平成18年6月5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-

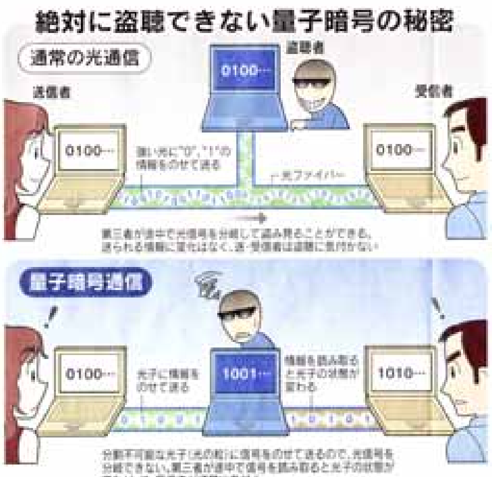
工学研究科電気電子情報工学専攻

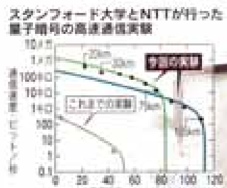
井上　恭

日本経済新聞 (9/4)

日本経済新聞 2005年（平成17年）9月4日（日曜日）

サイエンス






スタンフォード大学とNTTの共同実験（スタンフォード大学で）


量子暗号通信の実証実験（川崎市中原区のNECシステムプラットフォーム研究所）

ネット時代に究極の暗号

光子に情報搭載 通信の遅さ克服

キーワード

量子

計算機にも応用

朝日新聞 (12/13)

2005年（平成17年）12月13日 火曜日 朝日新聞

量子暗号、実用化近づく

盗聴・解読不能で高速通信

速度1億倍以上に


NTTが開発した量子暗号の送信機＝神奈川県厚木市のNTT物性科学基礎研究所で

新タイプも登場

内容

[1] **量子力学の話**

量子力学的考え方 (量子力学的重ね合わせ)

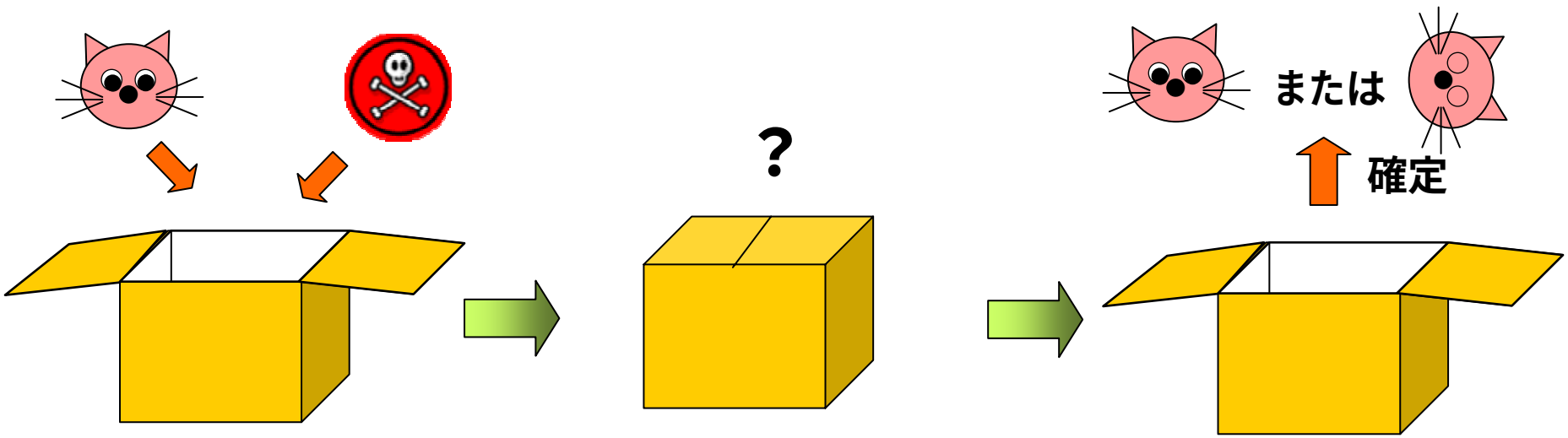
[2] **量子暗号**

量子力学的に安全が保証された暗号通信システム

[3] **量子コンピュータ**

重ね合わせを利用した超並列計算機

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

量子力学的には、どちらの状態もありとする。＝「量子力学的重ね合わせ」

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

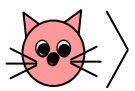
生きている　死んでいる

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

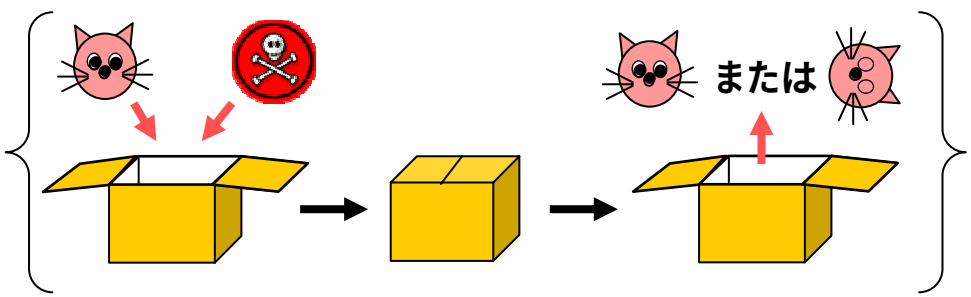
$|\psi> =$  $\rangle$　**または**　$|\psi> =$  $\rangle$

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、

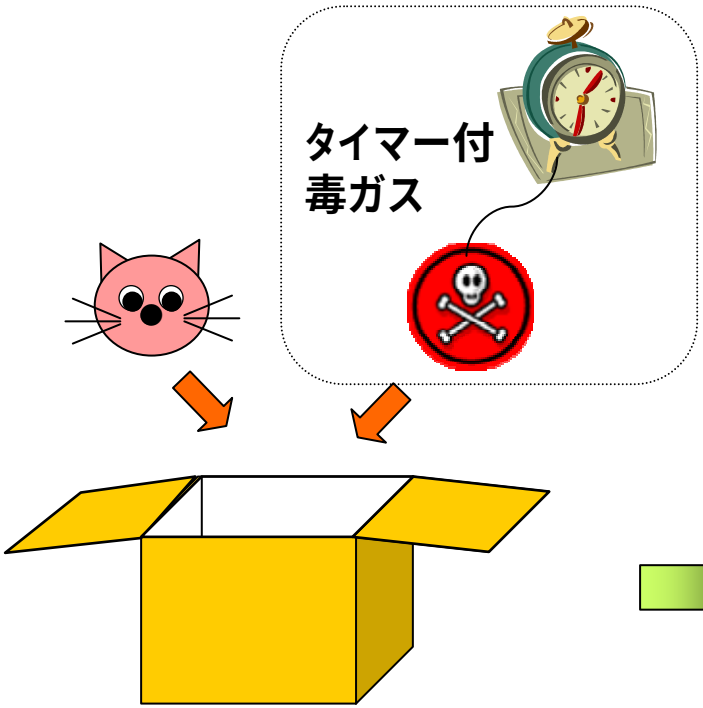


x**回繰り返すと** ⇨

 **が** $|a|^2 \times x$ **回**

 **が** $|b|^2 \times x$ **回**

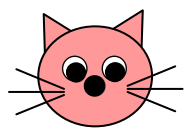
原理的にどちらかわからない事がポイント



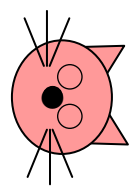
(時間がきたら必ず死ぬようにセット)

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



↓

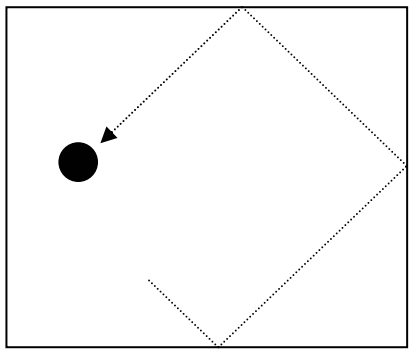
重ね合わせ状態ではない

量子力学の基本

物理状態は確率的

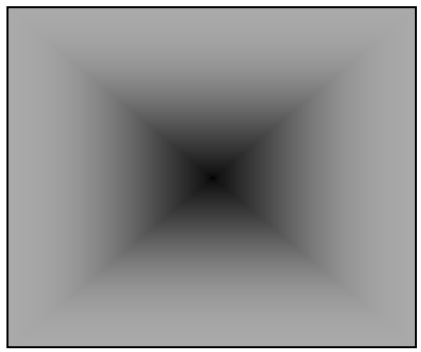
(例えば箱の中の電子)

古典力学



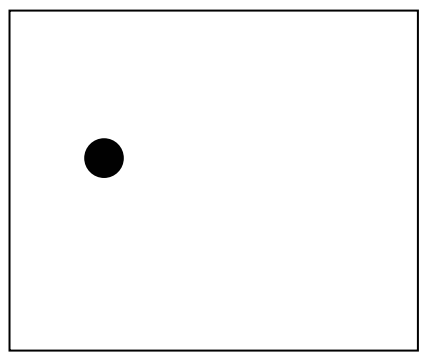
位置は確定

量子力学



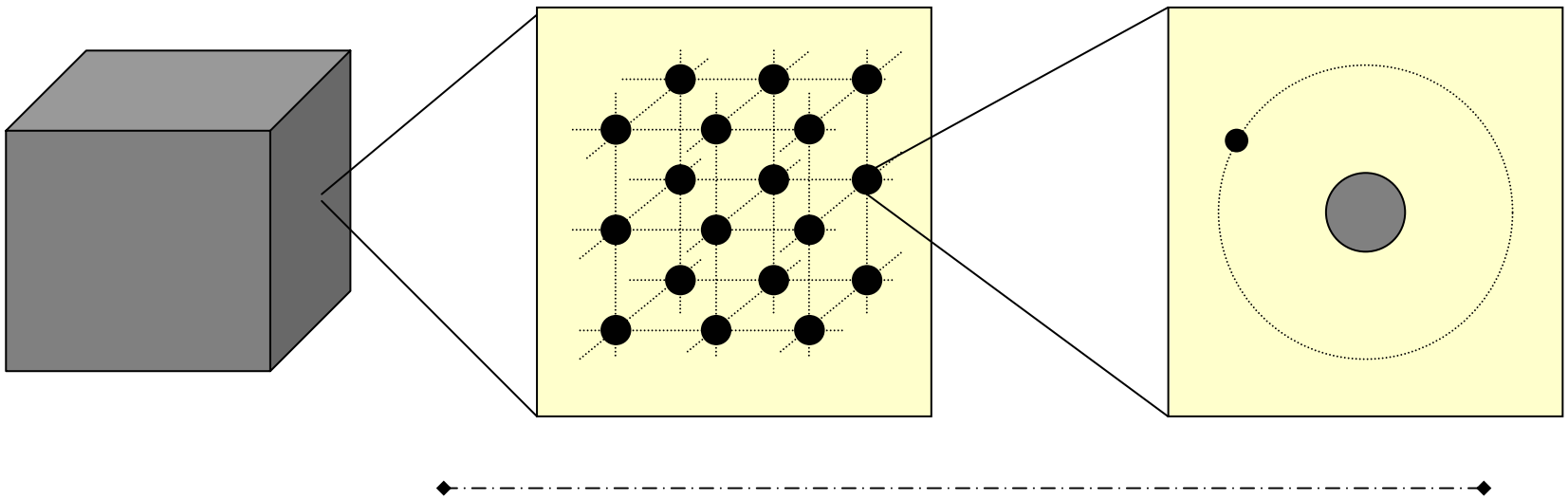
どこに居るか不確定。
確率分布だけが与えられる。

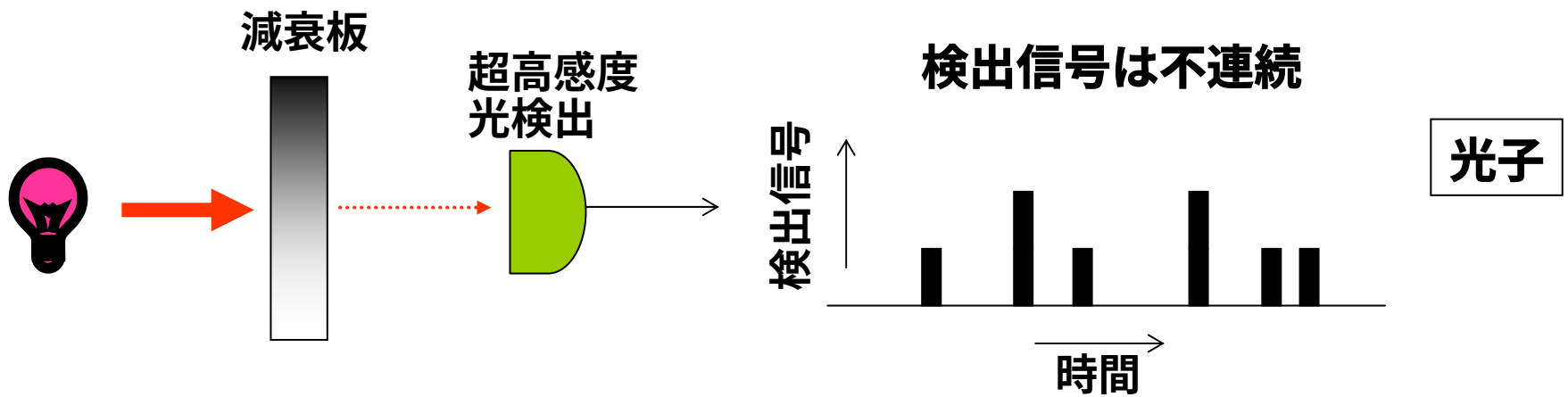
観測すると確定



量子力学の基本

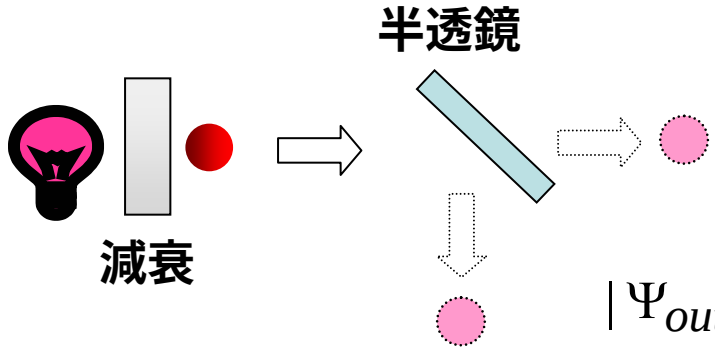
全てのものは
それ以上分割できない最小単位から成り立っている





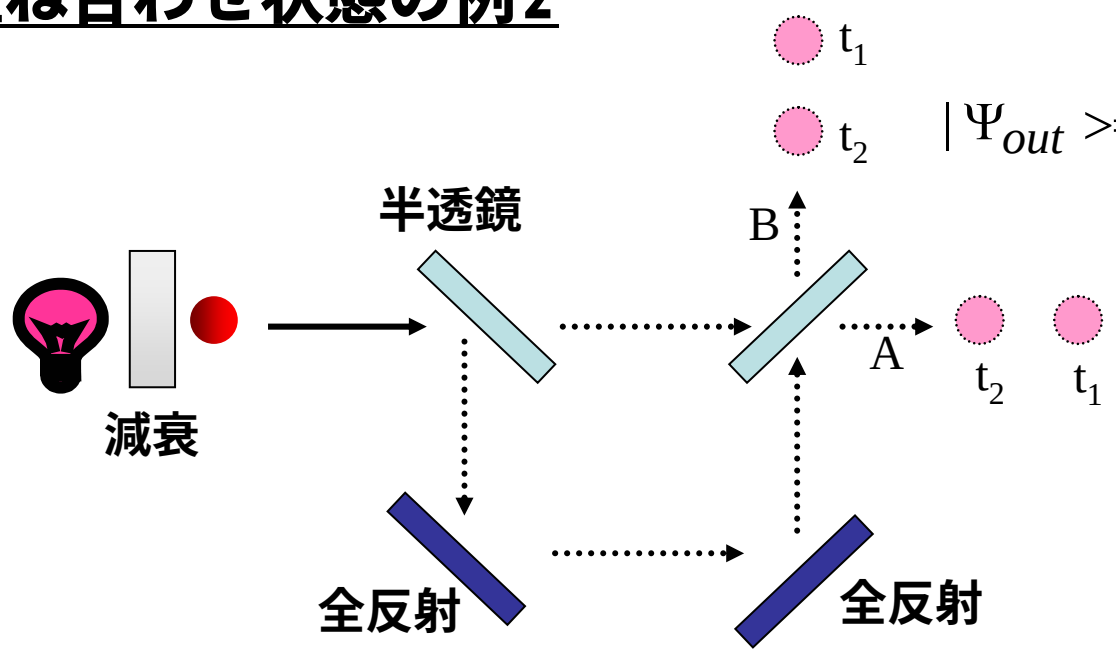
光子の場合

重ね合わせ状態（確率状態）の例1



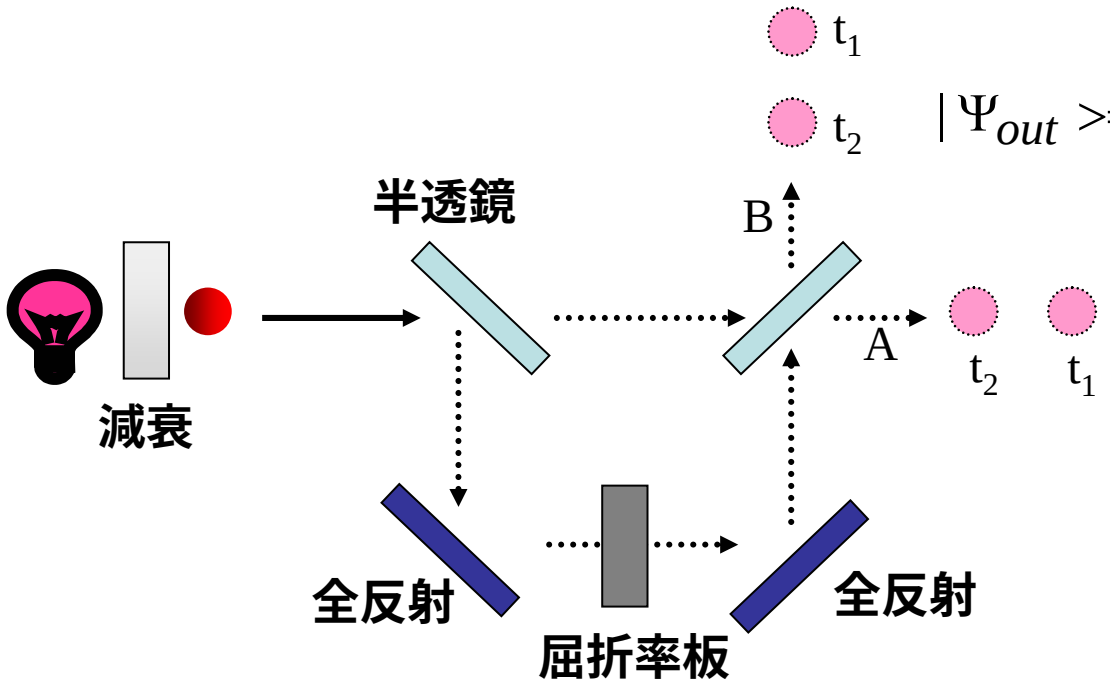
$$|\Psi_{out}>= a\,|\text{透過}> + b\,|\text{反射}>$$

重ね合わせ状態の例2



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

重ね合わせ状態の例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2’は、光子の確率は同じだけれど、状態としては違うはず。

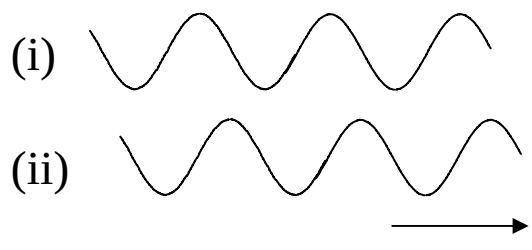
↓

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。

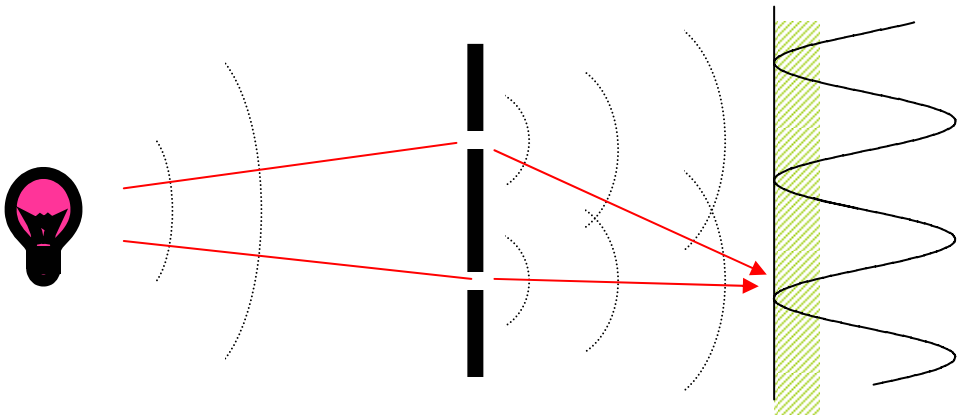
経路状態の違いは、複素数の位相で反映。

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

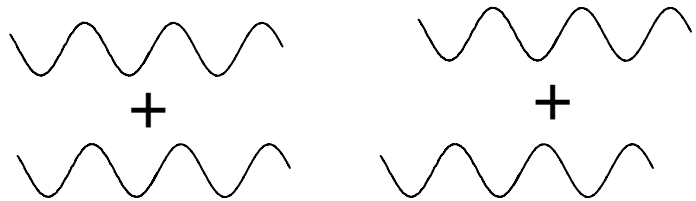
位相：例えば、波の振動の位置

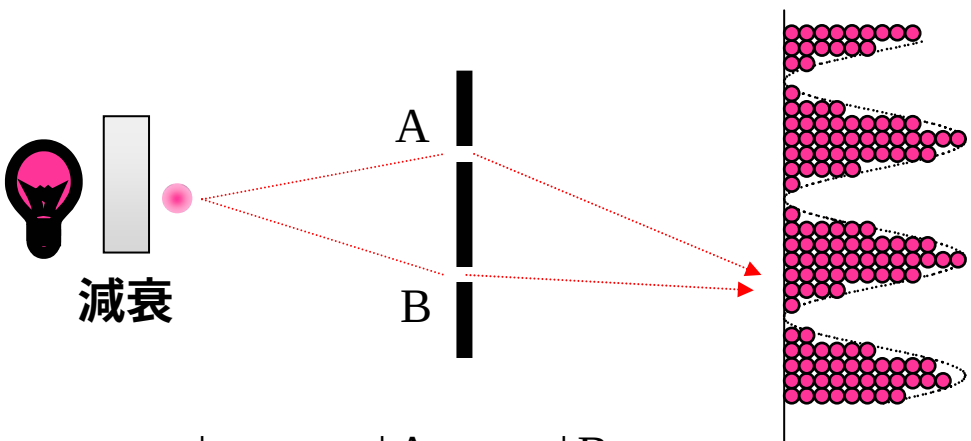


光の干渉



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。

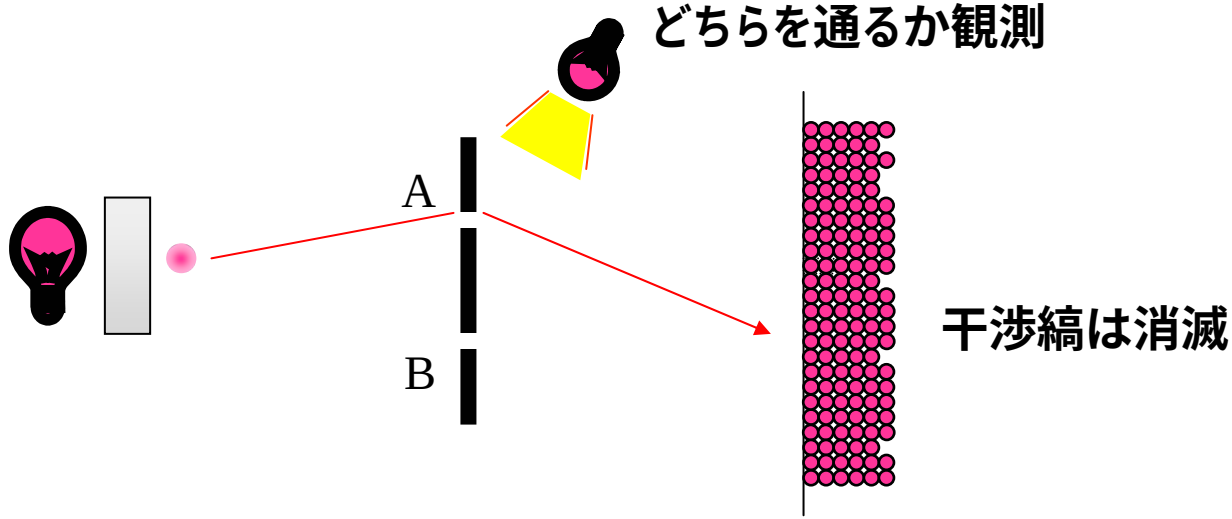




$$|\psi\rangle = c_a|\mathrm{A}\rangle + c_b|\mathrm{B}\rangle$$

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



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

観測

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

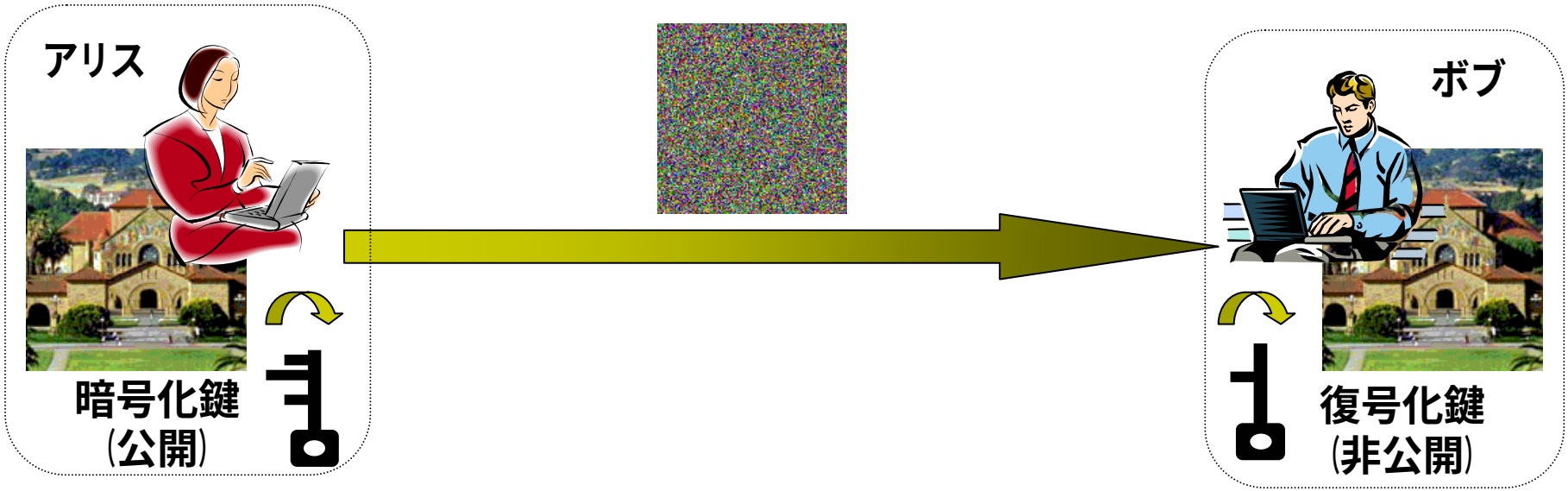
単にひとつのピンホールを通ったのと同じ。

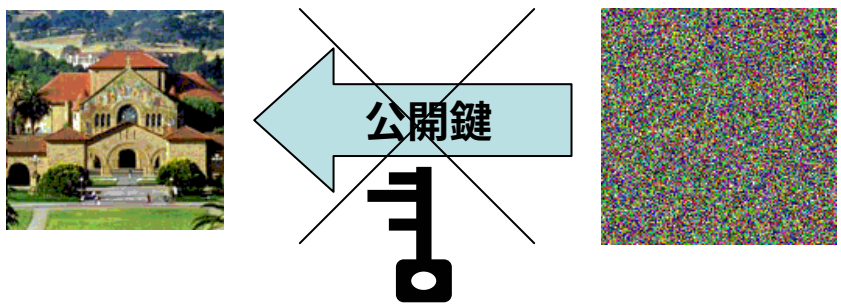
量子力学の重ねあわせの性質を安全な暗号システムに利用しよう

量子暗号（量子鍵配送）

(まずは、現在の暗号方式から)

公開鍵暗号



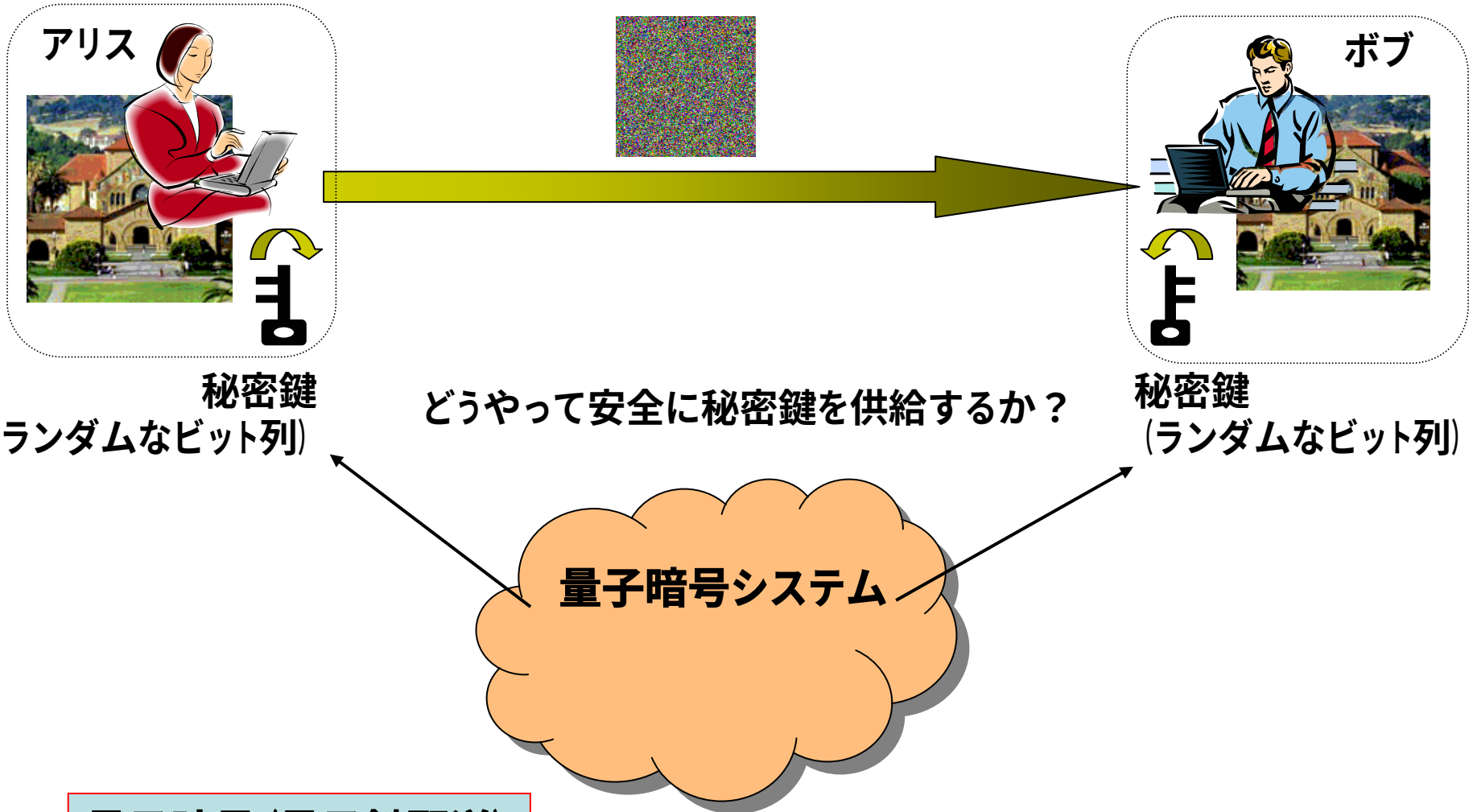


367 × 521 = 191207 ：簡単

191207 = X × Y ：難しい

原理的には解読可能

秘密鍵暗号

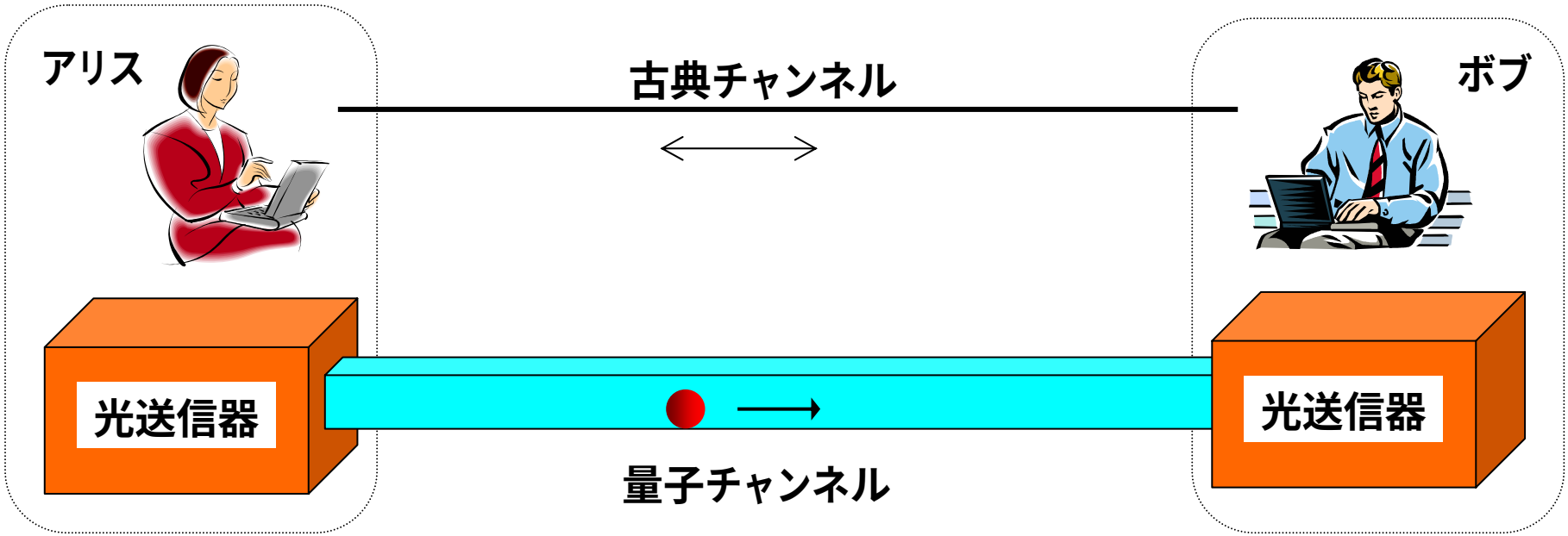


量子暗号 (量子鍵配送)

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

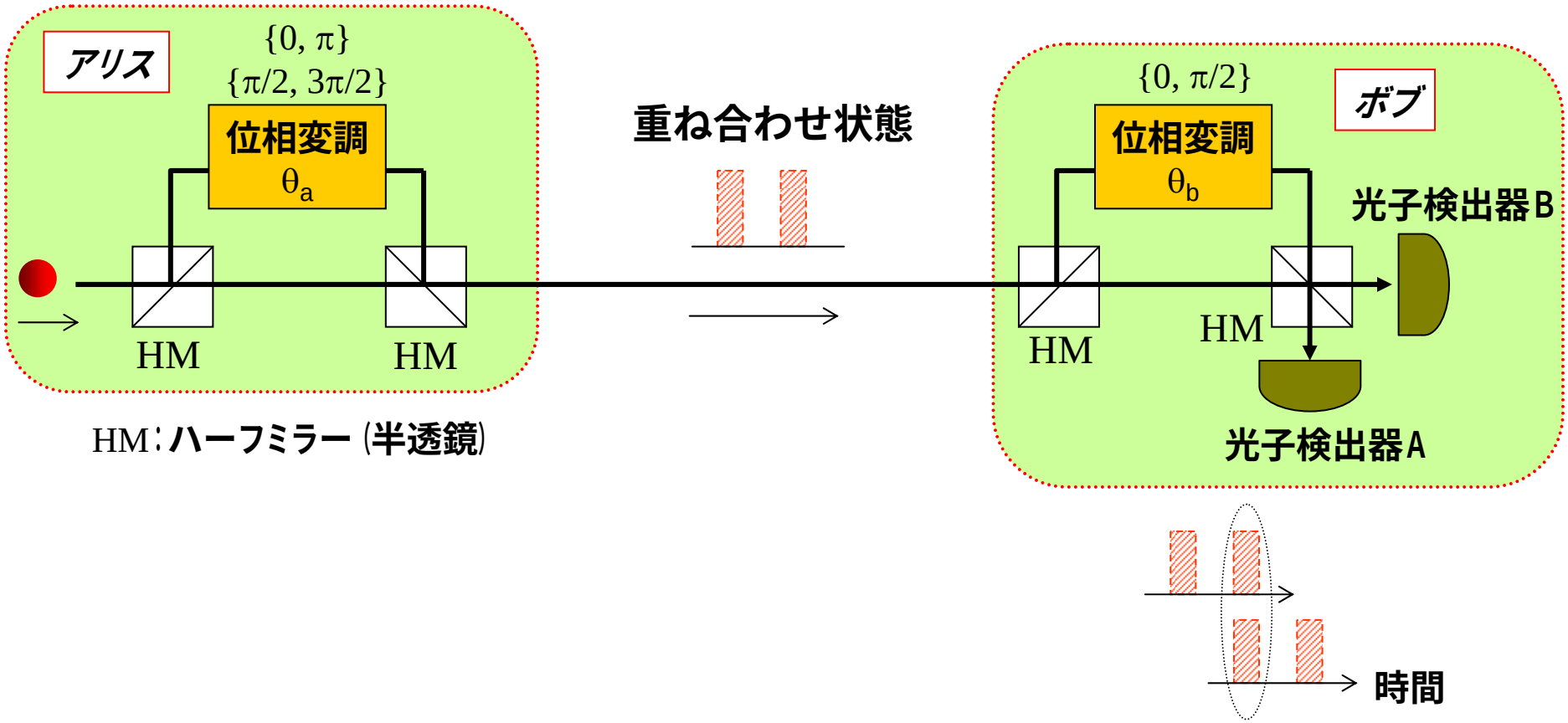


①量子チャンネルで光子を送受信

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

量子鍵配送システムの具体的構成例

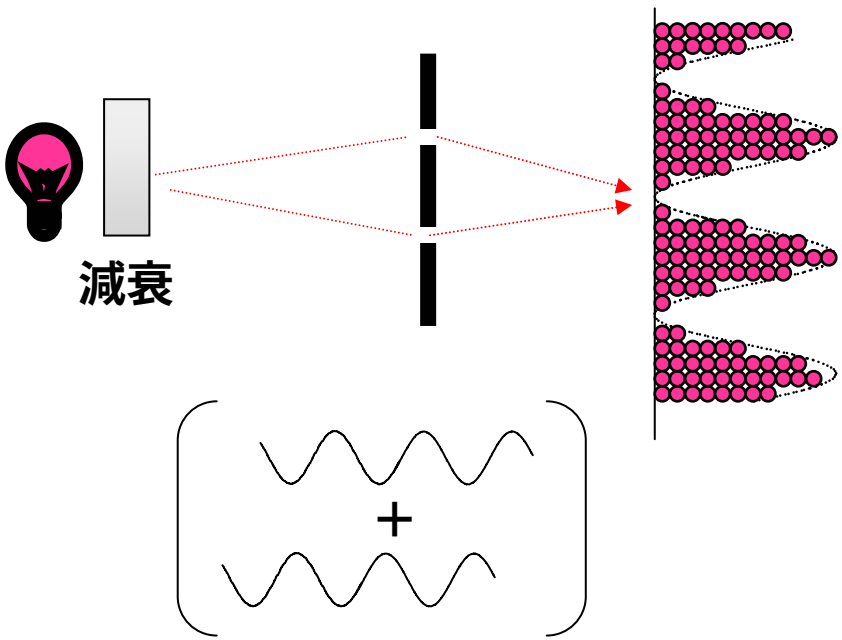


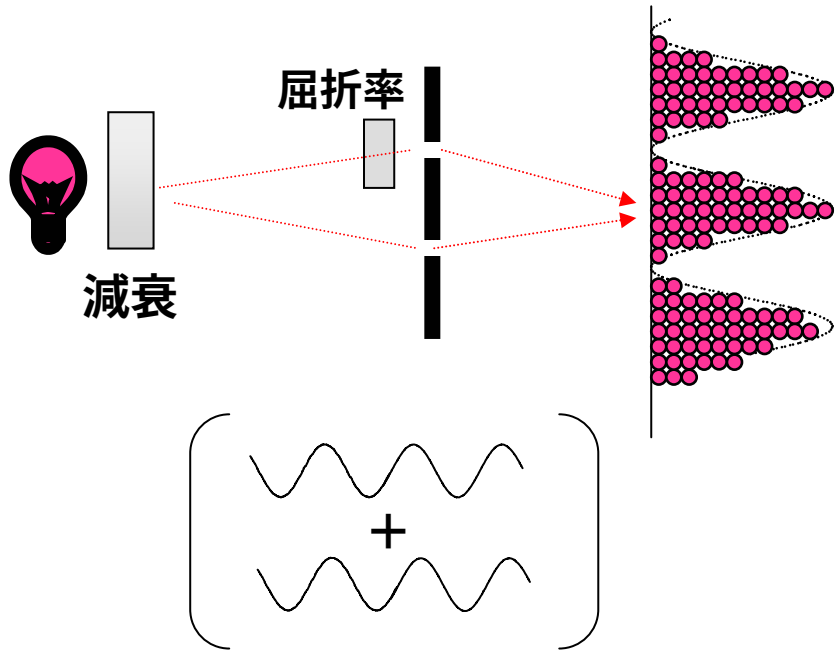
HM：ハーフミラー（半透鏡）

後のパルスが短経路を通った状態の係数と
先のパルスが長経路を通った状態の係数が干渉

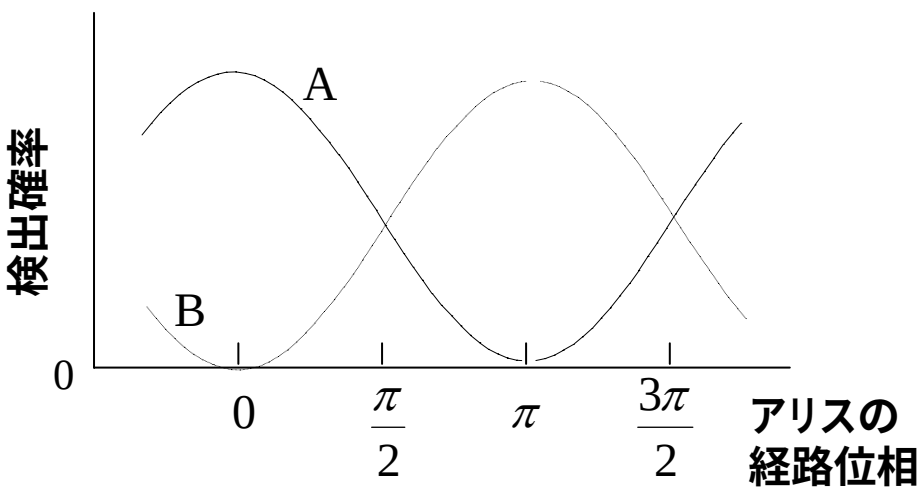
干渉の仕方は経由してきた経路の状態に依存

干渉の仕方は途中の経路状態に依存

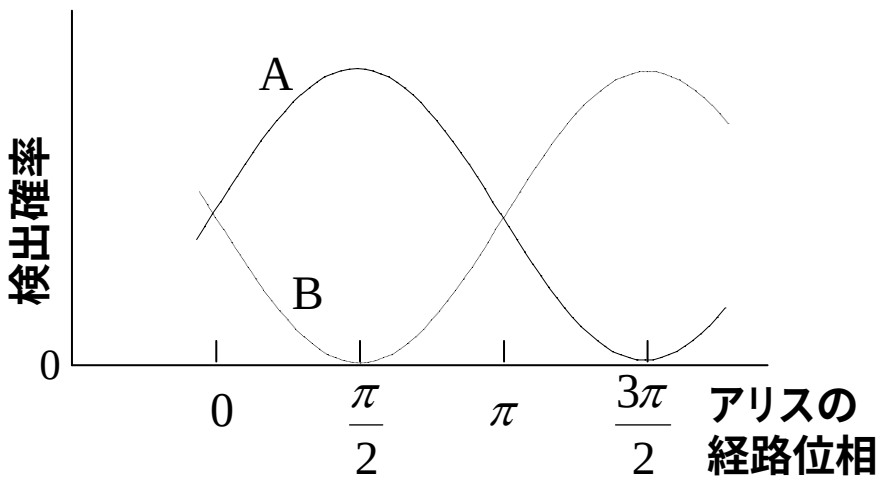




ボブ経路位相=0 の場合



ボブ経路位相=π/2 の場合



経路状態によって、

必ずA で検出される場合（Ⓐ）、

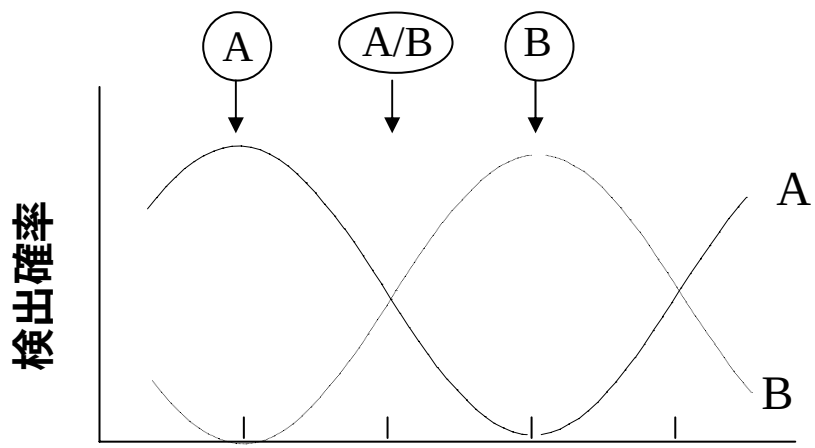
必ずBで検出される場合（Ⓑ）、

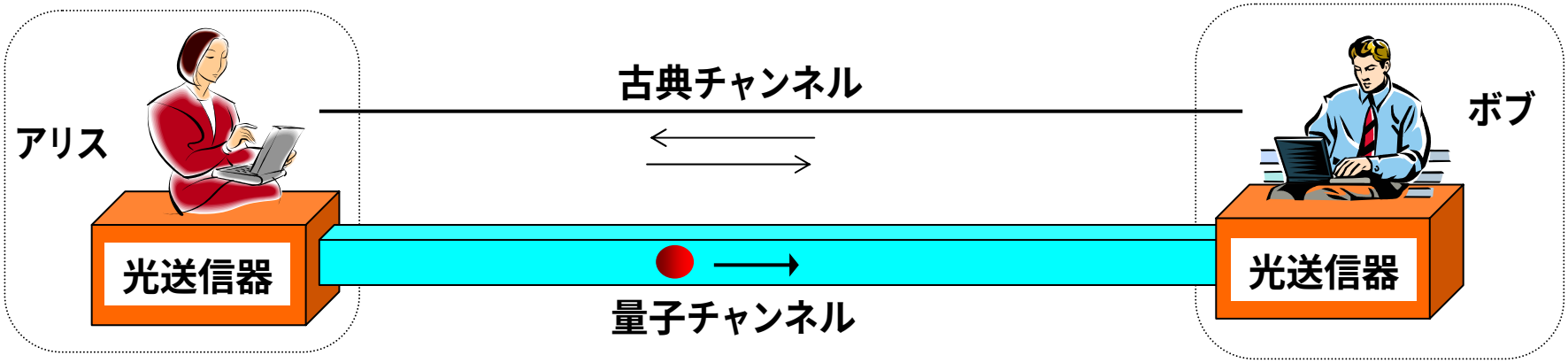
A、Bどちらでも検出され得る場合（Ⓐ/Ⓑ）、がある。

アリス側 位相 \ ボブ側位相	0	π/2
0	Ⓐ	Ⓐ/Ⓑ
π/2	Ⓐ/Ⓑ	Ⓐ
π	Ⓑ	Ⓐ/Ⓑ
3π/2	Ⓐ/Ⓑ	Ⓑ

⇒

アリス側 位相 \ ボブ側位相 θ_a \ θ_b	0	π/2
0	Ⓐ	Ⓐ/Ⓑ
π	Ⓑ	Ⓐ/Ⓑ
π/2	Ⓐ/Ⓑ	Ⓐ
3π/2	Ⓐ/Ⓑ	Ⓑ





この干渉特性を利用して秘密鍵を生成

手順　①アリス：θ_a をランダムに設定して光子を送信
②ボブ：θ_b をランダムに設定して光子を検出
} 多数回行う

③ボブ→アリス：どの光子が真ん中の時刻で検出されたか、
それについて自分の位相が0か$\pi/2$か、を通知。

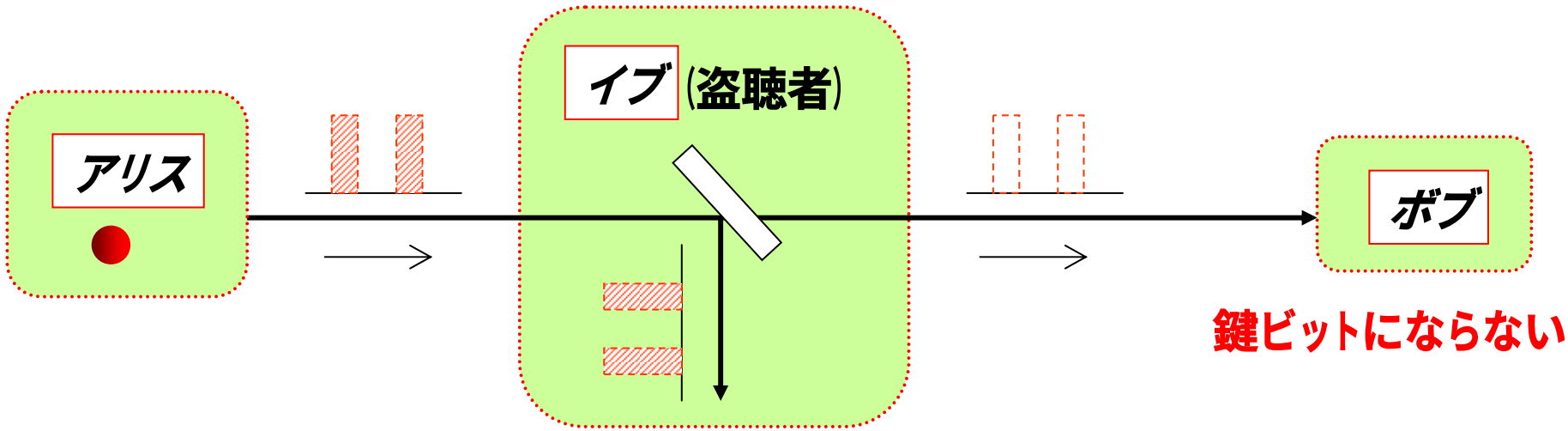
④アリス→ボブ：真ん中時刻で検出された光子について、
自分の位相が $\{0, \pi\}$ か $\{\pi/2, 3\pi/2\}$か、を通知。

⑤光子検出器が確定している場合について鍵ビット生成

$\theta_a = \{0, \pi\}$ かつ $\theta_b = 0$ の場合
$\theta_a = \{\pi/2, 3\pi/2\}$ かつ $\theta_b = \pi/2$ の場合
} A ⇒「0」
B ⇒「1」

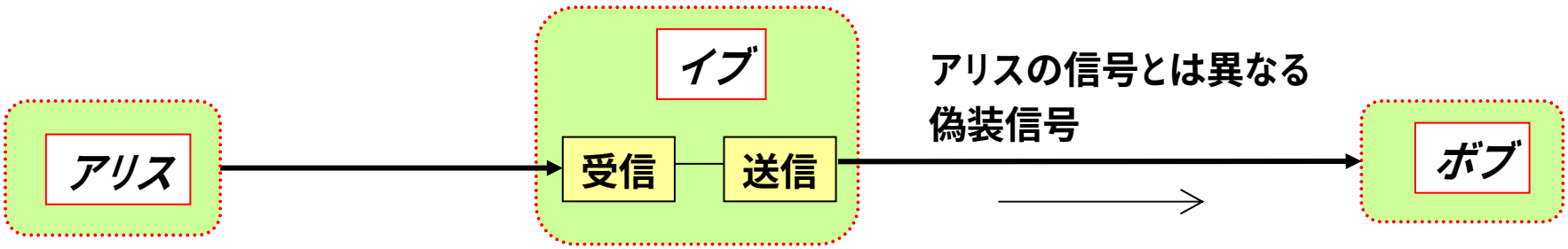
不確定な場合は無視。

なぜ安全か（その1）–盗み聞き盗聴に対して–



伝送信号をタッピング

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しよう。

But、確率状態か確定状態かは不明。

全てのビットを正しく受信できない。

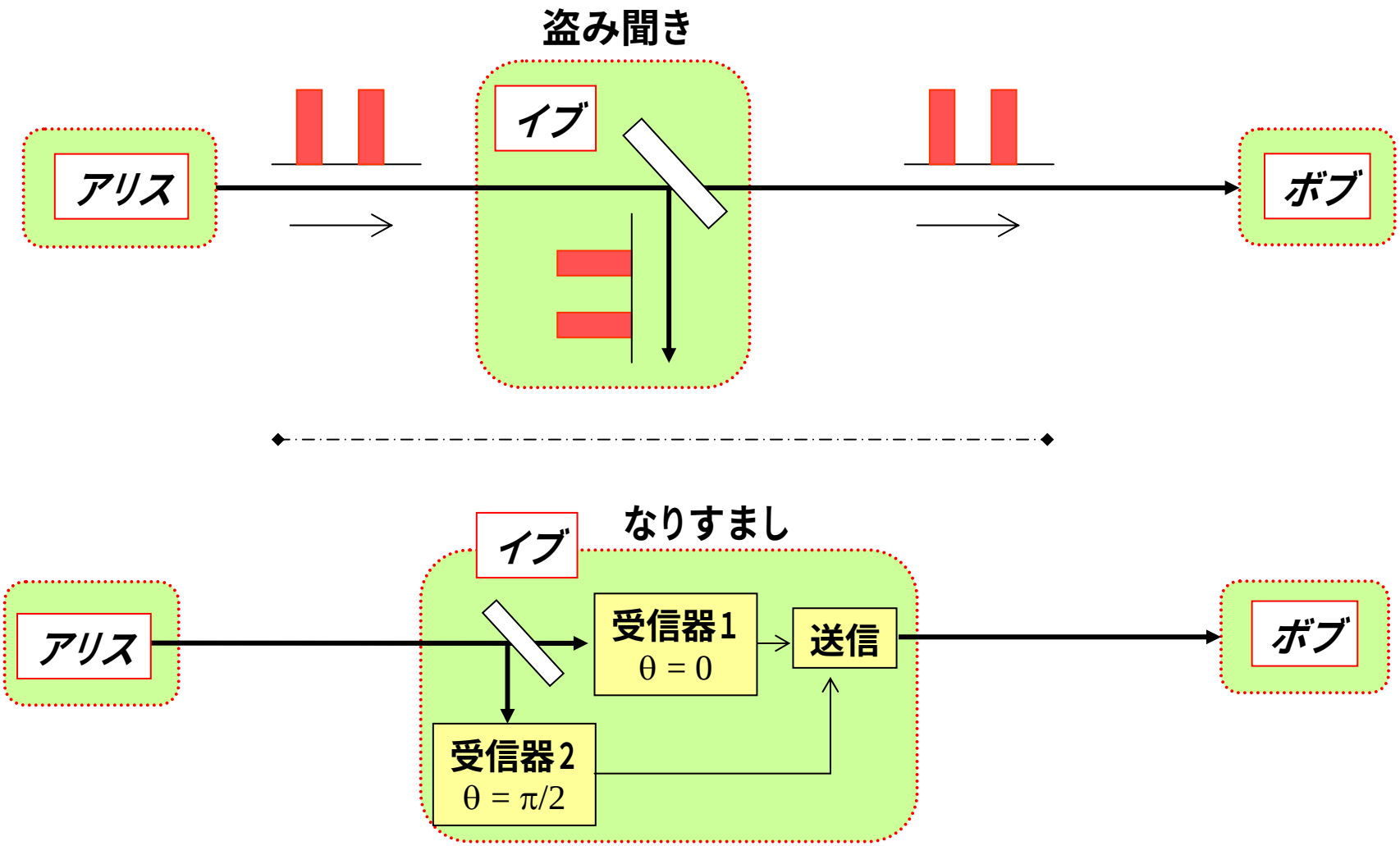
イブ位相

アリス側 位相	0	π/2
0	A	A/B
π/2	A/B	A
π	B	A/B
3π/2	A/B	B

(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、、、、



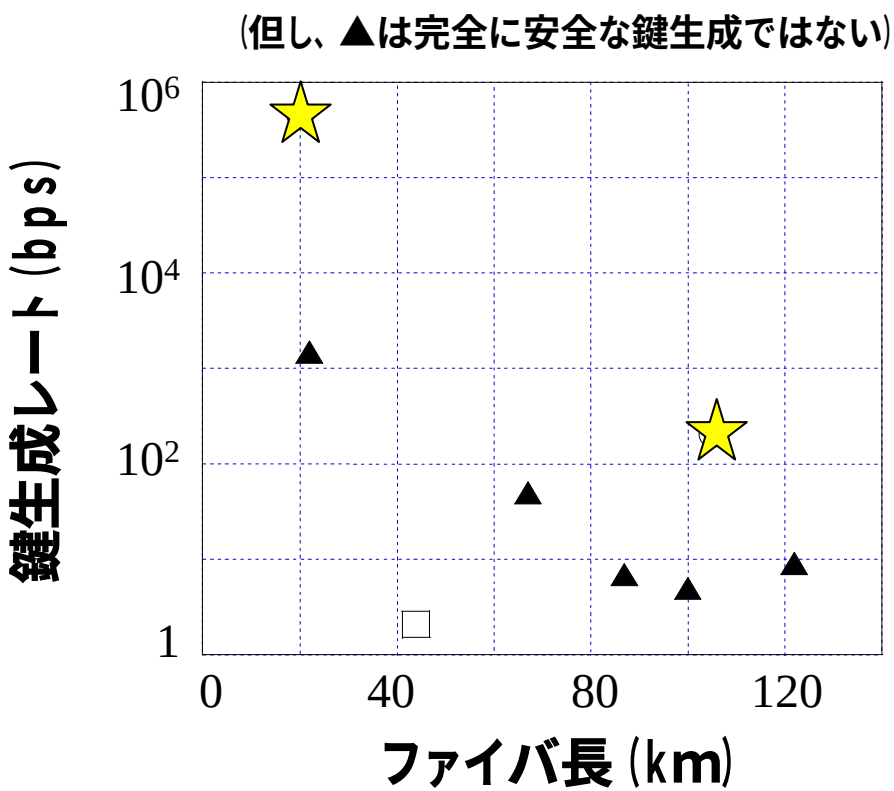
$\theta_a = 0, \pi/2, \pi, 3\pi/2$ の識別が可能

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

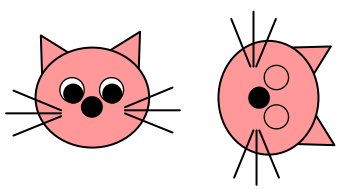


★ by NTT/Stanford

◆主な課題は光子検出器

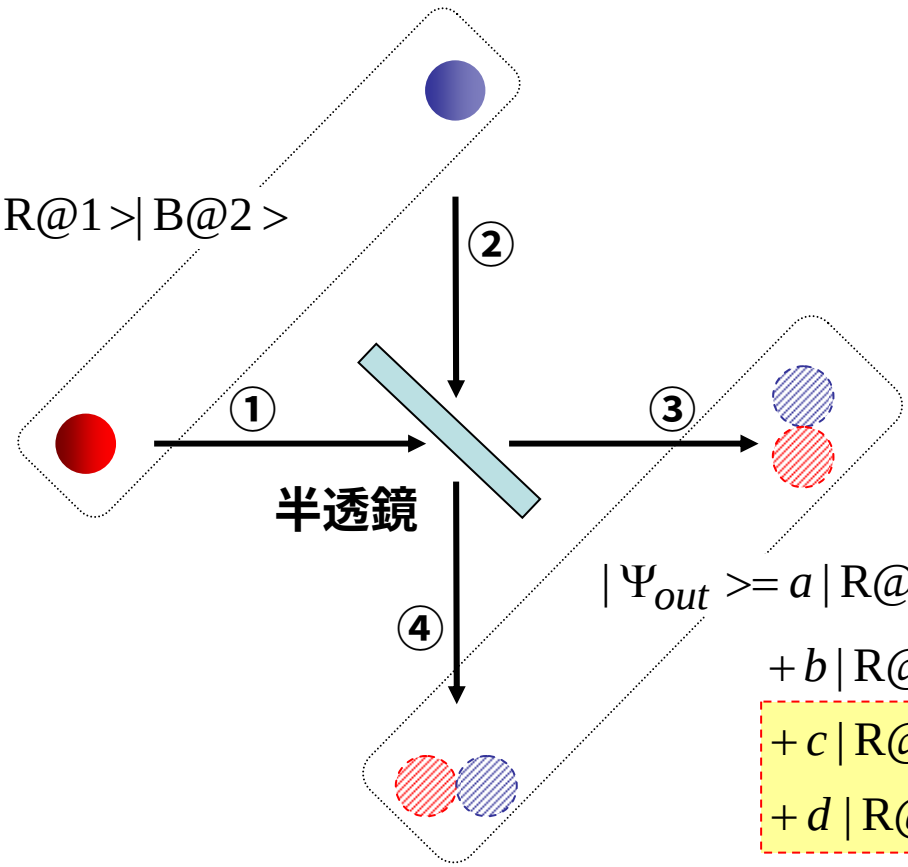
量子コンピュータ

－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



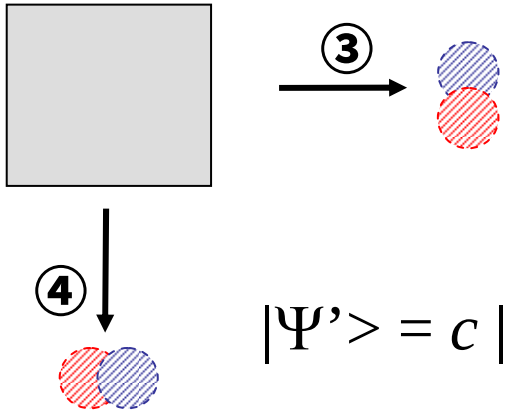
$|\Psi_{out}>= a\,|R@3>|B@3>$: 2光子とも③へ

$+ b\,|R@4>|B@4>$: 2光子とも④へ

$+ c\,|R@3>|B@4>$: Redは③へ、Blueは④へ

$+ d\,|R@4>|B@3>$: Redは④へ、Blueは③へ

各端子に光子が1個ずつ出力される状態に着目



$|\Psi'\rangle = c\,|●@3\rangle\,|●@4\rangle + c\,|●@3\rangle\,|●@4\rangle$

観測すると確定

$|\Psi''\rangle = |●@3\rangle\,|●@4\rangle$ **または** $|\Psi''\rangle = |●@3\rangle\,|●@4\rangle$

◆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

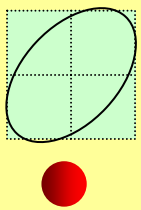
さて、量子コンピュータ

◆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

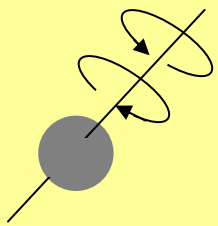
基本単位は量子ビット（Quantum bit: **Qビット**）

光子の偏波



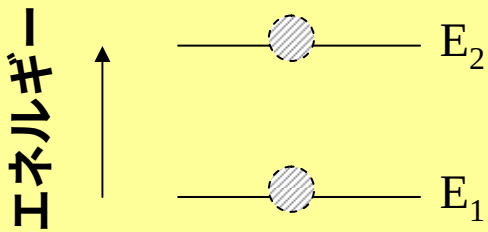
$|\psi> = a|H> + b|V>$

スピン



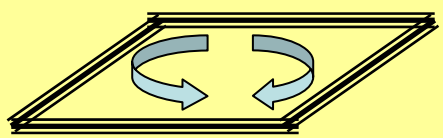
$|\psi> = a|\uparrow> + b|\downarrow>$

2つのエネルギー準位



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

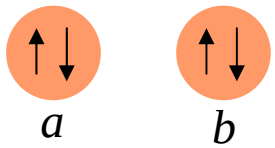
超伝導電流

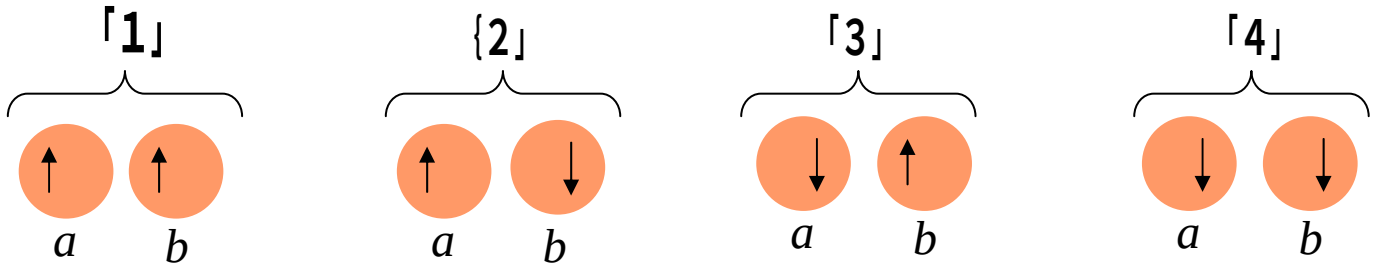


$|\psi> = a|R> + b|L>$

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

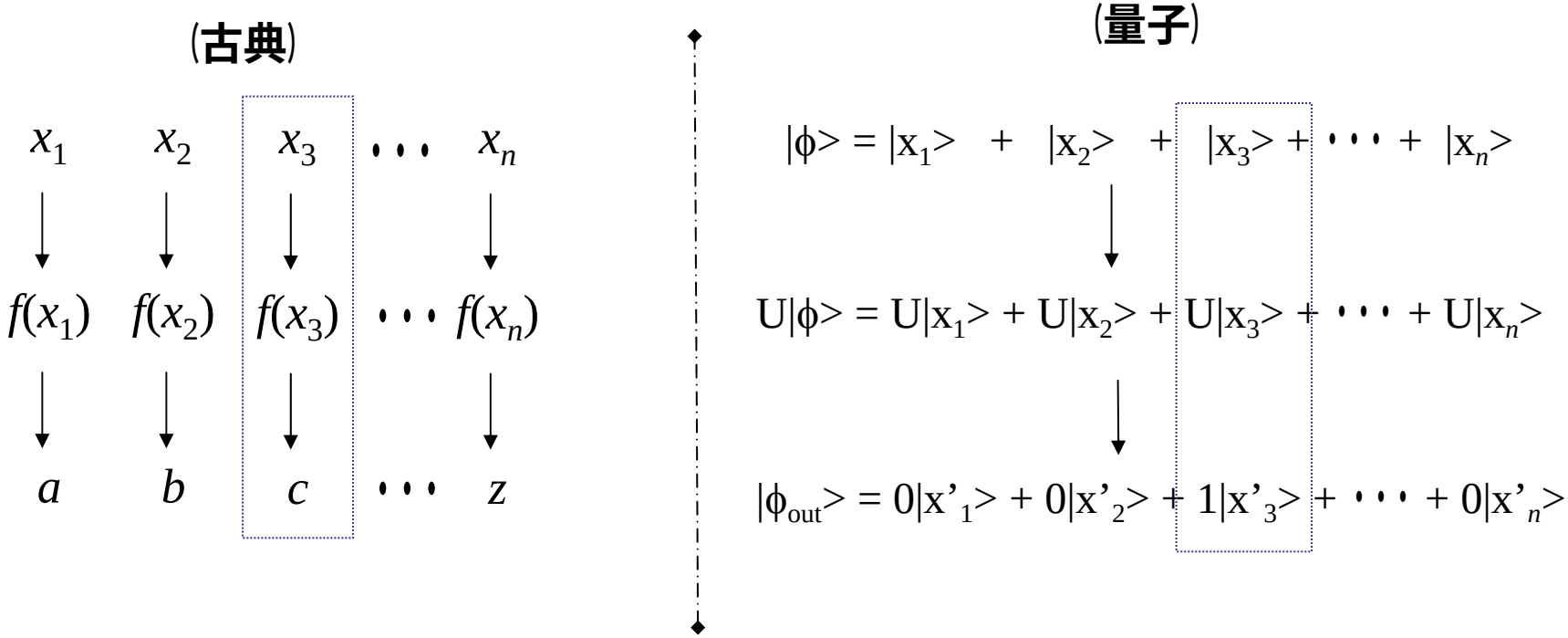
Q ビット n 個では

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

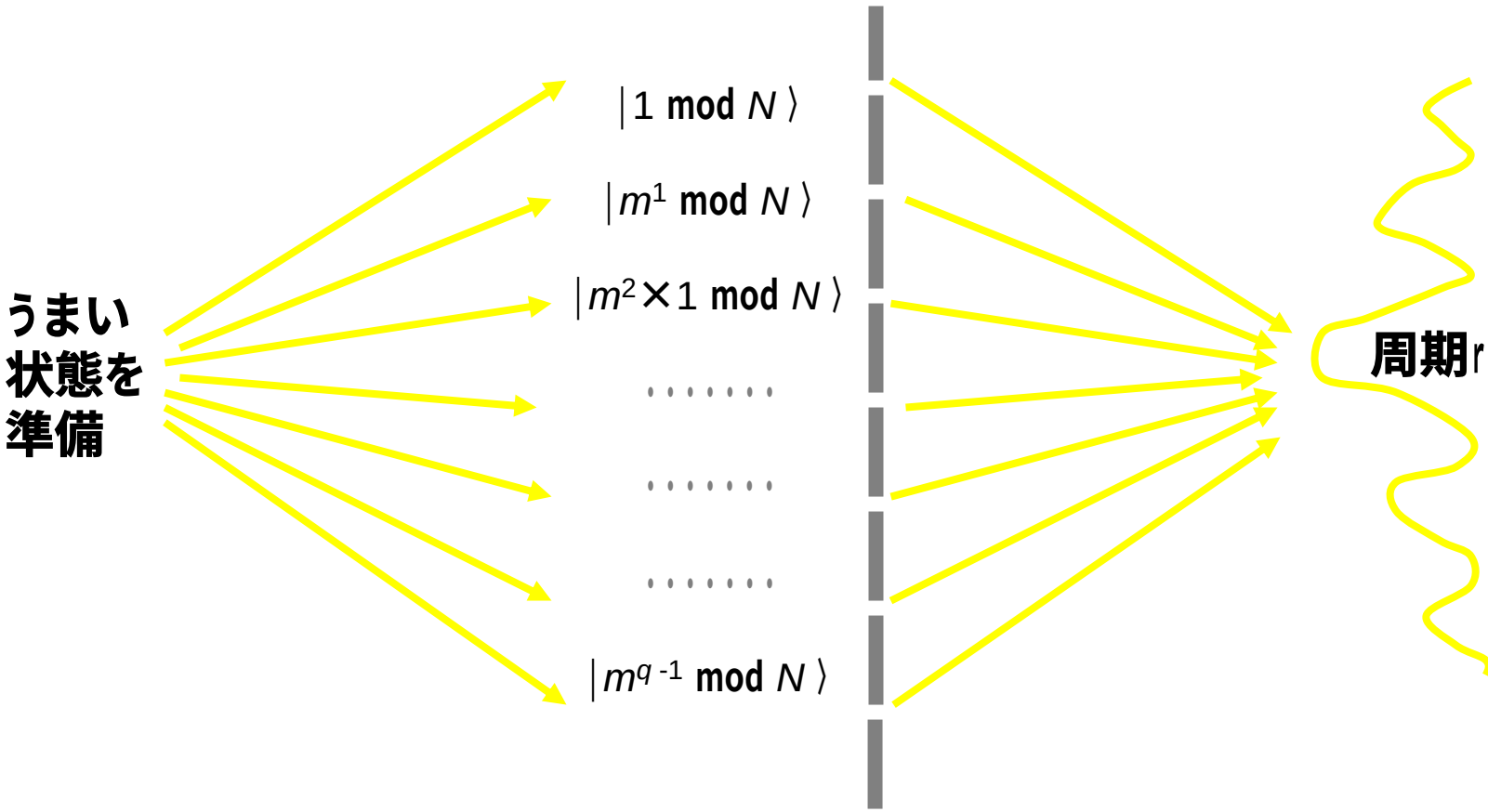
$f(x)=c$ を満たすxを見つけたい。

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



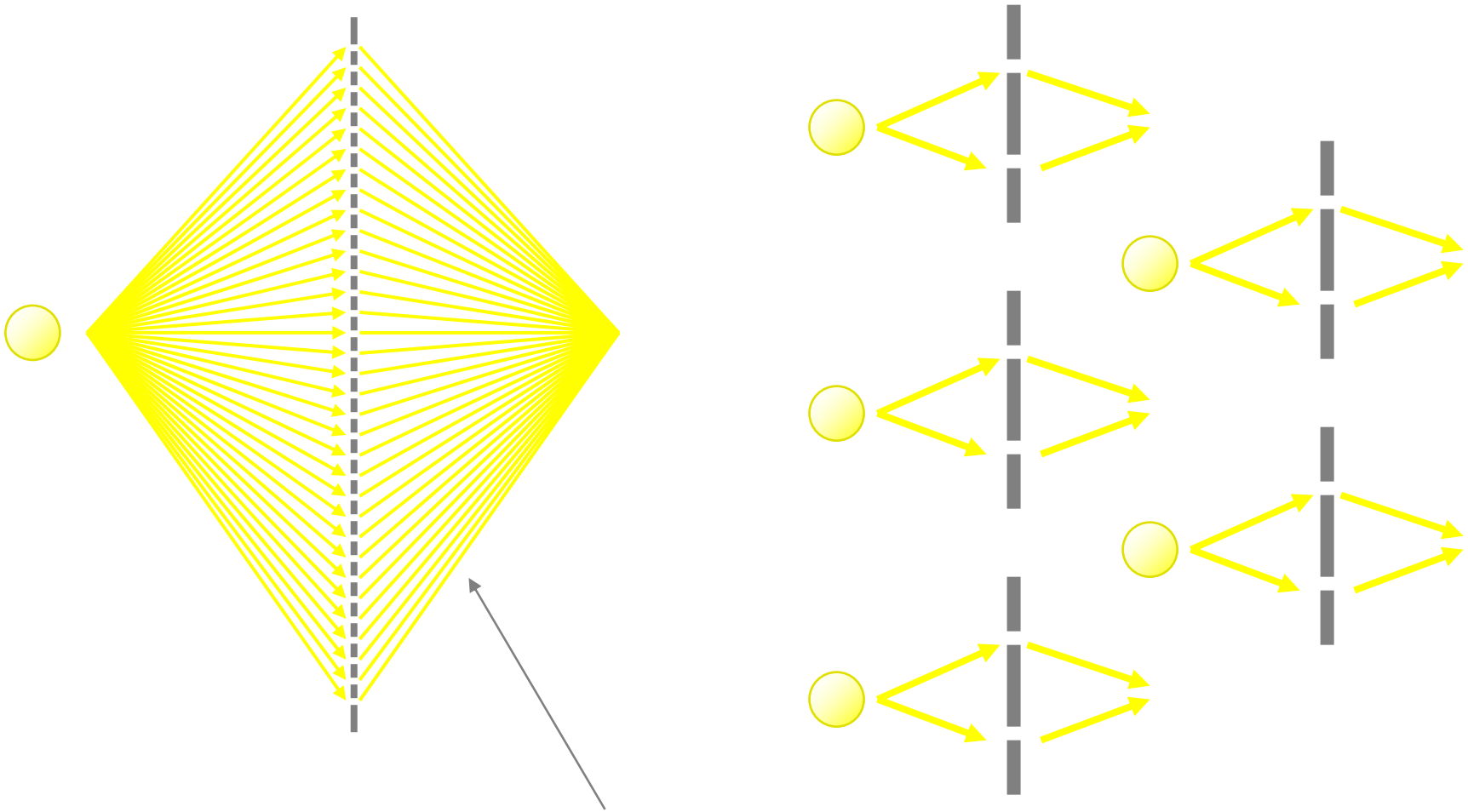
ここで疑問;

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、5個の量子があたかもひとつであるかのように振舞うことが必要

そこで、量子もつれを利用

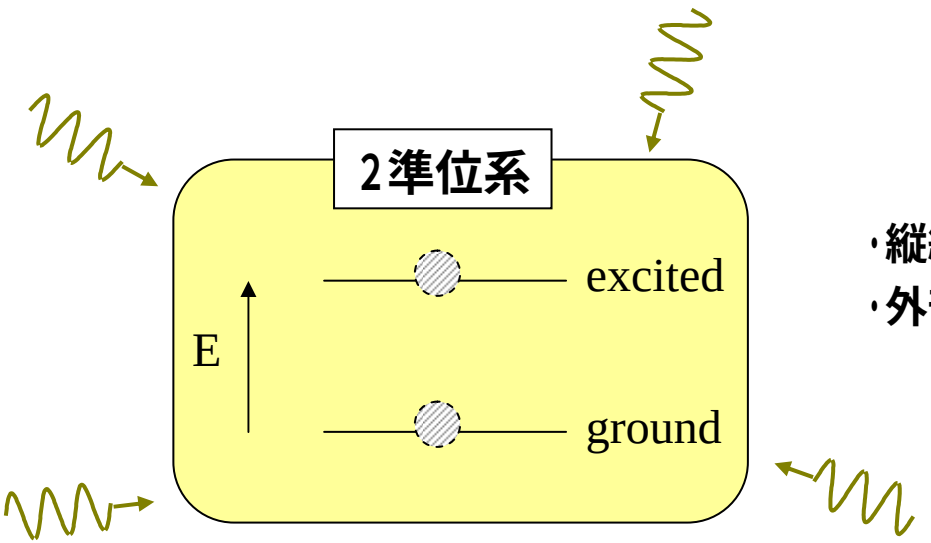
（基礎工・井元氏提供）

量子コンピュータ研究の状況

◆有効なアルゴリズムは、素因数分解（Shore's algorithm）とデータ検索。
（基本的にはアナログ処理。汎用計算には不向き。）

◆各種Qビット実現
古典計算より優位になるのはQビット数＞１００、現状の最高は7程度（MNR）。

◆Qビットの長時間保持が課題



・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

阪大の量子情報通信研究

科学技術振興機構（JST)戦略的創造研究推進事業チーム型研究
「量子情報処理システムの実現を目指した新技術の創出」に代表研究者4名

基礎工学研究科　井元研究室「光子を用いた量子演算処理新機能の開拓」
占部研究室「冷却イオンを用いた量子情報処理基礎技術」
北川研究室「分子スピン量子コンピュータ」
工学研究科　井上研究室「通信波長帯量子もつれ光子とその応用システム」

その他

理学研究科　藤原研究室（量子情報理論・量子推定）
小川研究室（凝縮系量子光学）
基礎工学研究科　伊藤研究室（励起子量子光学）
中野研究室（分子量子光学）
工学研究科　栖原研究室（量子もつれ発生デバイス）