光の量子的性質を利用した
安全な暗号通信・量子秘密共有

大阪大学工学研究科　　井上　恭

[内容]

[1] 量子暗号プロトコル　–位相エンコードBB84-

　　構成、動作原理、安全性

[2] 量子暗号実験

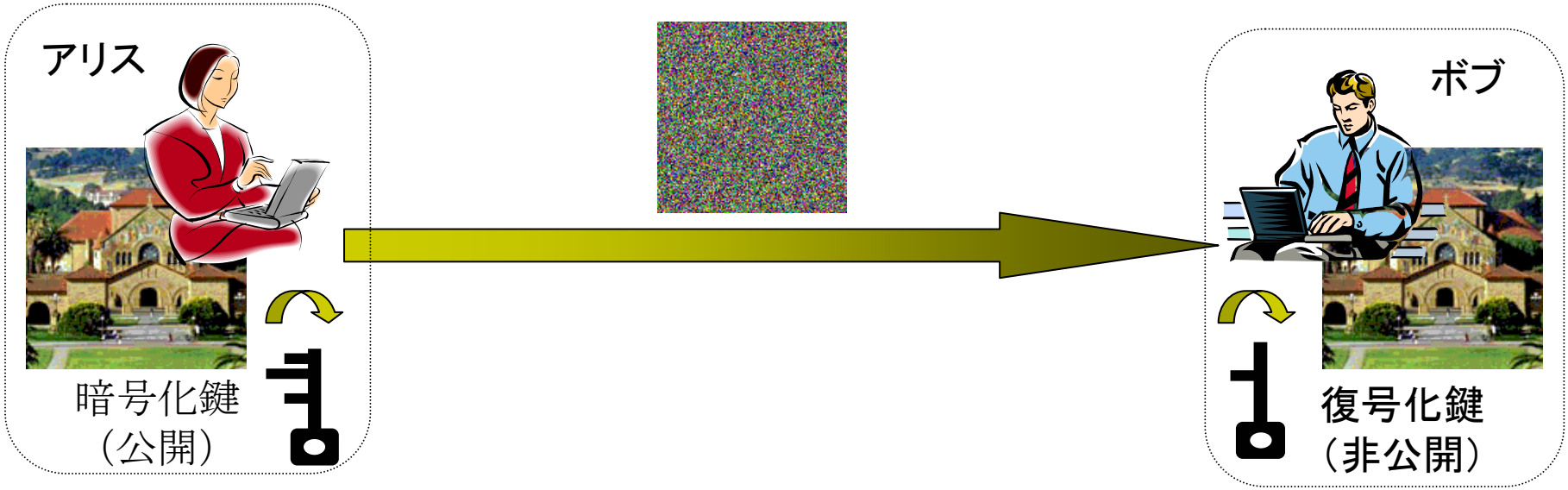
　　光子検出器

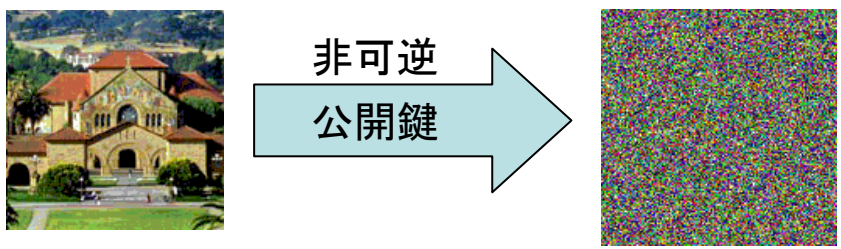
　　プラグ＆プレイ構成

[3] 差動位相シフト量子鍵配送

[4] 量子秘密共有

公開鍵暗号



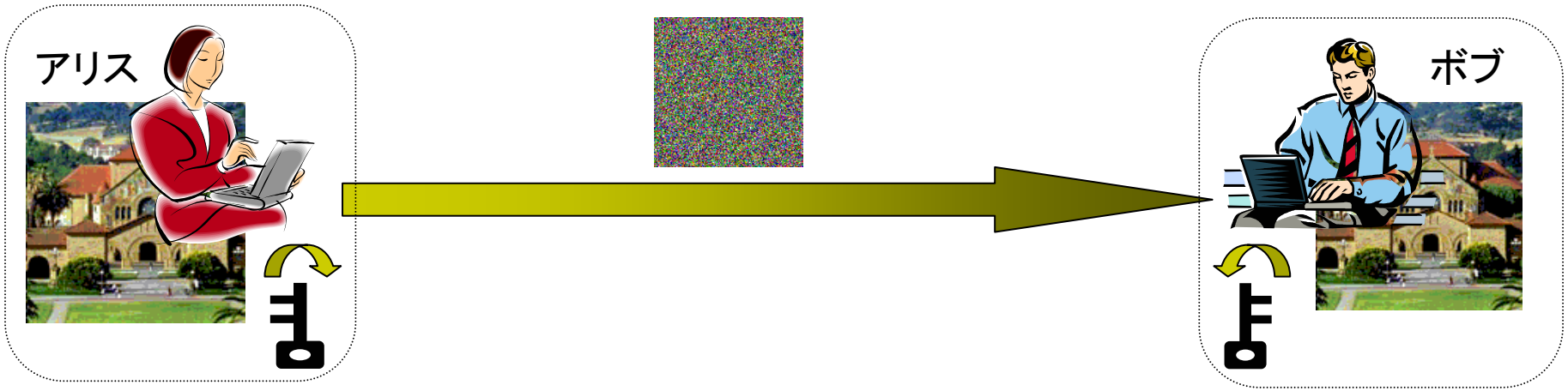


$367 \times 521 = 191207$: easy

$191207 = X \times Y$: difficult

原理的には解読可能

秘密鍵暗号



秘密鍵（ランダムなビット列）

秘密鍵

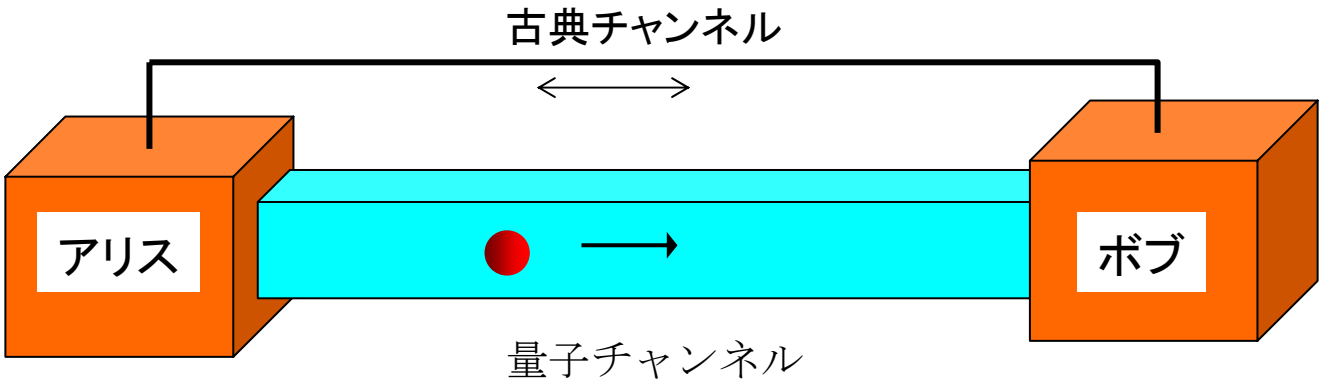
秘密鍵が1回しか使われなければ(one time pad)絶対に安全
But、秘密鍵をどうやって安全に供給するか？

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
（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。）

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（ランダムなビット列）

④誤り訂正・プライバシー増幅 → 最終秘密鍵

前提

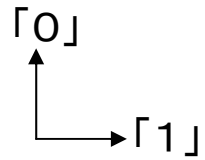
盗聴者は、量子チャンネルに対しては盗聴・改ざんができる。
古典チャンネルに対しては盗聴のみ。

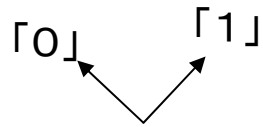
量子暗号プロトコル

BB84　2つの非直交基底系

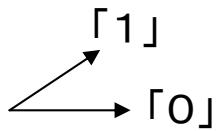
偏波エンコード

位相エンコード ←





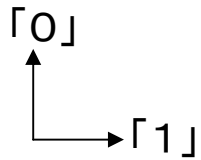
B92　2つの非直交状態

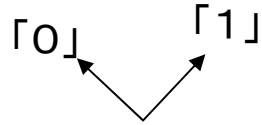


差動位相シフト方式　弱めたコヒーレントパルス列 ←

BBM92　エンタングル光子対（2つの非直交基底系利用）

＋



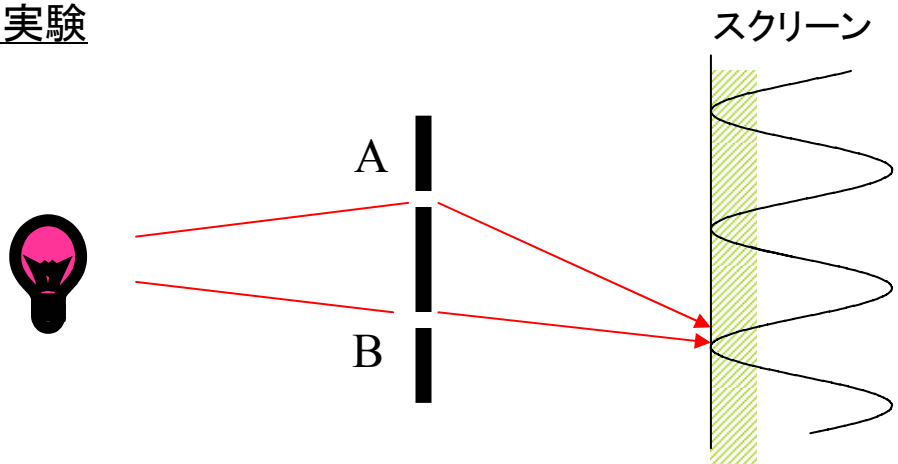


E91　エンタングル光子対（ベル不等式利用）

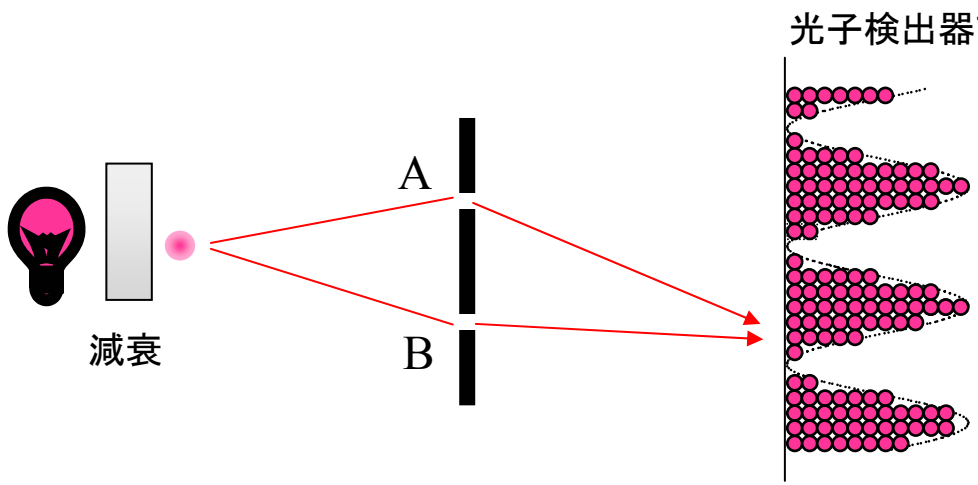
量子暗号で使われる量子性

-光の波動性と粒子性-

ヤングの干渉実験



$$E = ae^{ikL_a} + be^{ikL_b}$$

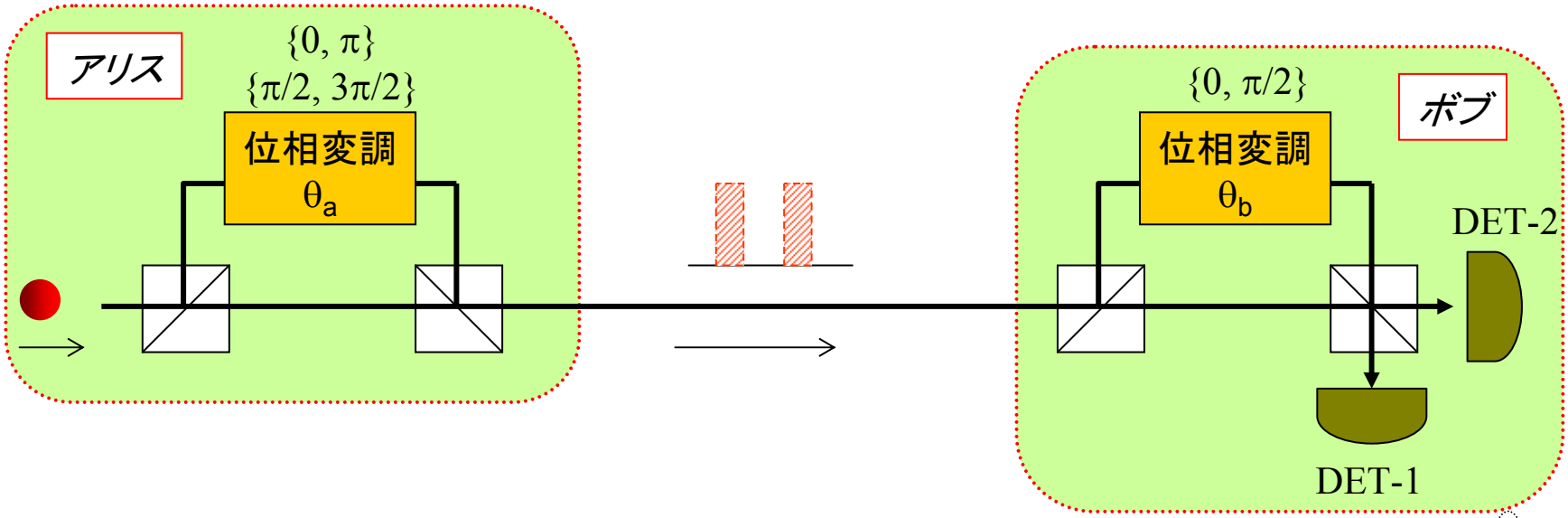


$$|\psi\rangle = ae^{ikL_a}|a\rangle + be^{ikL_b}|b\rangle$$

|a>: 光子がAを通った状態

|b>: 光子がBを通った状態

位相エンコードBB84



鍵生成手順

①光子を送受信

②ボブ→アリス：受信した光子を通知

③受信された光子について、

アリス→ボブ：$\theta_a = \{0, \pi\}$ か $\{\pi/2, 3\pi/2\}$か、を通知

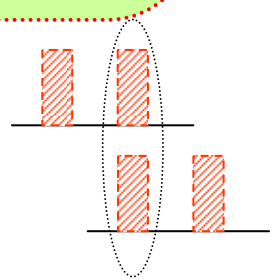
ボブ→アリス：$\theta_b = 0$か$\pi/2$か、を通知

④鍵ビット生成

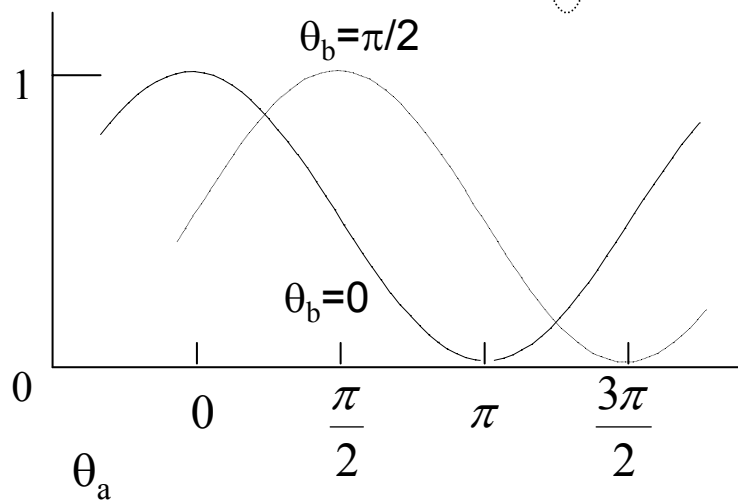
アリス：$\theta_a = 0, \pi/2$ ⇒「0」、$\theta_a = \pi, 3\pi/2$ ⇒「1」

ボブ：DET-1 ⇒ 「0」、DET-2 ⇒ 「1」

→秘密鍵

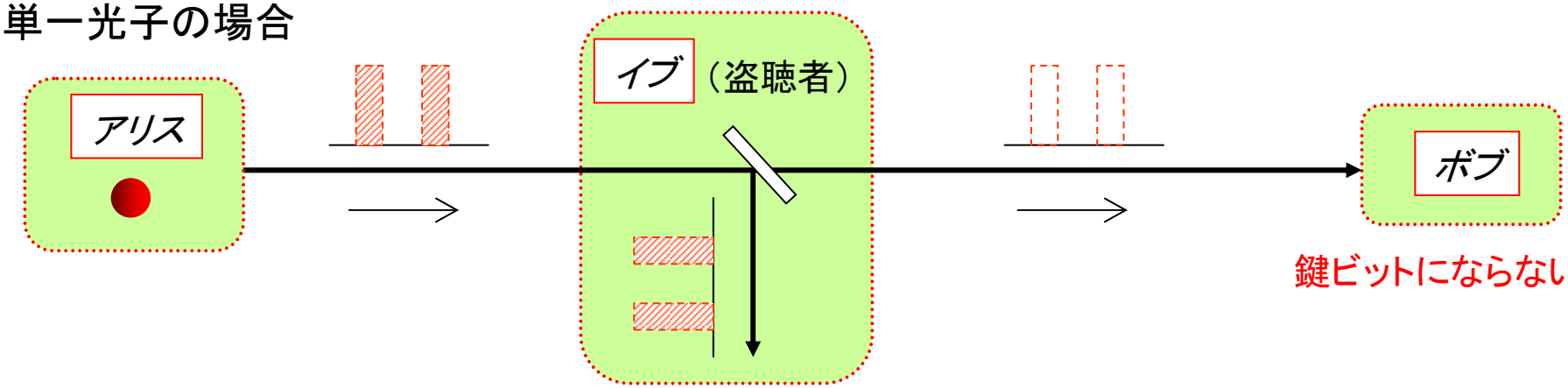


検出確率
@DET-1

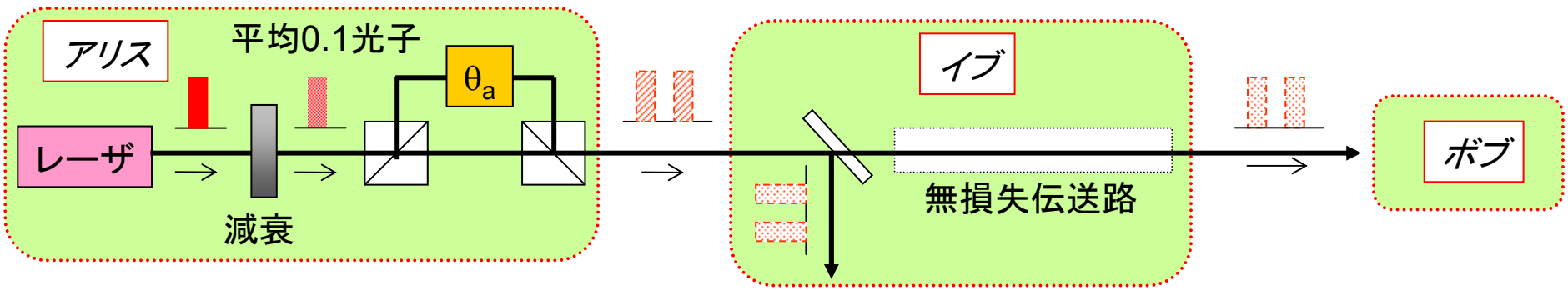


安全性1 –盗み聞き盗聴–

単一光子の場合



弱めたレーザ光の場合



有限の確率で、両方に光子

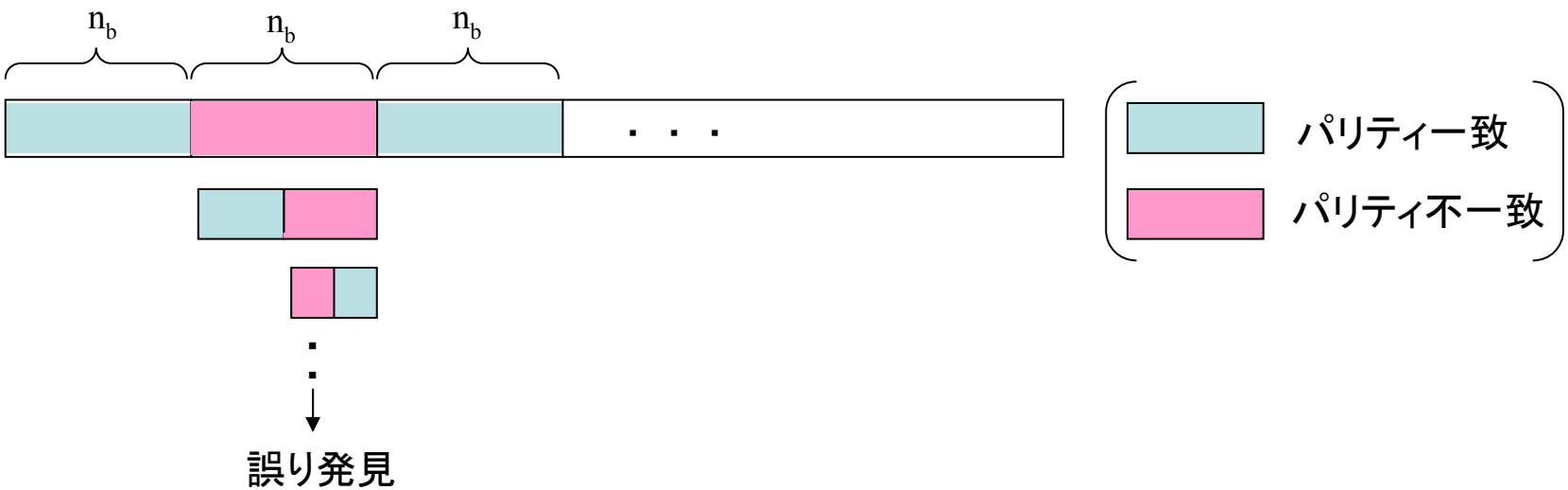
⇩

プライバシー増幅で対処

誤り訂正、プライバシー増幅

誤り訂正

ビット列をブロックに分けて、ブロックごとのパリティを比較



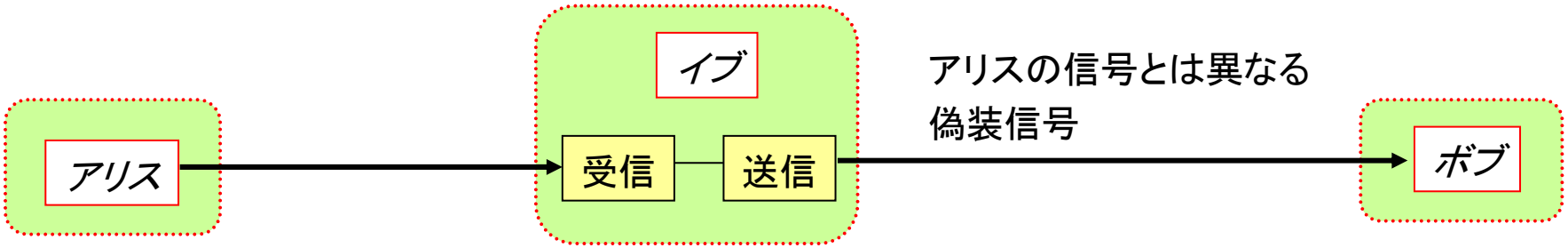
プライバシー増幅

ビット列を圧縮して一部漏洩に対処：nビット → mビット （m < n）

$$\begin{pmatrix} z_1 & z_2 & z_3 & \cdots & z_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & & & & \\ \vdots & & & & \\ a_{m1} & & & & \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$$z_i = \mathrm{mod}_2 \left[\sum_{j=1}^{n} a_{ij} x_j \right]$$

安全性2 –なりすまし盗聴–



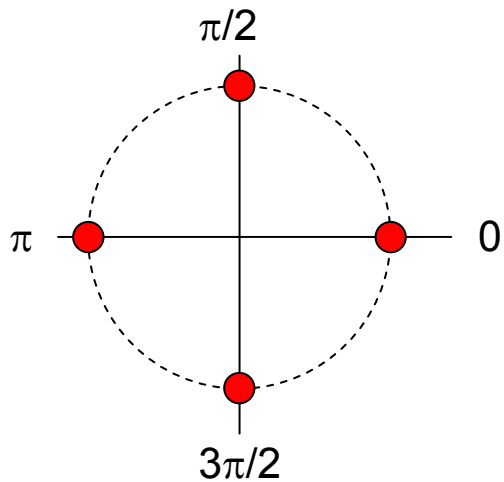
アリスの信号とは異なる
偽装信号

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

受信結果に基づいて偽装信号を送信。
But、全てのビットを正しく受信できない。



{0, π}を識別しようとすると、{π/2, 3π/2}は不定
{π/2, 3π/2}を識別しようとすると、{0, π}は不定

[内容]

[1] 量子暗号プロトコル　–位相エンコードBB84-

　　構成、動作原理、安全性

[2] 量子暗号実験

　　光子検出器

　　プラグ＆プレイ構成

[3] 差動位相シフト量子鍵配送

[4] 量子秘密共有

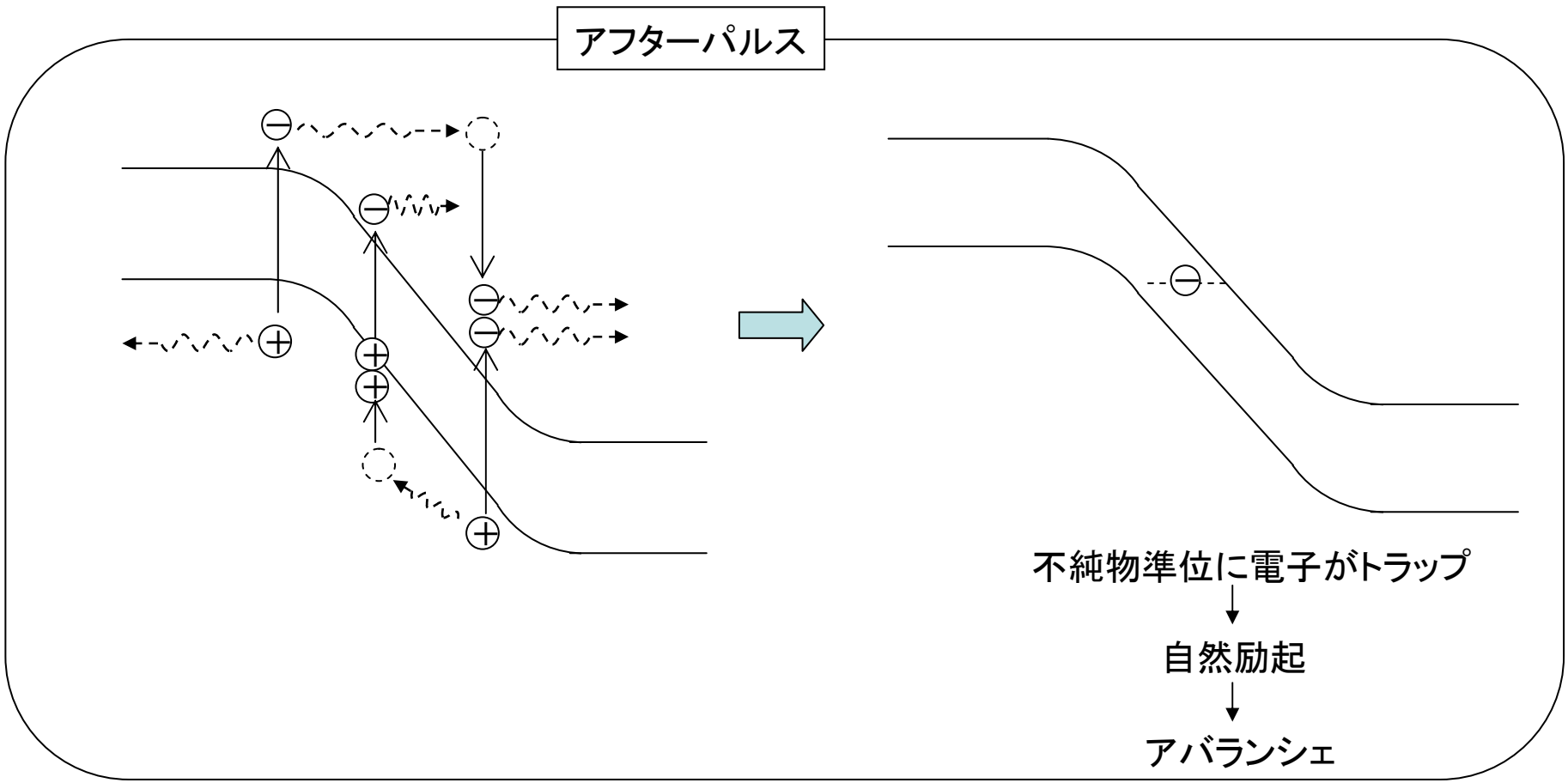
光子検出器

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

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）



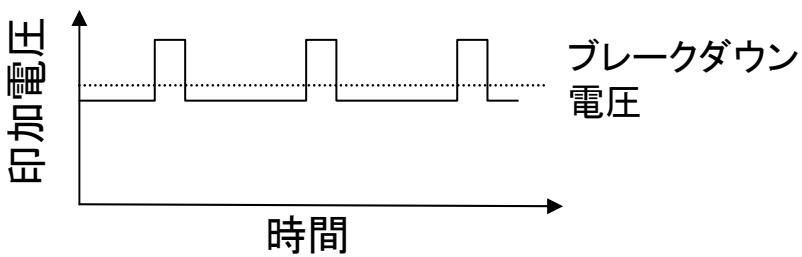
光子検出器の現状

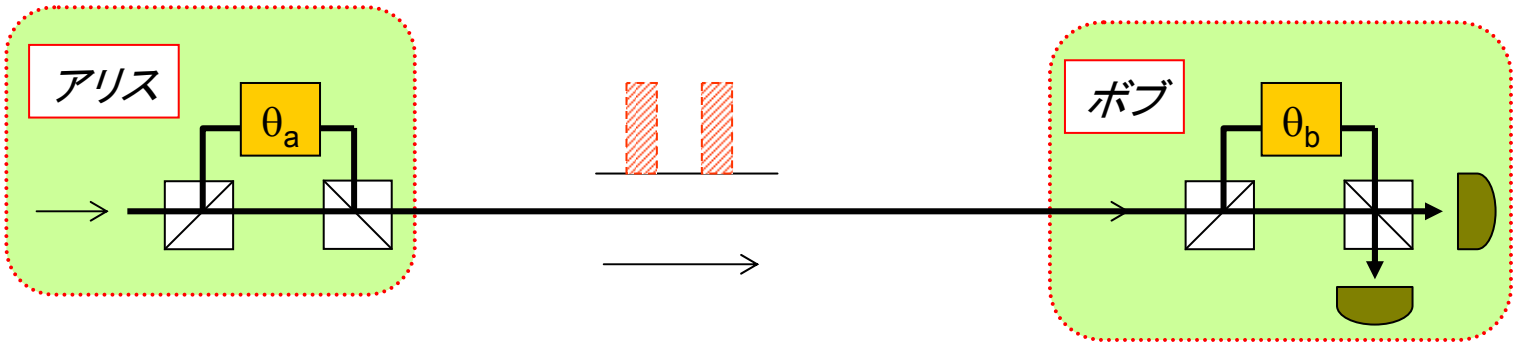
短波長帯：市販のSi-APDあり

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

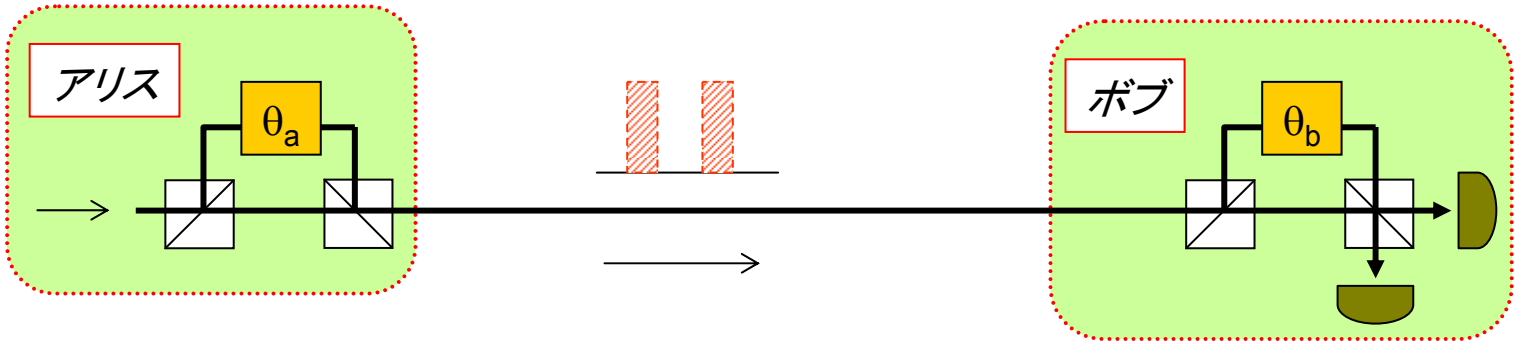
量子効率 ～ 10%、ダークカウント～10^{-5}/gate、繰り返し ＜ 数MHz



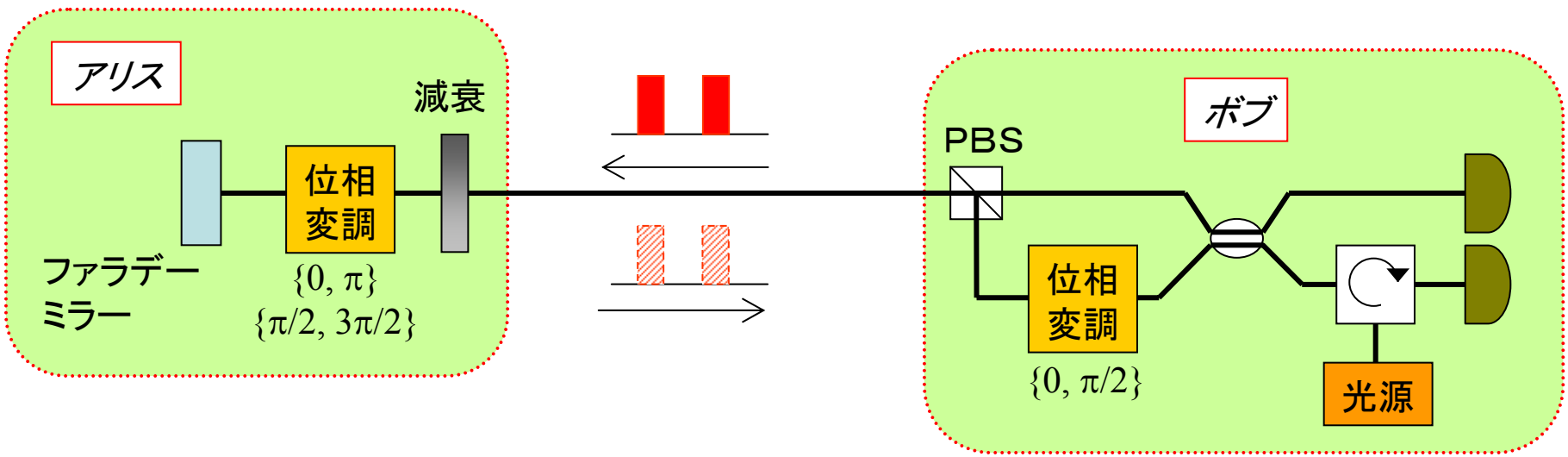

アリス
θa
ボブ
θb

量子暗号実験系：Plug & Play システム

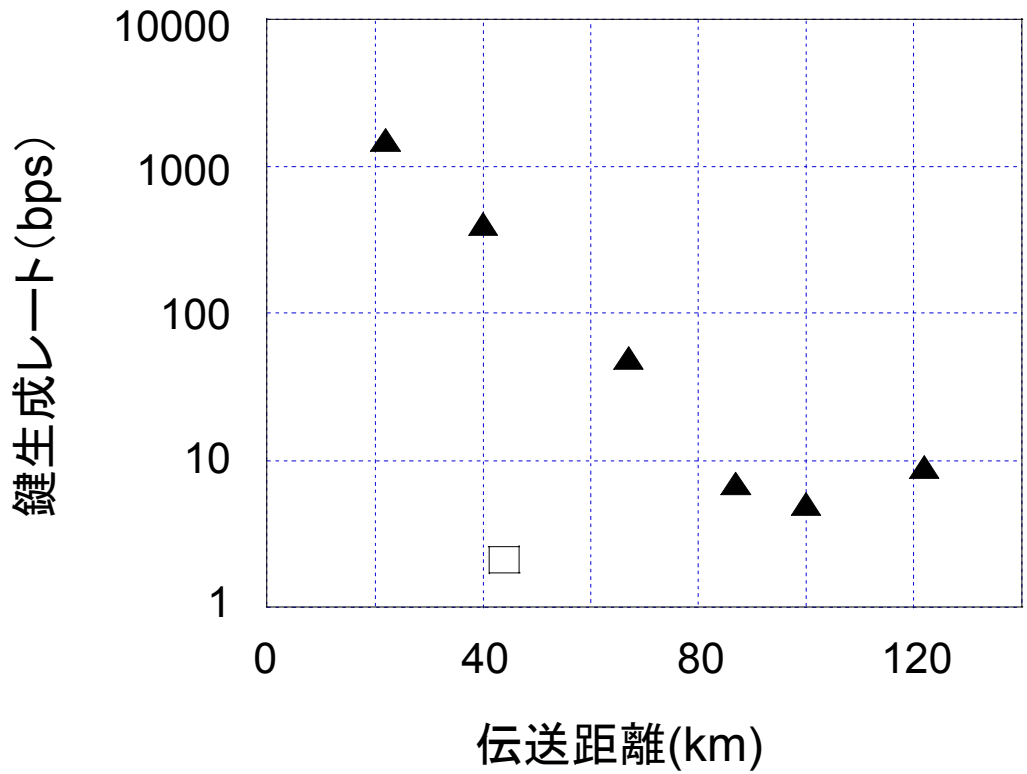
位相エンコードBB84を行うには、干渉計の安定性が難点



光を折り返す構成により位相変動を自動補償: plug & play構成



これまでの実験報告例



▲:光子数分岐攻撃は無視

主な制限要因は、

◆光子検出器

◆光子数分岐攻撃

[内容]

[1] 量子暗号プロトコル　–位相エンコードBB84-

　　構成、動作原理、安全性

[2] 量子暗号実験

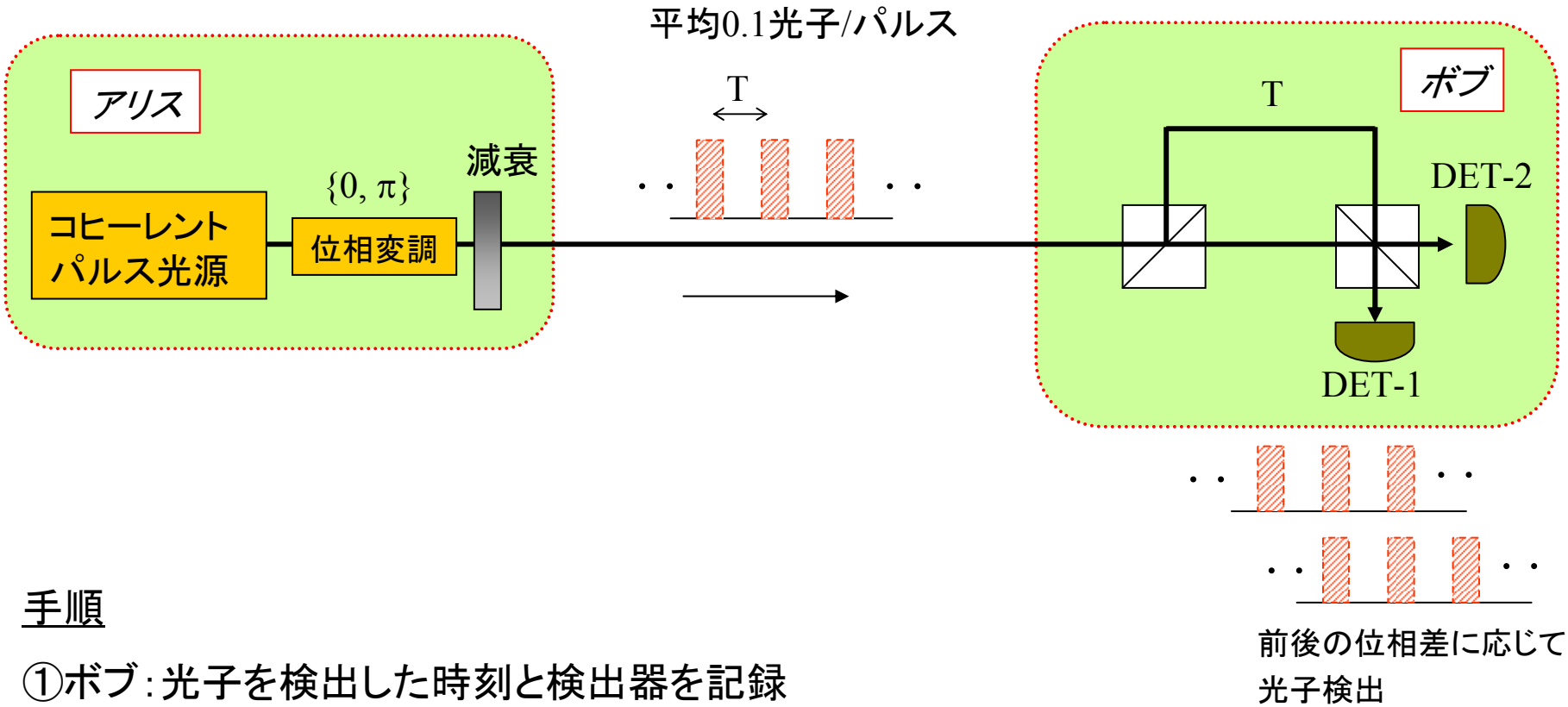
　　光子検出器

　　プラグ＆プレイ構成

[3] 差動位相シフト量子鍵配送

[4] 量子秘密共有

差動位相シフト量子鍵配送



手順

①ボブ：光子を検出した時刻と検出器を記録

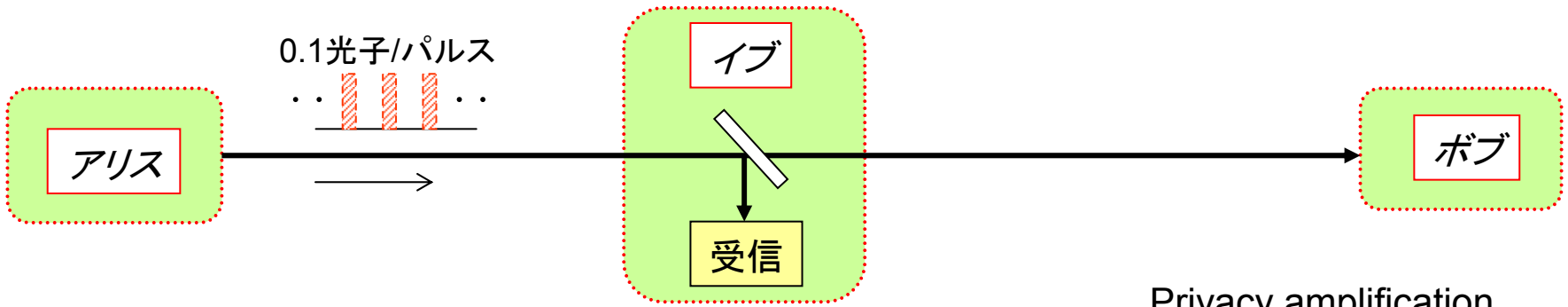
②ボブ→アリス：光子検出時刻を通知

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

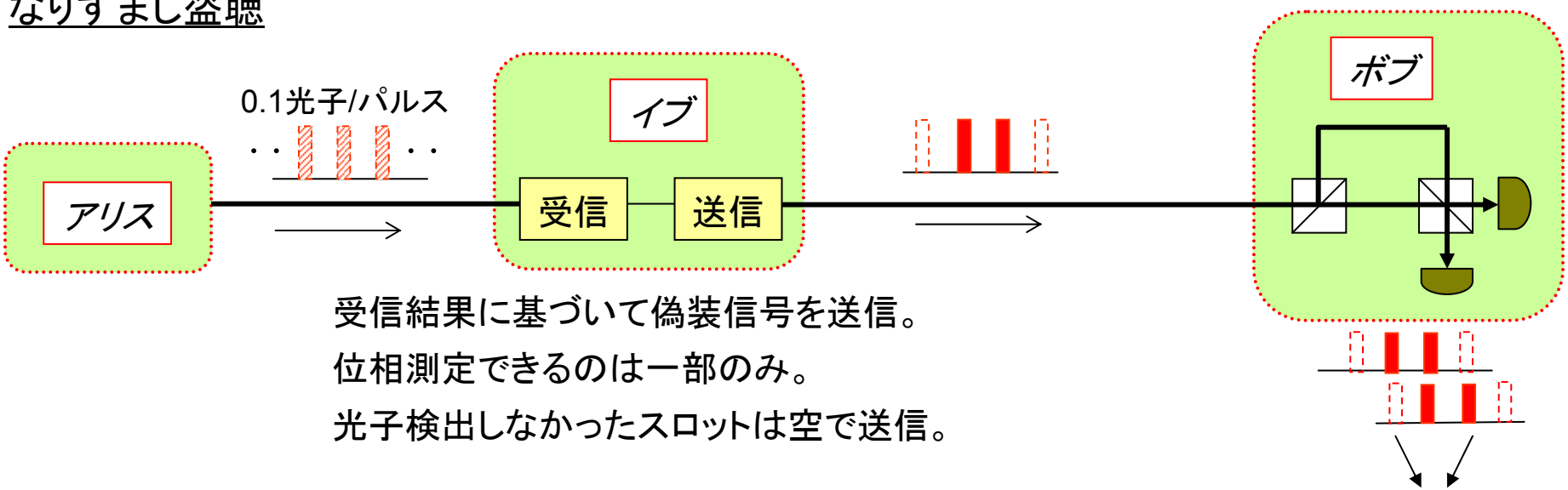
差動位相シフト方式の安全性

盗み聞き盗聴



同じパルスの光子を検出するのは稀 ← Privacy amplification により対処

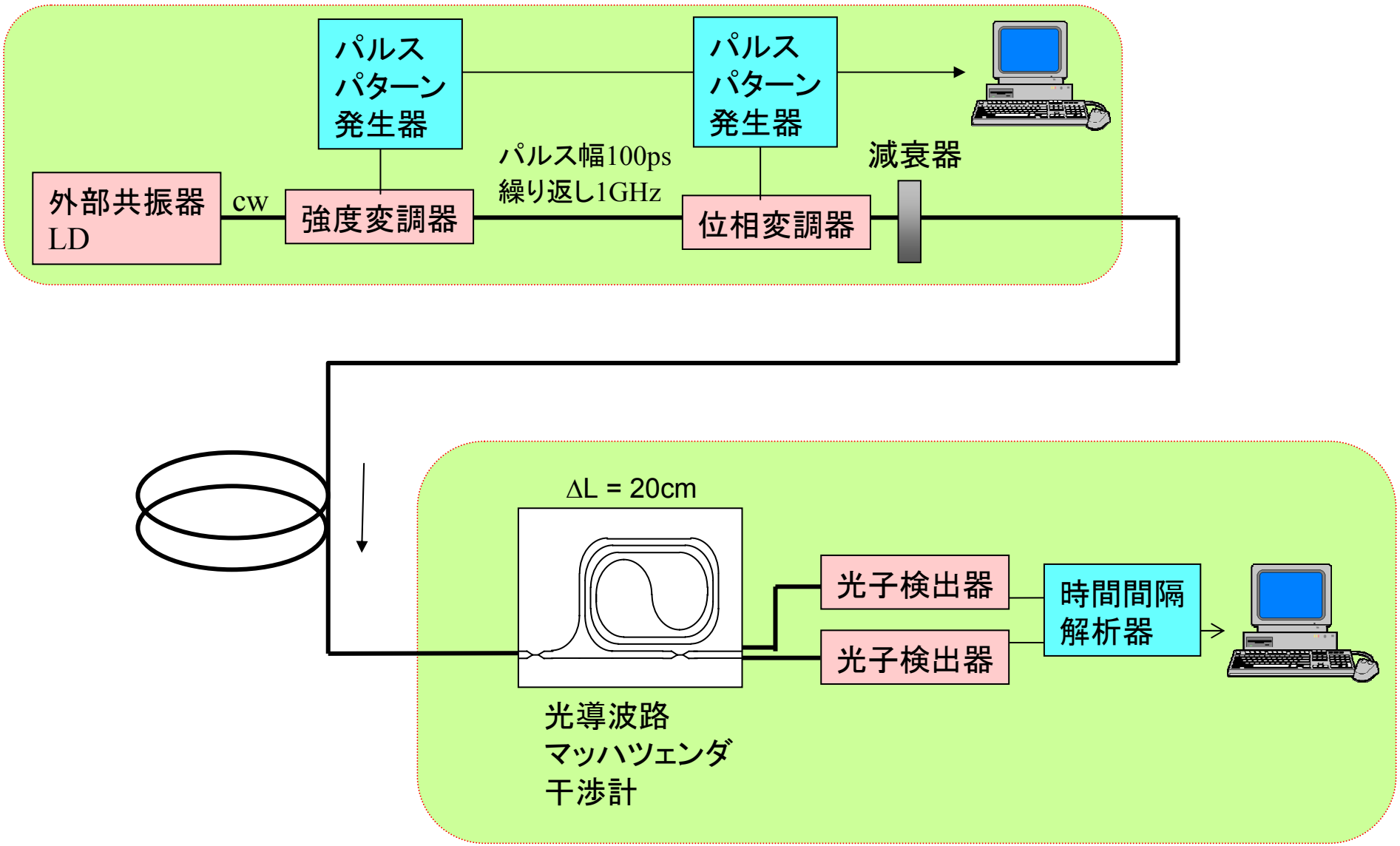
なりすまし盗聴



受信結果に基づいて偽装信号を送信。
位相測定できるのは一部のみ。
光子検出しなかったスロットは空で送信。

ビット誤り ← テストビットのチェックにより盗聴発覚

差動位相シフト方式　ー実験系ー

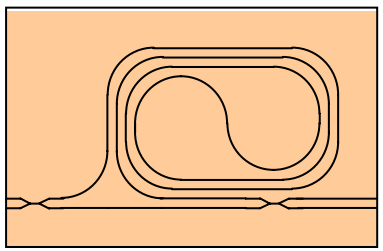


要素技術1

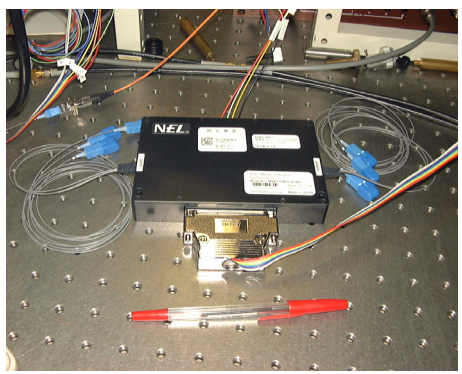
PLCマッハツェンダ干渉計

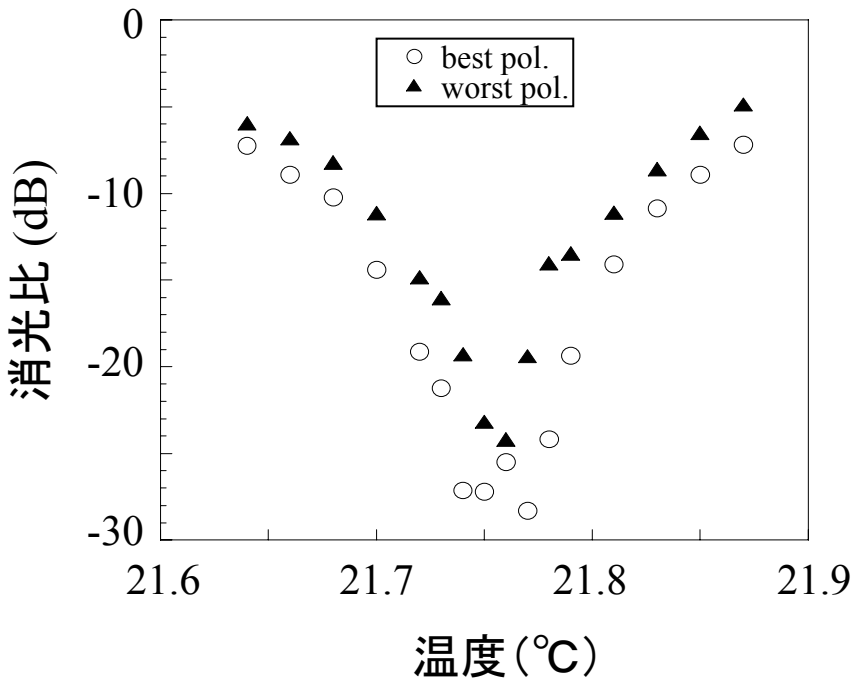
(PLC：Planar Lightwave Circuit)

光路長差20cm



損失 2.6 dB（fiber-fiber）



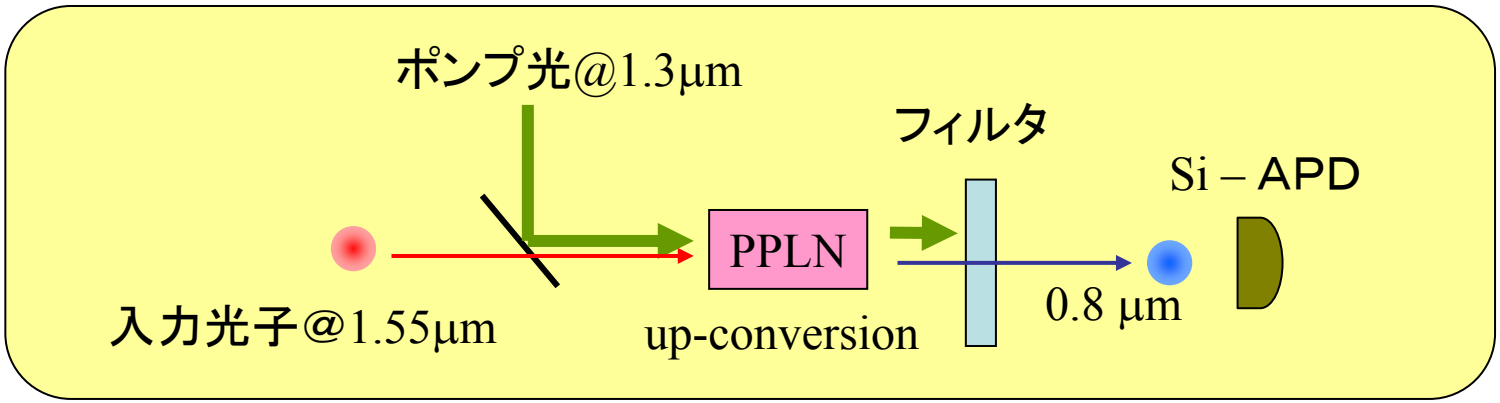


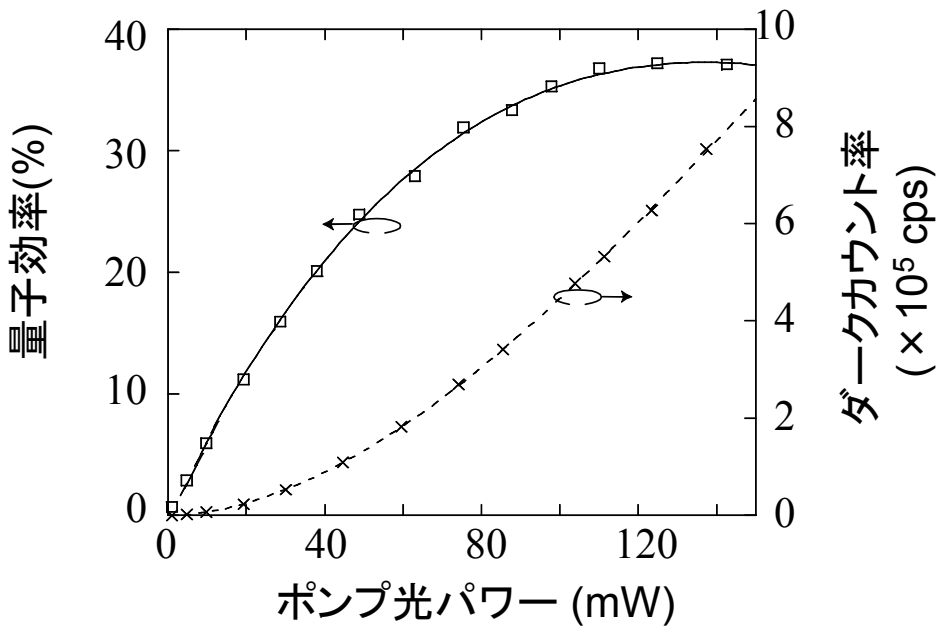
最悪偏波でも20dB以上の消光比

要素技術2

周波数変換型光子検出器

高性能なSi－APDを利用



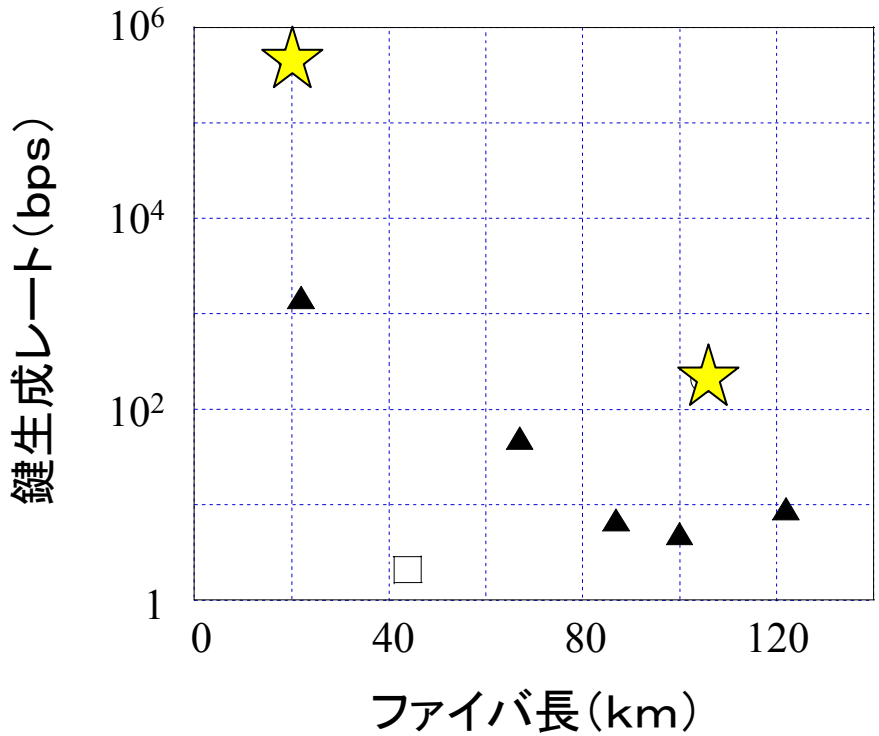


non-gating mode

↓

高い鍵生成レート

差動位相シフト方式　ー実験結果ー

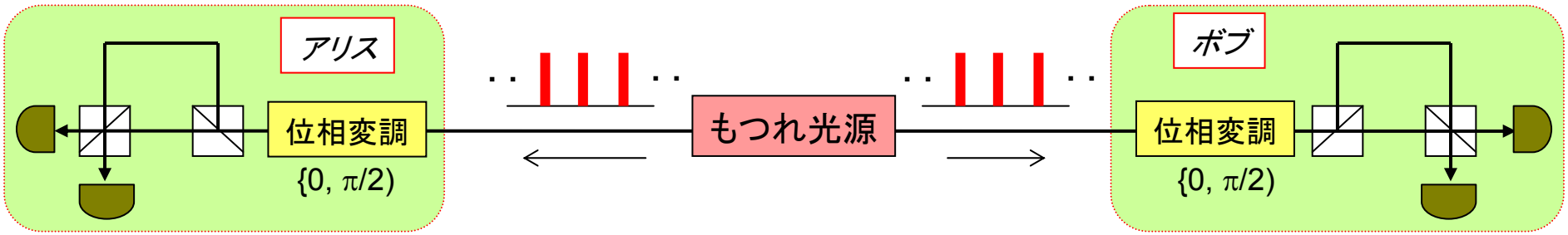


（今後の展開）

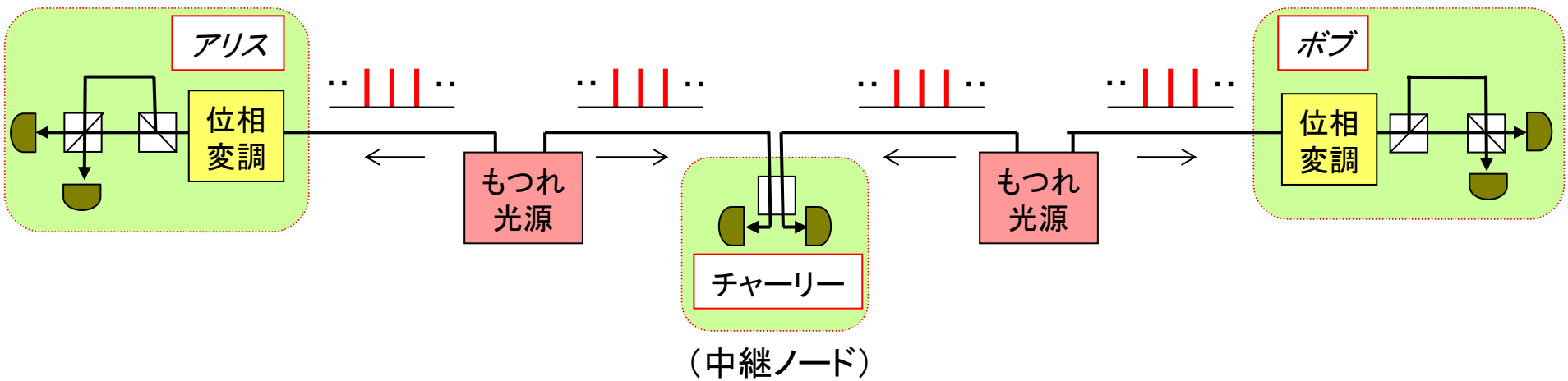
量子もつれによる量子鍵配送

量子もつれ利用による量子鍵配送の長距離化

量子もつれ鍵配送



量子リレー鍵配送



（中継ノード）

[内容]

[1] 量子暗号プロトコル　–位相エンコードBB84-

　　構成、動作原理、安全性

[2] 量子暗号実験

　　光子検出器

　　プラグ＆プレイ構成

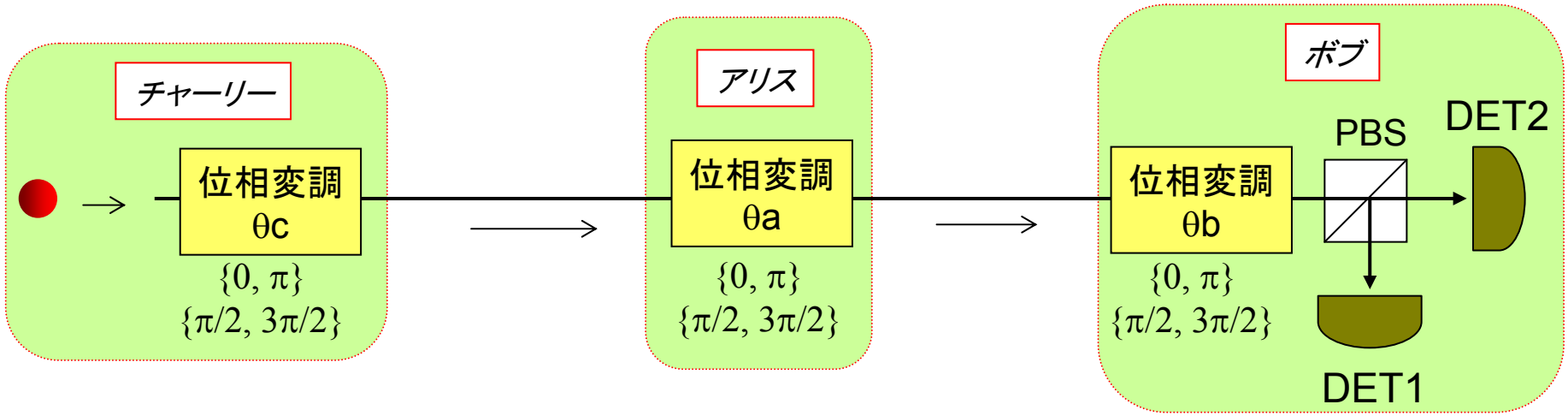
[3] 差動位相シフト量子鍵配送

[4] 量子秘密共有

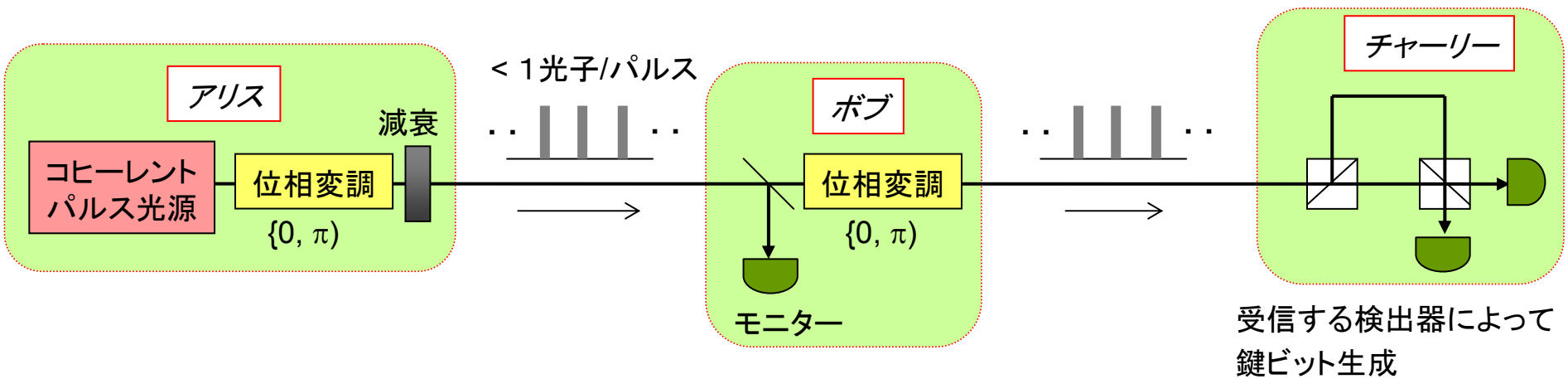
量子秘密共有(Quantum Secret Sharing)

チャーリーの暗号鍵をアリスとボブは共同作業によってのみ知ることができるシステム

従来提案:偏波エンコード



差動位相方式



光の量子的性質を利用した
安全な暗号通信・量子秘密共有

[内容]

[1] 量子暗号プロトコル　–位相エンコードBB84-

　　構成、動作原理、安全性

[2] 量子暗号実験

　　光子検出器

　　プラグ＆プレイ構成

[3] 差動位相シフト量子鍵配送

[4] 量子秘密共有