

量子情報の物理

ミクロな世界を支配する物理法則(量子力学)と
ICTを支える情報科学が融合した新しい科学

番 雅司

量子力学・・・ミクロな世界(原子や分子など)を
支配する力学

量子 = ミクロな世界の自然法則の基本概念
(by M. Planck in 1900)

情報理論・・・情報処理や通信ネットワークを支える
基礎となる理論

情報 = 計算や通信の基礎となる概念
(by C. Shannon in 1948)

量子情報 = 量子 + 情報

物理学と情報科学

物理学・・・自然現象の基本原理を理解し、新しい自然現象を発見することを目指す学問

情報科学・・・情報伝送や情報処理を効率的に安全に行う方法を研究する学問

物理学と情報科学の関係？

物理と情報の関係

デジタル信号で表された情報 “0100101101...”

電波や光の強弱、半導体の素子の状態によって0と1を表現

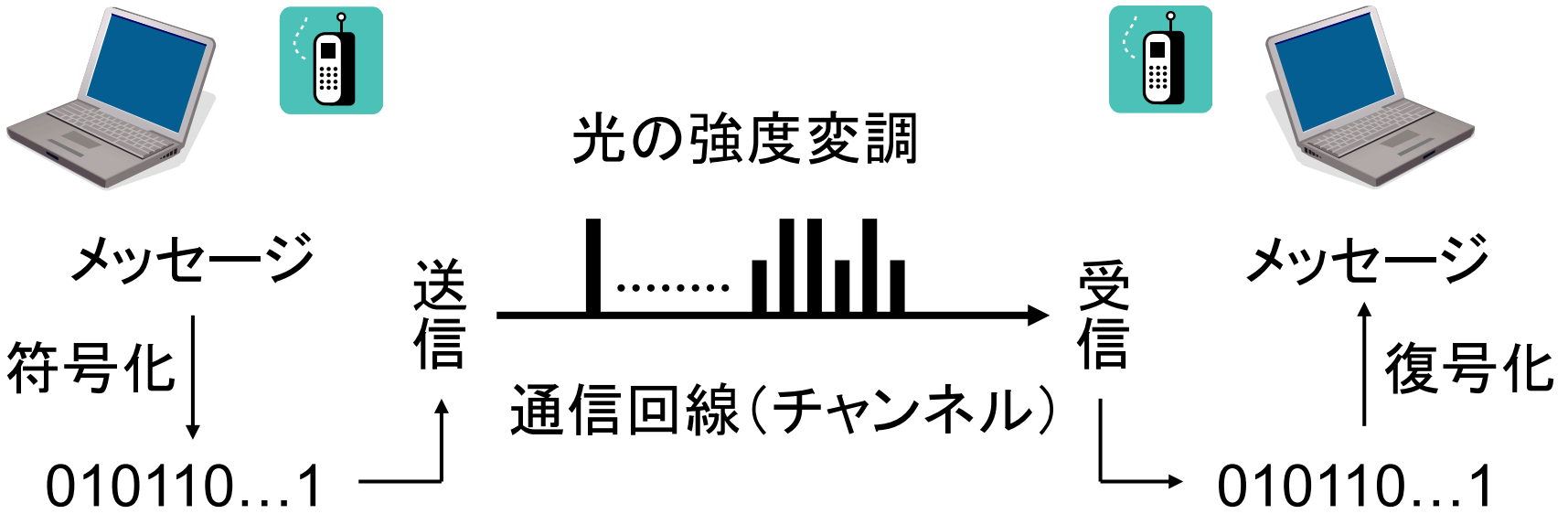
半導体、電波、光は物理法則に従う

情報処理 はデジタル信号からデジタル信号への変換

“0100101101...” → “1101001011...”
入力 出力

物理法則に従ったシステムの状態の変化

情報通信システム

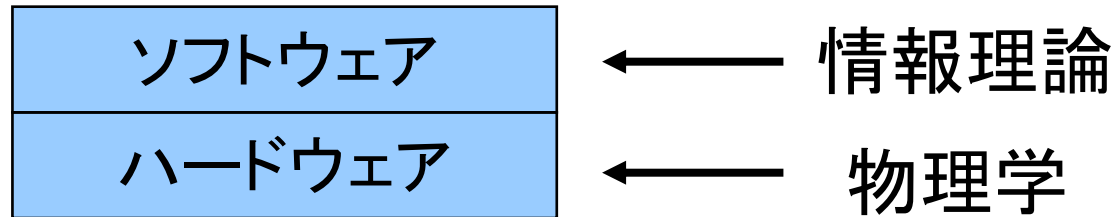


物理法則に従った状態の時間変化

(光の発生、変調、伝搬、測定)

情報通信・・・物理法則に従うシステム上に構築

情報・通信システム



現在の情報システムが従う物理法則

→ 古典物理学(電磁気学など)

量子情報システム

古典物理学に従うハードウェアから

量子力学に従うハードウェアに変更

★ 古典物理学の世界 ★

Newton力学
Maxwell電磁気学

我々の日常の世界

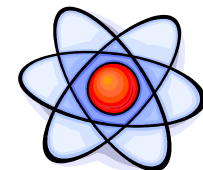


- システムのコピーが可能
- 観測してもシステムは不変
- システムの性質は局所的

★ 量子物理学の世界 ★

量子力学

原子・分子などミクロな
世界を支配する力学



- システムのコピーが不可能
- 観測するとシステムは変化
- 非局所的なシステムが存在

量子特有の性質を利用した情報の世界

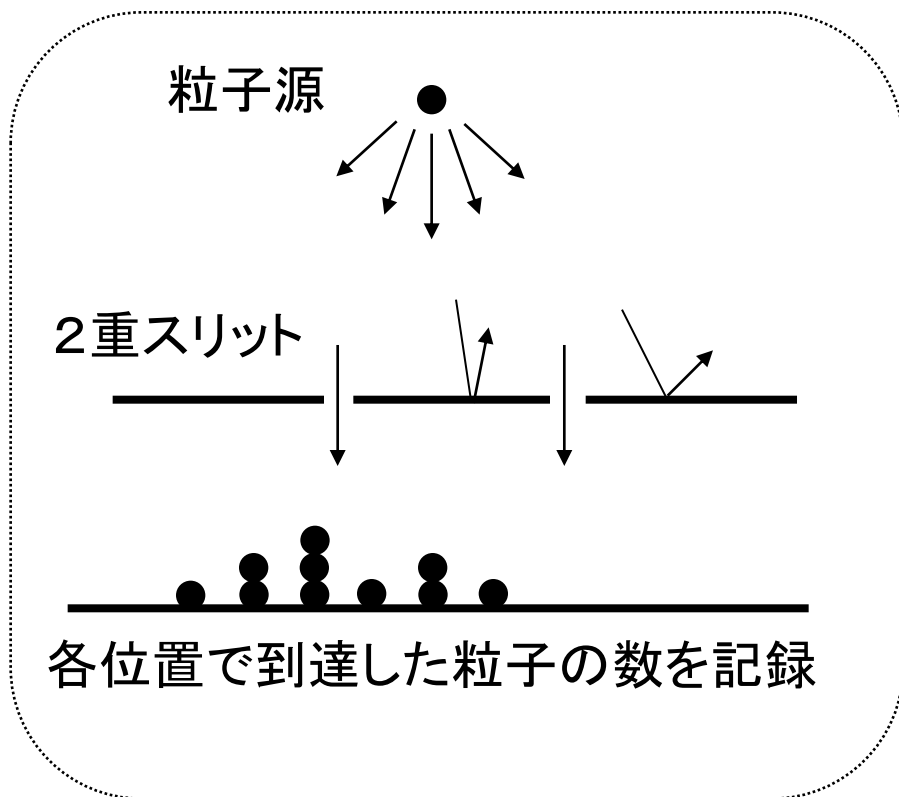
- 量子暗号: 解読不可能な究極のセキュリティ
- 量子通信: 量子テレポーテーションによる情報伝送
- 量子計算: 超並列処理による高速情報処理

情報・制御の概念を用いた自然法則の理解

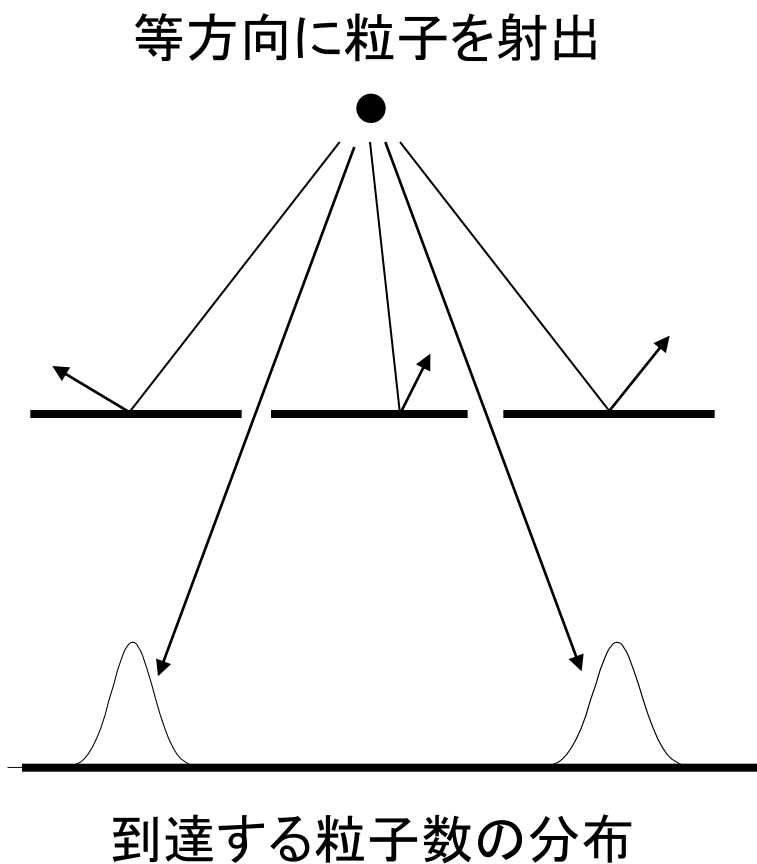
- 量子力学: ミクロな世界を支配する力学の基本原則
- 統計力学: 不可逆性に関する基礎理論

古典力学と量子力学の違い

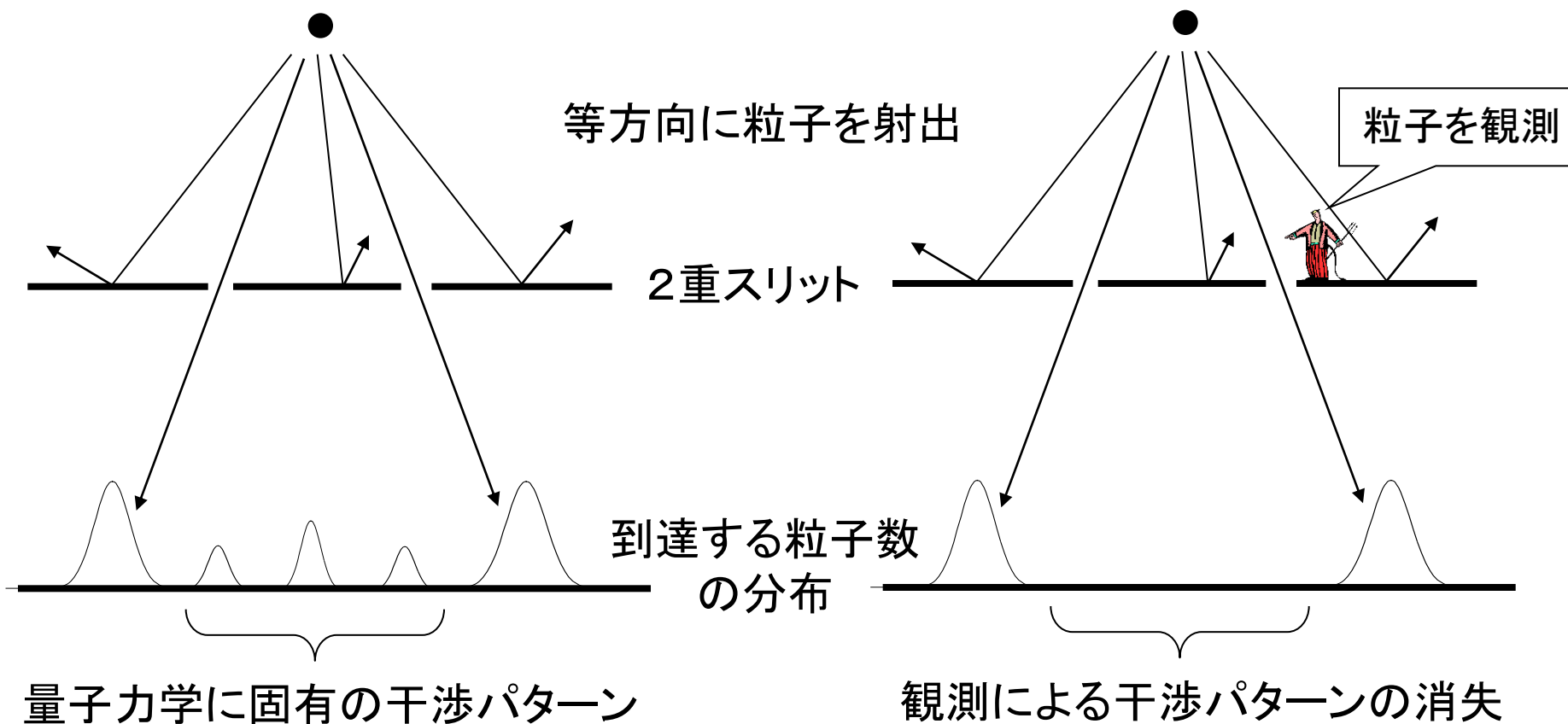
2重スリットの実験



粒子が古典力学に従う場合



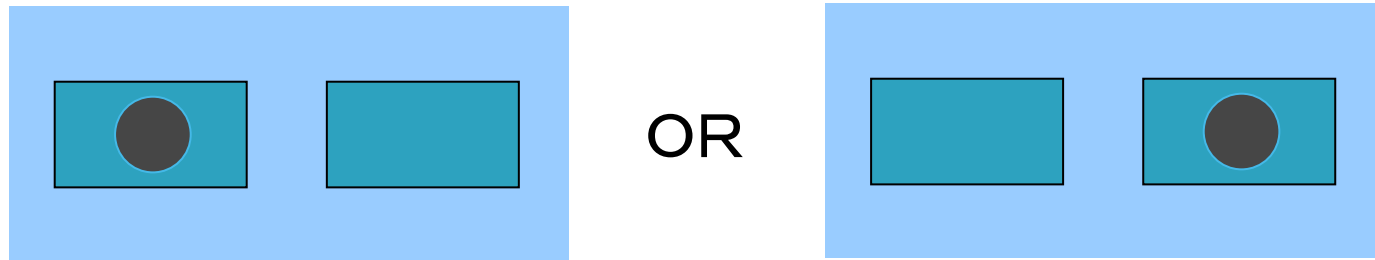
粒子が量子力学に従う場合



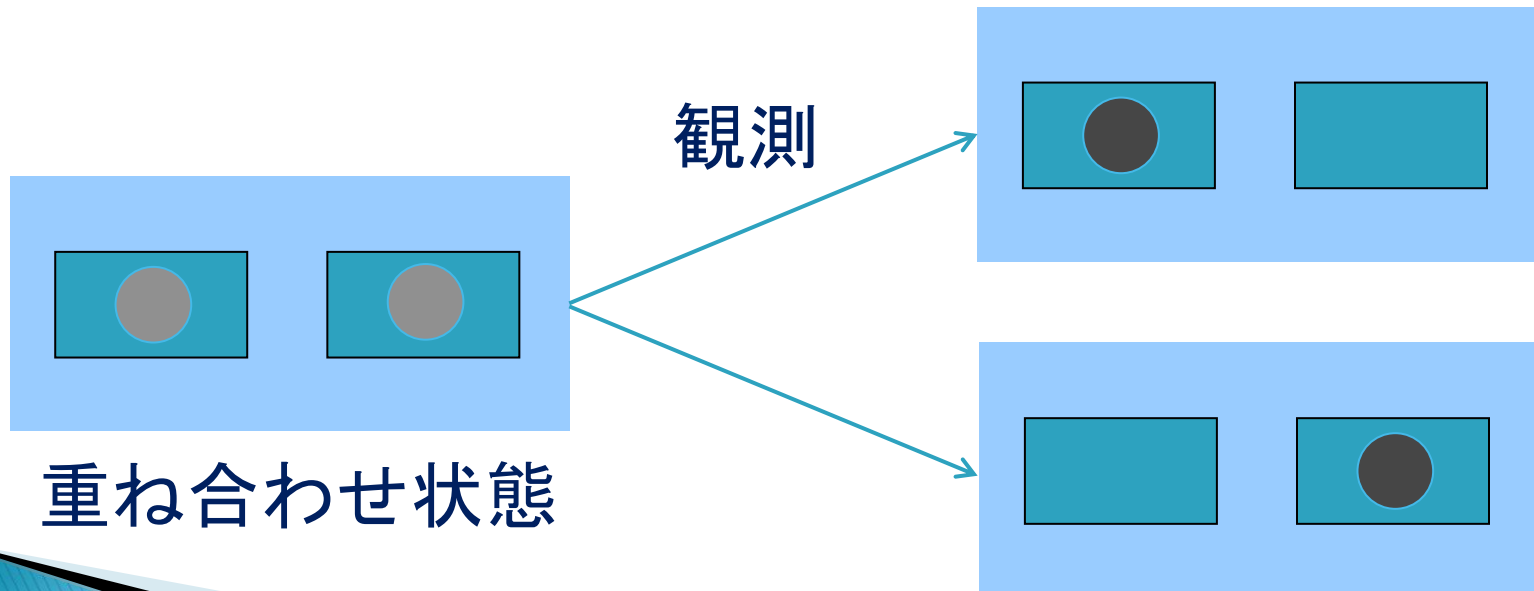
量子力学では、物質は粒子性と波動性の両方を持つ

- 状態の重ね合わせ
- 観測による状態の変化

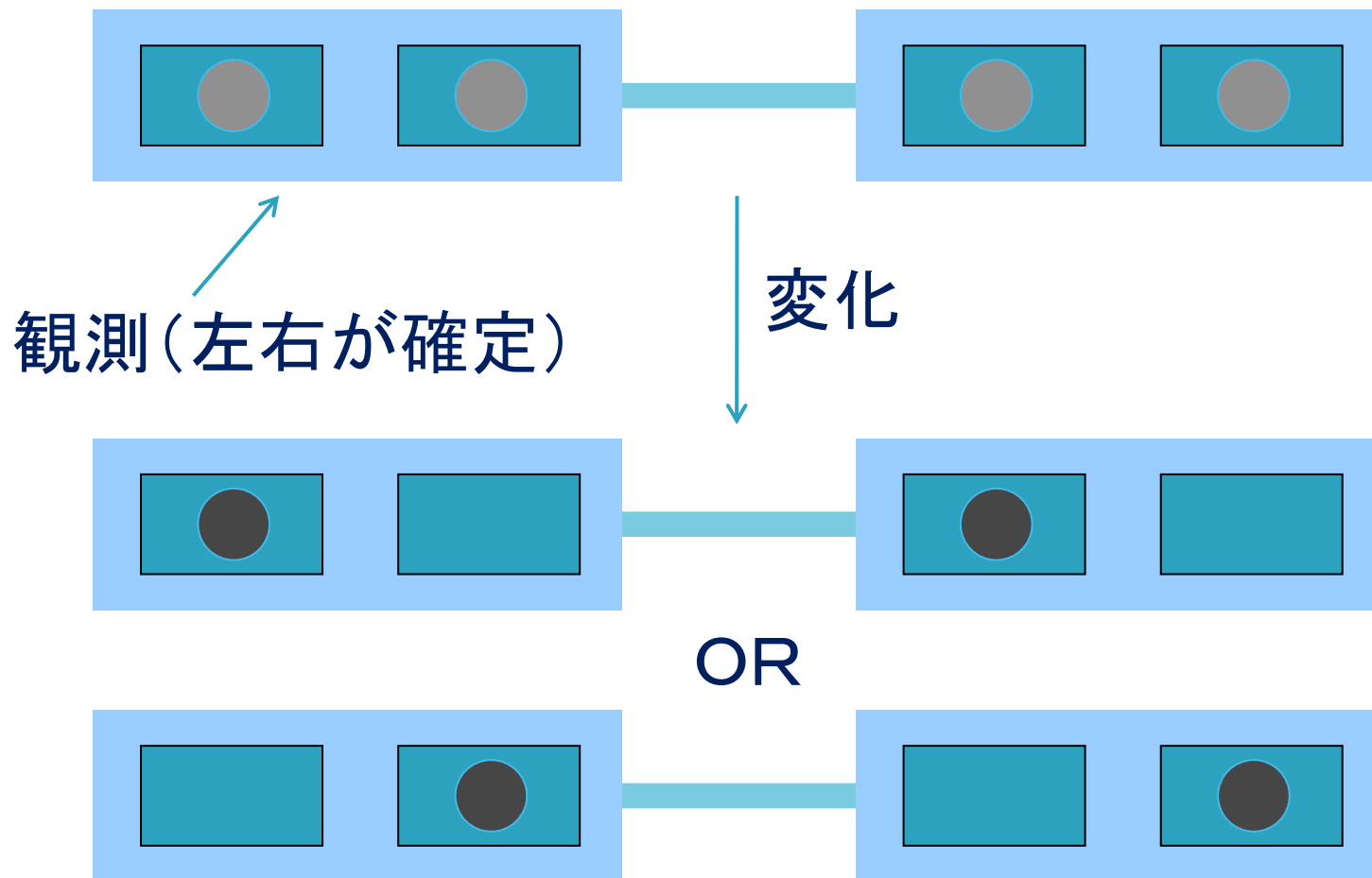
古典力学の世界(日常の世界)



量子力学の世界(原子分子の世界)



エンタングルメント(もつれた状態)



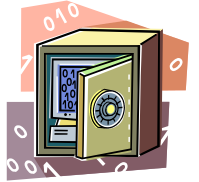
量子力学の基本原則

- 量子状態の重ね合わせ
- 量子測定による波束の収縮
(観測による状態の変化)
- エンタングルメント

従来の情報システムでは不可能であった新しい
情報処理、通信手段が実現可能

量子暗号、量子通信、量子コンピュータ

量子暗号



従来の暗号の安全性 = 数学的な計算の複雑さ・困難さ

公開鍵暗号・・・計算量的な安全性



コンピュータを使って解読するのに膨大な時間が掛かる
(大きな整数の因数分解は難しい)

量子暗号の安全性 = 自然法則によって保証された安全性

BB84プロトコル・・・無条件安全性



量子力学が正しい限り如何なる方法を用いても解読できない

状態の重ね合わせから導かれる不確定性原理、

複製不可能定理、識別不可能性による安全性の確保

量子通信



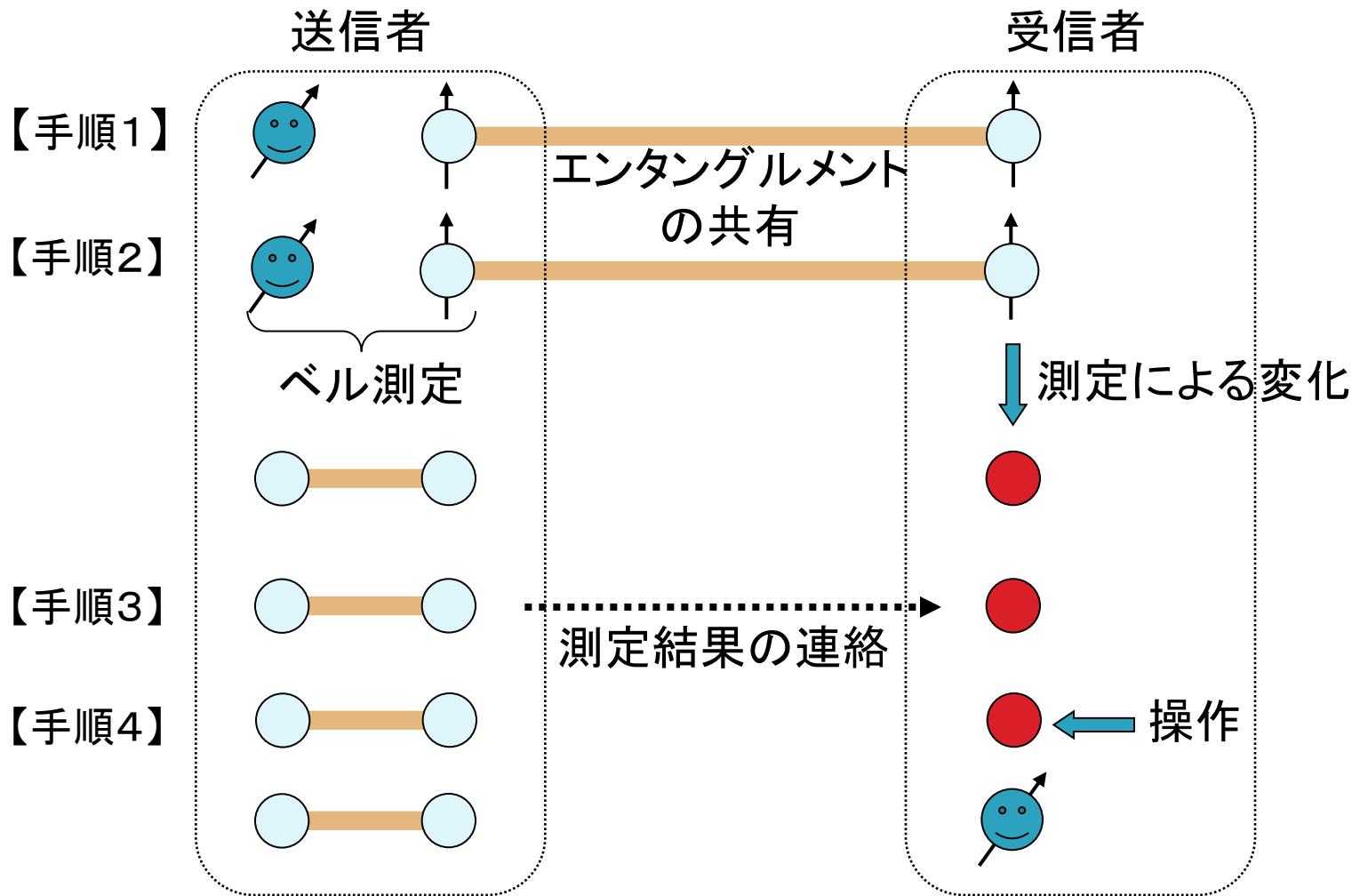
量子力学の基本原理を利用した新しい情報伝送方法

量子テレポーテーション・・・情報を担う実態(光、電波など)を直接送ることなく相手に情報を伝える方法

安全な情報伝送、量子コンピュータの要素技術

量子デンスコーディング・・・従来の通信の情報伝送効率の限界を超える高密度の情報伝送の方法

量子テレポーテーション



1998年 実験に成功！

量子計算



量子コンピュータ・・・量子力学の原理を用いた超並列処理

量子コンピュータが得意なこと

- データベース検索 (Groverのアルゴリズム)
- 因数分解、離散対数の計算 (Shorのアルゴリズム)



公開鍵暗号が解読可能

原子・分子の世界の力学が情報社会のセキュリティに
重大な影響を及ぼす

最後に

量子情報 (Quantum Information)

物理学と情報科学を融合した新しい研究分野



基礎から応用まで



基礎科学としての量子情報科学

未来のICTとしての量子情報技術