanglement)

ベル状態(対、ペア)

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

または**EPR状態**とも呼ばれる

Einstein–Podolsky–Rosen



Albert Einstein
(1879–1955)

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

Phys. Rev. **47**, 777 (1935) EPR

量子もつれ

ベル状態

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

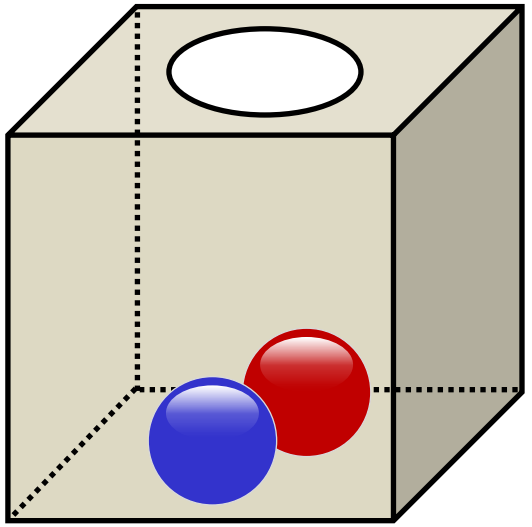
アリスが“0”を得るとボブは“1”

アリスが“1”を得るとボブは“0”

箱の中のボール…と同じこと?

アリスが“赤”を得るとボブは“青”

アリスが“青”を得るとボブは“赤”



量子もつれ

ベル状態

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

$$\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

基底の変換 $\{|0\rangle, |1\rangle\} \quad \leftrightarrow \quad \{|\rightarrow\rangle, |\leftarrow\rangle\}$

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2^3}}[(|\rightarrow\rangle + |\leftarrow\rangle)(|\rightarrow\rangle - |\leftarrow\rangle) - (|\rightarrow\rangle - |\leftarrow\rangle)(|\rightarrow\rangle + |\leftarrow\rangle)]$$

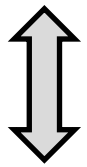
$$= \frac{1}{\sqrt{2^3}}(|\rightarrow\rangle|\rightarrow\rangle - |\rightarrow\rangle|\leftarrow\rangle + |\leftarrow\rangle|\rightarrow\rangle - |\leftarrow\rangle|\leftarrow\rangle$$
$$-|\rightarrow\rangle|\rightarrow\rangle - |\rightarrow\rangle|\leftarrow\rangle + |\leftarrow\rangle|\rightarrow\rangle + |\leftarrow\rangle|\leftarrow\rangle)$$

$$= \frac{1}{\sqrt{2}}(|\leftarrow\rangle_A|\rightarrow\rangle_B - |\rightarrow\rangle_A|\leftarrow\rangle_B)$$

量子もつれ

ベル状態

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$



$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|\leftarrow\rangle_A|\rightarrow\rangle_B - |\rightarrow\rangle_A|\leftarrow\rangle_B)$$

- もつれた状態は基底を変えても、もつれている
- アリスとボブが異なる基底で測定すると相関はない
  → アリスが計算(Z)基底で“0”を得たのち、ボブがX基底で測定を行うと“→”も“←” も50%の確率で得られる

量子もつれ

ベル状態

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

©AIP Emilio Segrè Visual Archives

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

Phys. Rev. **47**, 777 (1935) Einstein, Podolsky &Rosen

OCTOBER 15, 1935 PHYSICAL REVIEW VOLUME 48

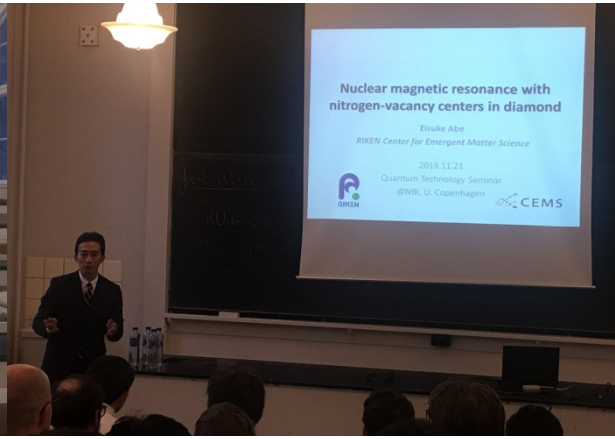
Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

N. BOHR, *Institute for Theoretical Physics, University, Copenhagen*

(Received July 13, 1935)

Phys. Rev. **48**, 696 (1935) Bohr

(from Wikipedia) ©A. Kamigori ©A. Kamigori



Niels Bohr Institutet

ベルの不等式

ベル状態

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

(from Wikipedia)

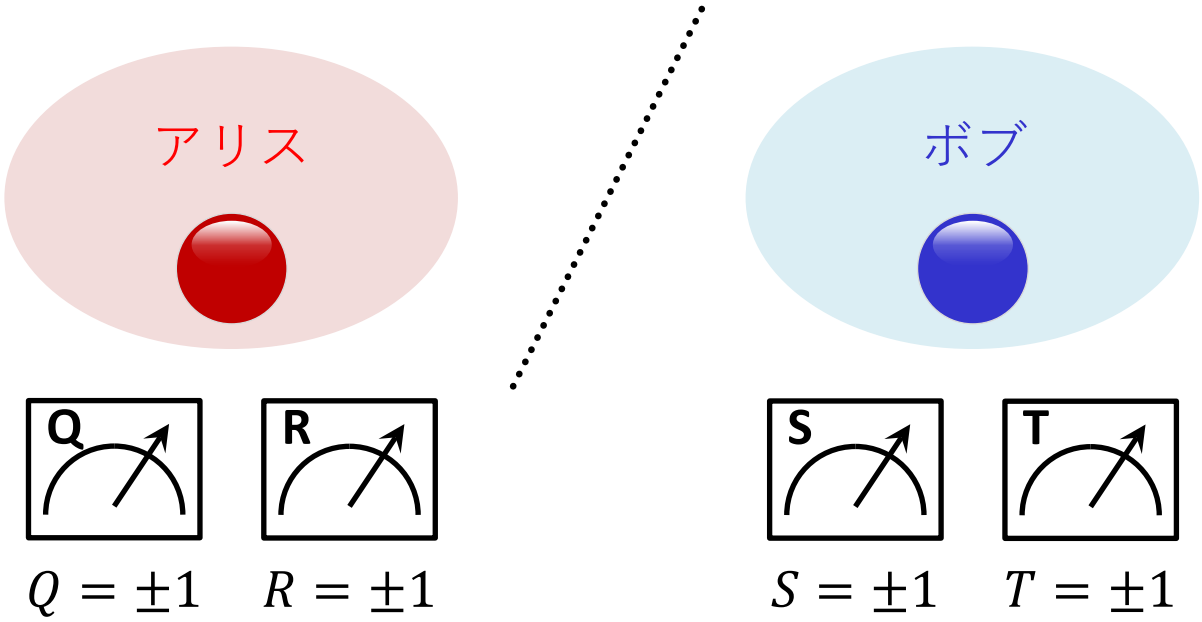
ざっくり言うと、
“量子力学における相関”は“普通の相関”とは違う
ということを定式化した

Physics **1**, 195 (1964) Bell “On the Einstein Podolsky Rosen Paradox”

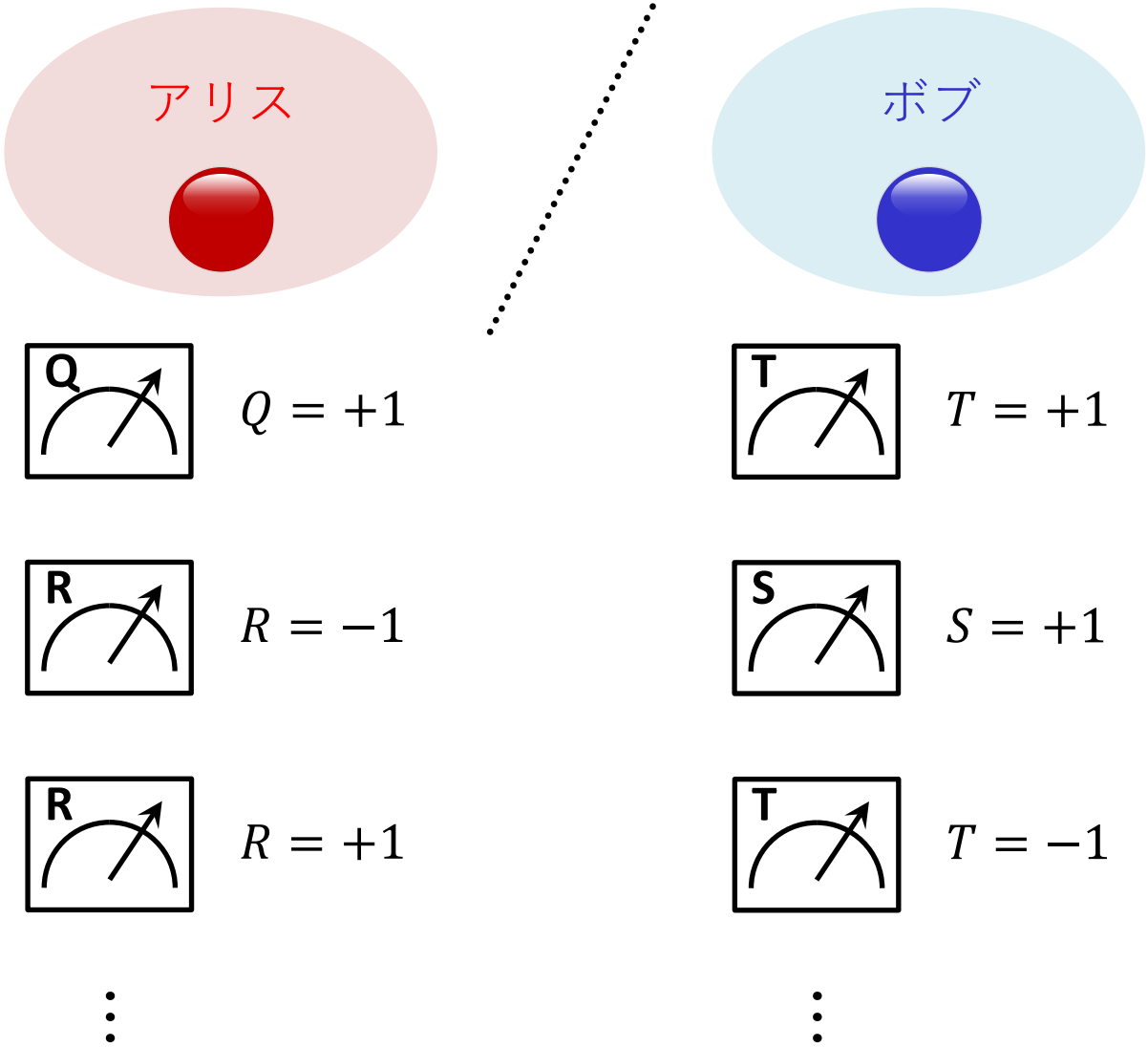
ベルの不等式

設定

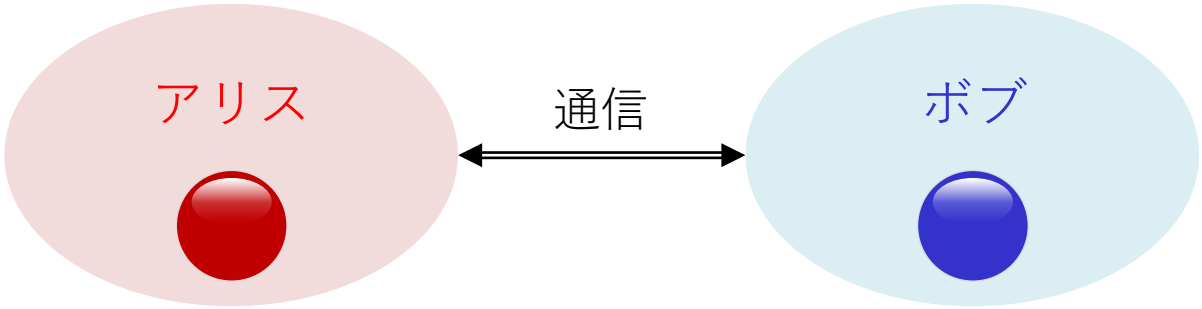
- ✓ **量子力学のことは一旦忘れて“常識”で考える**
- ✓ アリスは手元に届いた粒子(物体)に対して、2値(±1)を取る物理量**Q,R**いずれかをランダムに選んで測定する
- ✓ ボブも手元に届いた粒子の物理量**S,T**を測定する
- ✓ 2人の測定は**独立・同時**に実施される(光速でも情報伝達できないほど離れている)



ベルの不等式



ベルの不等式



多数回の測定後に、互いの測定結果を照合し$\boldsymbol{E}(QS+RS+RT-QT)$を求める

期待値計算

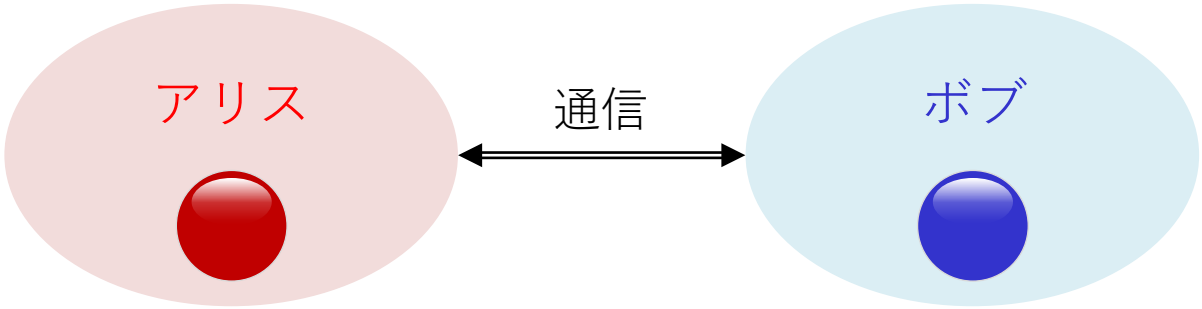
$$\boldsymbol{E}(QS+RS+RT-QT)=\sum_{q,r,s,t} p(q,r,s,t)(qs+rs+rt-qt)$$

Q,R,S,Tが値q,r,s,tを取る確率

$$\leq \sum_{q,r,s,t} p(q,r,s,t)\times 2 = 2$$

$$qs+rs+rt-qt=(q+r)s+(r-q)t=\begin{cases} 2rs & (q=r) \\ 2rt & (q=-r) \end{cases}=\pm 2$$

ベルの不等式



多数回の測定後に、互いの測定結果を照合し$\boldsymbol{E}(QS+RS+RT-QT)$を求める

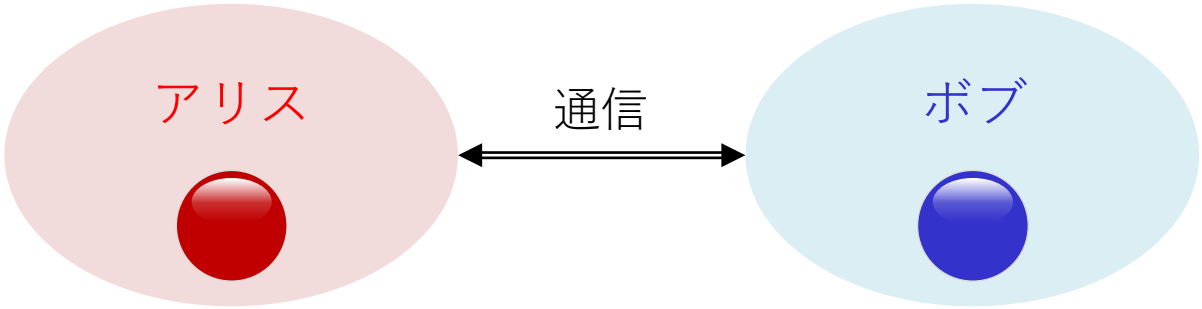
期待値計算

$$\boldsymbol{E}(QS+RS+RT-QT)=\sum_{q,r,s,t}p(q,r,s,t)qs+\sum_{q,r,s,t}p(q,r,s,t)rs$$

$$+\sum_{q,r,s,t}p(q,r,s,t)rt-\sum_{q,r,s,t}p(q,r,s,t)qt$$

$$=\boldsymbol{E}(QS)+\boldsymbol{E}(RS)+\boldsymbol{E}(RT)-\boldsymbol{E}(QT)$$

ベルの不等式



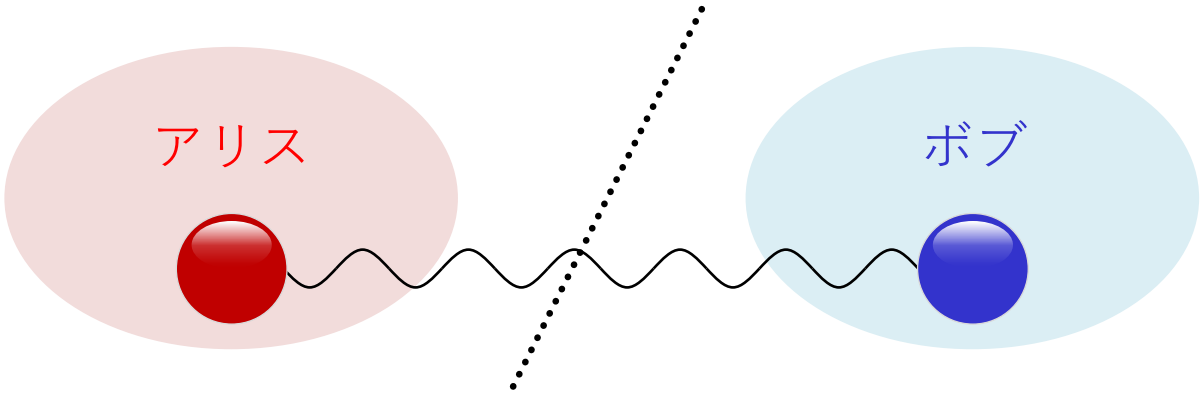
多数回の測定後に、互いの測定結果を照合し$\boldsymbol{E}(QS + RS + RT - QT)$を求める

CHSH不等式

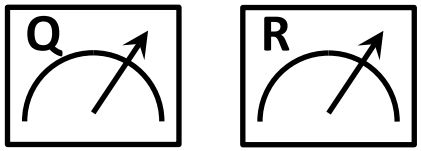
$$\boldsymbol{E}(QS) + \boldsymbol{E}(RS) + \boldsymbol{E}(RT) - \boldsymbol{E}(QT) \leq 2$$

Phys. Rev. Lett. **23**, 880 (1969) Clauser, Horne, Shimony, & Holt

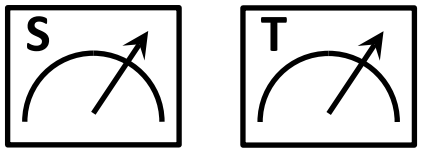
ベルの不等式



$$|\beta_{11}\rangle_{AB} = (|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)/\sqrt{2}$$



$Q = \pm 1$ $R = \pm 1$



$S = \pm 1$ $T = \pm 1$

Z_A X_A

$\frac{-Z_B - X_B}{\sqrt{2}}$ $\frac{Z_B - X_B}{\sqrt{2}}$

ベル状態に対して異なる基底で測定を行う → $\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = ?$

ベルの不等式

$$|\beta_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \qquad QS = \frac{-Z_AZ_B - Z_AX_B}{\sqrt{2}}$$

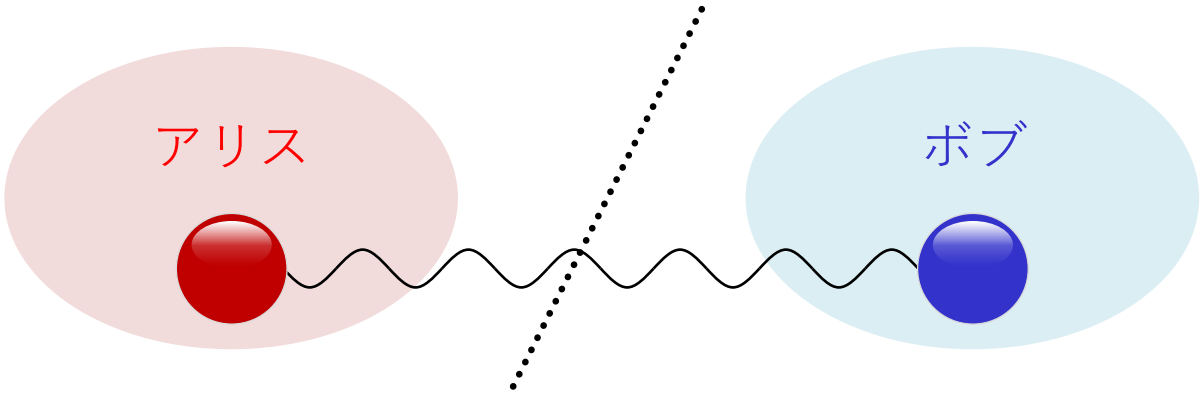
$$\langle QS\rangle = \langle\beta_{11}|QS|\beta_{11}\rangle$$

$$= \frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|)(-ZZ - ZX)(|01\rangle - |10\rangle)$$

$$= \frac{1}{2\sqrt{2}}(-\langle 01|ZZ|01\rangle + \langle 01|ZZ|10\rangle - \langle 01|ZX|01\rangle + \langle 01|ZX|10\rangle$$
$$+\langle 10|ZZ|01\rangle - \langle 10|ZZ|10\rangle + \langle 10|ZX|01\rangle - \langle 10|ZX|10\rangle)$$

$$= \frac{1}{2\sqrt{2}}(1 + 0 - 0 + 0 + 0 + 1 + 0 + 0) = \frac{1}{\sqrt{2}}$$

ベルの不等式



$$|\beta_{11}\rangle_{AB} = (|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)/\sqrt{2}$$

$$\langle QS\rangle = \frac{1}{\sqrt{2}} \qquad \langle RS\rangle = \frac{1}{\sqrt{2}} \qquad \langle RT\rangle = \frac{1}{\sqrt{2}} \qquad \langle QT\rangle = -\frac{1}{\sqrt{2}}$$

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}$$

$$\Updownarrow$$

$$\boldsymbol{E}(QS) + \boldsymbol{E}(RS) + \boldsymbol{E}(RT) - \boldsymbol{E}(QT) \leq 2$$

レポート課題 4 (20点)

(1) 1量子ビット状態

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix}$$

は演算子

$$\Psi = \begin{pmatrix} \cos\theta & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & -\cos\theta \end{pmatrix}$$

の固有状態で、固有値 = 1であることを確認せよ。

さらに、固有値 = −1となる状態$|\psi'\rangle$を見つけそのことを確認せよ。

(2) 任意の基底$\{|\psi\rangle, |\psi'\rangle\}$で$|\beta_{11}\rangle_{AB}$がもつれていることを確認せよ。

(3) $\langle RS\rangle, \langle RT\rangle, \langle QT\rangle$を計算せよ(講義の$\langle QS\rangle$の計算程度には丁寧に)。

講義内容

- 量子もつれとベルの不等式
- **量子テレポーテーション**
- 量子鍵配送

量子テレポーテーション

Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2,3]
Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]
[1] *IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598*
[2] *Département IRO, Université de Montréal, C.P. 6128, Succursale "A", Montréal, Québec, Canada H3C 3J7*
[3] *Laboratoire d'Informatique de l'École Normale Supérieure, 45 rue d'Ulm, 75230 Paris CEDEX 05, France*[a]
[4] *Department of Physics, Technion–Israel Institute of Technology, 32000 Haifa, Israel*
[5] *Department of Physics, Williams College, Williamstown, Massachusetts 01267*
(Received 2 December 1992)

An unknown quantum state $|\phi\rangle$ can be disassembled into, then later reconstructed from, purely classical information and purely nonclassical Einstein-Podolsky-Rosen (EPR) correlations. To do so the sender, "Alice," and the receiver, "Bob," must prearrange the sharing of an EPR-correlated pair of particles. Alice makes a joint measurement on her EPR particle and the unknown quantum system, and sends Bob the classical result of this measurement. Knowing this, Bob can convert the state of his EPR particle into an exact replica of the unknown state $|\phi\rangle$ which Alice destroyed.

目的: 未知の量子状態を、状態を壊す(読む)ことなく、古典通信路と量子もつれ対を用いて遠隔地に再生する

Charles Bennett
(1943–)

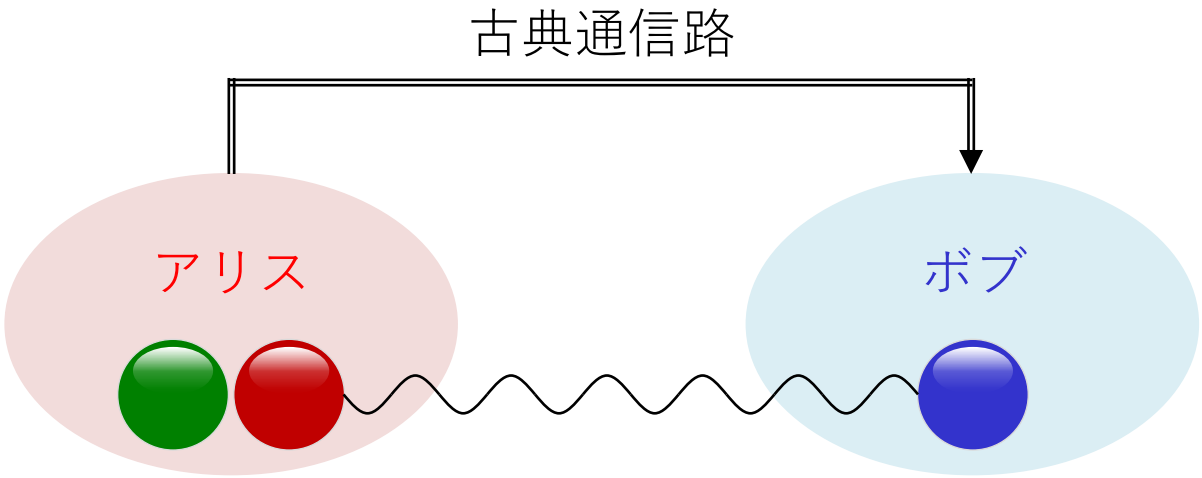
©Aya Furuta

Phys. Rev. Lett. **70**, 1895 (1993) Bennett *et al.*

量子テレポーテーション

設定(必要な道具立て)

- ✓ $|\psi\rangle$の内容はアリスも知らない
- ✓ アリスとボブが量子もつれ状態を事前に共有している
- ✓ アリスとボブの間に古典通信路が確保されている
- ✓ アリスは2量子ビットのベル測定を行うことができる
- ✓ ボブは1量子ビットゲートを行うことができる



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

未知の状態

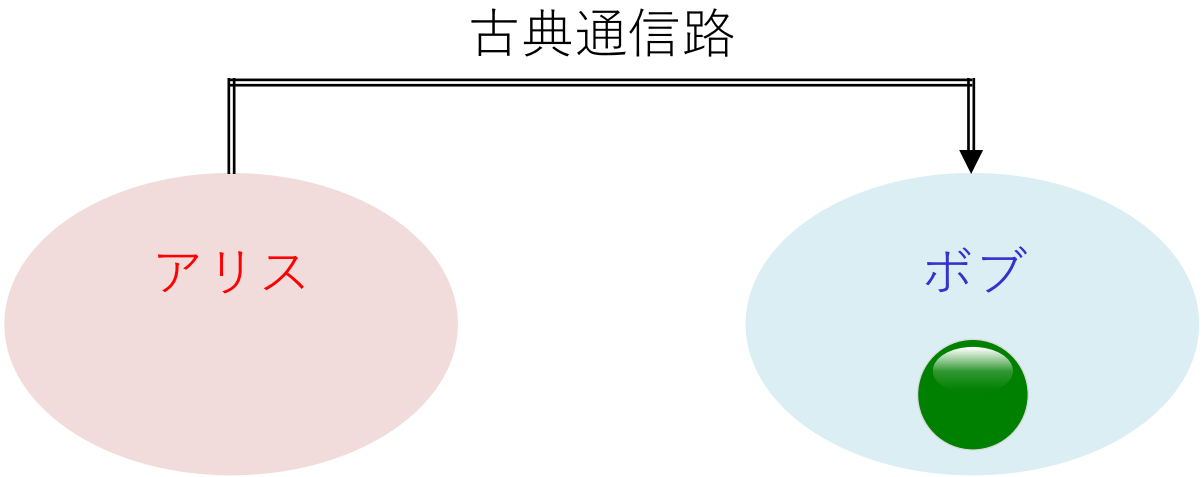
$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

もつれ対

量子テレポーテーション

設定(必要な道具立て)

- ✓ $|\psi\rangle$の内容はアリスも知らない
- ✓ アリスとボブが量子もつれ状態を事前に共有している
- ✓ アリスとボブの間に古典通信路が確保されている
- ✓ アリスは2量子ビットのベル測定を行うことができる
- ✓ ボブは1量子ビットゲートを行うことができる

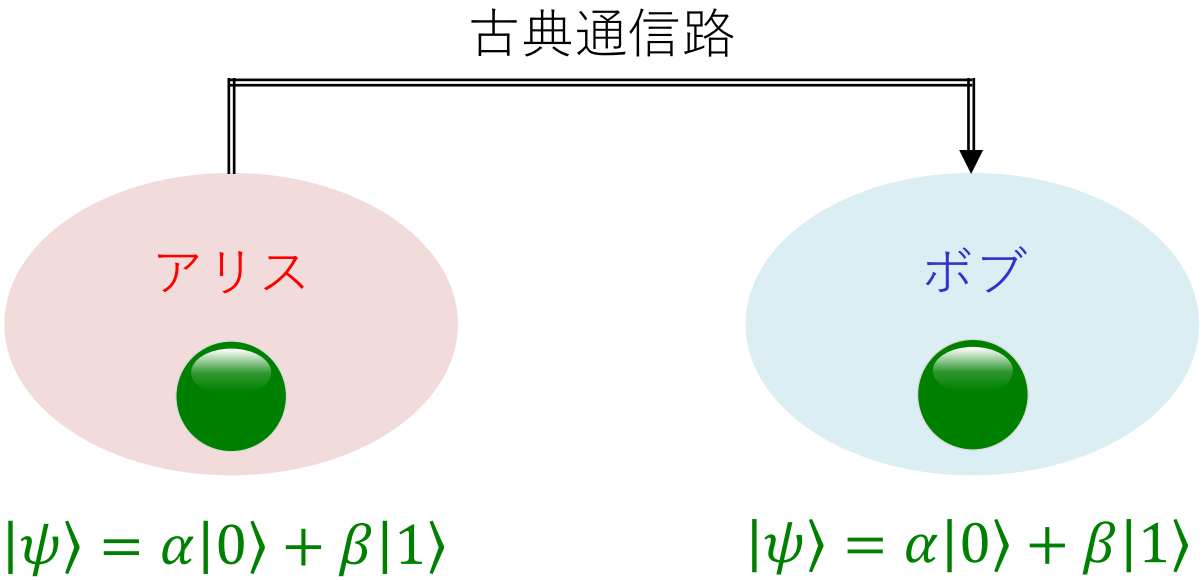


$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

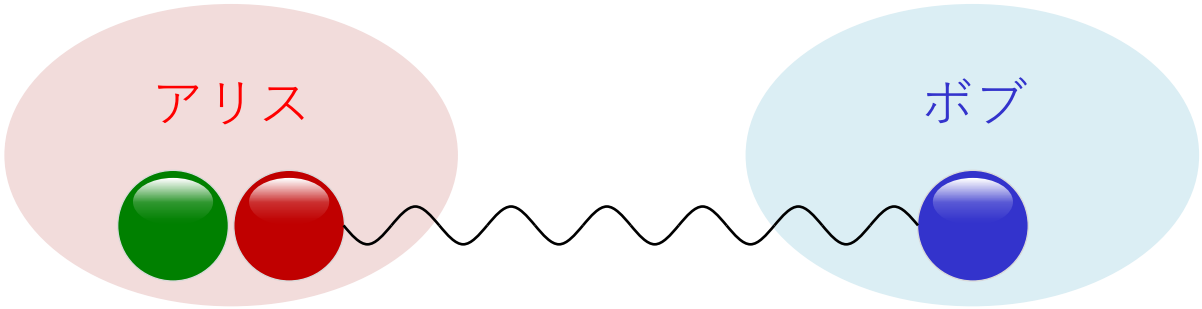
量子FAX?

アリスが状態を保持したまま、ボブが同じ状態を生成することはできるか?

→ 複製禁止定理



ステップ1: 状態準備



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

未知の状態

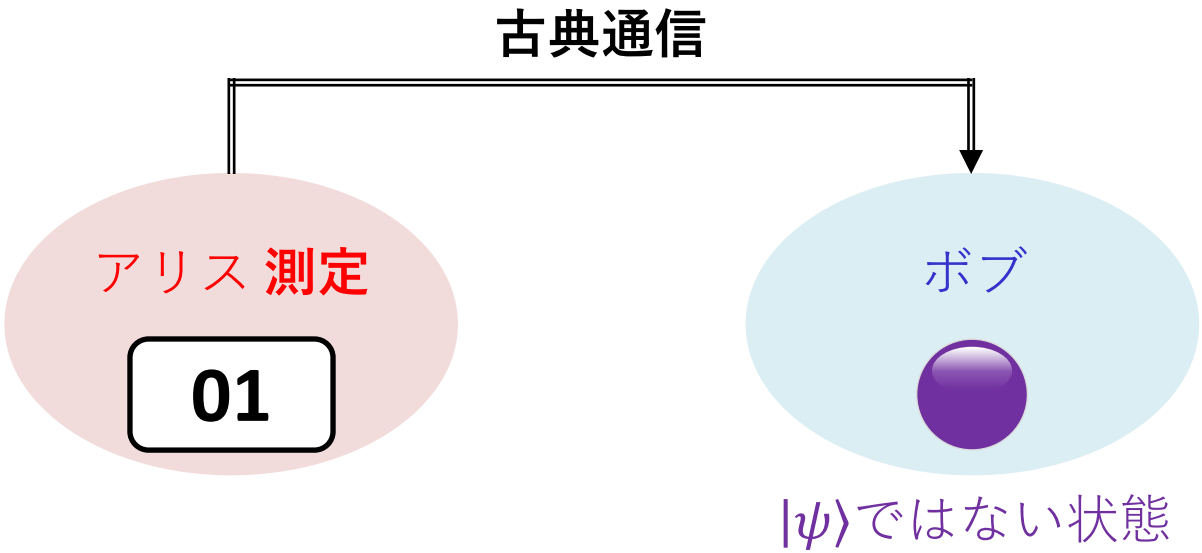
$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

もつれ対

ステップ2: ベル測定

ステップ2: ベル測定

ステップ3: 古典通信



ステップ4: 復元

アリス **測定**

01

ボブ **復元**

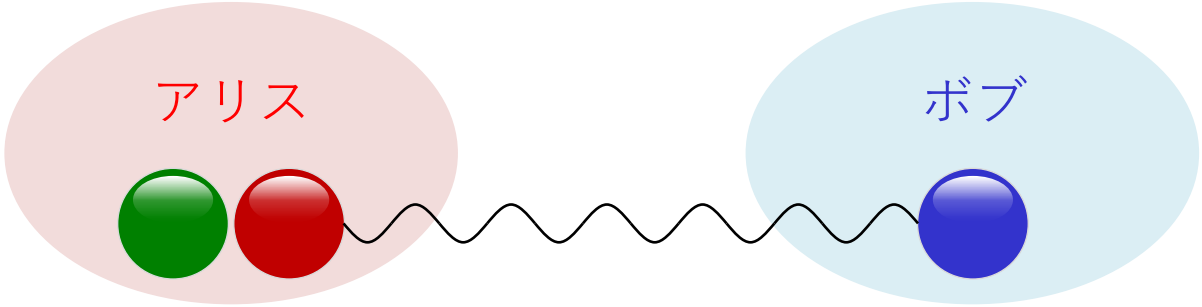
$|\psi\rangle_B = \alpha|0\rangle_B + \beta|1\rangle_B$

ステップ1: 状態準備

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$
$$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$
$$XZ|\psi\rangle = \alpha|1\rangle - \beta|0\rangle$$

$$|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$|\beta_{01}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$$
$$|\beta_{10}\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$$
$$|\beta_{11}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$$



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

未知の状態

$$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

もつれ対

確認

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

左辺 $(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|011\rangle + \frac{\alpha}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$

右辺各項

$$|\beta_{00}\rangle|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|001\rangle + \frac{\alpha}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

$$|\beta_{10}\rangle Z|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes (\alpha|0\rangle - \beta|1\rangle) = \frac{\alpha}{\sqrt{2}}|000\rangle - \frac{\beta}{\sqrt{2}}|001\rangle - \frac{\alpha}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$$

$$|\beta_{01}\rangle X|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \otimes (\alpha|1\rangle + \beta|0\rangle) = \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|010\rangle + \frac{\alpha}{\sqrt{2}}|101\rangle + \frac{\beta}{\sqrt{2}}|100\rangle$$

$$|\beta_{11}\rangle XZ|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes (\alpha|1\rangle - \beta|0\rangle) = \frac{\alpha}{\sqrt{2}}|011\rangle - \frac{\beta}{\sqrt{2}}|010\rangle - \frac{\alpha}{\sqrt{2}}|101\rangle + \frac{\beta}{\sqrt{2}}|100\rangle$$

ステップ2: ベル測定

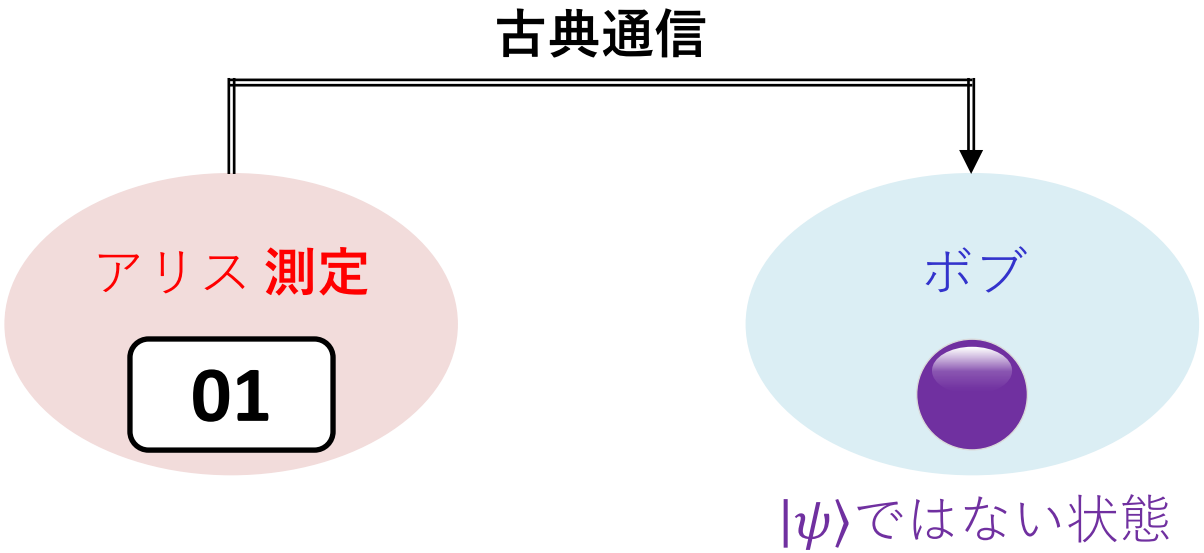
$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \boxed{\frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B} + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

- ✓ アリスが結果$xy = 01$を得たとする
- ✓ ボブの状態は$X|\psi\rangle_B$に確定するが、本人は知らない

ステップ3: 古典通信

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

✓ アリスは古典通信により結果をボブに伝える



ステップ4: 復元

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

✓ ボブは必要な1量子ビットゲートを実行して状態を復元する

アリス **測定**

01

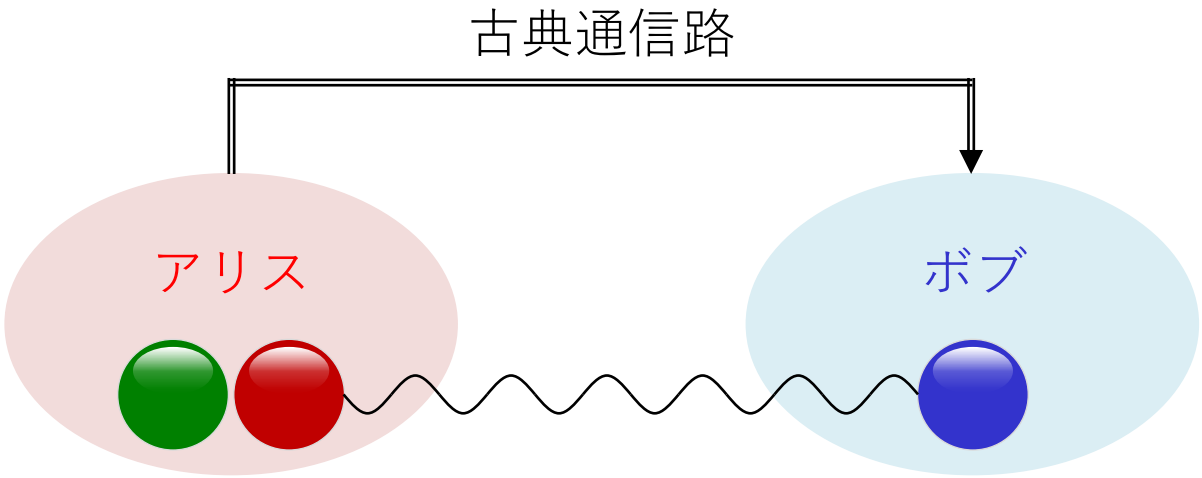
ボブ **復元**

$$|\psi\rangle_B = \alpha|0\rangle_B + \beta|1\rangle_B$$

量子テレポーテーション

設定(必要な道具立て)

- ✓ $|\psi\rangle$の内容はアリスも知らない
- ✓ **アリスとボブが量子もつれ状態を事前に共有している**
- ✓ アリスとボブの間に古典通信路が確保されている
- ✓ アリスは2量子ビットのベル測定を行うことができる
- ✓ ボブは1量子ビットゲートを行うことができる



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

未知の状態

$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

もつれ対

レポート課題 5 (10点)

量子テレポーテーションにおいて、アリスとボブが共有するもつれ対が$|\beta_{01}\rangle_{AB}$であった場合、アリスのベル測定の結果に応じて、ボブはどのような量子ゲートを実行すれば$|\psi\rangle$を復元できるか?
4通り全て答えよ。

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

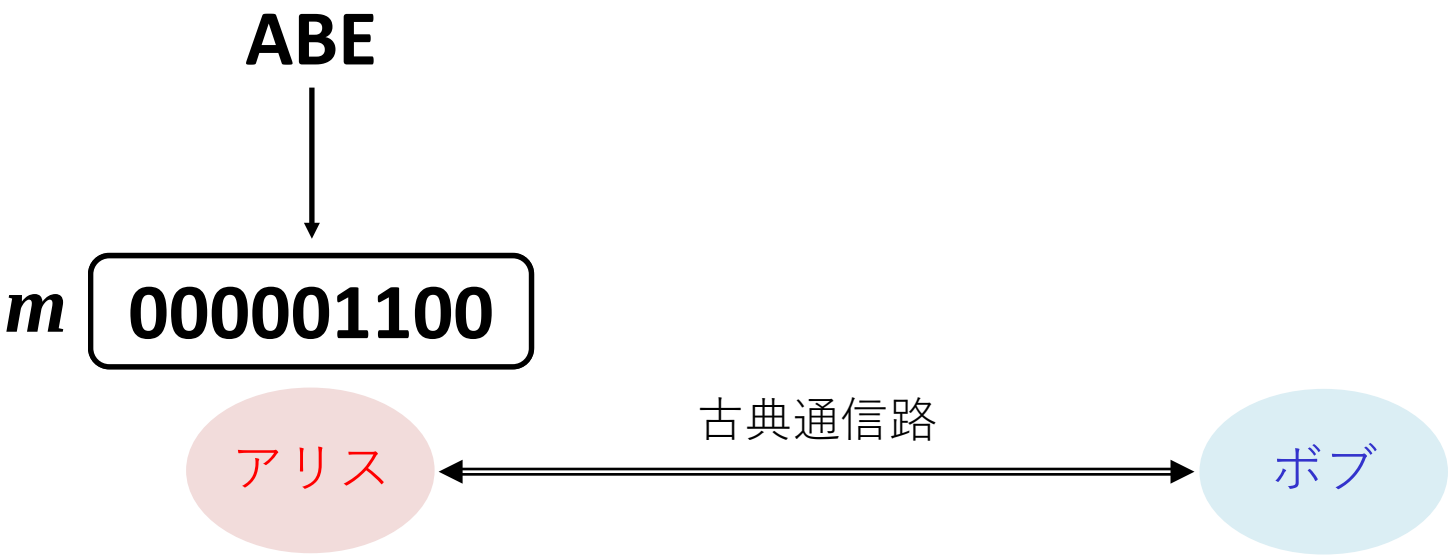
$$|\psi\rangle_V|\beta_{01}\rangle_{AB} = ?$$

講義内容

- 量子もつれとベルの不等式
- 量子テレポーテーション
- **量子鍵配送**

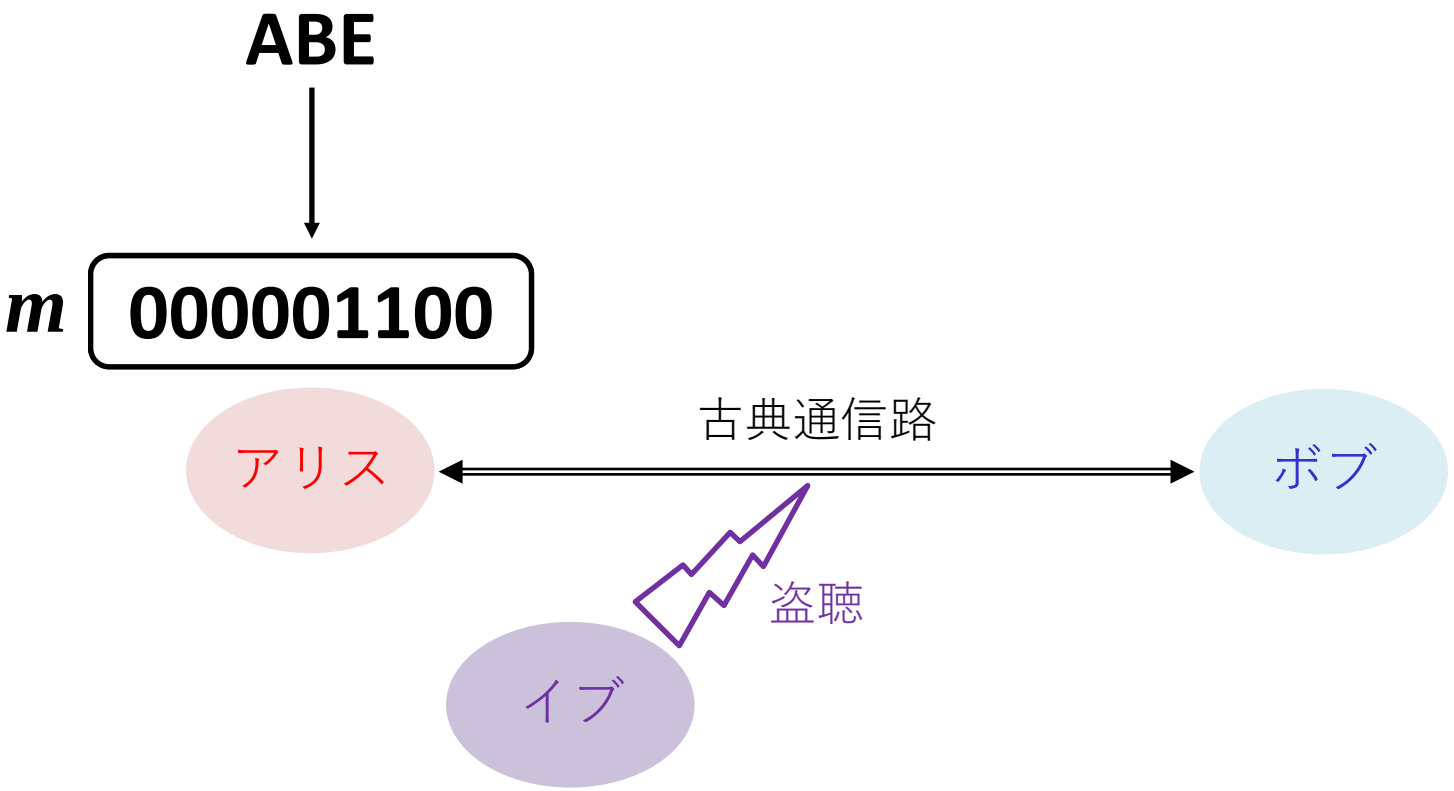
古典通信

- ✓ アルファベットを2進数に変換(A = 000, B = 001, C = 010...)
- ✓ ビット列$\boldsymbol{m}$をボブへ送信



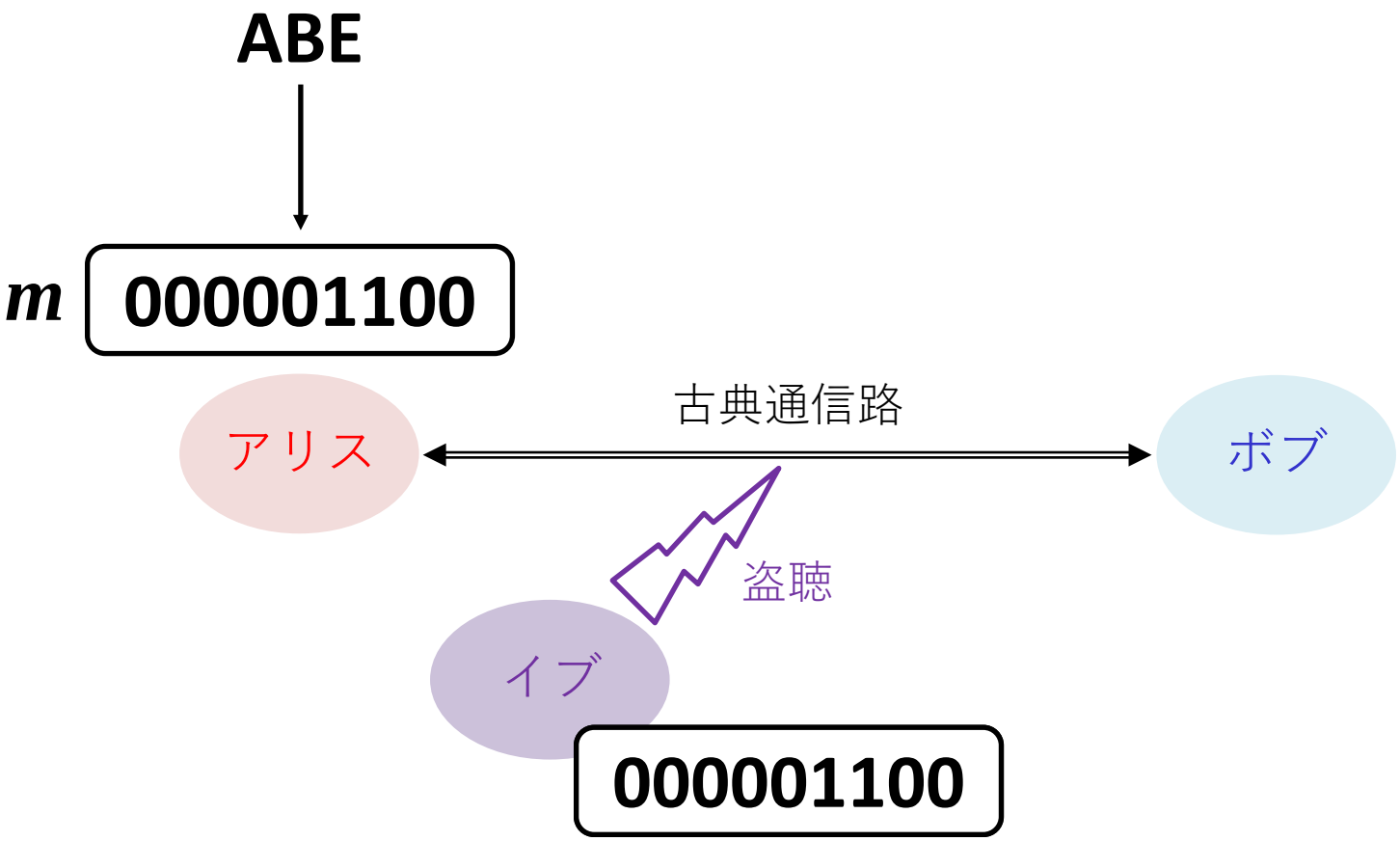
盗聴者のいる古典通信路

✓ イブは$\boldsymbol{m}$を横取り



盗聴者のいる古典通信路

- ✓ イブは$\boldsymbol{m}$を横取り
- ✓ さらにコピーをボブに送信し盗聴を気付かせない



秘匿通信: ワンタイムパッド

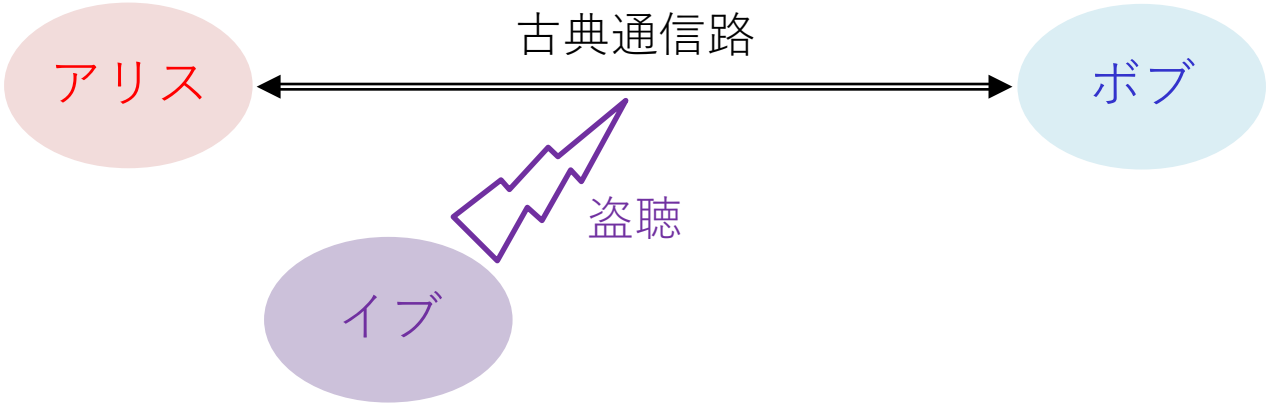
✓ アリスとボブは事前にランダムビット列$\boldsymbol{r}$(秘密鍵)を共有

$\boldsymbol{r}$ **0101110101011...**

0101110101011...

＋ $\boldsymbol{m}$ **000001100**

＝ $\boldsymbol{e}$ **010110110**



秘匿通信: ワンタイムパッド

✓ アリスとボブは事前にランダムビット列$\boldsymbol{r}$(秘密鍵)を共有

$\boldsymbol{r}$ **0101110101011...**

0101110101011...

$+\ \boldsymbol{m}$ **000001100**

$=\ \boldsymbol{e}$ **010110110**

秘匿通信: ワンタイムパッド

✓ ボブは$e + r$を実行して復号(rを知らないイブは復号できない)

r 010111010 1011...

$+ m$ 000001100

$= e$ 010110110

$=$ 000001100

010111010 1011...

$+$ 010110110

秘匿通信: ワンタイムパッド

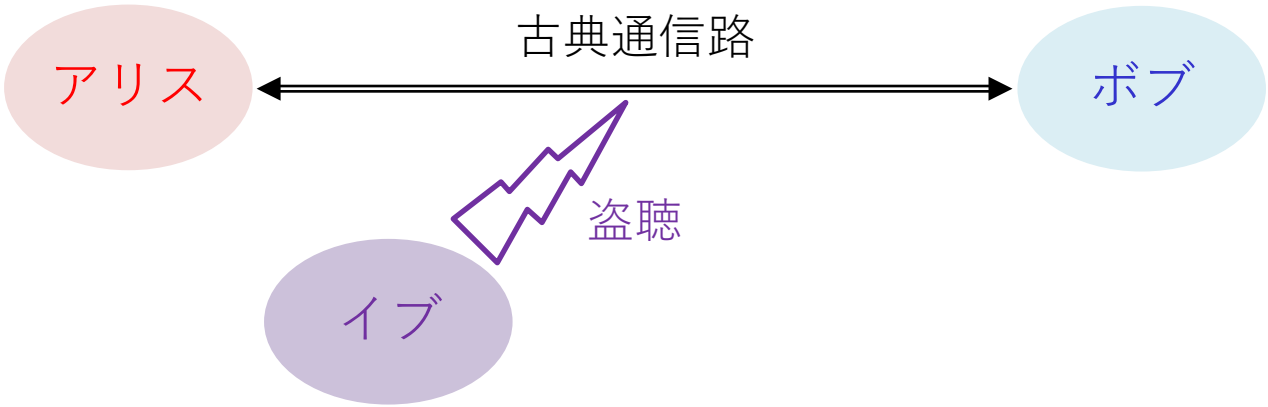
✓ 使ったrは破棄(再利用しない限り安全)

r ~~0101111010~~ 1011…

→ どうやってあらかじめrを共有するか?

→ “鍵配送”

~~0101111010~~ 1011…

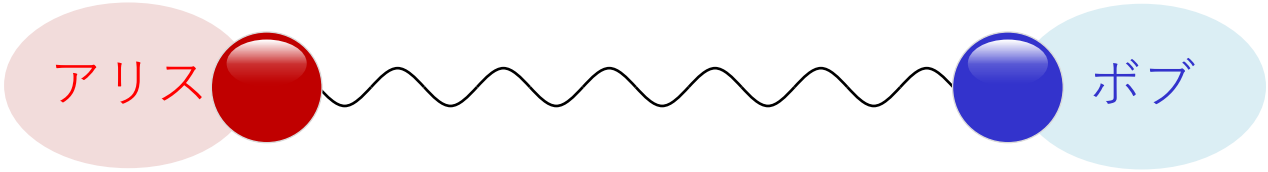


量子鍵配送

(Quantum Key Distribution)

→ 量子的な鍵配送(量子鍵の配送ではない)

量子もつれプロトコル(E91 & BBM92)



“Some people wonder if I am the same N. David Mermin as the coauthor, with Neil Ashcroft, of Solid State Physics. I am.”

David Mermin
(1935–)

Artur Ekert
(1961–)

©N. David Mermin
http://www.lassp.cornell.edu/mermin/

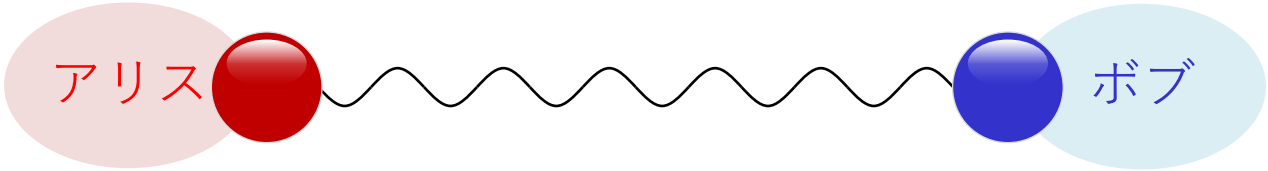
(from Wikipedia)

Phys. Rev. Lett. **67**, 661 (1991) Ekert “Quantum cryptography based on Bell's theorem”

Phys. Rev. Lett. **68**, 557 (1992) Bennett, Brassard, & Mermin “Quantum cryptography without Bell's theorem”

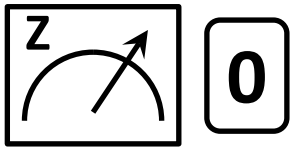
BBM92

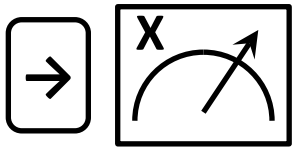
- ✓ アリスとボブの間で量子もつれ対を共有
- ✓ 各自がZ/X基底をランダムに選び手元の量子ビットを測定



$$|\beta_{00}\rangle_{AB} = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2}$$

$$= (|\rightarrow\rangle_A|\rightarrow\rangle_B + |\leftarrow\rangle_A|\leftarrow\rangle_B)/\sqrt{2}$$

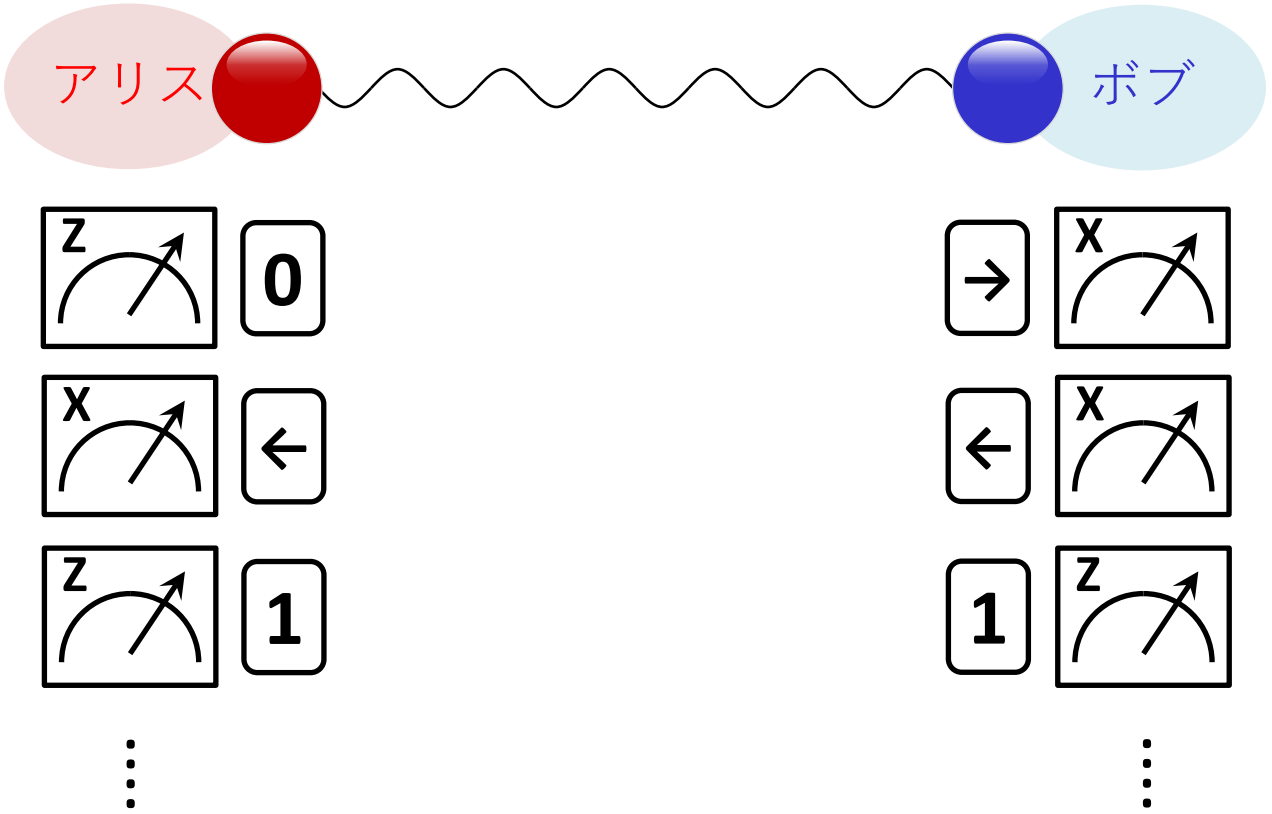




$$|0\rangle_B = (|\rightarrow\rangle_B + |\leftarrow\rangle_B)/\sqrt{2}$$

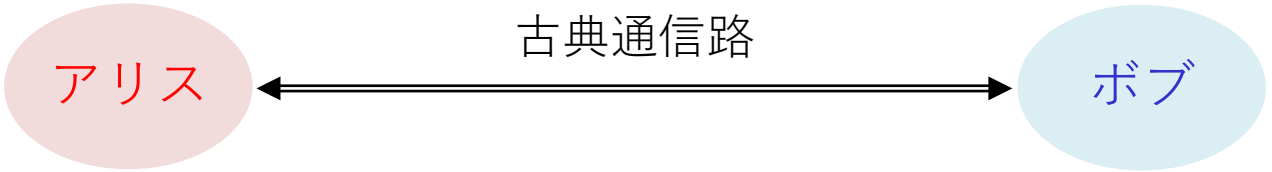
BBM92

- ✓ アリスとボブの間で量子もつれ対を共有
- ✓ 各自がZ/X基底をランダムに選び手元の量子ビットを測定
- ✓ 新たな量子もつれ対で同じことを繰り返す



BBM92

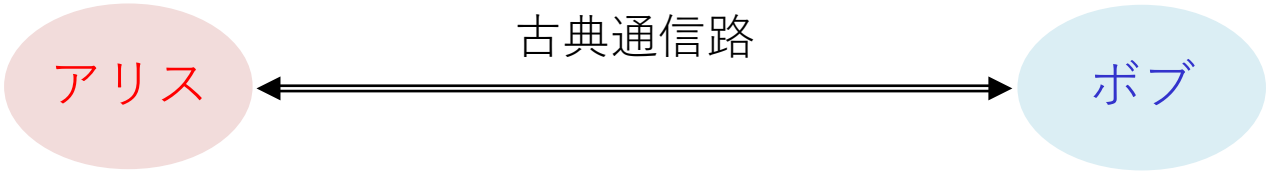
✓ 古典通信路を用いて用いた基底を確認



アリス	基底	Z	X	Z	Z	X	Z	Z	X	Z	X	X
	測定結果	0	←	1	1	→	0	1	→	0	→	←
ボブ	基底	X	X	Z	X	X	X	Z	Z	X	X	Z
	測定結果	→	←	1	←	→	←	1	0	→	→	1

BBM92

- ✓ 古典通信路を用いて用いた基底を確認
- ✓ 同一基底での結果のみを用いて$\boldsymbol{r}$を作る(→,←は0,1に読み替える)

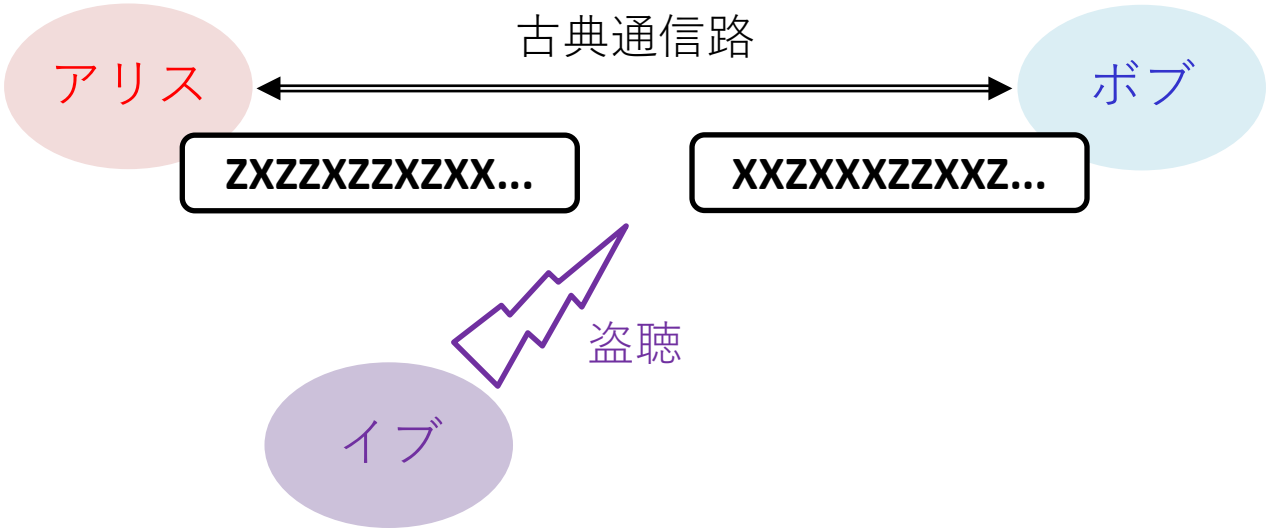


アリス	基底	Z	**X**	**Z**	Z	**X**	Z	**Z**	X	Z	**X**	X
	測定結果	0	**←**	**1**	1	**→**	0	**1**	→	0	**→**	←
ボブ	基底	X	**X**	**Z**	X	**X**	X	**Z**	Z	X	**X**	Z
	測定結果	→	**←**	**1**	←	**→**	←	**1**	0	→	**→**	1

$\boldsymbol{r}$ **11010…**

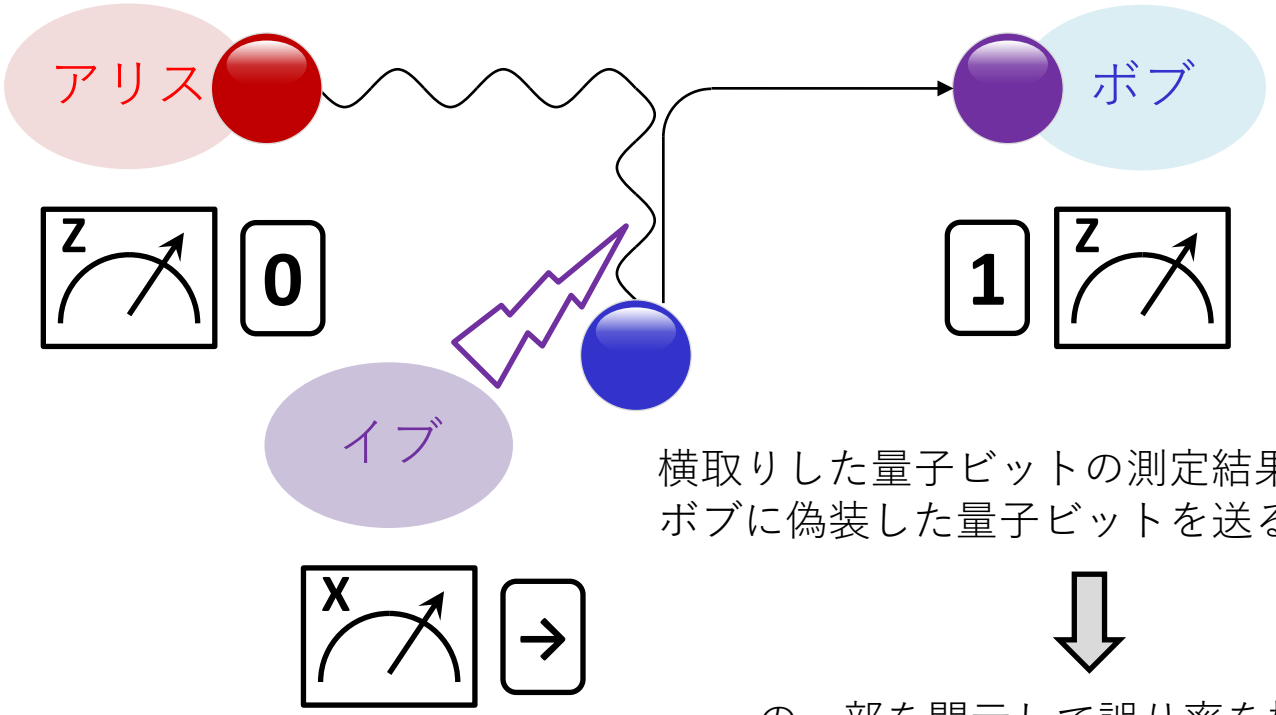
BBM92における盗聴

✓ 古典通信路を流れる基底の情報だけでは$\boldsymbol{r}$は推定できない



BBM92における盗聴

- ✓ 古典通信路を流れる基底の情報だけでは$\boldsymbol{r}$は推定できない
- ✓ 量子もつれ対を横取りしたら?



横取りした量子ビットの測定結果に基づいて
ボブに偽装した量子ビットを送る

$\boldsymbol{r}$の一部を開示して誤り率を検証する
ことでイブの存在を検知できる