量子暗号について

量子力学から量子暗号まで

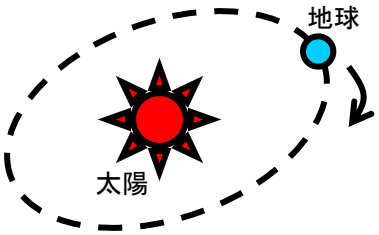
2009/5/16 Sao Haruka

目次

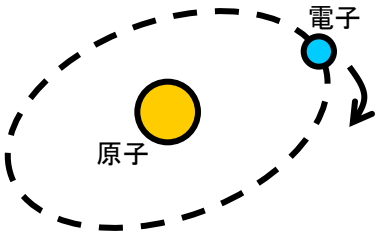
1. なぜ量子力学なのか

- **量子力学はなぜ必要？**

マクロな系



ミクロな系



一見すると同じ運動に見える

しかしミクロな系の運動は、既存の力学では説明できない

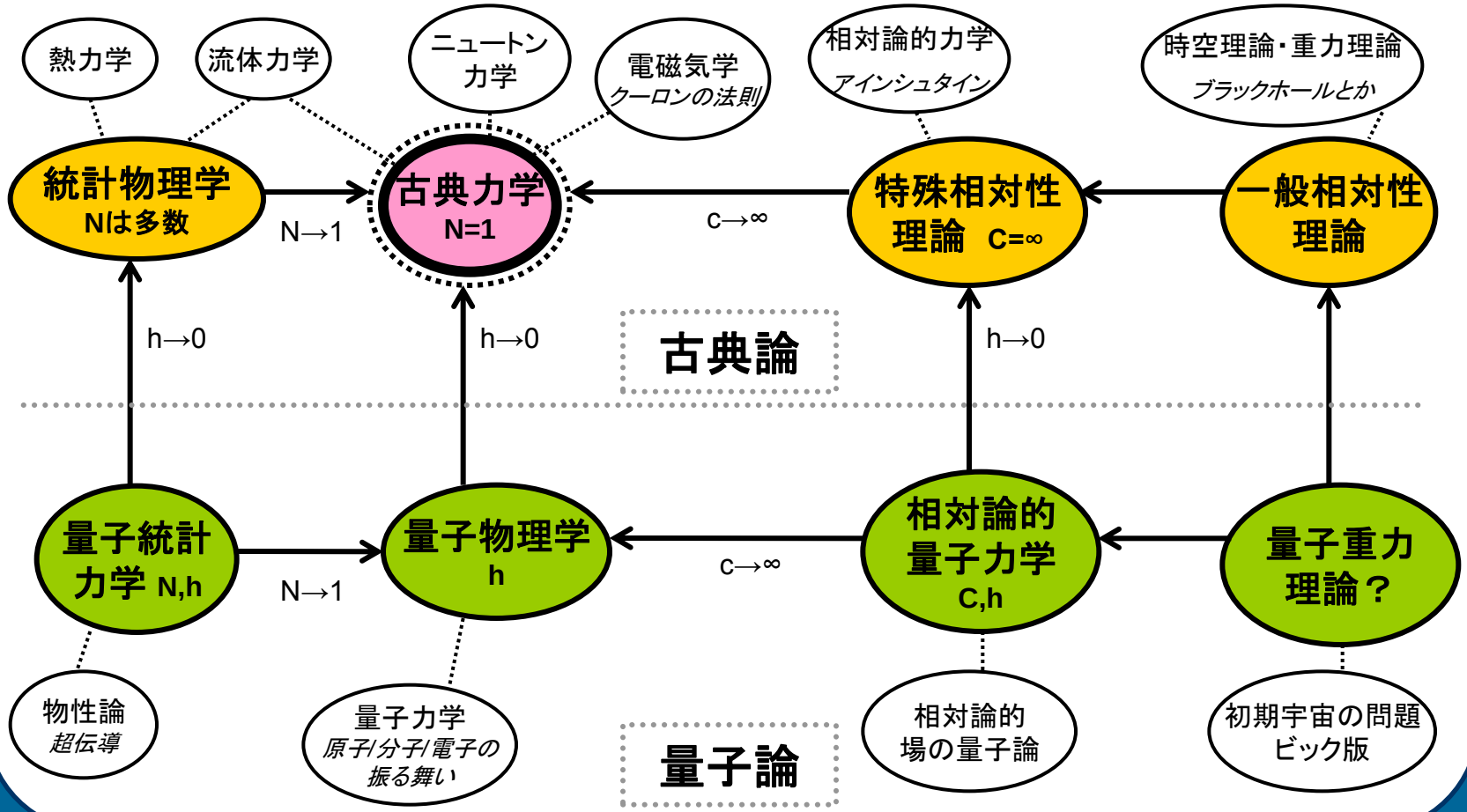
わたしたちの常識的理解に反する現象が起きている！

⇩

量子力学の誕生

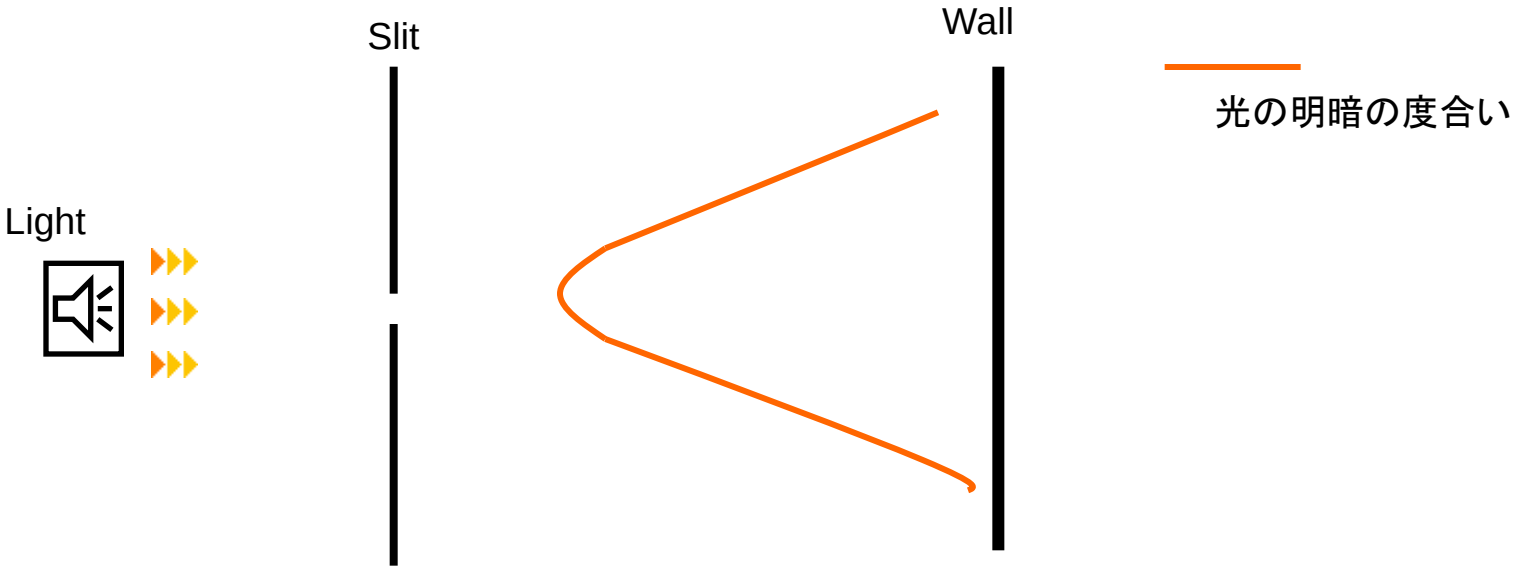
1-1. 物理の世界マップ

N:質点の数
h:プランク定数(10^{-27})
C:高速度(3×10^{8}m/s)



2-1. 光の干渉縞 スリット1本

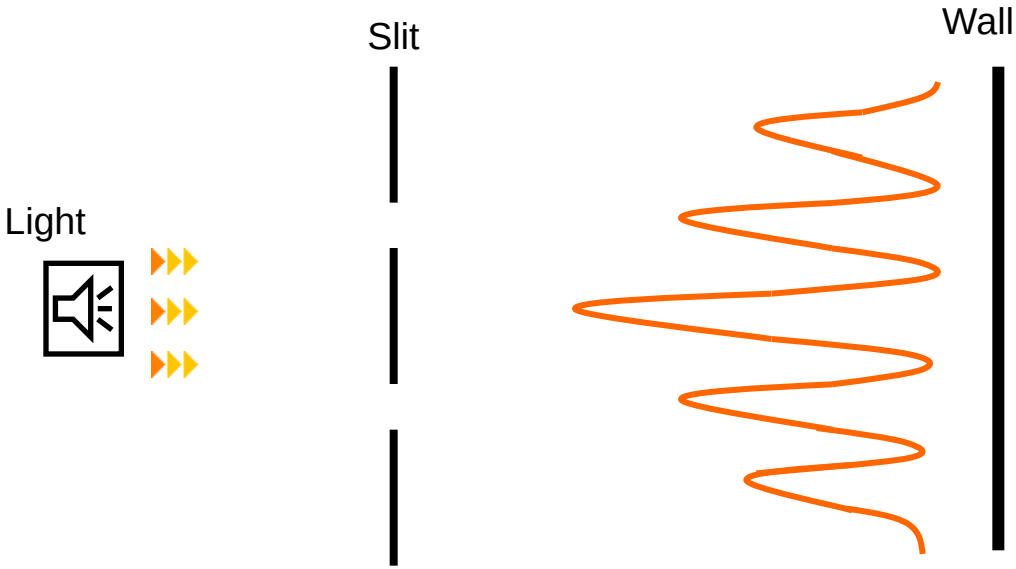
- スリットに光を当ててみよう



壁には、何が映るでしょう？

2-2. 光の干渉縞 スリット2本

- **スリットを2本にしてみる**

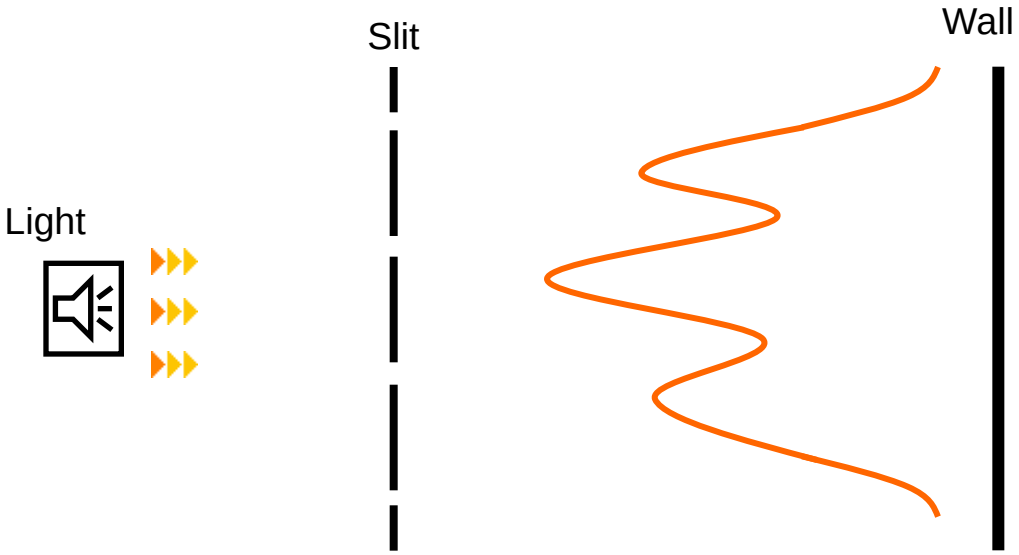


どんな模様に？

→ なんだか変じゃないですか？

2-3. 光の干渉縞 スリット4本

- **スリット4本だったら…？**

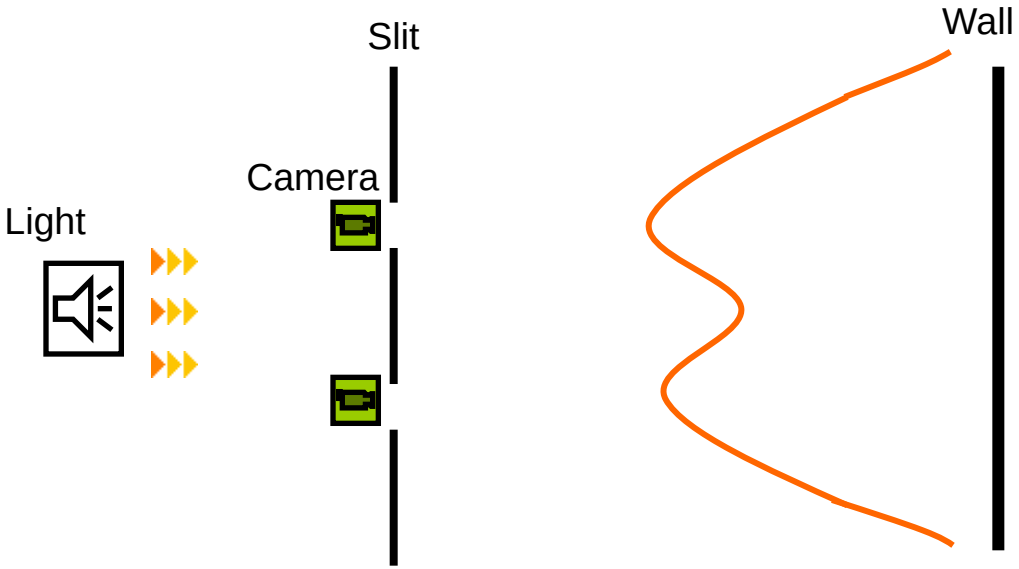


どうなるの？？？

→ 模様の数が減ってる？

2-4. 光の干渉縞 スリット2本 観測付き

- 一体各スリットをどんな光が通っていってるんでしょう？

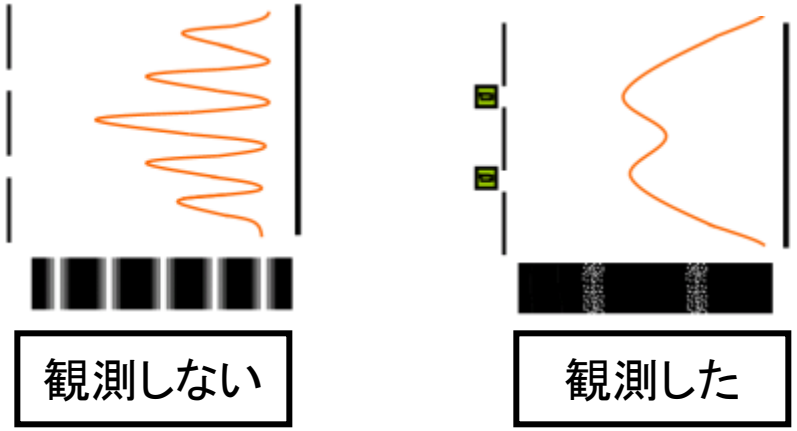


光の縞模様は、どんな風に出るのでしょうか？

→ さっきと結果が違う！！

2. 量子力学の特徴(1)

- 見る(観測する)というわたしたちの行為によって結果は変わってしまう



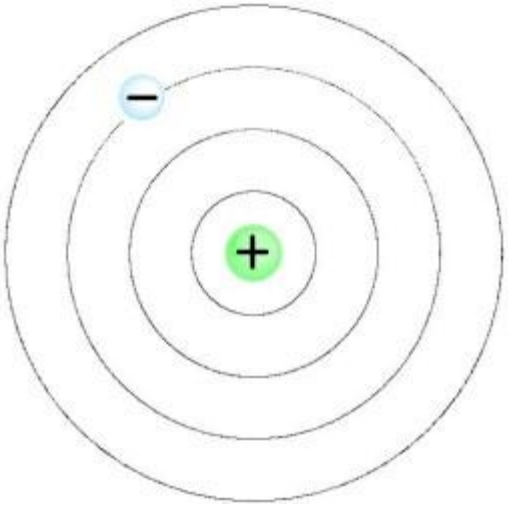
∴どんな経路を通って光が壁に届いているのかは判らない

特徴1 判るのは**結果のみ**、状態は判らない

特徴2 **観測する**ことによって、状態が変化(確定)する

3-1. 電子の軌道

- **電子の軌道について**
  - 原子の周りを電子が回っている



3-1. 光を当ててみる

- **この物質に光を当ててみるとどうなるのか？**

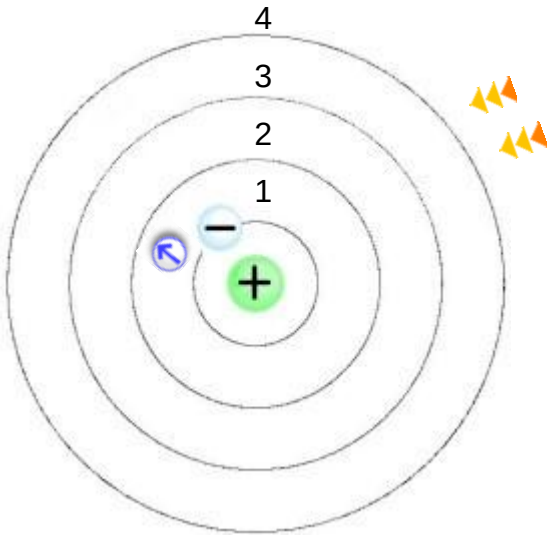
光を吸収して、電子は
1番目の軌道から
2番目の軌道に遷移する

↓

遷移するとき
その間のどこを通っているのかは
判らない

↓

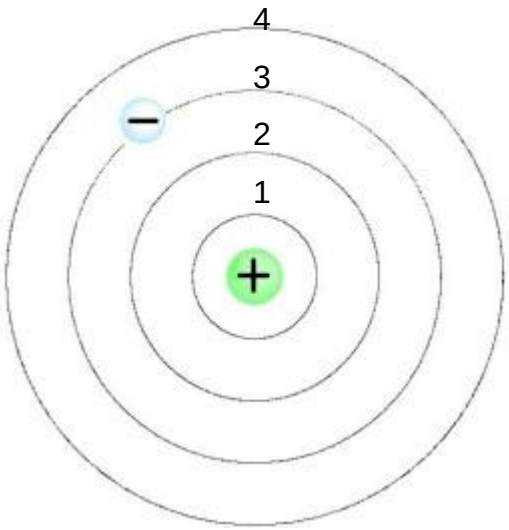
電子は自由な位置の半径を回ることは出来ない
ある決まった半径でしか、運動はできない



3. 量子力学の特徴(2)

特徴3

とびとびの位置にのみ存在する



4. 量子ビット

- **わたしたちの知っているビット：古典bit**
  - 1bit は“0 or 1”の値を取る

4. 量子ビット

- **量子力学的なビット：量子bit=qubit**
  - これも、1bit は “0 or 1” の値を取るんですが…
  - 表記を |0>, |1> と書きます

4. 量子ビット

- **古典bit と qubit の違いは？**

  - qubit は |0> or |1> 以外の**状態**も表せます

  - 1qubit を
    $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$
    という**重ね合わせ状態**（量子状態）で書くことができます

つまり

“ |0> か |1> か、まだ判らないが、何らかの状態を保持しているビット”

ということになります

4. 量子ビット

- **1qubitの状態**

$$|\psi\rangle = \alpha\ |0\rangle + \beta\ |1\rangle \qquad (4\text{-}1)$$

- **2qubitの状態**

$$|\psi\rangle = \alpha\ |00\rangle + \beta\ |01\rangle + \gamma\ |10\rangle + \delta\ |11\rangle \qquad (4\text{-}2)$$

:

5. 復習

- **ここでちょっと復習**

> 1. 判るのは結果のみ、状態は判らない
> 2. 観測することによって、状態が変化（確定）する
> 3. とびとびの位置にのみ存在する

この事実を元にすれば、1qubit の重ね合わせ状態の式はどんな現象を表していることになるのか？

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

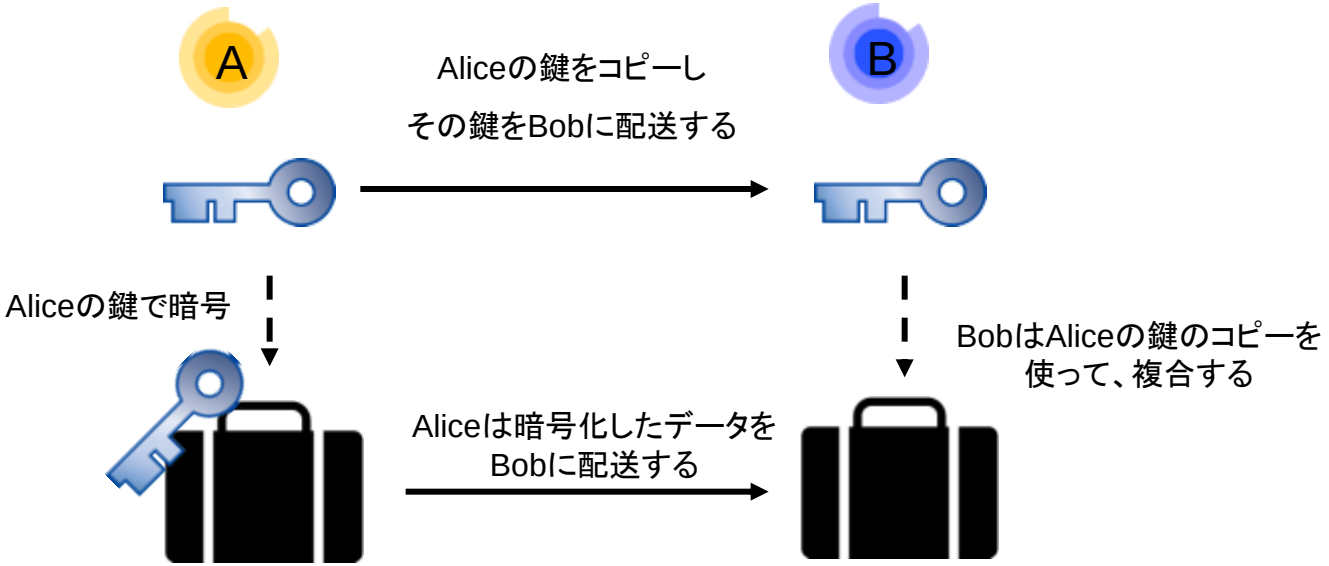
⇒ α、βの値は、決めることはできない（量子状態は判らない）

⇒ 例えばαを観測すると、βが決まってしまう（“見る”と、状態は確定する）

⇒ 結果は 0 or 1 (不連続な値を取る)

5-1. 既存の暗号技術

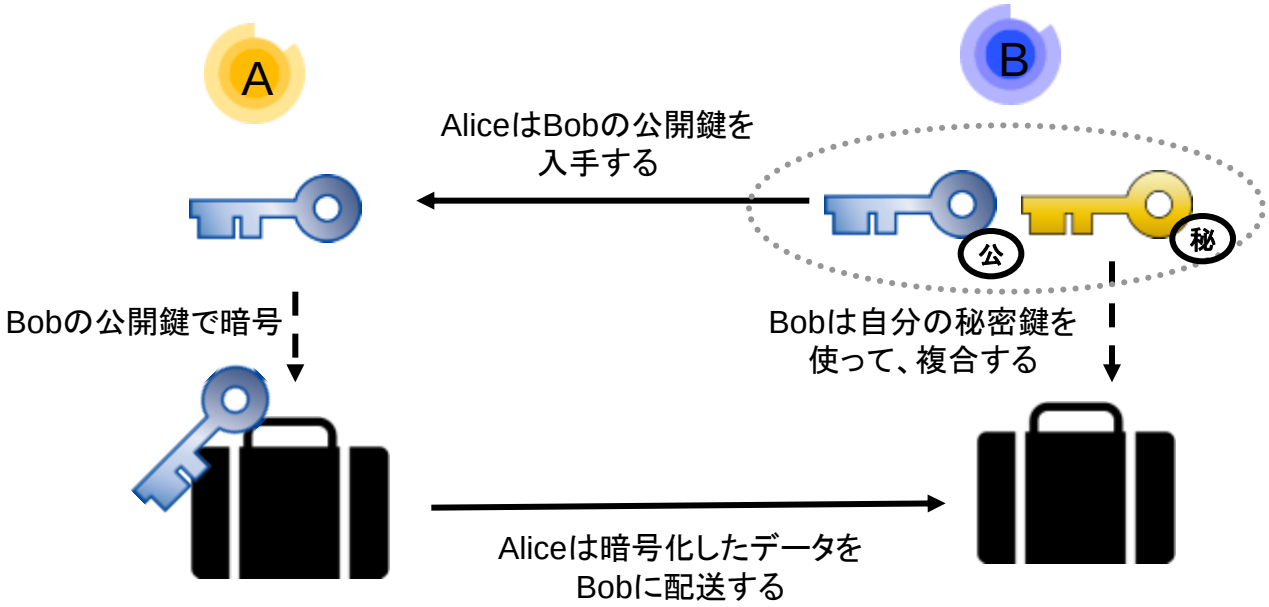
- **秘密鍵暗号システム**



鍵の配送が困難
Alice は複数個の鍵を管理しなければならない

5-1. 既存の暗号技術

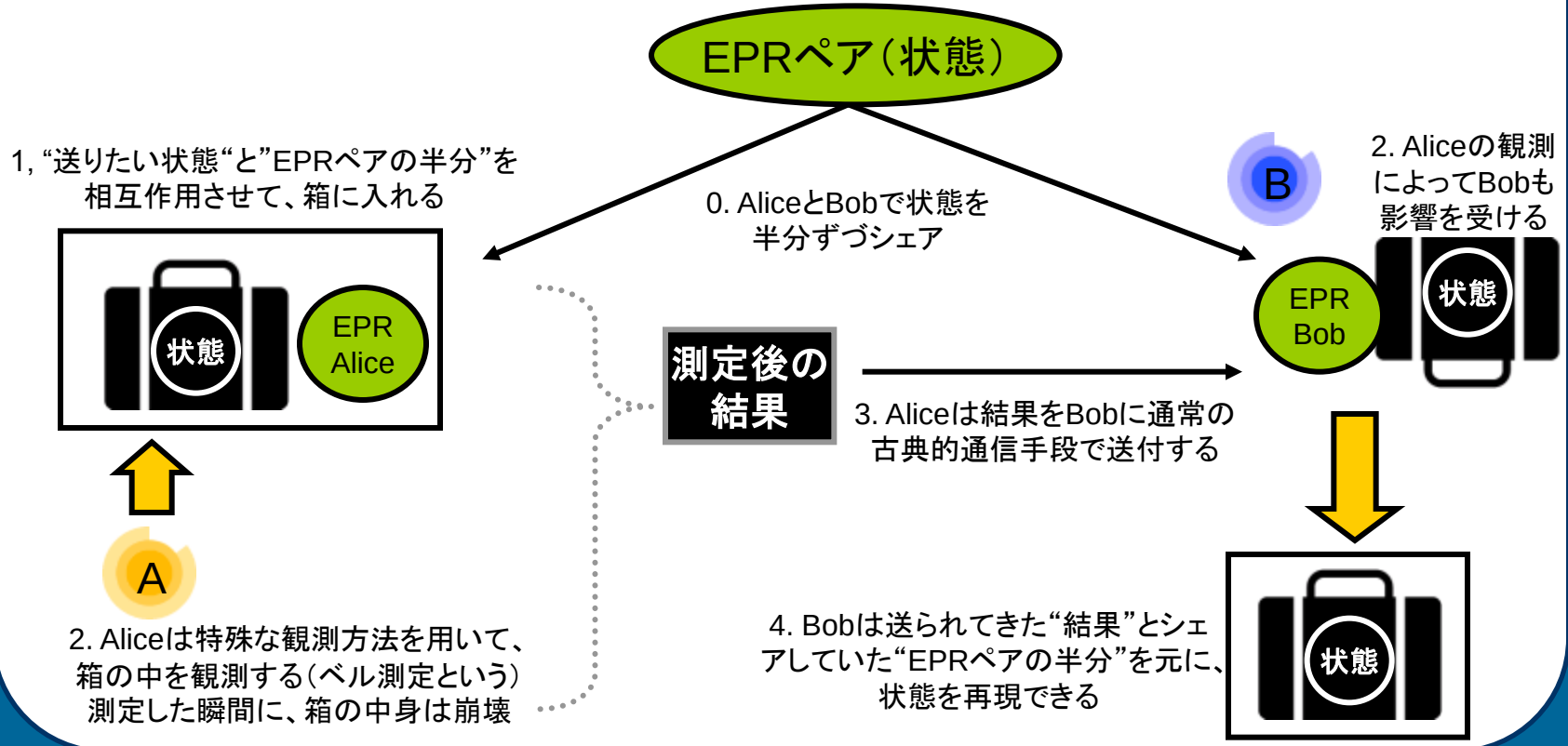
- **公開鍵暗号システム（RSA暗号）**



第3者の複合は困難だが、時間をかければ不可能ではない
複合に時間がかかる

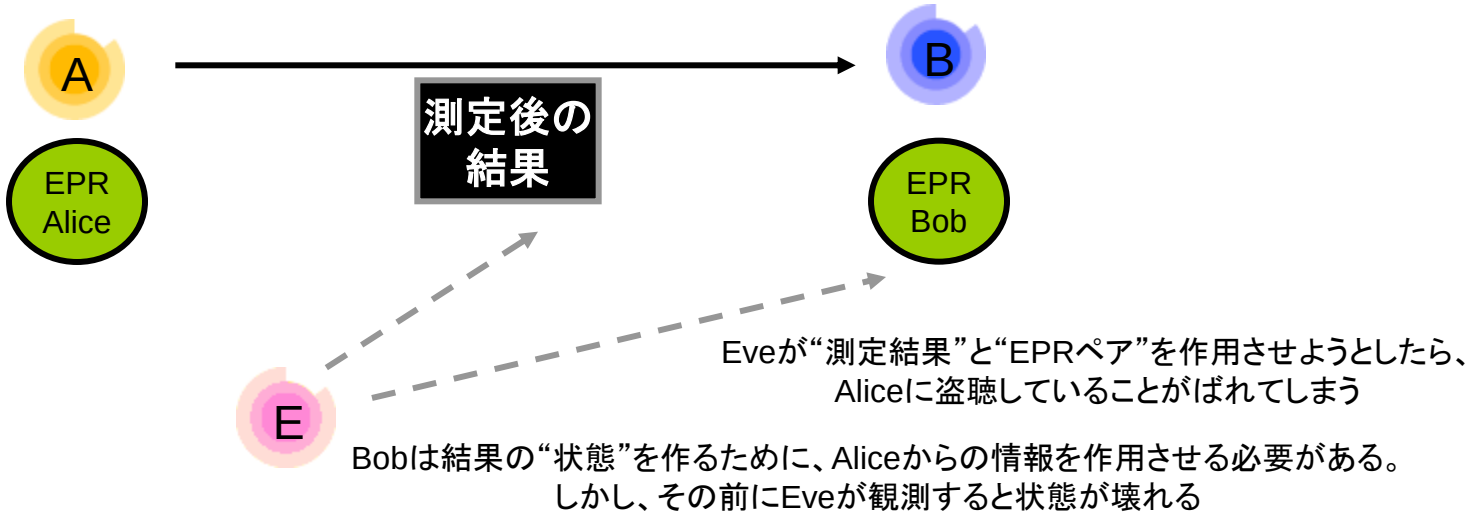
6. 量子テレポーテーション

- **もっとも基本的な量子暗号の仕組み**



6. 量子テレポーテーション

- **もし、だれかに傍受されたらどうなるのか？**
  - つまりAliceの測定後の結果と、Bobの持つEPRペアの片割れを Eve が不正に取得したとする



こっそり盗聴することは不可能

7. 実際にサーバはあるの？

- **NMRを用いた量子コンピュータ（核磁気共鳴）**
  - NMRとは：高分解能溶液（溶液中に10^{15}個の分子を含んでいる）
  - 溶液に電磁場をかけ、スピンを制御する
  - 2qubit の量子アルゴリズムは確立

8. 量子暗号に関する話

- **qubitを保存する方法は研究中**
  - 液体のままではまだまだ普及しない
- **EPRペアの配送方法？**
  - 配送途中で、雑音などで壊れそう
- **量子コンピュータの普及により、暗号が変わる！**
  - 既存の公開鍵暗号システムは使用できなくなる
    - 計算能力が早くなるため、解読されやすくなる
- **量子コンピュータに必要な観測回路、演算回路は、天才でないと作れない**
  - &（and）や |（or）回路は、古典コンピュータにまかせよう

終わり