Quantum Cryptography Using Any Two Nonorthogonal States

2つの互いに非直交な状態を用いた量子暗号

Charles H. Bennett.
Physical Review Letters
68, 3121 (1992).

平野研究室 11-041-020 河野　かおり

概要

任意の2つの互いに非直交な状態を用いて
量子鍵配送を行う
B92プロトコルの紹介をする

発表の流れ

1．B92プロトコルとは
- 秘密鍵を用いた通信について
- B92プロトコルの鍵の共有方法
- 単一光子の偏光状態を用いたB92プロトコル
- B92プロトコルの鍵の共有方法（具体例）

2．B92プロトコルの安全性
- Bobに届く状態が変化しない場合
- 通信路に損失がある場合

3．参照光を用いたB92プロトコル
- 微弱レーザー光と参照光を送信する方法
- なりすまし攻撃に対する安全性

4．まとめ

発表の流れ

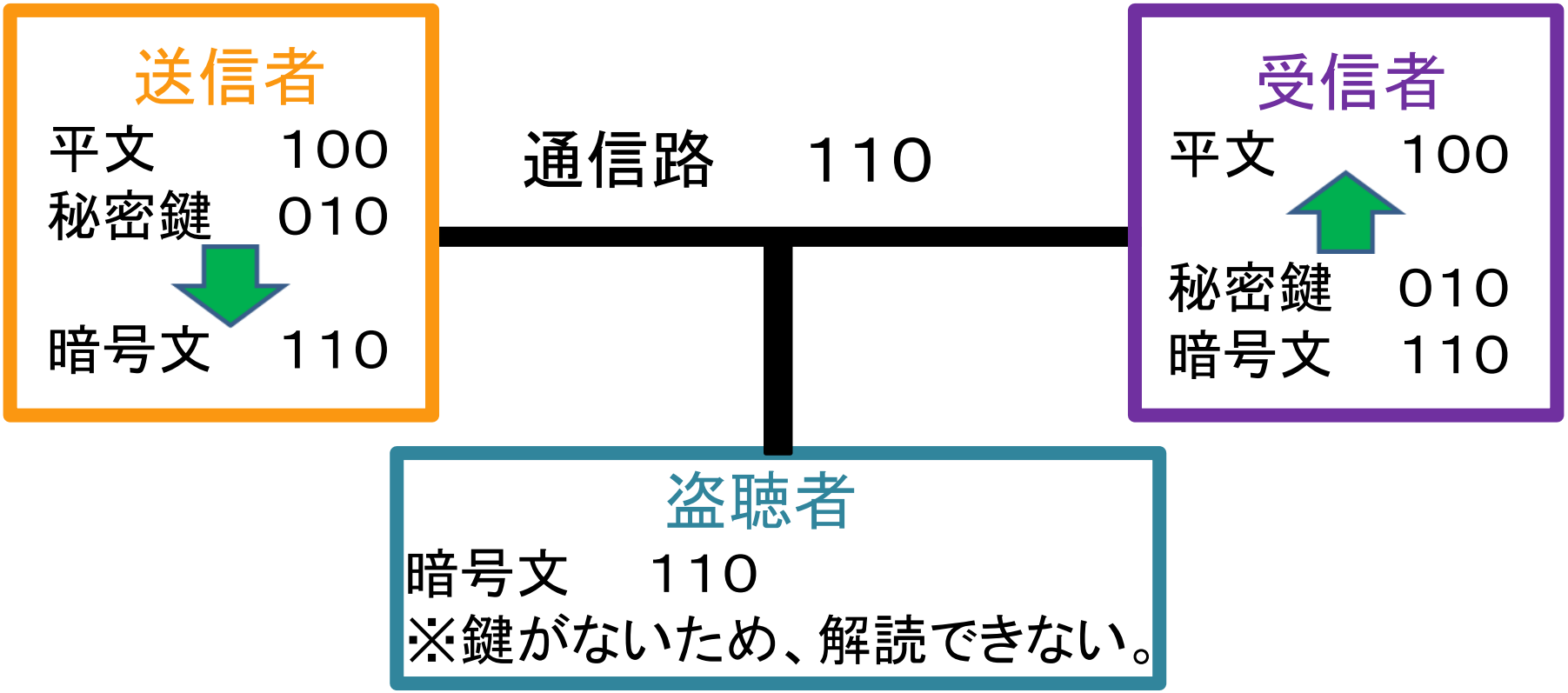
1．B92プロトコルとは
- 秘密鍵を用いた通信について
- B92プロトコルの鍵の共有方法
- 単一光子の偏光状態を用いたB92プロトコル
- B92プロトコルの鍵の共有方法（具体例）

2．B92プロトコルの安全性
- Bobに届く状態が変化しない場合
- 通信路に損失がある場合

3．参照光を用いたB92プロトコル
- 微弱レーザー光と参照光を送信する方法
- なりすまし攻撃に対する安全性

4．まとめ

秘密鍵を用いた通信について



送信者と受信者だけが、鍵を持つと安全な通信を行うことができる。

秘密鍵の共有を実現する方法.....量子鍵配送

発表の流れ

1．B92プロトコルとは
- 秘密鍵を用いた通信について
- B92プロトコルの鍵の共有方法
- 単一光子の偏光状態を用いたB92プロトコル
- B92プロトコルの鍵の共有方法（具体例）

2．B92プロトコルの安全性
- Bobに届く状態が変化しない場合
- 通信路に損失がある場合

3．参照光を用いたB92プロトコル
- 微弱レーザー光と参照光を送信する方法
- なりすまし攻撃に対する安全性

4．まとめ

B92プロトコルの鍵の共有方法

2つの互いに非直交な状態を送信し、2つの方法で測定することで
鍵となるビット値を共有する

①2つの互いに非直交な状態を送信する

送信者 Alice

$|u_0\rangle$ ビット値 0

$|u_1\rangle$ ビット値 1

受信者 Bob

P_0=1-$|u_1\rangle\langle u_1|$ ビット値 0

P_1=1-$|u_0\rangle\langle u_0|$ ビット値 1

非直交状態だと、

$\langle u_0|u_1\rangle = r \neq 0$

②2つの方法を用いて測定する

③検出された場合をAliceに伝える

④どのビット値がBobに検出されたか分かる

AliceとBobでビット値を共有できる

AliceとBobが同じビット値を共有できる

Aliceが送信する状態

$\|u_0\rangle \rightarrow P_0$	$\langle u_0\|P_0\|u_0\rangle$=1-$\|r\|^2$	1-$\|r\|^2$の確率で検出される
$\|u_0\rangle \rightarrow P_1$	$\langle u_0\|P_1\|u_0\rangle$=0	検出されない
$\|u_1\rangle \rightarrow P_0$	$\langle u_1\|P_0\|u_1\rangle$=0	検出されない
$\|u_1\rangle \rightarrow P_1$	$\langle u_1\|P_1\|u_1\rangle$=1-$\|r\|^2$	1-$\|r\|^2$の確率で検出される

Bobの測定方法

P_0=1-$|u_1\rangle\langle u_1|$

P_1=1-$|u_0\rangle\langle u_0|$

- ビット値が一致しない時　→　検出されない
- ビット値が一致する時　→　1-$|r|^2$の確率で検出される

AliceとBobが同じビット値を共有できる

Aliceが送信する状態

$\|u_0\rangle \to P_0$	$\langle u_0\|P_0\|u_0\rangle$=1-$\|r\|^2$	1-$\|r\|^2$の確率で検出される
$\|u_0\rangle \to P_1$	$\langle u_0\|P_1\|u_0\rangle$=0	検出されない
$\|u_1\rangle \to P_0$	$\langle u_1\|P_0\|u_1\rangle$=0	検出されない
$\|u_1\rangle \to P_1$	$\langle u_1\|P_1\|u_1\rangle$=1-$\|r\|^2$	1-$\|r\|^2$の確率で検出される

Bobの測定方法

P_0=1-$|u_1\rangle\langle u_1|$

P_1=1-$|u_0\rangle\langle u_0|$

$$\begin{aligned}\langle u_0|P_0|u_0\rangle &= \langle u_0|(1-|u_1\rangle\langle u_1|)|u_0\rangle \\ &= \langle u_0|u_0\rangle - \langle u_0|u_1\rangle\langle u_0|u_1\rangle \\ &= 1-|\langle u_0|u_1\rangle|^2 \\ &= 1-|r|^2\end{aligned}$$

- ビット値が一致しない時 → 検出されない
- ビット値が一致する時 → 1-$|r|^2$の確率で検出される

AliceとBobが同じビット値を共有できる

Aliceが送信する状態

$\|u_0\rangle \to P_0$	$\langle u_0\|P_0\|u_0\rangle = 1-\|r\|^2$	$1-\|r\|^2$の確率で検出される
$\|u_0\rangle \to P_1$	$\langle u_0\|P_1\|u_0\rangle = 0$	検出されない
$\|u_1\rangle \to P_0$	$\langle u_1\|P_0\|u_1\rangle = 0$	検出されない
$\|u_1\rangle \to P_1$	$\langle u_1\|P_1\|u_1\rangle = 1-\|r\|^2$	$1-\|r\|^2$の確率で検出される

Bobの測定方法

$P_0 = 1-|u_1\rangle\langle u_1|$

$P_1 = 1-|u_0\rangle\langle u_0|$

$$\begin{aligned}\langle u_0|P_1|u_0\rangle &= \langle u_0|(1-|u_0\rangle\langle u_0|)|u_0\rangle \\ &= \langle u_0|u_0\rangle - \langle u_0|u_0\rangle\langle u_0|u_0\rangle \\ &= 1-|\langle u_0|u_0\rangle|^2 \\ &= 0\end{aligned}$$

- ビット値が一致しない時 → 検出されない
- ビット値が一致する時 → $1-|r|^2$の確率で検出される

AliceとBobが同じビット値を共有できる

Aliceが送信する状態

$\|u_0\rangle \rightarrow P_0$	$\langle u_0\|P_0\|u_0\rangle = 1-\|r\|^2$	$1-\|r\|^2$の確率で検出される
$\|u_0\rangle \rightarrow P_1$	$\langle u_0\|P_1\|u_0\rangle = 0$	検出されない
$\|u_1\rangle \rightarrow P_0$	$\langle u_1\|P_0\|u_1\rangle = 0$	検出されない
$\|u_1\rangle \rightarrow P_1$	$\langle u_1\|P_1\|u_1\rangle = 1-\|r\|^2$	$1-\|r\|^2$の確率で検出される

Bobの測定方法

$P_0 = 1-|u_1\rangle\langle u_1|$

$P_1 = 1-|u_0\rangle\langle u_0|$

- ビット値が一致しない時 → 検出されない
- ビット値が一致する時 → $1-|r|^2$の確率で検出される

発表の流れ

1．B92プロトコルとは
- 秘密鍵を用いた通信について
- B92プロトコルの鍵の共有方法
- 単一光子の偏光状態を用いたB92プロトコル
- B92プロトコルの鍵の共有方法（具体例）

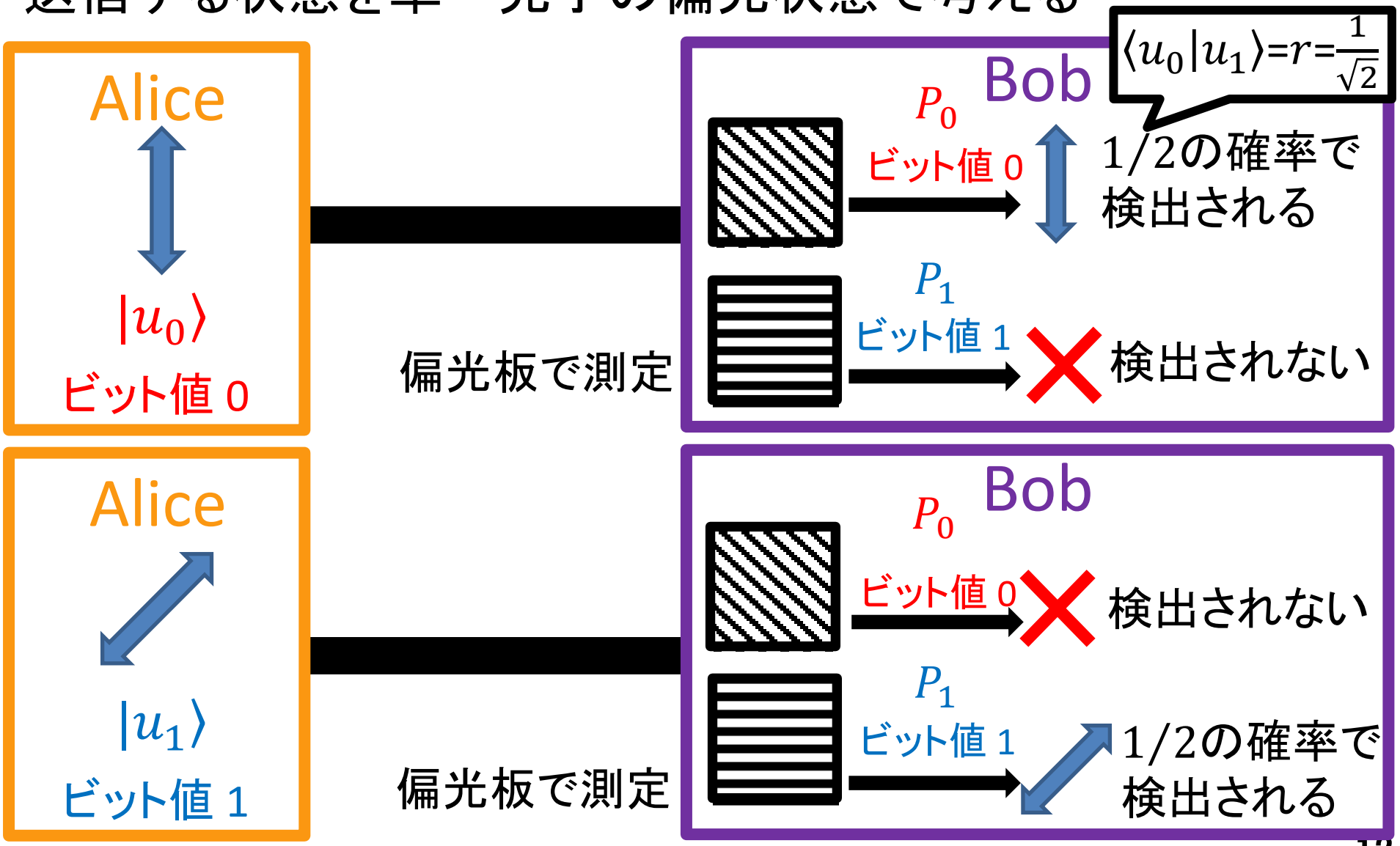
2．B92プロトコルの安全性
- Bobに届く状態が変化しない場合
- 通信路に損失がある場合

3．参照光を用いたB92プロトコル
- 微弱レーザー光と参照光を送信する方法
- なりすまし攻撃に対する安全性

4．まとめ

単一光子の偏光状態を用いたB92プロトコル

送信する状態を単一光子の偏光状態で考える



発表の流れ

1．B92プロトコルとは
- 秘密鍵を用いた通信について
- B92プロトコルの鍵の共有方法
- 単一光子の偏光状態を用いたB92プロトコル
- B92プロトコルの鍵の共有方法（具体例）

2．B92プロトコルの安全性
- Bobに届く状態が変化しない場合
- 通信路に損失がある場合

3．参照光を用いたB92プロトコル
- 微弱レーザー光と参照光を送信する方法
- なりすまし攻撃に対する安全性

4．まとめ

B92プロトコルの鍵の共有方法(具体例)

Alice

①2つの互いに非直交な状態をランダムに送信する

量子状態	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_1\rangle$	$\|u_0\rangle$

②2つの方法をランダムに用いて測定する

Bob

③検出された場合をAliceに伝える

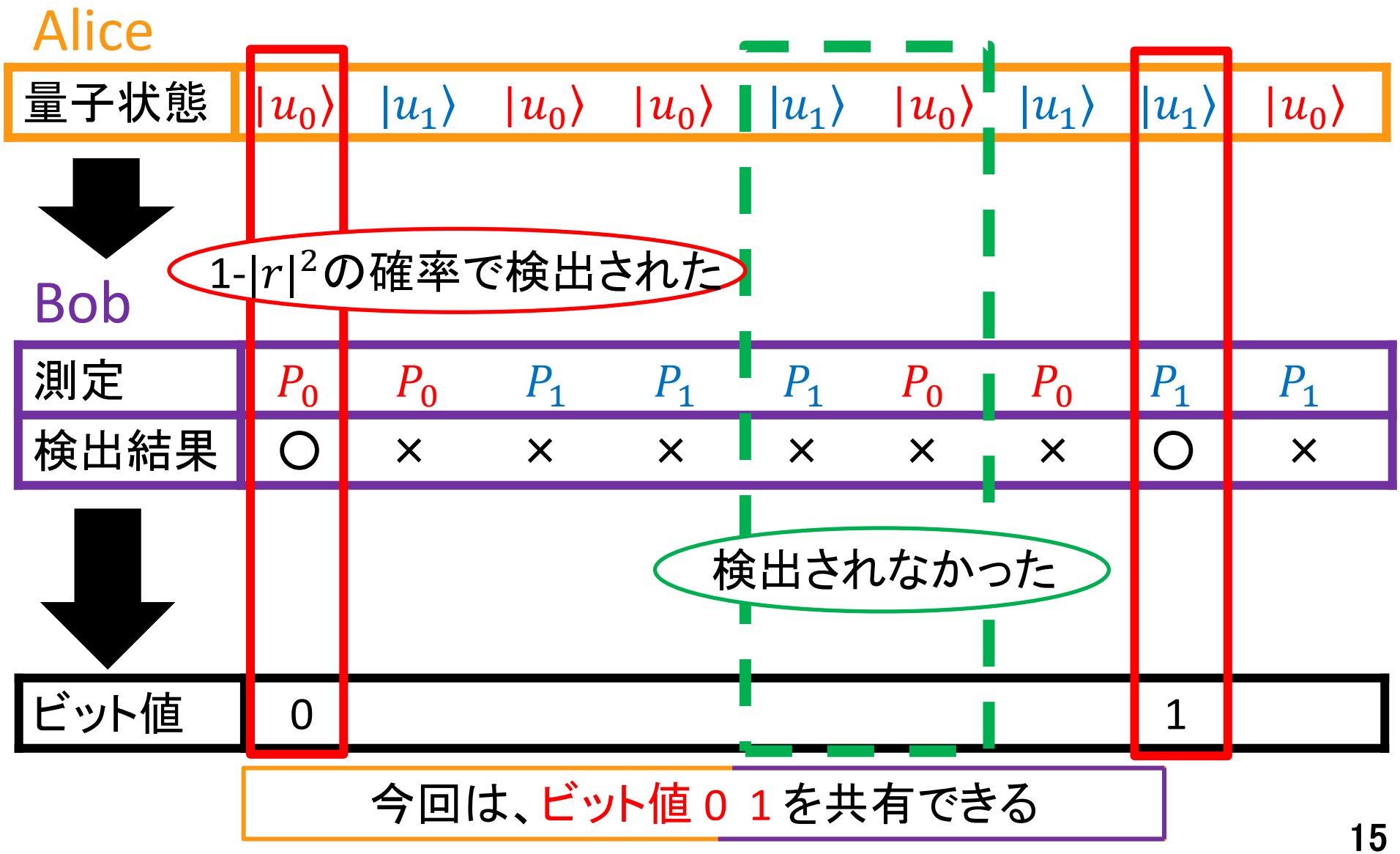
測定	P_0	P_0	P_1	P_1	P_1	P_0	P_0	P_1	P_1
検出結果	○	×	×	×	×	×	×	○	×

④どのビット値がBobに検出されたか分かる

ビット値	0	1

AliceとBobでビット値を共有できる

B92プロトコルの鍵の共有方法(具体例)



発表の流れ

1．B92プロトコルとは
- 秘密鍵を用いた通信について
- B92プロトコルの鍵の共有方法
- 単一光子の偏光状態を用いたB92プロトコル
- B92プロトコルの鍵の共有方法（具体例）

2．B92プロトコルの安全性
- Bobに届く状態が変化しない場合
- 通信路に損失がある場合

3．参照光を用いたB92プロトコル
- 微弱レーザー光と参照光を送信する方法
- なりすまし攻撃に対する安全性

4．まとめ

Bobに届く状態が変化しない場合

Bobに届いた状態がAliceが送信した状態と変化していない場合、
安全に量子鍵配送が行える。

$|u_0\rangle$ $|u_1\rangle$が互いに非直交だと、$\langle u_0|u_1\rangle \neq 0$……①

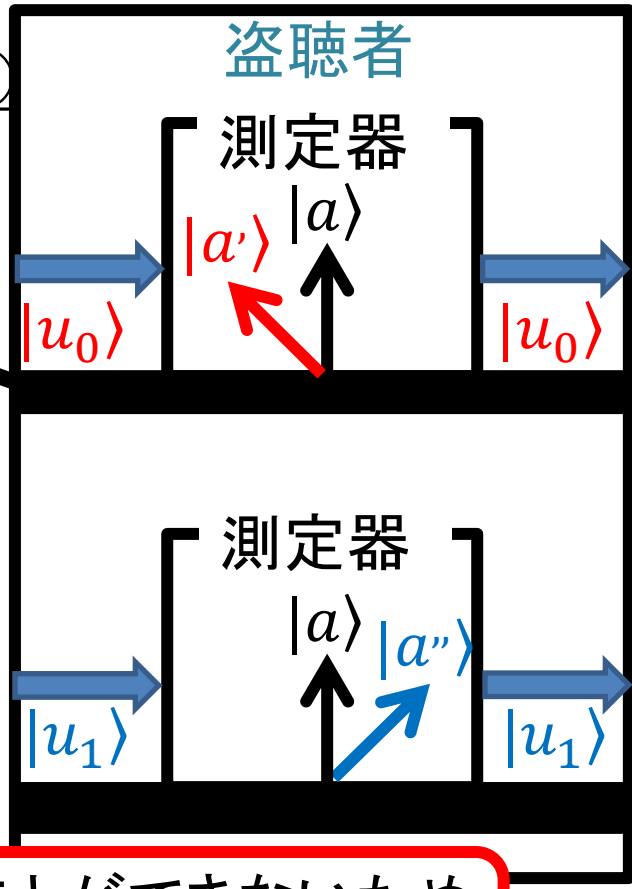
$U(|u_0\rangle|a\rangle)=|u_0\rangle|a'\rangle$　$U(|u_1\rangle|a\rangle)=|u_1\rangle|a''\rangle$

$\langle a|\langle u_0|U^\dagger U|u_1\rangle|a\rangle=\langle a'|\langle u_0|u_1\rangle|a''\rangle$

$\langle u_0|u_1\rangle=\langle a'|a''\rangle\langle u_0|u_1\rangle$

$\langle a'|a''\rangle=1$

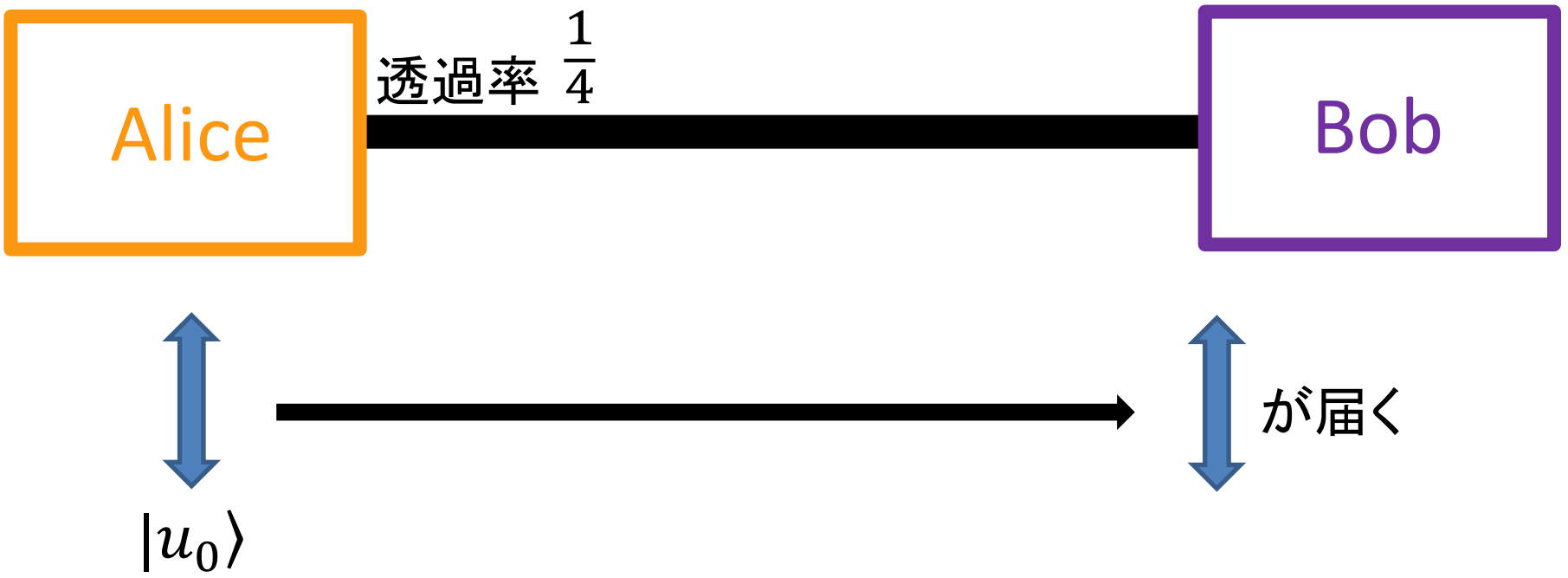
よって、$|a'\rangle=|a''\rangle$



盗聴者は、状態を変化させずに情報を得ることができないため、
安全に量子鍵配送が行える

通信路に損失がある場合

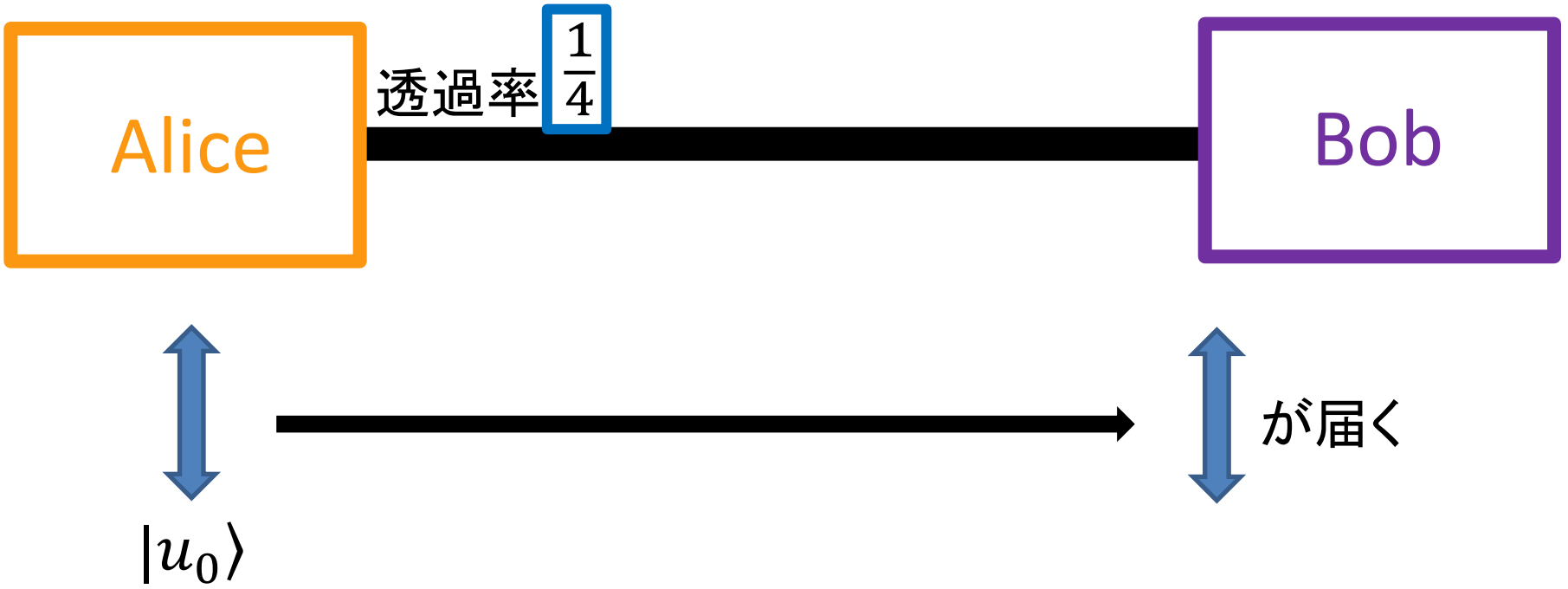
透過率が25%の通信路の場合



Aliceが送信した光子がBobに届く確率 → $\frac{1}{4}$

通信路に損失がある場合

透過率が25%の通信路の場合



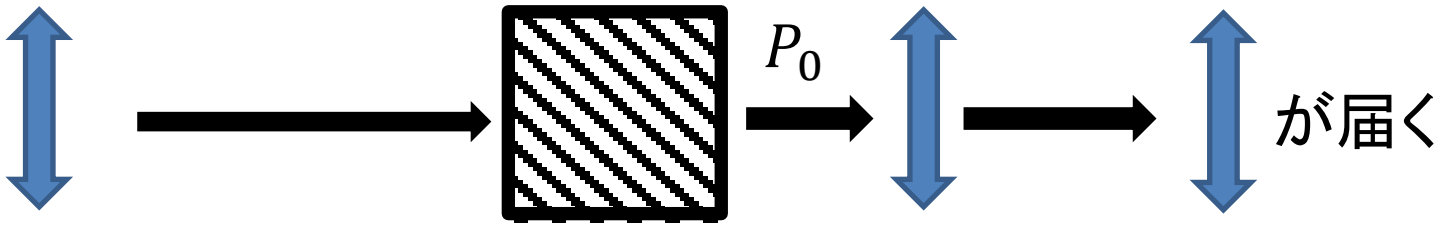
Aliceが送信した光子が
Bobに届く確率 → $\frac{1}{4}$

通信路に損失がある場合

Eveが透過率100%の通信路に置き換えてなりすまし攻撃をした場合

なりすまし攻撃をする → 検出された時 →再送する
検出されなかった時 →再送しない

Alice　透過率１　盗聴者　Eve　Bob



$|u_0\rangle$

ビット値 0

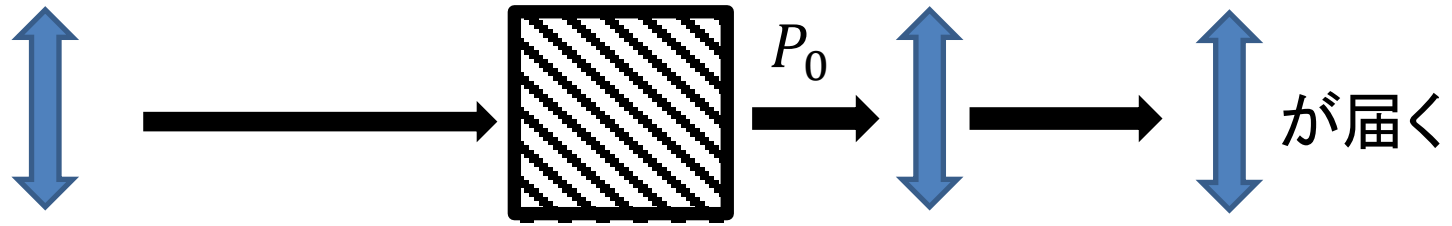
・測定方法を$1/2$の確率で選ぶ
・$1/2$ の確率で検出

Aliceが送信した光子がBobに届く確率 → $1 \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

通信路に損失がある場合

Eveが透過率100%の通信路に置き換えてなりすまし攻撃をした場合

なりすまし攻撃をする → 検出された時 →再送する
検出されなかった時 →再送しない



$|u_0\rangle$

ビット値 0

・測定方法を $1/2$ の確率で選ぶ
・$1/2$ の確率で検出

Aliceが送信した光子がBobに届く確率 → $1 \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$

通信路に損失がある場合

Eveが透過率100%の通信路に置き換えてなりすまし攻撃をした場合

なりすまし攻撃をする → 検出された時 →再送する
検出されなかった時 →再送しない

Alice

Bob

Eve=透過率25%の通信路

Eveがいることに気付かず
鍵を共有してしまうので、
安全ではない

なりすまし攻撃をされても
安全に通信を行うためには
どうしたらいいのか？

が届く

$|u_0\rangle$

ビット値 0

Aliceが送信した光子が
Bobに届く確率

$$1 \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$$

発表の流れ

1．B92プロトコルとは
- 秘密鍵を用いた通信について
- B92プロトコルの鍵の共有方法
- 単一光子の偏光状態を用いたB92プロトコル
- B92プロトコルの鍵の共有方法（具体例）

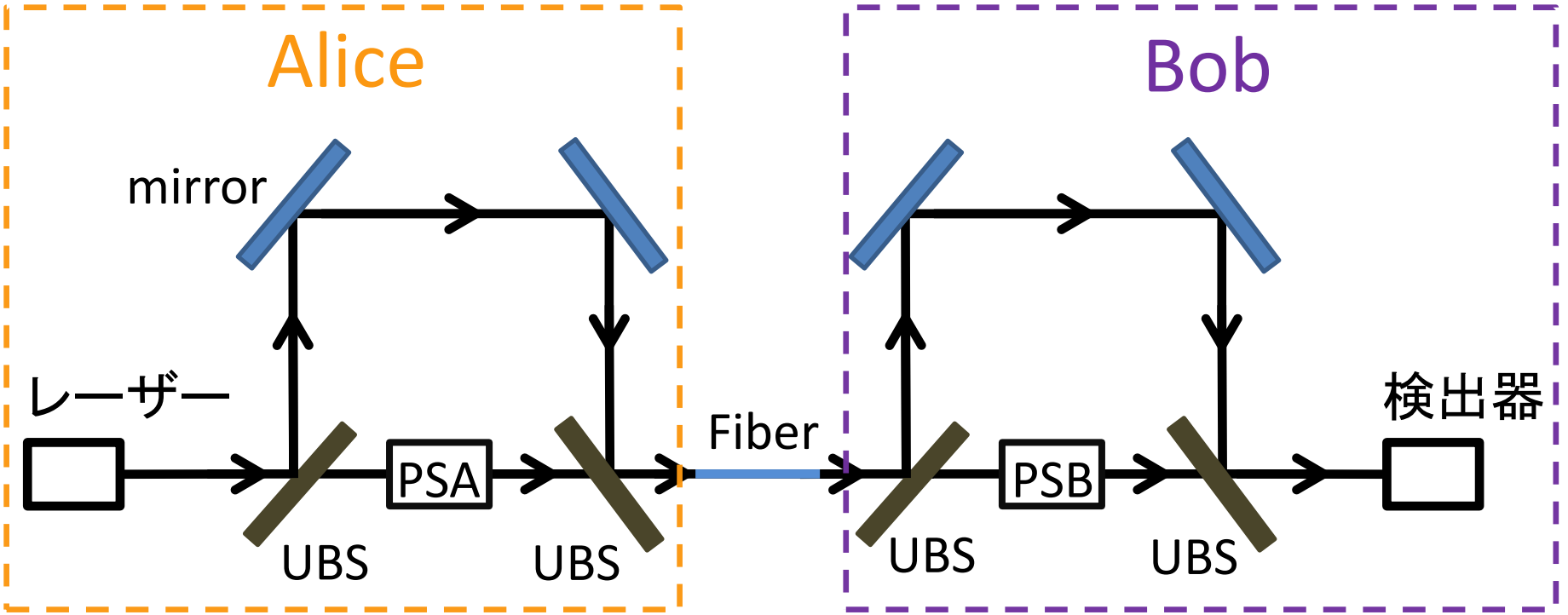
2．B92プロトコルの安全性
- Bobに届く状態が変化しない場合
- 通信路に損失がある場合

3．参照光を用いたB92プロトコル
- 微弱レーザー光と参照光を送信する方法
- なりすまし攻撃に対する安全性

4．まとめ

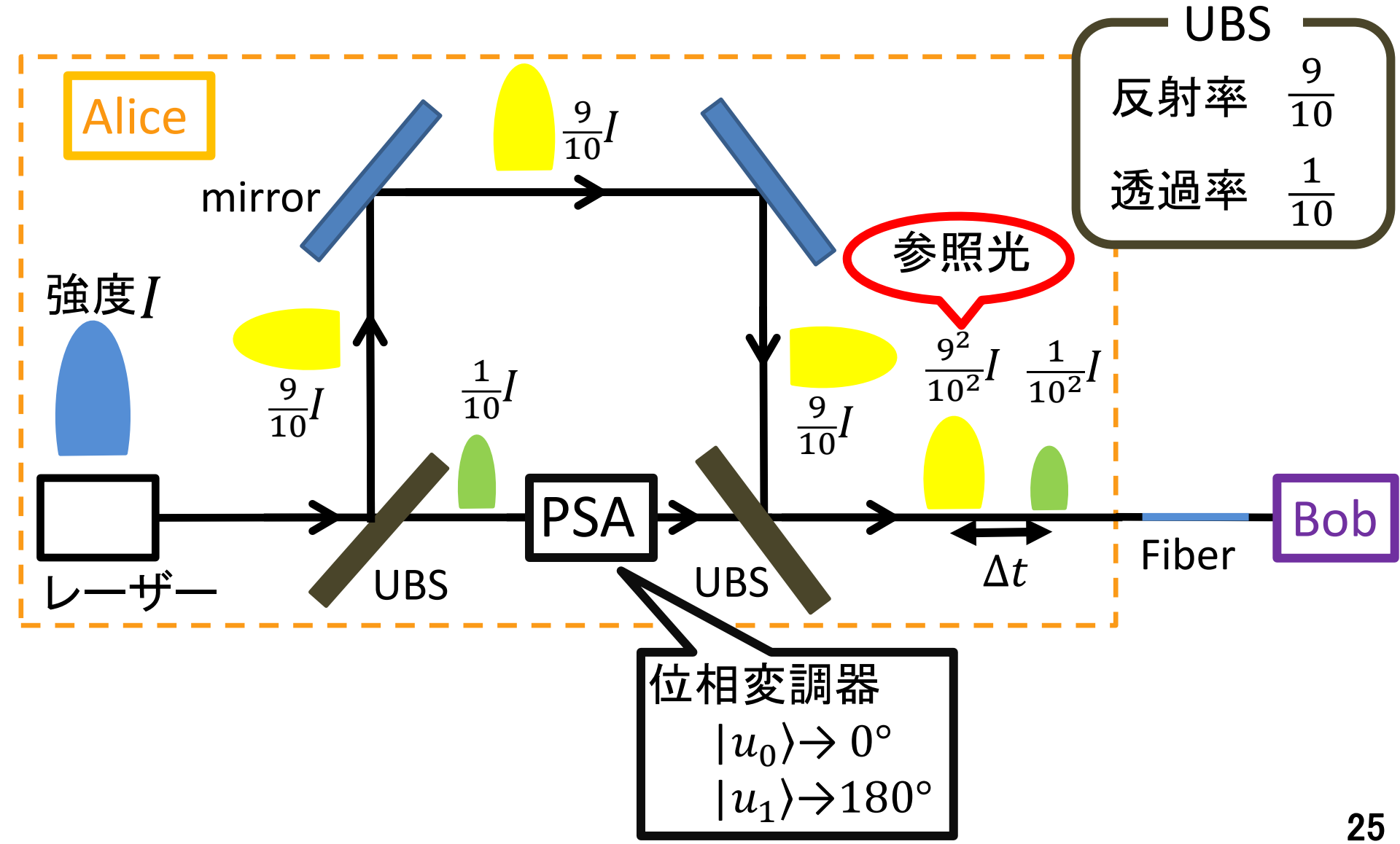
微弱なレーザー光と参照光を送信する方法

2つの非直交状態を表す微弱レーザー光と参照光を送信する方法

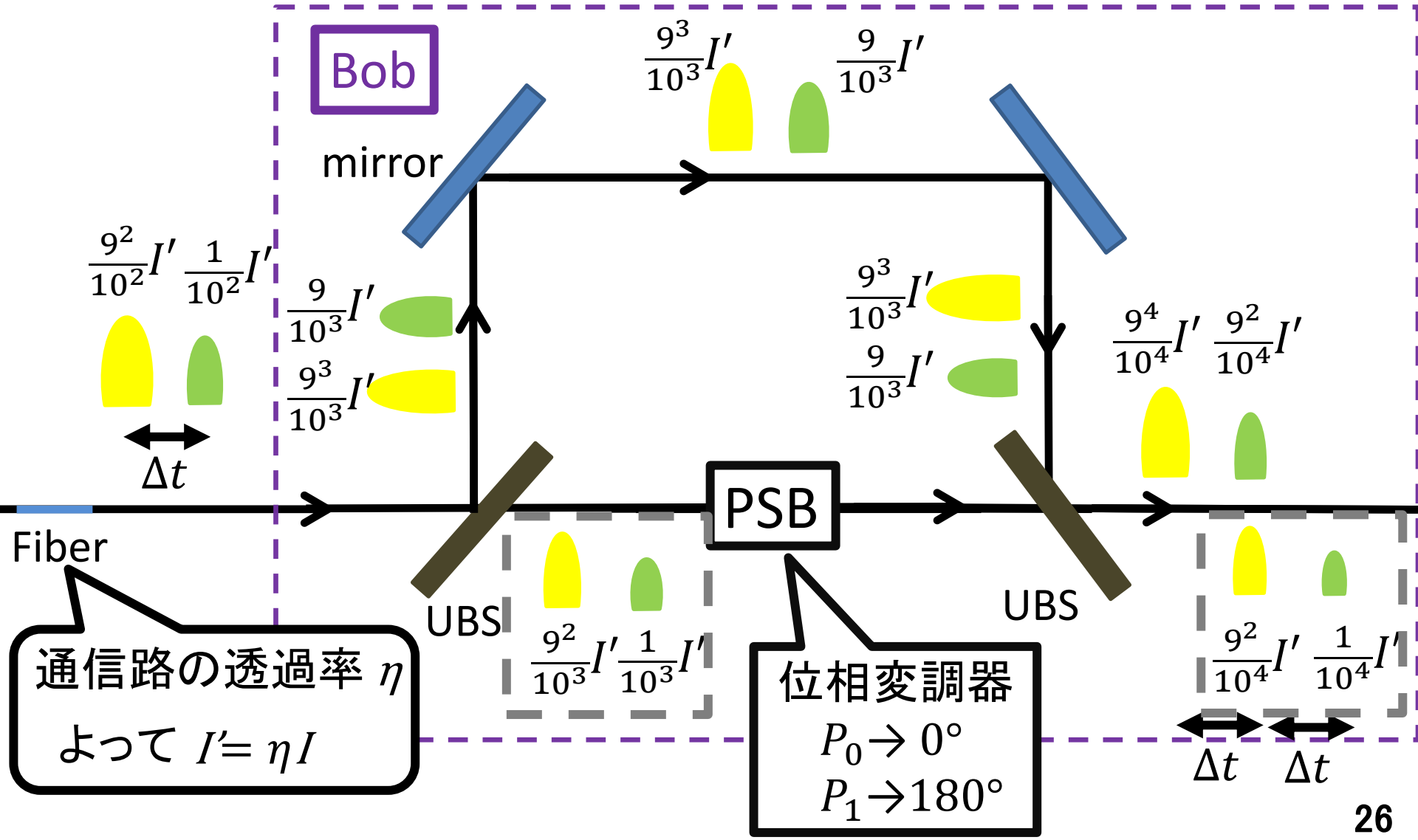


- UBS→Unsymmetric Beam Splitter
  →反射率が高く、透過率が低い
- PSA,PSB→位相変調器

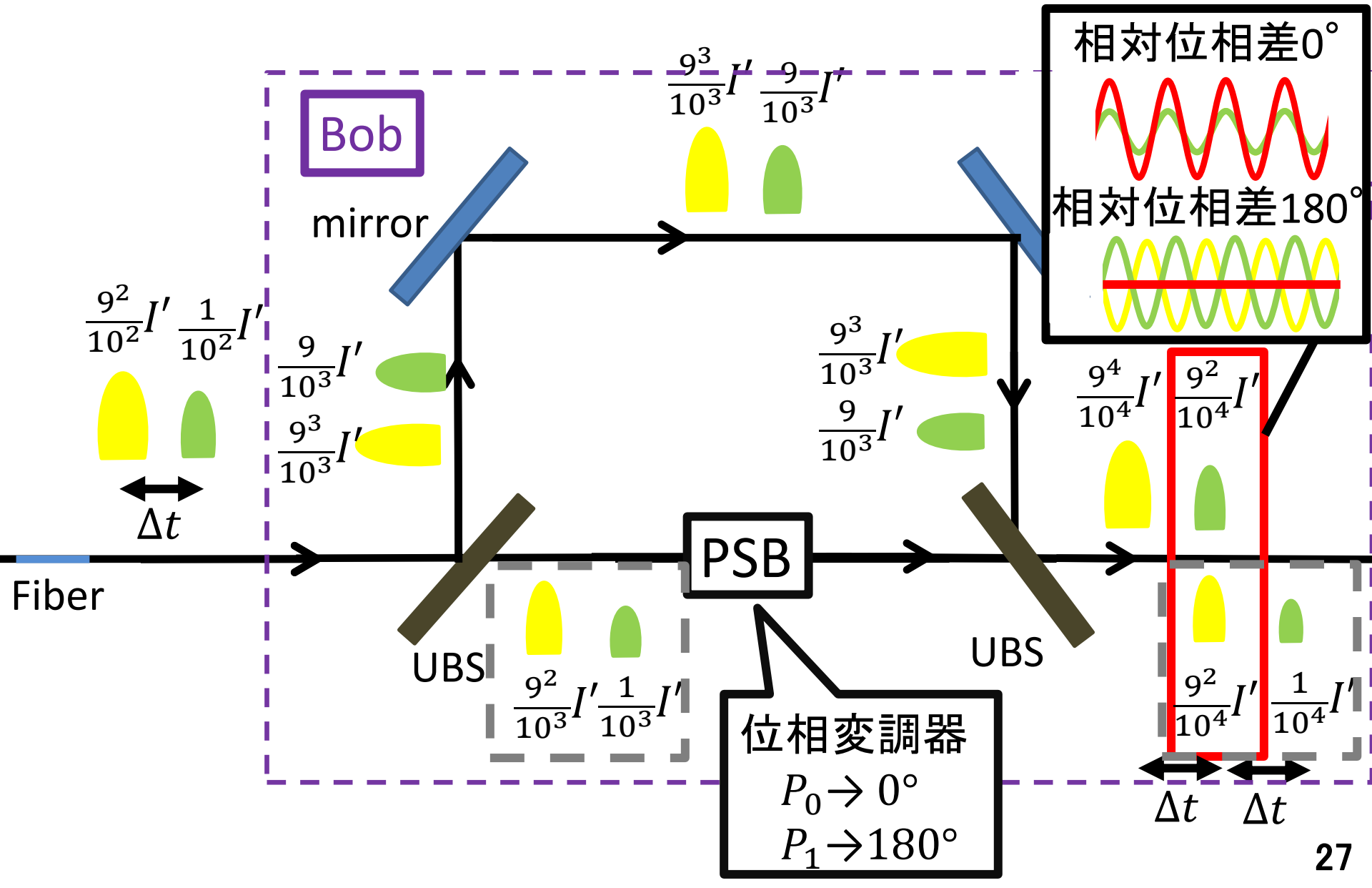
微弱なレーザー光と参照光を送信する方法



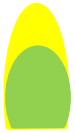
微弱なレーザー光と参照光を送信する方法



微弱なレーザー光と参照光を送信する方法



微弱なレーザー光と参照光を送信する方法

Alice		Bob				
PSA	量子状態	PSB	測定方法	検出器	bit	検出されるパルス
$0°$	$\|u_0\rangle$	$0°$	P_0	○	0	
$0°$	$\|u_0\rangle$	$180°$	P_1	-	-	
$180°$	$\|u_1\rangle$	$0°$	P_0	-	-	
$180°$	$\|u_1\rangle$	$180°$	P_1	○	1	

弱め合うため検出されない

なりすまし攻撃に対する安全性

盗聴者の攻撃として

なりすまし攻撃をする → 検出された時 → 再送する
検出されなかった時 → 再送しない

Bobに再送しない場合、参照光はどうするのか？

参照光を再送しない場合、
強度が非常に強い光が届かないため、
盗聴にすぐに気付くことができる。

なりすまし攻撃に対する安全性

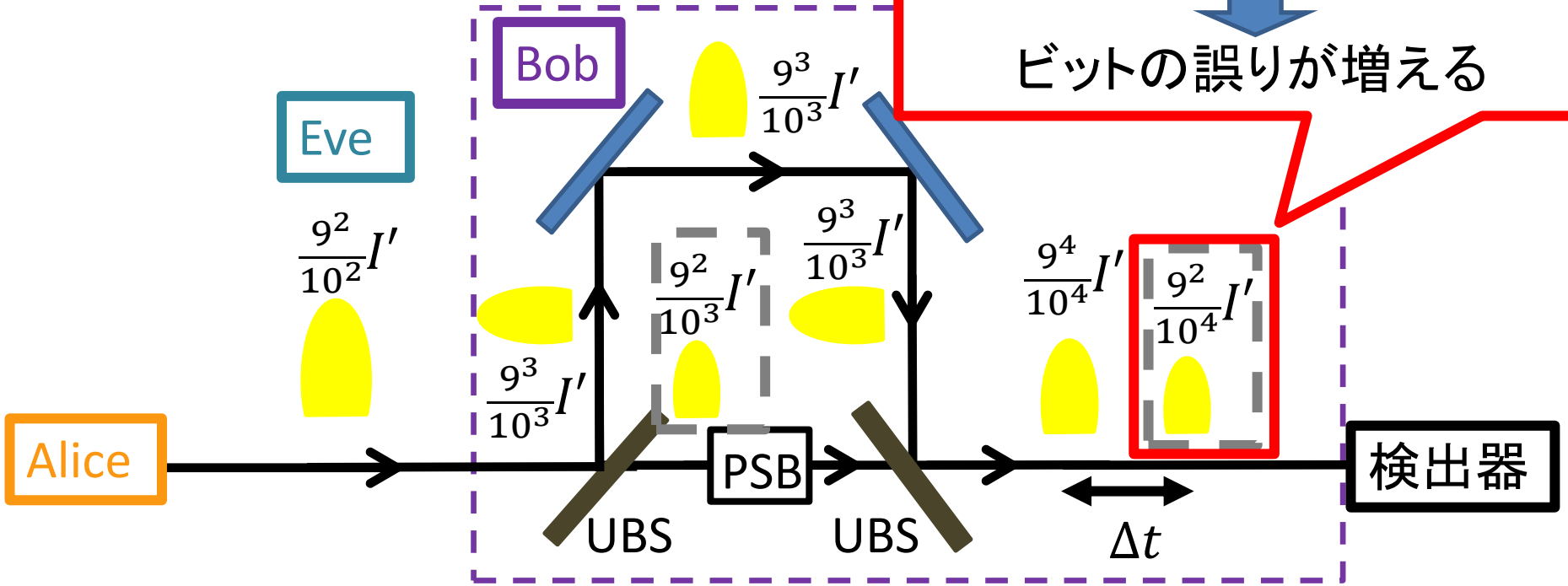
Eve → 検出されなかった時

参照光のみ再送する

ビット値が一致しない場合でも検出されてしまう。

ビットのくい違いが生じる

ビットの誤りが増える



なりすまし攻撃に対する安全性

盗聴者の攻撃として

なりすまし攻撃をする → 検出された時 → 再送する
検出されなかった時 → 再送しない

Bobに再送しない場合、参照光はどうするのか？

再送しない場合

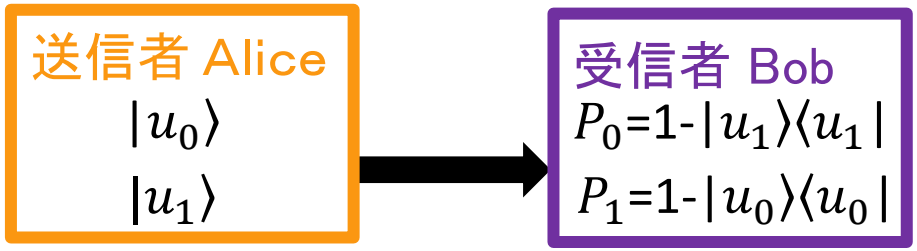
強度が強い光が届かないので、
盗聴に気付く

再送する場合

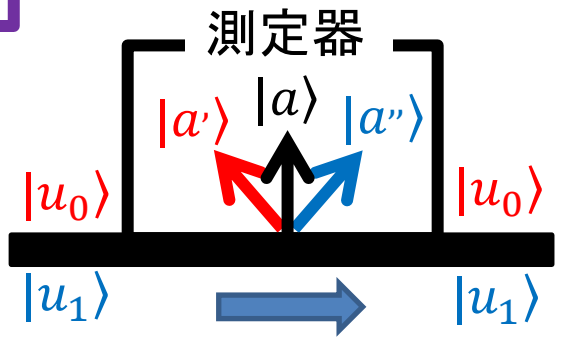
ビット値の誤りが増えるので、
盗聴に気付く

まとめ

- B92プロトコルとは、2つの非直交状態を用いる量子鍵配送



- Bobに届いた状態が、
  Aliceの送信した状態と変化していない場合
  Eveは盗聴できない



- なりすまし攻撃された場合
  - 単一光子の偏光状態を用いた方法では、
    安全に量子鍵配送を行うことができない

  - 参照光を用いる方法であれば、
    安全に量子鍵配送を行うことができる

予備スライド

何故微弱なレーザー光が非直交状態だとみなせるのか

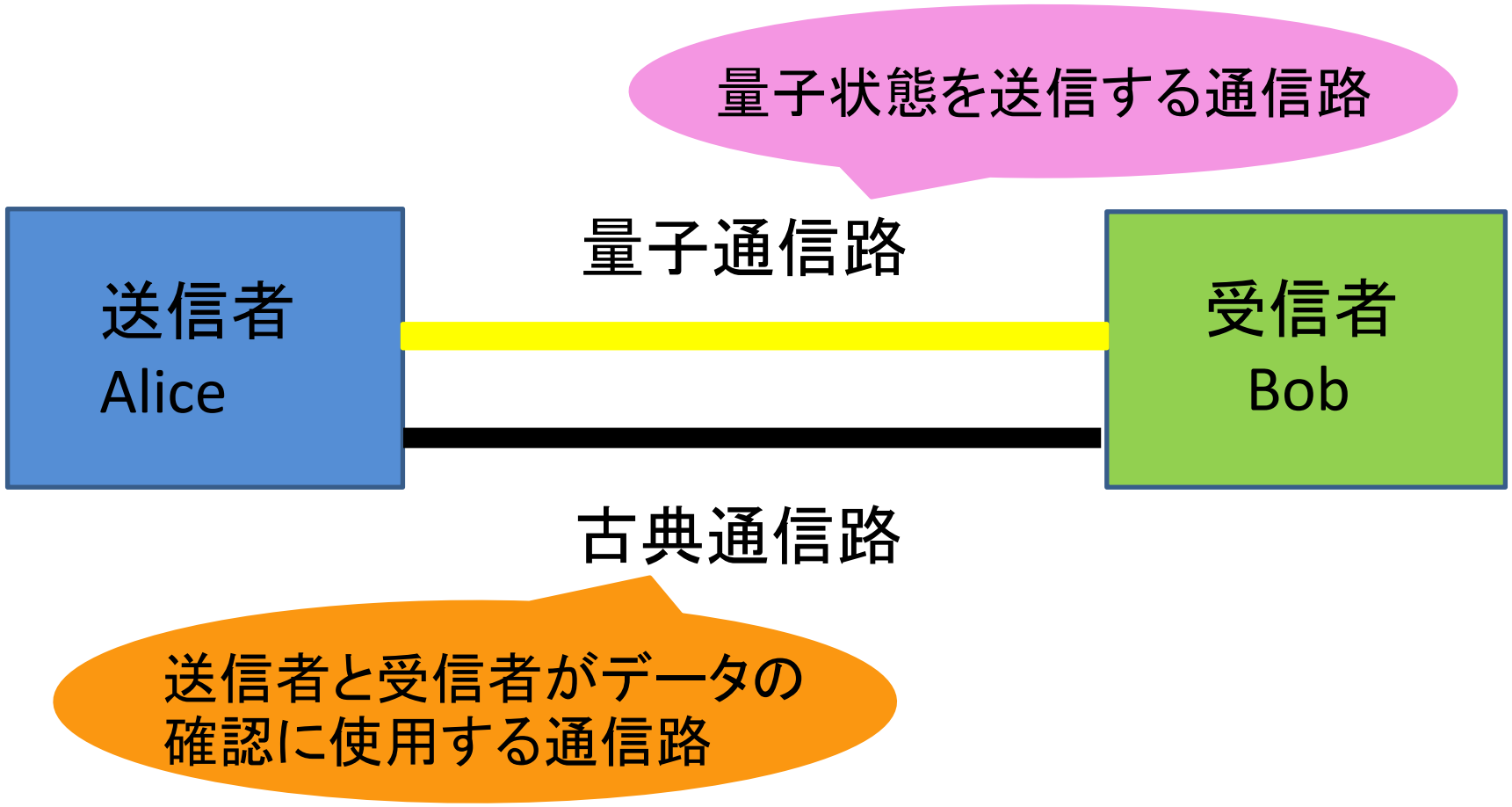
$$\langle -\alpha|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum \frac{|-\alpha^*|^n}{\sqrt{n!}} \langle n| e^{-\frac{|\alpha|^2}{2}} \sum \frac{\alpha^m}{\sqrt{m!}} |m\rangle$$

$$= e^{-|\alpha|^2} \sum\sum \frac{(-\alpha^*)^n \alpha^m}{\sqrt{n!}\sqrt{m!}} \langle n|m\rangle$$

$$= e^{-|\alpha|^2} \sum \frac{(-|\alpha|^2)^n}{n!}$$

$$= e^{-2|\alpha|^2}$$

量子鍵配送



量子通信路と古典通信路を用いて秘密鍵を生成する。

非直交状態を偏光状態に対応させる

非直交状態を表す	$\|u_0\rangle$	$\|u_1\rangle$
対応するビット	0	1
対応させる偏光状態	$\|\updownarrow\rangle$	$\|\nearrow\rangle$

Alice

2つの非直交状態に対して
垂直な状態を用意する。

$\|u_{0\perp}\rangle$	$\|u_{1\perp}\rangle$
$\|\leftrightarrow\rangle$	$\|\searrow\rangle$

$|\leftrightarrow\rangle\langle\leftrightarrow|+|\updownarrow\rangle\langle\updownarrow|=1$
$|\searrow\rangle\langle\searrow|+|\nearrow\rangle\langle\nearrow|=1$

Bobの
測定基底を
偏光状態で
表すと……

$P_0=1-|u_1\rangle\langle u_1|$
$=|\searrow\rangle\langle\searrow|+|\nearrow\rangle\langle\nearrow|-|\nearrow\rangle\langle\nearrow|$
$=|\searrow\rangle\langle\searrow|$

$P_1=1-|u_0\rangle\langle u_0|$
$=|\leftrightarrow\rangle\langle\leftrightarrow|+|\updownarrow\rangle\langle\updownarrow|-|\updownarrow\rangle\langle\updownarrow|$
$=|\leftrightarrow\rangle\langle\leftrightarrow|$

Bob

測定基底	$P_0=1-\|u_1\rangle\langle u_1\|$	$P_1=1-\|u_0\rangle\langle u_0\|$
偏光状態	$\|\searrow\rangle\langle\searrow\|$	$\|\leftrightarrow\rangle\langle\leftrightarrow\|$

B92プロトコルの方法④

もし盗聴者が存在しなければ、
検出できた結果には完全に

$|u_0\rangle \rightarrow P_0$
$|u_1\rangle \rightarrow P_1$ で測定した。 ⇒ 得られたビット値は AliceとBobで一致している。

という相関があるべき。

検出できている結果のうち、
一致していると確かめた一部を捨てる。

残りを使って最終鍵を作る。

微弱なコヒーレント光と非直交について

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

コヒーレント状態を表す式

$$\cong \left(1 - \frac{|\alpha|^2}{2}\right)|0\rangle + \alpha|1\rangle + \frac{\alpha^2}{\sqrt{2}}|2\rangle + \circ(\alpha^3)$$

平均光子数$|\alpha|^2 \ll 1$

微弱なコヒーレント光
（レーザー光）

$$\langle -\alpha|\alpha\rangle \cong 1 - 2|\alpha^2|$$
$$\cong e^{-2|\alpha^2|}$$
$$\neq 0$$

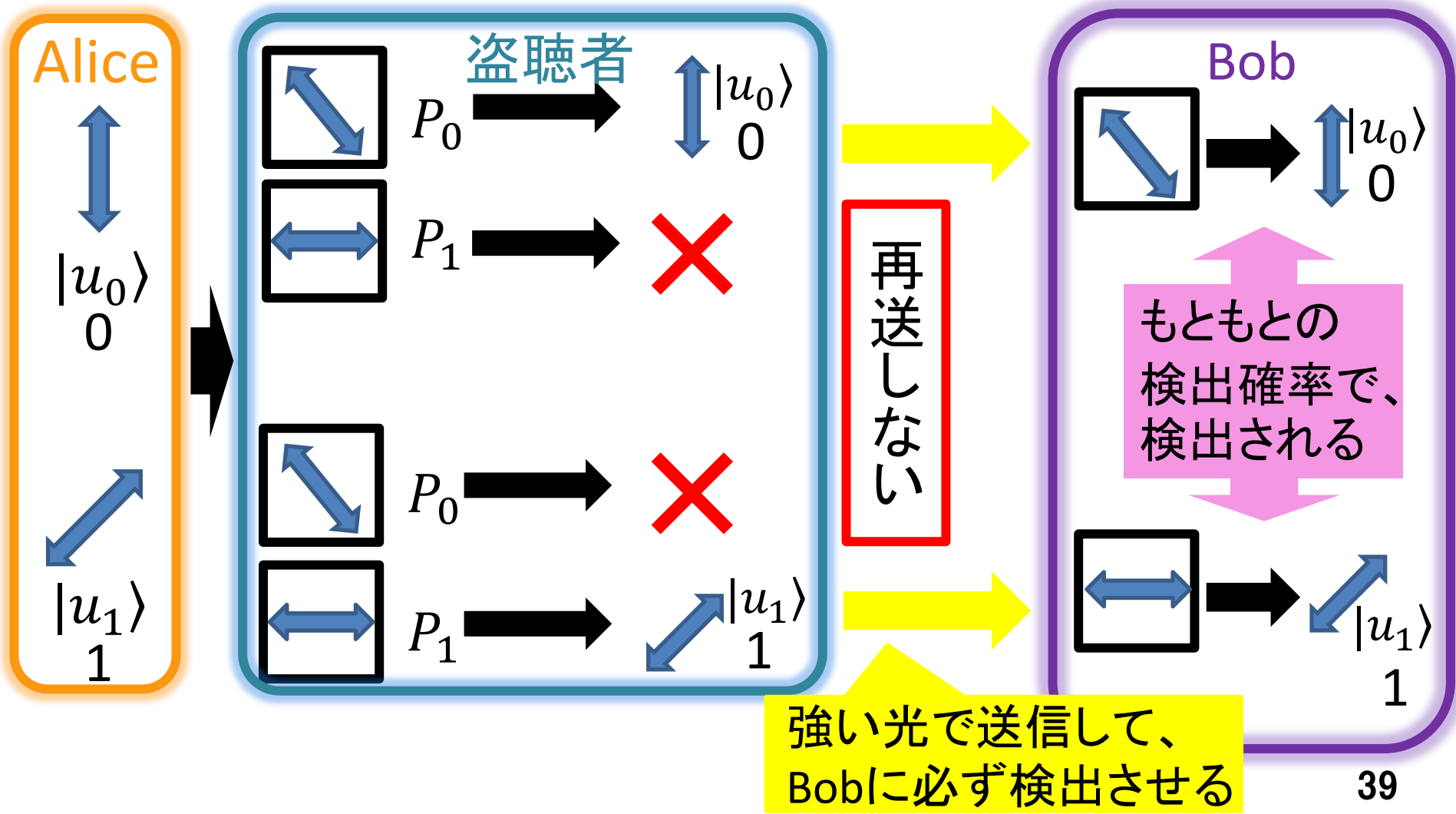
非直交状態だと
$\langle u_0|u_1\rangle \neq 0$

微弱なレーザー光だと非直交状態だとみなせる。

$$|\alpha\rangle, |-\alpha\rangle \rightarrow |u_0\rangle, |u_1\rangle$$

盗聴ができてしまう場合の例

状態が変化してしまう方法でも盗聴ができてしまう場合がある



盗聴者とB92プロトコル①

非直交状態を用いる理由.....

2つの非直交状態を用いるとコピーできないという性質。

2つの非直交状態ではコピーできない証明

$|\psi\rangle \otimes |s\rangle$

$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$

$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$

$|\Psi\rangle$を$|s\rangle$にコピーすることを考える

$|\psi\rangle$を$|s\rangle$にコピーしたとする...①

$|\phi\rangle$を$|s\rangle$にコピーしたとする...②

盗聴者とB92プロトコル②

$$\langle s|\otimes\langle \emptyset|U^{-1}U|\psi\rangle\otimes|s\rangle = \langle \emptyset|\otimes\langle \emptyset|\psi\rangle\otimes|\psi\rangle$$

$$\langle \emptyset|\psi\rangle = \langle \emptyset|\psi\rangle^2$$

$\langle \emptyset|\psi\rangle$=1 or 0ということが分かる

非直交だとコピーが作れないことが分かる。

$|\psi\rangle$と$|\emptyset\rangle$をそれぞれ$|u_0\rangle$と$|u_1\rangle$とみなす。