量子光通信

ー光通信研究者から見てー

NTT物性科学基礎研究所

井上　恭

[内容]

1. 量子暗号
2. 量子テレポーテーション
3. 基本デバイス – 単一光子光源 –

情報通信技術
量子通信

暗号システムなど柱

総務省の研究推進会議 2020年実現へ工程表

総務省の「量子情報通信研究推進会議」（江崎玲於奈座長＝芝浦工業大学長）は20日、次世代通信と期待される量子情報通信ネットワークの2020年実現に向けた研究開発戦略を発表した。光の粒子にデータを載せて伝送する技術で、現行の光通信の限界速度を2倍以上にできるという。要素技術開発が進められており、初めて目標年度を定めた開発ロードマップ（行程表）を報告した。

量子情報通信技術は1・5ミリ単位の光粒子でデータを伝送する技術。光の波動で伝送する現行の光通信に比べ、安全性が高いうえに大容量の通信ができるようになる。

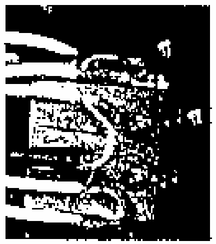
今回の研究開発戦略では、量子情報通信の第1世代となる暗号システム、第2世代の通信衛星光化技術、第3世代の量子中継や量子分散処理ネットワークなどを、20年までに段階的に実現する方針だ。

量子情報通信技術は90年代から欧米を中心に研究が進んでいる。すでに第1世代の量子暗号は5年以内の実用化が視野に入っているという。総務省は01年に同会議を立ち上げ、推進方策を検討してきた。今回の開発戦略を基に、中核となる研究開発拠点の設置や国際的な連携を進める。

量子暗号を長距離伝送

東芝・NECなど100キロ超に成功

盗聴やすきんを完全に防げる「量子暗号通信」で百キロ㍍を超える長距離を伝送することに東芝とNECなどが相次いで成功した。量子暗号の実用化に道を開く成果。一方、量子暗号技術を部分的に取り入れて従来の通信の安全性を高めるシステムを米欧のベンチャー企業が年内にも売り出すなど、世界的に開発競争が本格化している。



NECが開発した量子暗号通信システム受信器の心臓部

盗聴完全防御、実用化に道

NECと科学技術振興事業団、通信・放送機構の共同研究グループと、東芝欧州研究所（英ケンブリッジ）はそれぞれ、量子暗号通信の情報の担い手である光の粒（光子）を感知する高感度の検出器を開発。これを受信側に組み込むなどの工夫で、従来不可能だった百キロ㍍を超える通信に成功した。

NECなどは既存の光ファイバーを用いて百㌔㍍を伝送。東芝欧州研は付帯設備が低い高性能光ファイバーを使って百㌔㍍の通信に成功した。

いずれも通常の光通信用の波長一・五五㍃（㍃は百万分の一）㍍の光を用いた。

量子暗号通信は、現在の光通信のように信号を途中で増幅することができないため、光ファイバー内で光子がなくなったり受信側で検出し損ねるなどの問題があり、長距離伝送が難しかった。

東芝欧州研のA・シールズ・グループ長は「検出器をさらに改良することで伝送距離を二百㌔㍍まで延ばせる」と話す。それ以上の長距離通信には、新たな半導体素子の開発などの新技術が必要という。

▼量子暗号　現在の暗号とは全く異なる原理を使った暗号技術。情報を光の最小単位である光子一個一個に載せて送る。盗聴されると、送った情報にその痕跡が残るのが特徴。送信側と受信側が暗号の鍵となる秘密の符号を事前に共有する「共通鍵暗号」に応用する場合、鍵をこの技術を用いて伝送。盗聴の痕跡が無いことを確認し使えば通信の秘密を確実に保てる。

米欧ベンチャー　システムを販売
従来通信に応用

量子暗号通信の実用化をにらみ、米欧のベンチャー企業が従来の通信技術を改良、今年中にも相次いでシステムを販売する見通しだ。

米MagiQ社（本社ニューヨーク）は、従来の暗号通信に量子暗号を組み合わせることで、高い安全性と経済性を兼ね備えた暗号通信システムを開発した。量子暗号を使って暗号鍵を伝送するのが特徴。

鍵を瞬間使い捨てにするので将来の量子暗号のような一〇〇%の安全性は得られないが、頻繁に新しい鍵を盗聴の心配なく送れるため、安全性は飛躍的に高まる。通信速度も普通の光通信と同等だ。

すでにサンプル出荷を始めたのが、スイス・ジュネーブ大学からのスピンオフ企業、IDクワンティーク社も近く量子通信システムの販売に乗り出す見通し。

ただ、両社とも伝送距離は六十㌔㍍程度とみられる。MagiQは企業内の比較的近い拠点間で専用線のように使う「仮想私設網（VPN）」などに搭載する（A・ハモンド副社長）考えだ。

主要都市間などを結ぶシステム作りには東芝などが進めている伝送距離の大幅延長が不可欠。米IBMも素子の開発に取り組んでいる。

量子暗号を高速伝送

科技振興事業団とNTTが開発　衛星通信利用に道

米スタンフォード大学の山本喜久教授などをリーダーとする科学技術振興事業団とNTTは、絶対に破れない未来の暗号である量子暗号を高速で効率良く伝送するシステムを開発、通信実験に成功した。量子暗号衛星通信の実現に道を開くという。

量子暗号では光子（光の粒）一つ一つに情報を乗せて送る。研究グループは光子を一個ずつ発生する素子を開発し、送信装置に組み込んだ。光子が複数出ることもある従来の素子に比べ、情報を効率よく伝送できる。

実験では、従来の十倍の毎秒二十㌔ビットでの情報伝送に成功した。伝送の途中で光が吸収・散乱されて弱まっても、元の光の〇・一五%が届けば安全性が確保できることを確認。従来方式の理論的な限界である〇・五%を破った。

盗聴不可能な「量子暗号」

伝送距離87キロメートル

三菱電機、世界最長を達成

三菱電機は十四日、原理的に盗聴が不可能な「量子暗号」による情報伝送で世界最長の八十七㌔㍍を達成したと発表した。既存の光ファイバー網を流用でき、すぐにでも実用化が可能という。国防や金融など通信の安全性が求められる分野での利用を見込む。

三菱電機の量子暗号システム

量子暗号は光子という光の粒子一個ずつに情報を乗せて伝送する。第三者が途中でのぞき見ると光子の状態が変化するので盗聴が検知できるため、解読が困難な暗号通信が可能になる。

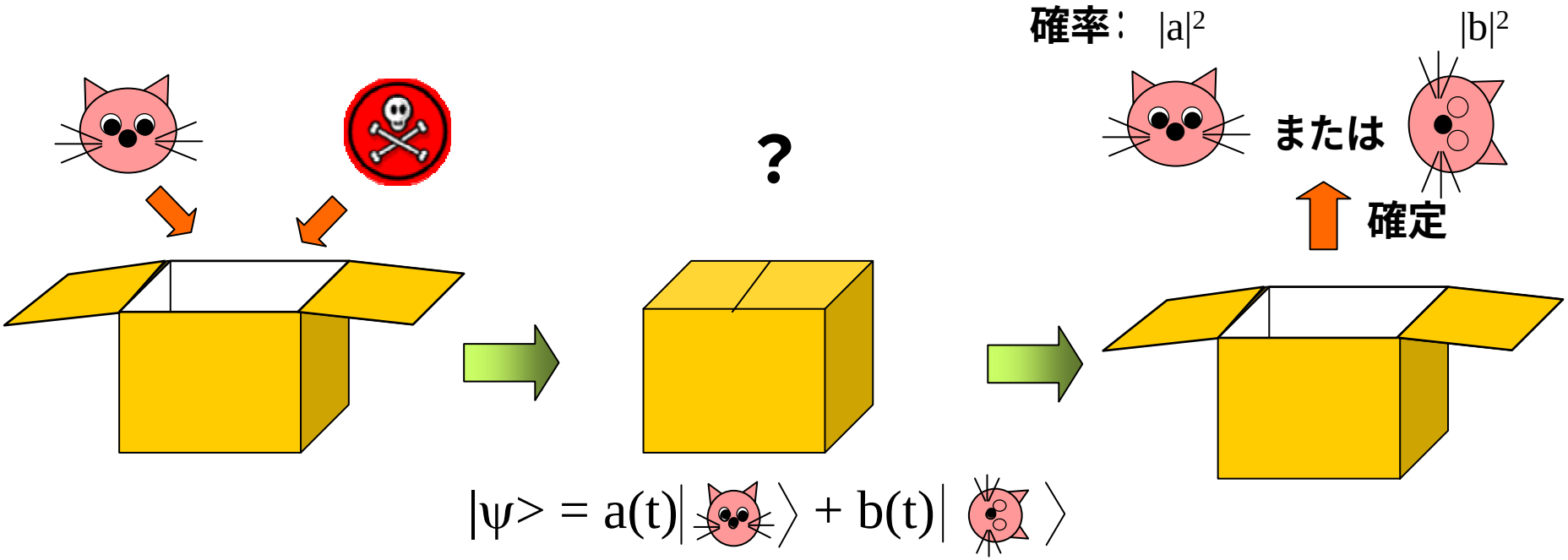
光子が光ファイバー中を通るうちに減衰、受信側で光子を検出できなくなるため、長距離通信が難しく、実用化の障害になっていた。

今回、光子検出に使う素子などを改良、[illegible]した。[illegible]間の距離に相当する八十七㌔㍍を達成。米ロスアラモス国立研究所の持つ四十八㌔㍍という記録を大幅に更新した。

三菱電機は伝送距離を延ばしたのに加え、伝送速度も実用上十分な性能を達成した。離れた二地点で通信する際、暗号化する側と元に戻す側で共通の鍵を使う従来の共通鍵暗号の方式を組み合わせ、情報量の小さい共通鍵の送受信にだけ量子暗号を使うことで伝送速度を向上した。

三菱電機はさらに伝送距離を延ばす研究や実際のシステムに組み込んだ実証実験を進める。通信・放送機構の委託研究で開発を進めた。

シュレディンガーの猫



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

一般的には

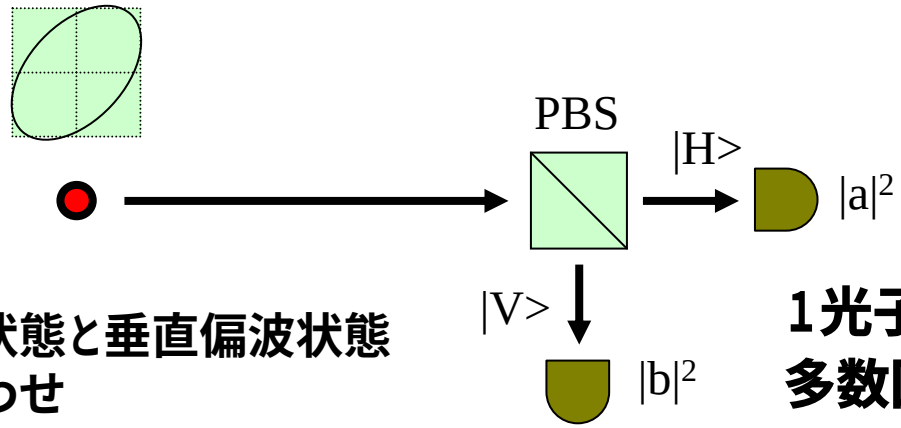
$|\psi\rangle = a|X\rangle + b|Y\rangle$　　$\{|X\rangle, |Y\rangle\}$**は直交基底系**　$(\langle X|Y\rangle = 0)$

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

量子情報ではこの性質をもっぱら利用

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$|a|^2 : |b|^2$の計測数

↓

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）

↓

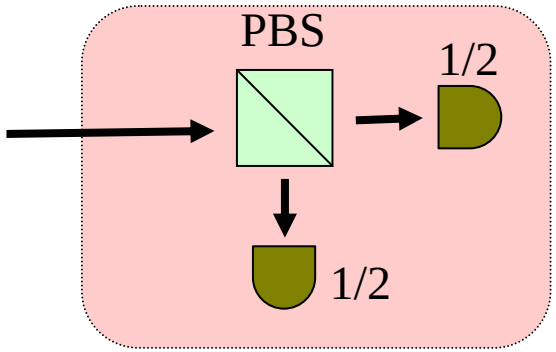
量子暗号に利用

（と難しく言わなくても）
状態が複数のパラメータを備えていれば、
一回の測定では状態を特定できない。
偏波なら縦・横の成分比とその相対位相

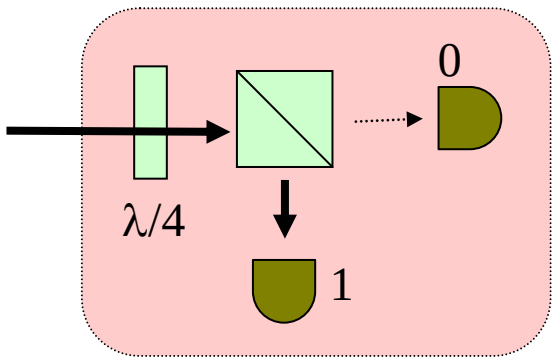
観測基底

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

$$= |R\rangle$$



直線偏波基底



円偏波基底

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

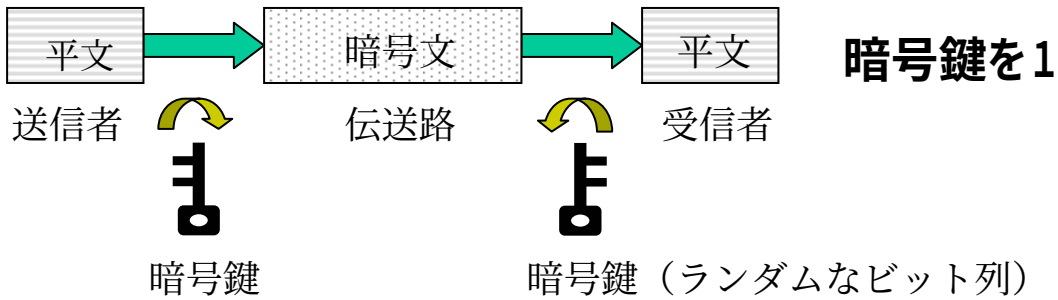
$$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$$

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

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

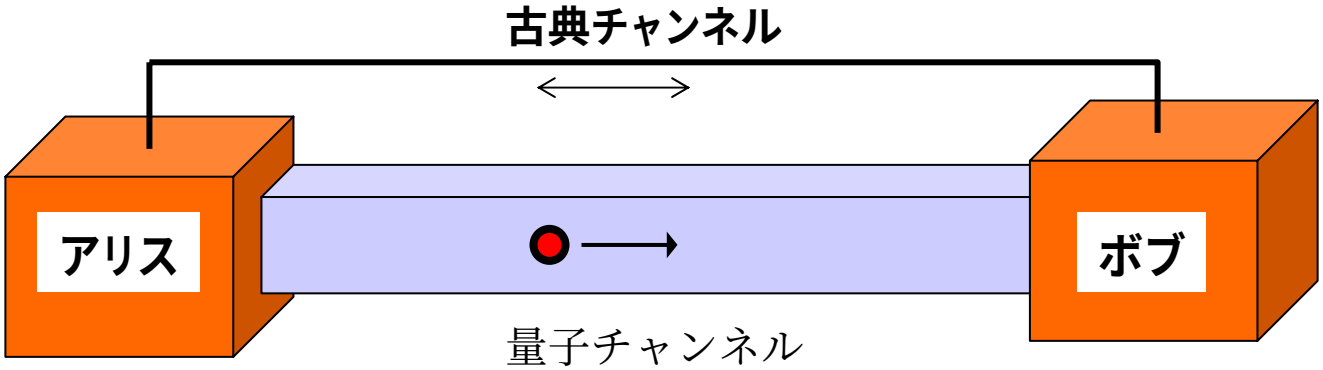
売り文句

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。）

？　どんなに非現実的な盗聴手段でもＯＫ

量子暗号の基本構図



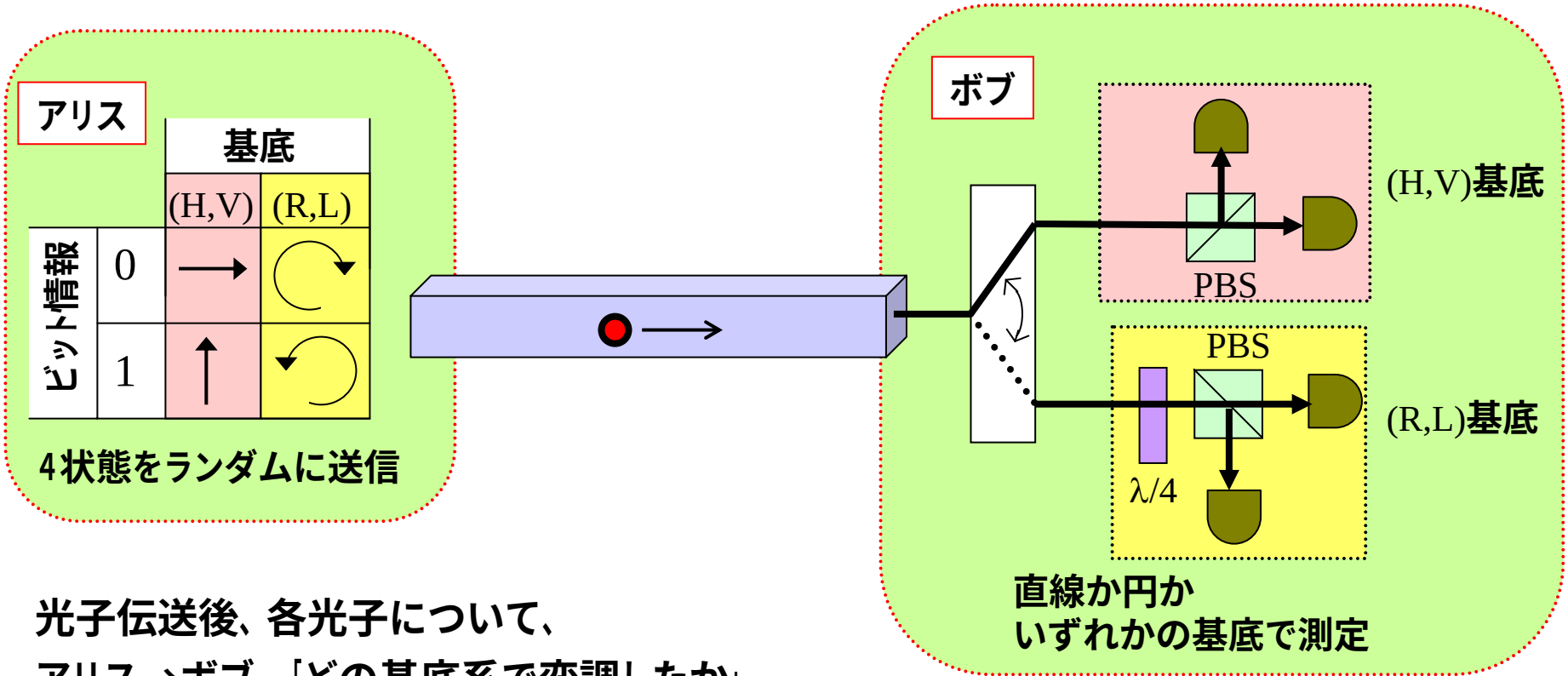
①量子チャンネルで光子を送受信
②古典チャンネルで基底に関する情報交換
③生秘密鍵生成
④誤り訂正･プライバシー増幅 → 最終秘密鍵

盗聴ルール

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。

? 盗聴者はいかなる手段も取り得るはずでは、、、

BB84方式 (by Bennett and Brassard in 1984)

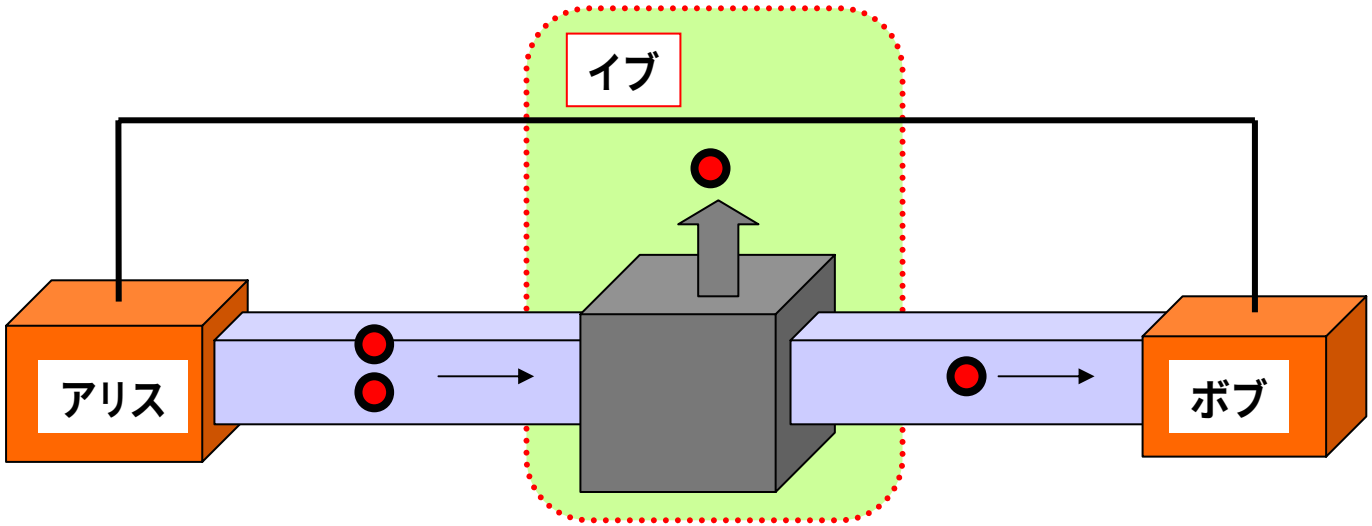


光子伝送後、各光子について、
アリス→ボブ 「どの基底系で変調したか」
ボブ→アリス 「どの基底系で光子を検出したか」

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

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
・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

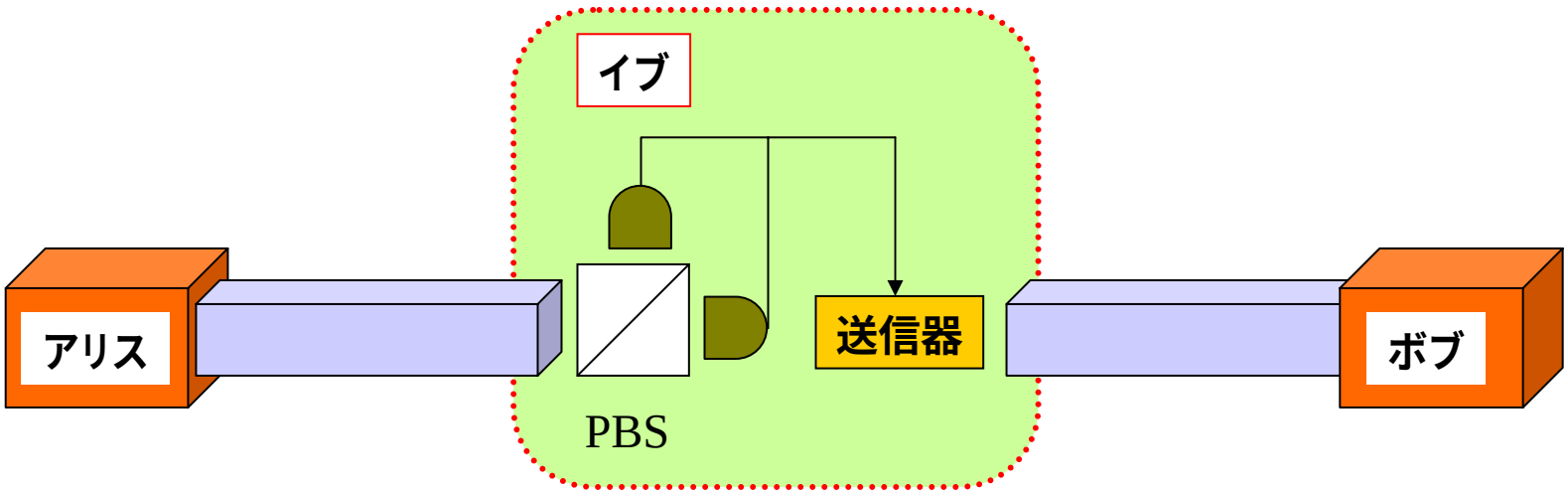
イブ

①2光子を含んでいるパルスを検知 ? how
②そのうちの1光子をタッピングし、保存 ? how
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



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

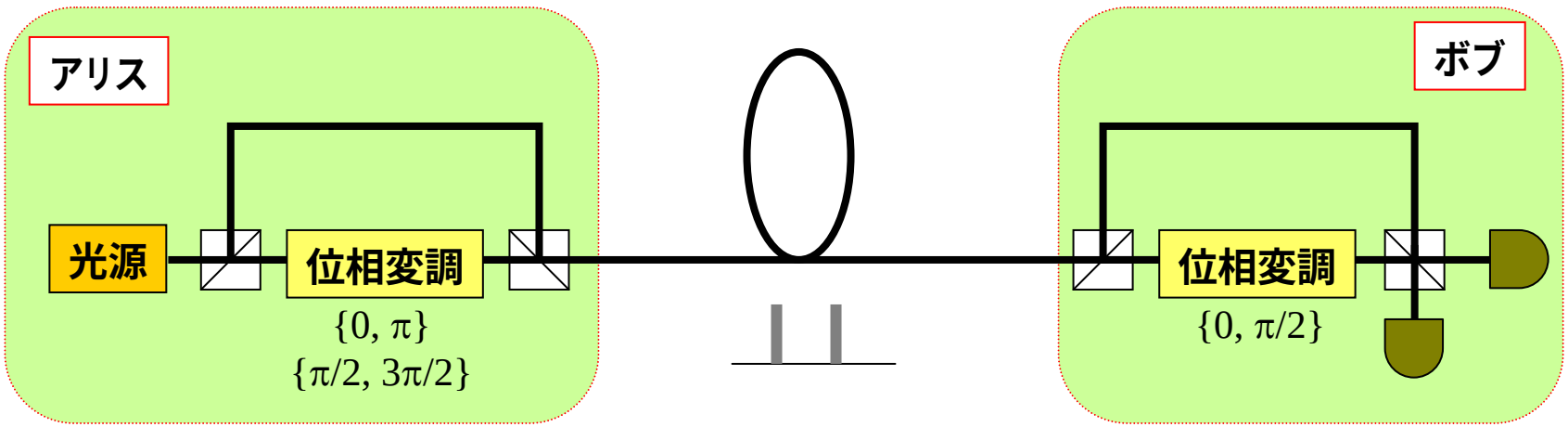
不一致の場合 → 1/2の確率で誤り → テストビットチェックにより盗聴発覚
誤りがなければ安全

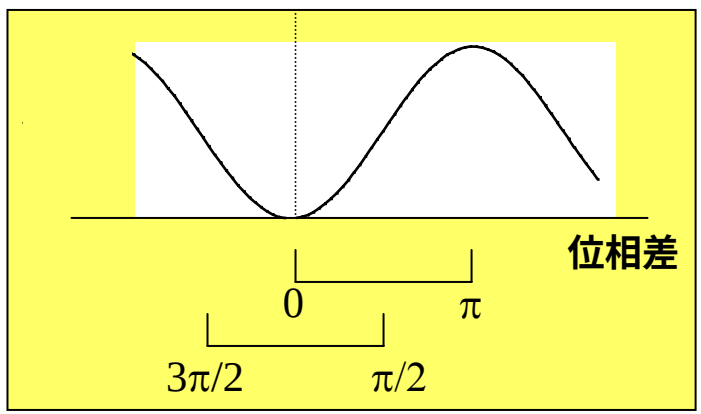
? ファイバ監視技術 (OTDR) により検出可能

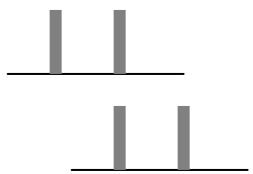
位相エンコードBB84

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

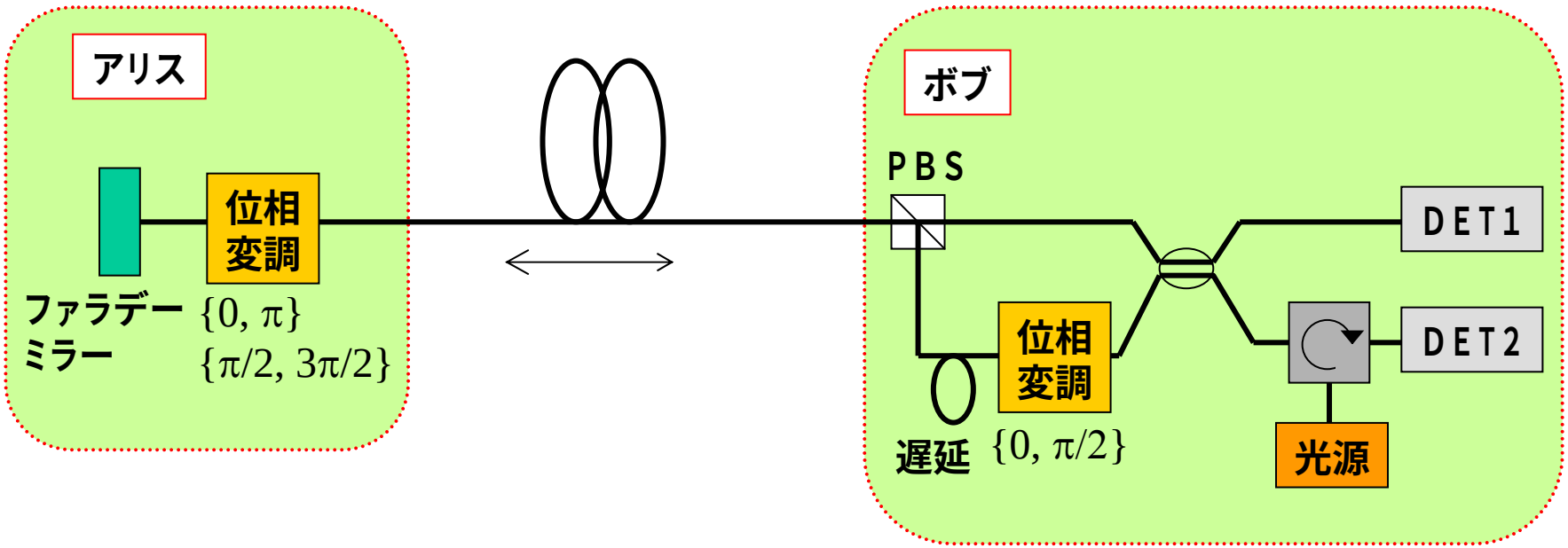






Plug & Play システム

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, π} ⇔ 直線偏波系、{π/2, 3π/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

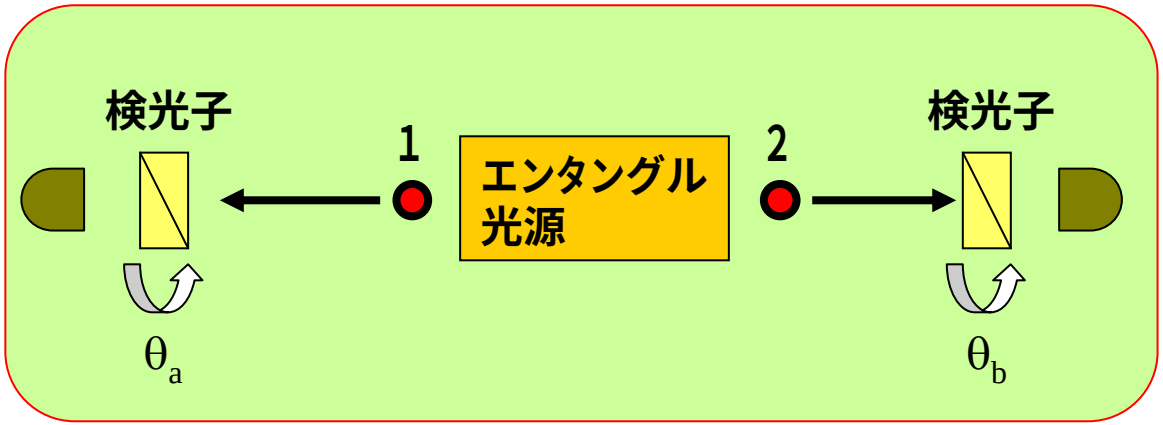
伝送距離 (km)	鍵供給速度 (bit/s)	機関	年
30	260	British Tel.（英）	1995
48	10	Los Alamos研（米）	2000
40(80)	10(2)	Heriot-Watt大（英）	2001
67	50	Geneva大 （スイス）	2002
100	< 5	NEC （日）	2003

課題：

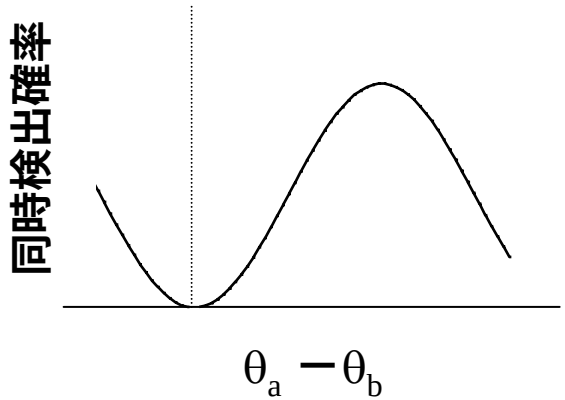
- **ファイバ伝送波長帯の光子検出器（効率、ダークカウント、繰り返し周波数）**
- **レーリ散乱（plug&playの場合）**
- **偏波 or 干渉計の制御・安定性（一方向の場合）**
- **単一光子光源の開発**

量子エンタングルメント（波動関数の非局在性）

量子コンピュータの基本エレメント



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)

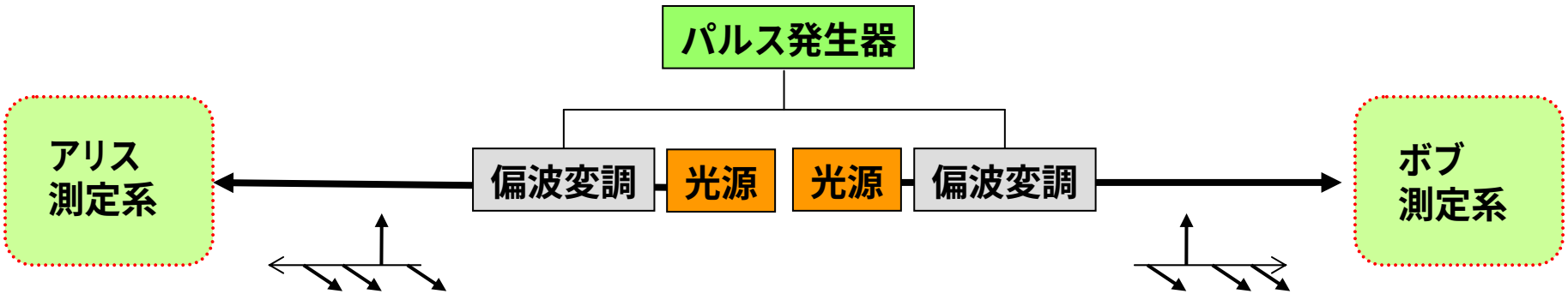
$$= \frac{1}{\sqrt{2}}(|+45\rangle_1|+45\rangle_2 + |-45\rangle_1|-45\rangle_2) \longrightarrow$$ 一方が+45 (or -45)だと他方も+45 (or -45)

（|+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の場合



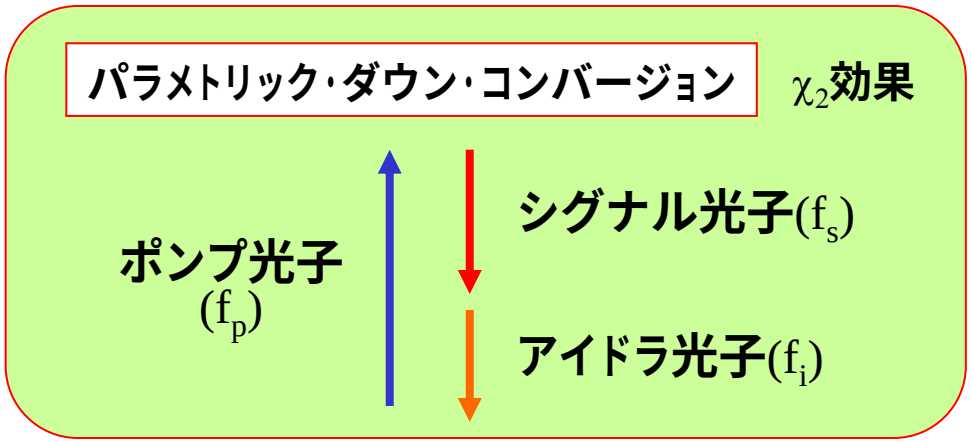
縦・横偏波系で測定 ⟶ 一方がH (or V)だと他方もH (or V)

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



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 $|H>_s|H>_i$

非線形媒質 $|V>_s|V>_i$

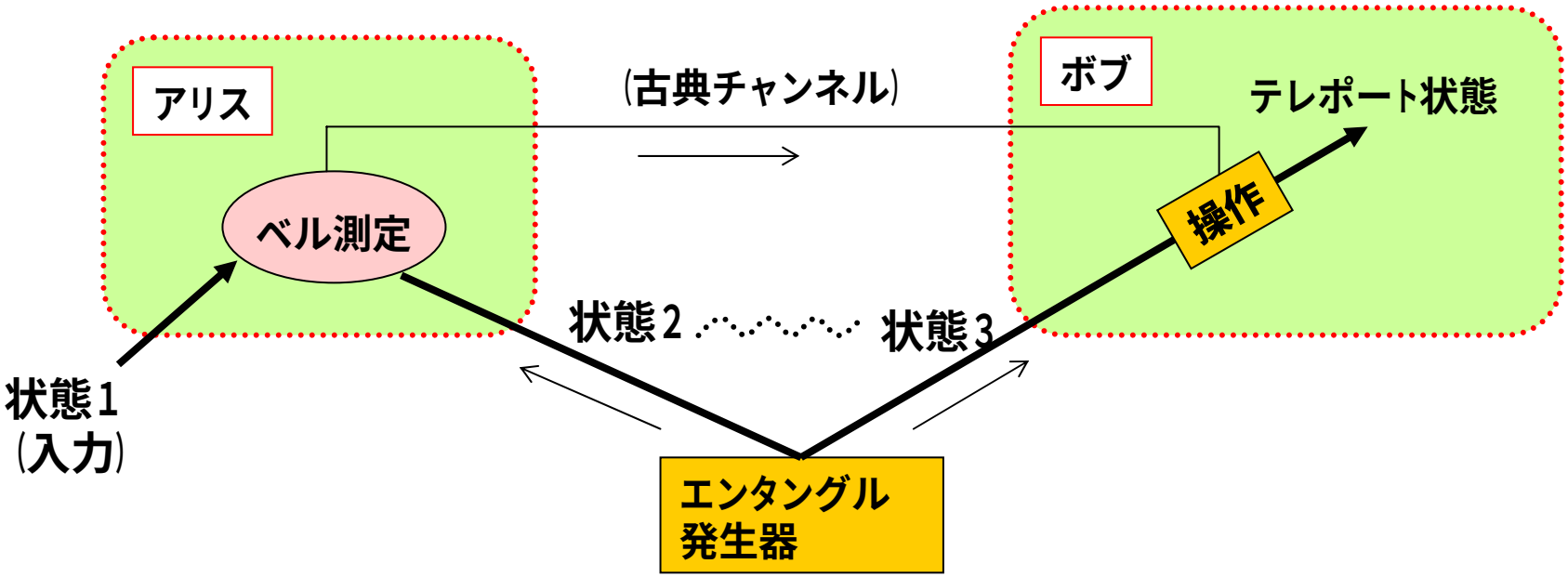
$|H>_s|H>_i$ or $|V>_s|V>_i$

with appropriate pump power

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

量子テレポーテーション

任意の量子状態を量子チャンネルを使わずにアリスからボブへ転送する



手順：(1) エンタングル状態 (状態2、3) の片方ずつをアリスとボブに供給

(2) アリスは状態1と状態2の相対関係を測定 (ベル測定)

(3) アリスは測定結果をボブに通知

(4) ボブはアリスの測定結果に基づいて状態3を操作→状態1が再現

? ボブはアリスの測定結果を知るまで状態3を保持 (量子メモリが必要)

状態1（転送元）：$|\phi\rangle_1 = a|H\rangle_1 + b|V\rangle_1$

状態2、3（エンタングルメント）：$|\psi\rangle_{23} = \frac{1}{\sqrt{2}}(|V\rangle_2|H\rangle_3 - |H\rangle_2|V\rangle_3)$

↓

全状態：$|\Psi\rangle_{123} = \frac{a}{\sqrt{2}}(|V\rangle_1|V\rangle_2|H\rangle_3 - |V\rangle_1|H\rangle_2|V\rangle_3) + \frac{b}{\sqrt{2}}(|H\rangle_1|V\rangle_2|H\rangle_3 - |H\rangle_1|H\rangle_2|V\rangle_3)$

↓

（状態1＋2の基底系で展開）

$$|\Psi^{(\pm)}\rangle_{12} = \frac{1}{\sqrt{2}}(|V\rangle_1|V\rangle_2 \pm |H\rangle_1|H\rangle_2)$$
$$|\Phi^{(\pm)}\rangle_{12} = \frac{1}{\sqrt{2}}(|V\rangle_1|H\rangle_2 \pm |H\rangle_1|V\rangle_2)$$

$$|\Psi\rangle_{123} = \frac{1}{\sqrt{2}}\{|\Psi^{(+)}\rangle_{12}(a|V\rangle_3 - b|H\rangle_3) + |\Psi^{(-)}\rangle_{12}(a|V\rangle_3 + b|H\rangle_3) + |\Phi^{(+)}\rangle_{12}(-a|V\rangle_3 + b|H\rangle_3) + |\Phi^{(-)}\rangle_{12}(-a|V\rangle_3 - b|H\rangle_3)\}$$

↓

（状態1＋2を基底系で測定＝ベル測定）

↓

4状態のどれかひとつに収縮

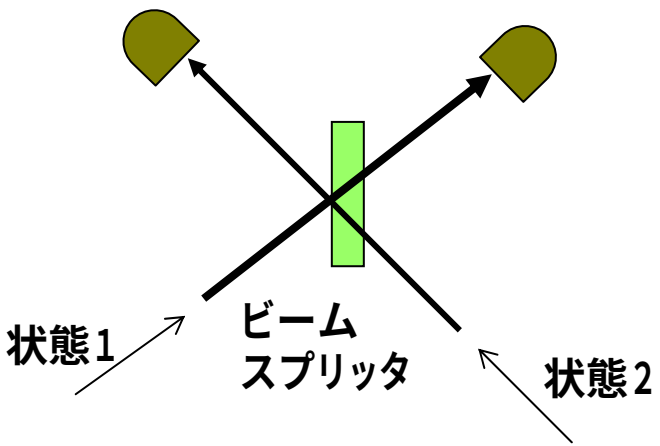
↓

ベル測定結果に応じて状態3を変換 → 状態1と同じ状態

ベル測定

2状態系の基底状態への射影

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

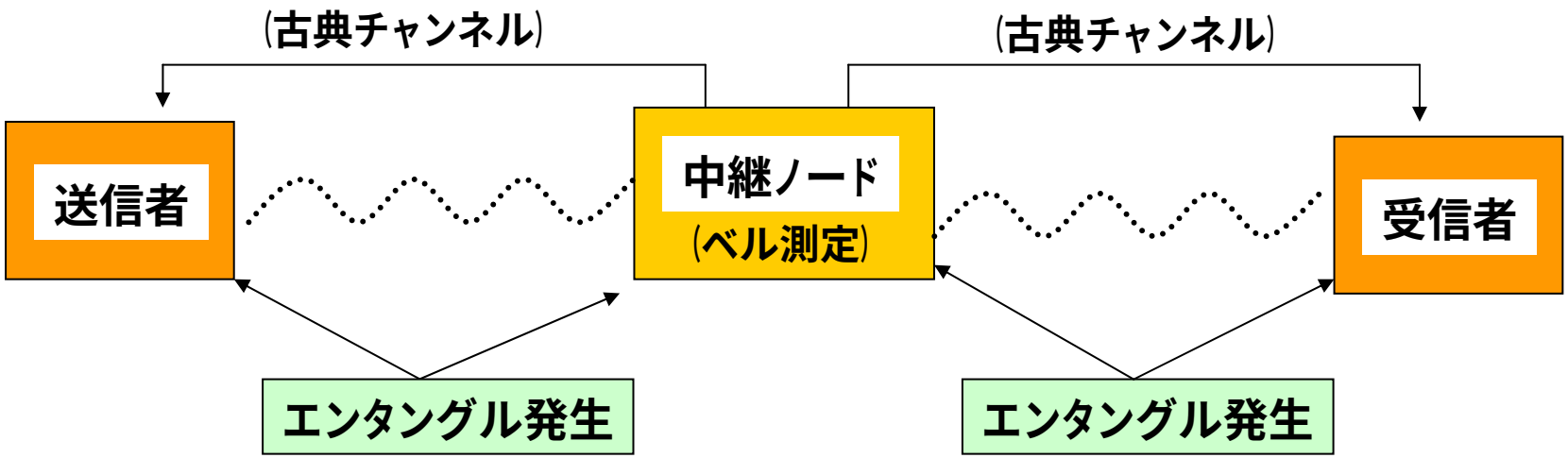


同時検出したら$|\Phi^{(-)}\rangle_{12}$と判定

- 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

？ 4基底状態すべてを識別する具体的な測定法は知られていない

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

？　量子メモリが必要

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

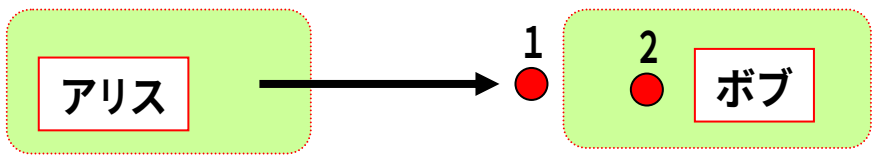
(a) 何もしない ⟶ $|\Psi^{(+)}>=(|V>_1|V>_2+|H>_1|H>_2)/\sqrt{2}$

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

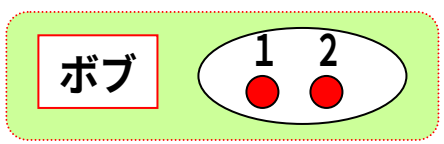
(c) |V>と|H>を入れ替え ⟶ $|\Phi^{(+)}>=(|H>_1|V>_2+|V>_1|H>_2)/\sqrt{2}$

(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



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

↓

2ビット情報

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

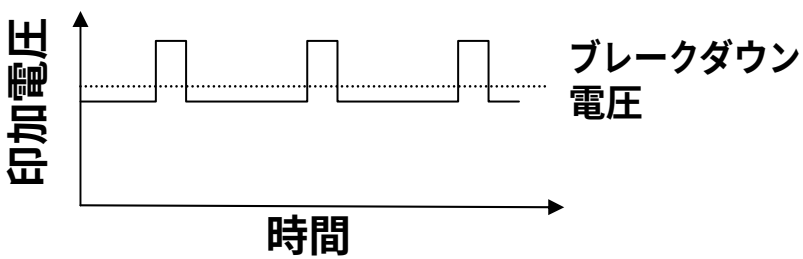
求められるのは、高量子効率、低ダークカウント、高繰り返し（アフターパルス）

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

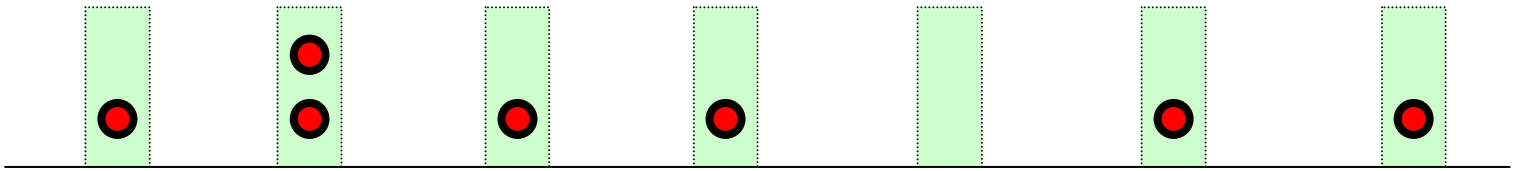
量子効率 ～ 10%、ダークカウント～10^{-5}/gate、繰り返し＜1MHz



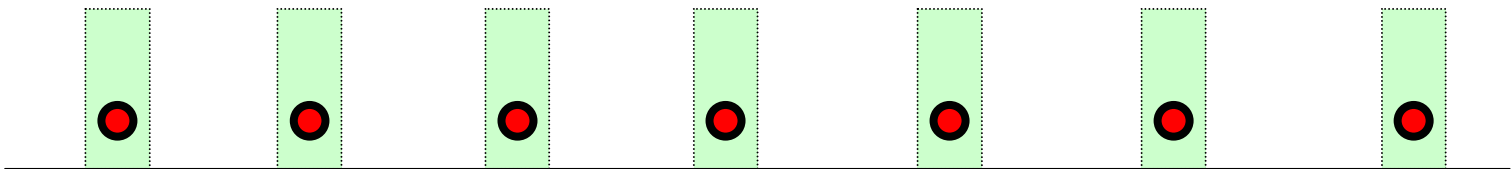
量子光通信用デバイスー単一光子光源ー

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)



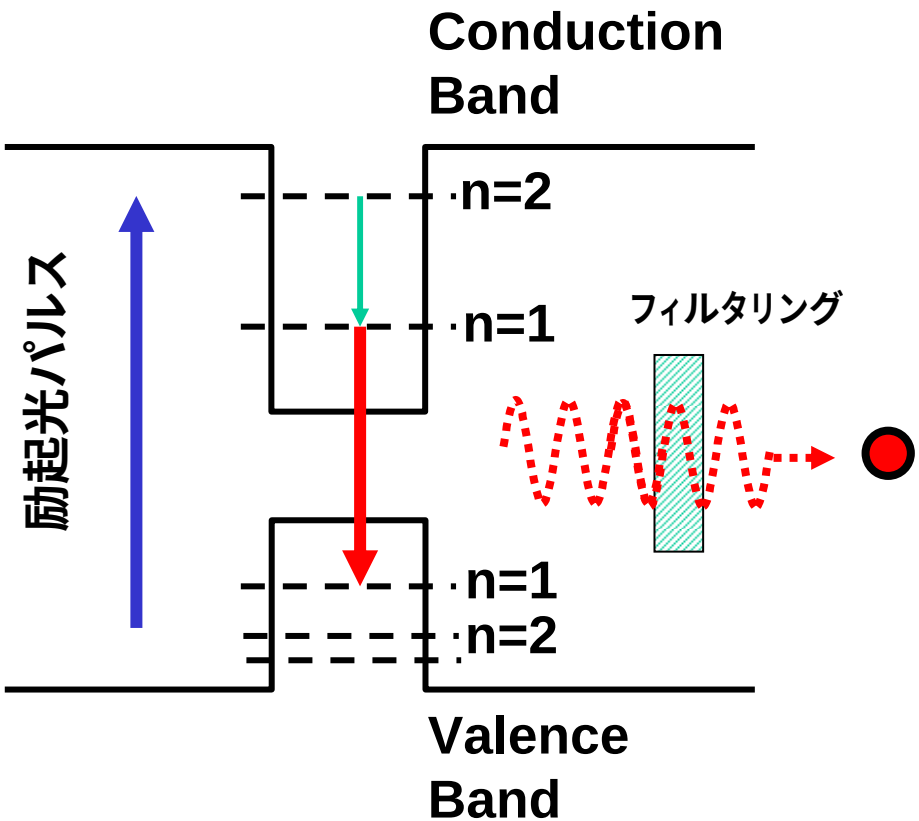
単一光子光 (サブポワソン)



時間

半導体量子ドット光源

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

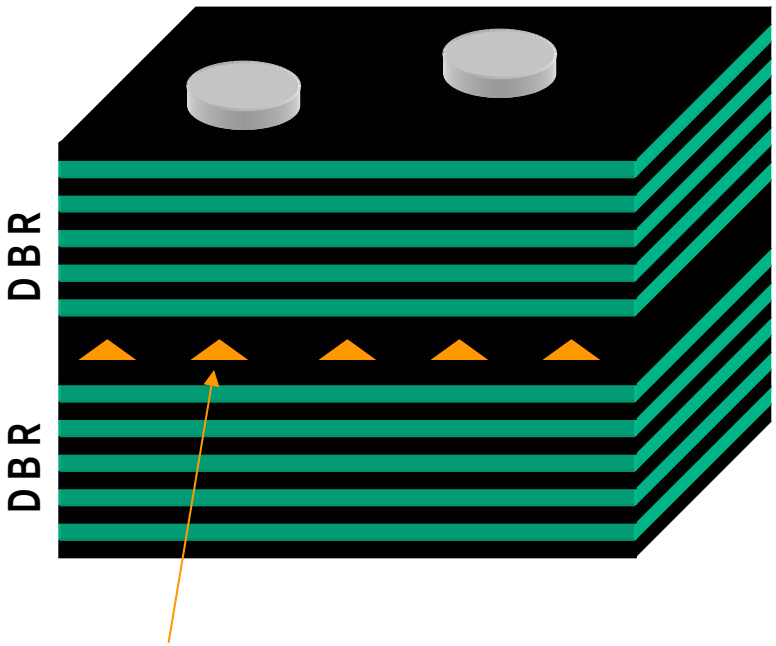
↓

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

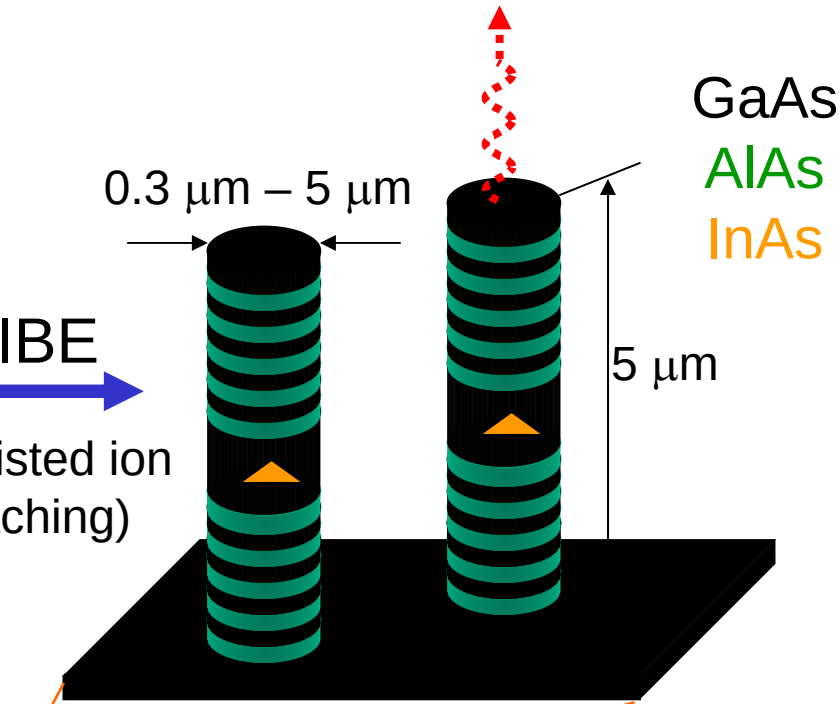
作製 (by Stanford University)

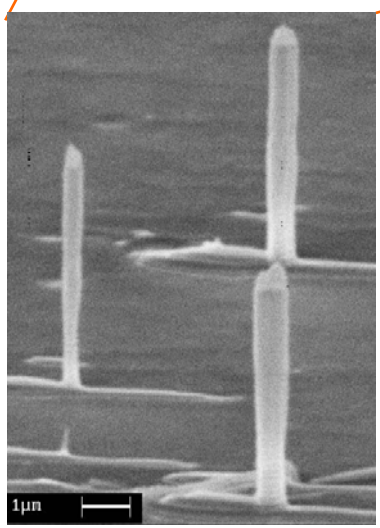


量子ドット

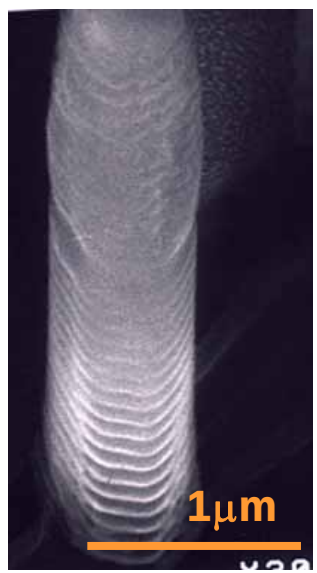
CAIBE

(Cl_2 assisted ion beam etching)





1μm

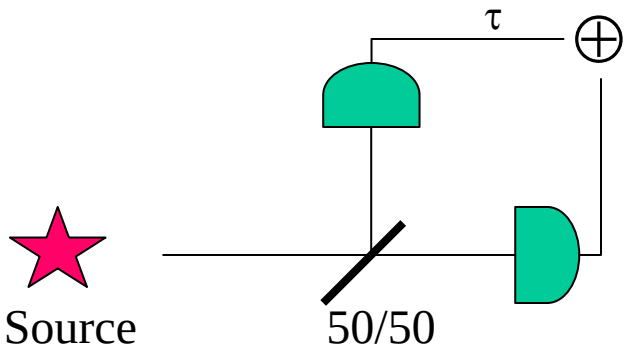


自然放出光子を効率良く取り出すために

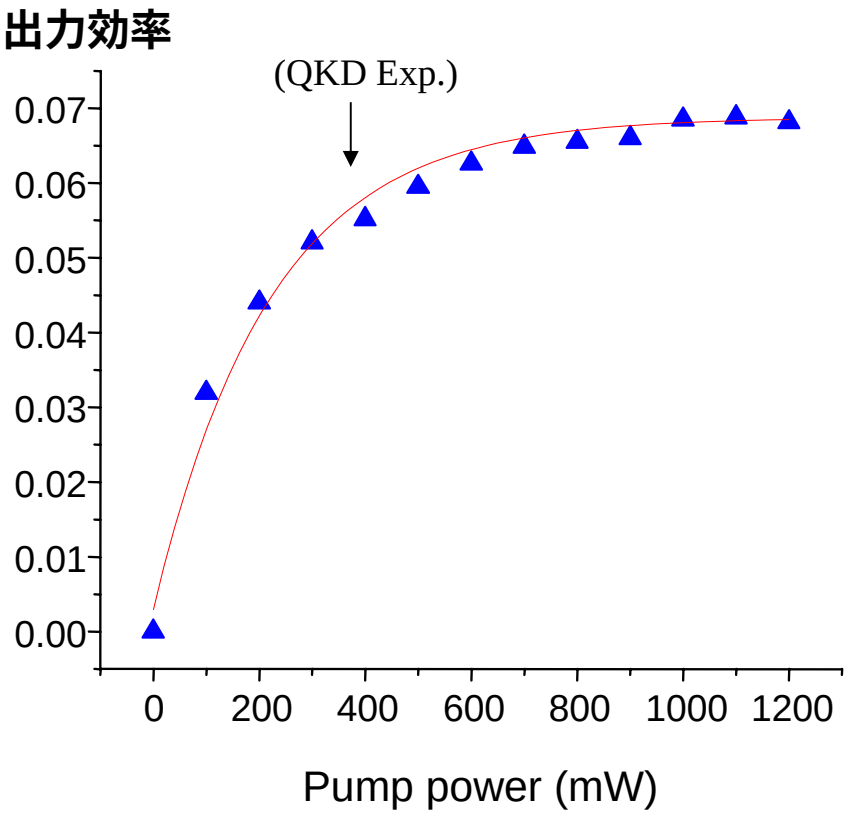
ポスト型マイクロ共振器を形成

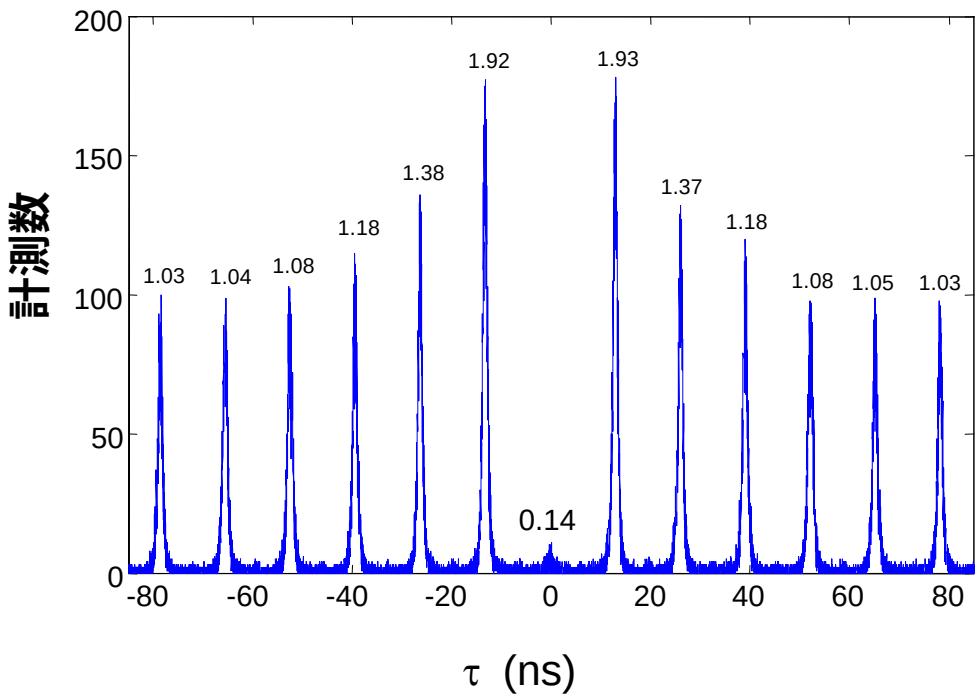
出力特性

同時計数

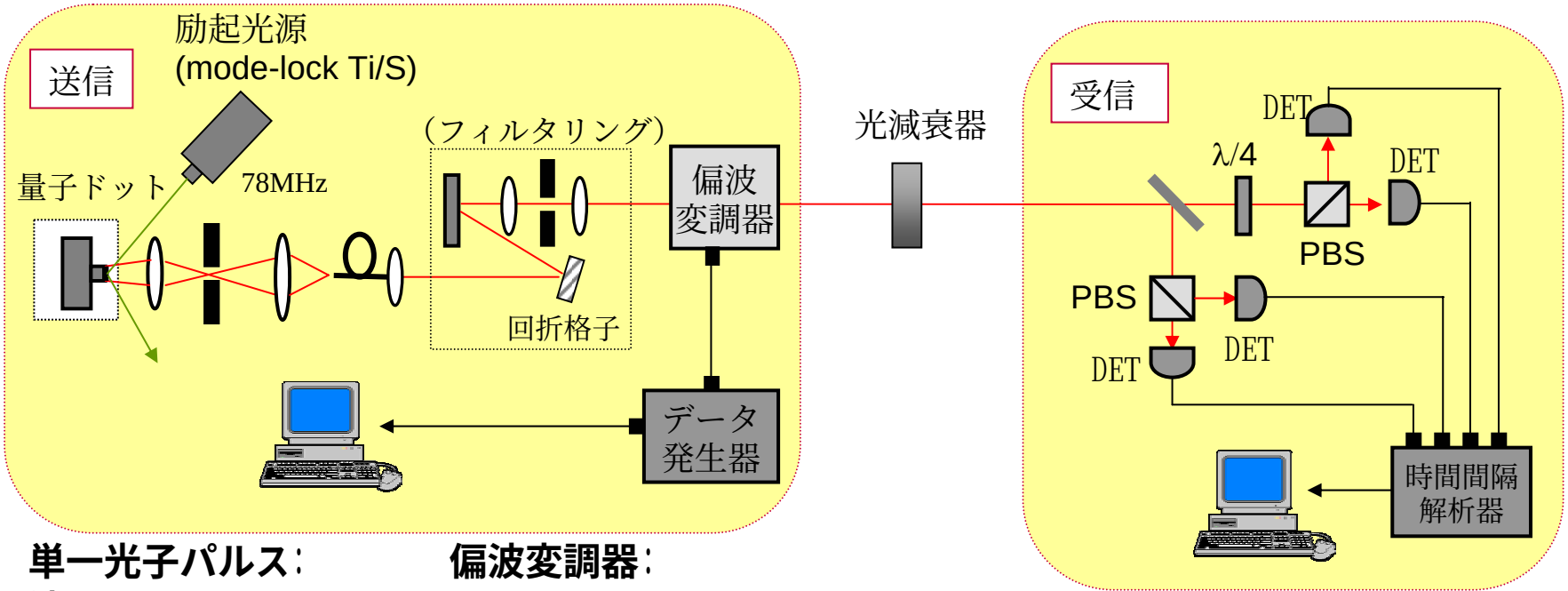


saturation curve



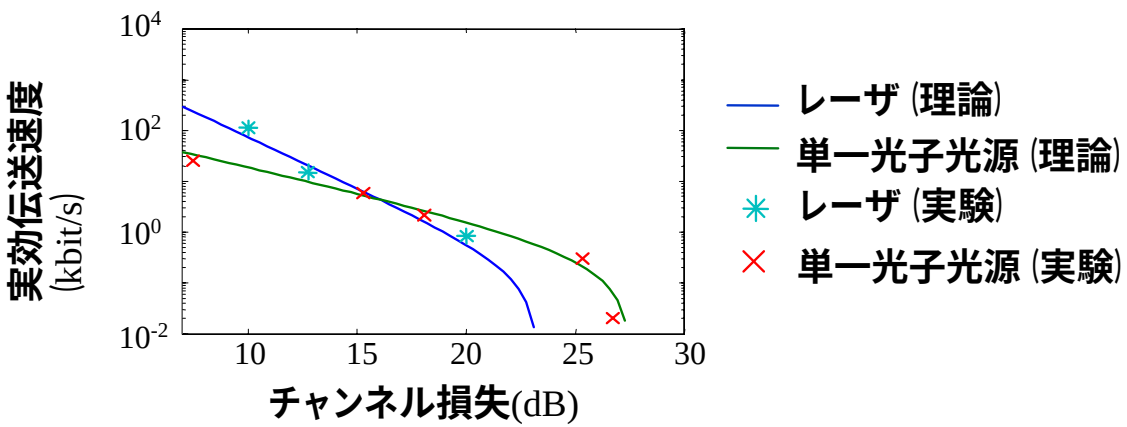


単一光子光源を用いた量子暗号実験



単一光子パルス:
波長＝900nm
パルス幅＝2~300ps

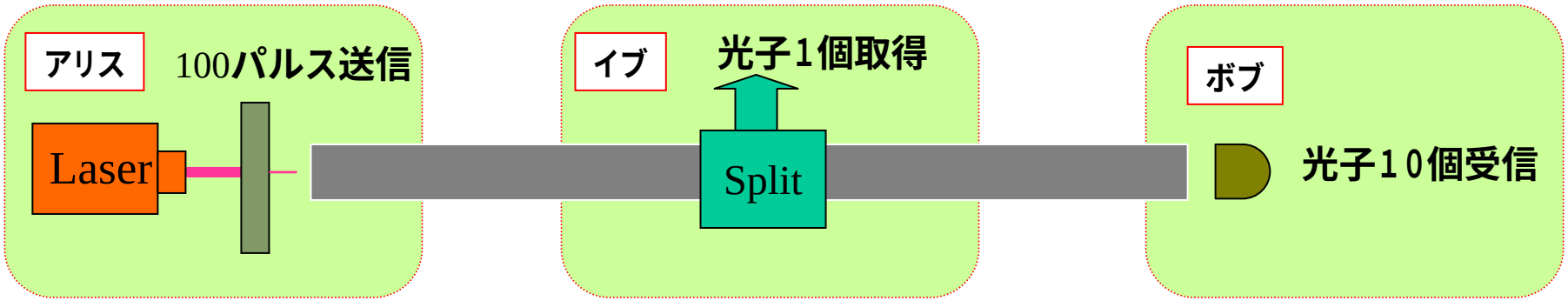
偏波変調器:
{縦・横} {右廻り・左廻り}
の4偏波にランダム変調



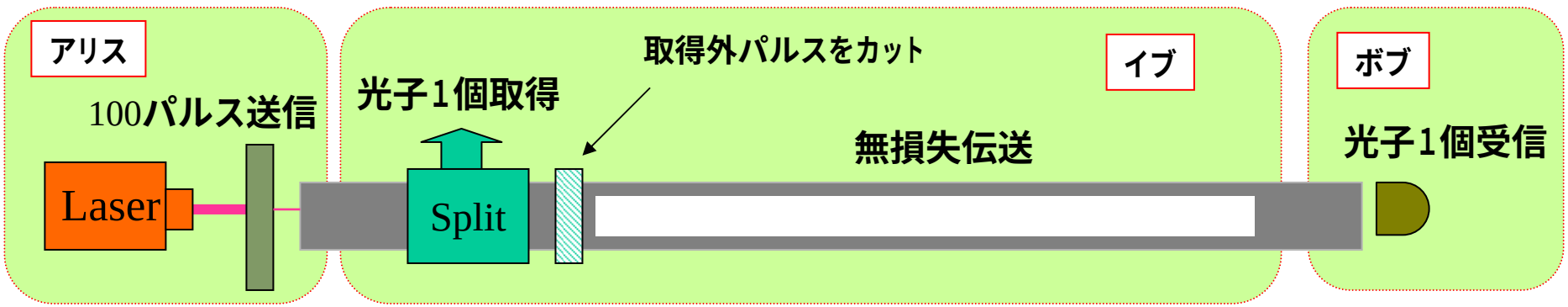
弱コヒーレント光に対する beam splitting attack

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。

光通信研究者がみた量子光通信

1. 量子暗号
   - (電気段に対する盗聴には無効)
   - (非現実的な盗聴に対処)
   - (ファイバ伝送路の光信号が盗聴される？)
2. 量子テレポーテーション
   - (量子状態をそのまま送ればいいでは？)
   - (量子メモリが必要)
   - (成功率25%)
3. 基本デバイス – 単一光子光源 –