量子情報通信の話

- 量子力学と情報通信の融合 -

大阪大学工学研究科

井上　恭

目次

[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）

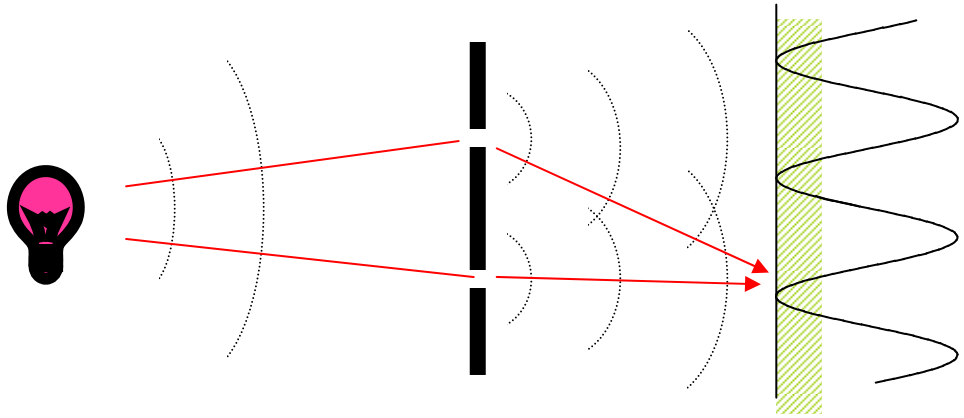
[2] 量子暗号

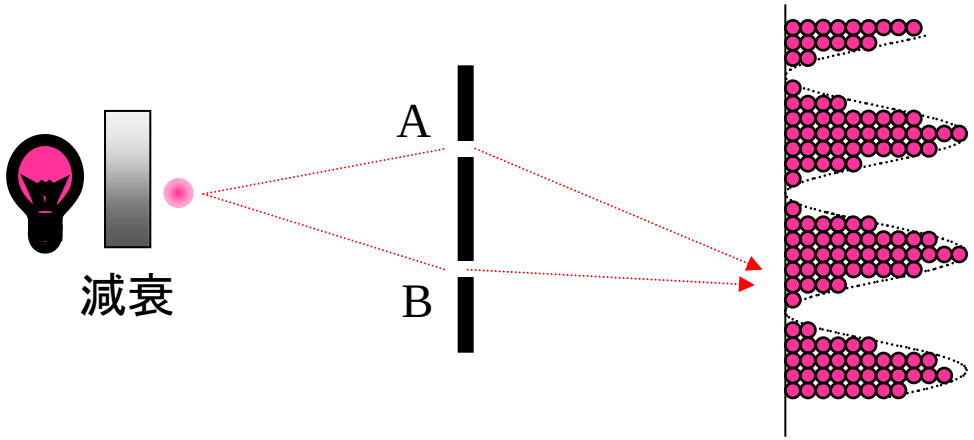
　　量子力学的に安全性が保証された暗号通信システム

[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

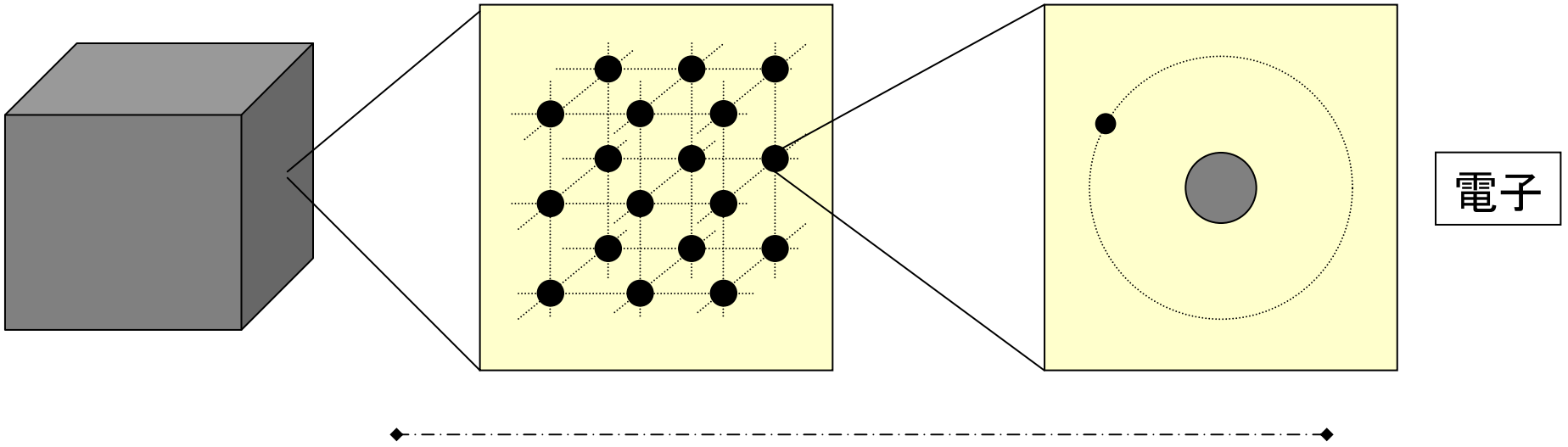
ヤングの干渉

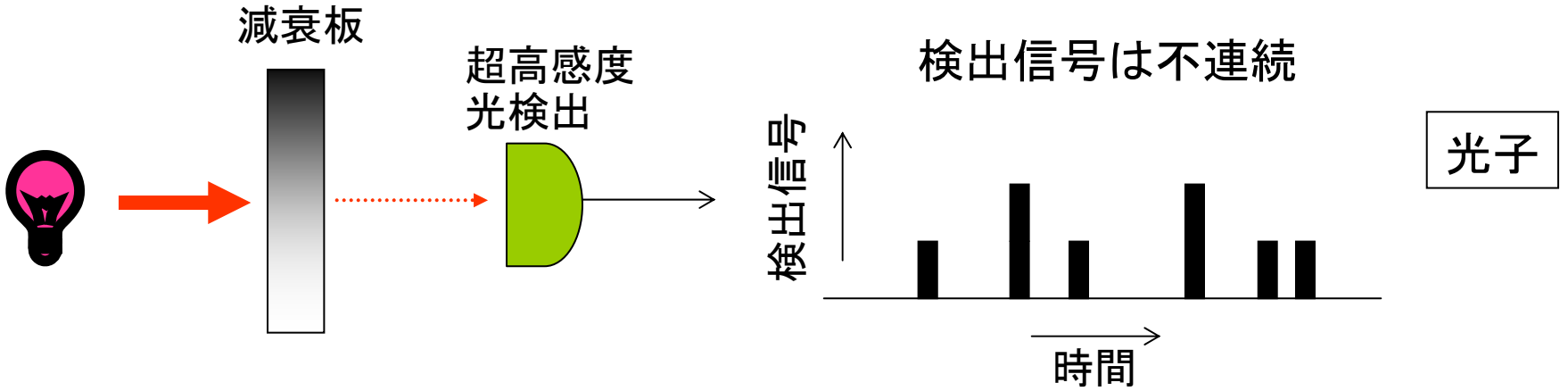




光は波であり粒である？

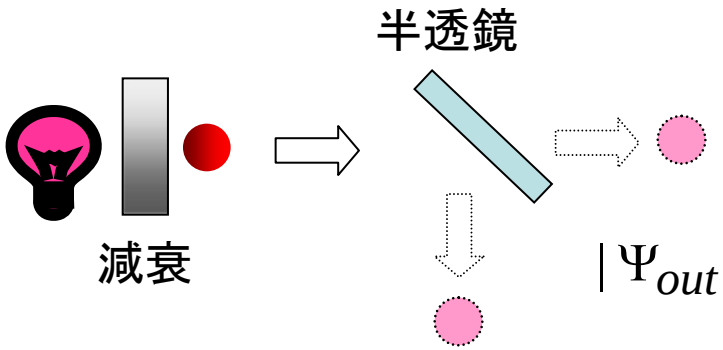
光のエネルギーには最小単位がある＝光子





量子状態は確率的
-重ね合わせ状態-

例１

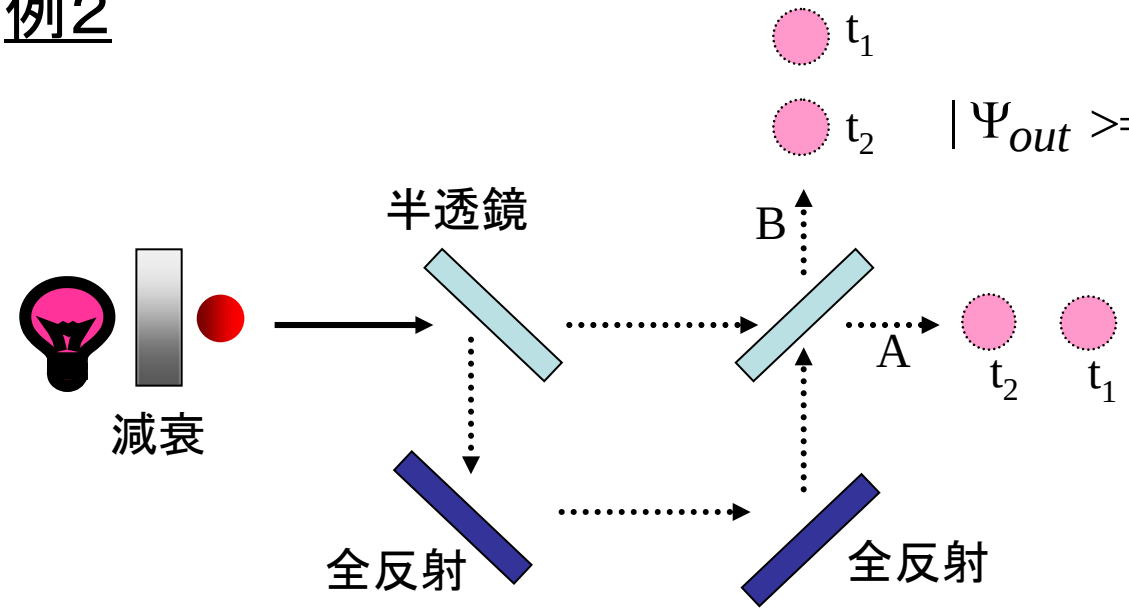


・光子は透過か反射かのどっちか
・どっちへいくかは確率的

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

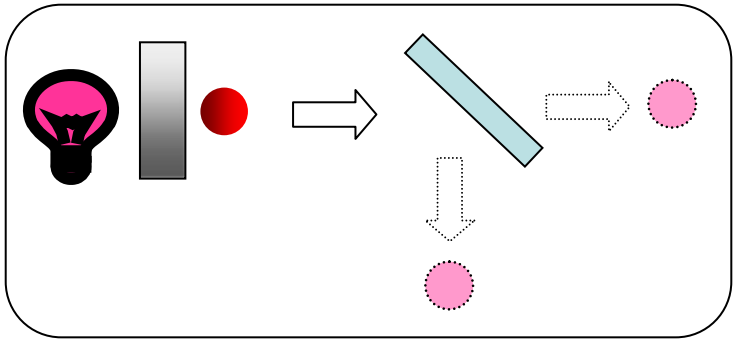
確率振幅

例２

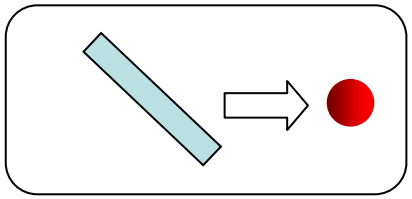


$$|\Psi_{out}>= c_1\,|\,\mathrm{A},\mathrm{t}_1> + c_2\,|\,\mathrm{A},\mathrm{t}_2> + c_3\,|\,\mathrm{B},\mathrm{t}_1> + c_4\,|\,\mathrm{B},\mathrm{t}_2>$$

量子状態は観測すると確定状態になる
（観測による状態変化）

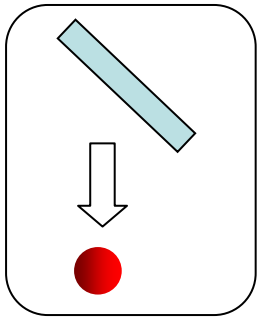


$|\Psi_{out}\rangle = a|\text{透過}\rangle + b|\text{反射}\rangle$



$|\Psi_{out}\rangle = |\text{透過}\rangle$

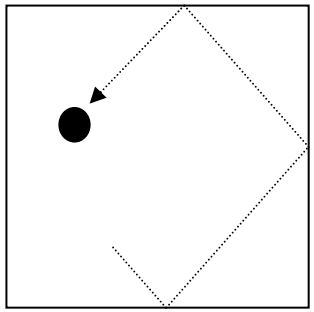
または



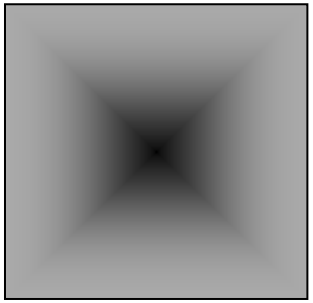
$|\Psi_{out}\rangle = |\text{反射}\rangle$

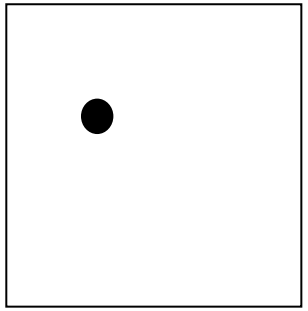
箱の中の電子

（古典）



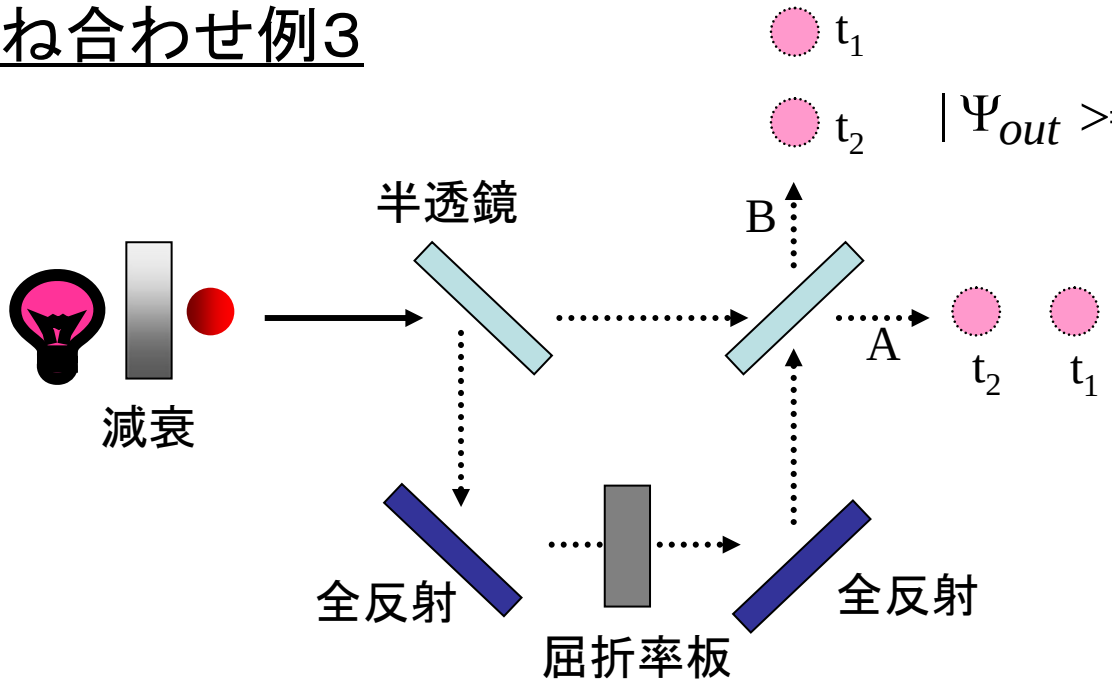
（量子）





確率振幅は複素数

重ね合わせ例3



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

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。

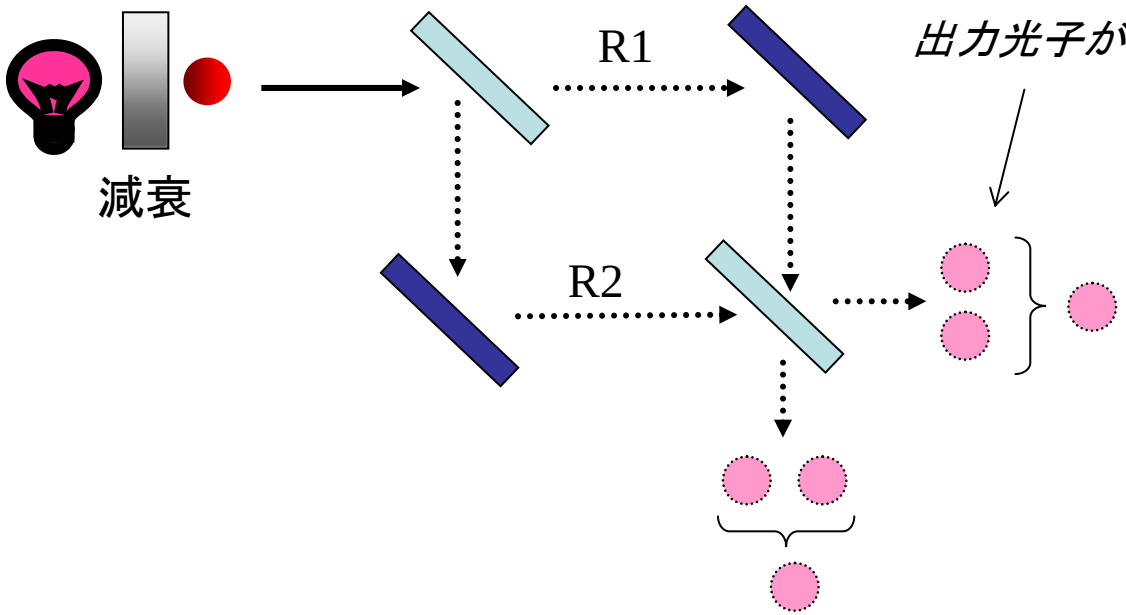
↓

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。

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

確率振幅は干渉する

重ね合わせ例4



出力光子がどちらを通ったかは識別できない

$$c_1|\bullet>_{R1} + c_2|\bullet>_{R2}$$

$$=$$

$$(c_1 + c_2)|\bullet>$$

確率 : $|c_1 + c_2|^2$

$$=$$

$$|c_1|^2 + |c_2|^2 + 2\mathrm{Re}[c_1 c_2^*]$$

$$c_3|\bullet>_{R1} + c_4|\bullet>_{R2}$$

$$=$$

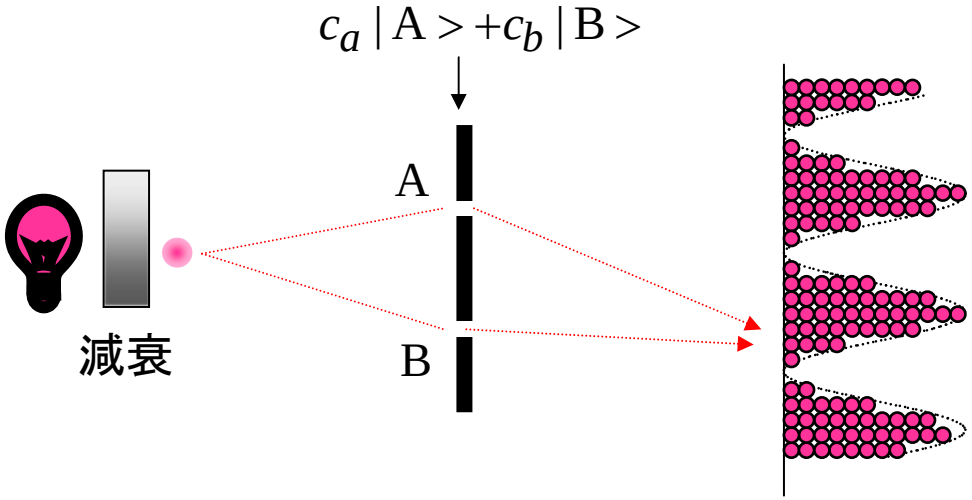
$$(c_3 + c_4)|\bullet>$$

干渉

確率 : $|c_3 + c_4|^2 = |c_3|^2 + |c_4|^2 + 2\mathrm{Re}[c_3 c_4^*]$

で、1光子のヤングの干渉

光子の干渉



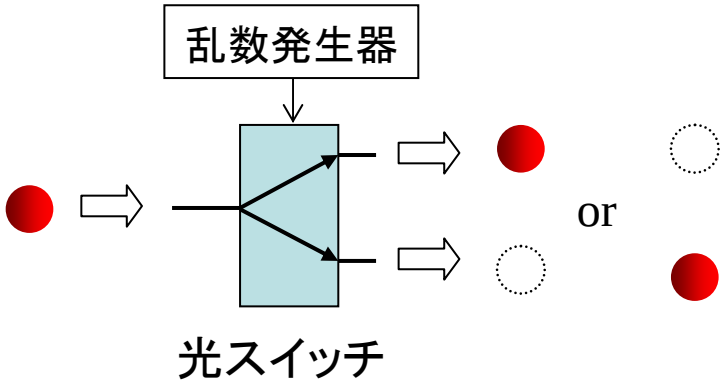
2つのスリットを経由した光子状態の係数が干渉

1光子の干渉結果を超短時間に積分したのが通常光波の干渉結果

ただし

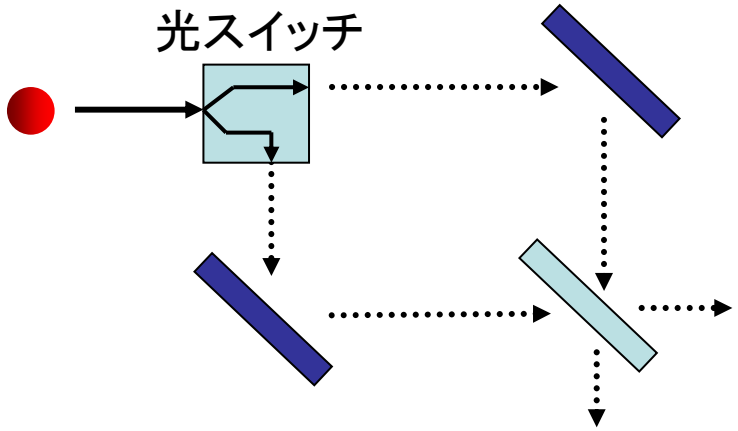
重ね合わせ状態であるためには、原理的に決まっていないことがポイント

重ね合わせでない例1



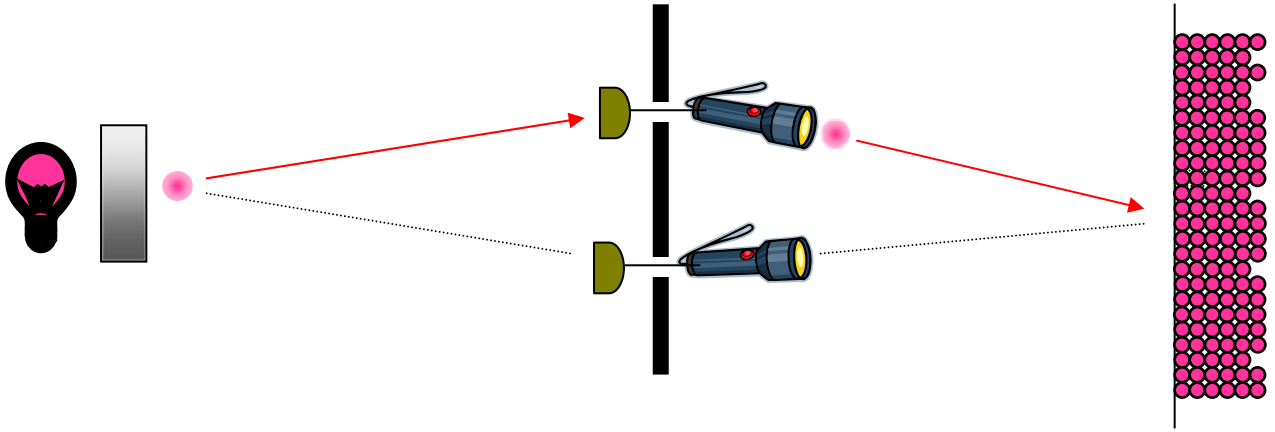
原理的にはどちらかに決まっている。
||
「重ね合わせ」ではない。

重ね合わせでない例2



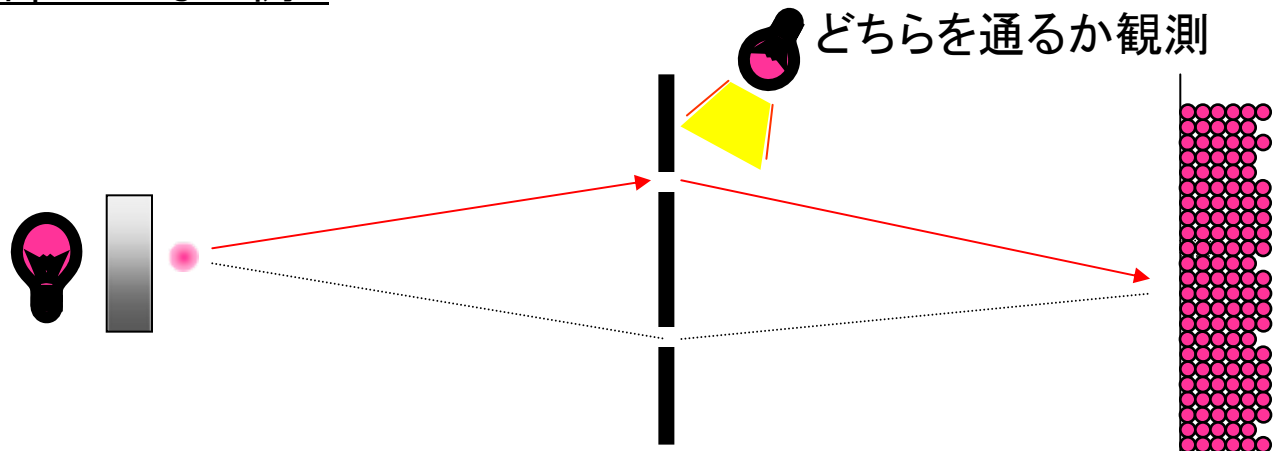
干渉せず

重ね合わせでない例3



干渉縞は消滅

重ね合わせでない例4

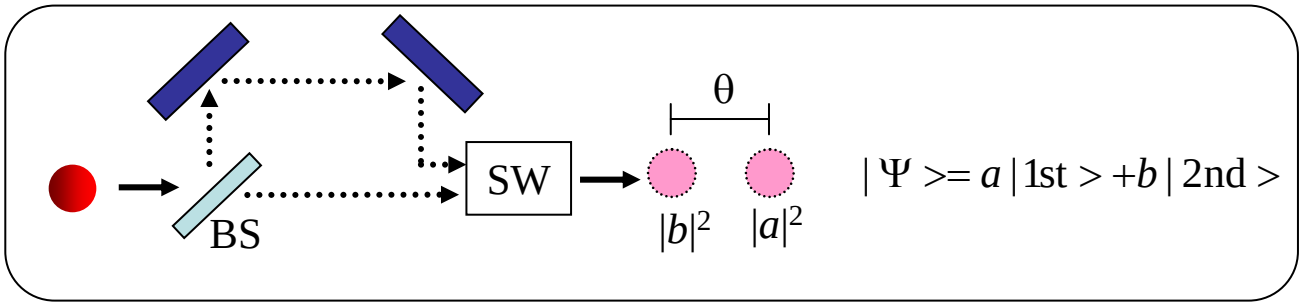


$$|\psi>=c_a|\mathrm{A}>+c_b|\mathrm{B}>$$

観測

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

重ね合わせ状態は1回の測定では特定できない

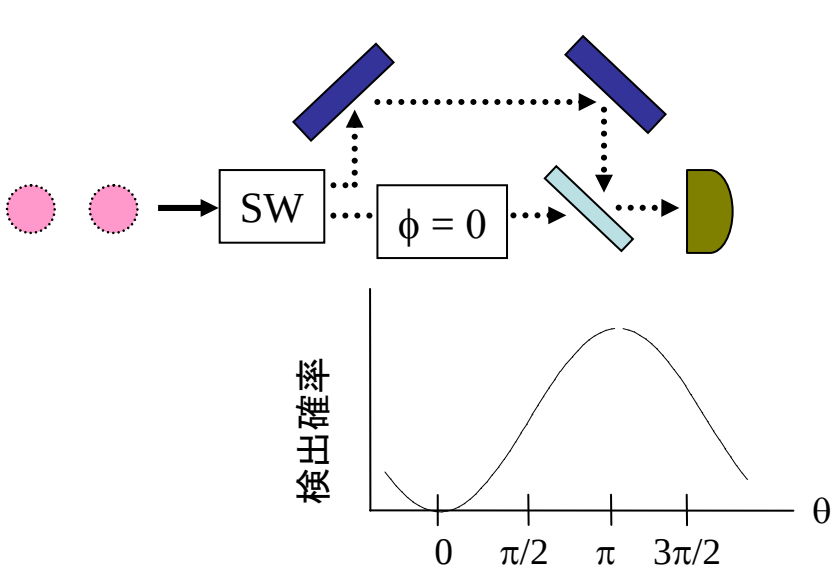


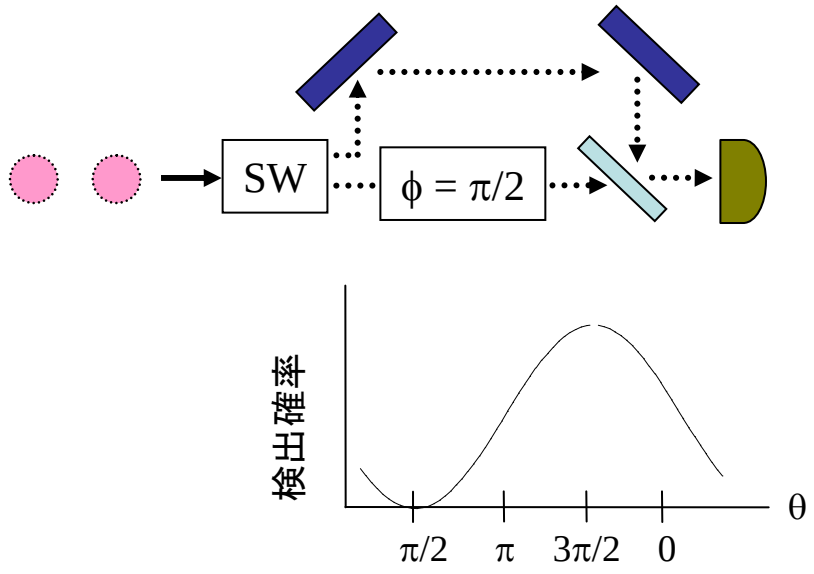
ビームスプリッタ(BS)の分岐比が不明の場合　（e.g., $\{|a|, |b|\}$が不明）

出射側で何回も光子検出して、$\{|a|^2, |b|^2\}$を推定。

ビームスプリッタの分岐比が分かっている場合（e.g., $|a| = |b| = 1/\sqrt{2}$ for 1:1)

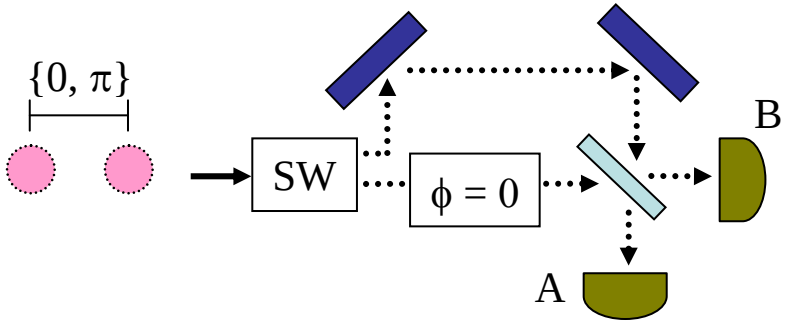
$\{a, b\}$の相対位相θ が不明　→　2種類の干渉測定を何回も行う





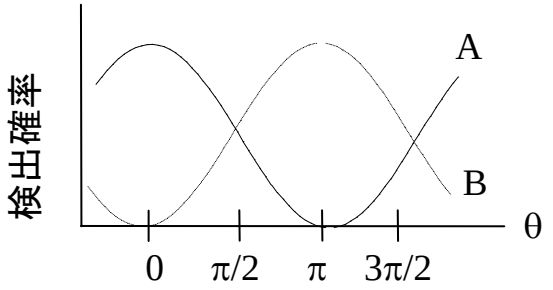
被測定系の状態の候補が2つの時は、特定できる場合とできない場合とがある。

分岐比は1:1で θ = {0, π}

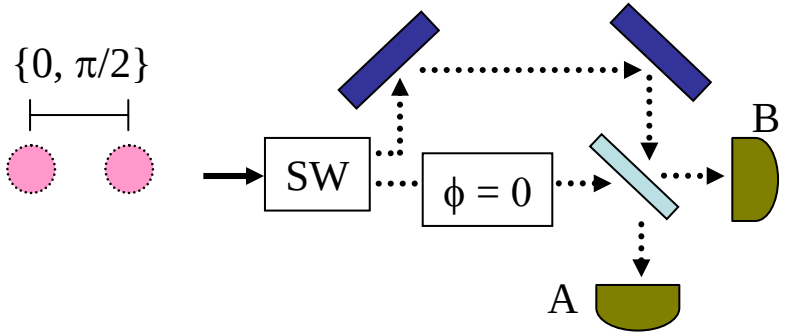


Aで光子検出→θ = 0
Bで光子検出→θ = π

特定可



分岐比は1:1で θ = {0, π/2}



Aで光子検出→θ = 0 or π/2
Bで光子検出→θ = π/2

特定できる場合とできない場合がある。

不確定性原理　（非直交な2状態は100%の確率では識別できない。）

そこで

以上のような量子状態の性質

（重ね合わせ、量子干渉、観測と状態変化、不確定性、など）

を情報通信・情報処理に応用しよう

⇩

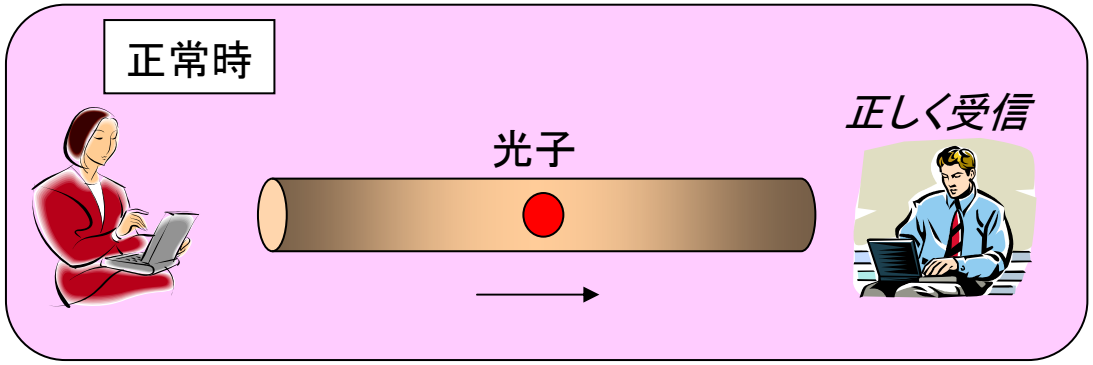
量子暗号

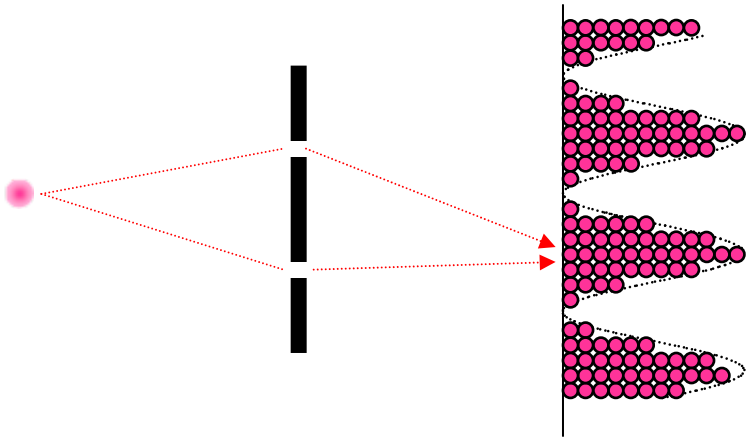
量子コンピュータ

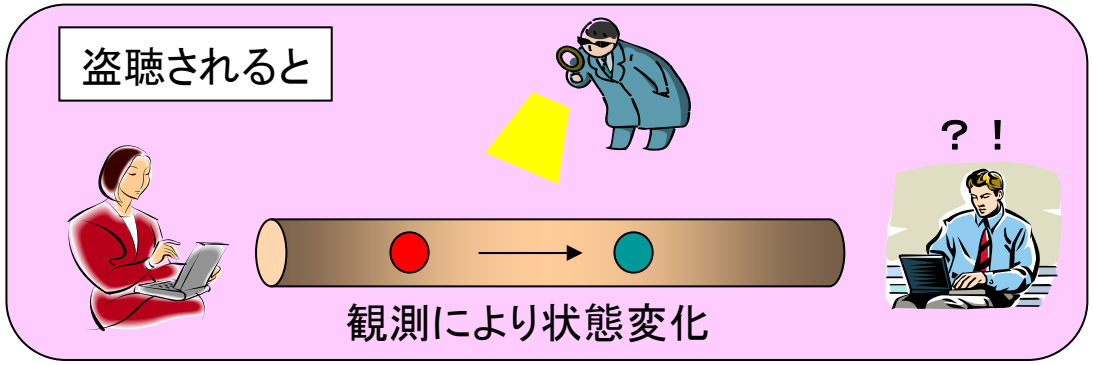
そこで(1)

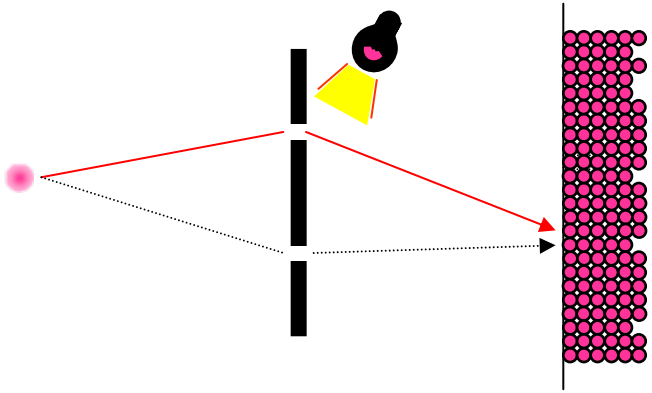
量子暗号(量子鍵配送)

量子力学的重ね合わせを利用した暗号通信システム







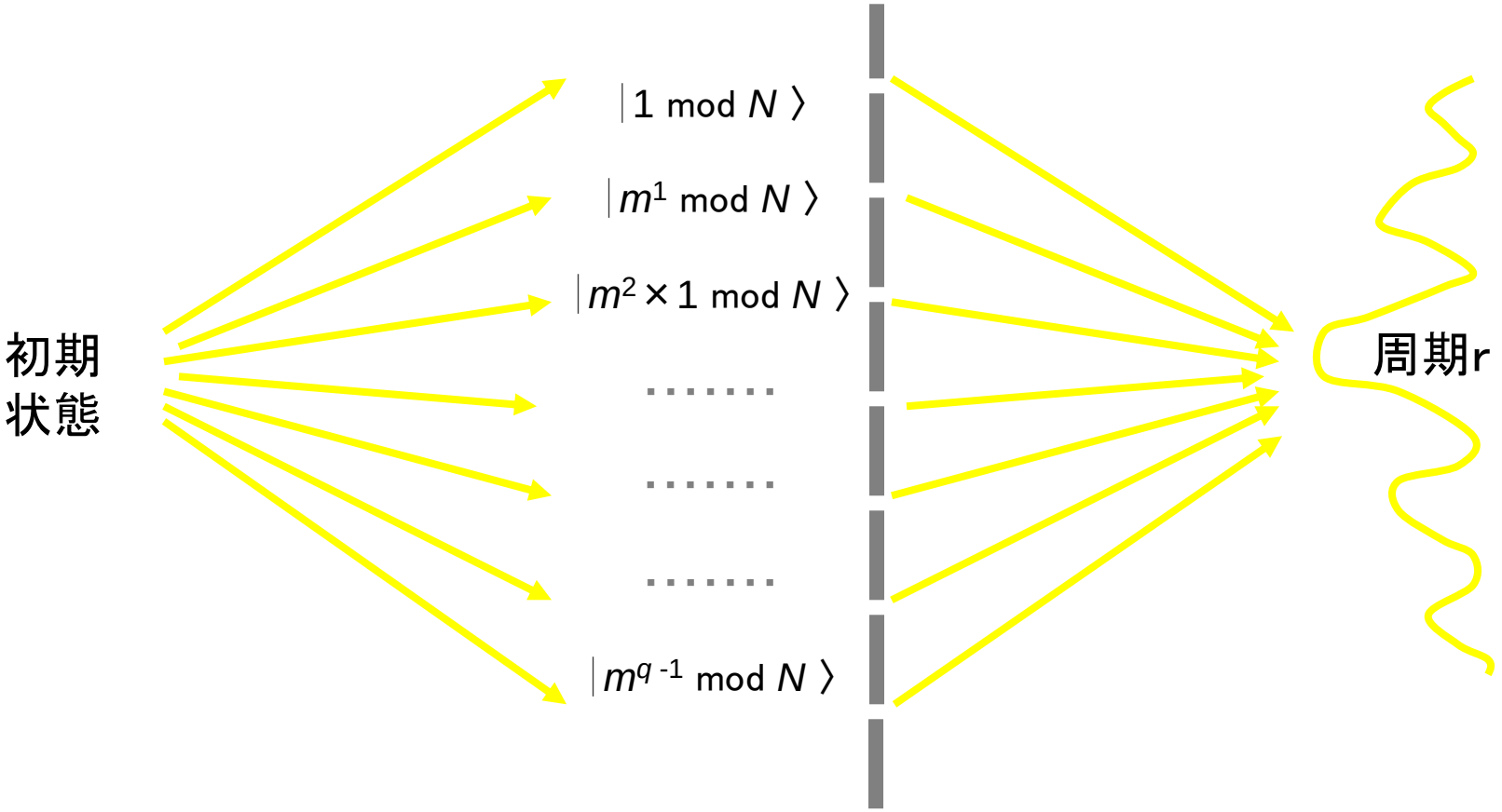


量子状態の変化から盗聴検知

そこで(2)

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システム

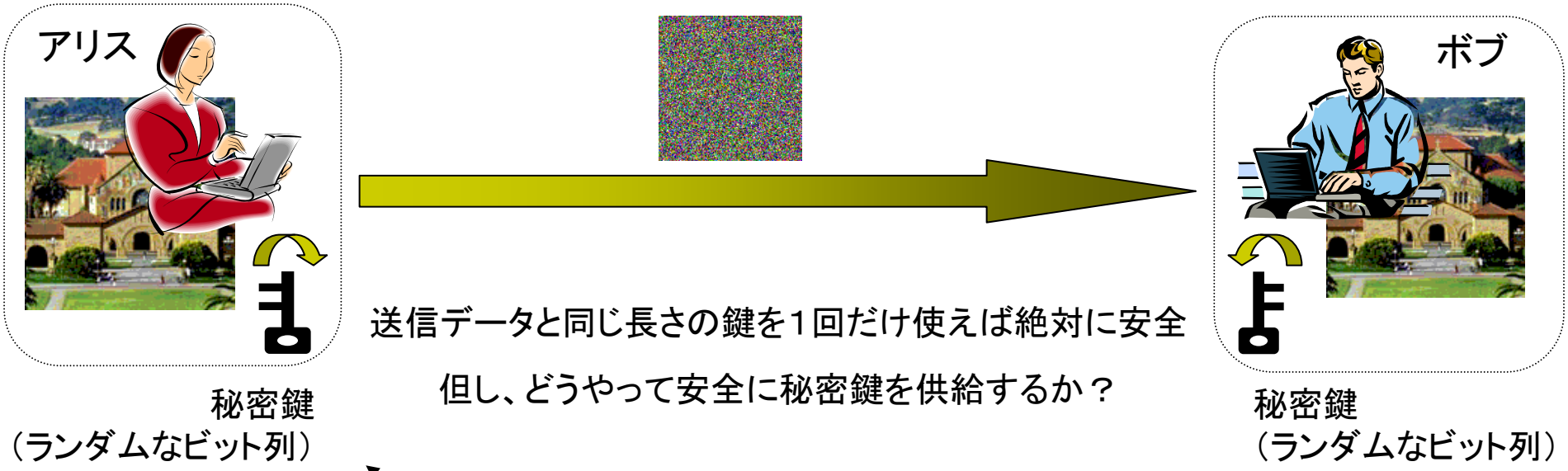


量子暗号通信

(1) 基本構成と原理

(2) 実現技術

秘密鍵暗号



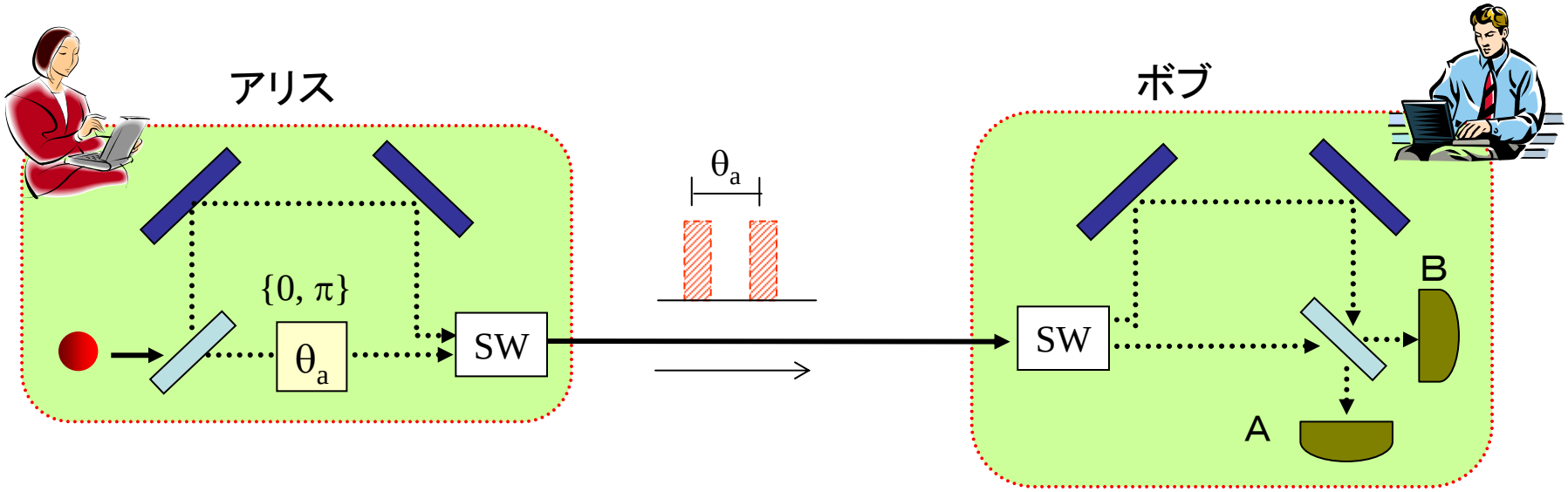
量子暗号（量子鍵配送）

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

BB84プロトコル

鍵配送の構成・原理



$\theta_a = 0$ ⇔ 検出器A

$\theta_a = \pi$ ⇔ 検出器B

アリス

$\theta_a = 0$ ⟶ ビット「0」

$\theta_a = \pi$ ⟶ ビット「1」

ボブ

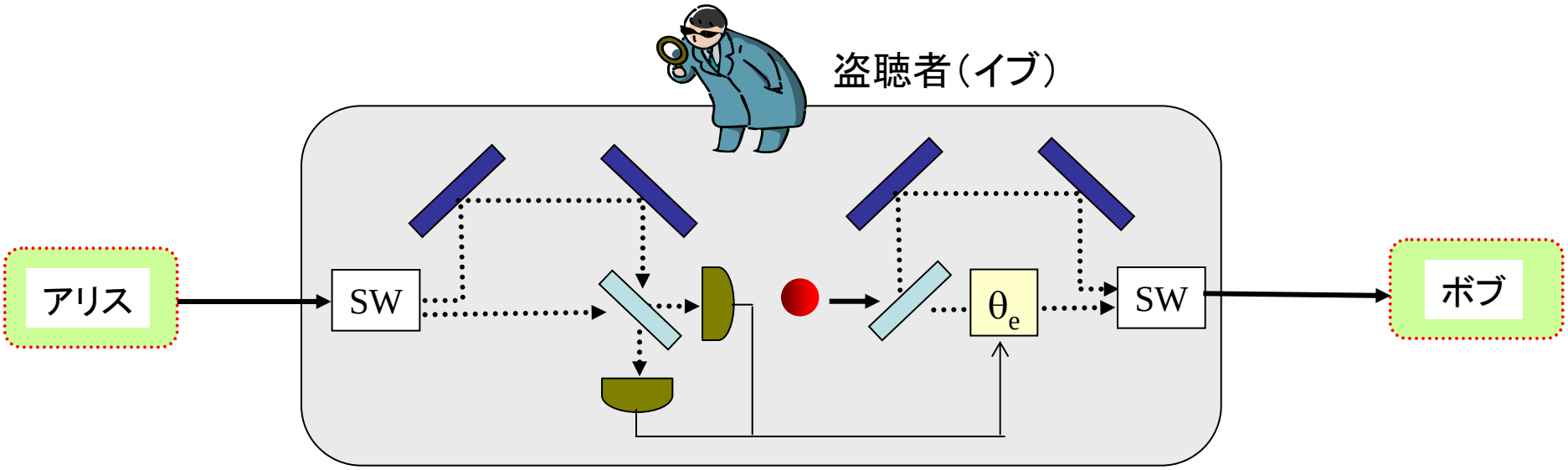
検出器A ⟶ ビット「0」

検出器B ⟶ ビット「1」

⇒ アリスとボブで同じビット値

但し、これではただの位相変調信号伝送

これだけでは盗聴可能

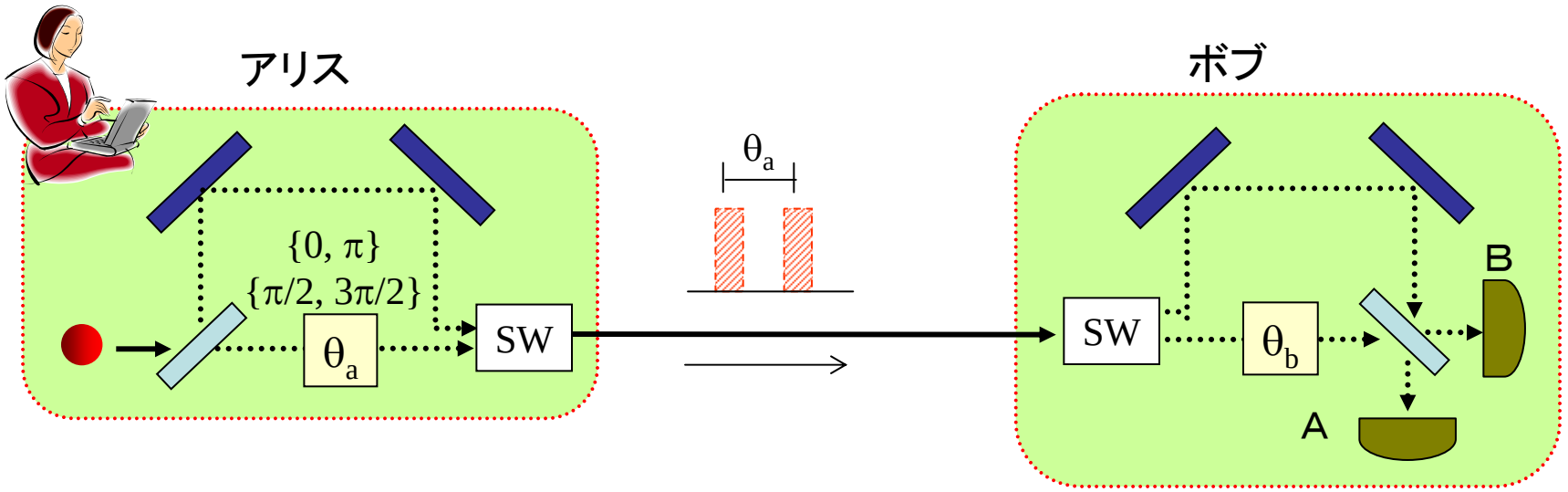


① θ_a を測定

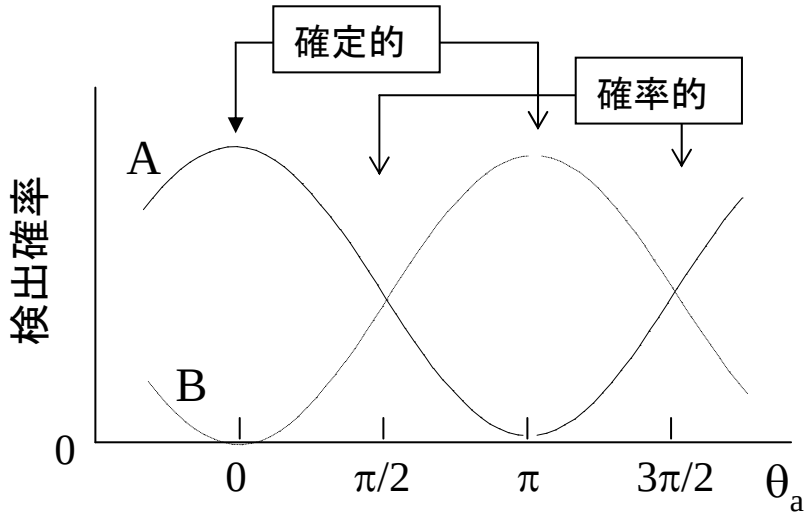
②測定値を印加した光子をボブに送信

そこで

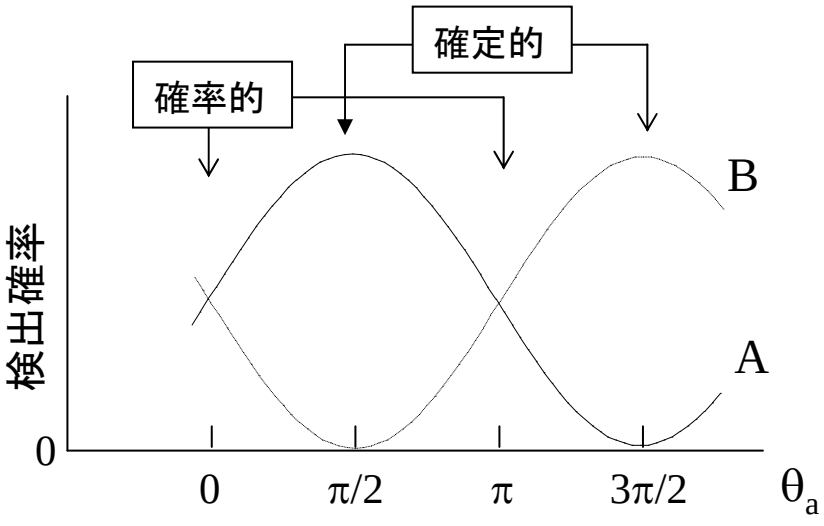
4つの位相値を使用



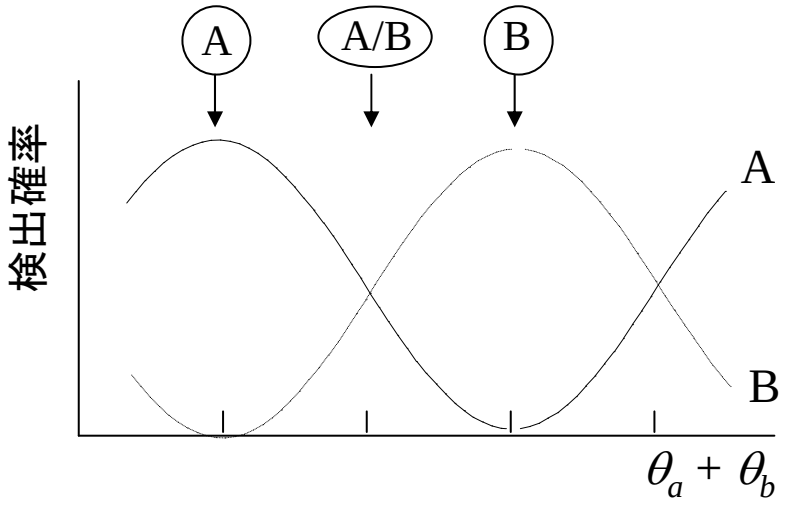
$\theta_b = 0$ の場合



$\theta_b = \pi/2$ の場合



どのθ_a に対して測定結果が確定的か確率的かは、
θ_b によって決まる。



ボブ位相

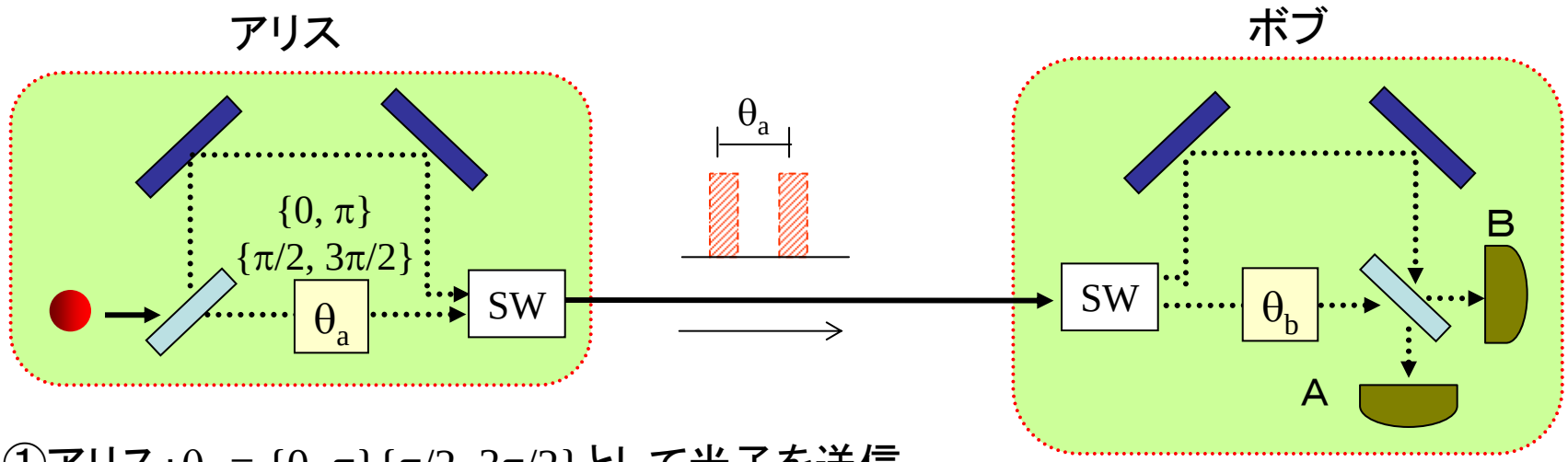
アリス位相	0	π/2
0	A	A/B
π/2	A/B	A
π	B	A/B
3π/2	A/B	B

並べ替え

ボブ位相

アリス位相 (θ_a \ θ_b)	0	π/2
0	A	A/B
π	B	A/B
π/2	A/B	A
3π/2	A/B	B

鍵生成手順



①アリス：θ_a = {0, π}{π/2, 3π/2}として光子を送信

②ボブ：θ_b = {0, π/2}として光子を検出

③ボブ→アリス：光子検出時刻及びその時のθ_bを通知

④アリス→ボブ：検出光子について、θ_aが {0, π} か {π/2, 3π/2}か、を通知

⑤確定光子検出について

θ_a = {0, π} かつ θ_b = 0 の場合
θ_a = {π/2, 3π/2} かつ θ_b = π/2 の場合

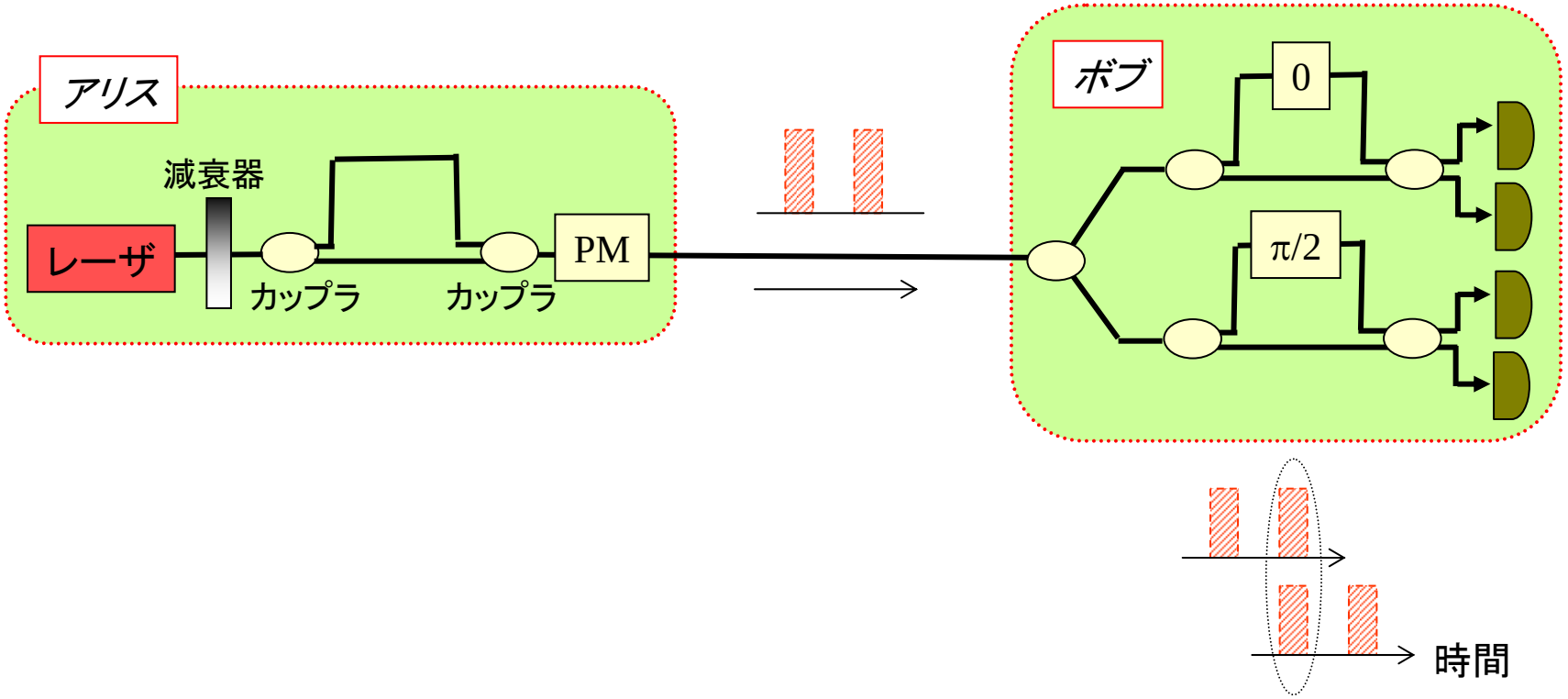
} A ⇒「0」
B ⇒「1」

鍵ビット

θ_a \ θ_b	0	π/2
0	A	A/B
π	B	A/B
π/2	A/B	A
3π/2	A/B	B

不確定検出は無視
（ランダムビット列を作ることが目的なのでこれでOK)

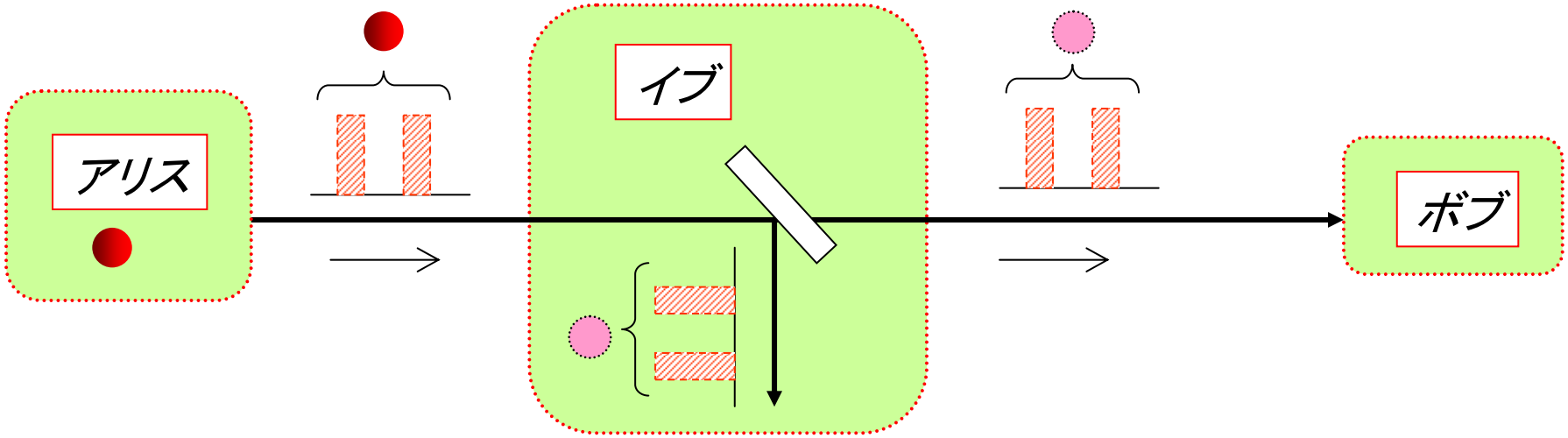
実際の構成



真ん中の時刻では前後のパルスが干渉 ⟶ ビット生成

前パルスが短経路
後パルスが長経路
} の場合は干渉しないが、それは無視する。

なぜ安全か（その1）–盗み聞き盗聴に対して–

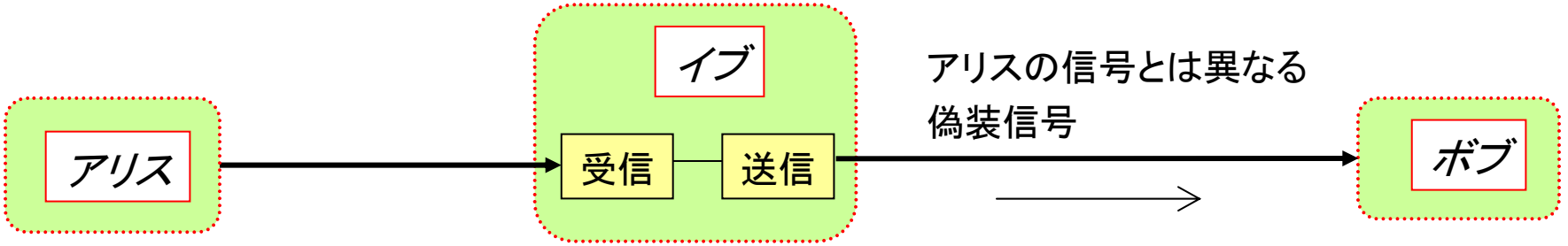


伝送信号を分岐して測定

イブが光子を測定したらボブは何も測定しない。
ボブが光子を測定したらイブは何も測定しない。

⇨ *鍵ビットの盗聴にならない*

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、4位相値は正しく判別することは不可能。

不確定性原理

ある確率でビット誤り

↓

テストビットのチェックにより
盗聴発覚

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

例えば、

アリスは$\theta_a = \pi/2$で送信。→ ビット「0」

↓

イブは位相0で測定し、Bで光子検出。

↓

イブは位相差 π の光子を送信。

↓

ボブは$\theta_b = \pi/2$で測定し、Bで光子検出。→ ビット「1」

不一致

実現への課題

単一光子検出器

APD（アバランシェ・フォトダイオード）をブレークダウン電圧以上で使用するのが標準的

性能指数は、量子効率：1光子入力に対しアバランシェが起こる確率

ダークカウント：光子未入力時に起こるカウント

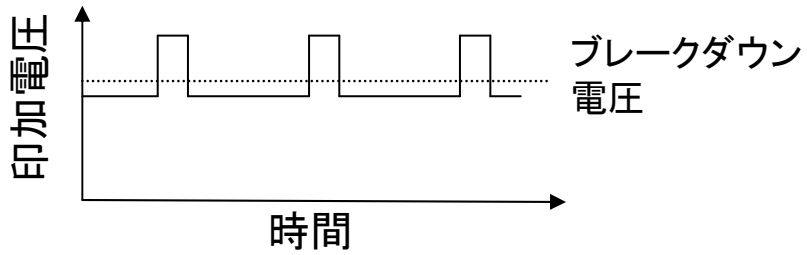
アフターパルス：正規のアバランシェに続けて起こる誤カウント（高速化の障害）

短波長帯：市販のSi-APDあり

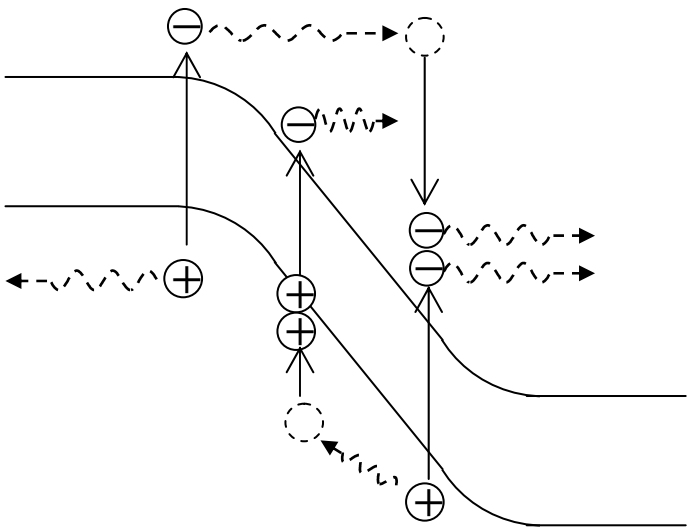
量子効率 ～ 60%、ダークカウント < 100cps

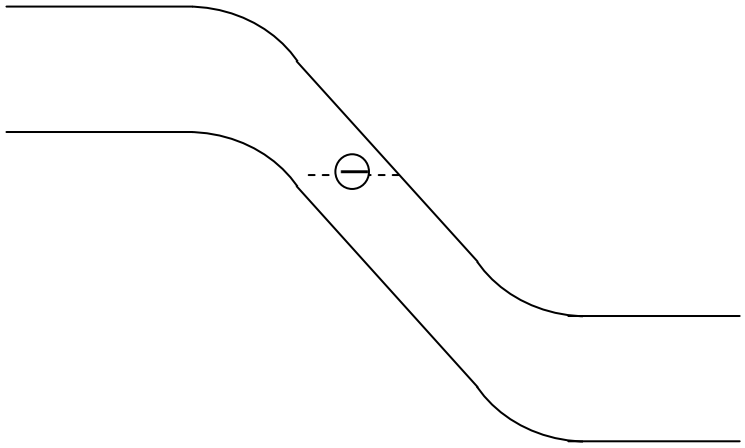
長波長帯（ファイバ通信波長帯）：冷却InGaAs-APDをゲートモードで使用

量子効率 ～ 10%、ダークカウント～10^{-5}/gate、繰り返し ＜ 数MHz



アフターパルス





不純物準位に電子がトラップ

↓

自然励起

↓

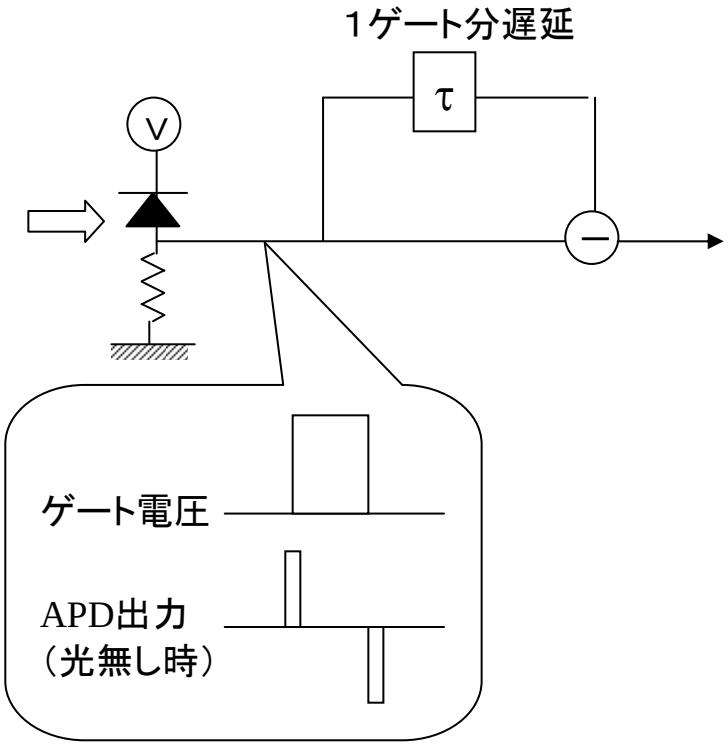
アバランシェ

APD光子検出器の高速化

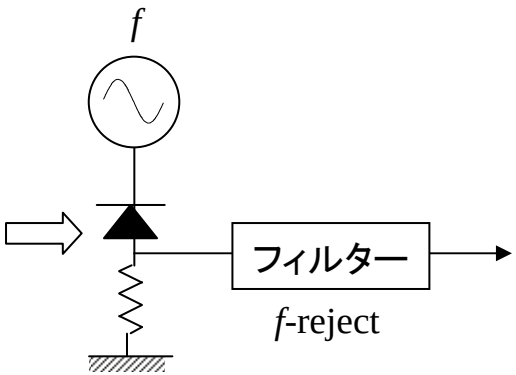
印加電圧を小さくする → アバランシェ低減 → 捕獲電子数減少 → アフターパルス小

そのためには、SNの良い検出器構成

自己遅延法



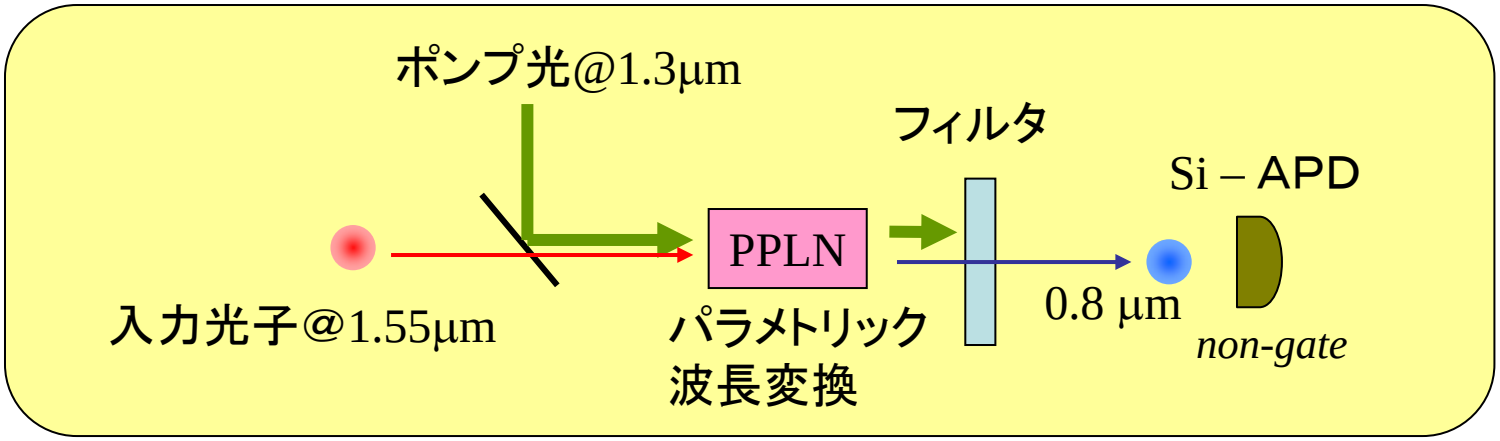
正弦波ゲート法



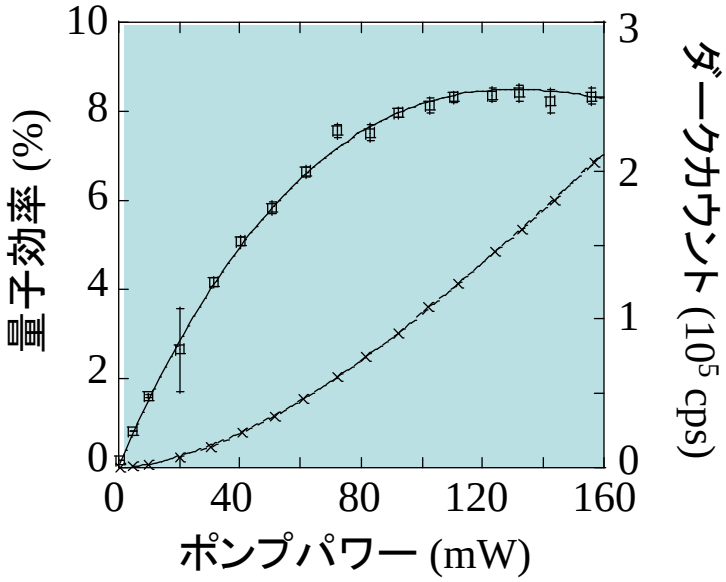
～ 1 GHz

波長変換型光子検出器

高性能なSi-APDを利用しよう → ゲート動作不要 → 高速化

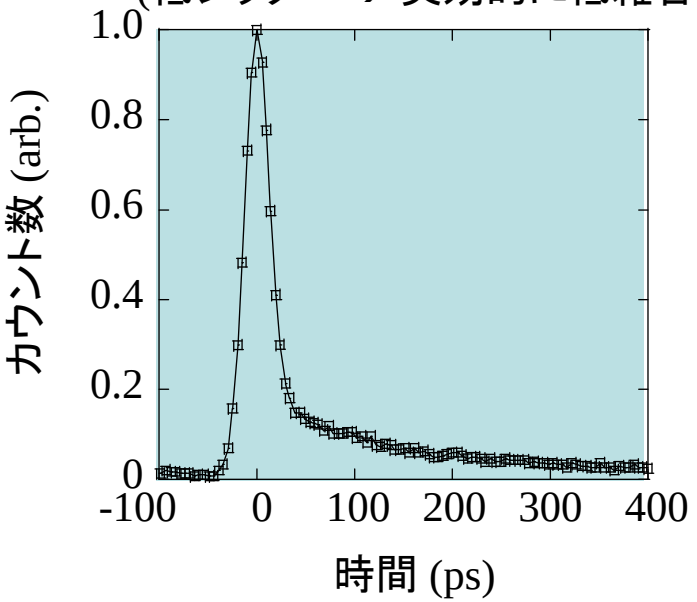


効率＆ダークカウント



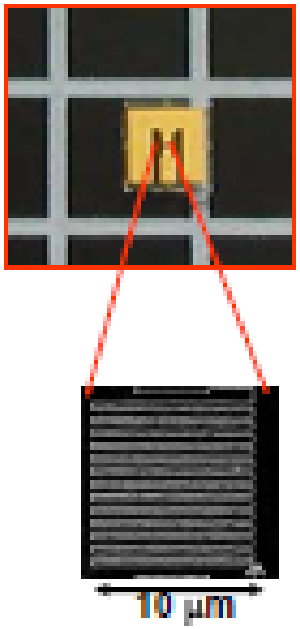
ジッター

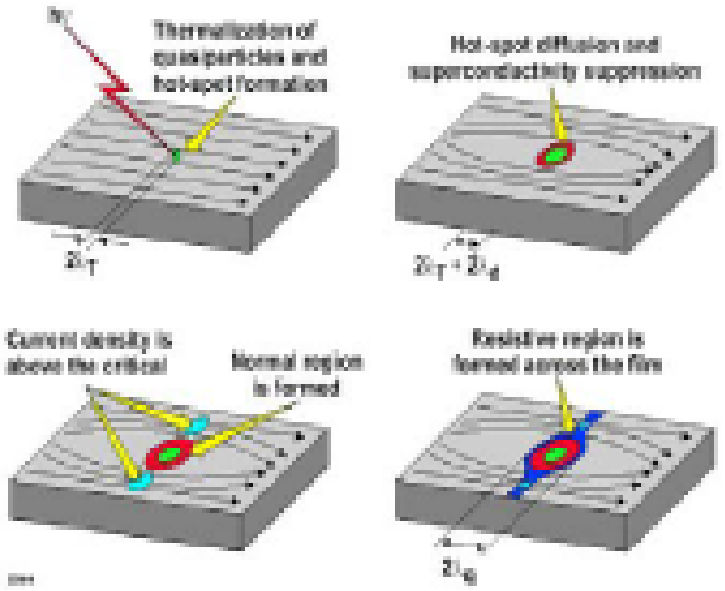
(低ジッター → 実効的に低雑音)



超伝導光子検出器

超伝導素子に光子入射 → 光子吸収 → 発熱 → 超伝導状態変化 → 出力信号

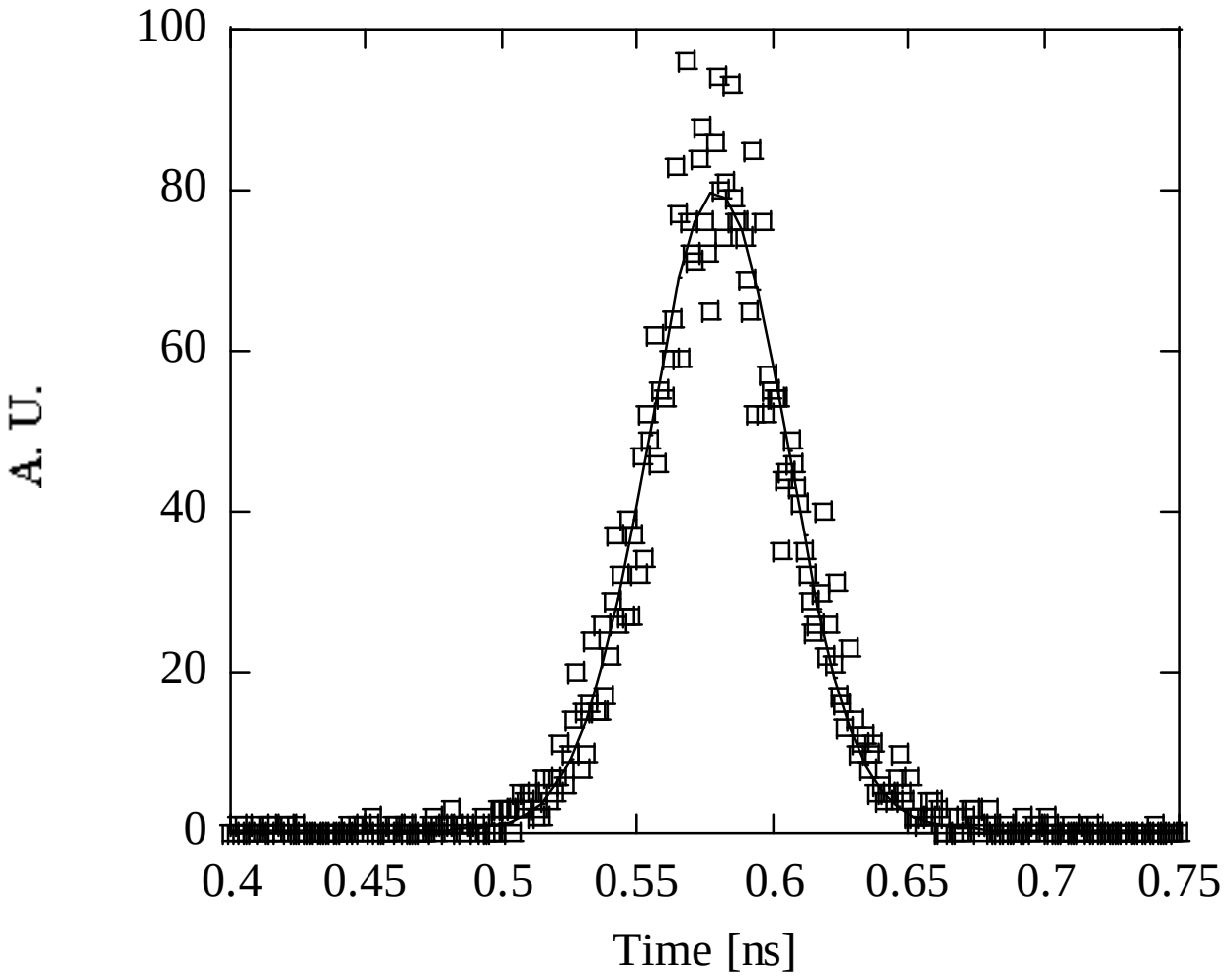




- Current Biased
- Recovery inductance limited
- Low jitter (10's ps)
- System Detection Efficiency

NIST

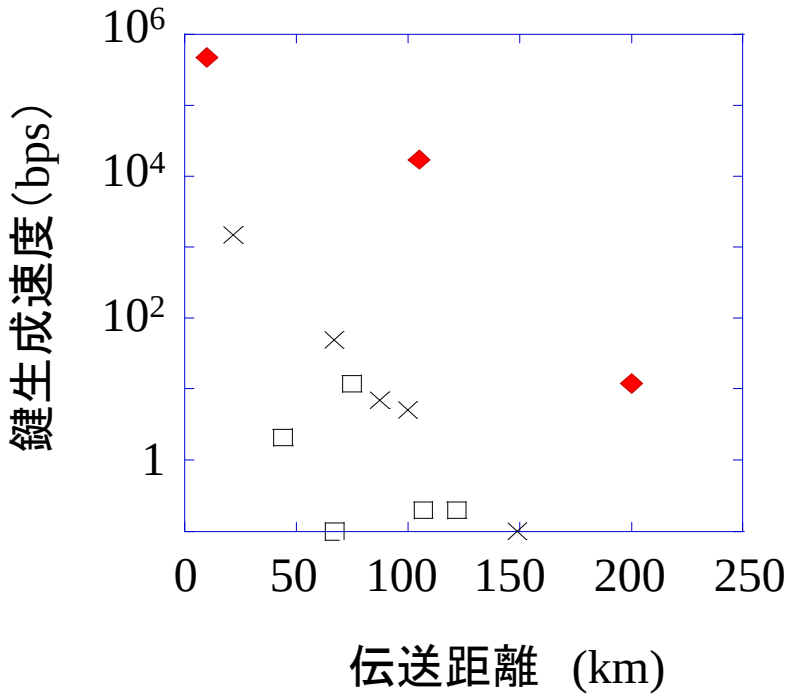
超伝導光子検出器特性例



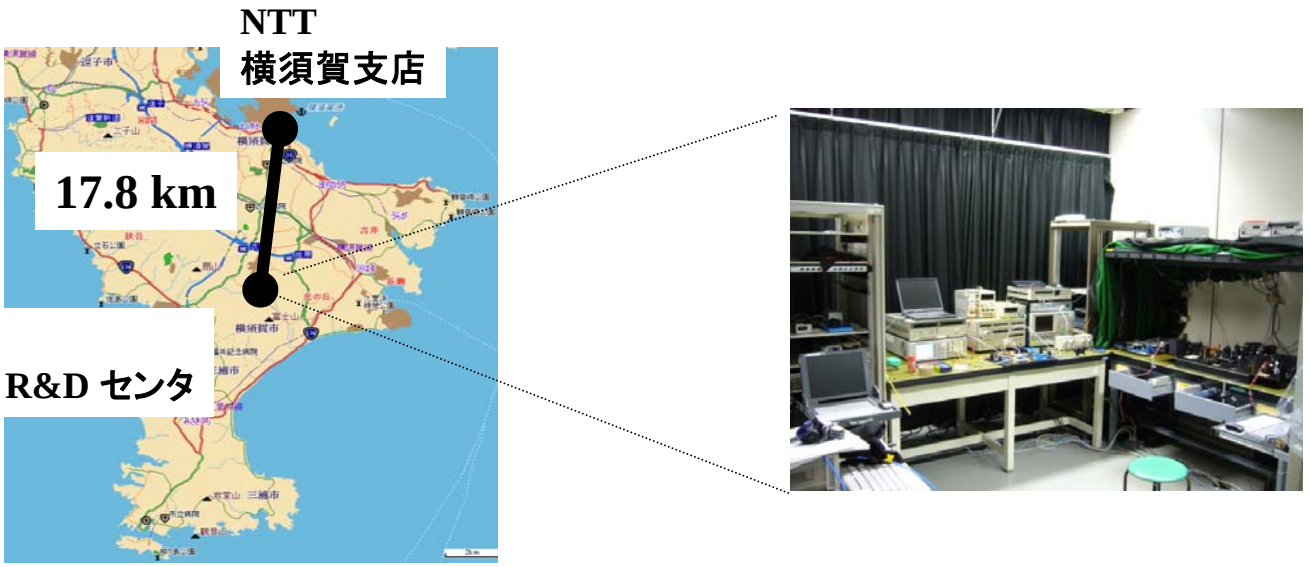
入力光: 10 ps pulse
時間分解能: 60 ps.

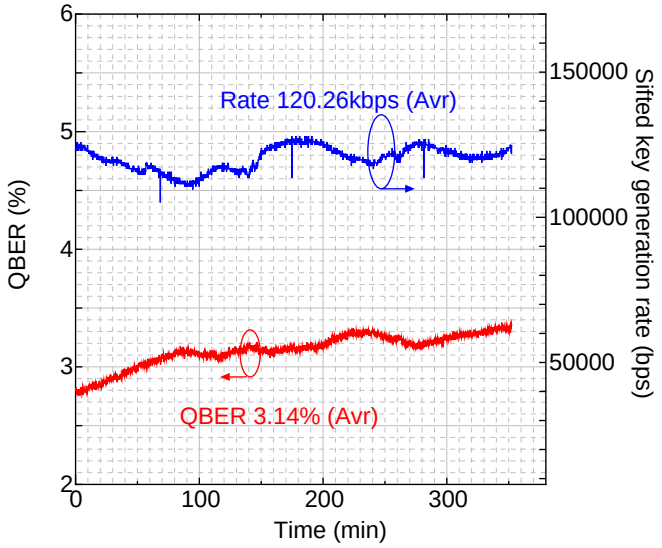
量子効率: 0.7%
ダークカウント: < 10 cps

量子鍵配送実験例



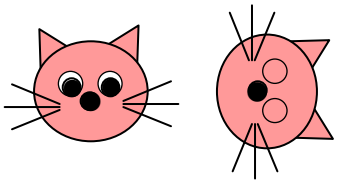
現場環境下実験


NTT
横須賀支店
17.8 km
NTT
横須賀 R&D センタ


Rate 120.26kbps (Avr)
QBER 3.14% (Avr)
QBER (%)
Sifted key generation rate (bps)
Time (min)
6
5
4
3
2
150000
100000
50000
0
100
200
300

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－

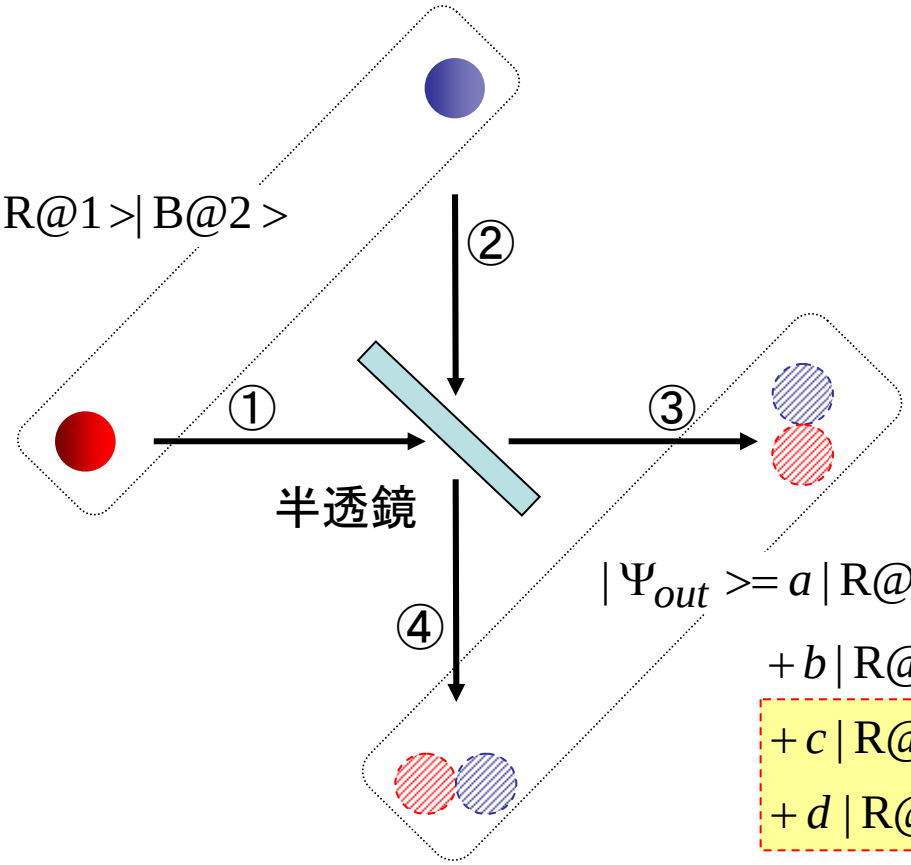


その前に

量子コンピューティングで利用する重ね合わせ
－量子もつれ－

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（product state）



複数量子の重ね合わせ状態

$|\Psi_{out}>= a\,|R@3>|B@3>$:2光子とも③へ

$+ b\,|R@4>|B@4>$: 2光子とも④へ

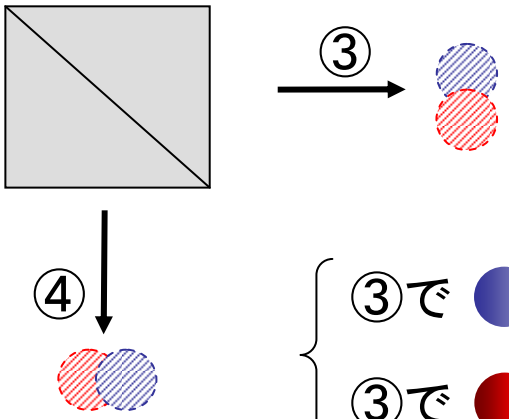
$+ c\,|R@3>|B@4>$: Redは③へ、Blueは④へ

$+ d\,|R@4>|B@3>$: 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

さらに

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●

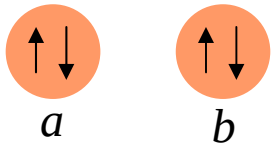
量子もつれ状態

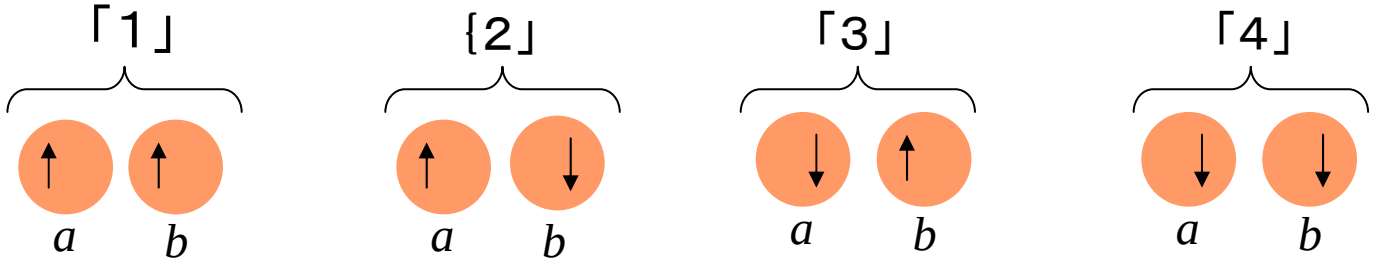
$$|\Psi> = c|● >_3|● >_4 + d|● >_3|● >_4$$

では量子コンピュータ

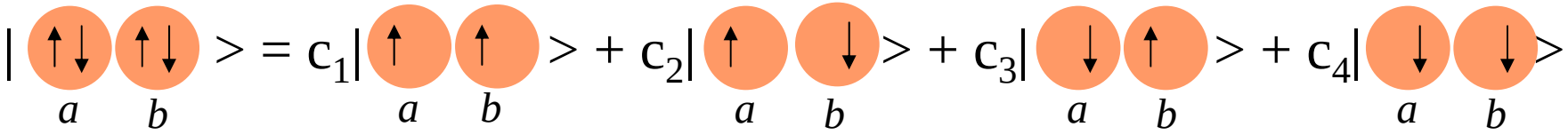
重ね合わせにより複数の数を同時に表現

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、



$= c_1「1」 + c_2「2」 + c_3「3」 + c_4「4」$

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

（古典）

x_1 x_2 x_3 ・・・ x_n

↓ ↓ ↓ ↓

$f(x_1)$ $f(x_2)$ $f(x_3)$ ・・・ $f(x_n)$

↓ ↓ ↓ ↓

a b c ・・・ z

（量子）

$|\phi> = |x_1> + |x_2> + |x_3> + \cdots + |x_n>$

↓

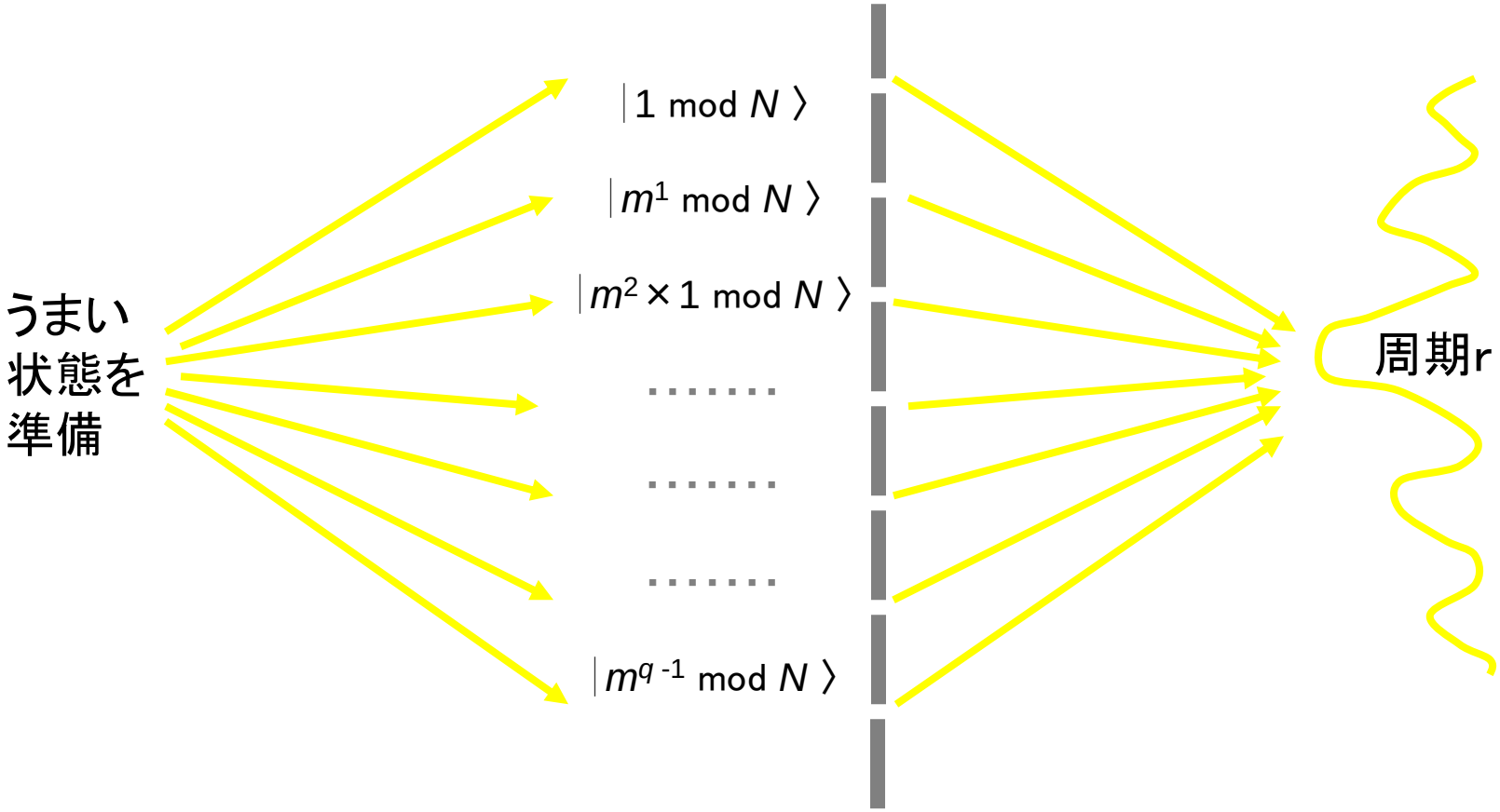
$U|\phi> = U|x_1> + U|x_2> + U|x_3> + \cdots + U|x_n>$

↓

$|\phi_{out}> = 0|x'_1> + 0|x'_2> + 1|x'_3> + \cdots + 0|x'_n>$

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

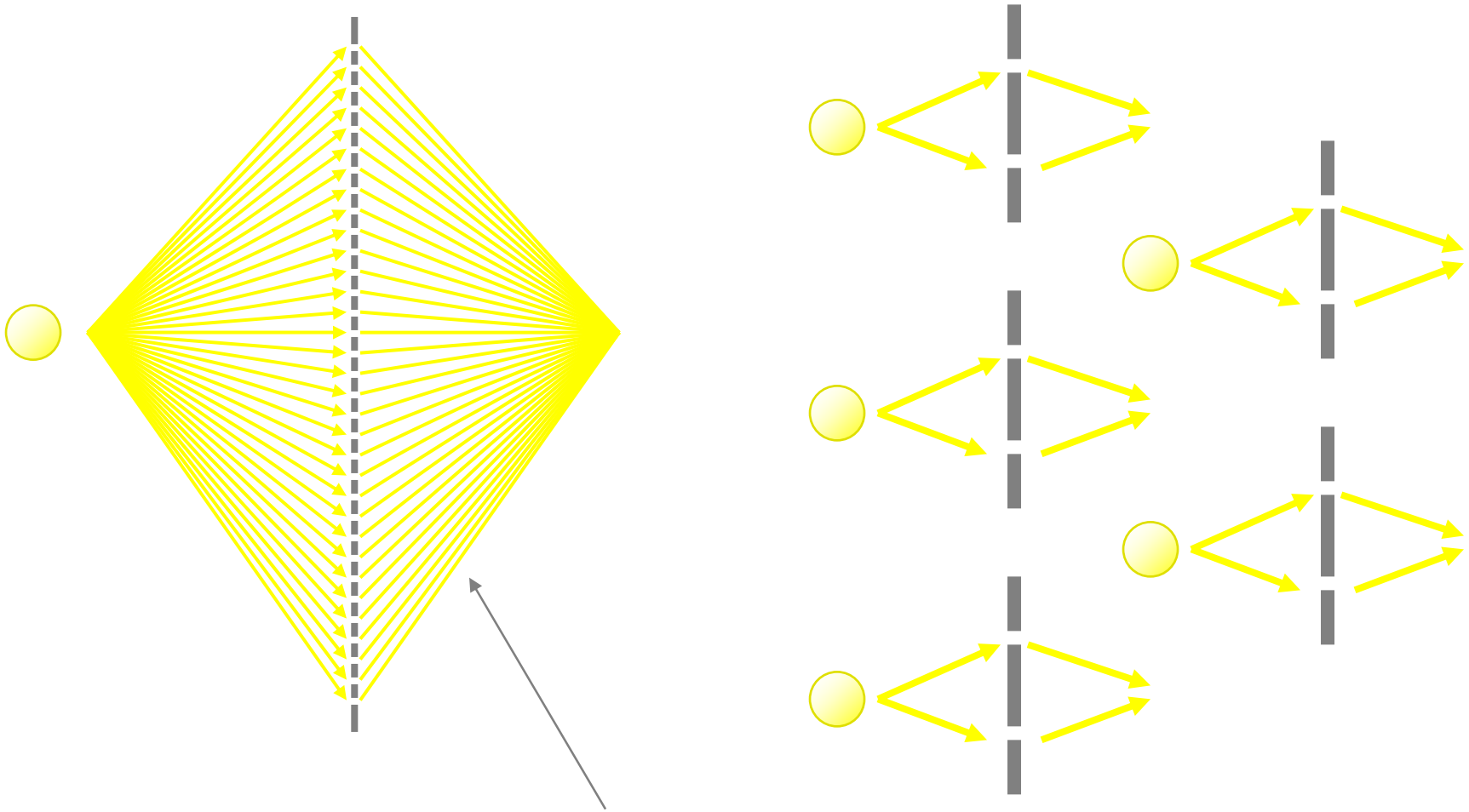


ここで疑問;

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）

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

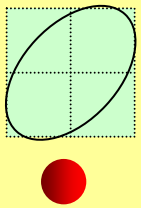
量子コンピュータまとめ

◆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

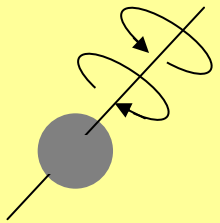
基本単位は量子ビット（Quantum bit: Qビット）

光子の偏波



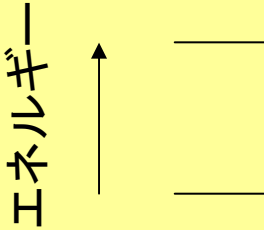
$|\psi\rangle = a|H\rangle + b|V\rangle$

スピン



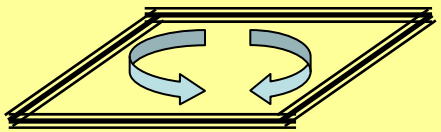
$|\psi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$

2つのエネルギー準位



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

超伝導電流



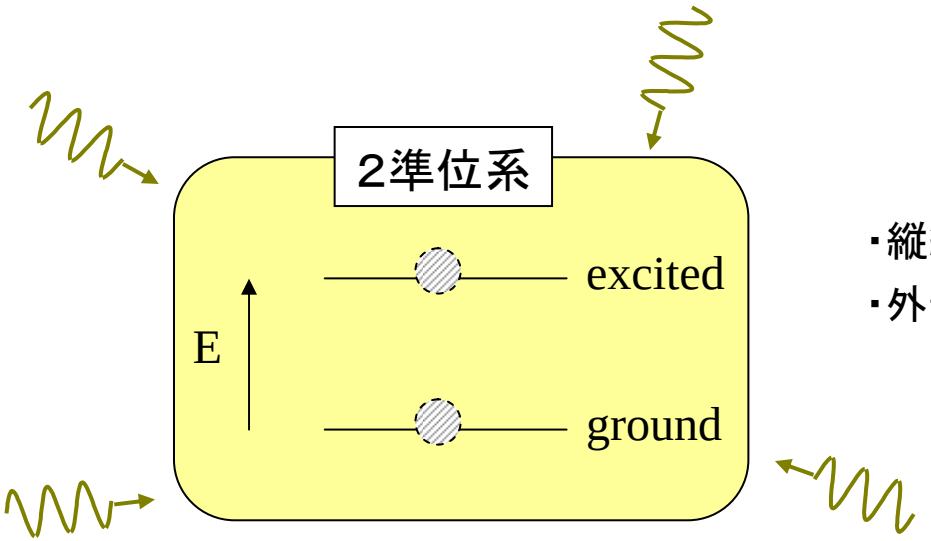
$|\psi\rangle = a|R\rangle + b|L\rangle$

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

量子情報通信の話

- 量子力学と情報通信の融合 -

[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

　　量子力学的に安全性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

（HP:「大阪大学　井上恭　講義ノート」で検索し、「Inoue Lab. –Members-」をクリック）