光通信研究者からみた量子暗号

大阪大学工学研究科

井上　恭

量子暗号で使われる量子力学

○物理的な状態は、複素ベクトル空間（ヒルベルト空間）上の状態ベクトルで表わされる。

$|\alpha\rangle$　　（ケット）

○物理的な観測量（observable）はエルミート演算子Aで表わされる。

○Aに対応する固有ケットが存在する：$A|\phi_i\rangle = a|\phi_i\rangle$　　⇒　　$|\phi_i\rangle$：固有状態＝基底状態

○任意の物理状態は基底状態で展開できる。

$|\alpha\rangle = \Sigma c_i|\phi_i\rangle$

○観測すると、系は観測された物理量の一つの基底状態に跳び移る。

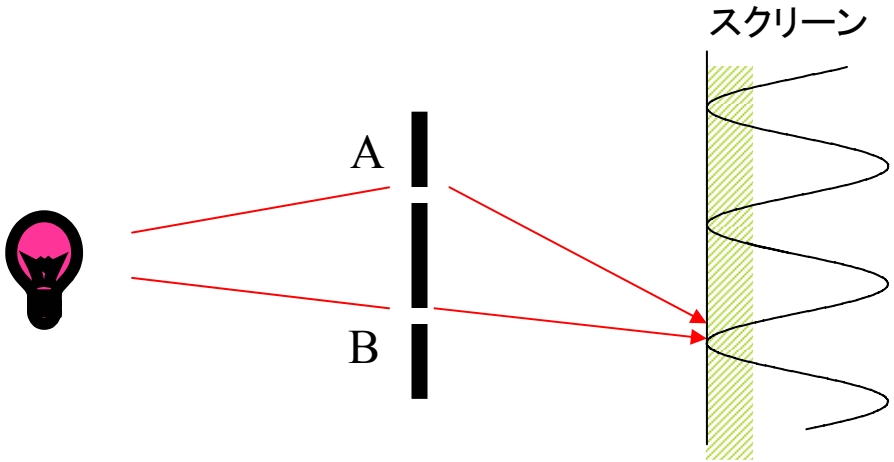
跳び移る確率は展開係数の絶対値二乗

（元の系が基底状態であれば不変）

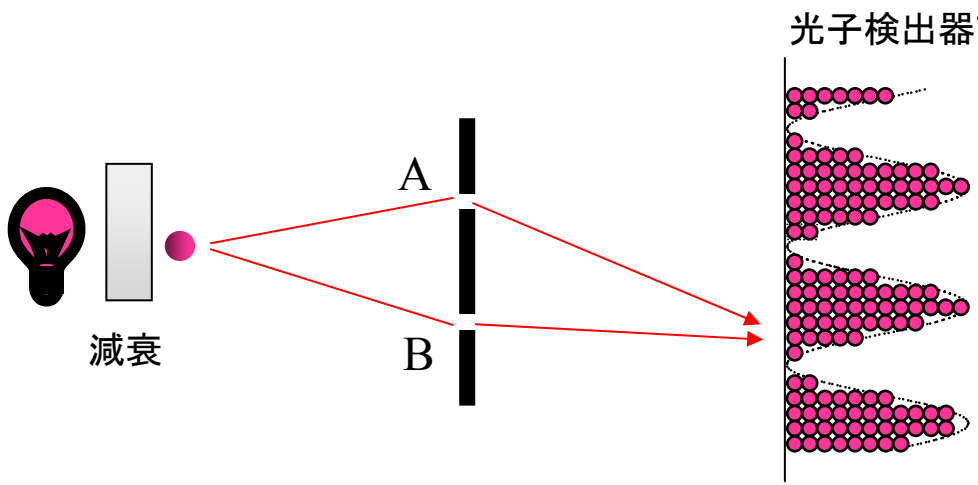
$|\alpha\rangle : \Sigma c_i|\phi_i\rangle$　— 観測 →　$|\phi_i\rangle$　　with $|c_i|^2$

○非直交状態（$\langle\phi|\psi\rangle \neq 0$）は同時観測不可

ヤングの干渉実験



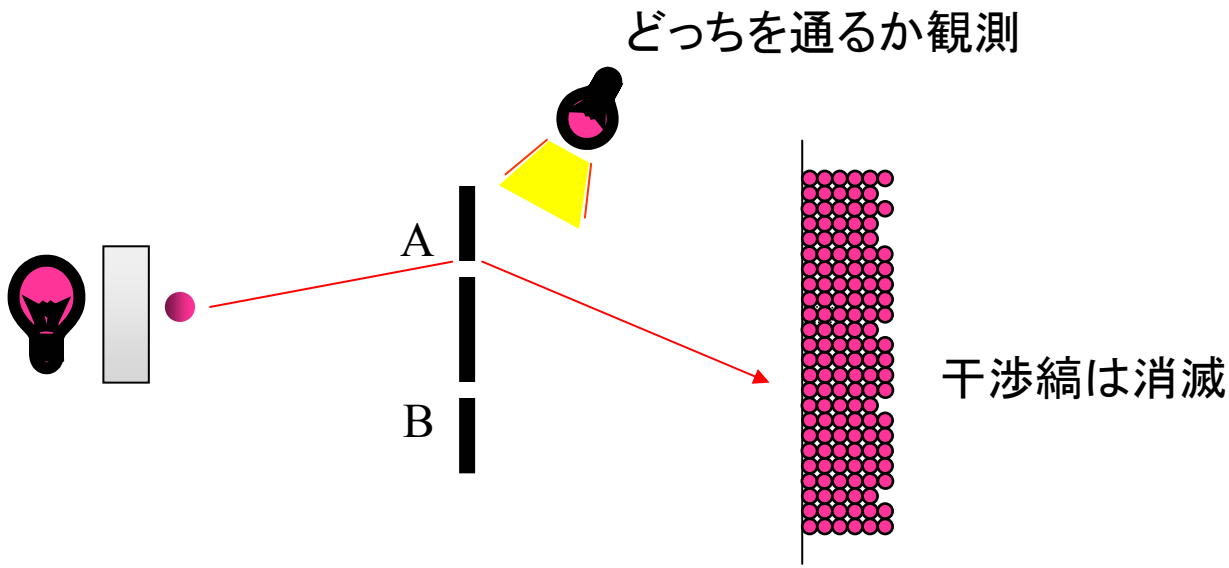
$$E = a\mathrm{e}^{ikL_\mathrm{a}} + b\mathrm{e}^{ikL_\mathrm{b}}$$



$$|\psi\rangle = a\mathrm{e}^{ikL_\mathrm{a}}|\mathrm{a}\rangle + b\mathrm{e}^{ikL_\mathrm{b}}|\mathrm{b}\rangle$$

|a>: 光子がAを通った状態

|b>: 光子がBを通った状態

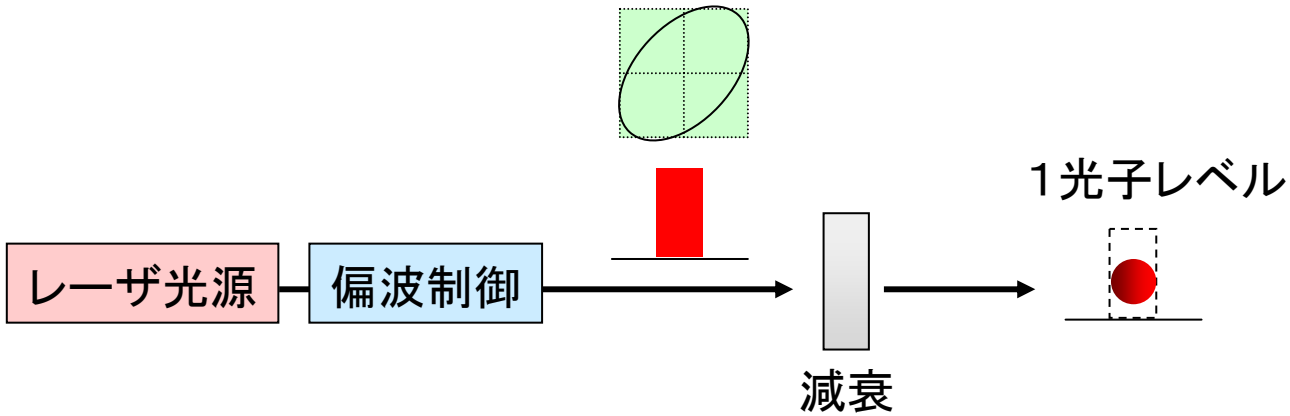


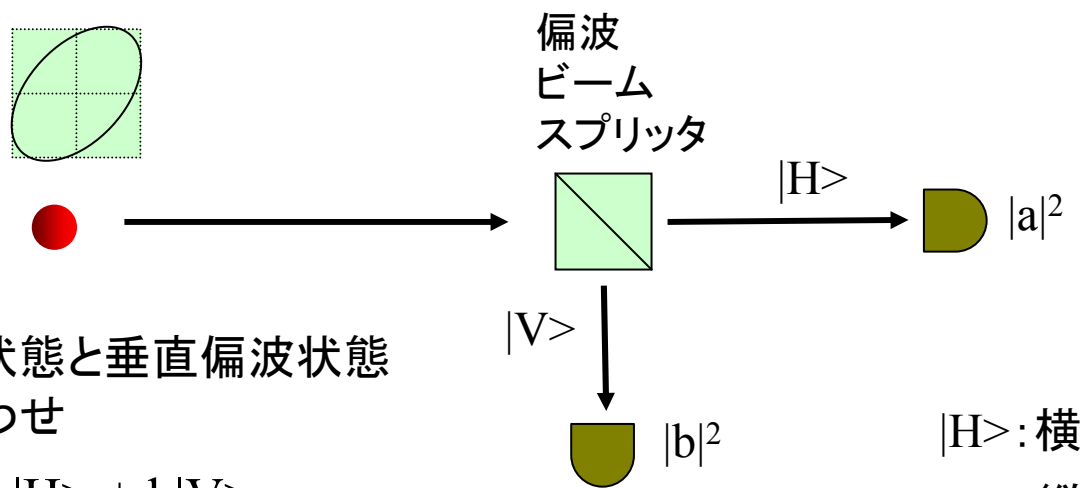
観測により量子状態は変化

⇩

量子暗号

光子の偏波の場合





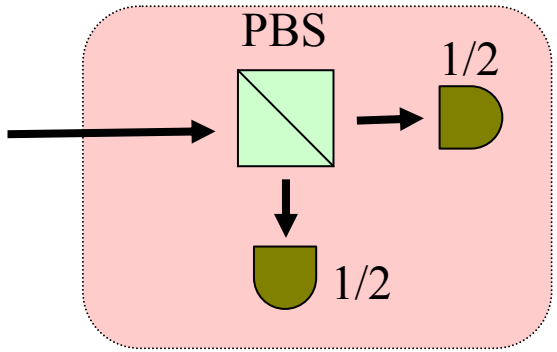
水平偏波状態と垂直偏波状態の重ね合わせ

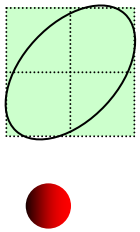
$$|\psi\rangle = a|H\rangle + b|V\rangle$$

$|H\rangle$：横偏波光子状態

$|V\rangle$：縦偏波光子状態

{H, V}基底

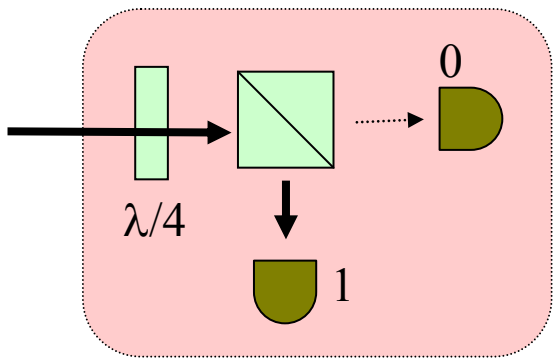




$|\psi> = a|H> + b|V>$

$$= \frac{1}{\sqrt{2}}\{(a - ib)|R> + (a + ib)|L>\}$$

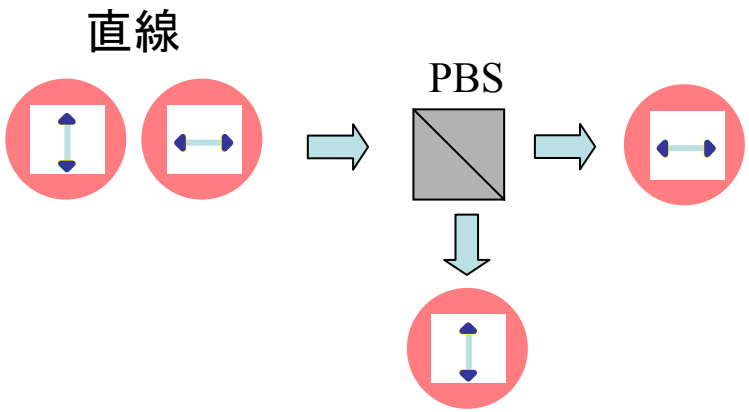
{R, L}基底

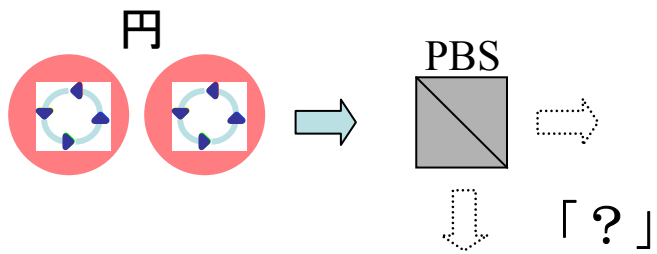


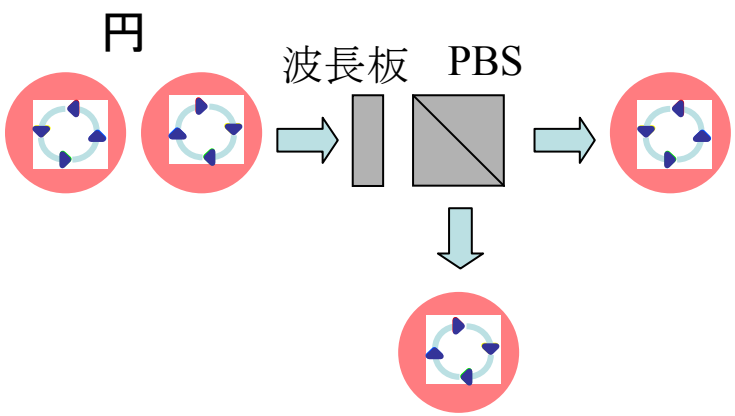
$$|R> = \frac{1}{\sqrt{2}}(|H> + i|V>)$$: 右回り円偏波光子状態

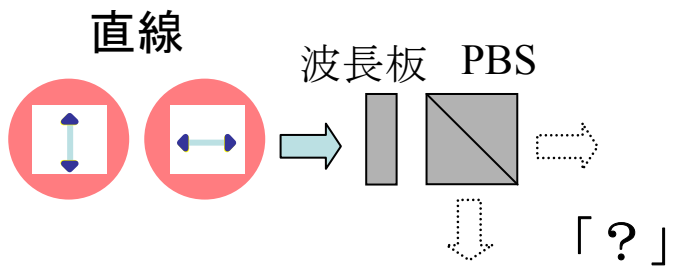
$$|L> = \frac{1}{\sqrt{2}}(|H> - i|V>)$$: 左回り円偏波光子状態

状態と観測基底



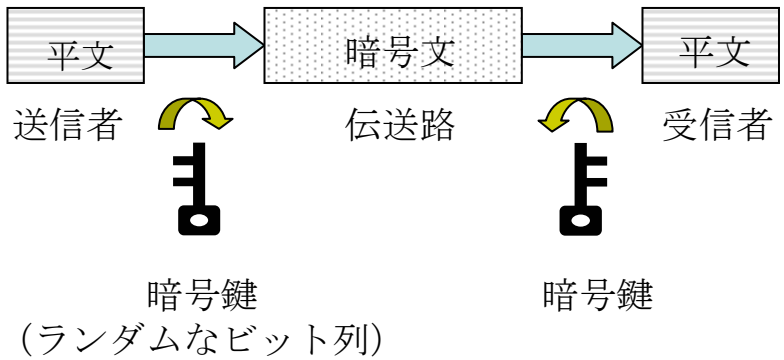






量子暗号（量子鍵配送）

（秘密鍵暗号通信）



目的

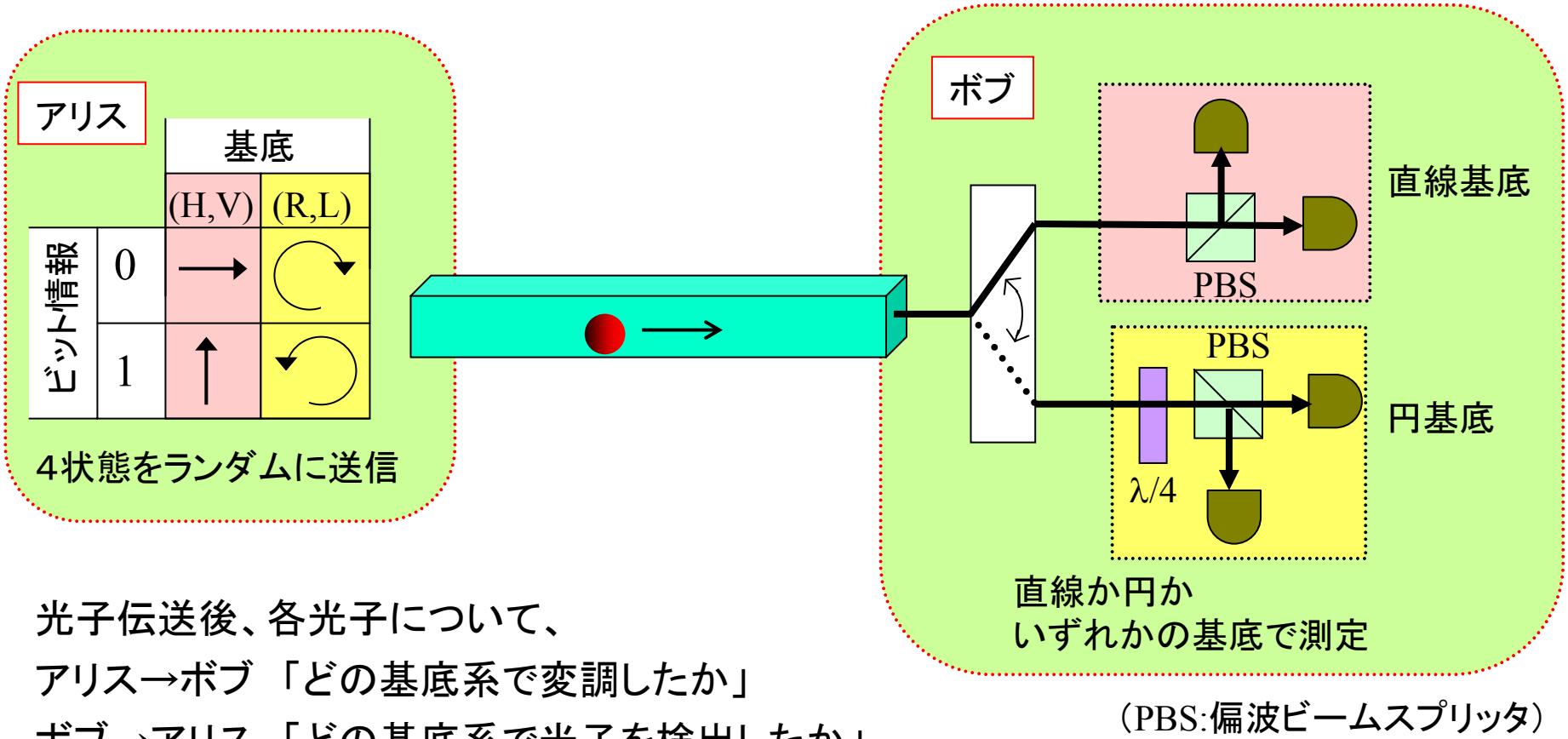
量子力学的に秘匿性が保証された秘密鍵を離れた2者に供給

売り文句

どんな技術革新があっても絶対に大丈夫

（盗聴者は物理法則に反しない限り、いかなる手段も取り得る。）

BB84量子鍵配送方式



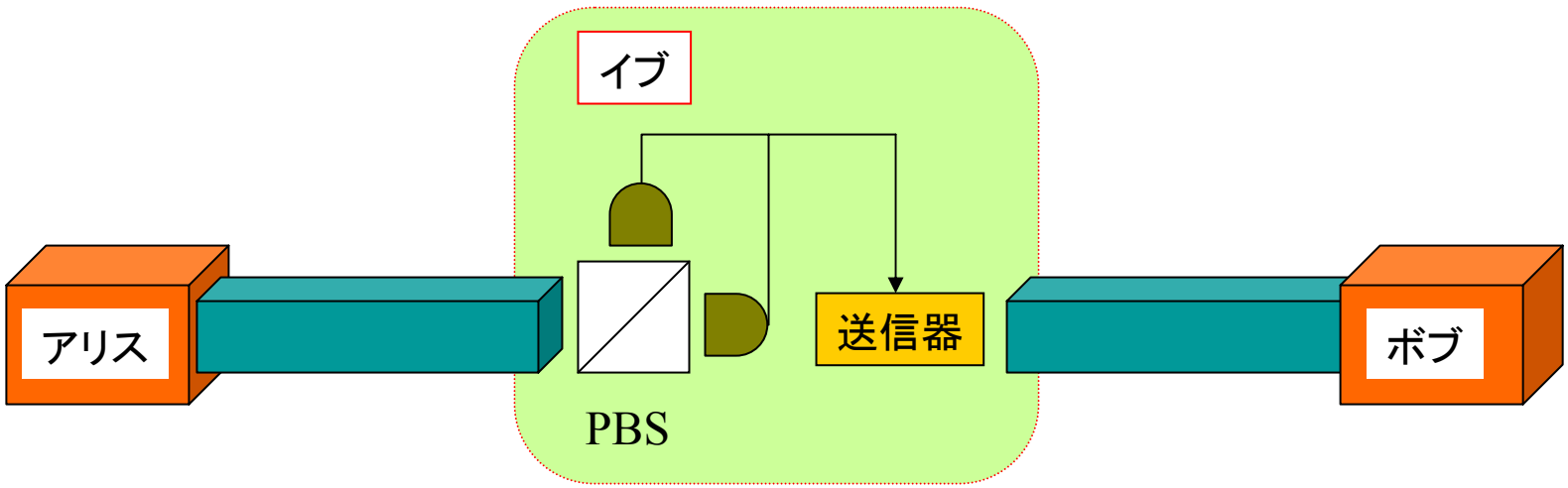
光子伝送後、各光子について、
アリス→ボブ 「どの基底系で変調したか」
ボブ→アリス 「どの基底系で光子を検出したか」

（PBS:偏波ビームスプリッタ）

基底の一致していればアリスとボブで同じビット情報 → 秘密鍵ビット
基底不一致の場合は廃棄

安全性

盗聴者（イブ）が、
伝送路を切断→伝送信号を受信→受信結果に基づいてダミー信号を送信
しようとすると、

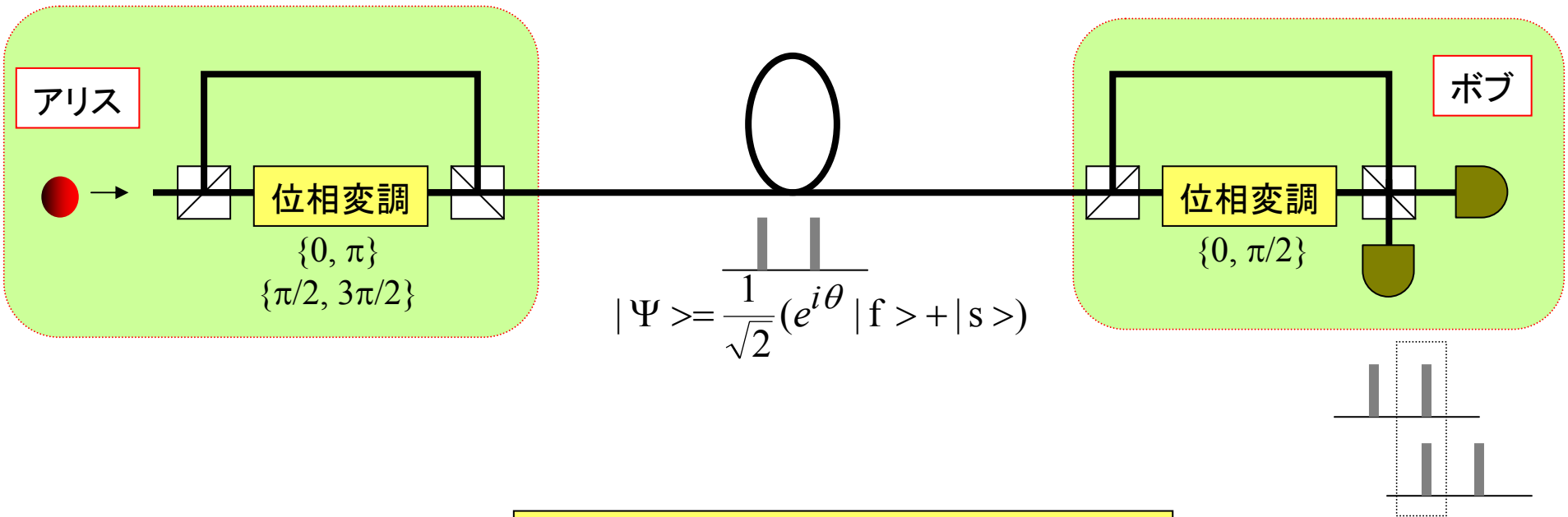


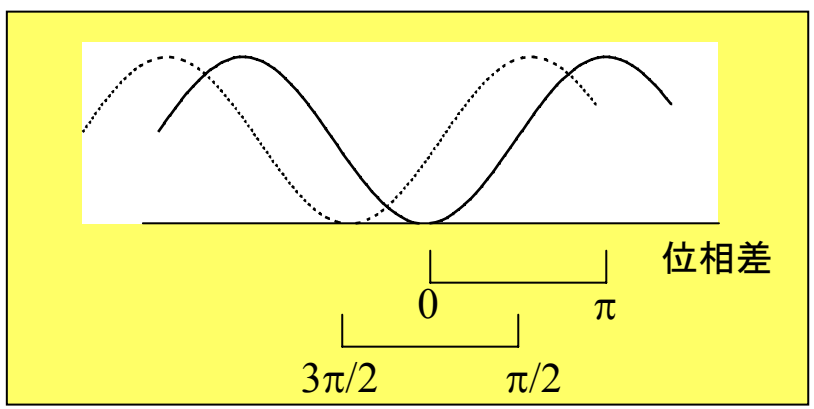
イブの測定基底がアリスの変調基底に
一致の場合 → 盗聴成功
不一致の場合 → 1/2の確率で誤り → テストビットチェックにより盗聴発覚

位相エンコードBB84

直線偏波・円偏波変調は直交2成分の位相差を$\{0, \pi/2, \pi, 3\pi/2\}$とするのと同等

偏波変調を2パルス間の位相差変調に置き換え





要するに、、、、

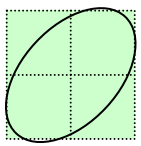
光子は1回しか測定できない

1回で測定できるのはひとつの観測量（パラメータ）のみ

↓

1回では測定できないパラメータに情報を載せれば、100%の盗聴は不可

偏波



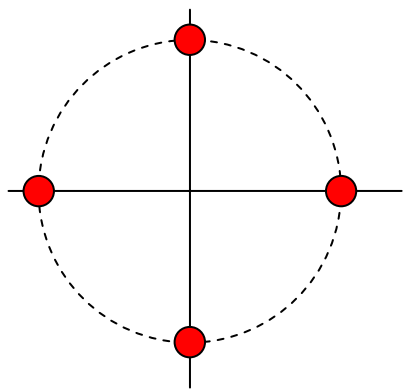
パラメータは、

縦横成分比＆その相対位相

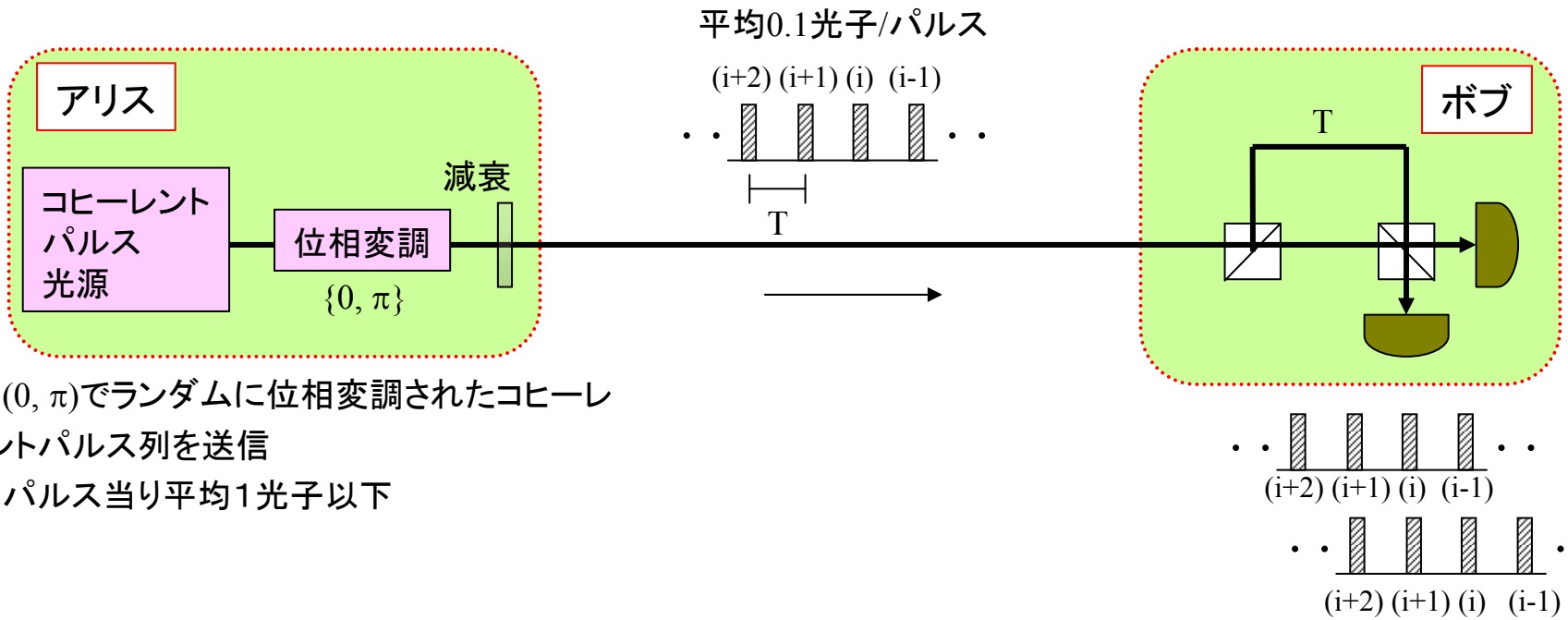
or

ポワンカレ球上の緯度＆経度

位相



差動位相シフト量子鍵配送方式
（DPS－QKD：Differential Phase Shift QKD)



・(0, π)でランダムに位相変調されたコヒーレントパルス列を送信

・パルス当り平均1光子以下

・前後のパルスの位相差が、
　0 → 検出器1、 π → 検出器2

・光子が受かるのは稀

鍵生成手順

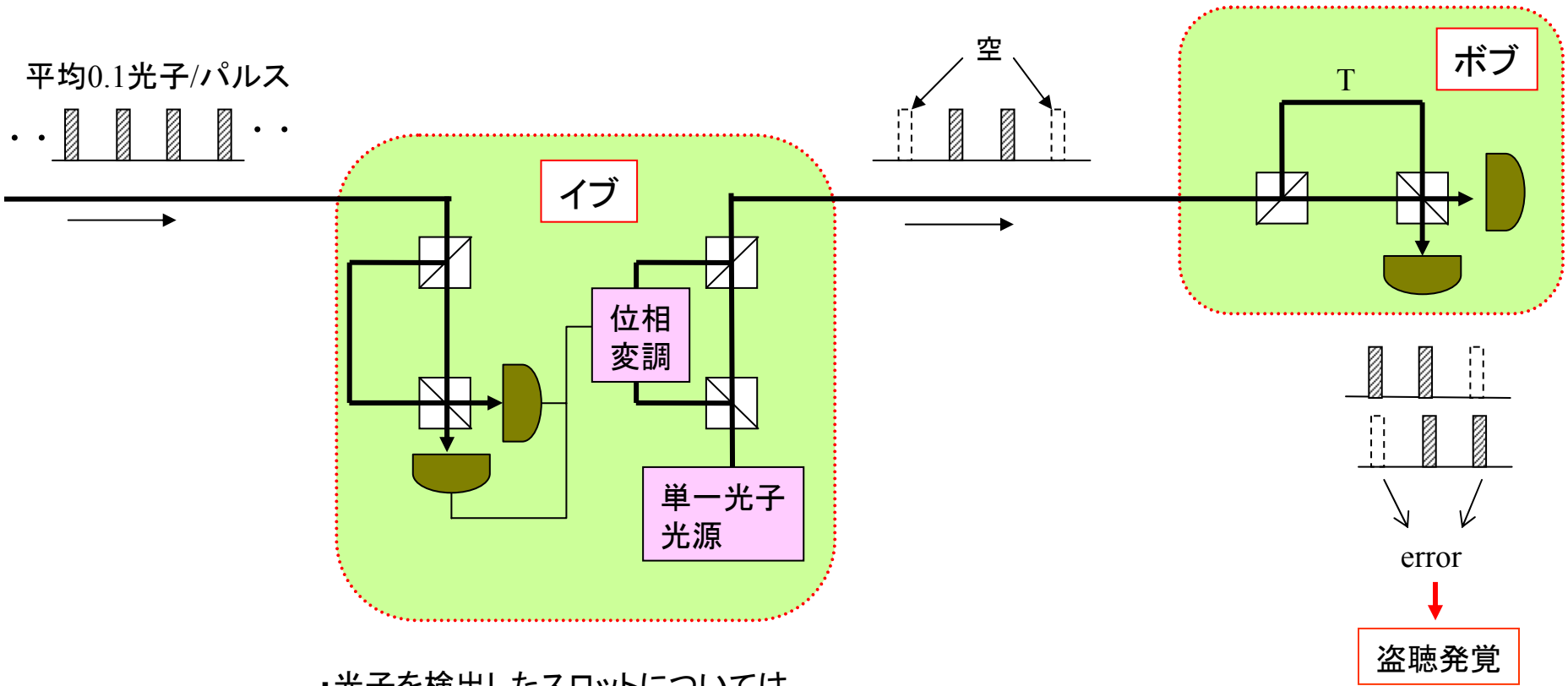
①ボブ：光子を検出した時刻と検出器を記録

②ボブ→アリス：光子検出時刻を通知

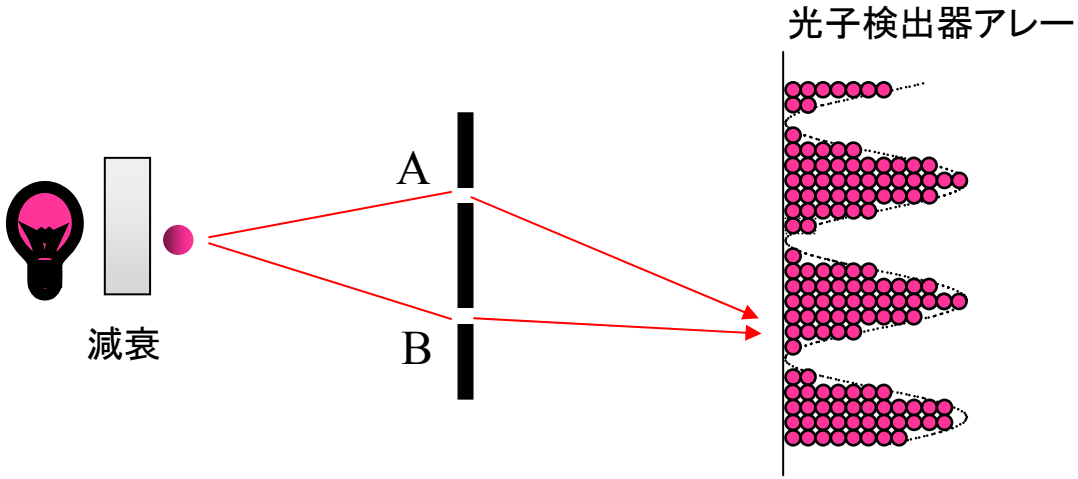
③アリス：自分の変調データから光子検出した検出器を特定

④検出器1＝「0」、検出器2＝「1」とすればアリスとボブで同じビット列 → 秘密鍵

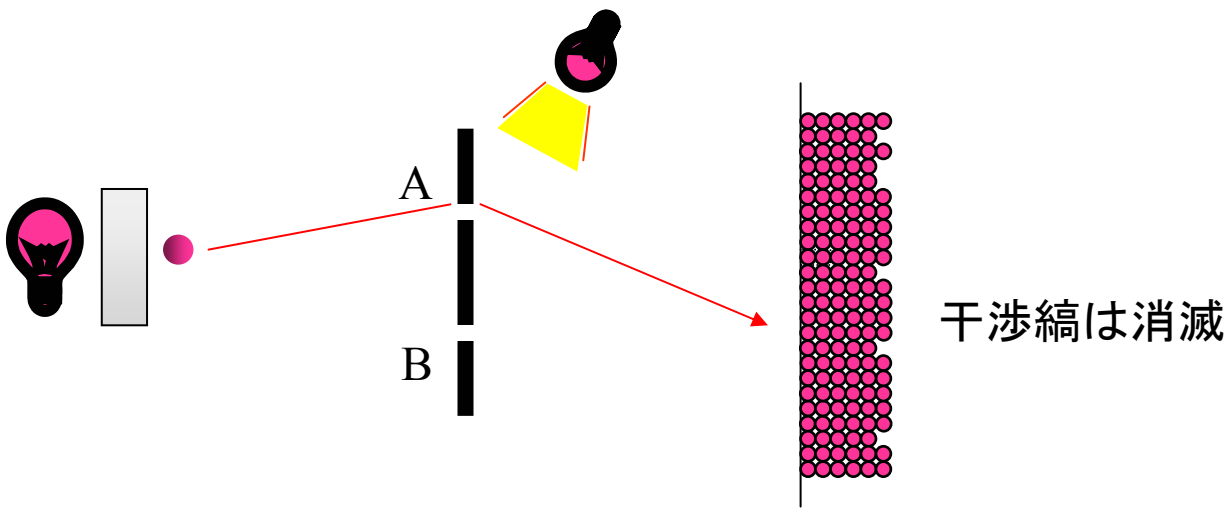
DPS-QKDに対する盗聴：intercept/resend攻撃



・光子を検出したスロットについては、
　単一光子を2連続パルスにして送信
・検出しないスロットは、何も送らない



どっちを通るか観測



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

どんな技術革新があっても絶対に大丈夫；究極の安全性を保証

||

盗聴者は物理法則に反しない限り、いかなる手段も取り得る。

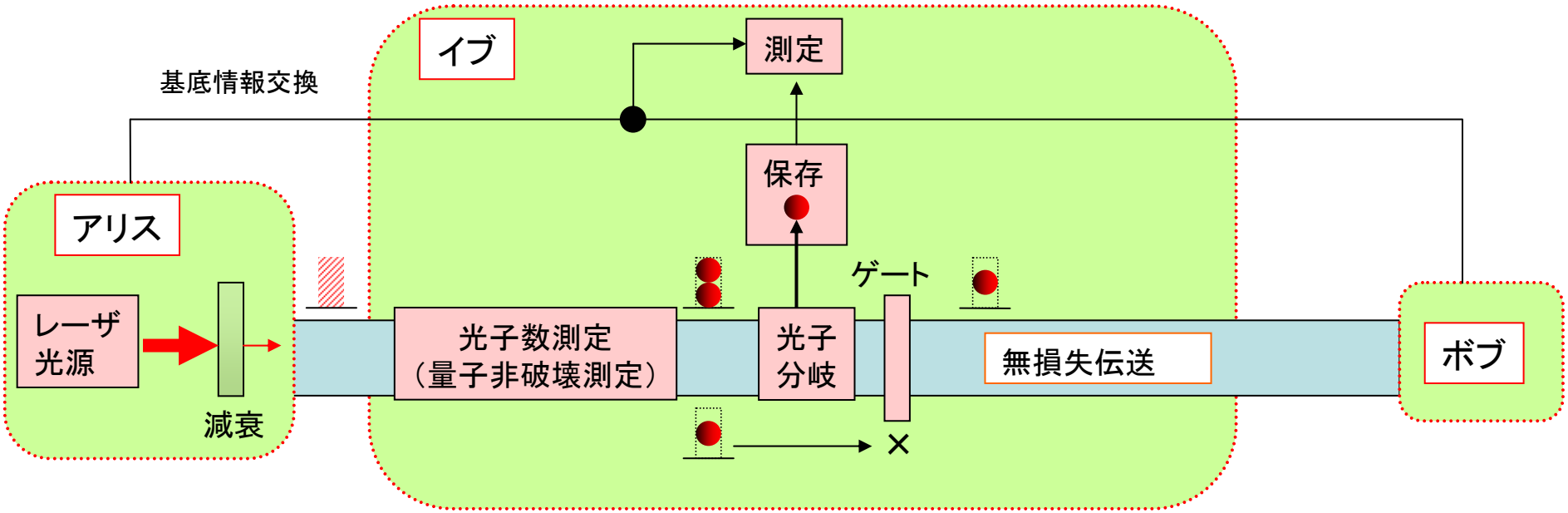
Intercept/resend攻撃（なりすまし盗聴）

①盗聴者は伝送路を遮断

②伝送信号を受信

③受信結果に基づいてダミー信号を送信

光子数分岐攻撃（Photon number splitting attack）



①光子数を非破壊で測定する

②2光子あるパルスから1光子だけ分岐する

③分岐した光子を保存する

④残りの光子は無損失伝送路でボブへ送る

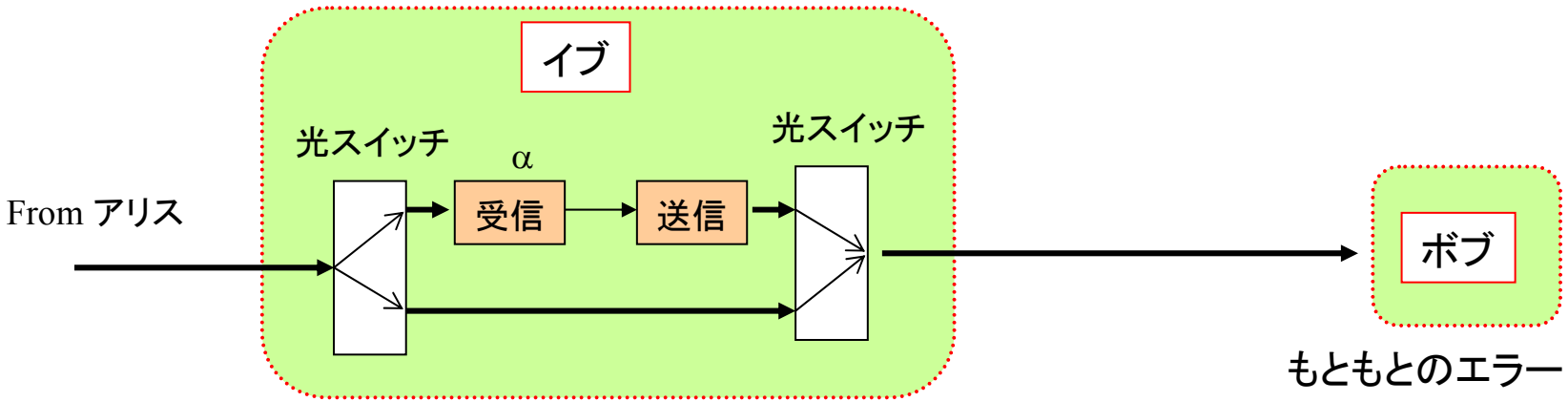
⑤1光子/パルスの場合は、せき止める

⑥アリス-ボブの基底情報を盗み聞く

⑦基底情報に基づいて保存しておいた光子を測定する

部分intercept/resend攻撃

アリス/ボブの送受信系に装置の不完全性（e.g., 信号消光比、PBS or 干渉計消光比、雑音）によるビット誤りがあると、それにイブはそれに紛れて一部盗聴可能



もともとのエラー：e

盗聴によるエラー：α/4

↓

α/4 << e だとα分は盗聴成功

⇩

最悪値として、α/4 = eとする

||

α = 4eの情報はイブに漏洩

イブは不完全な送受信系を完全なものに置き換えられる

さいごに

Q. 量子暗号は実用になるか？

A. 技術的に可能かという意味でなら可能性あり

売り物になるかという意味では「？」

今だかつて光伝送路信号を盗聴されたという話は聞いたことがない

Q. なぜ研究しているの？

A1. ひょっとしたら実用になるかもしれない。

A2. 量子暗号自体はものにならなくても、何かしらの副産物が出てくるかもしれない。

A3. 量子力学に基づき究極的な安全な暗号通信を実現、というと世間に受ける

A4. （実際の必要性はともかく）量子暗号を使っているから絶対安全、

というイメージで商売になるかもしれない。

A5. 究極的なものを純粋に追い求める理学的探究心。

A6. 論文が書ける。

A7. 知的ゲームとして面白い。

A8. 量子現象（e.g.,光子の干渉）が実際に起こる不思議さ、それを応用する面白さ。