量子暗号研究の動向

大阪大学

井上　恭

内容

[1] **量子暗号の概略**

[2] **各種プロトコル**

BB84、B92、BBM92、DPS

[3] **実験**

(1) **光子検出器**

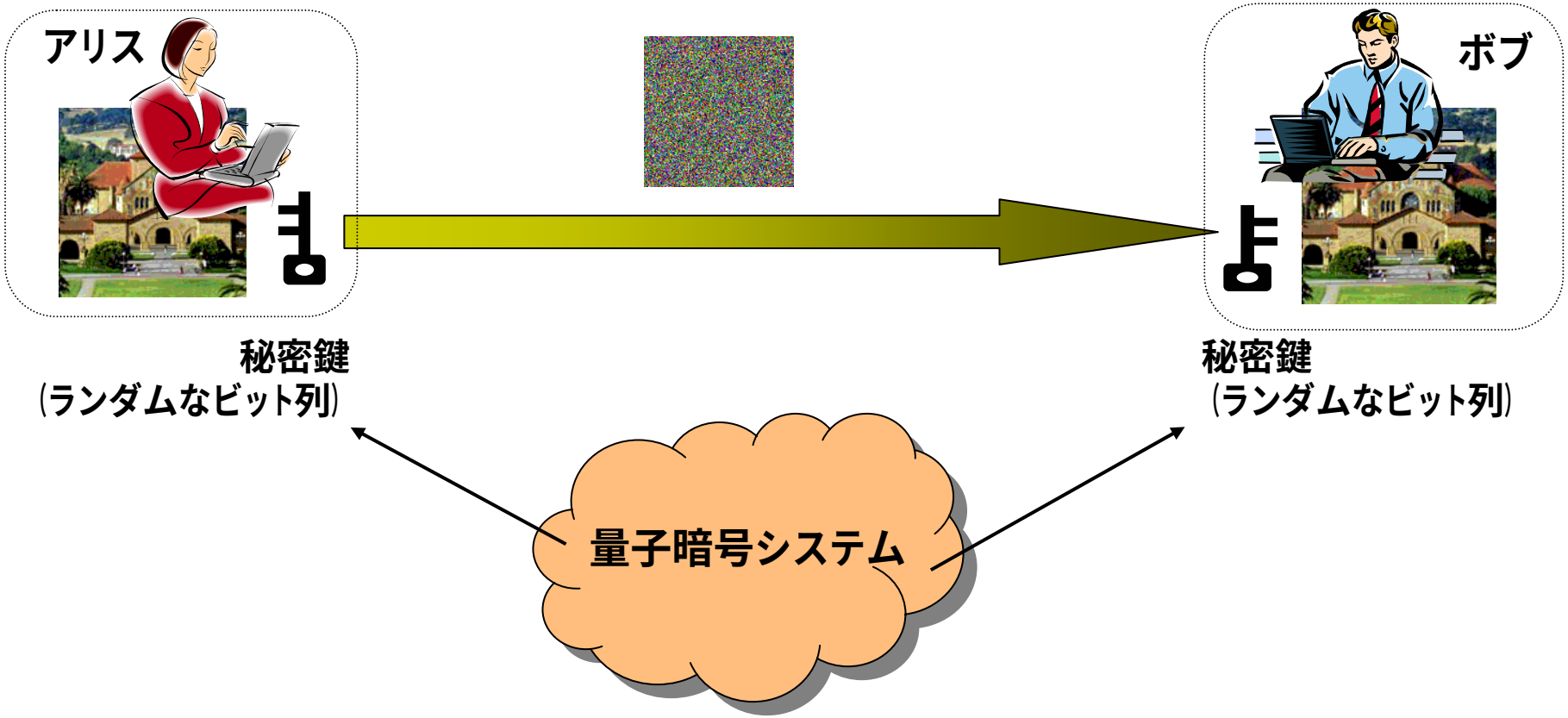
(2) BB84　**プラグ＆プレイ**

(3) DPS

[4] **連続変数量子鍵配送**

[5] **量子もつれ鍵配送**

量子鍵配送



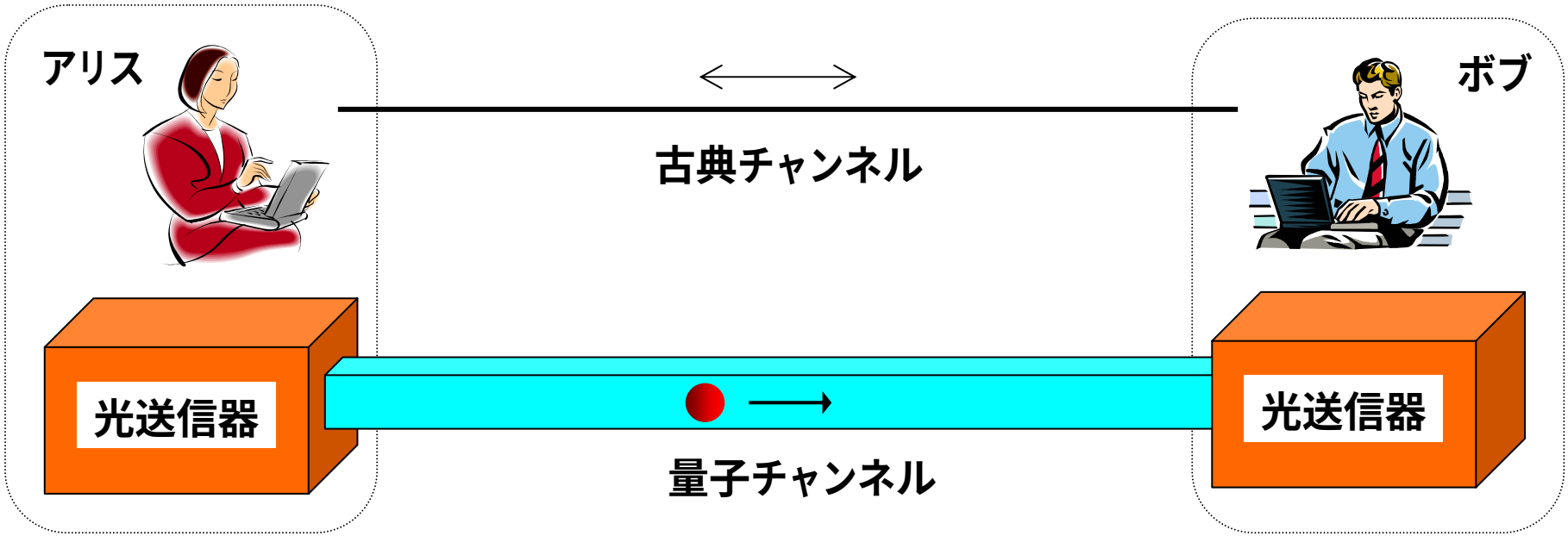
量子暗号 (量子鍵配送)

目的 量子力学的に秘匿性が保証された秘密鍵を2者に供給

売り文句 安全性は量子力学的に保証

前提 盗聴者は物理法則に反しない限り何でもできる。それでも安全。

量子鍵配送の基本構図



①量子チャンネルで光子を送受信

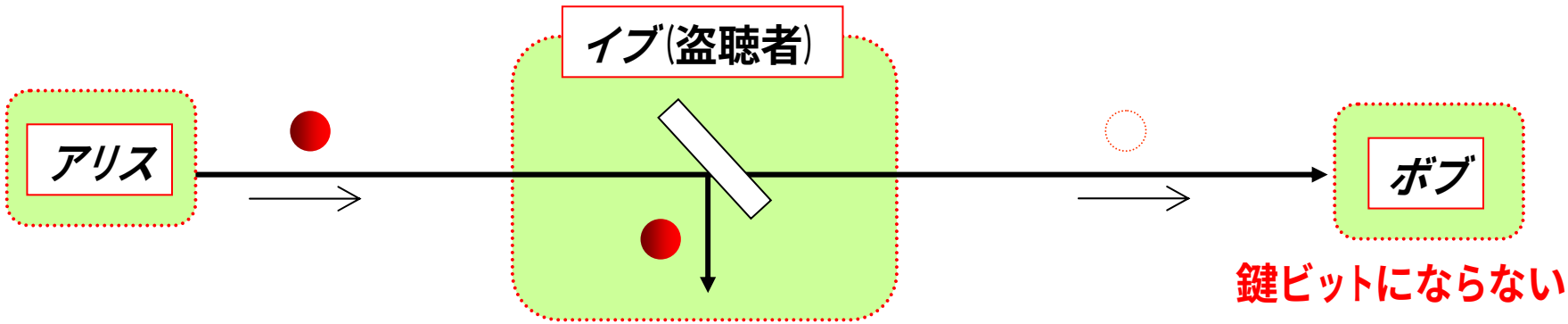
②古典チャンネルで送受信系に関する情報交換

③鍵ビット生成

④誤り訂正・秘匿性増強 → 秘密鍵

量子鍵配送の安全性

ビームスプリット盗聴



鍵ビットにならない

なりすまし盗聴

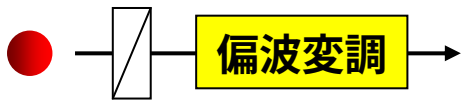
受信結果に基づいて偽装信号を送信。
が、光子状態は確率的（重ね合わせ状態）。
ので、1回の測定で正確な状態識別は不可能。

ビット誤り
↓
テストビットチェックより
盗聴発覚

各種プロトコル

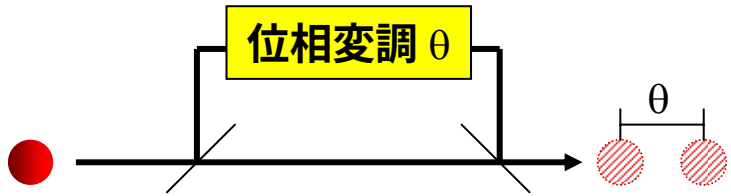
BB84　4つの非直交状態

偏波エンコード



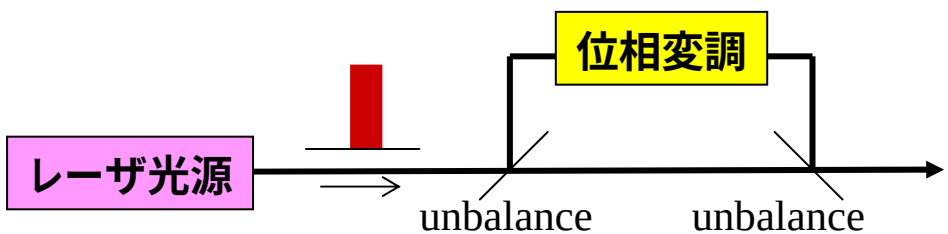
ビット情報	直線	円
「0」	↔	↻
「1」	↕	↺

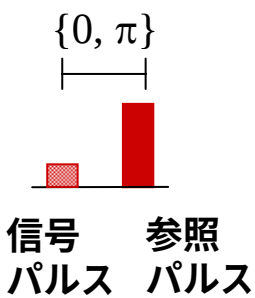
位相エンコード

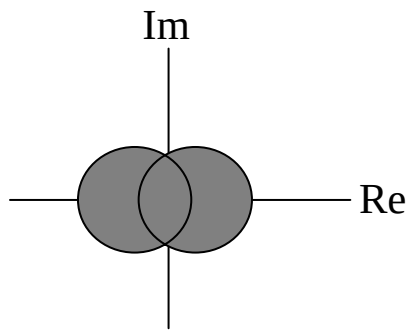


ビット情報	{0, π}	$\left\{-\frac{\pi}{2}, \frac{\pi}{2}\right\}$
「0」	0	-π/2
「1」	π	π/2

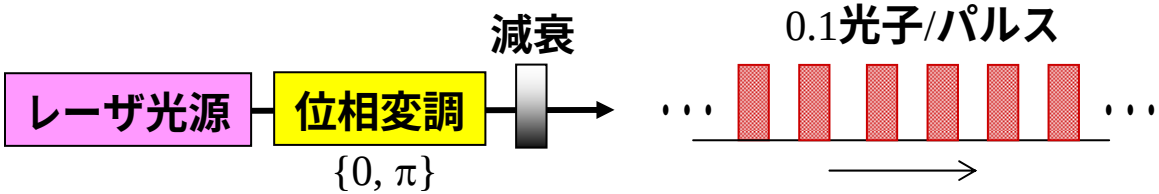
B92　2つの非直交状態



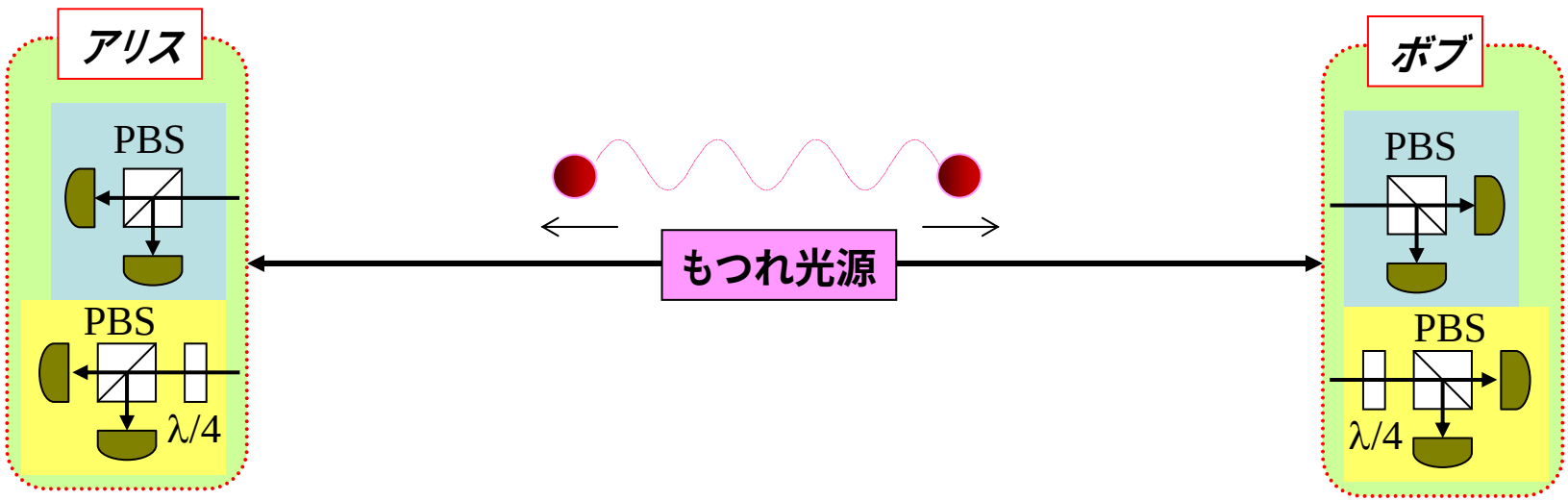




DPS　弱コヒーレント光パルス列

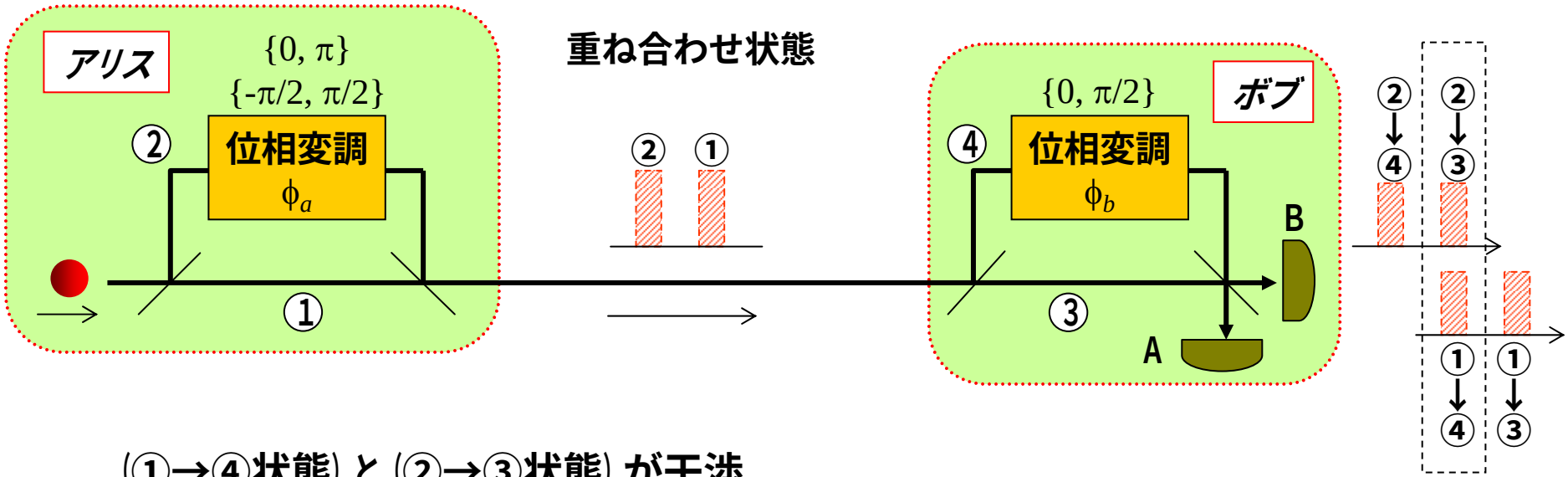


BBM92　量子もつれ光子＋BB84



では具体的に

位相エンコードBB84：構成



(①→④状態) と (②→③状態) が干渉

$$\begin{cases} \theta_1 + \theta_4 = \theta_2 + \theta_3 & \Rightarrow \text{検出器A} \\ \theta_1 + \theta_4 = \theta_2 + \theta_3 + \pi & \Rightarrow \text{検出器B} \end{cases} \Rightarrow \begin{cases} \phi_b - \phi_a = 0 & \Rightarrow \text{検出器A} \\ \phi_b - \phi_a = \pi & \Rightarrow \text{検出器B} \end{cases}$$

ϕ_a \ ϕ_b	0	π/2
-π/2	A/B	B
0	A	A/B
π/2	A/B	A
π	B	A/B

位相エンコードBB84：鍵生成手順

①アリス：ϕ_a をランダムに設定して光子を送信

②ボブ：ϕ_b をランダムに設定して光子を検出

③ボブ→アリス：どの光子が真ん中の時刻で検出されたか、
それについて自分の位相が0かπ/2か、を通知。

④アリス→ボブ：真ん中時刻で検出された光子について、
自分の位相が $\{0, \pi\}$ か $\{\pi/2, 3\pi/2\}$か、を通知。

⑤光子検出器が確定している場合について鍵ビット生成

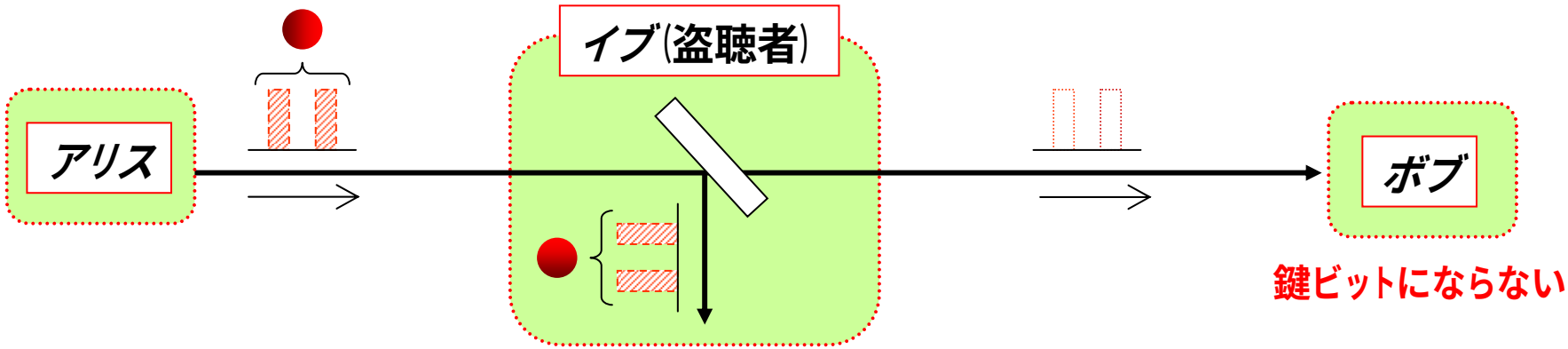
$\phi_a = \{0, \pi\}$ かつ $\phi_b = 0$ の場合
$\phi_a = \{-\pi/2, \pi/2\}$ かつ $\phi_b = \pi/2$ の場合
} A ⇒「0」 B ⇒「1」

不確定な場合 (A/B) は無視。

ϕ_a \ ϕ_b	0	π/2
-π/2	A/B	(B)
0	(A)	A/B
π/2	A/B	(A)
π	(B)	A/B

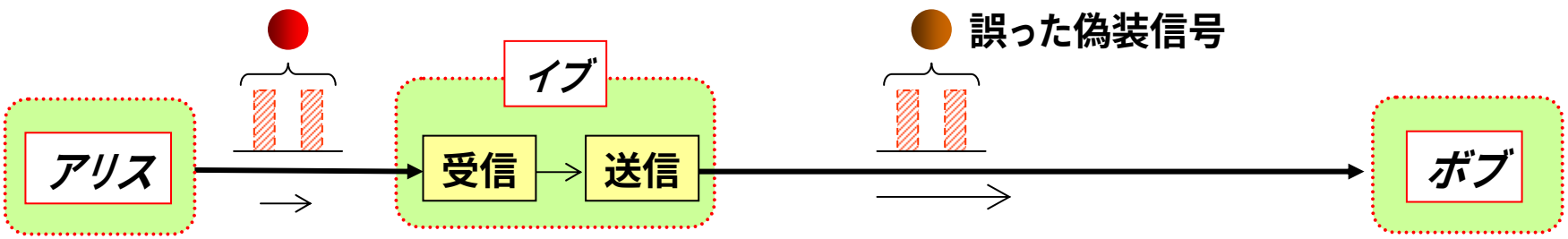
位相エンコードBB84：安全性

ビームスプリット盗聴

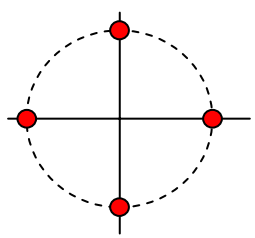


鍵ビットにならない

なりすまし盗聴



4つの位相値を全て識別するのは不可能



ビット誤り

↓

テストビットチェックより
盗聴発覚

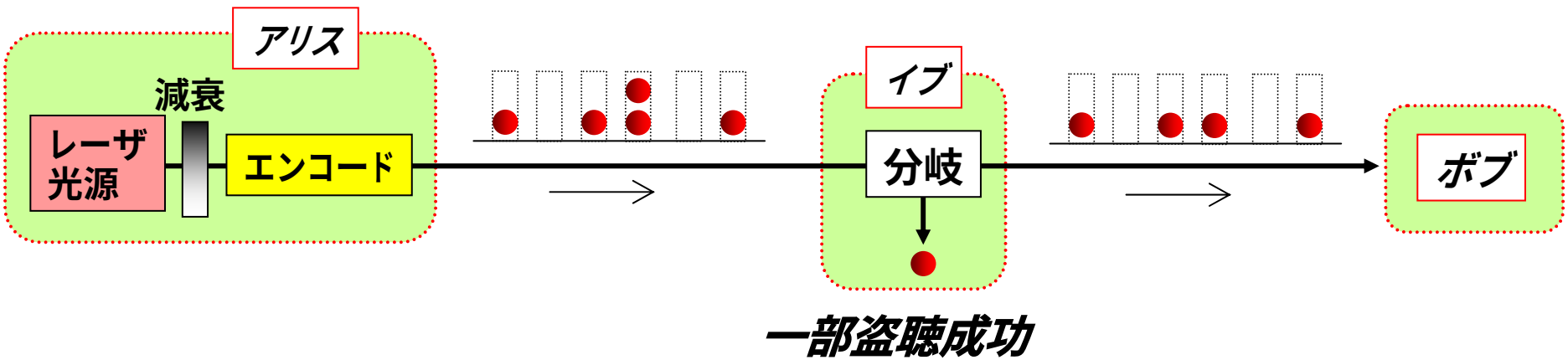
ところが

減衰レーザ光には2光子/信号の場合あり

実際には弱めたレーザ光を擬似単一光子をして使用

↓

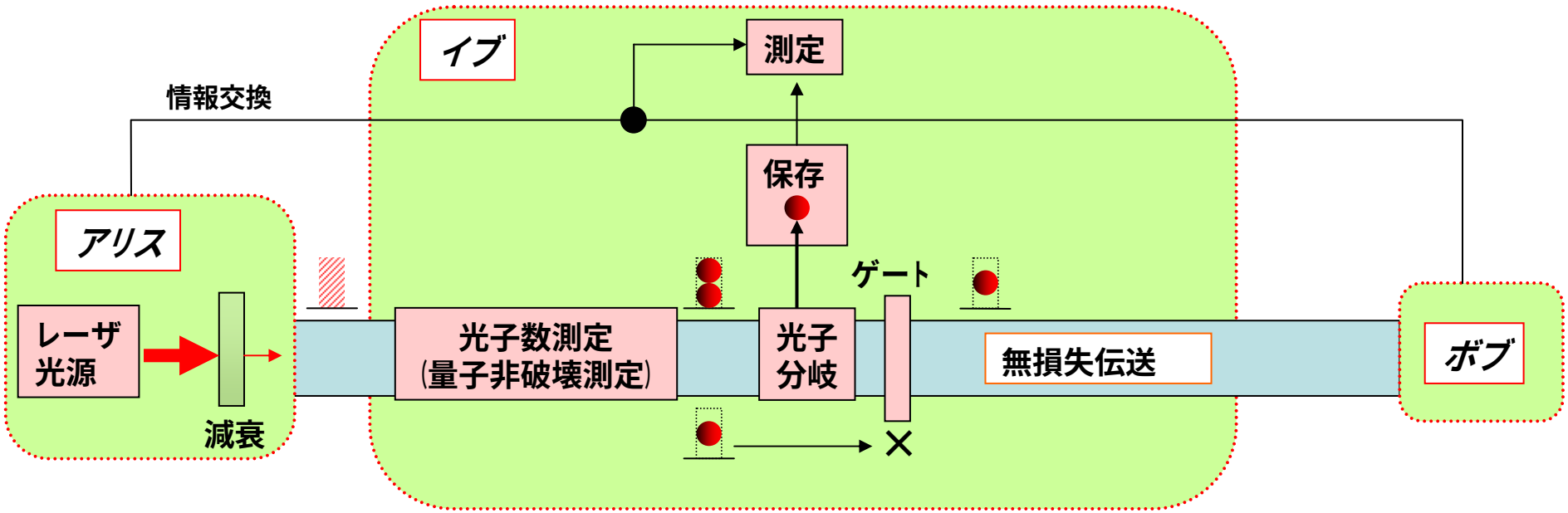
量子揺らぎにより、2光子発生確率あり。



一部盗聴成功

イブが万能とするとさらにやっかい

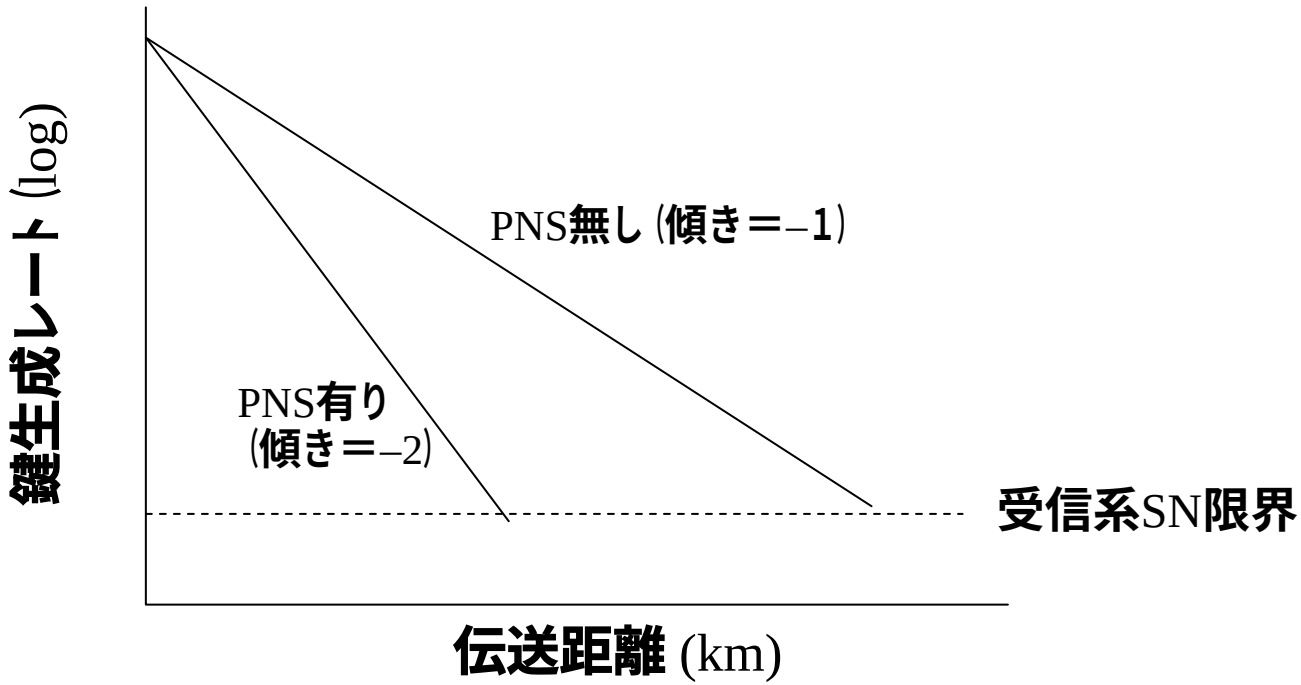
光子数分岐盗聴



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モード情報に基づいて保存しておいた光子を測定する

2光子パルスの確率＝伝送路損失の場合 ⇒ 100%盗聴

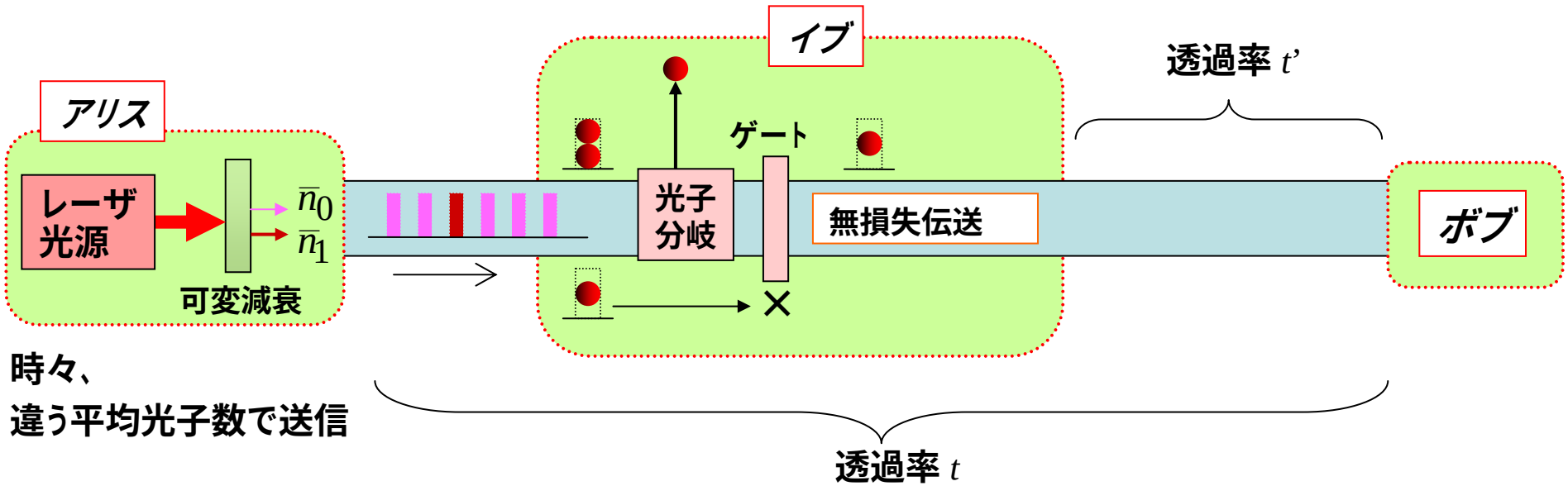
光子数分岐 (PNS)盗聴に対処するには、
2光子確率を小さくする＝送信光レベルを小さくする



伝送距離に厳しい制限

そこで

デコイBB84量子鍵配送



時々、
違う平均光子数で送信

送信光子数	ボブ受信光子数 正常時	光子数分岐攻撃時
$\bar{n}_0$	$t\bar{n}_0$	$t'P_2(\bar{n}_0)$
$\bar{n}_1$	$t\bar{n}_1$	$t'P_2(\bar{n}_1)$

盗聴がばれないためには、

$$\begin{cases} t\bar{n}_0 = t'P_2(\bar{n}_0) \\ t\bar{n}_1 = t'P_2(\bar{n}_1) \end{cases} \Rightarrow \frac{\bar{n}_0}{\bar{n}_1} = e^{-(\bar{n}_0-\bar{n}_1)}\left(\frac{\bar{n}_0}{\bar{n}_1}\right)^2$$

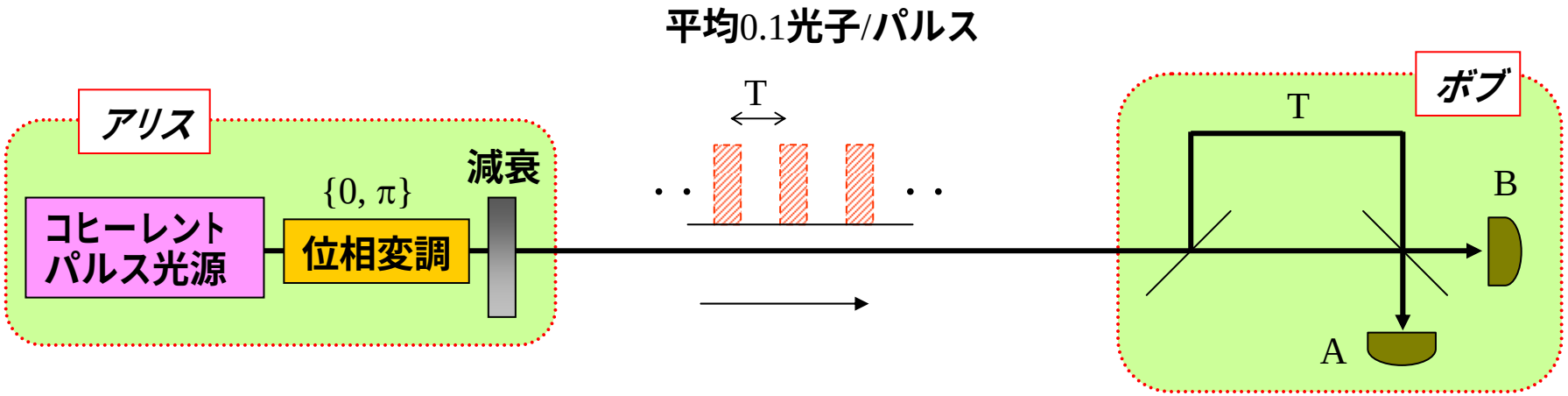
この等式を満たすのは不可能

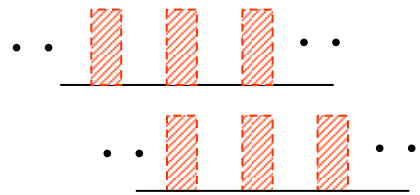
盗聴発覚

$P_2(\bar{n}) = \dfrac{e^{-\bar{n}}\bar{n}^2}{2}$：平均光子数$\bar{n}$の時の２光子確率

ニュータイプ

DPS（差動位相シフト）量子鍵配送





前後の位相差に応じて
光子検出

鍵生成手順

①ボブ：光子を検出した時刻と検出器を記録

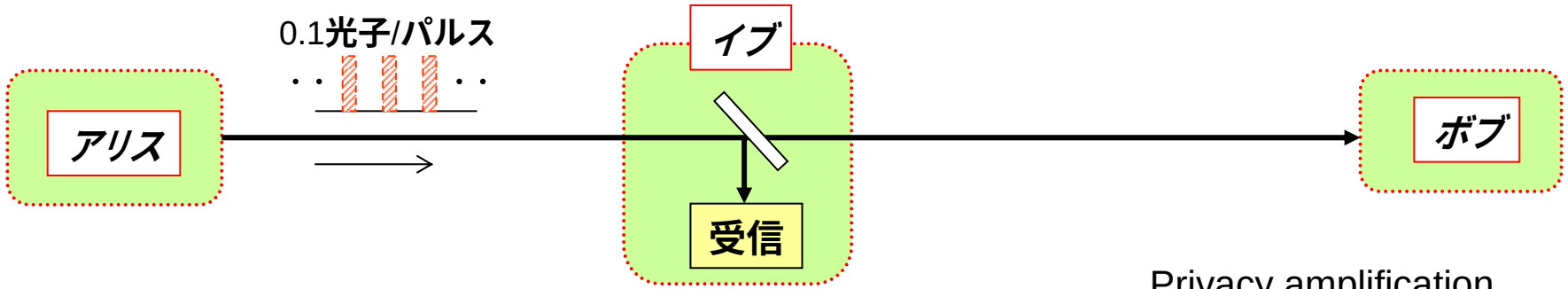
②ボブ→アリス：光子検出時刻を通知

③アリス：検出時刻と位相変調データから光子検出した検出器がわかる

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

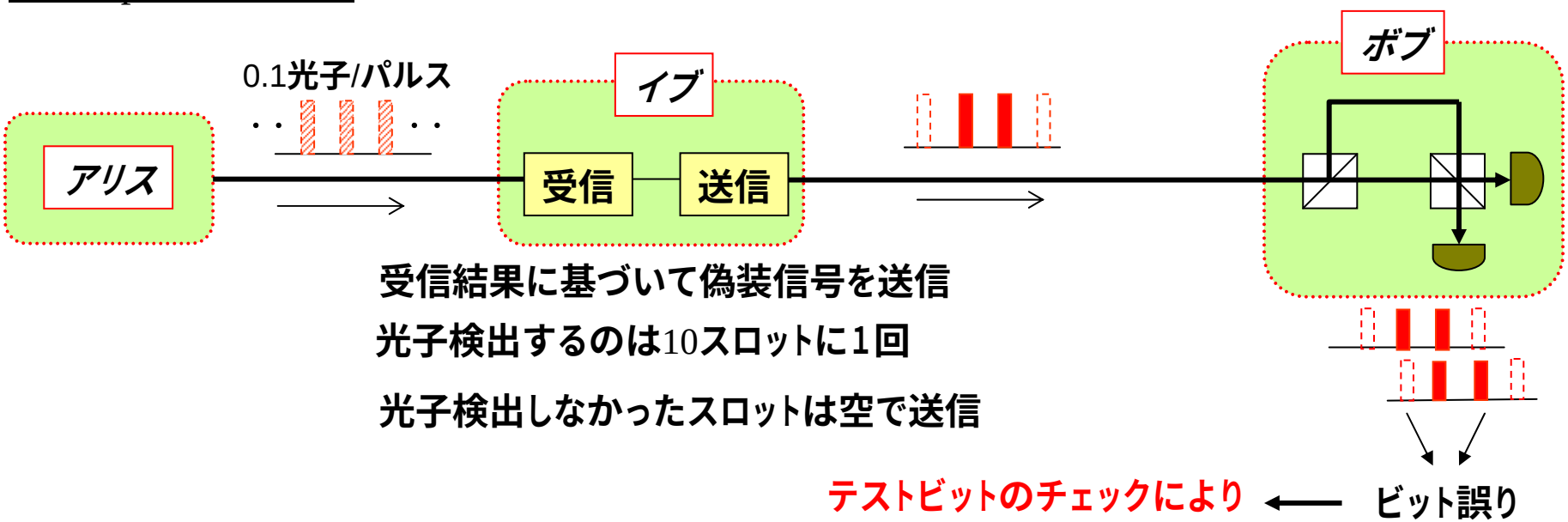
DPS方式の安全性

ビームスプリット盗聴



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

intercept/resend盗聴



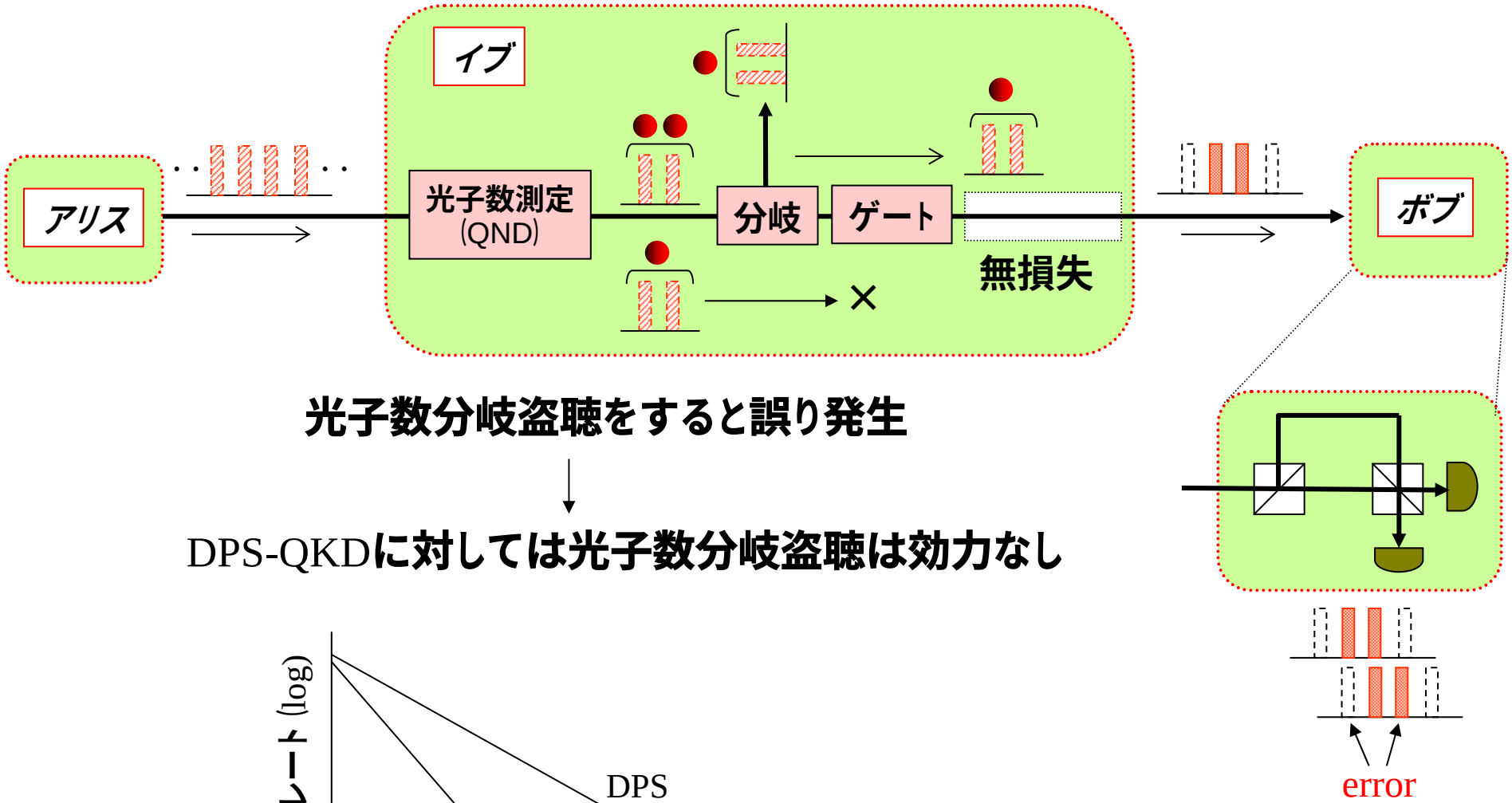
受信結果に基づいて偽装信号を送信

光子検出するのは10スロットに1回

光子検出しなかったスロットは空で送信

テストビットのチェックにより盗聴発覚 ← ビット誤り

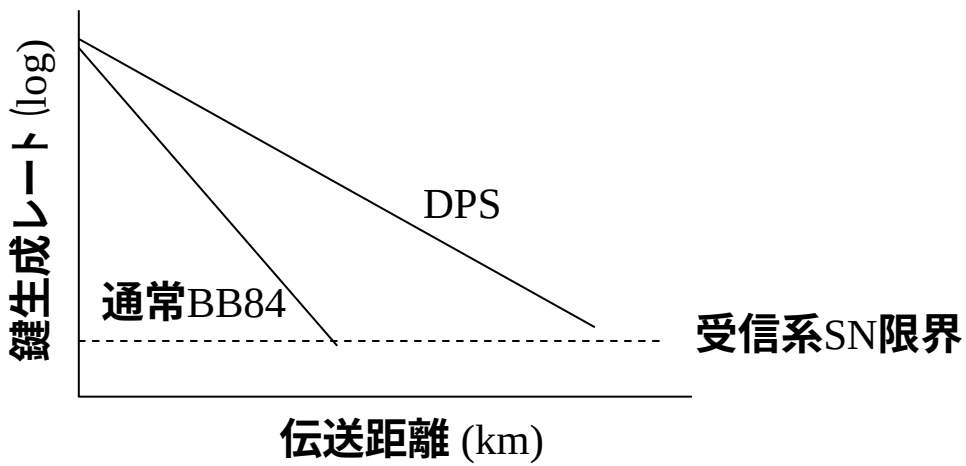
DPS方式に対する光子数分岐盗聴



光子数分岐盗聴をすると誤り発生

↓

DPS-QKD**に対しては光子数分岐盗聴は効力なし**



内容

[1] **量子暗号の概略**

[2] **各種プロトコル**

BB84、B92、BBM92、DPS

[3] **実験**

(1) **光子検出器**

(2) BB84　**プラグ＆プレイ**

(3) DPS

[4] **連続変数量子鍵配送**

[5] **量子もつれ鍵配送**

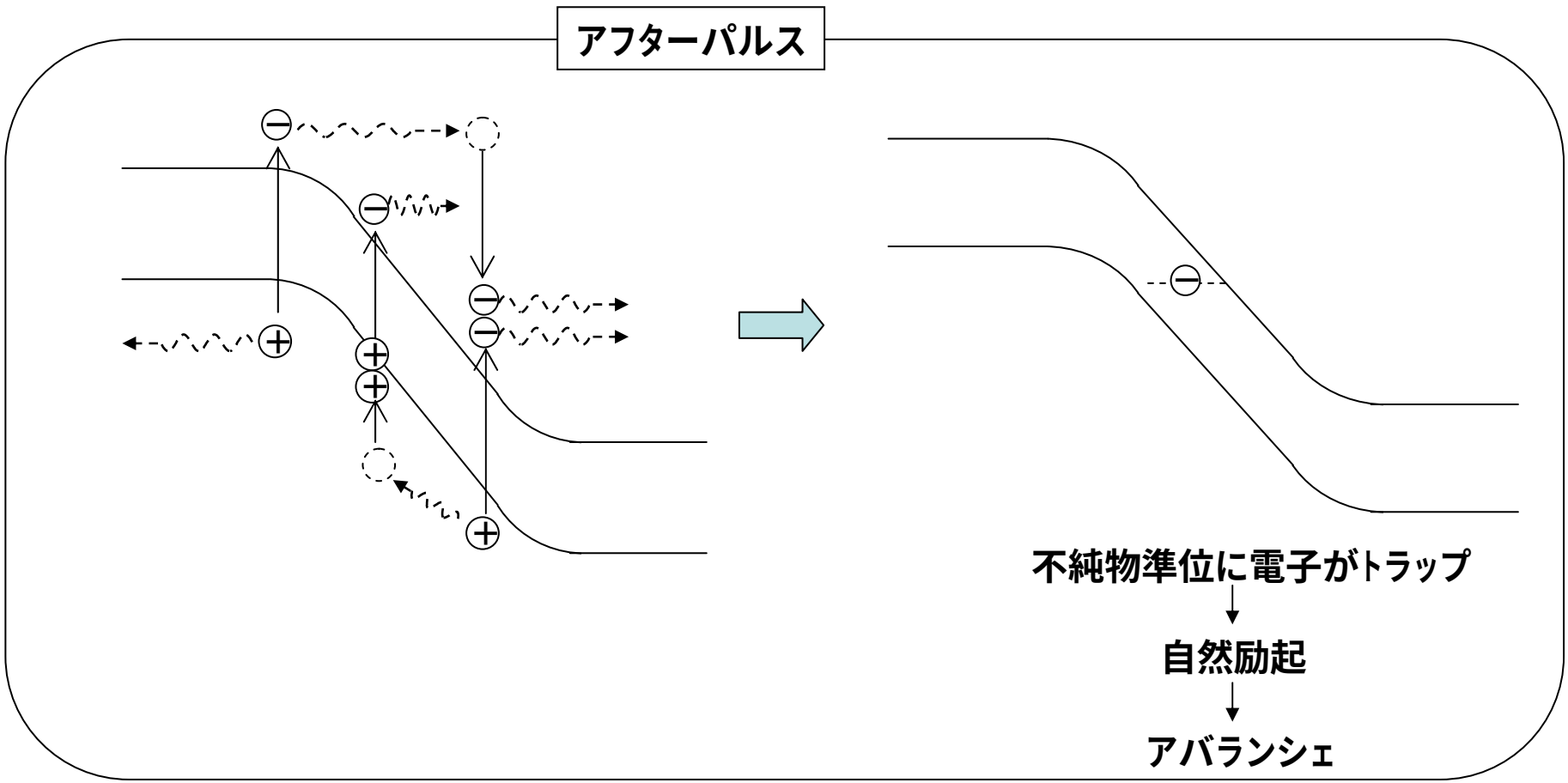
APD光子検出器

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）



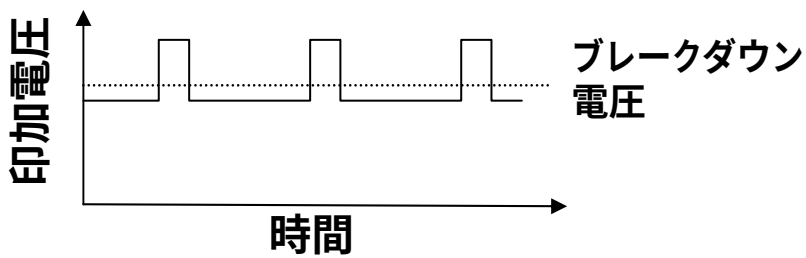
APD光子検出器の現状

短波長帯：市販の Si-APD**あり**

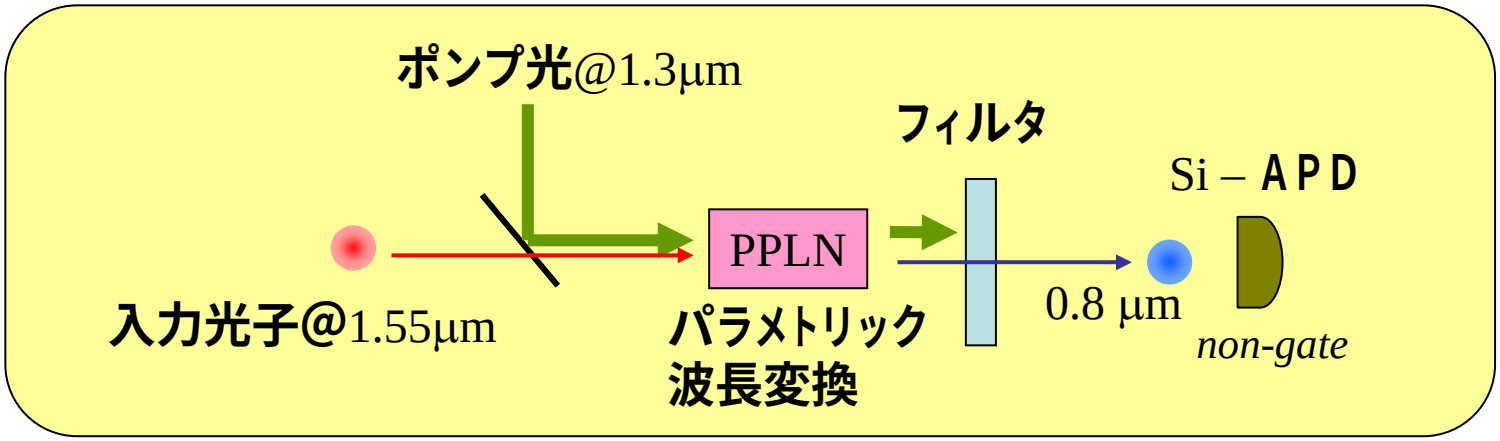
量子効率 ～ 60%、**ダークカウント** < 100cps

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**

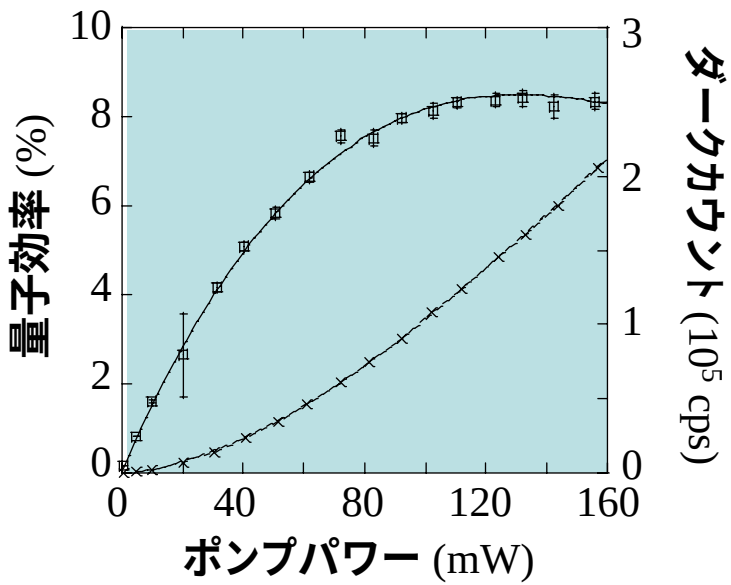
量子効率 ～ 10%、**ダークカウント～**10^{-5}/gate、**繰り返し ＜ 数**MHz



波長変換型光子検出器

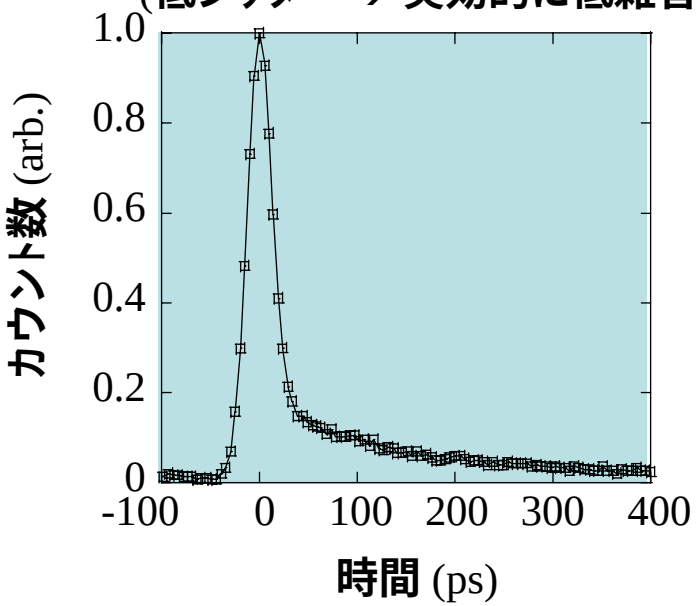


効率＆ダークカウント



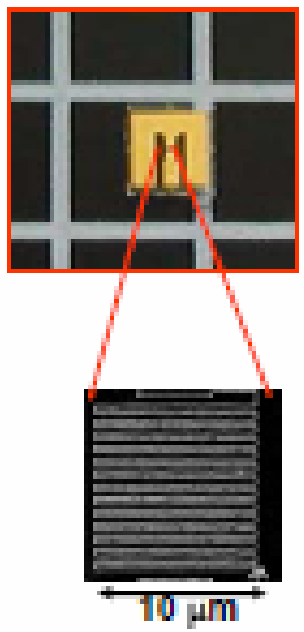
ジッター

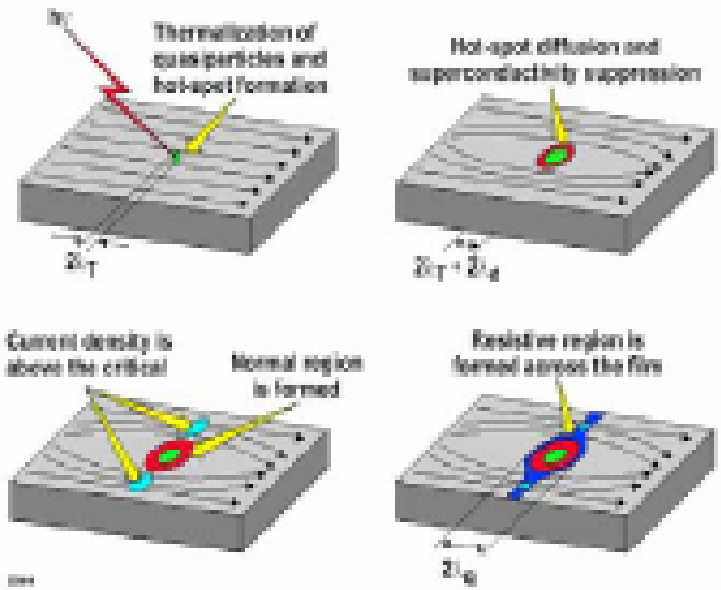
(低ジッター → 実効的に低雑音)



超伝導光子検出器

超伝導素子に光子入射 → 光子吸収 → 発熱 → 超伝導状態変化 → 出力信号

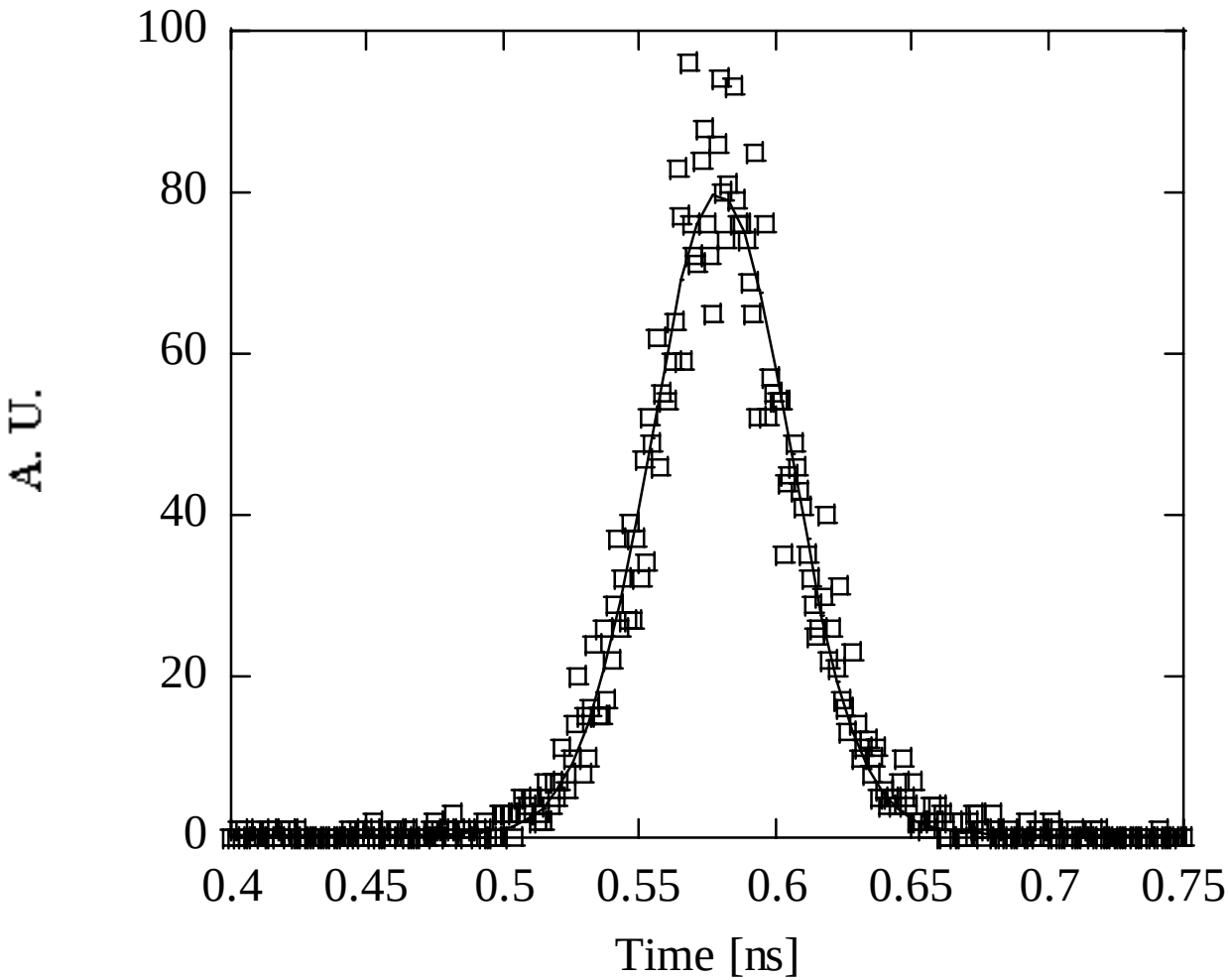




- Current Biased
- Recovery inductance limited
- Low jitter (10's ps)
- System Detection Efficiency

NIST

超伝導光子検出器特性例

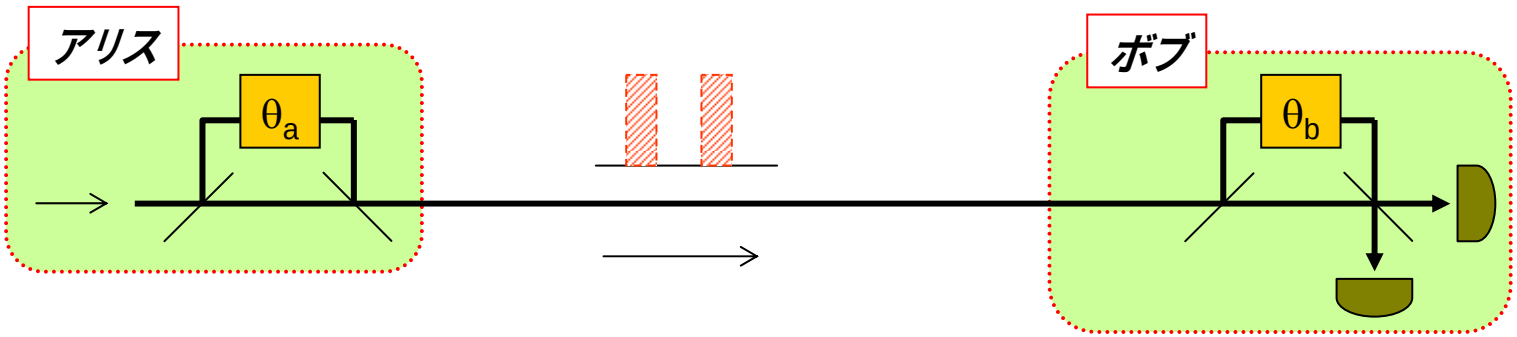


入力光：10 ps pulse
時間分解能：60 ps.

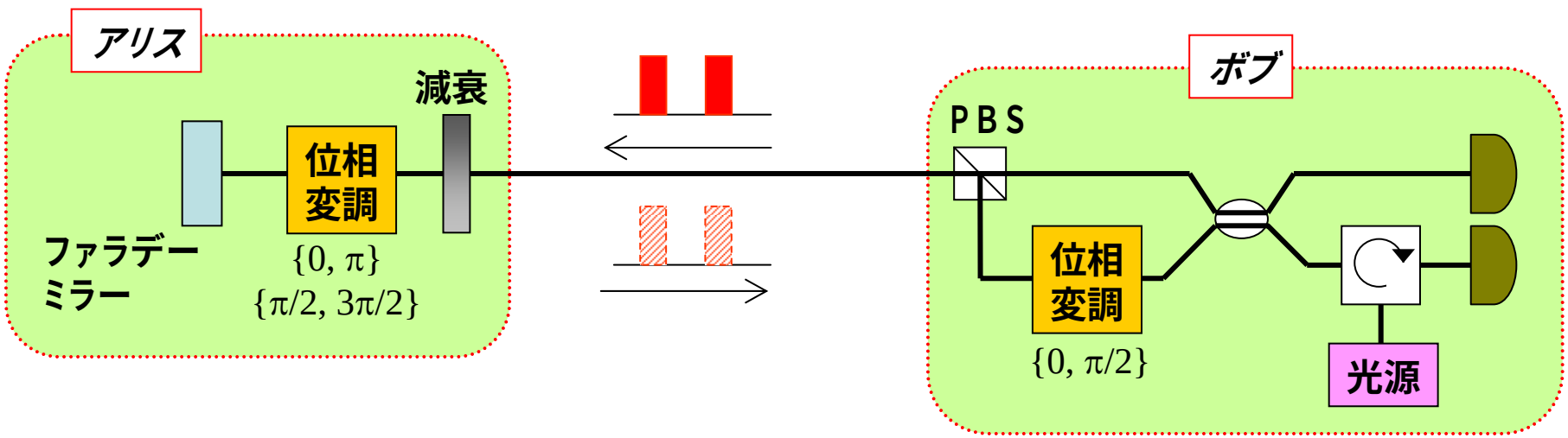
量子効率：0.7%
ダークカウント：< 10 cps

BB84ーQKD実験：プラグ＆プレイシステム

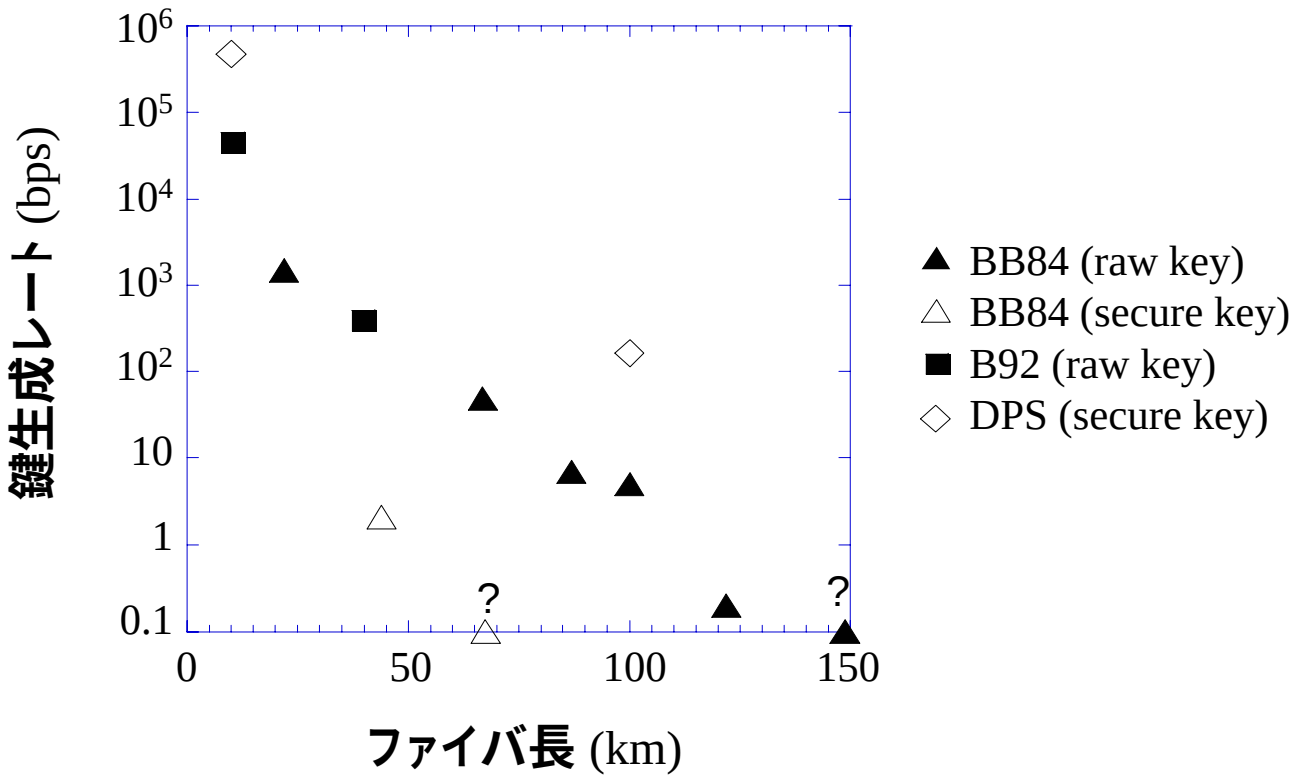
位相エンコードＢＢ８４を行うには、干渉計の安定性が難点



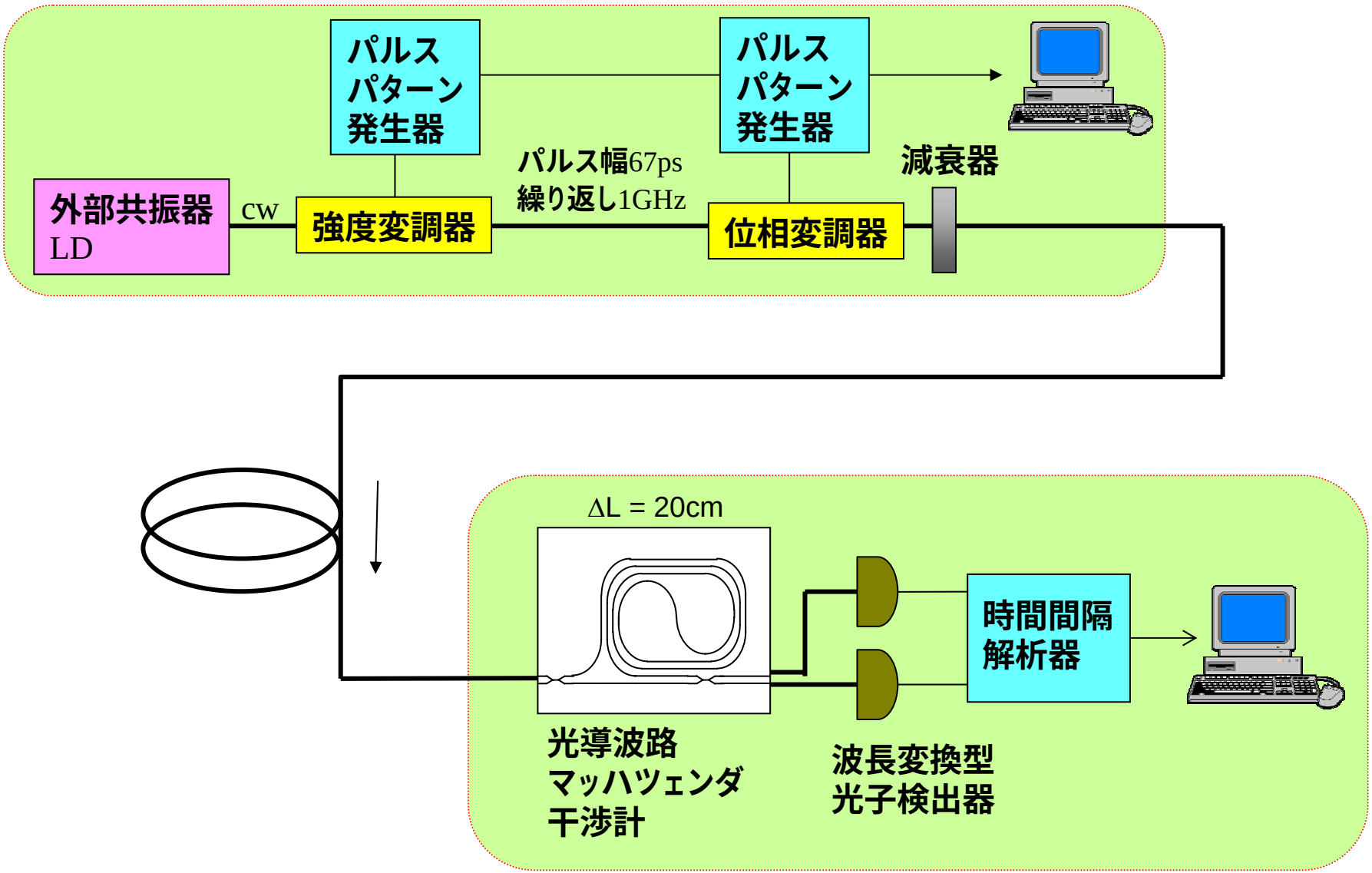
光を折り返す構成により位相変動を自動補償: plug & play構成



これまでの量子鍵配送実験報告例



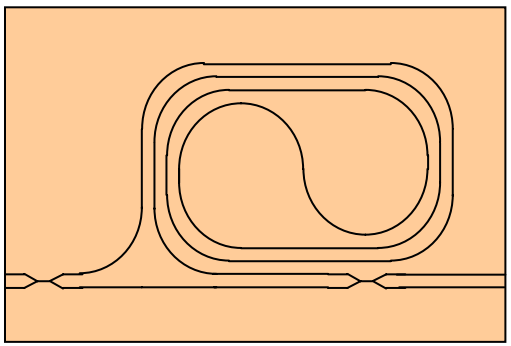
DPS－QKD実験


パルス
パターン
発生器
パルス
パターン
発生器
外部共振器
LD
CW
強度変調器
パルス幅67ps
繰り返し1GHz
位相変調器
減衰器
ΔL = 20cm
時間間隔
解析器
光導波路
マッハツェンダ
干渉計
波長変換型
光子検出器

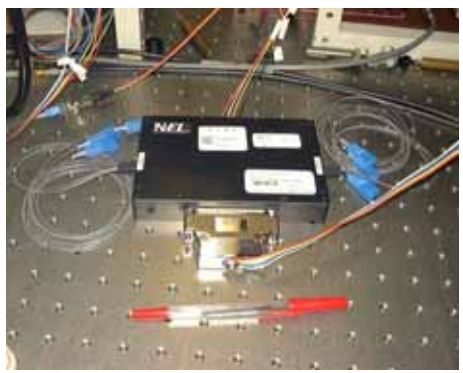
要素デバイス

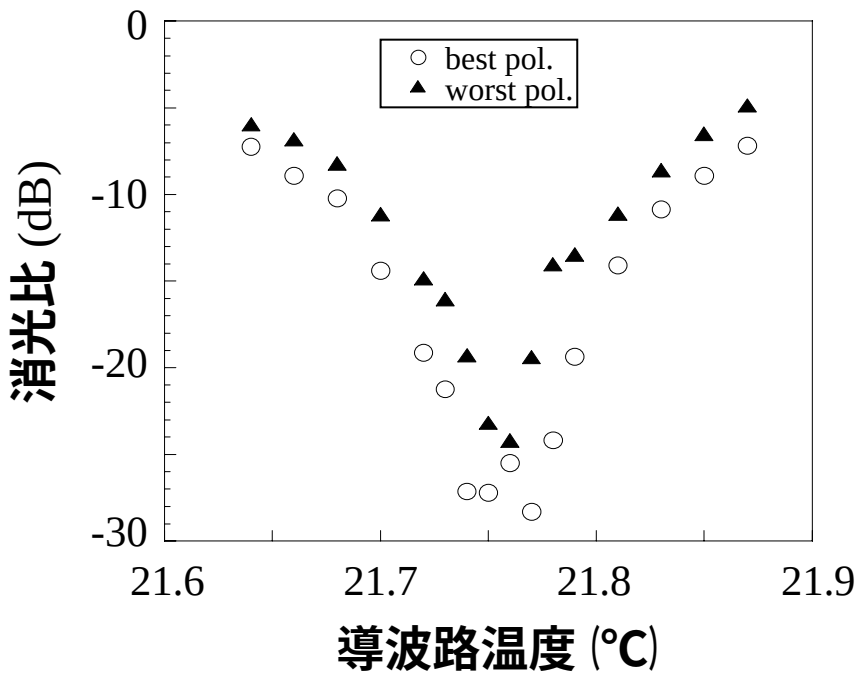
PLCマッハツェンダ干渉計

光路長差20cm
(時間差 1ns)



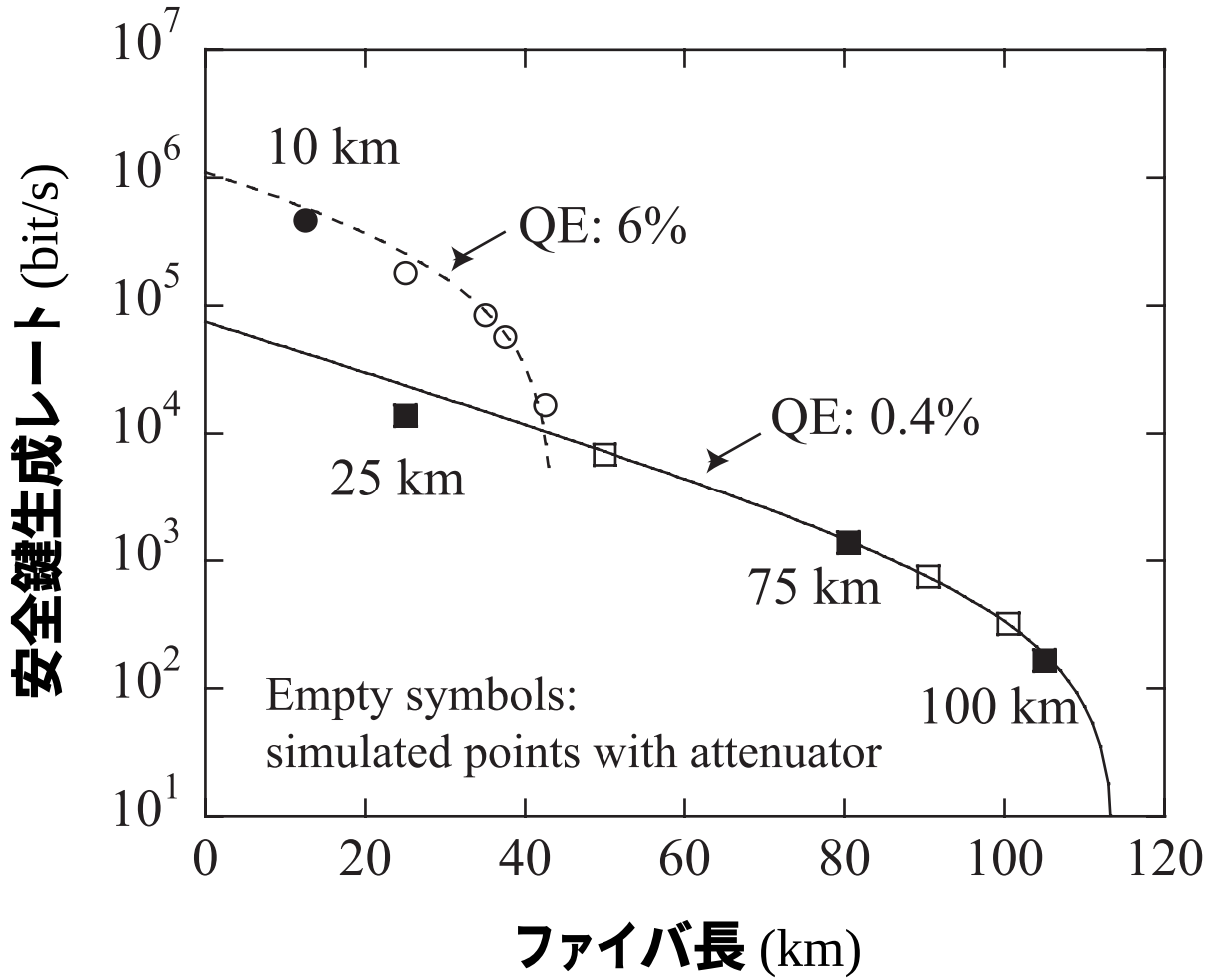
損失 2 dB (fiber-fiber)





最悪偏波でも20dB以上の消光比

DPS-QKD実験結果


安全鍵生成レート (bit/s)
10^7
10^6
10^5
10^4
10^3
10^2
10^1
10 km
QE: 6%
QE: 0.4%
25 km
75 km
100 km
Empty symbols:
simulated points with attenuator
0
20
40
60
80
100
120
ファイバ長 (km)

内容

[1] **量子暗号の概略**

[2] **各種プロトコル**

[3] **実験**

[4] **連続変数量子鍵配送**

量子鍵配送の難関は光子検出

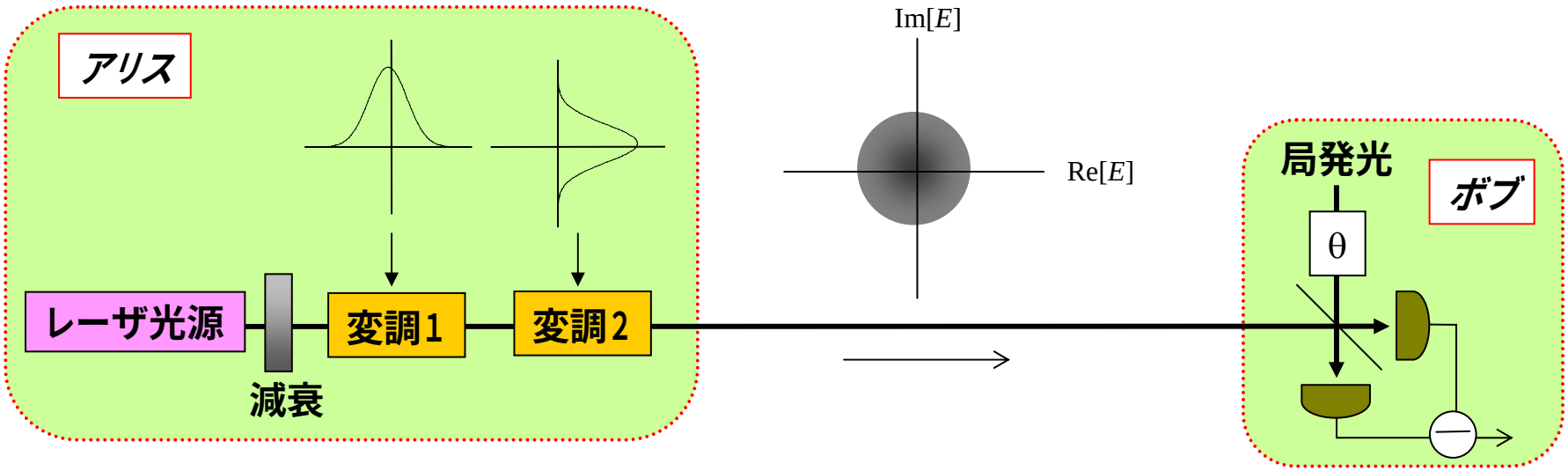
↓

通常の光検出器が使えないか

[5] **量子もつれ鍵配送**

連続変数量子鍵配送 (Continuous Variable QKD)

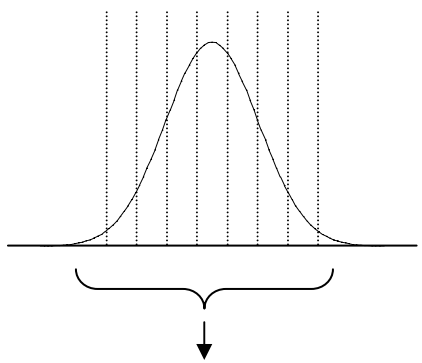
ー量子雑音を利用する量子鍵配送ー



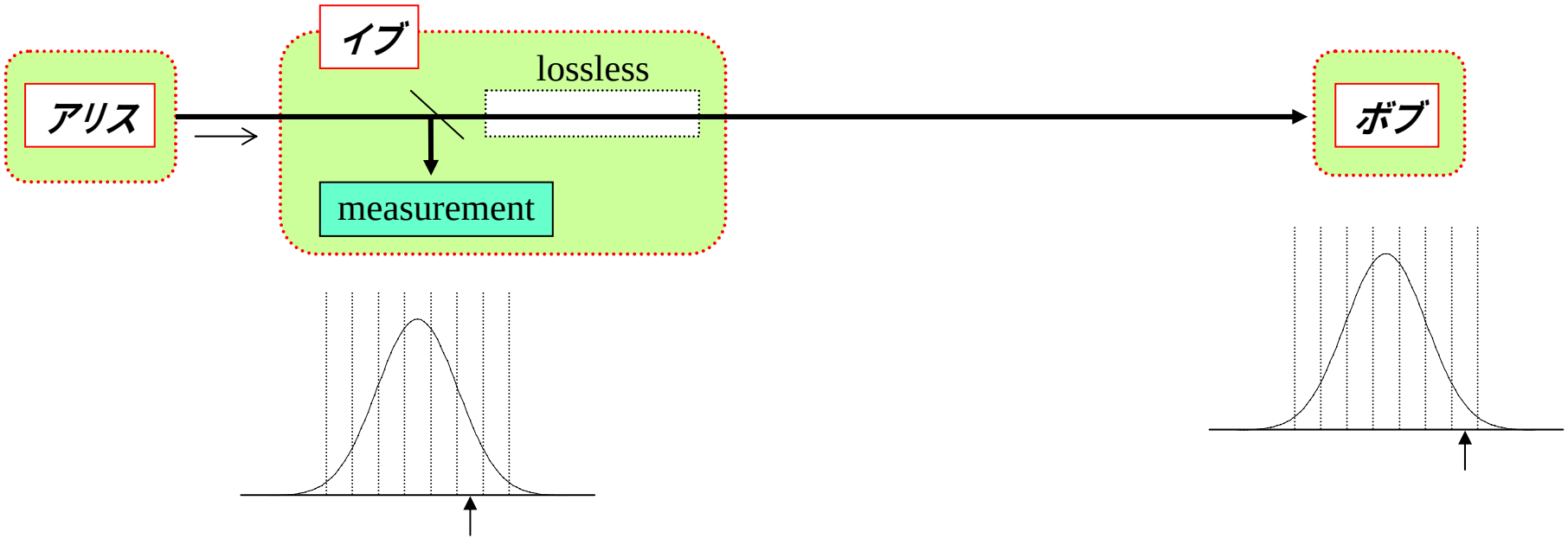
通常の受光素子が使用可能

↓

高ビットレート



CV-QKDの安全性



量子雑音のため
- アリス/ボブ間のビットに不一致 → アリス/ボブ相互情報量 I_{AB}
- イブ/ボブ間のビットに不一致 → イブ/ボブ相互情報量 I_{EB}

今の場合、$I_{AB} > I_{EB}$

⇩

誤り訂正・秘匿性増強により秘密鍵生成可能

課題は量子雑音限界の受信器

内容

[1] **量子暗号の概略**

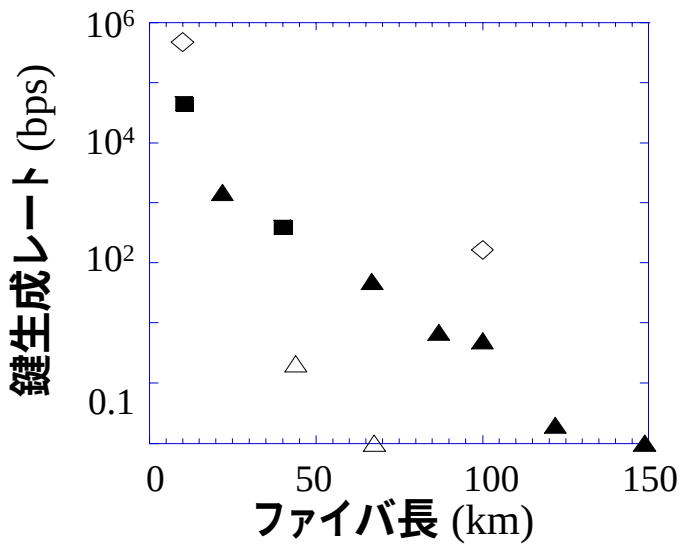
[2] **各種プロトコル**

[3] **実験**

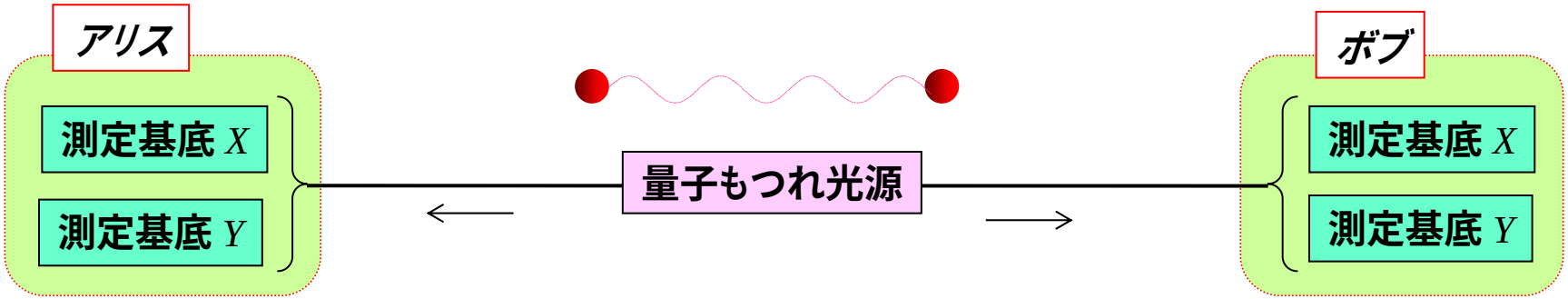
[4] **連続変数量子鍵配送**

[5] **量子もつれ鍵配送**

単一光子伝送には距離制限 ⟶ もつれ利用による超距離化

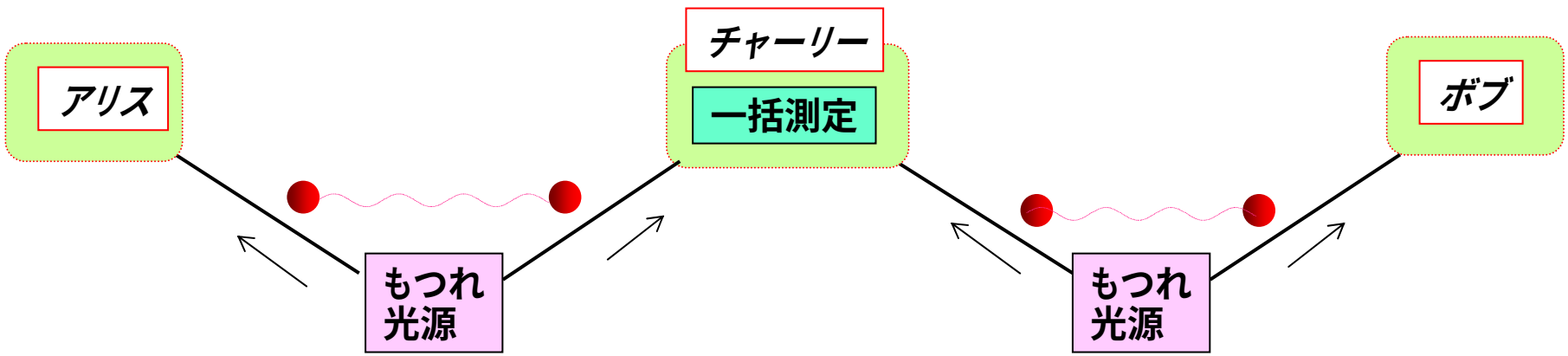


BBM92量子鍵配送



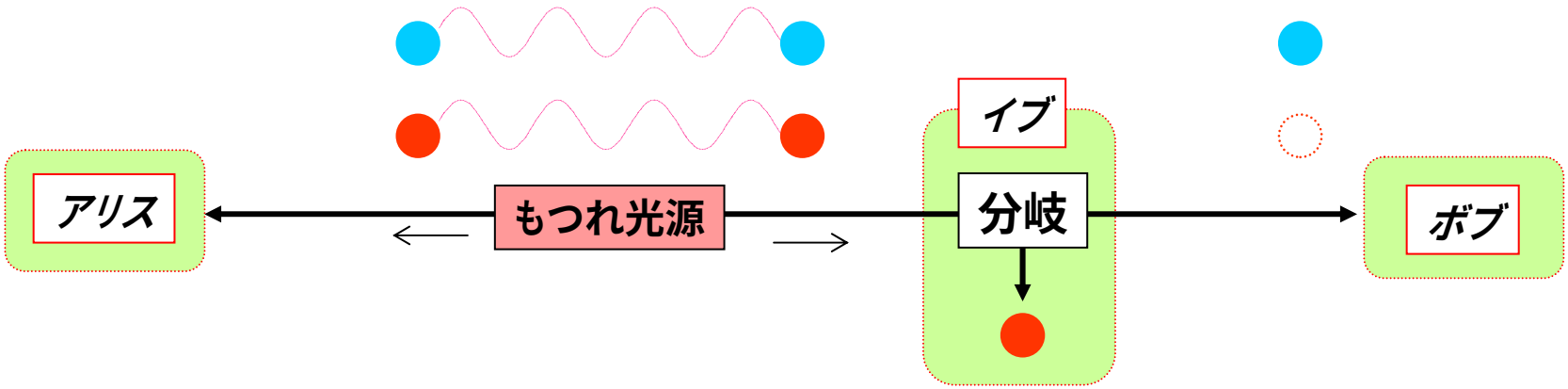
基底が一致すると測定結果に相関　→　鍵ビット生成

量子リレー鍵配送



アリスーボブ間の長距離化

ビームスプリット盗聴に対して



分岐光子はアリス/ボブの光子とは無相関

↓

分岐しても盗聴にはならない

↓

高い安全性

もつれＱＫＤは、現在、原理確認実験が行なわれている段階

まとめ

[1] **量子暗号の概略**

[2] **各種プロトコル**

BB84、B92、BBM92、DPS

[3] **実験**

(1) **光子検出器**

(2) BB84　**プラグ＆プレイ**

(3) DPS

[4] **連続変数量子鍵配送**

[5] **量子もつれ鍵配送**