情報通信工学序論

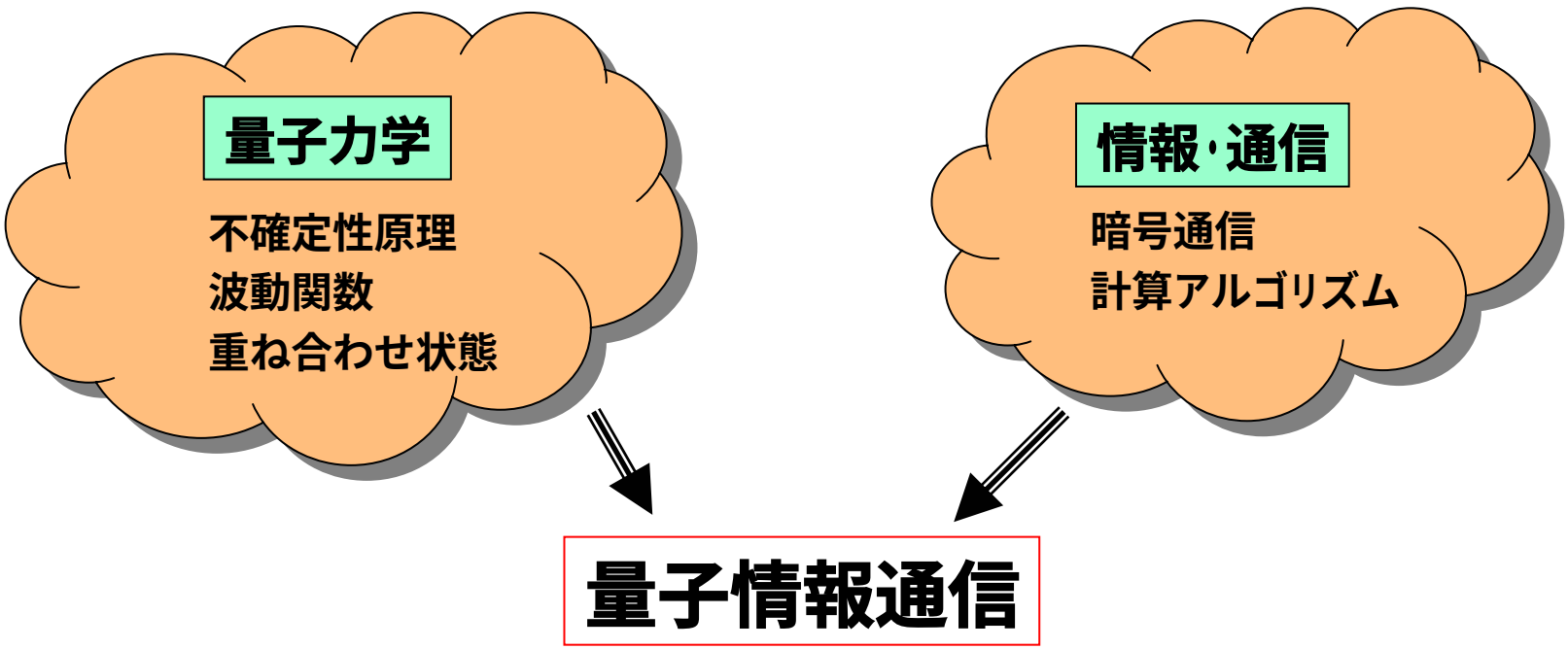
平成18年11月30日

量子情報の話

-究極の暗号通信から超並列情報処理まで-

電気電子情報工学専攻
情報通信部門
極限光通信工学領域
井上　恭

量子力学と暗号通信・情報処理との融合

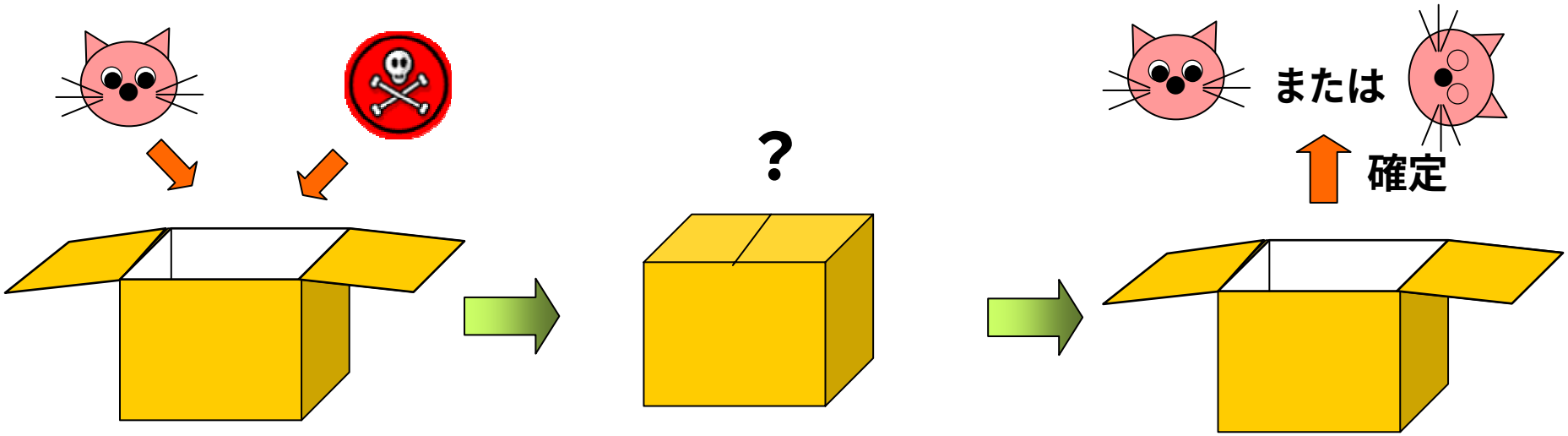


今日の内容

1. 量子力学の原理1
2. 量子暗号
3. 量子力学の原理2
4. 量子コンピュータ

まずは量子力学の話

シュレディンガーの猫



問題：　箱の中の猫の状態は？

答1：　生きているか死んでいるかのどちらか。決まっているけど見えないだけ。← 古典

答2：　生きているかもしれないし、死んでいるかもしれない。
わからないのだからどちらもあり。← 量子

量子力学では、どちらの状態もありと考える。＝「重ね合わせ状態」

$|\psi> = a(t)|$  $\rangle + b(t)|$  $\rangle$

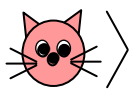
生きている　死んでいる

但し、閉じ込めた直後と長時間経過後だと様子も違うだろう。

↓

重み付け係数 a, b で区別

観測すると、どちらかに決定

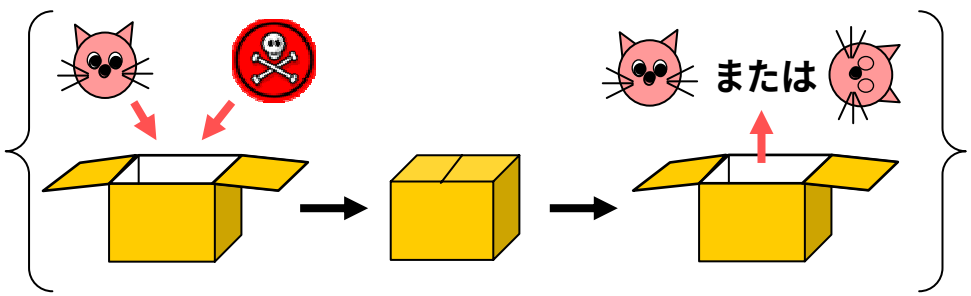
$|\psi> =$  $\rangle$　**または**　$|\psi> =|$  $\rangle$

どちらになるかは確率的

$|$  $\rangle$ **の確率** $= |a|^2$

$|$  $\rangle$ **の確率** $= |b|^2$

確率的の意味は、

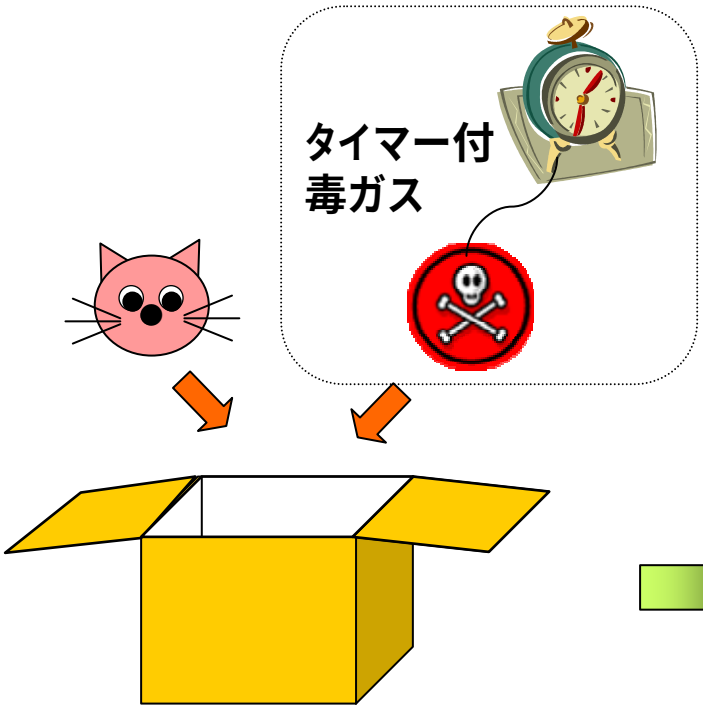


x**回繰り返すと** ⇨

 **が** $|a|^2 \times x$ **回**

 **が** $|b|^2 \times x$ **回**

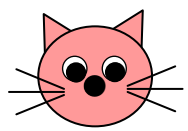
原理的にどちらかわからない事がポイント



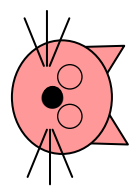
(時間がきたら必ず死ぬようにセット)

封印状態でも原理的に生死はわかる

タイマー動作時刻前は



タイマー動作時刻後は



↓

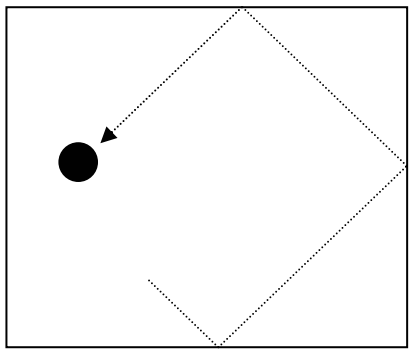
重ね合わせ状態ではない

量子力学の基本その1

物理状態は確率的

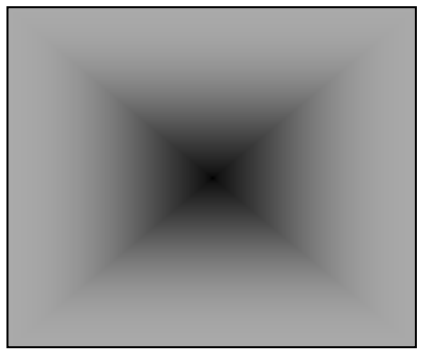
(例えば箱の中の電子)

古典力学



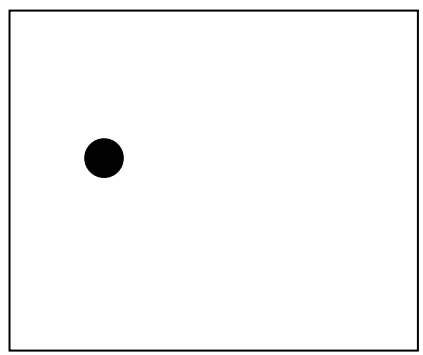
位置は確定

量子力学



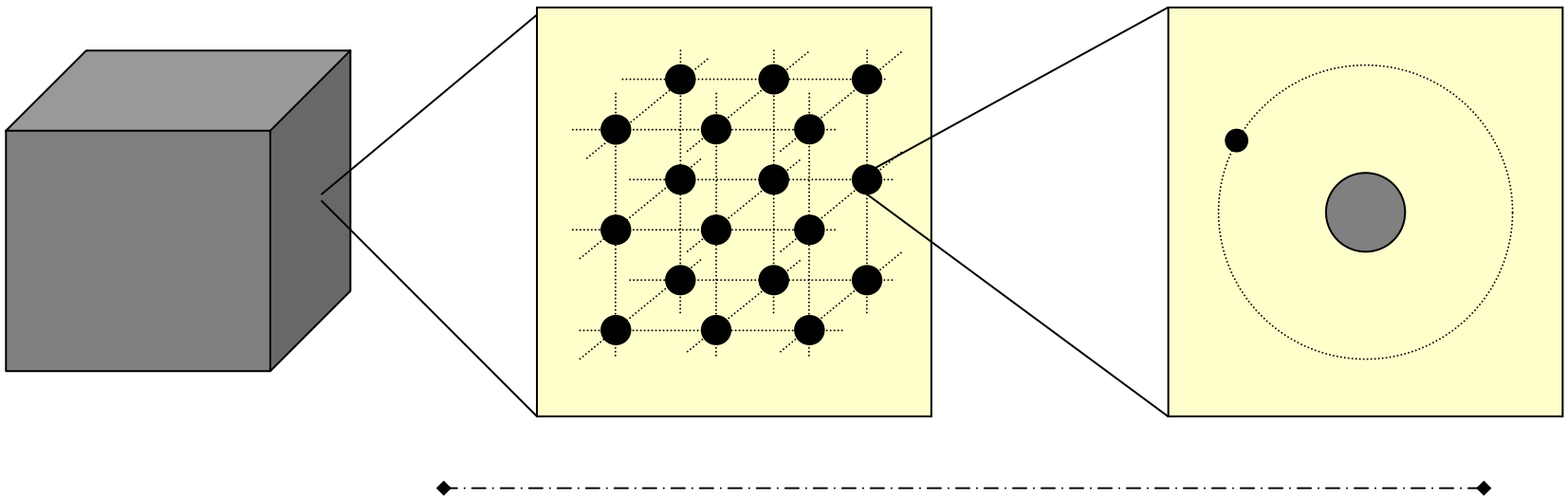
どこに居るか不確定。
確率分布だけが与えられる。

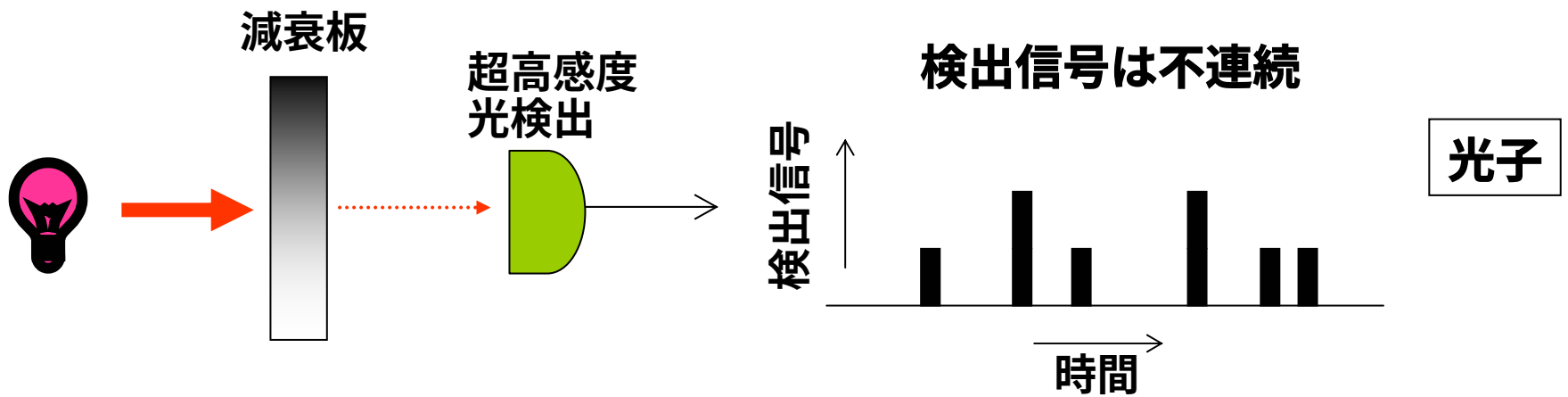
観測すると確定



量子力学の基本その2

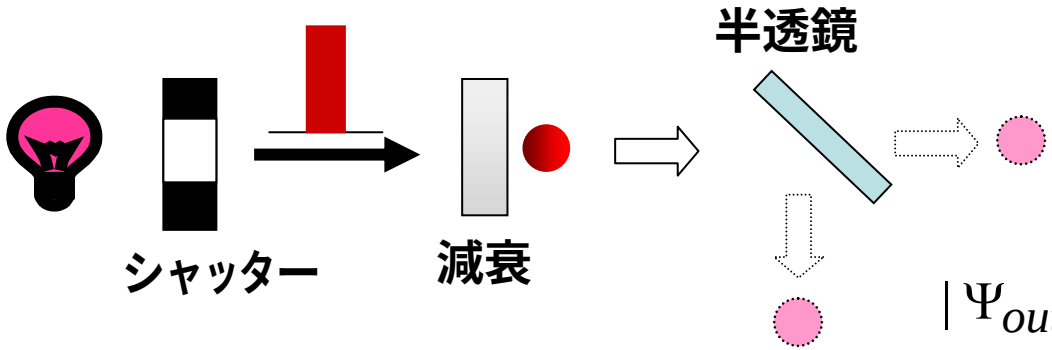
全てのものは
それ以上分割できない最小単位から成り立っている





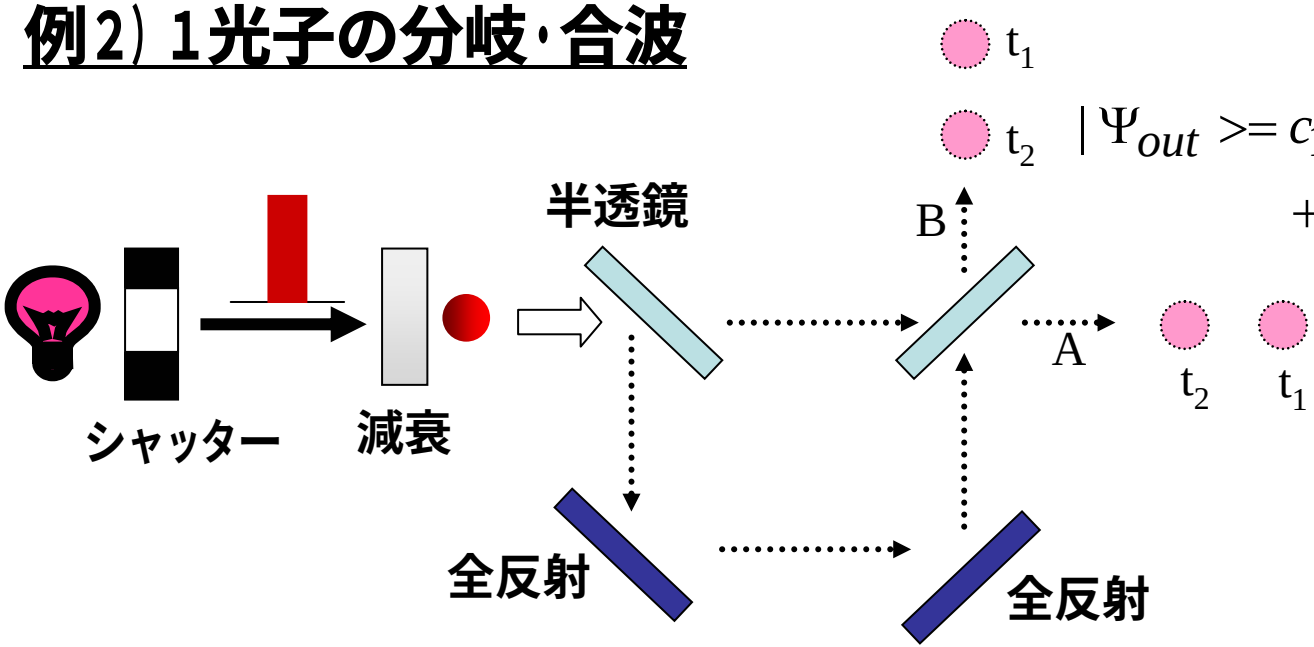
最小単位の重ね合わせ状態

例1）1光子の分岐



$$|\Psi_{out}>= a\,|\text{透過}> + b\,|\text{反射}>$$

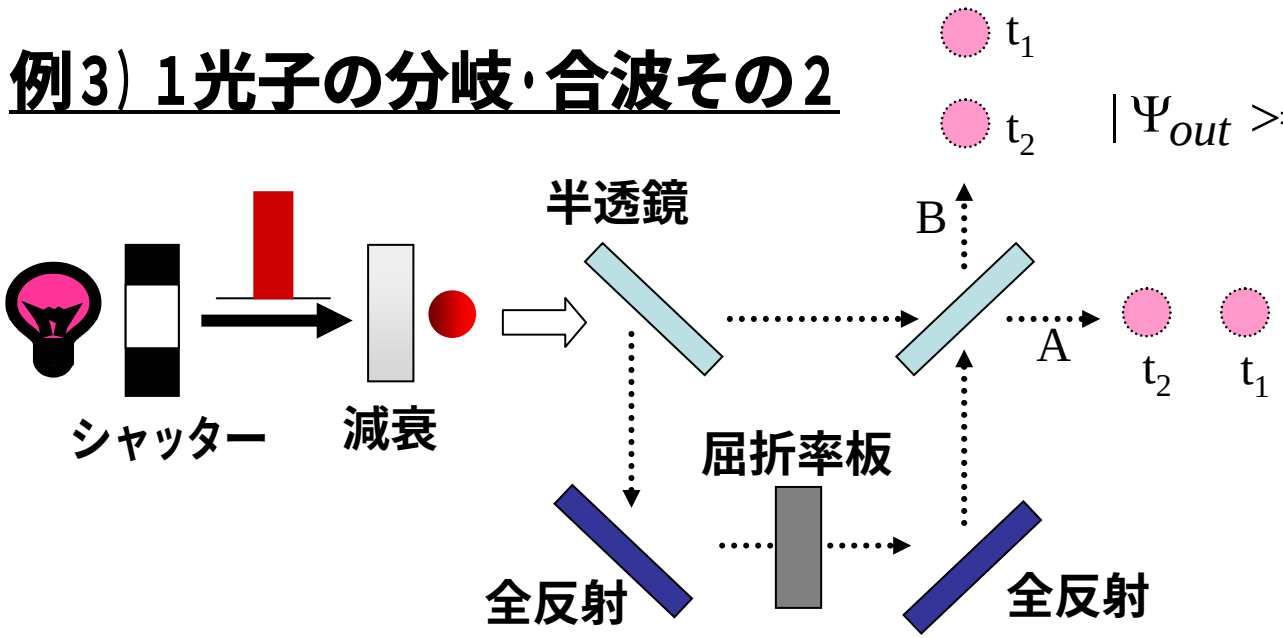
例2）1光子の分岐･合波



$$|\Psi_{out}>= c_1\,|\mathrm{A},\mathrm{t}_1> + c_2\,|\mathrm{A},\mathrm{t}_2> + c_3\,|\mathrm{B},\mathrm{t}_1> + c_4\,|\mathrm{B},\mathrm{t}_2>$$

重ね合わせの係数は複素数

例3）1光子の分岐・合波その2



$$|\Psi_{out}>= c_1|\mathrm{A},\mathrm{t}_1>+c_2|\mathrm{A},\mathrm{t}_2> +c_3|\mathrm{B},\mathrm{t}_1>+c_4|\mathrm{B},\mathrm{t}_2>$$

例2と例3は、光子の確率は同じだけれど、状態としては違うはず。

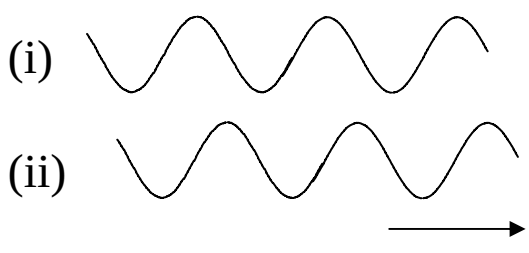
↓

これを区別するには、重み付け係数を複素数とし、|係数|^2 で確率を与えるようにする。

経路状態の違いは、複素数の位相で反映。

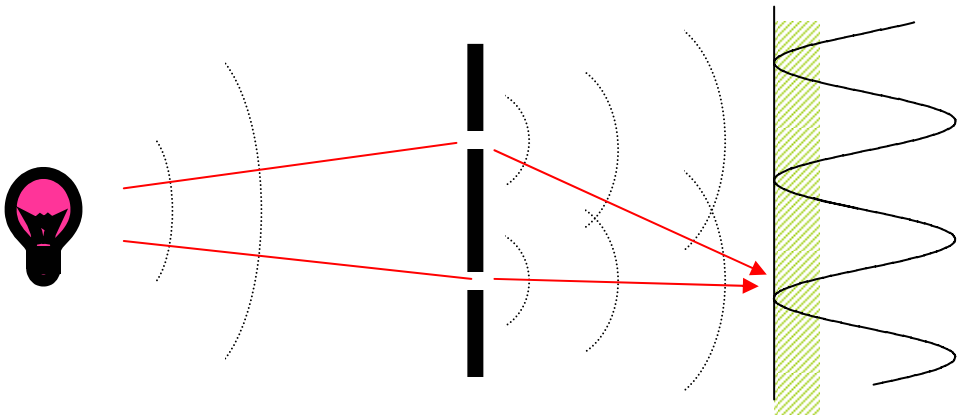
$$c = Ae^{i\theta}$$

位相：例えば、波の振動の位置

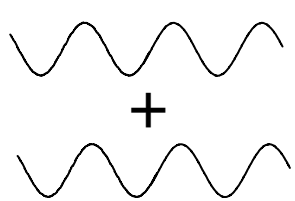


量子力学の原理

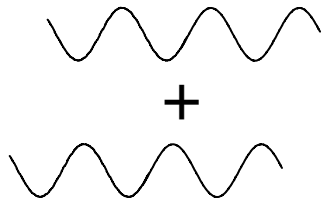
重ね合わせは干渉する



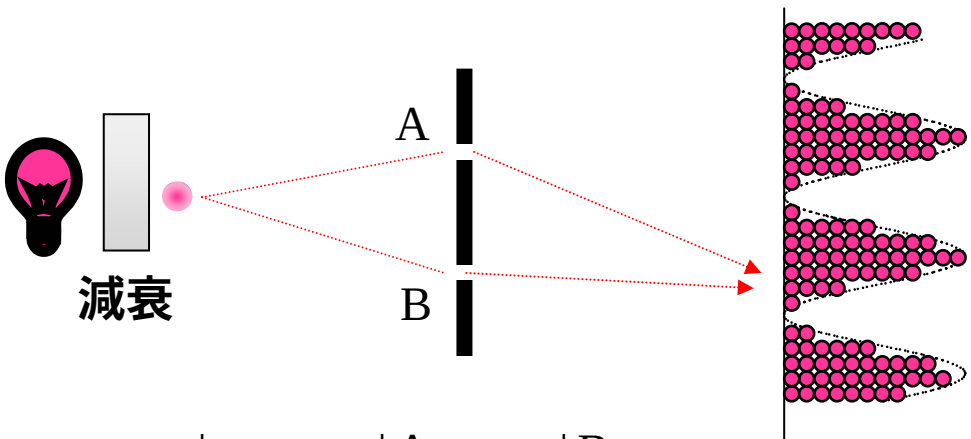
2つのピンホールを経由した光が強めあったり弱めあったり。



強め合う



弱め合う

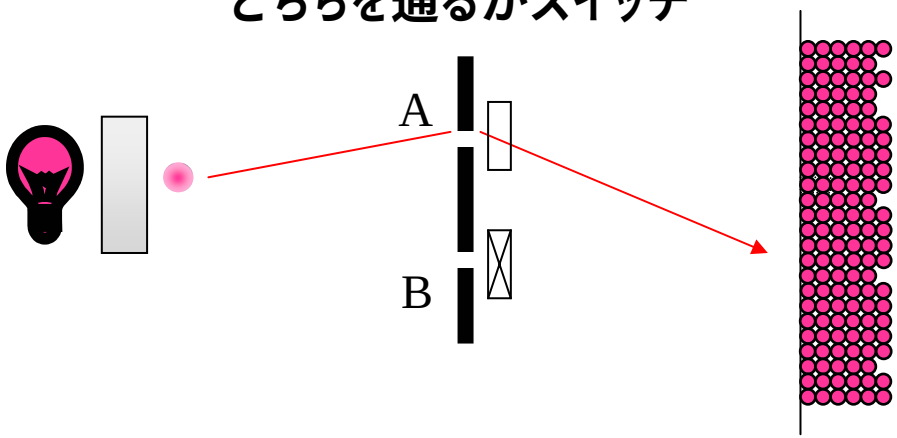


$$|\psi>=c_a|\mathrm{A}>+c_b|\mathrm{B}>$$

2つのピンホールを経由した光子状態の係数が強めあったり弱めあったり。

|A>：光子がAを通った状態
|B>：光子がBを通った状態

どちらを通るかスイッチ



干渉縞は消滅

$$|\psi>= c_a |\mathrm{A}> + c_b |\mathrm{B}>$$

$$|\psi>=|\mathrm{A}> \quad \text{or} \quad |\psi>=|\mathrm{B}>$$

単にひとつのピンホールを通った状態

量子情報通信

量子力学的重ね合わせを安全な暗号鍵配布システムに利用しよう

↓

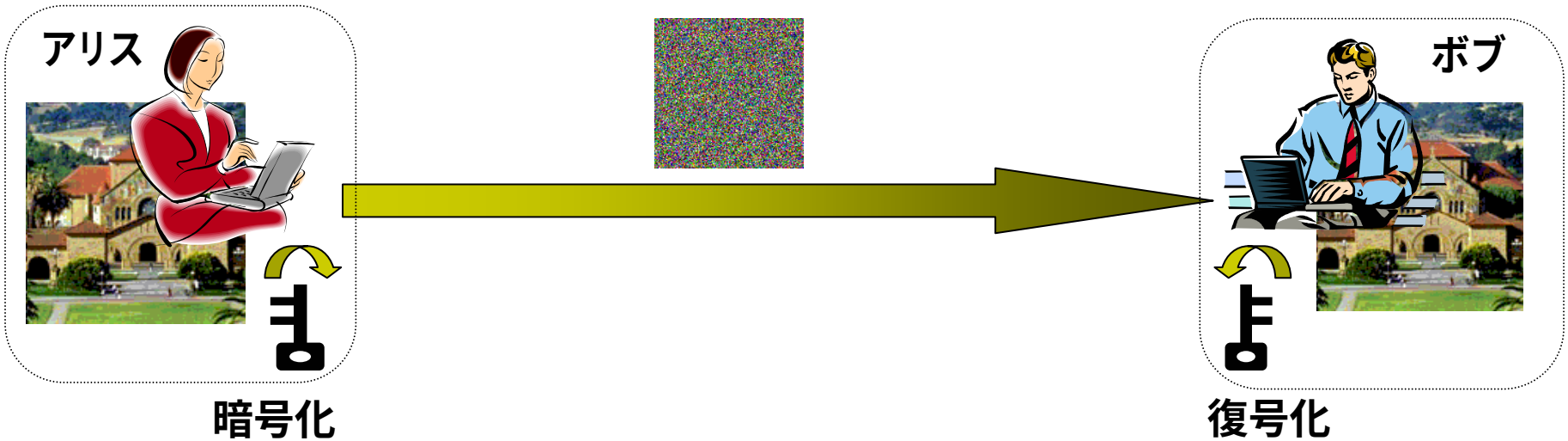
量子暗号 (量子鍵配送)

量子力学的重ね合わせを超並列計算に利用しよう

↓

量子コンピュータ

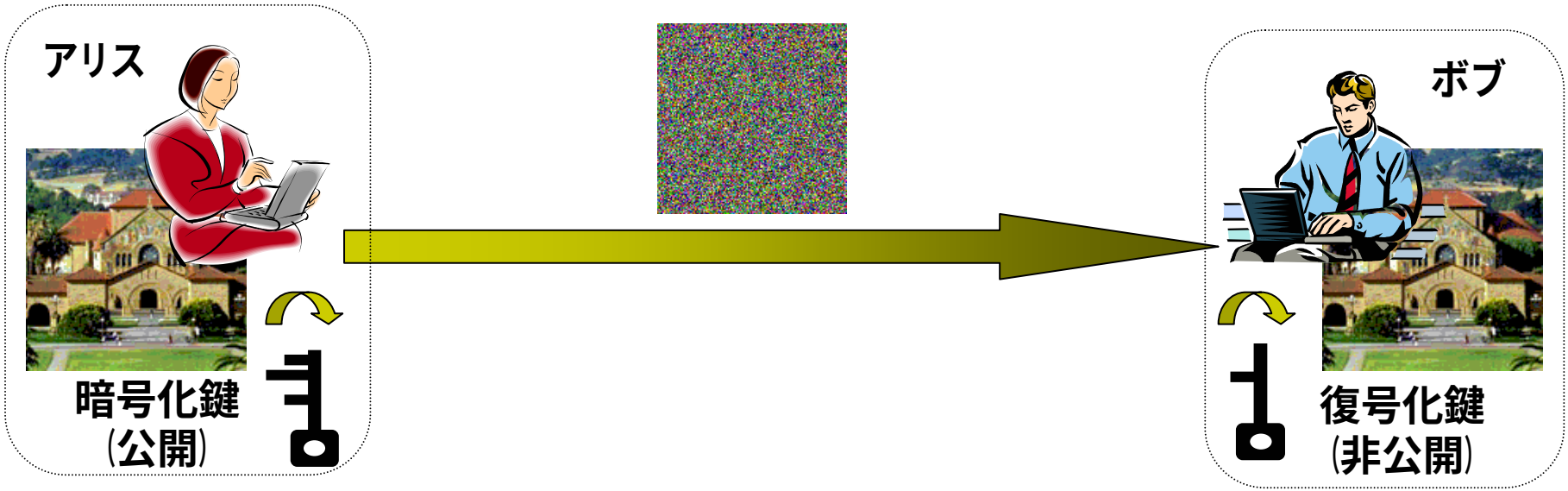
暗号通信

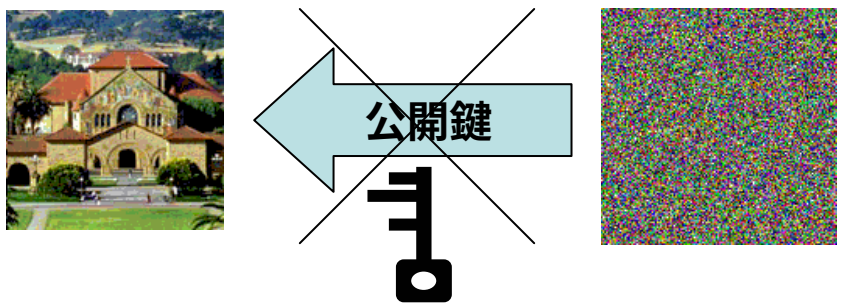


暗号化方法/複合化方法をどうやって離れた2者で共有するかが問題

そこで現代暗号では

公開鍵暗号方式



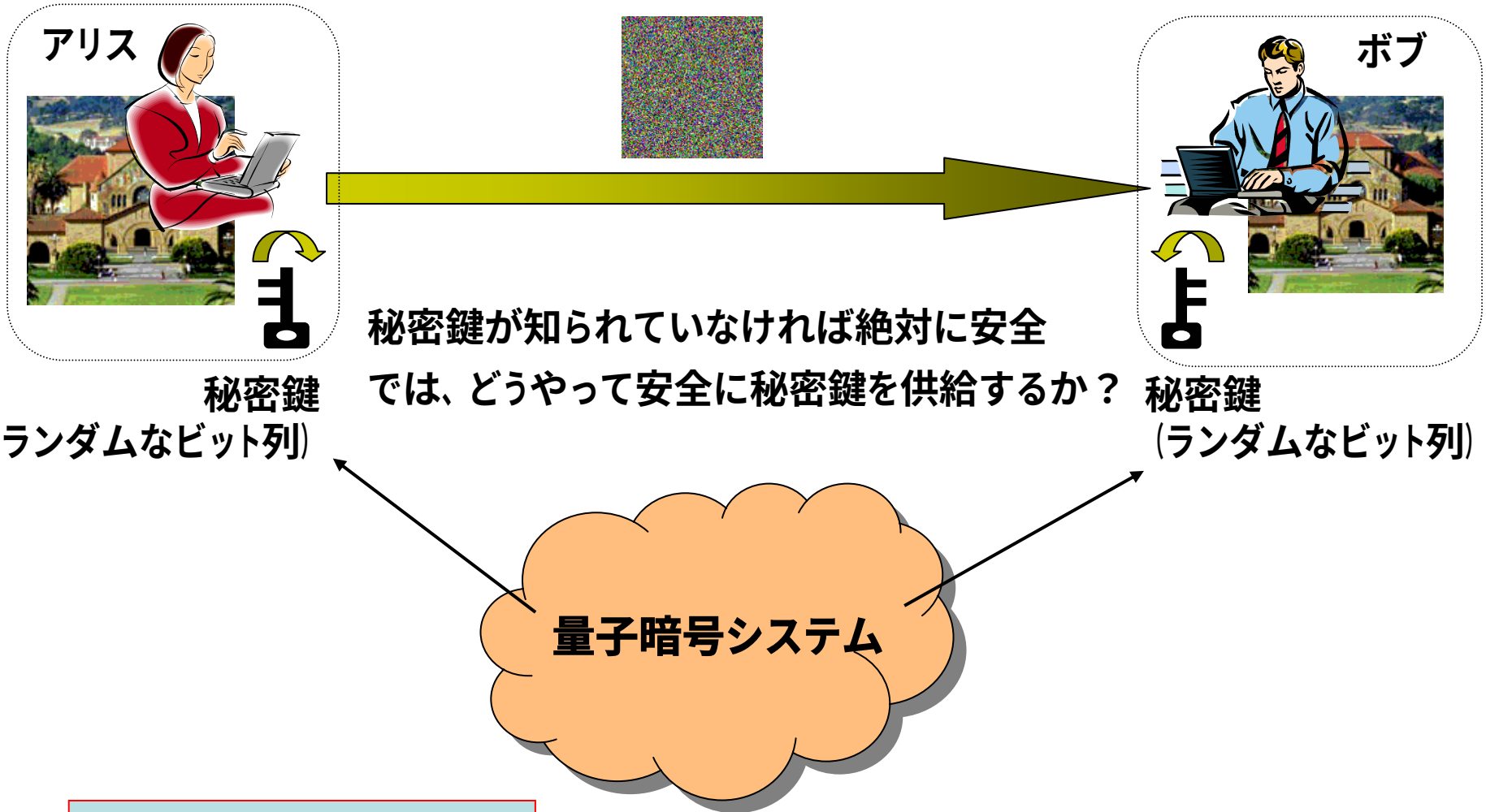


367 × 521 = ? ：簡単（答は191207）

? × ? = 191207 ：難しい

原理的には解読可能

秘密鍵暗号

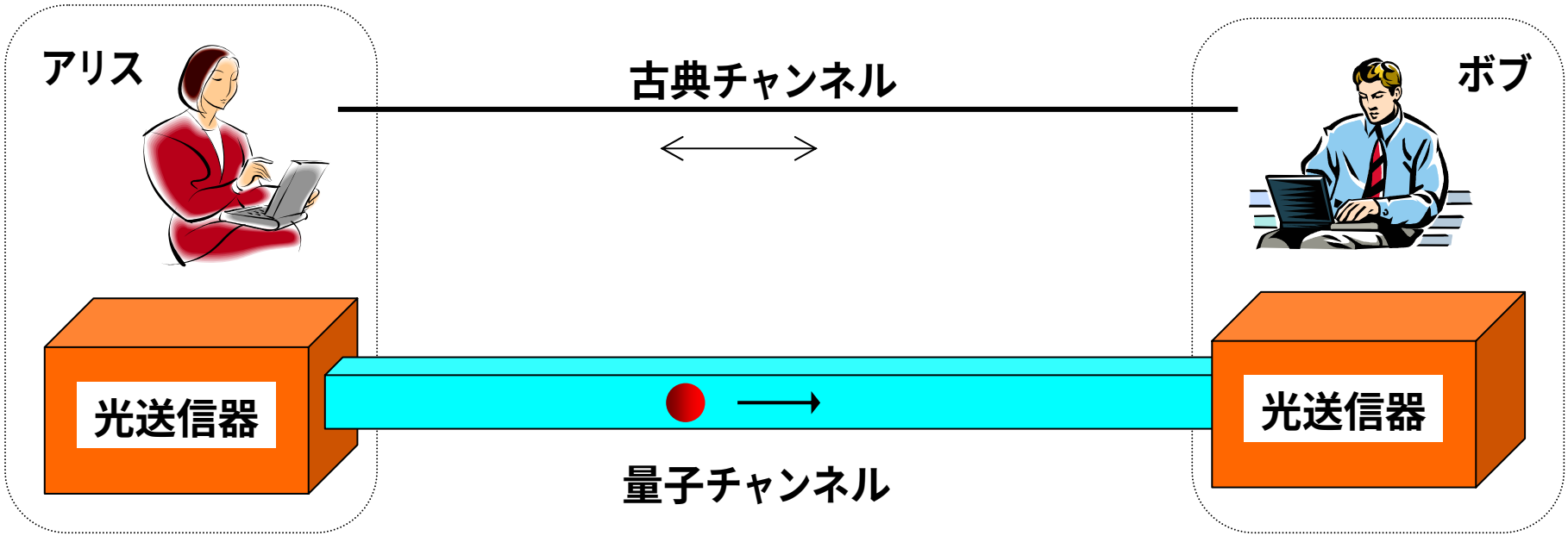


量子暗号 (量子鍵配送)

目的 量子力学的に秘匿性が保証された秘密鍵を離れた2者に供給

売り文句 安全性は量子力学的に保証

量子鍵配送の基本構図



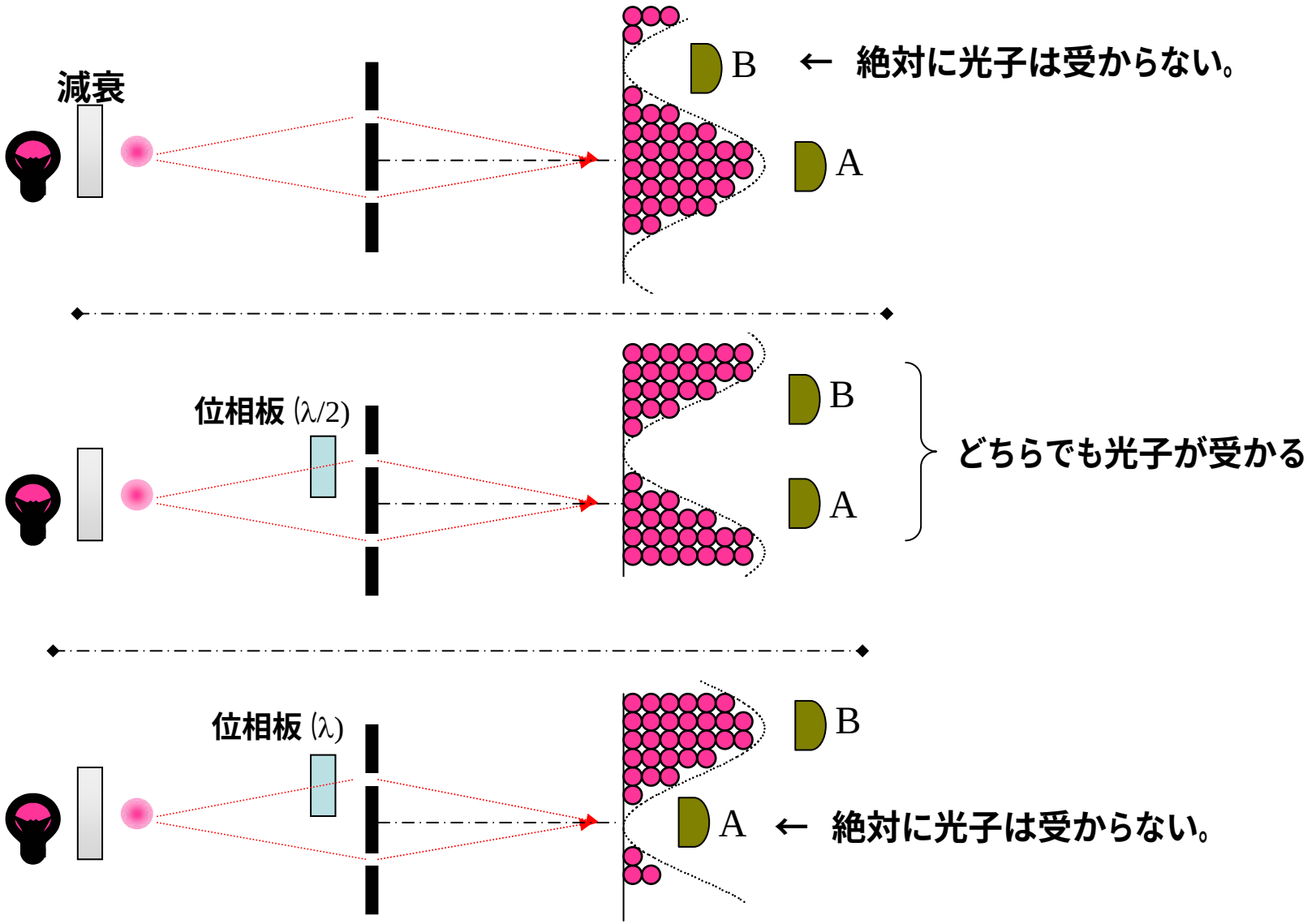
①量子チャンネルで光子を送受信

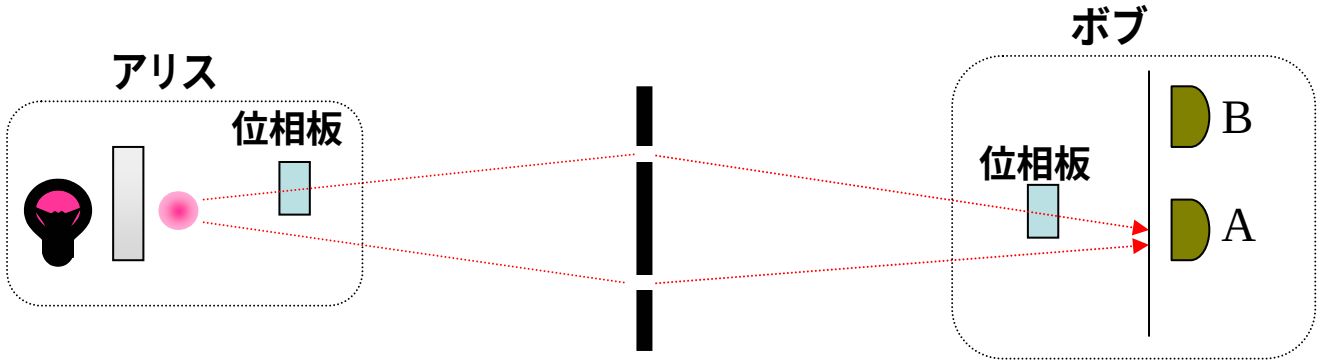
②古典チャンネルで基底に関する情報交換

③**秘密鍵**（ランダムなビット列）生成

量子チャンネルで光子を送受信

重ね合わせの干渉を利用して情報伝送





位相板の入れ方によって、

- 検出器Aのみが光子検出 (A)
- 検出器Bのみが光子検出 (B)
- 検出器Aまたは検出器Bが光子検出 (A/B)

アリス位相板 \ ボブ位相板	0	λ/2
0	A	A/B
λ/2	A/B	B
λ	B	A/B
3λ/2	A/B	A

この特性を利用して秘密鍵生成

① アリスはボブに光子を送信。その際、アリス/ボブは位相板をランダムに挿入。
- 特定の位相板の組み合わせの場合に、光子検出は確定的 -

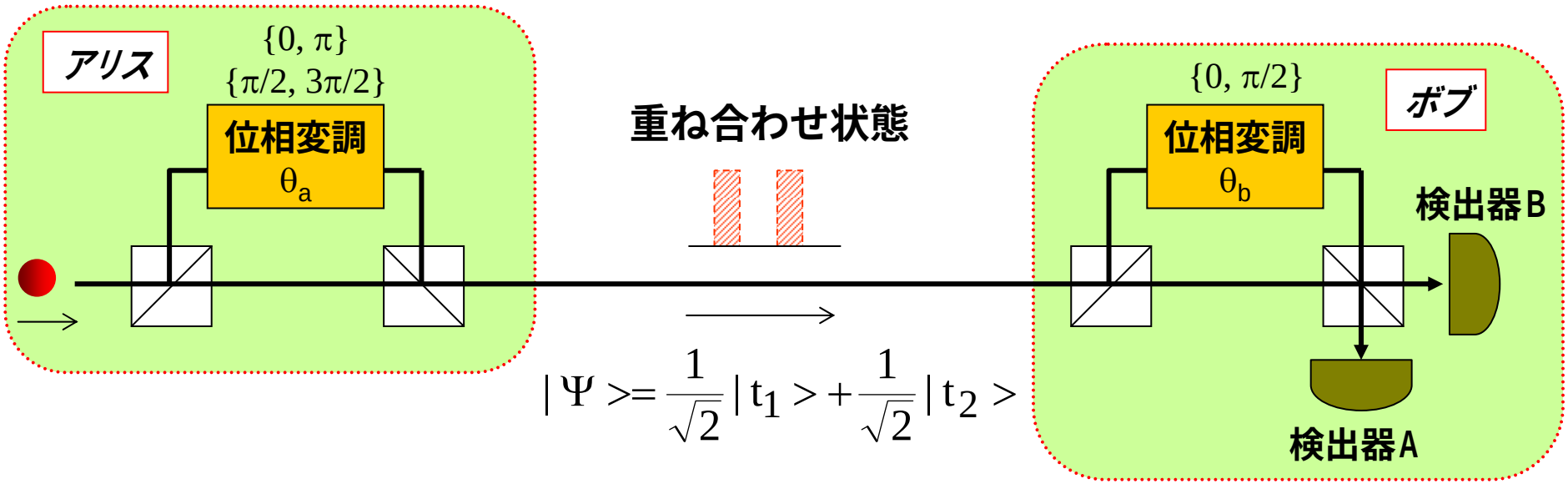
②アリス/ボブは、挿入した位相板を報せ合う。

③ 確定的である光子検出から鍵ビットを生成； 検出器A →「0」、検出器B →「1」

ファイバー伝送するには

実際の構成例

時間軸上の重ね合わせ状態を送受信



光子の経路は4通り

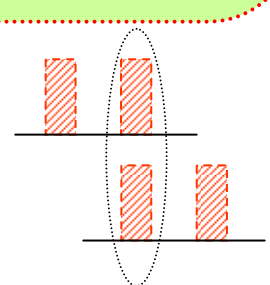
①アリスの短経路 － ボブの短経路

②アリスの短経路 － ボブの長経路

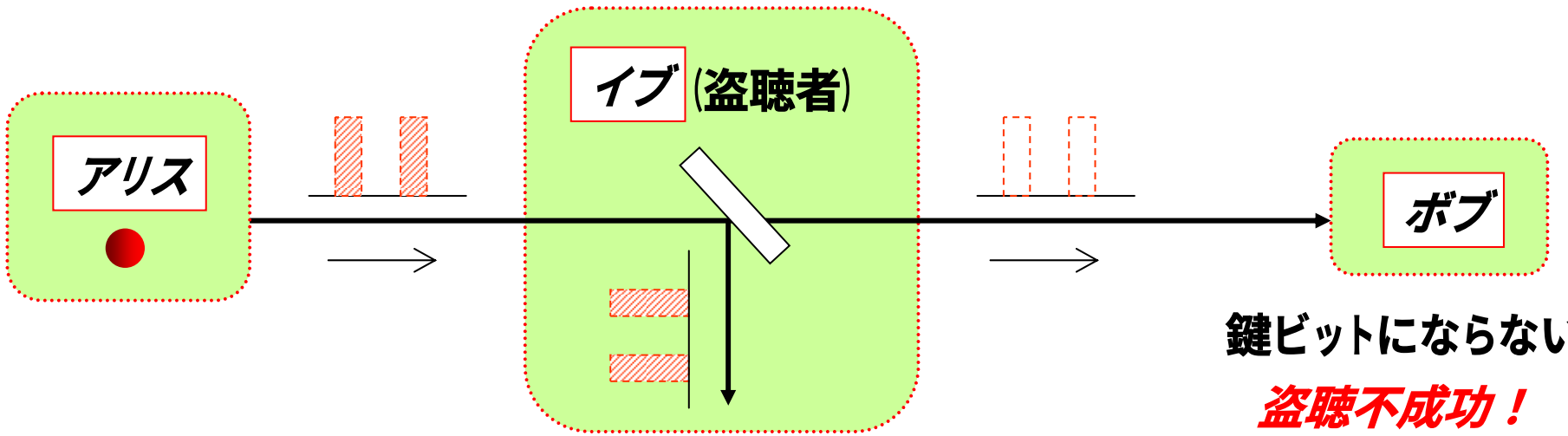
③アリスの長経路 － ボブの短経路

→ *干渉*

④アリスの長経路 － ボブの長経路



なぜ安全か（その1）
–盗み聞き盗聴に対して–



なぜ安全か（その2）
–なりすまし盗聴に対して–

受信結果に基づいて偽装信号を送信。

But、ボブと同じ位相板を使わないと正しい受信ができない。

ビット誤り

↓

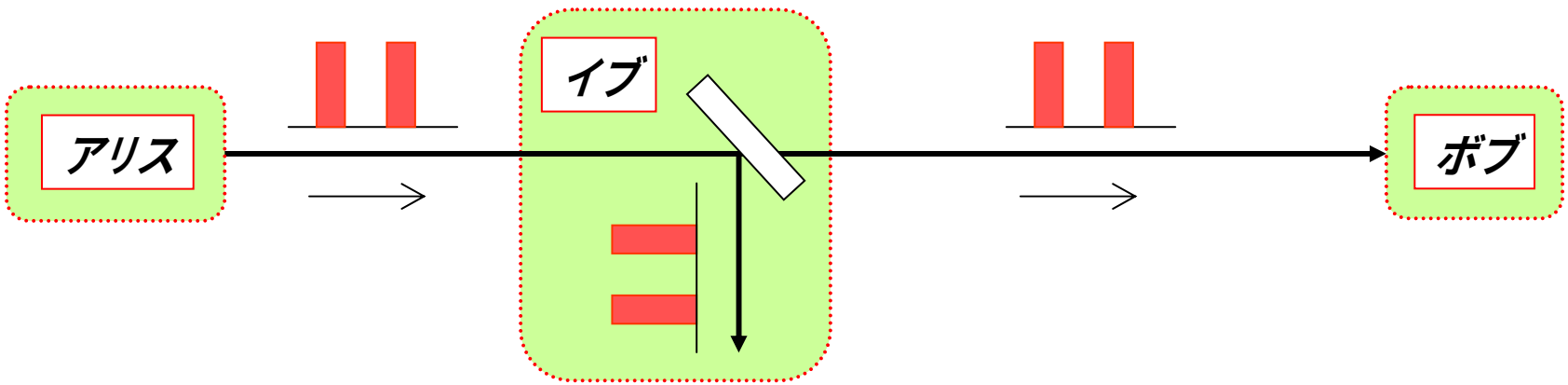
テストビットのチェックにより盗聴発覚

要するに

光子が最小単位であること（粒子性）を利用して安全性を確保

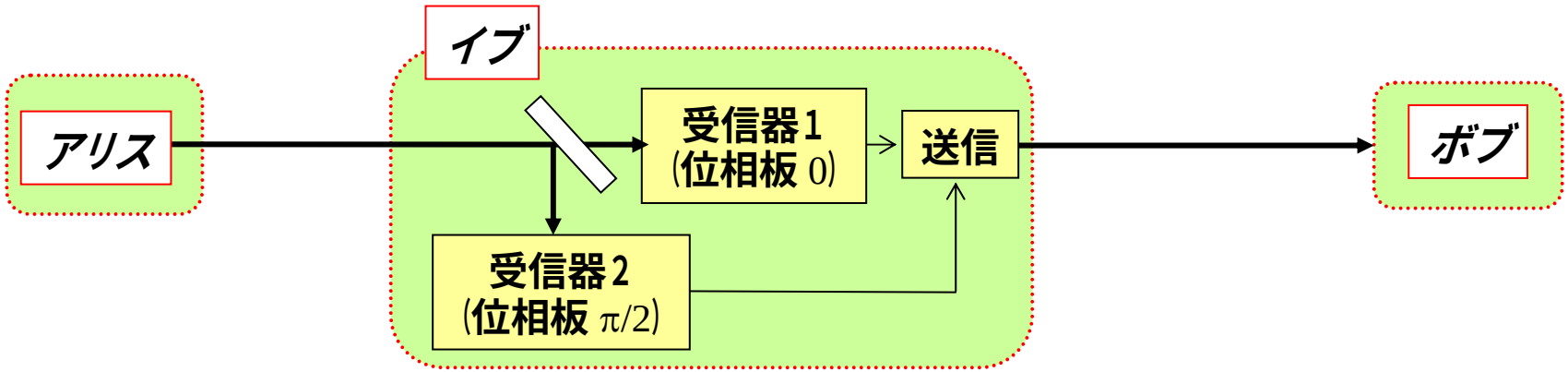
粒子性がなかったら、、、、、、、、

<u>盗み聞き盗聴されると</u>

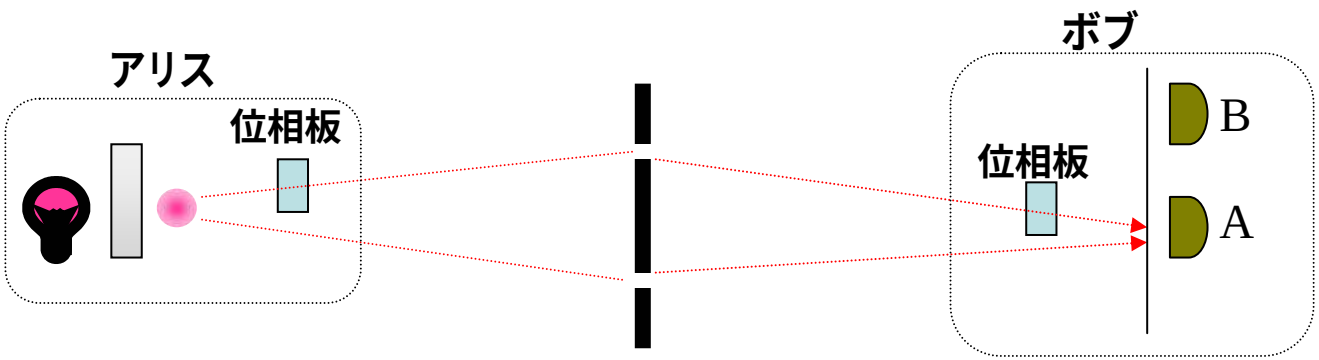


2分岐できて盗聴可能

なりすまし盗聴されると



両方の位相板を試すことができて、
正しい受信が可能。



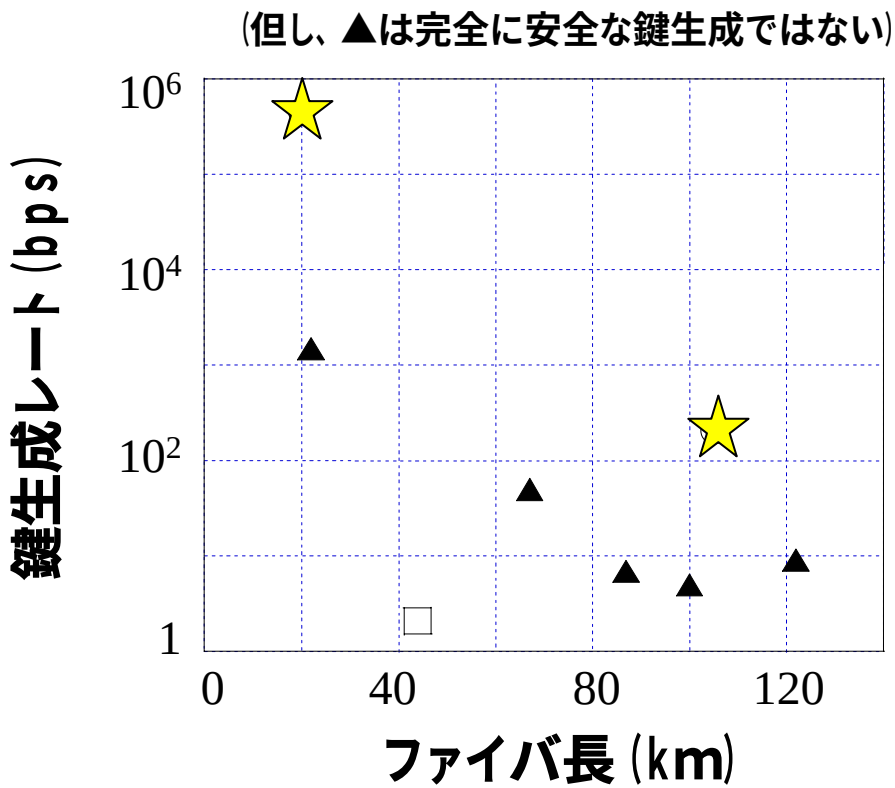
アリス位相板 \ ボブ位相板	0	λ/2
0	A	A/B
λ/2	A/B	B
λ	B	A/B
3λ/2	A/B	A

量子暗号まとめ

◆重ね合わせ状態の干渉効果を利用して秘密鍵を生成

◆光の粒子性を利用して安全性を確保

これまでの実験報告例

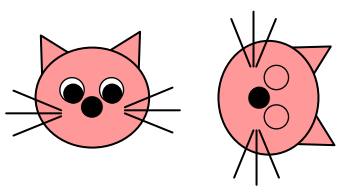


★ by NTT/Stanford

◆主な課題は光子検出器

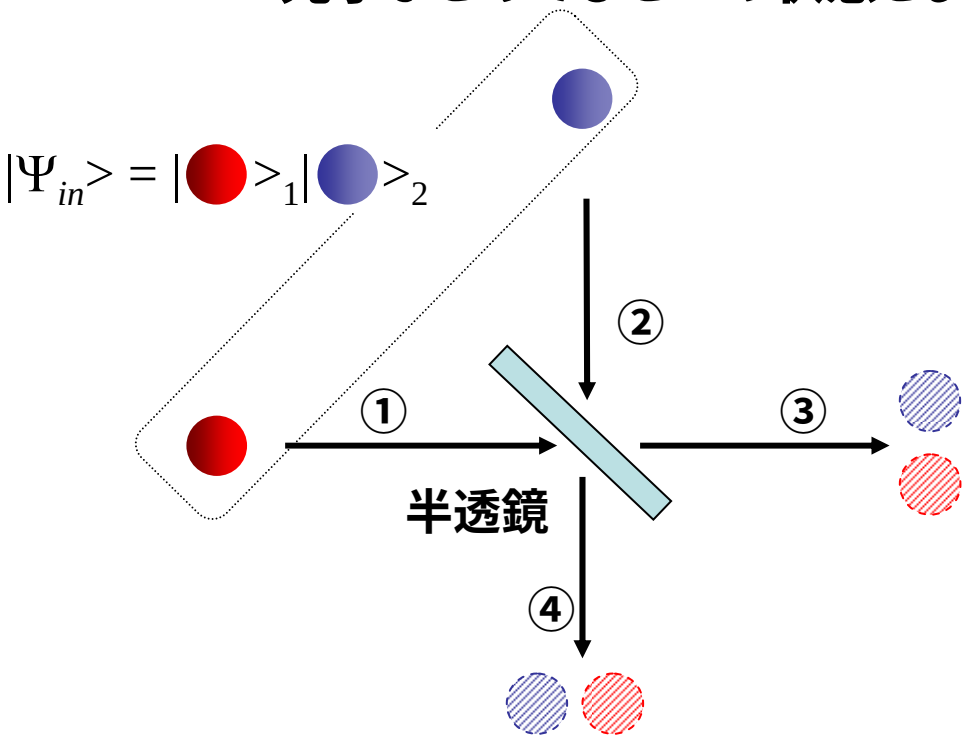
量子コンピュータ

－量子力学的重ね合わせを利用した超並列計算－



量子コンピューティングで利用する重ね合わせ
ー量子もつれー

半透鏡の両側から1光子ずつ入力
2光子まとめてひとつの状態として見る



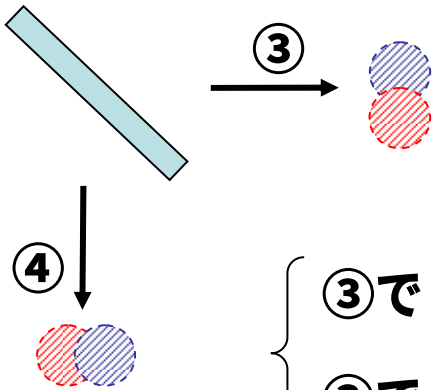
出力パターンは4通り
(1) 2光子とも③へ
(2) 2光子とも④へ
(3) ●は③へ、●は④へ
(4) ●は④へ、●は③へ

重ね合わせ

$$|\Psi_{out}\rangle = \overset{(1)}{|\bullet\rangle_3|\bullet\rangle_3} + \overset{(2)}{|\bullet\rangle_4|\bullet\rangle_4} + \overset{(3)}{|\bullet\rangle_3|\bullet\rangle_4} + \overset{(4)}{|\bullet\rangle_4|\bullet\rangle_3}$$

各端子に光子が1個ずつ出力される状態に着目

2つの出力側でそれぞれ光子が検出される場合に着目



③で ● なら、④では必ず ●

③で ● なら、④では必ず ●

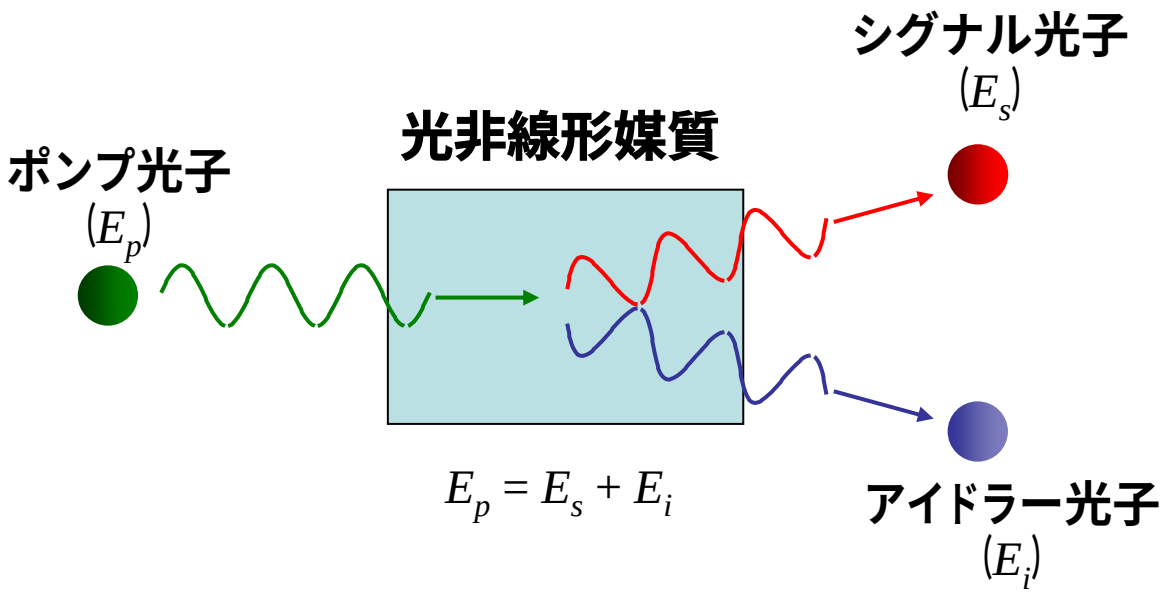
ただし観測するまでどちらかは不明　＝　2光子の重ね合わせ状態

◆一方の経路だけを観測すると、●だったり●だったり

◆両方とも観測すると、一方が● なら他方は必ず●

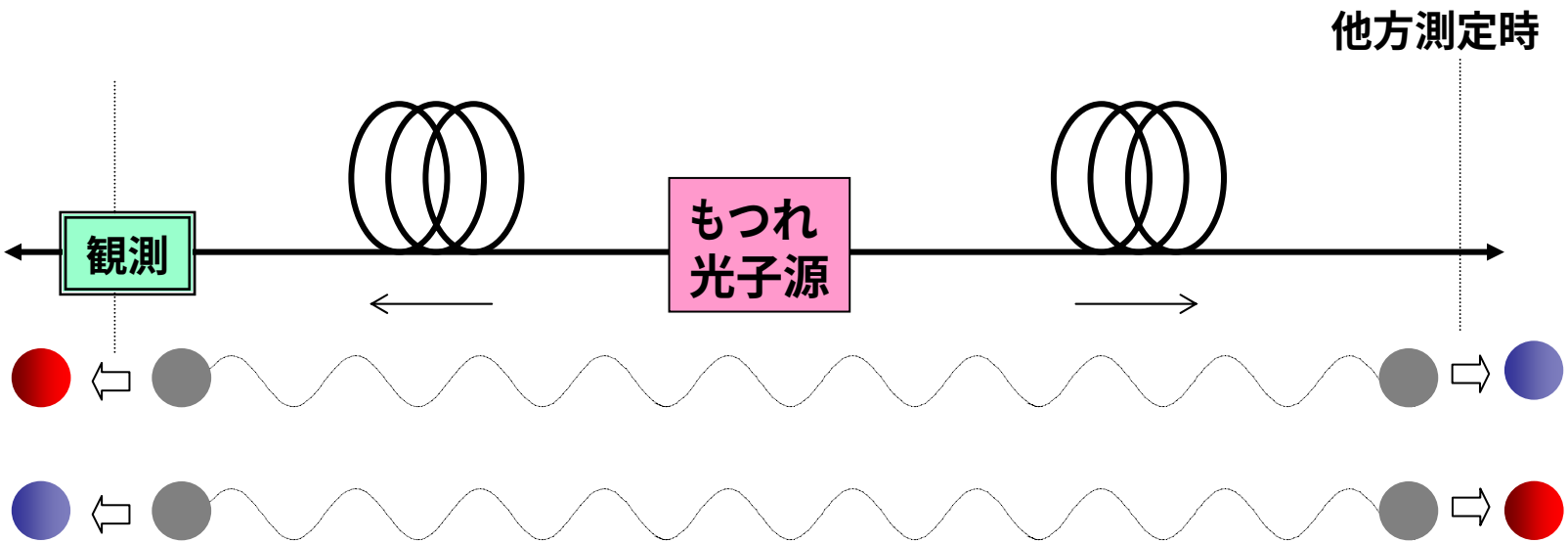
量子もつれ状態

量子もつれ発生法



量子もつれの不思議 (1)

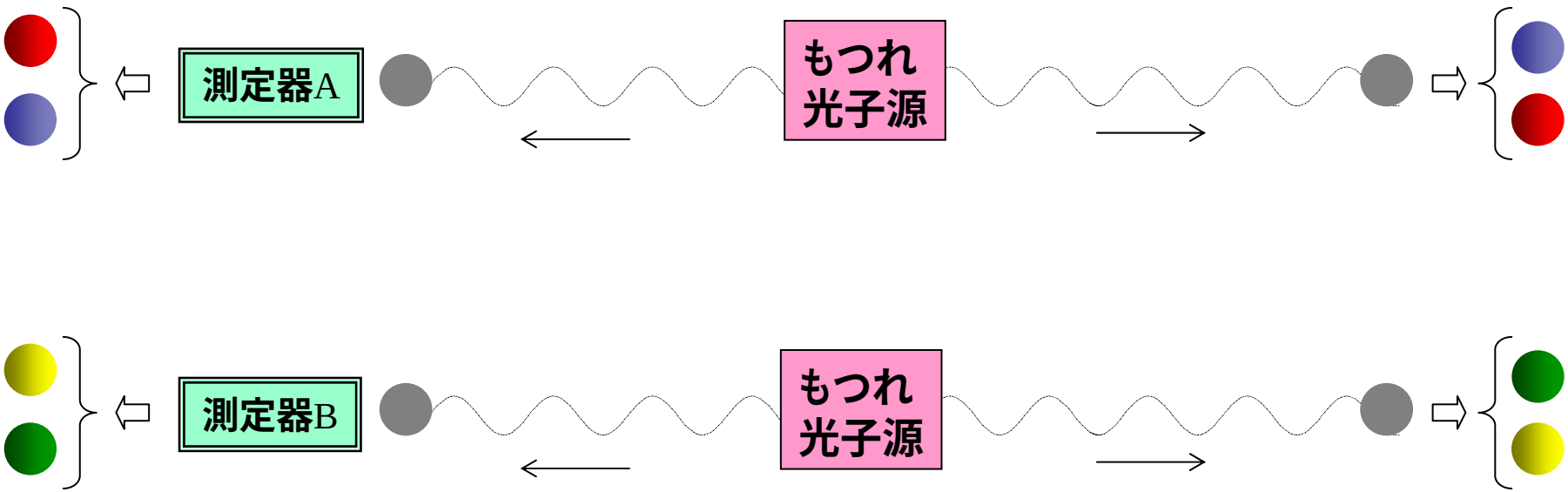
2光子がどんなに離れていても、
一方の状態を確定すると他方の状態が一瞬にして決まる。



註:「始めから決まっているけど観測していないだけ」ではなく、
「観測前は原理的に不確定」
これの実証実験あり (ベル不等式の破れ実験)

量子もつれの不思議 (2)

重ね合わせの表わし方はひとつではない。
それに応じて、確定する状態は測定方法によって異なる。



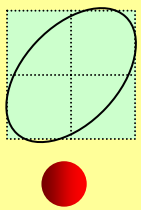
さて、量子コンピュータ

◆量子力学的重ね合わせにより複数の数を同時に表現

◆量子もつれの性質利用して超並列処理

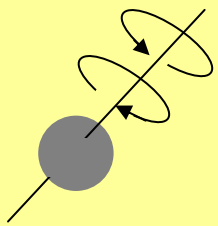
基本単位は量子ビット（Quantum bit: **Qビット**）

光子の偏波



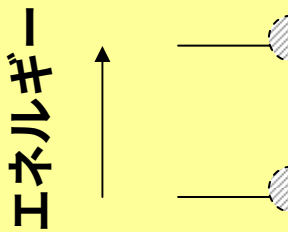
$|\psi> = a|H> + b|V>$

スピン



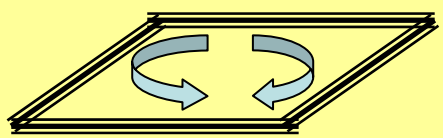
$|\psi> = a|\uparrow> + b|\downarrow>$

2つのエネルギー準位



$|\psi> = a|e> + b|g>$

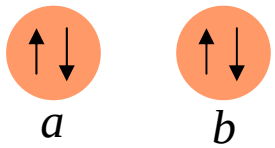
超伝導電流

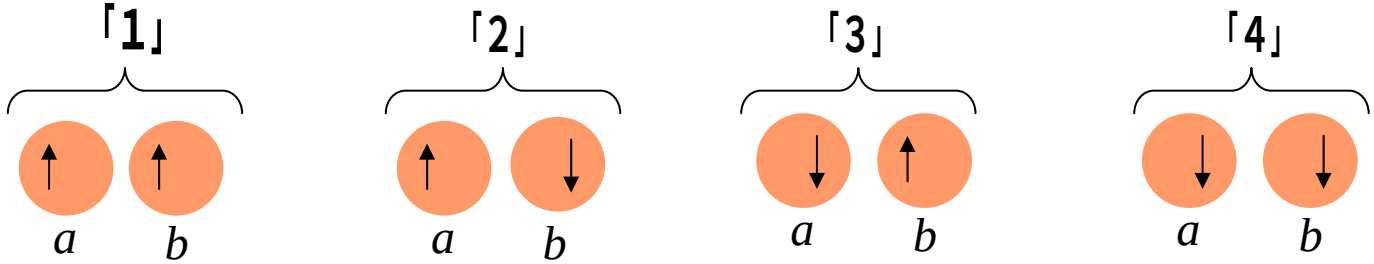


$|\psi> = a|R> + b|L>$

重ね合わせにより複数の数を同時に表現

Qビット2個 では





各Qビットは↑と↓の重ね合わせ状態、よって全体の状態は、

$$|\ a\ b\ > = c_1|\ a\ b\ > + c_2|\ a\ b\ > + c_3|\ a\ b\ > + c_4|\ a\ b\ >$$

$$= c_1\,「1」 + c_2\,「2」 + c_3\,「3」 + c_4\,「4」$$

4値を同時に表現
古典ビットでは4値のうちのひとつ

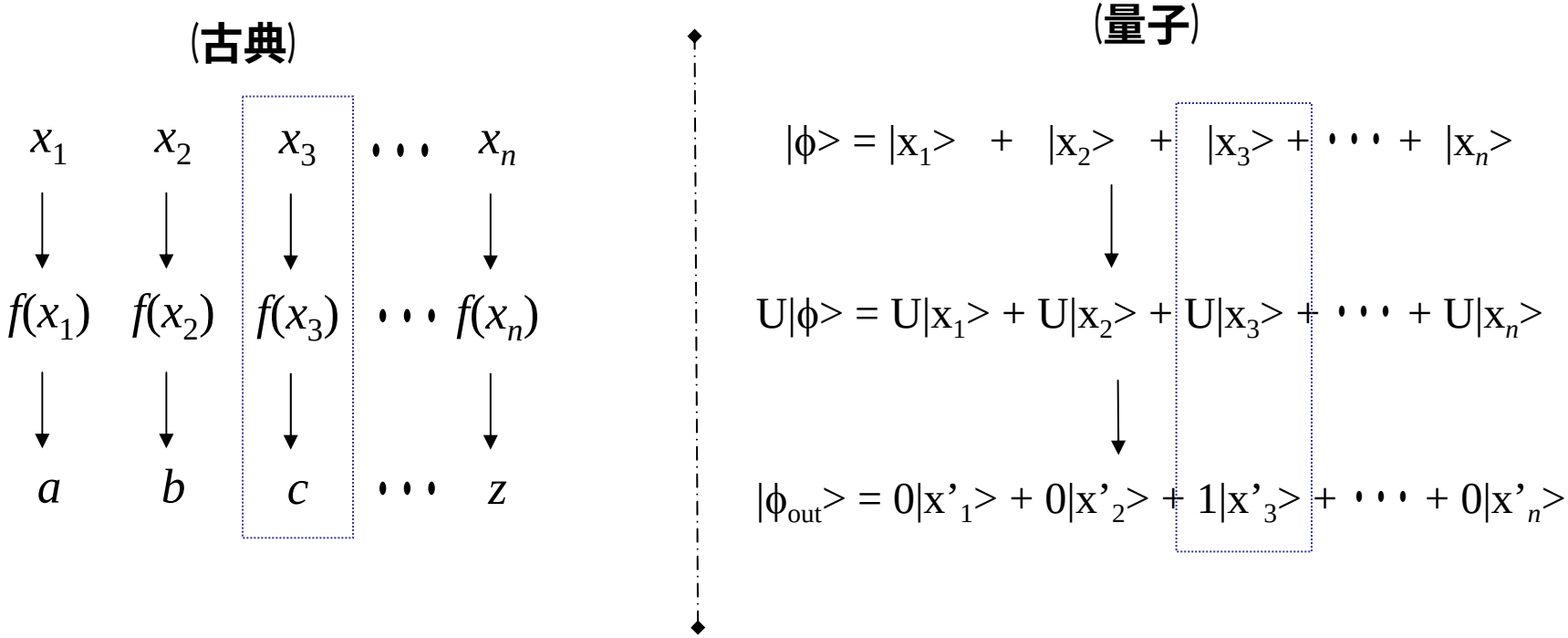
Q ビット n 個では

2^n個の値を同時に表現

重ね合わせを利用して並列計算

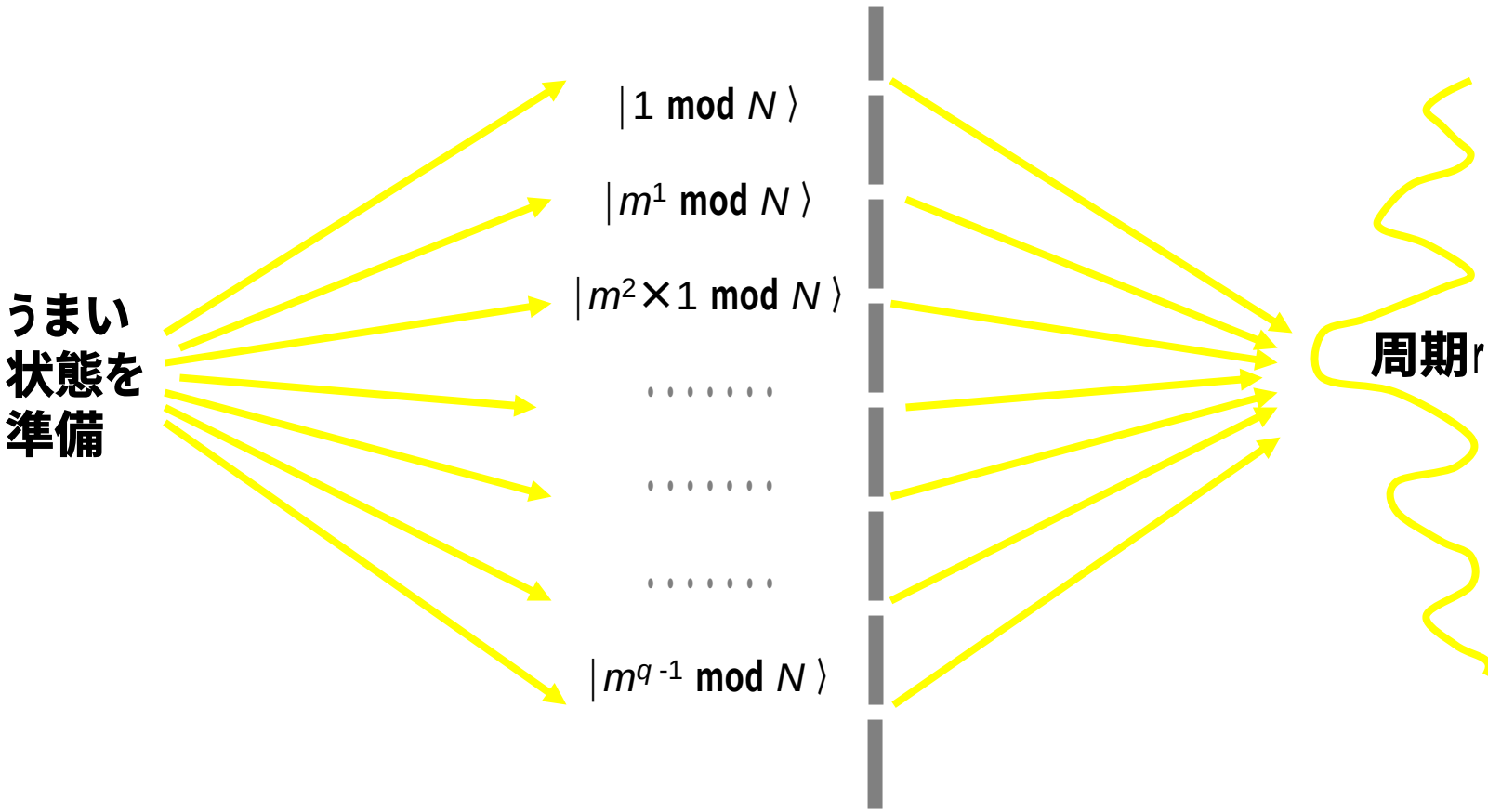
$f(x)=c$ を満たすxを見つけたい。

例えば素因数分解
367 × 521 = 191207
191207 = X × Y



並列処理のイメージ

重ね合わせの干渉効果を利用して一括処理



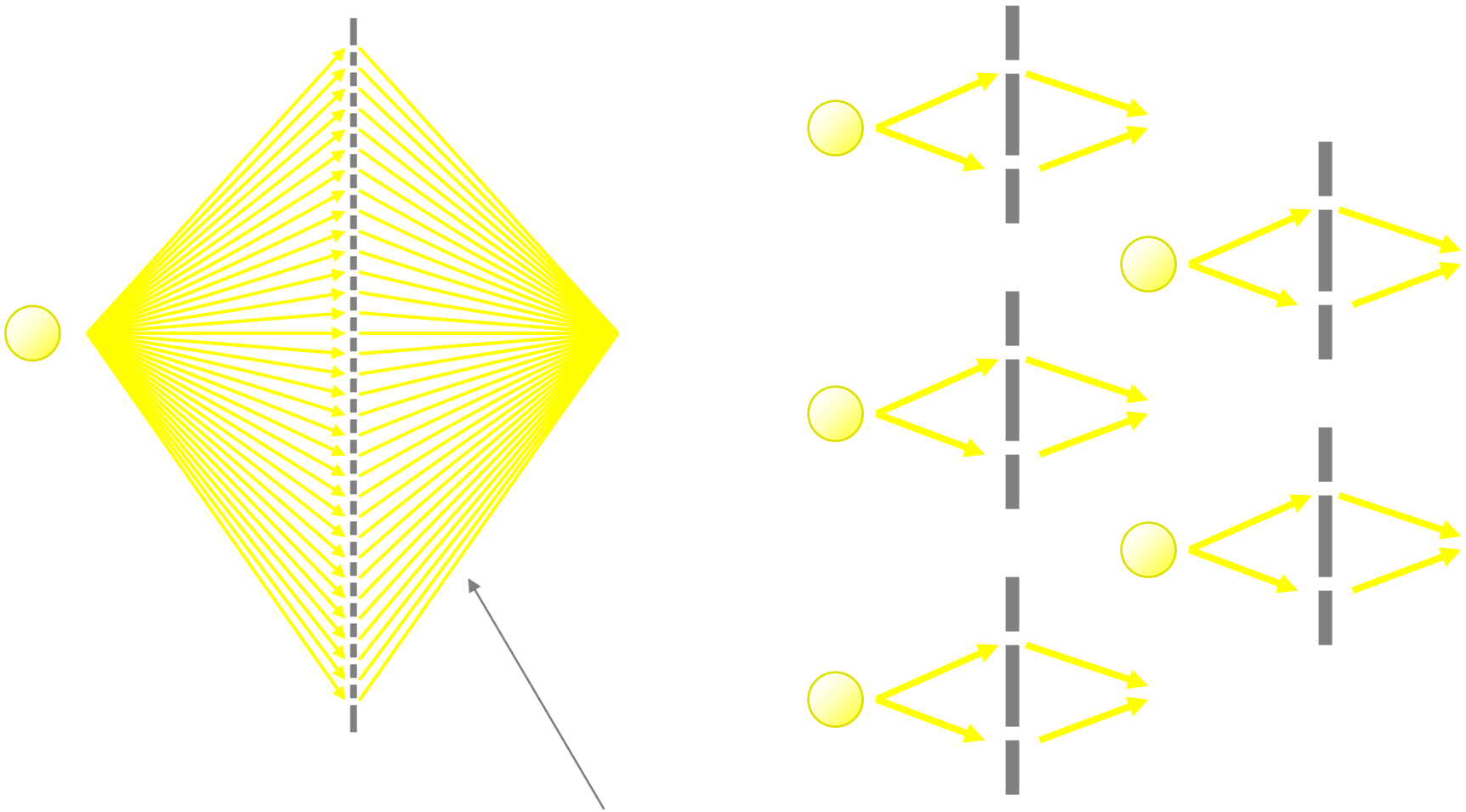
ここで疑問;

時間的ステップ数の爆発的増大が、空間的穴の数に変わるだけではないか？

→ 量子もつれを使って解決！(次ページ)

(基礎工・井元氏提供)

多重スリットと数個の二重スリットは同等



干渉する「場合の数」：32個のスリット＝2重スリット系×5

ただし「もつれた量子状態」が必要

でもとにかく2^{300}個の重ね合わせ ＝ たった300個の量子ビット

（基礎工・井元氏提供）

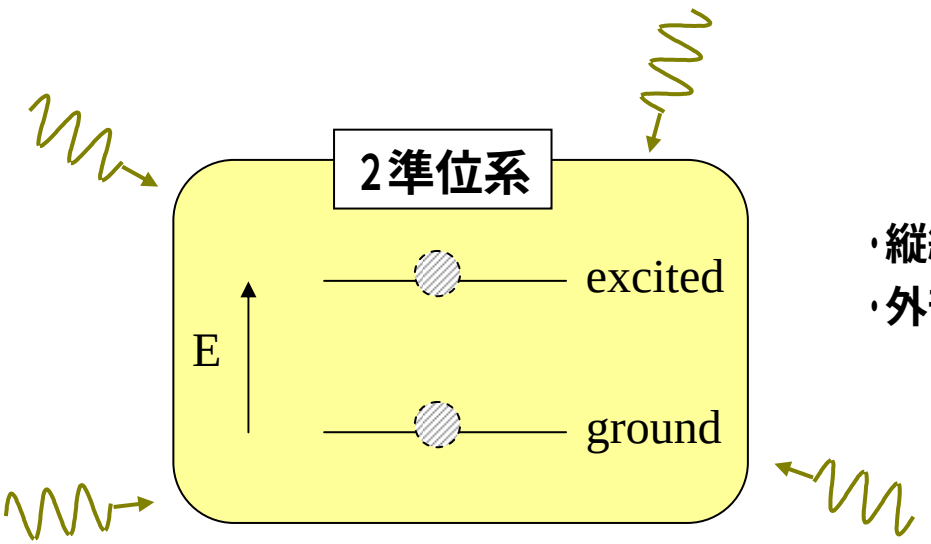
量子コンピュータの課題

◆有効性が分かっているのは、素因数分解（Shore's algorithm）とデータ検索（Grover's algorithm)だけ。（基本的にはアナログ処理。汎用計算には不向き。）

◆qubitの実現

古典計算より優位になるのはqubit数＞１００、現状は7が最高（MNR)。

◆デコヒーレンスの克服



・縦緩和により、上準位→下準位

・外部からの擾乱により位相が乱される（横緩和）

緩和時間 ＞ 計算時間

（液体ヘリウム使用が常識）

情報通信工学序論

平成17年11月30日

量子情報の話

-究極の暗号通信から超並列情報処理まで-

1. 量子力学の原理1
2. 量子暗号
3. 量子力学の原理2
4. 量子コンピュータ

ホームページ：電気電子情報工学専攻 → 情報通信部門
→ 井上研究室 → 職員紹介 → 井上