# II類P2 小川研究室：卒研配属について

研究室の研究テーマ（情報理論，量子情報，数学，物理に興味のある人が向いています）

- **情報理論**
  情報スペクトル理論，情報理論的暗号（盗聴通信路符号化），データ圧縮，誤り訂正符号

- **量子情報理論** （情報の記憶・伝送を担う媒体の量子効果を考慮した情報理論，量子通信，量子計算）
  量子通信路符号化，量子状態の識別理論，量子誤り訂正，量子暗号，量子秘密分散，
  エンタングルメント変換，量子スピンチェイン，量子情報スペクトル理論

  （参考）2022年ノーベル物理学賞：A. Aspect, J. F. Clauser, A. Zeilinger,
  量子もつれ光子を用いたベルの不等式の破れの実験と量子情報科学の先駆的研究
- 大学院授業・量子情報数理特論
  http://www.quest.lab.uec.ac.jp/ogawa/qmath2025/

- **数理工学，学習理論，統計的データ解析**
  情報幾何学，ニューラルネットワーク（深層学習，ボルツマンマシン）の数理

  （参考）2024年ノーベル物理学賞：J. J. Hopfield, G. E. Hinton,
  人工ニューラルネットワークによる機械学習を可能にした基礎的発見と発明に対する業績

- 研究室メンバー（2025年度）
  – B4：5名, M1：2名, M2：2名, D：3名
- 研究室見学
  – 水曜日 13時〜16時：11/5, 11/12, 11/26 （見学＆面談可能）
  – その他の時間はアポイントのメールを下さい.

# ワンタイムパッド（情報理論的暗号の一番簡単な例）

送信者アリス

受信者ボブ

| 送信メッセージ “HELLO” | 受信メッセージ “HELLO” |
|---|---|
| $a = 11010000 \cdots$ | $a = 11010000 \cdots$ |

shared key　ランダムなビット列を事前に共有　shared key

$b = 01101010 \cdots$　　$b = 01101010 \cdots$

$\Downarrow \oplus$ 暗号化　　復号 $\oplus \Uparrow$

| 暗号文 | 公開通信路 $\longrightarrow$ | 暗号文 |
|---|---|---|
| $c = 10111010 \cdots$ | | $c = 10111010 \cdots$ |

盗聴者 イブ ↘ 😎

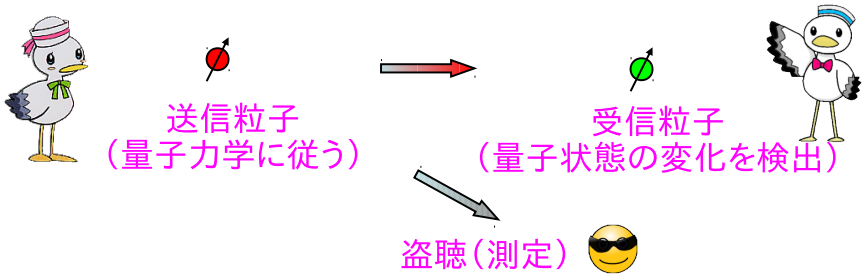
暗号文を盗聴　$c = 10111010 \cdots$

（メッセージをランダムに反転したものなので，元が分からない）

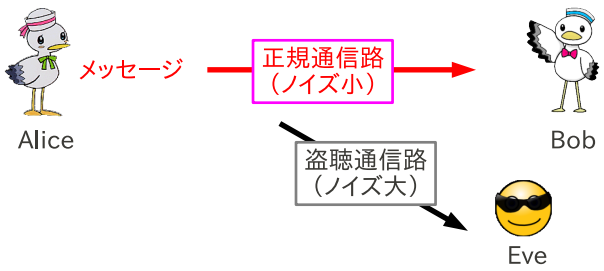
遠隔で離れているため，カギ共有の問題が生じる

# ワンタイムパッドや暗号通信のカギ共有はどうするの？

- 現在は公開カギ暗号系（RSA暗号等）が使われている：素因数分解の困難さを利用
  量子コンピューターが実現すると安全性が崩れることが理論的に示されている
  （現在稼働中の量子コンピューターは小規模・ノイズ多く研究初期段階）
- **量子暗号**



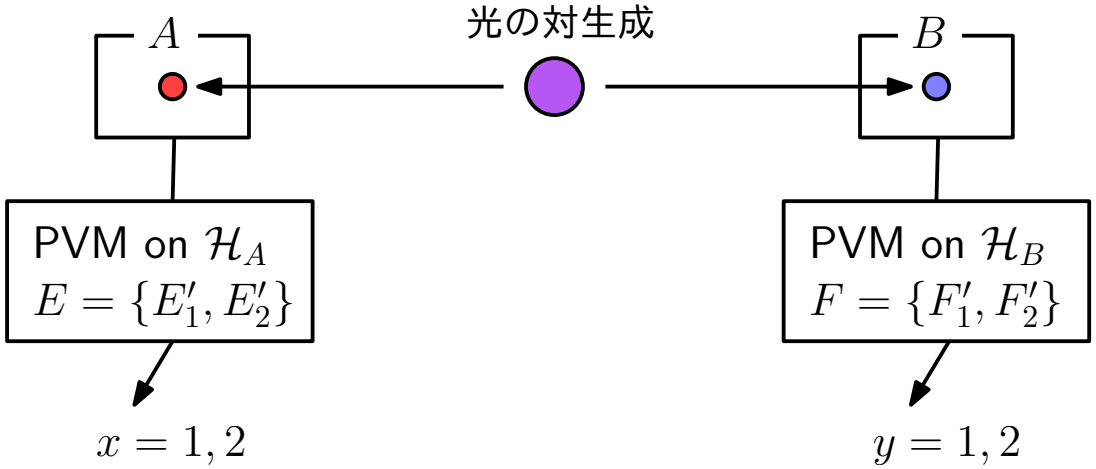

  - 「物理法則（量子力学，量子状態はコピーできない）＋情報理論」が安全性を確保
- **盗聴通信路符号化**




  - ノイズ差を利用して上手に符号化，情報理論により安全性（無条件安全性）を確保できる
  - 量子暗号の安全性証明や，量子誤り訂正の動作原理にもなっている
  - 実用的には線形符号（ハッシュ）を利用（研究室で修論研究：特許公開）

# 最大エンタングル状態と測定値の相関

$$|\Phi_{AB}\rangle = \frac{|e_1\rangle \otimes |f_1\rangle + |e_2\rangle \otimes |f_2\rangle}{\sqrt{2}} = \frac{|e_1'\rangle \otimes |f_1'\rangle + |e_2'\rangle \otimes |f_2'\rangle}{\sqrt{2}}$$




測定結果 $\nearrow$ $|e_1'\rangle$ $\nearrow$ $|f_1'\rangle$ （確率 1/2）

$\nwarrow$ $|e_2'\rangle$ $\nwarrow$ $|f_2'\rangle$ （確率 1/2）

(ii) 系AでPVM $E_1' = |e_1'\rangle\langle e_1'|$, $E_2' = |e_2'\rangle\langle e_2'|$，系BでPVM $F_1' = |f_1'\rangle\langle f_1'|$, $F_2' = |f_2\rangle\langle f_2|$ を行うと，

$$P_{\Phi_{AB}}(x, y) = \|(E_x' \otimes F_y')\,|\Phi_{AB}\rangle\,\|^2 = \begin{cases} \frac{1}{2} & x = y \\ 0 & x \neq y \end{cases}$$

(i) (ii) のいずれのケースでも $x = y = 1$ または $x = y = 2$ が確率 $1/2$ で生起する（完全相関）.

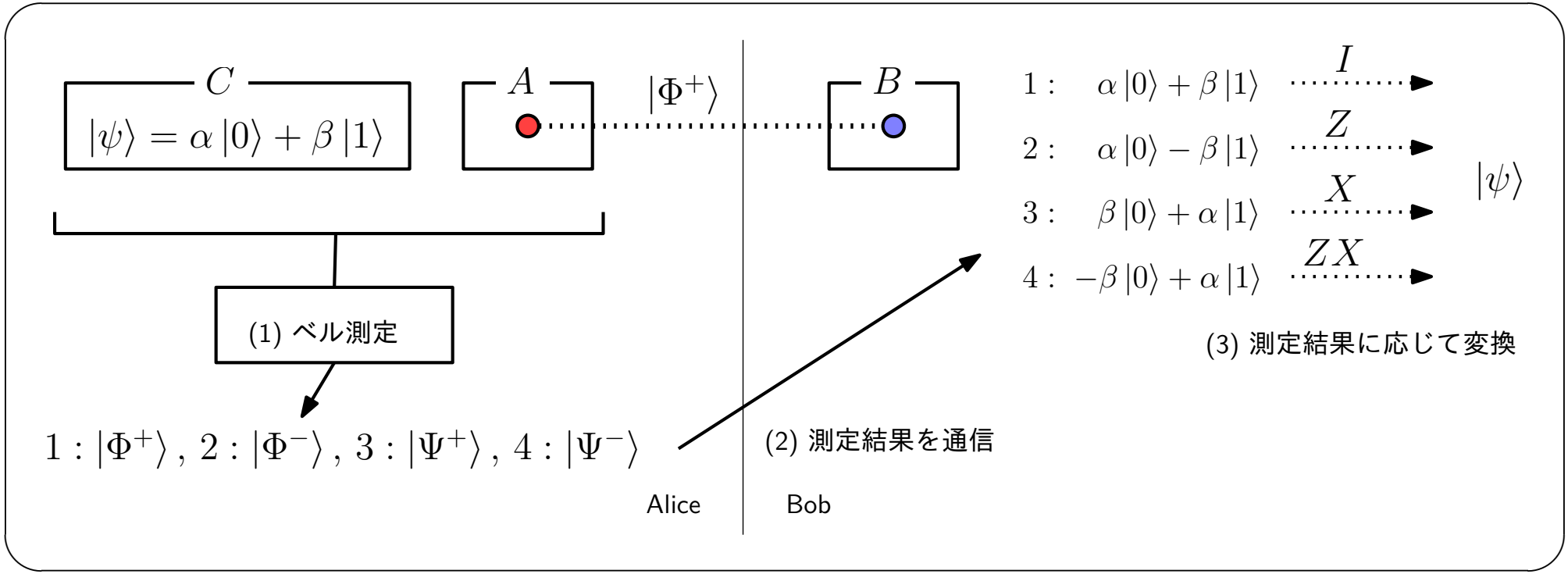
# 量子テレポーテーション

- Aliceが所有する系$C$における，未知のベクトル状態を，遠隔にいるBobに送信したい．

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathbb{C}^2 \quad (\alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1)$$

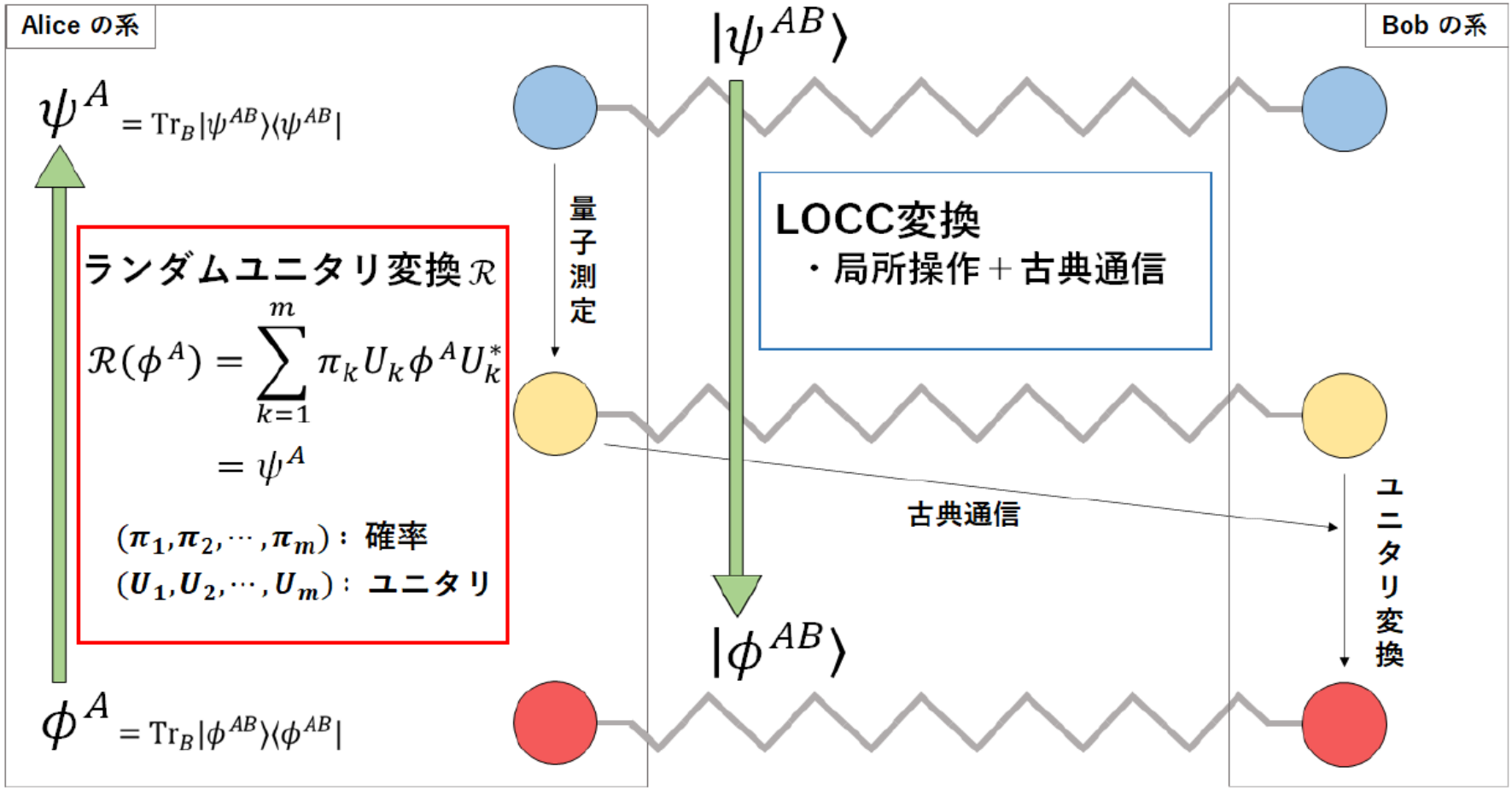
- 測定を行うと破壊されてしまう．
- Aliceの系$A$と，Bobの系$B$の合成系で，最大エンタングル状態を共有していると仮定．

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



# LOCC変換（局所操作・古典通信による量子操作）

- 弱い（薄い）エンタングルメントを完全なエンタングルメントに変換する理論




- 研究室では，量子情報スペクトル理論により，量子スピンチェインのLOCC変換の変換効率について研究しています．

# ボルツマンマシンと情報幾何

研究室では，量子情報幾何を応用して，量子ボルツマンマシンのクラスター近似方法について研究しています．

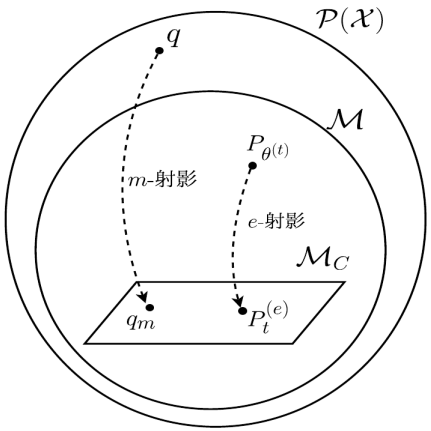
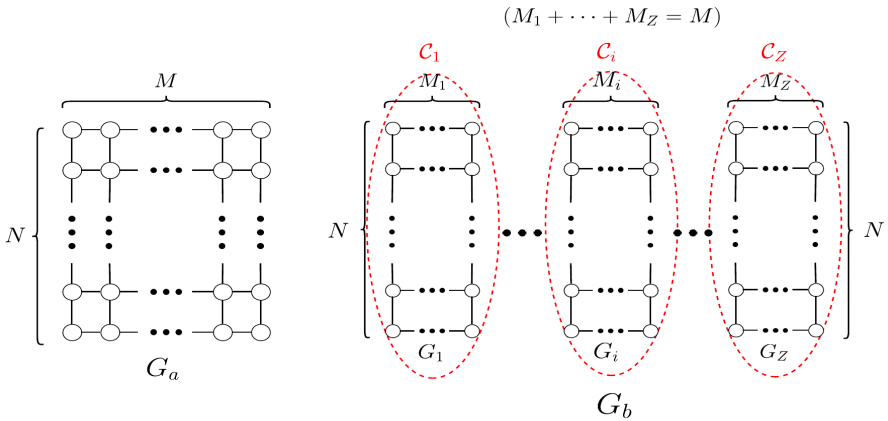
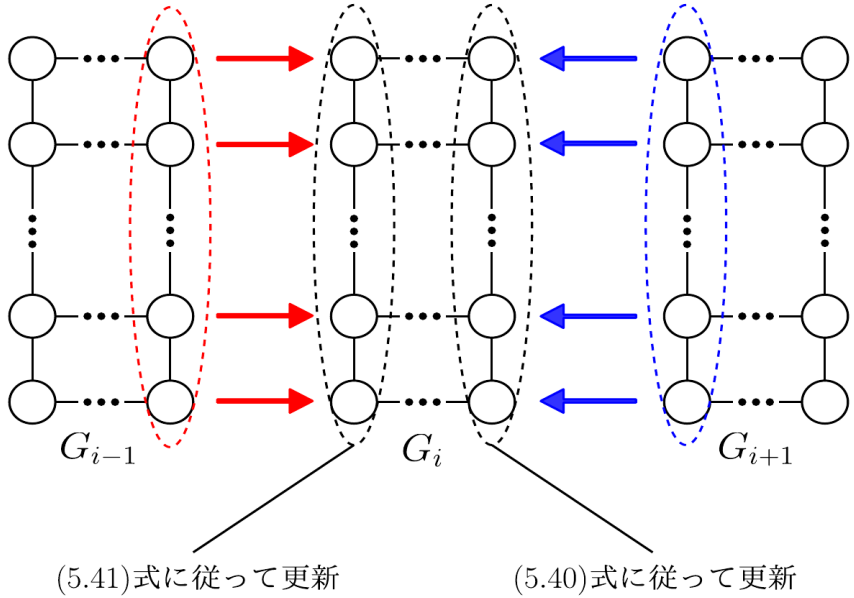



図 4.1: 平均場近似を用いた学習アルゴリズムの幾何学的イメージ




クラスター近似のアルゴリズム

# 研究のテーマ（目標：量子情報処理の理論基盤の研究）

## 過去の修士論文

(1) 情報理論，盗聴通信路符号化
- 盗聴通信路符号化における特性関数を用いた安全性評価について（特許 7040761）
- 通信路特性に依存しないユニバーサル盗聴通信路符号化方式
- 線形符号を用いたビットコミットメントプロトコルの構成方法

(2) 量子情報理論
- エンタングルメント純粋化と蒸留プロトコルに関する情報スペクトル的研究
- 量子スピンチェイン上のダイバージェンスレートと状態遷移可能性
  （2022年3月，電子情報通信学会SITAサブソサイエティ学生優秀発表賞）
- 純粋化を介した双対性を持つ量子単調計量の一般化に関する研究
  （2020年12月，電子情報通信学会SITAサブソサイエティ学生優秀発表賞）

(3) ボルツマンマシン（ニューラルネットワーク）
- 頂点模型との等価性を用いたボルツマンマシンの期待値計算法に関する研究
- ボルツマンマシンにおけるクラスター型模型への近似に関する情報幾何学的考察
  （2018年2月，電子情報通信学会SITAサブソサイエティ学生優秀発表賞）

## 卒研での研究の様子

- 前期ではテキストの輪読を通して，情報理論，量子情報理論を習得します．
  セミナーの準備のしかたについて（東京大学・河東泰之先生）
  https://www.ms.u-tokyo.ac.jp/~yasuyuki/sem.htm
- 後期では，数理的な理論に基づき，計算機用いた研究を行うことが多いです．