量子情報通信

NTT物性科学基礎研究所

井上　恭

[内容]

1. 量子情報通信で利用する量子力学
2. 量子暗号
3. 量子テレポーテーション他
4. 基本デバイス

[内容]

1.**量子情報通信で利用する量子力学**

状態と観測問題（→量子暗号）

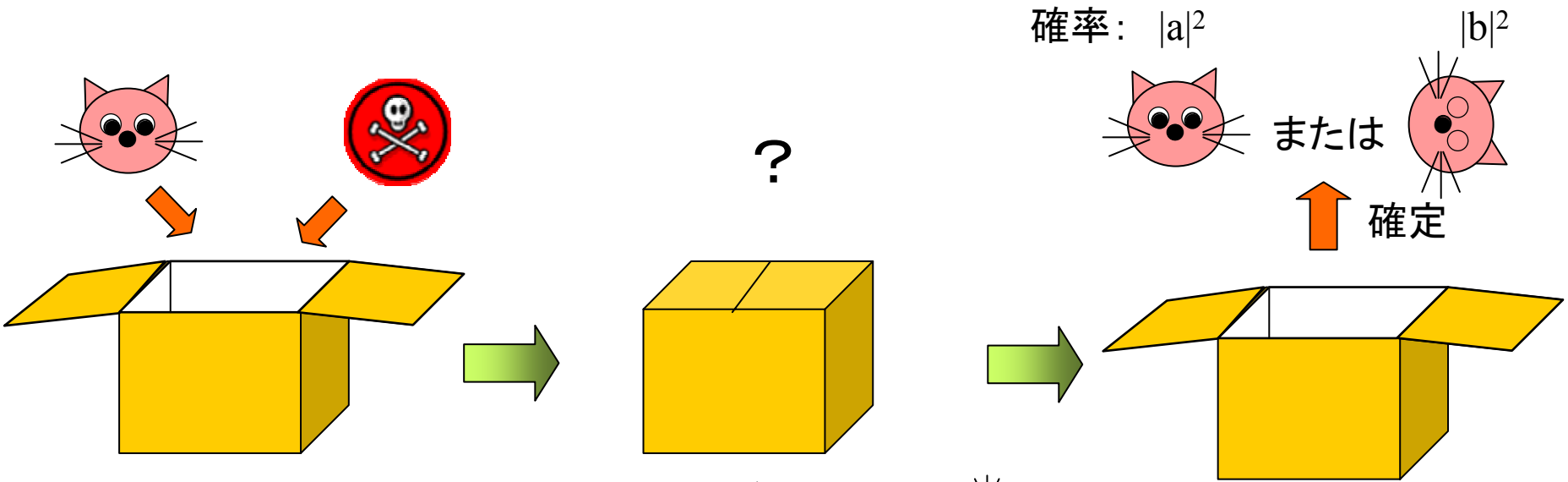
量子エンタングルメント（→量子テレポーテーション他）

2. 量子暗号

3. 量子テレポーテーション他

4. 基本デバイス

シュレディンガーの猫



$$|\psi> = a(t)|\text{生きている}\rangle + b(t)|\text{死んでいる}\rangle$$

一般的には

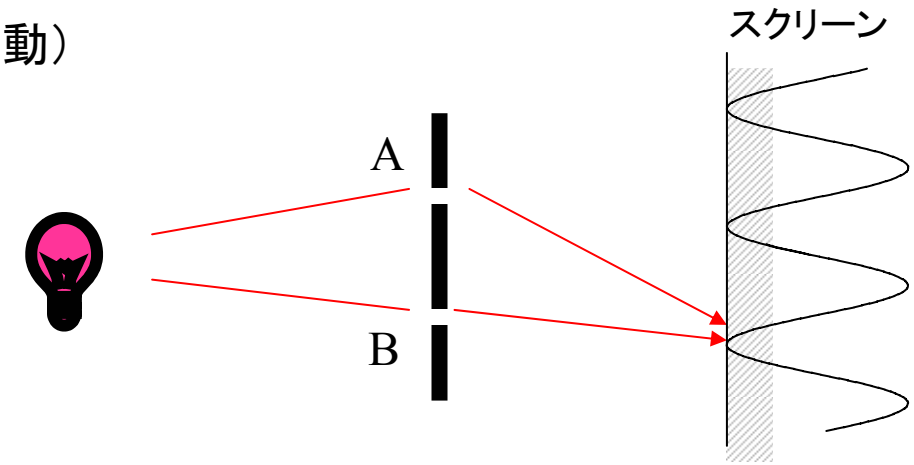
$|\psi> = a|X> + b|Y>$　　$\{|X>, |Y>\}$は直交基底系　$(<X|Y> = 0)$

・量子状態は確率振幅で重み付けした重ね合わせ状態

・観測行為により確定状態に収縮

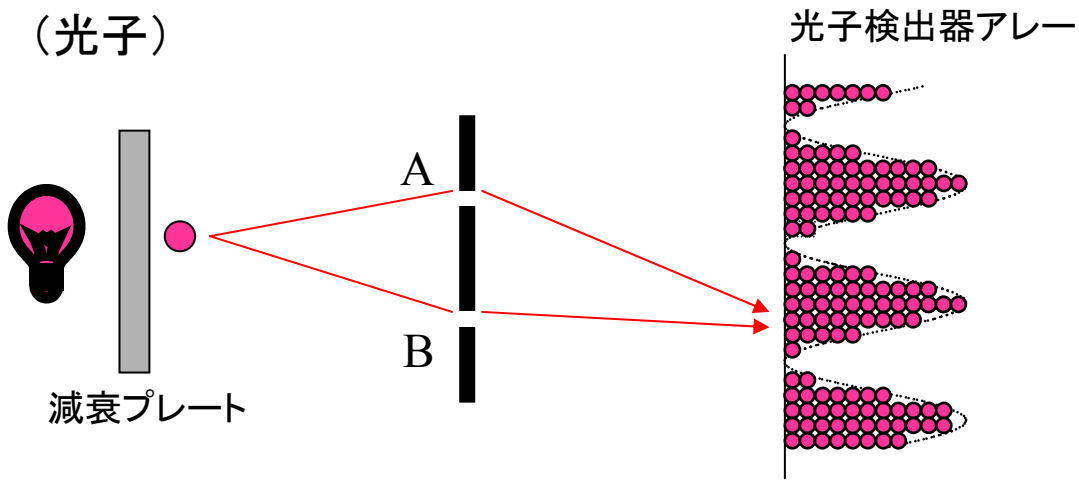
ヤングの干渉実験

（波動）



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

（光子）

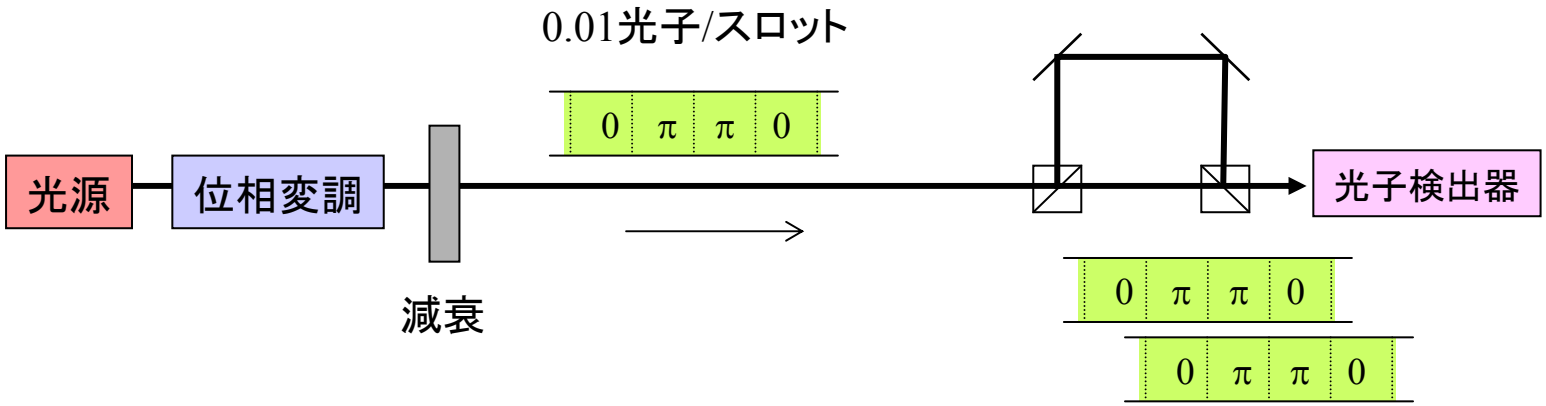


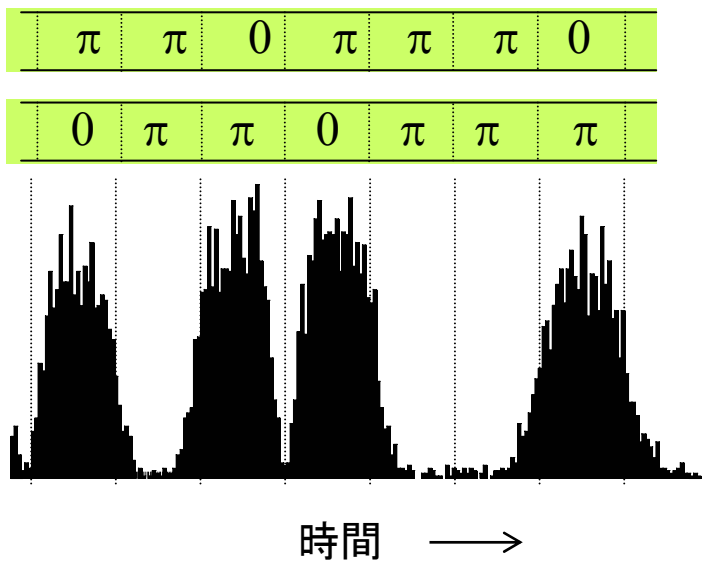
$$|\psi\rangle = a\mathrm{e}^{ikL_\mathrm{a}}|\mathrm{a}\rangle + b\mathrm{e}^{ikL_\mathrm{b}}|\mathrm{b}\rangle$$

|a>: 光子がAを通った状態

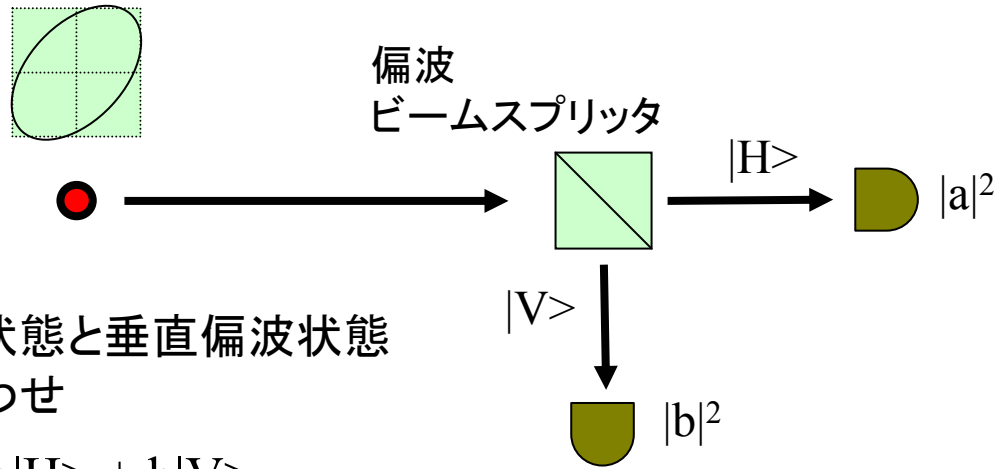
|b>: 光子がBを通った状態

光子干渉実験例


0.01光子/スロット
0 π π 0
光源
位相変調
減衰
光子検出器
0 π π 0
0 π π 0


π π 0 π π π 0
0 π π 0 π π π
時間

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

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

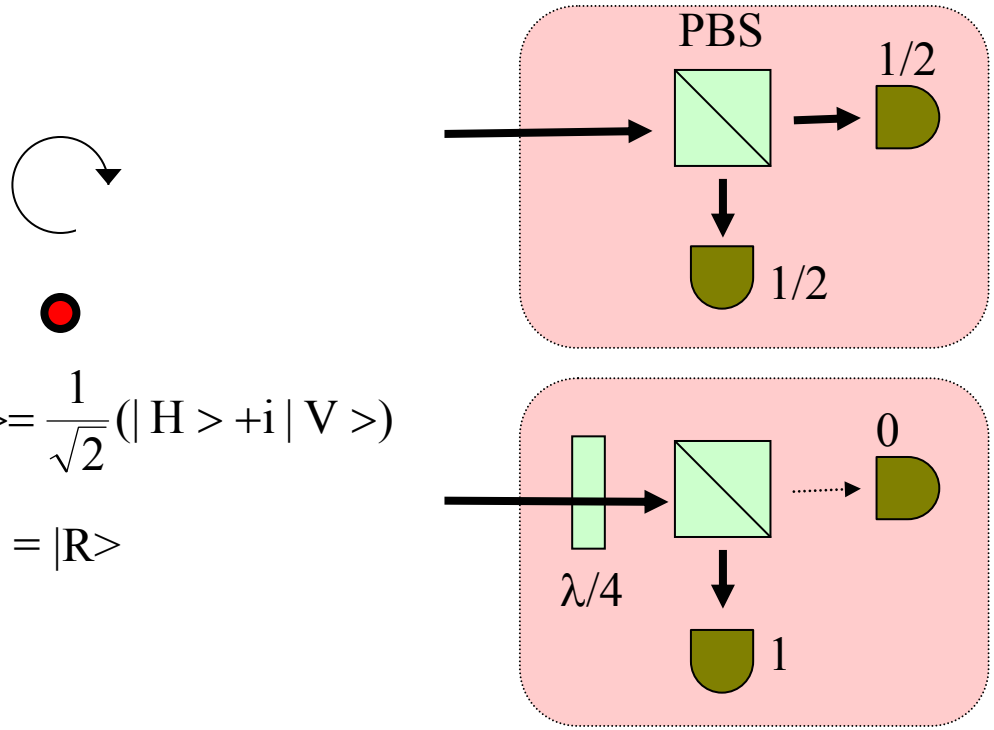
|H>：水平偏波状態
|V>：垂直偏波状態
$|a|^2 + |b|^2 = 1$

1光子については透過または反射
多数回測定すると$|a|^2 : |b|^2$の測定数

↓

1回の測定では状態を特定できない
（コピーも不可：non-cloning theory）

観測基底



$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$$

$$= |R\rangle$$

{H, V}基底

{R, L}基底

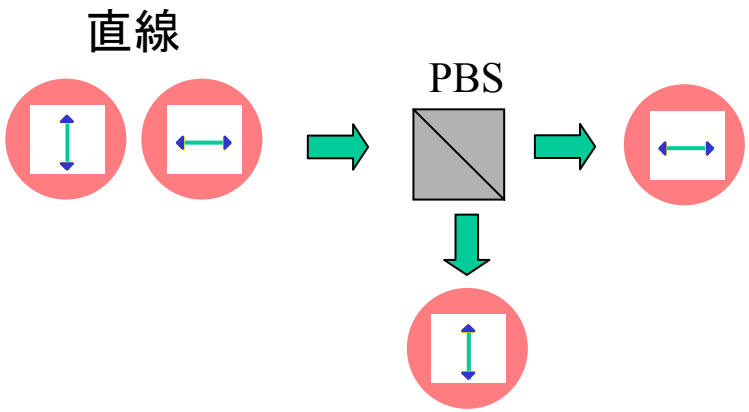
$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$$

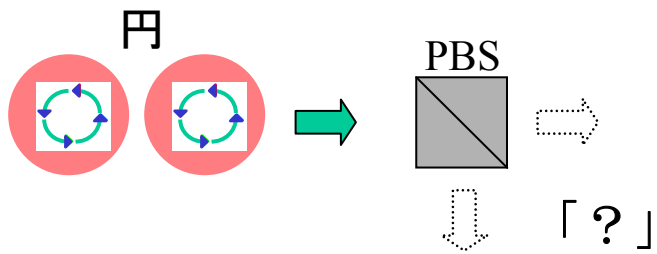
$$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$$

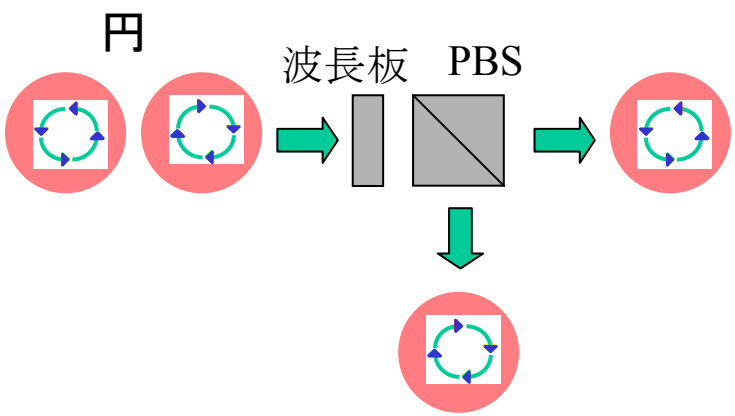
観測結果は測定基底に依存

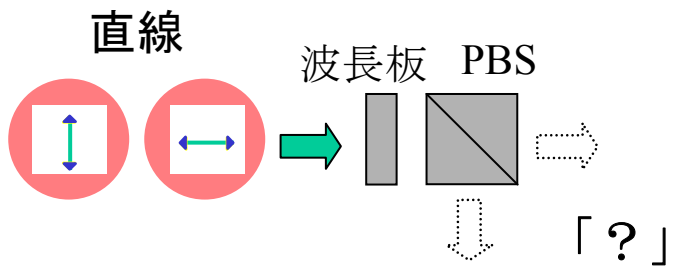
被観測状態が測定基底に一致していれば、確度100%の測定結果

状態と観測基底

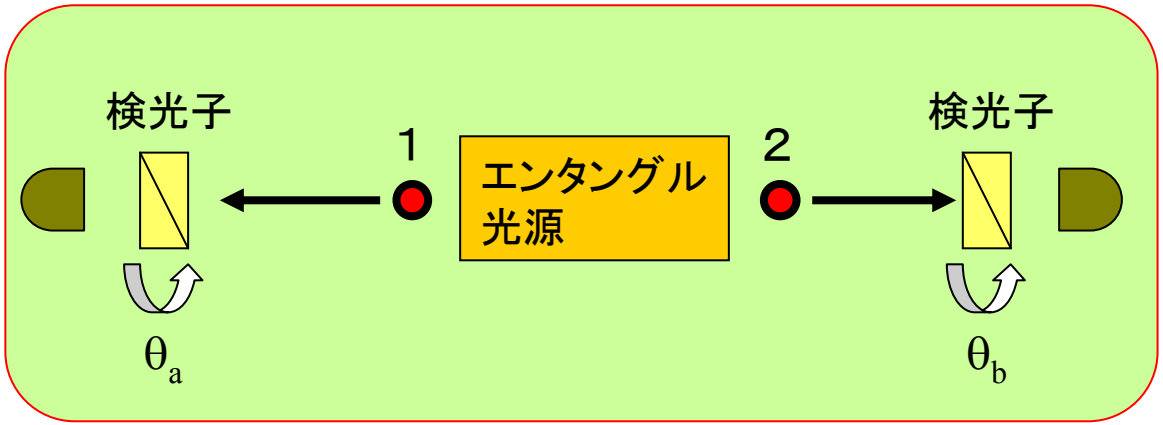




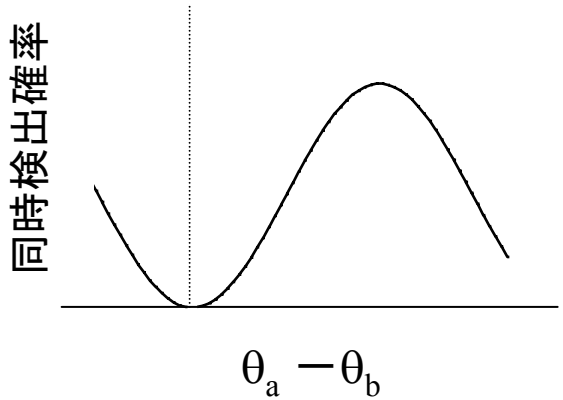




量子エンタングルメント（波動関数の非局在性）



一方だけの検出結果はランダムが、同時測定すると相関あり

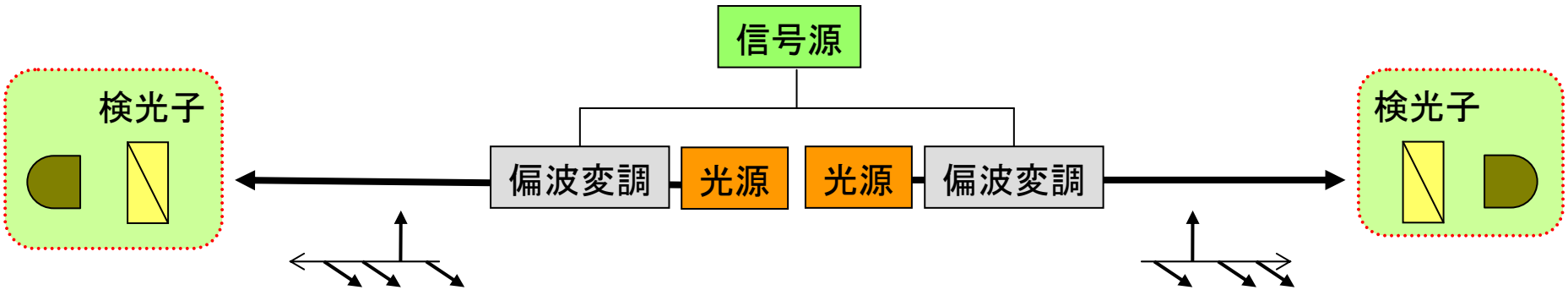


$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2) \longrightarrow$$ 一方がH (or V)だと他方もH (or V)

$$= \frac{1}{\sqrt{2}}(|+45\rangle_1|+45\rangle_2 + |-45\rangle_1|-45\rangle_2) \longrightarrow$$ 一方が+45 (or -45)だと他方も+45 (or -45)
（|+45>：右斜め直線、|-45>：左斜め直線）

$$= \frac{1}{\sqrt{2}}(|R\rangle_1|L\rangle_2 + |L\rangle_1|R\rangle_2) \longrightarrow$$ 一方がR (or L)だと他方もR (or L)
（|R>：右回り円、|L>：左回り円）

古典エンタングルメント



縦・横偏波系で測定 ⟶ 一方がH (or V)だと他方もH (or V)

円偏波系で測定 ⟶ 無相関

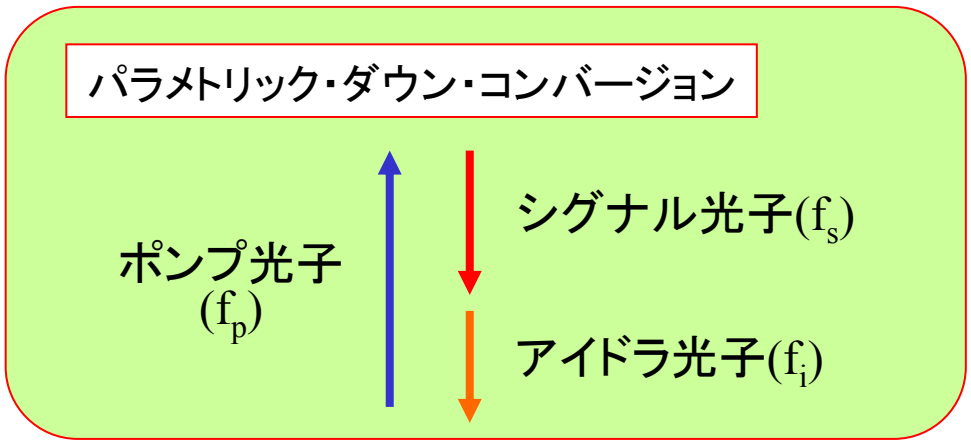
量子：観測するまで原理的に状態は不定

古典：原理的には状態は定まっている。観測しないだけ。

エンタングル光子対発生法

2次の光非線形効果を利用；$P = \chi_1 E + \chi_2 EE + \cdots$

$$E(f_1) + E(f_2) \rightarrow P(f_3 = f_1 + f_2) \rightarrow E(f_3)$$



同一偏波光子が必ず対で発生
（typeI位相整合の場合）

$$|\psi> = |H>_s |H>_i$$

ポンプ光

非線形媒質 → 非線形媒質

$|H>_s|H>_i$ → $|V>_s|V>_i$

$|H>_s|H>_i$ or $|V>_s|V>_i$

with appropriate pump power

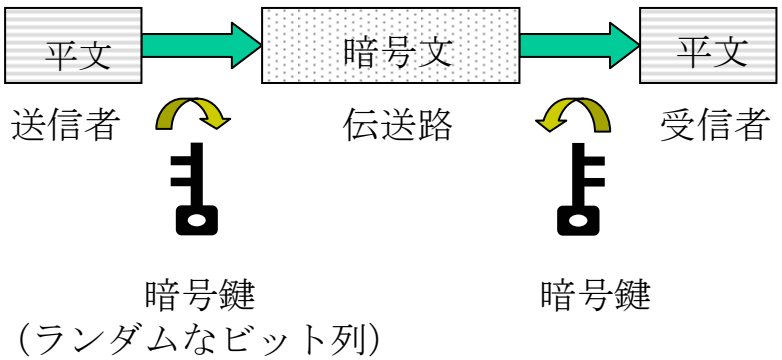
$$|\psi> = \frac{1}{\sqrt{2}}(|H>_s|H>_i + |V>_s|V>_i)$$

[内容]

1. 量子情報通信で利用する量子力学
2. **量子暗号**
3. 量子テレポーテーション他
4. 基本デバイス

量子暗号（量子鍵配送）

（秘密鍵暗号通信）



暗号鍵を1回しか使わなければ絶対に安全

目的

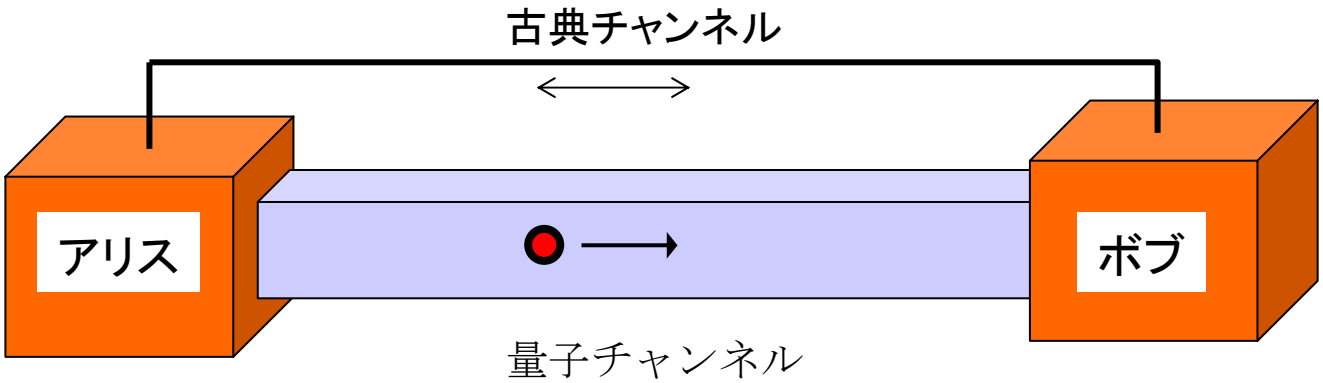
量子力学的に秘匿性が保証された秘密鍵を離れた2者に供給

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。）

量子暗号の基本構図



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生秘密鍵生成

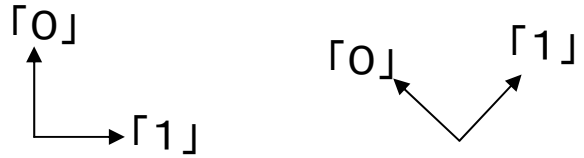
④誤り訂正・プライバシー増幅 → 最終秘密鍵

前提

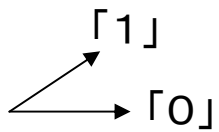
盗聴者は、量子チャンネルに対しては盗聴・改ざんができる。
古典チャンネルに対しては盗聴のみ。

各種量子暗号方式

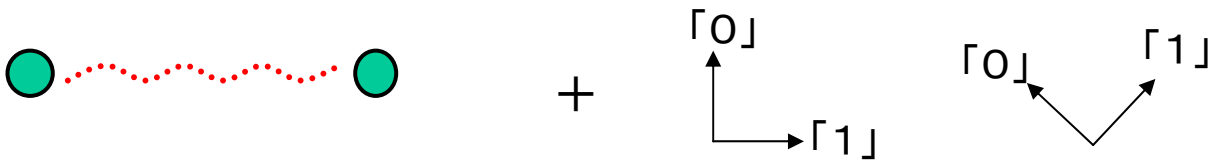
BB84　2つの非直交基底系



B92　2つの非直交状態

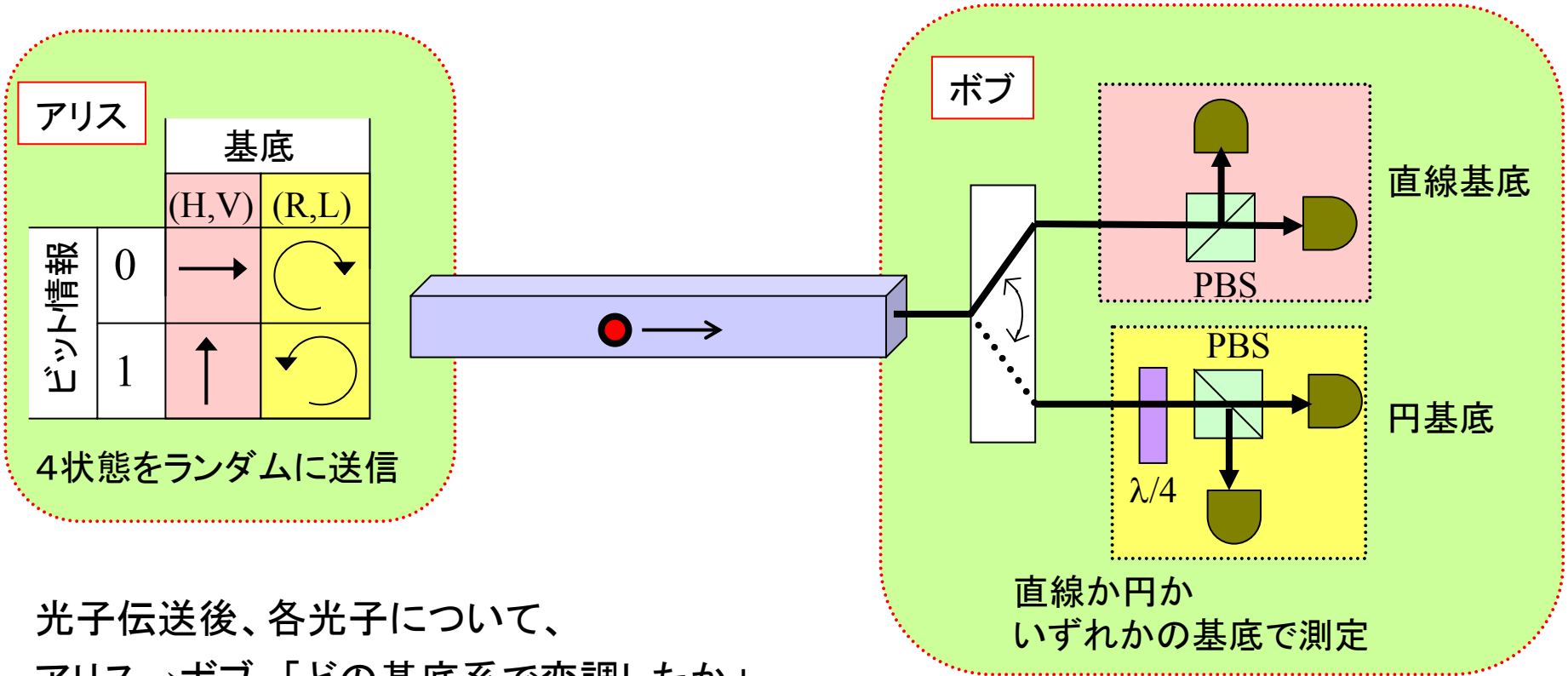


BBM92　エンタングル光子対（2つの非直交基底系利用）



E91　エンタングル光子対（ベル不等式利用）

BB84方式 (by Bennett and Brassard in 1984)



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

誤り訂正

Block Parity

$$X = 110101$$

$$p = \left(\sum_i X_i \right) \bmod 2$$

$$= \begin{cases} 0 & \text{Even number of 1's} \\ 1 & \text{Odd number of 1's} \end{cases}$$

Basic Idea (Block parity check)

$X =$	1	1	0	0	0	1	0	1	0	0	1	0	1	1	1 0
$p_x =$			0				0				1				1
$Y =$	1	1	0	1	0	1	0	1	0	0	1	0	0	0	1 0
$p_Y =$			1				0				1				1

- Error correction done by public discussion.
- Each exchanged parity bit is 1 bit of leaked information
- Want to find all errors with minimum block parity exchange

Noiseless Coding Theorem

Given:

$$U = f(X) \quad H(X \mid YU) \approx 0$$

$$\log_2 |U| = \kappa$$

Then:

$$\lim_{N \to \infty} \frac{\kappa}{N} \geq h(e)$$

プライバシー増幅

- Even with small error rate Eve can learn non-negligible fraction of key.
- Privacy amplification compresses raw key to shorter completely secure key.
- Amount of compression depends on how much information was leaked.

Simple Algorithm

$$X = \boxed{1\ 1\ 0\ 0}\ \boxed{0\ 1\ 0\ 1}\ \boxed{0\ 0\ 1\ 0}\ \boxed{1\ 1\ 1\ 0}$$

$$K = \quad 0 \qquad 0 \qquad 1 \qquad 1$$

General Algorithm

G – Set of functions which map N bit strings to r bit strings.

Step 1: Randomly pick function g from class G
Step 2: Compress key:

$$K = g(X)$$

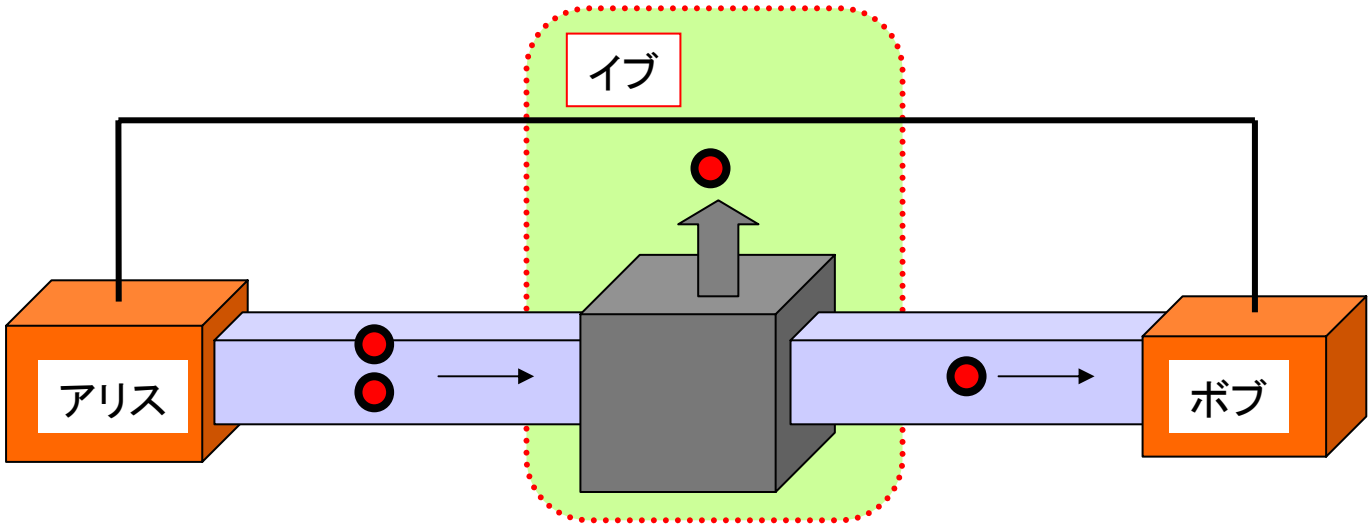
BB84

Uncertainty principle can provide a bound on necessary compression.

$$r \le -N \log_2 \left(\frac{1}{2} + 2e - 2e^2 \right) - \kappa$$

盗聴法1: beam splitting attack（盗み聞き）

伝送路を分岐して信号光の一部を盗む



・光子を1個ずつ送れば、取られた光子はボブには届かない→秘密鍵にはならない
・ただしレーザ光の場合、ポワソン分布にしたがって有限の確率で2光子/パルス

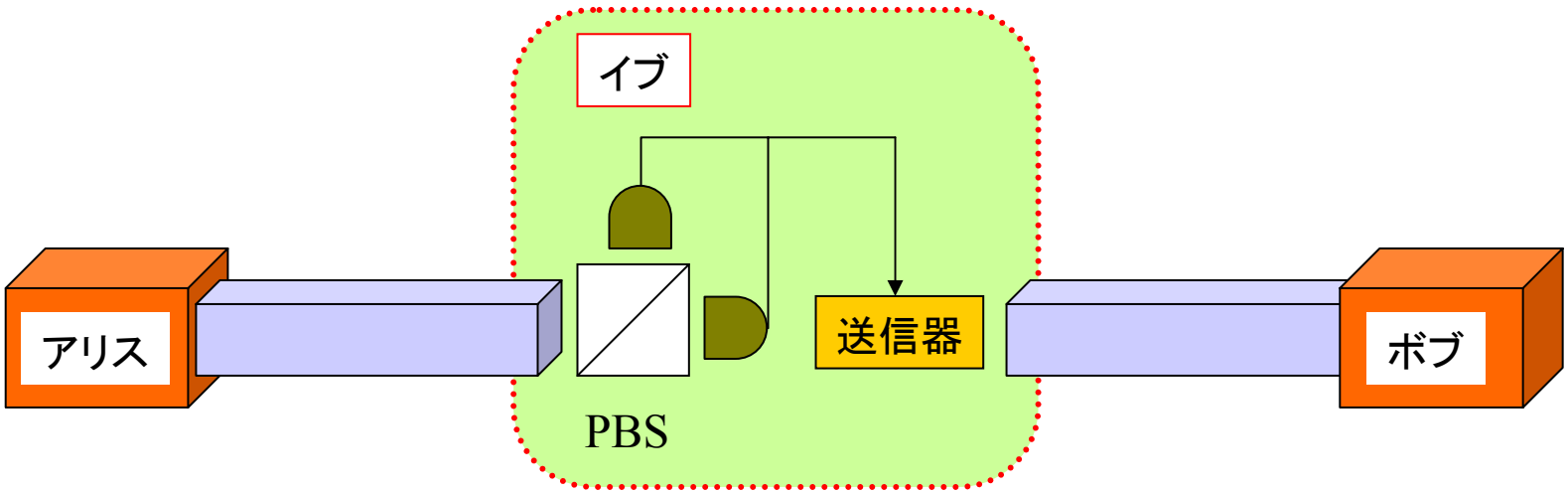
イブ

①2光子を含んでいるパルスを検知
②そのうちの1光子をタッピングし、保存
③古典チャンネルでの情報交換を盗聴し、それに基づき保存してる光子を測定

減衰レーザ光（e.g.,平均0.1光子/パルス）＋データ処理（プライバシー増幅）で対処

盗聴法2: intercept/resend attack （なりすまし）

伝送路をカット → 伝送信号を受信 → 受信結果に基づいて偽装信号を送信



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

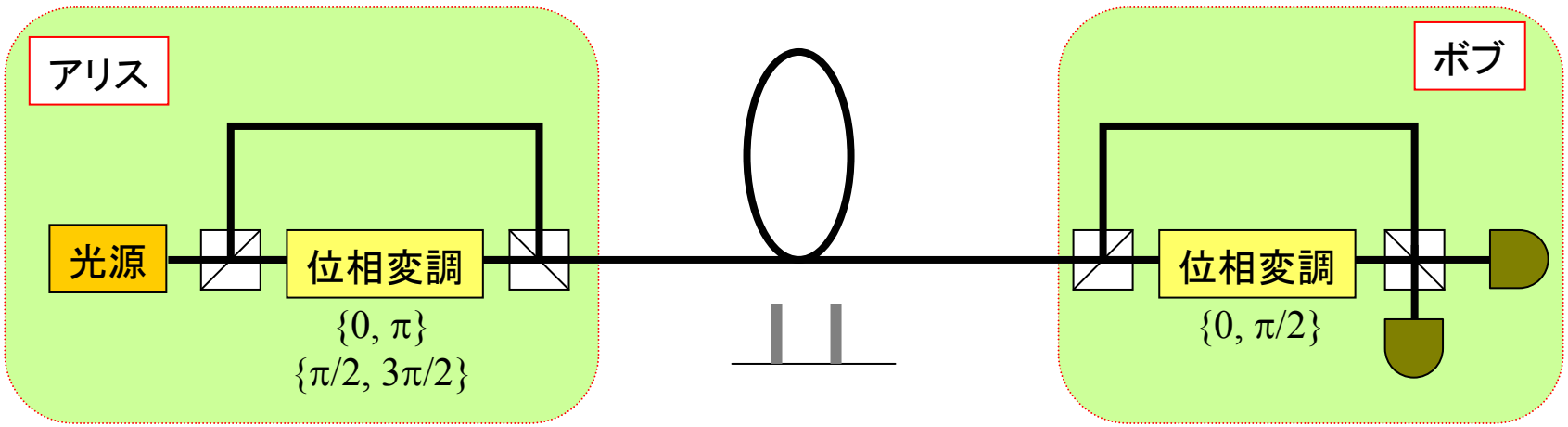
不一致の場合 → 1/2の確率で誤り → テストビットチェックにより盗聴発覚

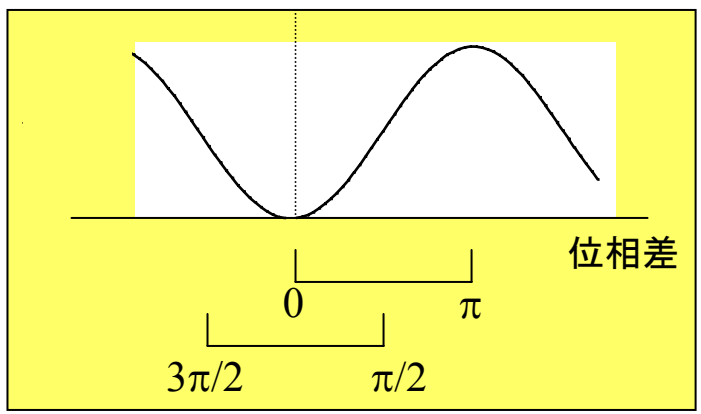
誤りがなければ安全

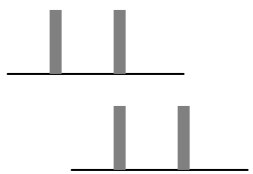
位相エンコードBB84

直線偏波・円偏波変調は直交2成分の位相差を{0, π/2, π, 3π/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

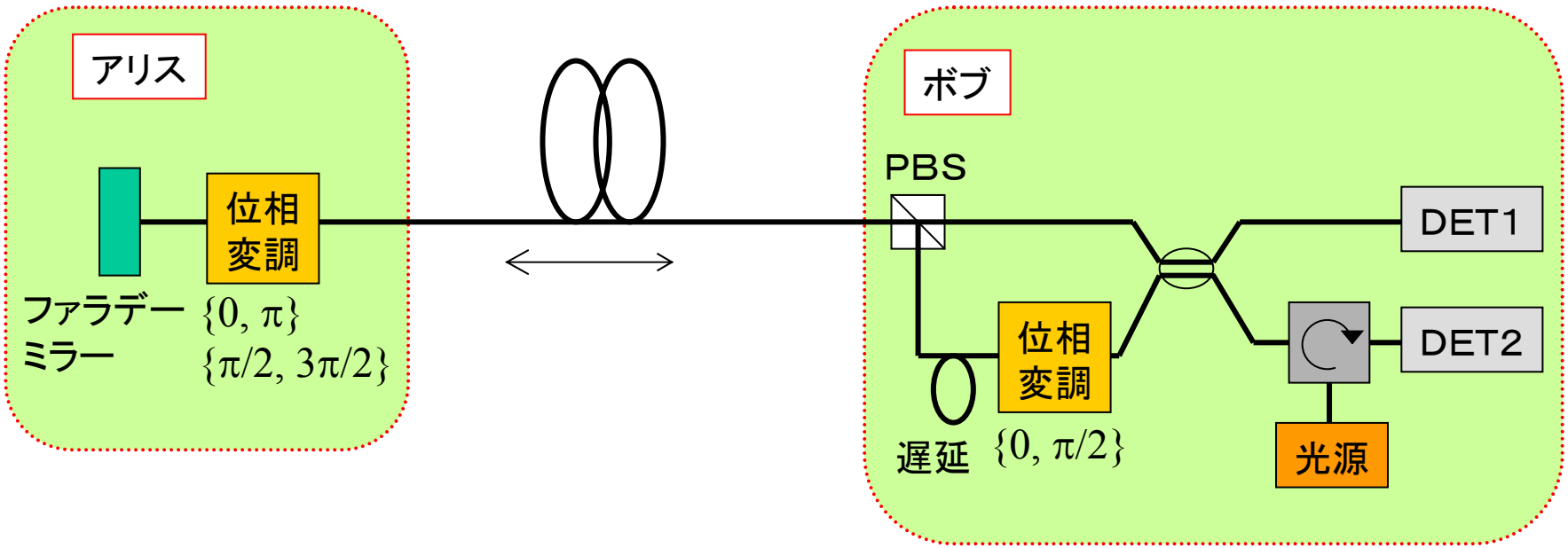






Plug & Play システム

光を折り返す構成によりファイバの偏波変動を自動補償



偏波の縦・横成分を時系列に分けて送信後、合波

アリス位相変調；$\{0, \pi\}$ ⇔ 直線偏波系、$\{\pi/2, 3\pi/2\}$ ⇔ 円偏波系

ボブ位相変調；0 ⇔ 直線偏波系選択、π ⇔ 円偏波系選択

実験例

伝送距離 (km)	鍵供給速度 (bit/s)	機関	年
30	260	British Tel.（英）	1995
48	10	Los Alamos研（米）	2000
40(80)	10(2)	Heriot-Watt大（英）	2001
67	50	Geneva大 （スイス）	2002
100	< 5	NEC（日）	2003

課題:

・ファイバ伝送波長帯の光子検出器（効率、ダークカウント、繰り返し周波数）

・レーリ散乱（plug&playの場合）

・偏波 or 干渉計の制御・安定性（一方向の場合）

・単一光子光源の開発

[内容]

1. 量子情報通信で利用する量子力学
2. 量子暗号
3. 量子テレポーテーション他

   量子中継、Dense Coding、量子符号化

4. 基本デバイス

量子テレポーテーション

目的　A点にある量子状態をB点で再現しよう

↓(but)

量子状態は1回測定では不確定かつ収縮

ファックスのように別の媒体に焼き直して転送することは不可

↓（そこで）

量子エンタングルメントを利用

応用

量子コンピュータ間を結ぶ量子ネットワーク

量子中継

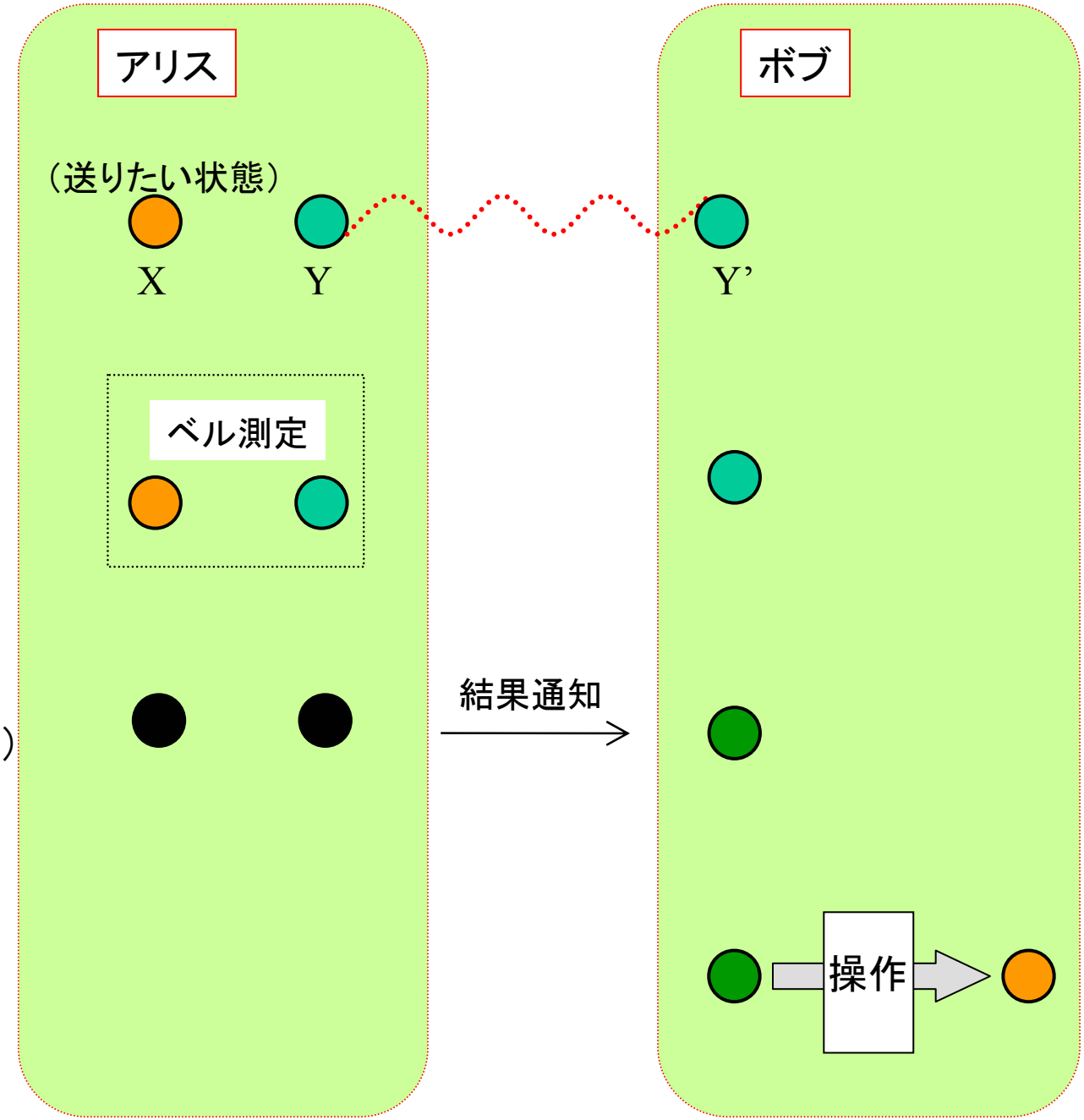
手順

①AとBはエンタングル対の片方ずつを保有
（YとY’には相関）

②Aは転送元状態とエンタングル量子とを一括測定
（XとYの相対関係を測定）

③AはBへ測定結果を通知
（XとY’の相対関係がわかる）

④Bは測定結果に基づいてエンタングル量子を操作
→転送元状態が再現



状態X（転送元）：$|\phi>_X = a|H>_X + b|V>_X$

状態Y、Y’（エンタングルメント）：$|\psi>_{YY'} = \frac{1}{\sqrt{2}}(|V>_Y|H>_{Y'} - |H>_Y|V>_{Y'})$

↓

全状態：
$$|\Psi>_{XYY'} = \frac{a}{\sqrt{2}}(|V>_X|V>_Y|H>_{Y'} - |V>_X|H>_Y|V>_{Y'}) + \frac{b}{\sqrt{2}}(|H>_X|V>_Y|H>_{Y'} - |H>_X|H>_Y|V>_{Y'})$$

↓

（状態X＋Yの基底系で展開）

$$\begin{cases} |\Psi^{(\pm)}>_{XY} = \frac{1}{\sqrt{2}}(|V>_X|V>_Y \pm |H>_X|H>_Y) \\ |\Phi^{(\pm)}>_{XY} = \frac{1}{\sqrt{2}}(|V>_X|H>_Y \pm |H>_X|V>_Y) \end{cases}$$

$$|\Psi>_{XYY'} = \frac{1}{\sqrt{2}}\{|\Psi^{(+)}>_{XY}(a|V>_{Y'} - b|H>_{Y'}) + |\Psi^{(-)}>_{XY}(a|V>_{Y'} + b|H>_{Y'}) + |\Phi^{(+)}>_{XY}(-a|V>_{Y'} + b|H>_{Y'}) + |\Phi^{(-)}>_{XY}(-a|V>_{Y'} - b|H>_{Y'})\}$$

↓

（状態X＋Yを2状態基底系で測定＝ベル測定）

↓

4状態のどれかひとつに収縮

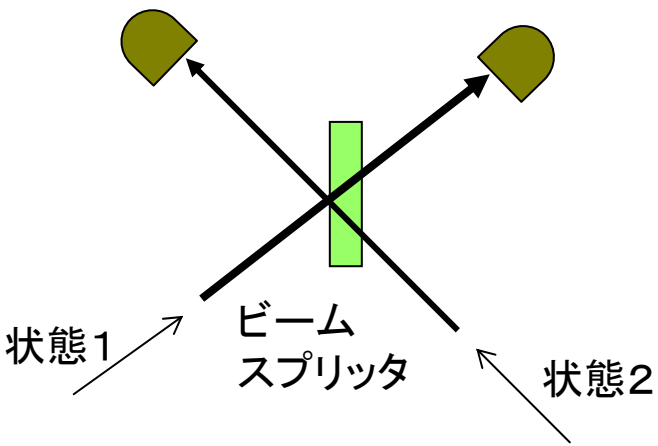
↓

ベル測定結果に応じて状態Y’を変換 → 状態Xと同じ状態

ベル測定

2状態系の基底状態への射影

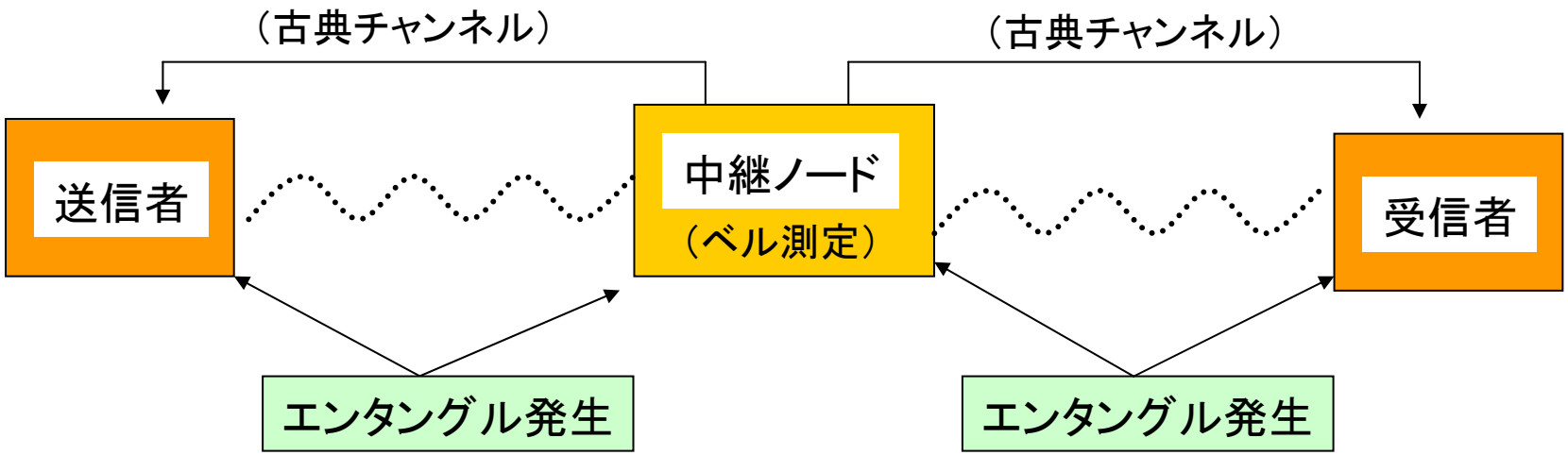
$$
\begin{cases}
|\Psi^{(+)}\rangle_{12} = \dfrac{1}{\sqrt{2}}(|V\rangle_1|V\rangle_2 + |H\rangle_1|H\rangle_2) \\
|\Psi^{(-)}\rangle_{12} = \dfrac{1}{\sqrt{2}}(|V\rangle_1|V\rangle_2 - |H\rangle_1|H\rangle_2) \\
|\Phi^{(+)}\rangle_{12} = \dfrac{1}{\sqrt{2}}(|V\rangle_1|H\rangle_2 + |H\rangle_1|V\rangle_2) \\
|\Phi^{(-)}\rangle_{12} = \dfrac{1}{\sqrt{2}}(|V\rangle_1|H\rangle_2 - |H\rangle_1|V\rangle_2)
\end{cases}
$$



同時検出したら$|\Phi^{(-)}\rangle_{12}$と判定

- ボゾンなので$|\psi\rangle$ではない
- BSでの位相シフトを考慮すると$|\phi^{(+)}\rangle$ではない

量子中継



①エンタングルスワッピング（量子テレポーテーションの親戚）により
　送受信者に複数のエンタングル対（不完全）を供給
②複数の不完全なエンタングル対から完全なエンタングル対を再生（エンタングル純粋化）
③送受信者に同じ量子状態

量子Dense Coding

光子１個で2ビット情報を送る

①アリスとボブがエンタングルメントの一方ずつを保有

$$|\Psi^{(+)}>=\frac{1}{\sqrt{2}}(|V>_1|V>_2+|H>_1|H>_2)$$

②アリスは1に次のどれかを施す

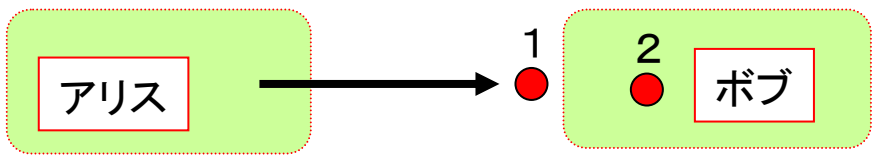
(a) 何もしない ⟶ $|\Psi^{(+)}>=(|V>_1|V>_2+|H>_1|H>_2)/\sqrt{2}$

(b) |V>と|H>との間に位相差π ⟶ $|\Psi^{(-)}>=(|V>_1|V>_2-|H>_1|H>_2)/\sqrt{2}$

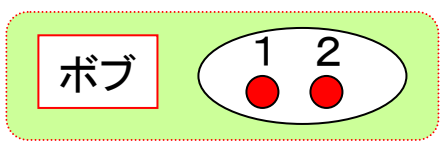
(c) |V>と|H>を入れ替え ⟶ $|\Phi^{(+)}>=(|H>_1|V>_2+|V>_1|H>_2)/\sqrt{2}$

(d) |V>と|H>を入れ替え＋位相差π ⟶ $|\Phi^{(-)}>=(|H>_1|V>_2-|V>_1|H>_2)/\sqrt{2}$

③アリスはボブに1を送信



④ボブは(1+2)をベル測定→4状態のどれであるかを判定



$|\Psi^{(+)}>\Leftrightarrow(00)$, $|\Psi^{(-)}>\Leftrightarrow(01)$, $|\Phi^{(+)}>\Leftrightarrow(10)$, $|\Phi^{(-)}>\Leftrightarrow(11)$,

↓

2ビット情報

量子符号化

前提：光子１個レベル以下で古典ビット列を送るシステム

↓

受信端で識別エラー

↓

冗長度をもたせてブロック符号化（誤り訂正符号化）しよう

↙ ↘

古典

各ビットを個別測定し復号化

$$X = [0 \;\; 1 \;\; 1 \;\; \cdots \;\; 0]$$

個別測定

量子

ブロックを一括測定して復号化

$$|\Psi> = \underbrace{|\psi_1> \otimes |\psi_2> \otimes \cdots |\psi_k>}$$

一括測定（エンタングル操作）

必要なビット数　＞　必要なビット数

1. 量子情報通信で利用する量子力学
2. 量子暗号
3. 量子テレポーテーション他
4. **基本デバイス**

    光子検出器

    単一光子光源

光子検出器

通常、APD（アバランシェ・フォトダイオード）を使用

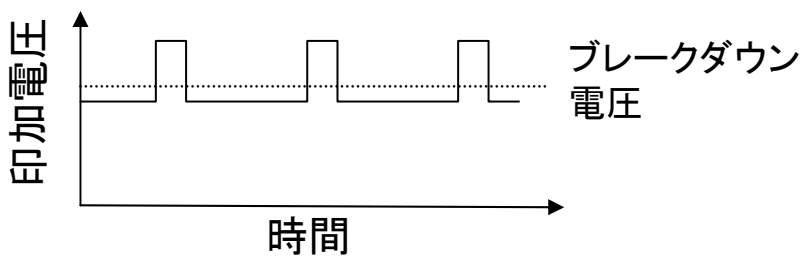
求められるのは、高量子効率、低ダークカウント、高繰り返し（アフターパルス）

短波長帯：市販のSi-APDあり

量子効率 ～ 50%、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

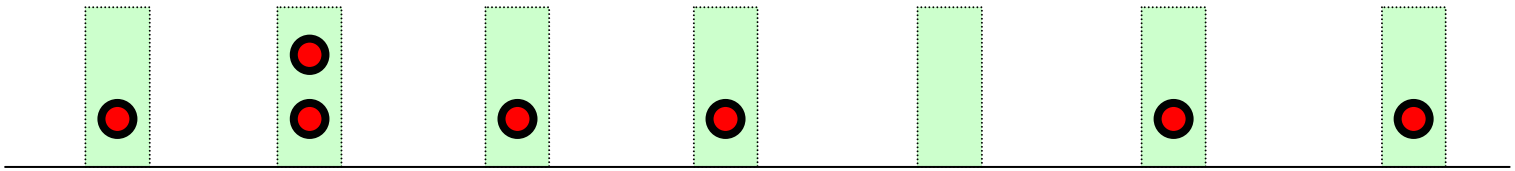
量子効率 ～ 10%、ダークカウント～10^{-5}/gate、繰り返し ＜ 1MHz



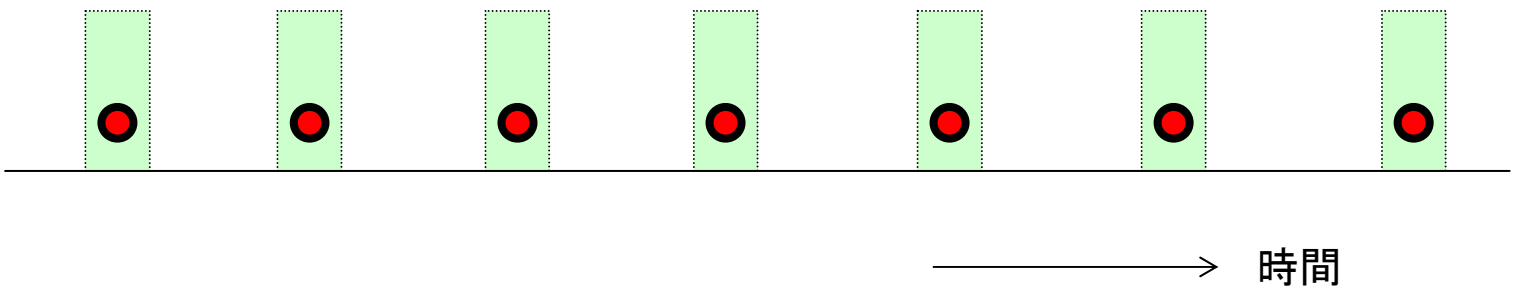
単一光子光源

量子光通信では、光子1個ずつを扱うのが基本

レーザ光（ポワソン分布）

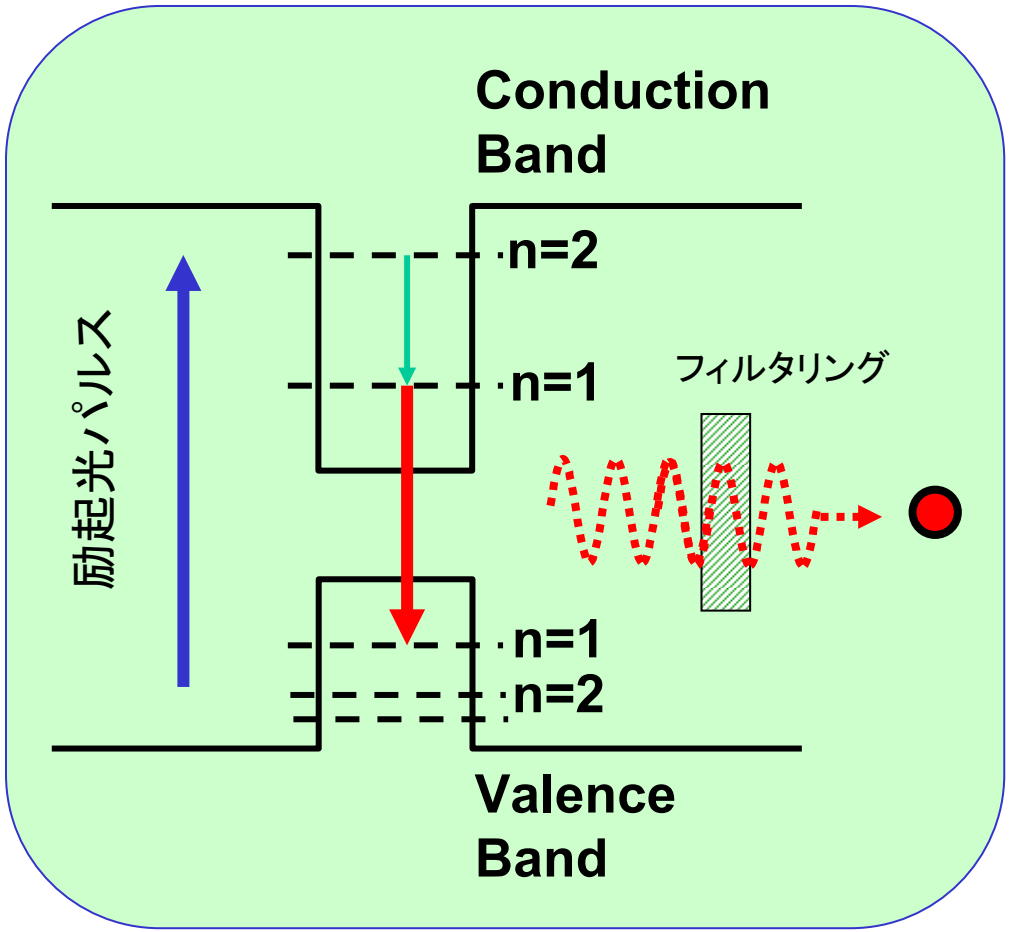


単一光子光（サブポワソン）



半導体量子ドット光源 (@ Stanford University)

量子ドットを数Kに冷却　→　原子likeなエネルギー準位



ひとつの準位に1個の励起子

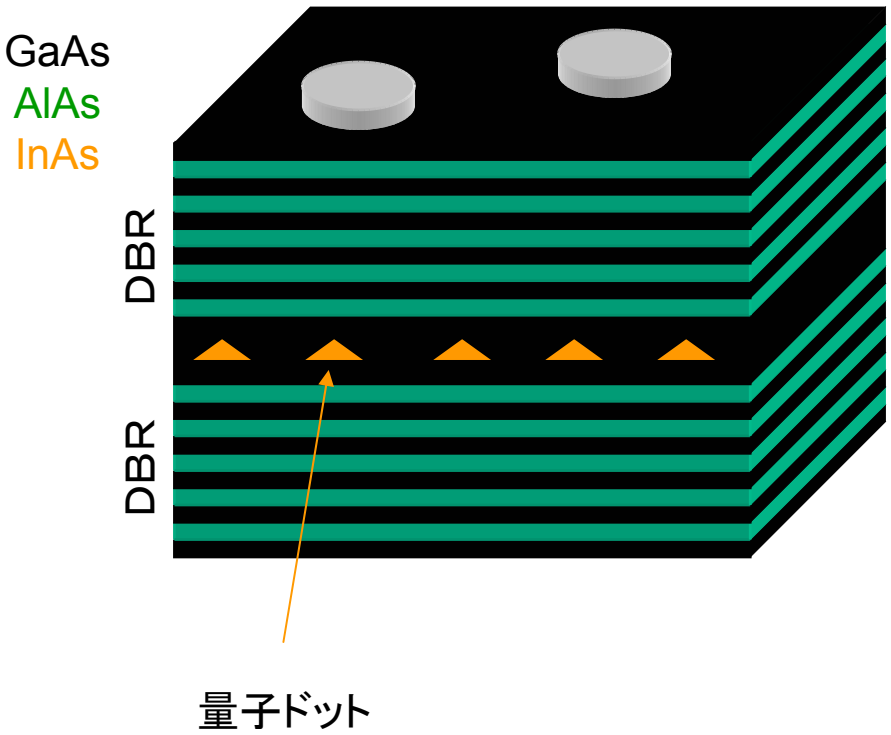
↓

特定の準位間からの自然放出光子は1個

↓

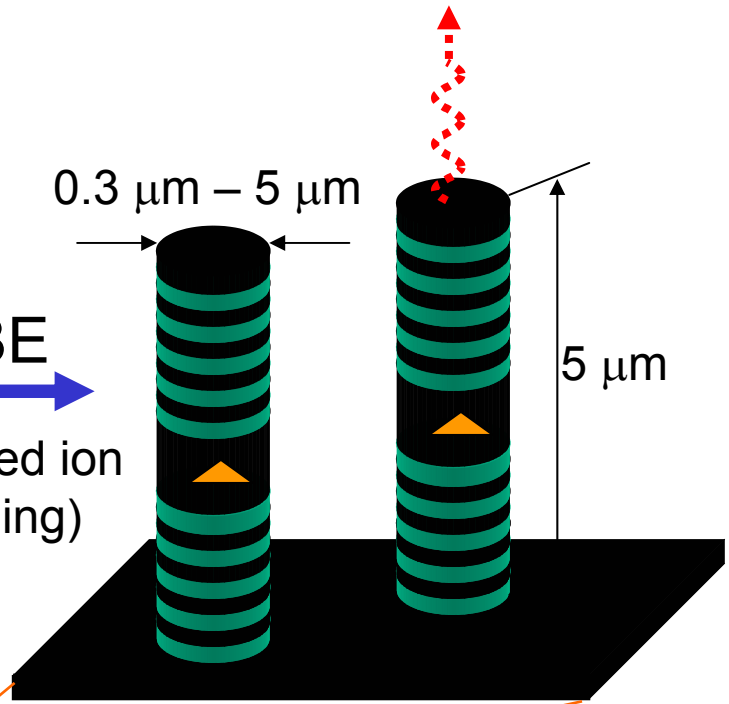
フィルタリングにより1光子/パルス

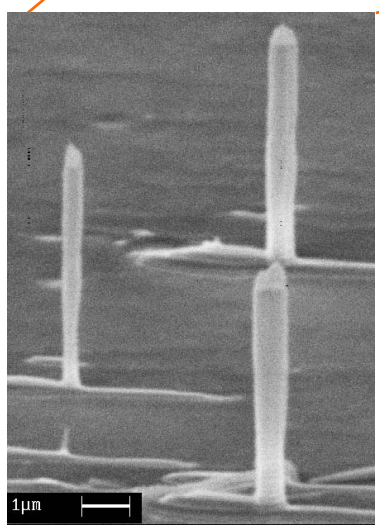
作製



CAIBE

(Cl_2 assisted ion beam etching)





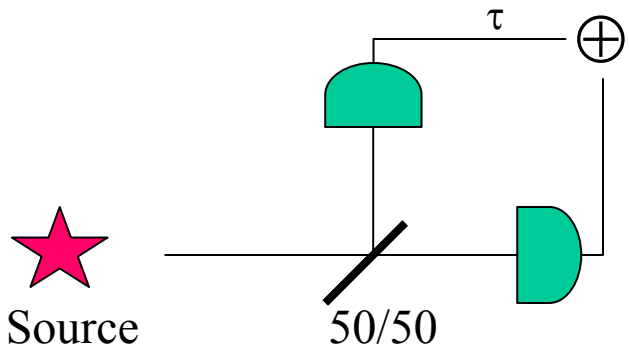
1μm

自然放出光子を効率良く取り出すために

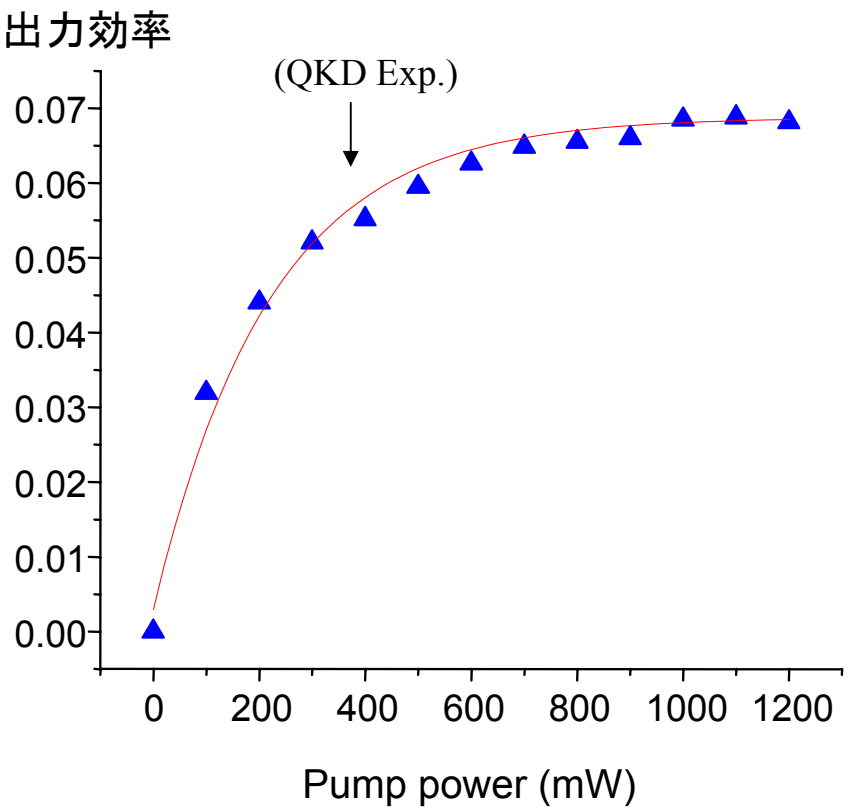
ポスト型マイクロ共振器を形成

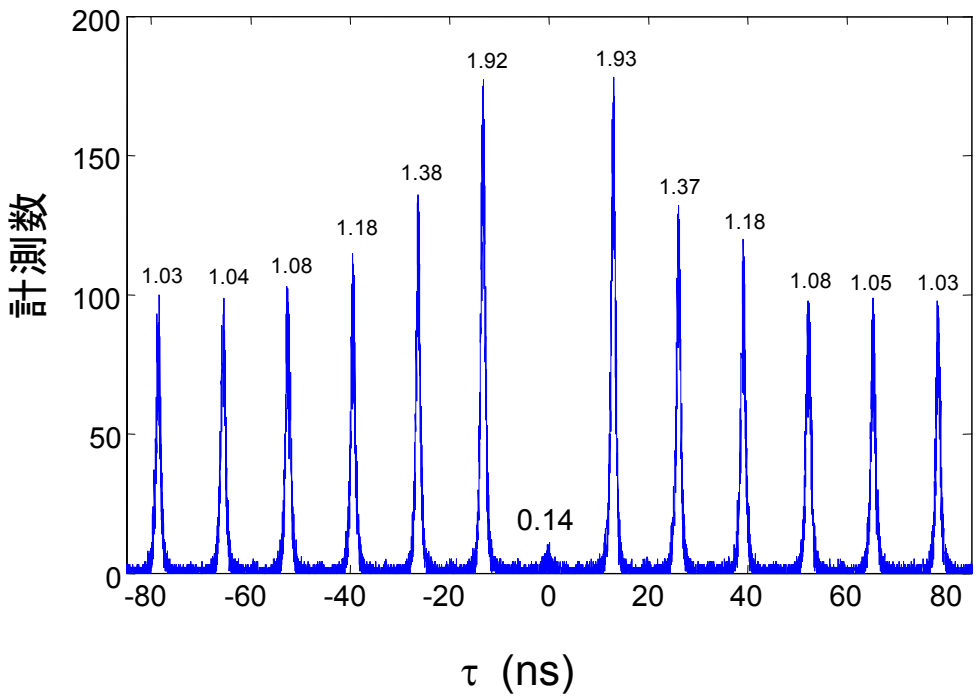
出力特性

同時計数

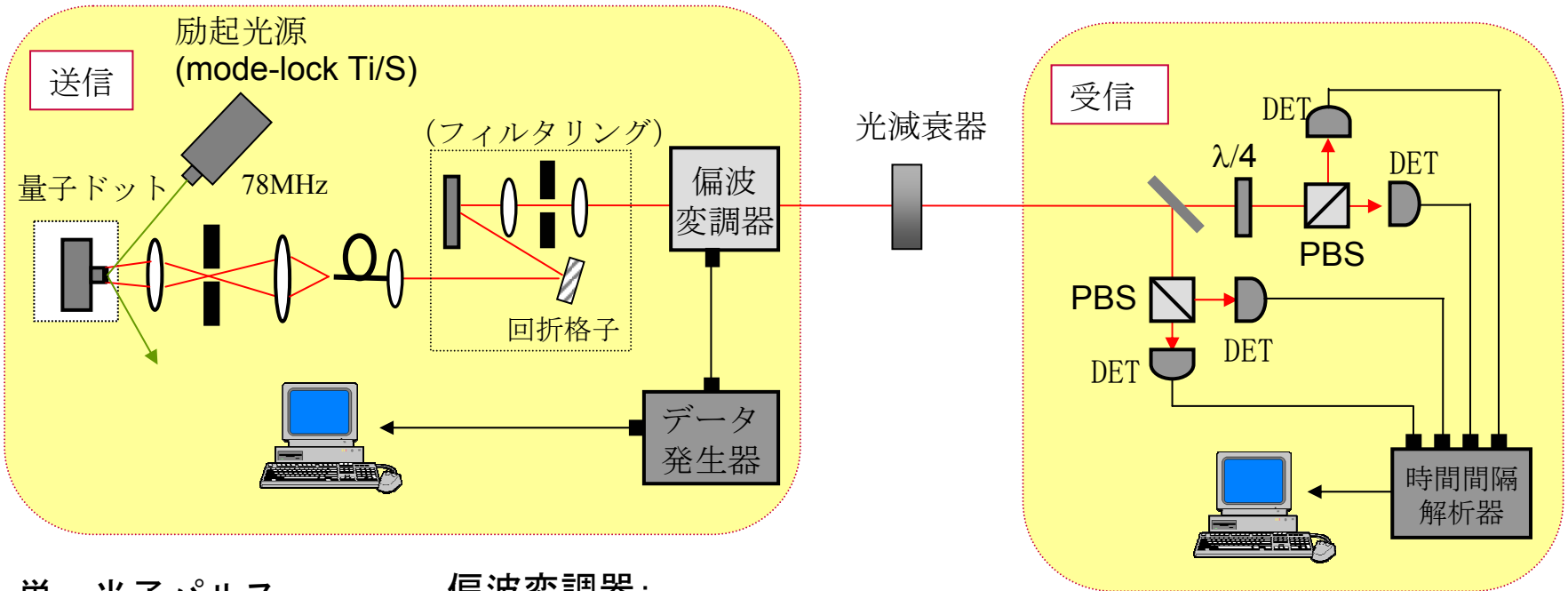


saturation curve





単一光子光源を用いた量子暗号実験

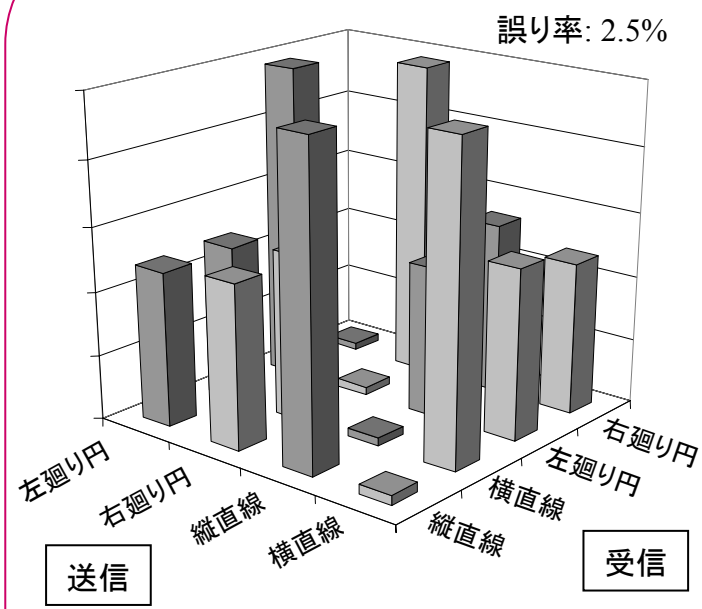


単一光子パルス:
波長＝900nm
パルス幅＝2~300ps

偏波変調器:
{縦・横}{右廻り・左廻り}
の4偏波にランダム変調

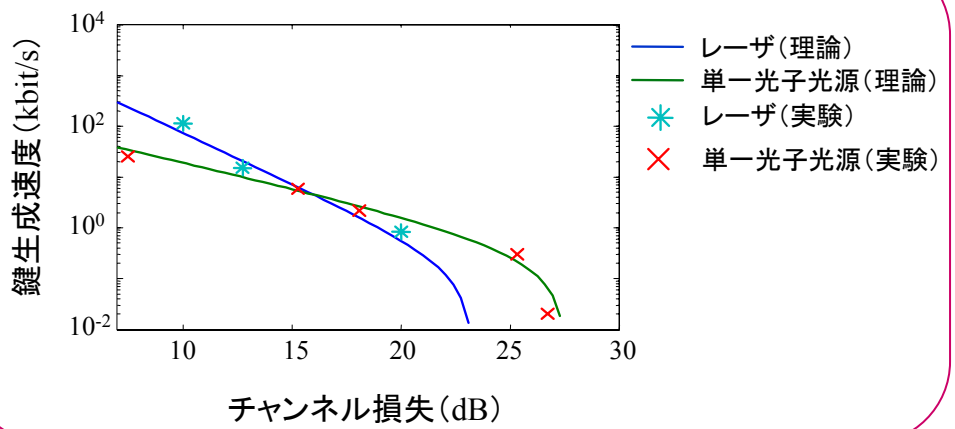
実験結果

送受信間の相関

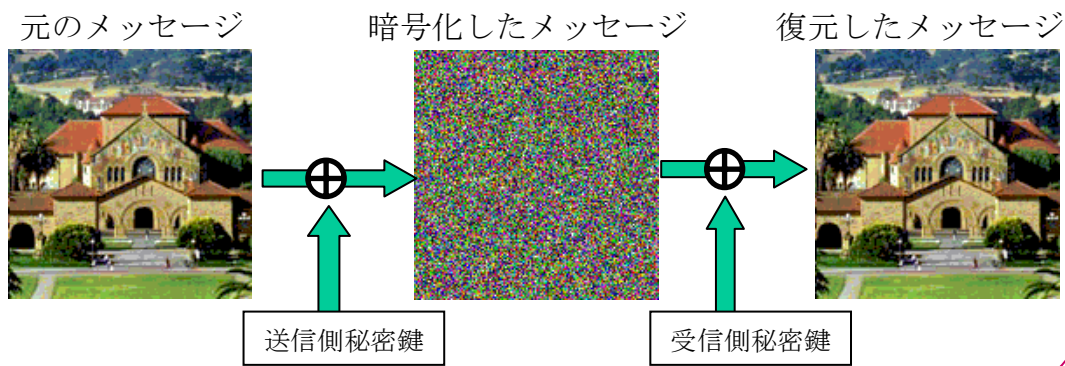


基底が一致→100%の相関
基底不一致→50%の相関

単一光子光源とレーザ光源との比較



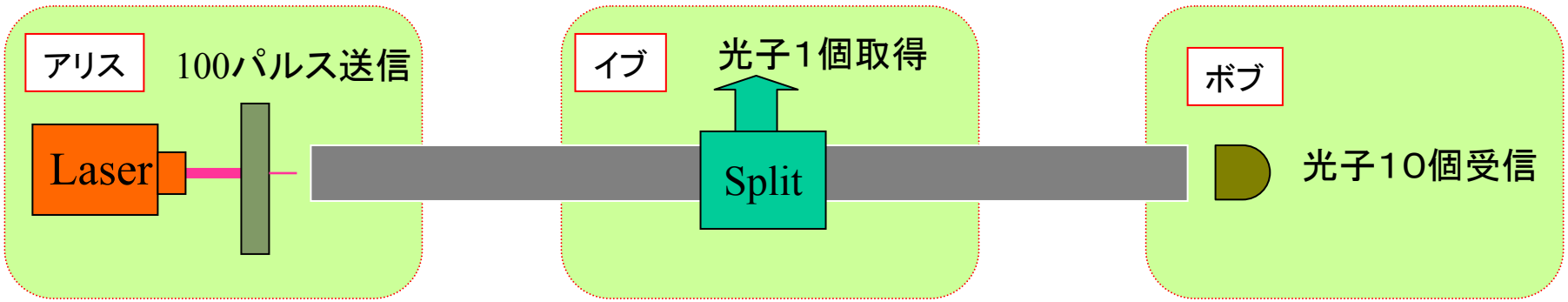
暗号化デモンストレーション



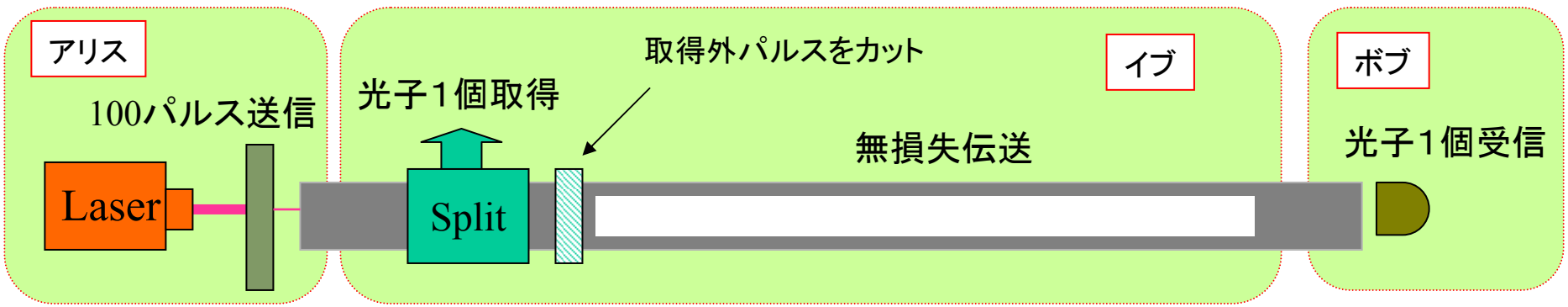
コヒーレント光に対する beam splitting attack

例えば、アリスは0.1光子/パルス送信、1/100の確率で1パルスに2光子存在

伝送損失小（近距離）



伝送損失大（10dB）



弱コヒーレント光は伝送損失大の場合、盗聴に弱い。

量子情報通信

1. 量子情報通信で利用する量子力学
   - 状態と観測問題
   - 量子エンタングルメント

2. 量子暗号

3. 量子テレポーテーション他
   - 量子中継、dense coding、量子符号化

4. 基本デバイス
   - 光子検出
   - 単一光子光源