量子鍵配送システム

-量子もつれ光子対-

井上　恭

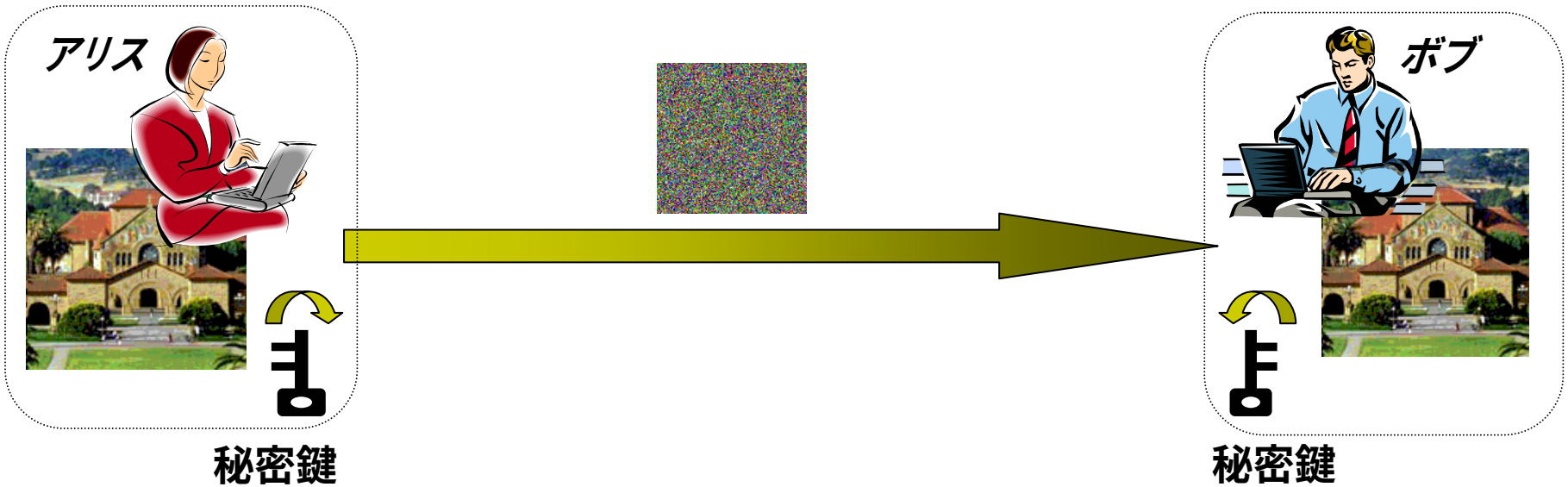
大阪大学工学研究科

内容

1. 量子鍵配送とは
   - 単一光子システムとその課題
2. 量子もつれ光子による鍵配送
   - 概略
   - ファイバ伝送向け量子もつれ状態
   - システム構成
3. 実験
   - 光ファイバによるもつれ光子発生
   - 鍵配送実験

もっとも古典的な暗号通信

秘密鍵暗号方式

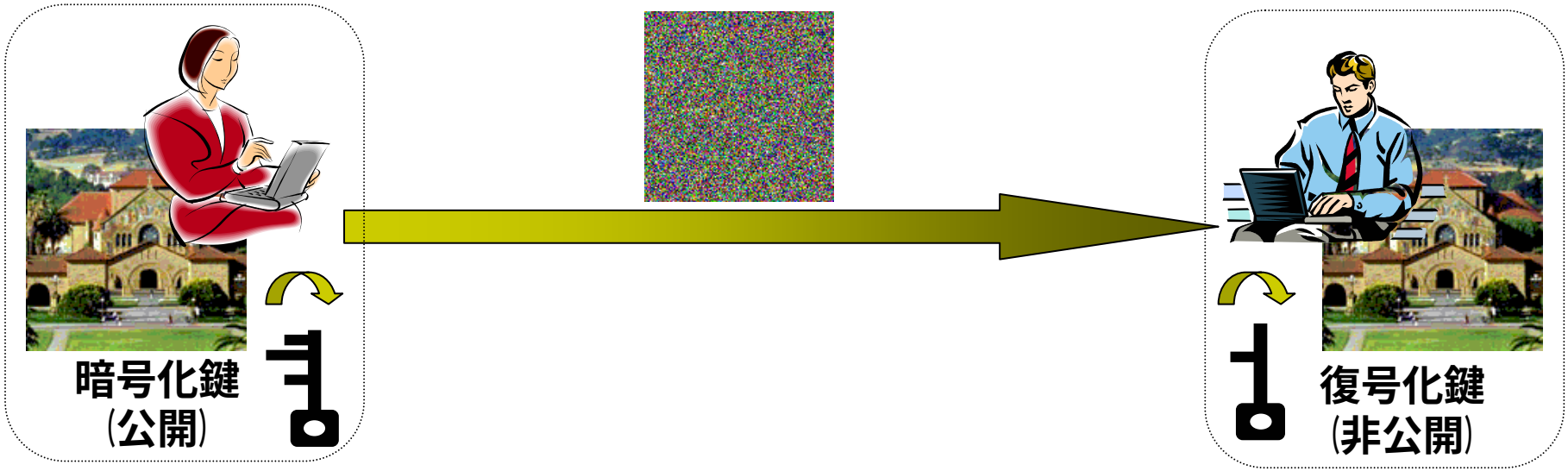


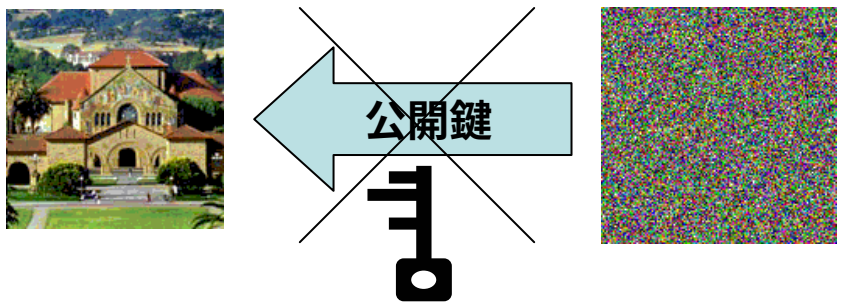
平文と同じ長さの鍵を一回しか使わなければ絶対に安全

ただし、問題は秘密鍵の安全性

そこで現代暗号通信では

公開鍵暗号





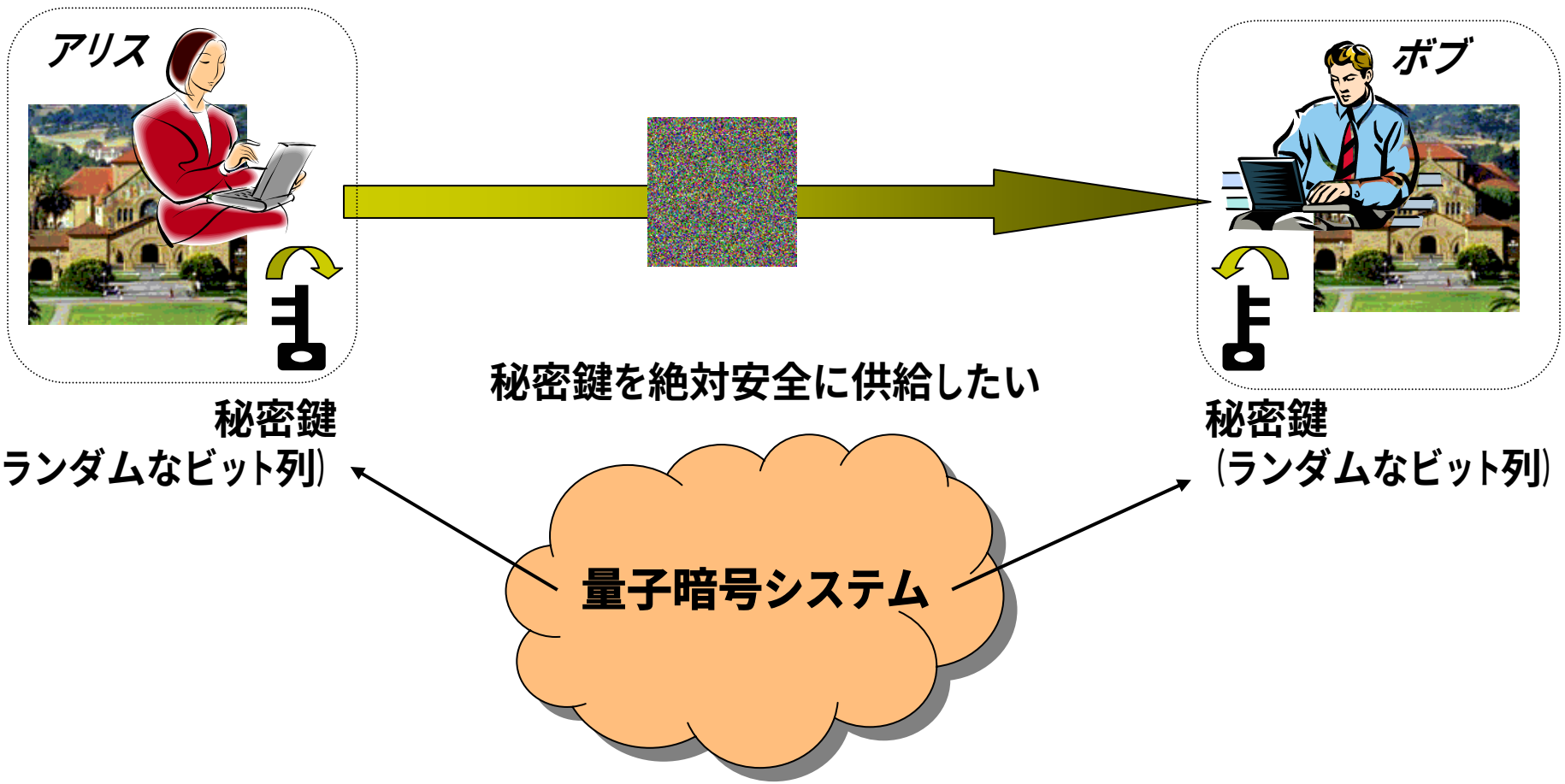
367 × 521 = Z ：簡単 (答えは191207)

X × Y = 191207 ：難しい

原理的には解読可能

そこで

量子暗号

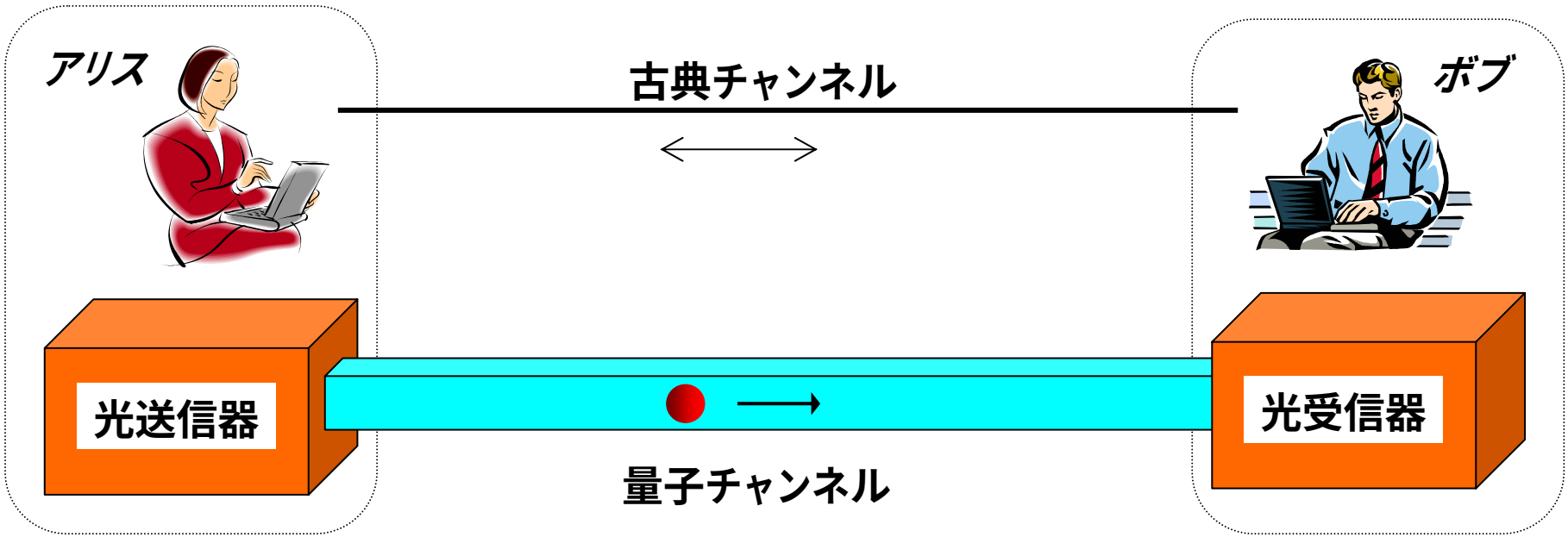


量子暗号 (量子鍵配送)

機能 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 安全性は量子力学的に保証

量子鍵配送の基本構図



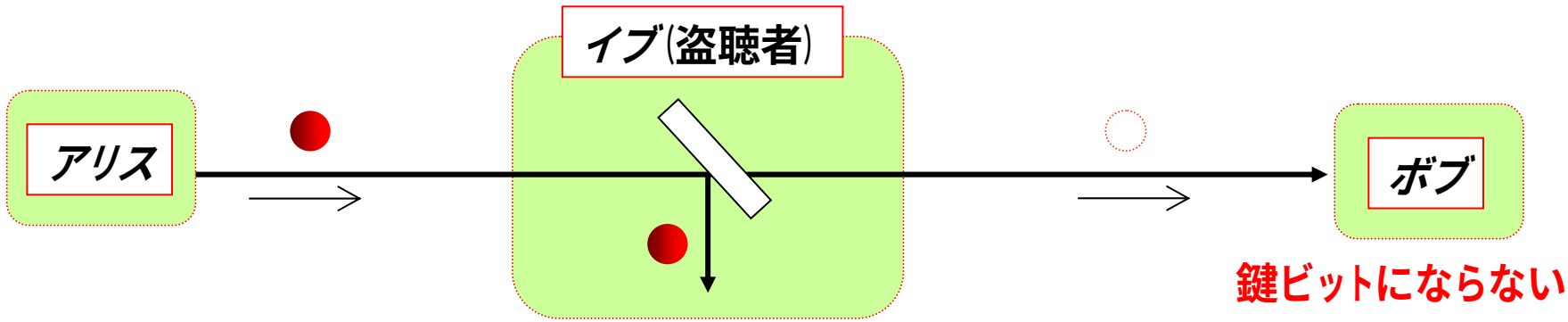
①量子チャンネルで光子を送受信

②古典チャンネルで基底に関する情報交換

③**秘密鍵**（ランダムなビット列）生成

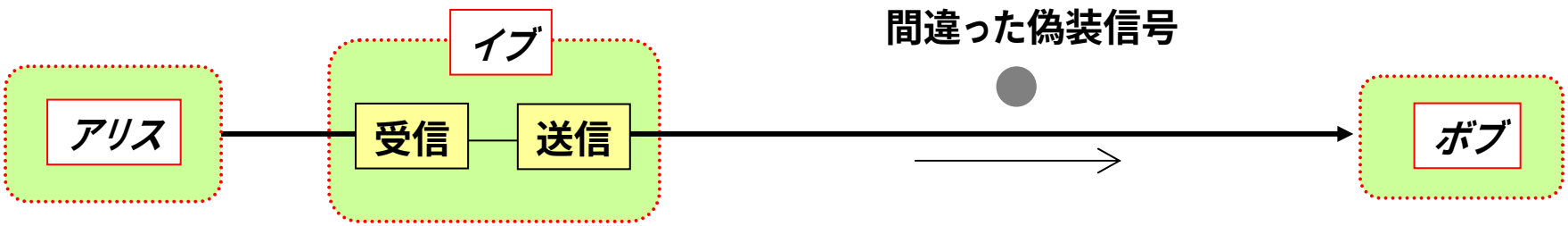
量子鍵配送の安全性

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



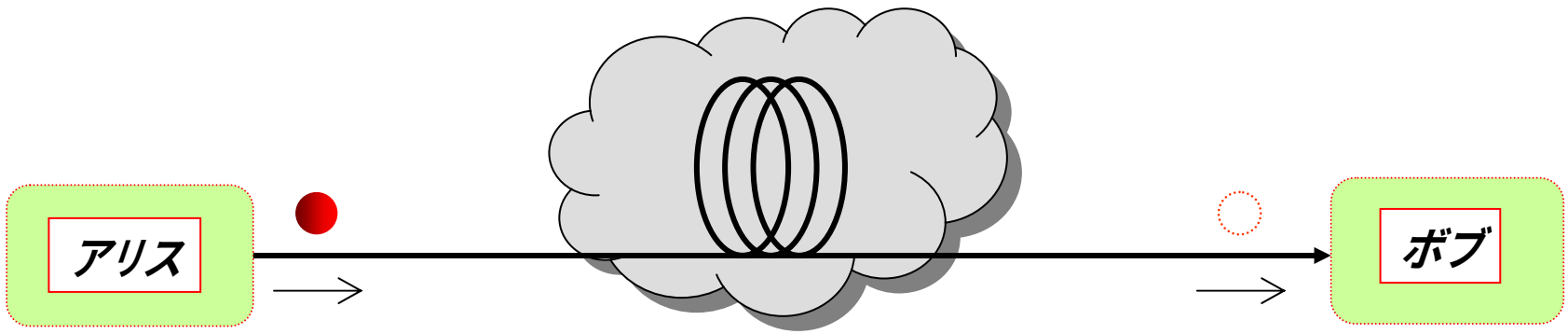
間違った偽装信号

受信結果に基づいて偽装信号を送信。
But、100%正しい受信はできない。

ビット誤り
↓
テストビットのチェックにより
盗聴発覚

課題1

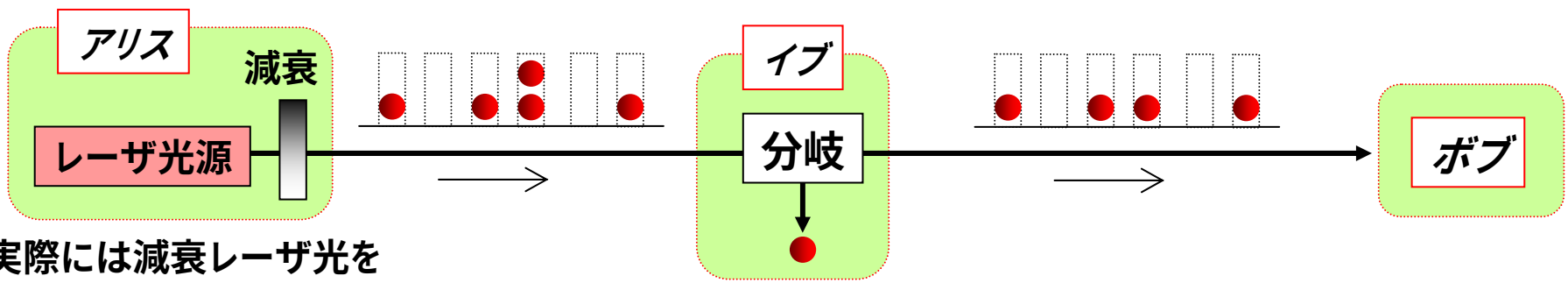
1光子は伝送損失により消滅



伝送距離に制限

課題2

実際には2光子/パルスの場合あり

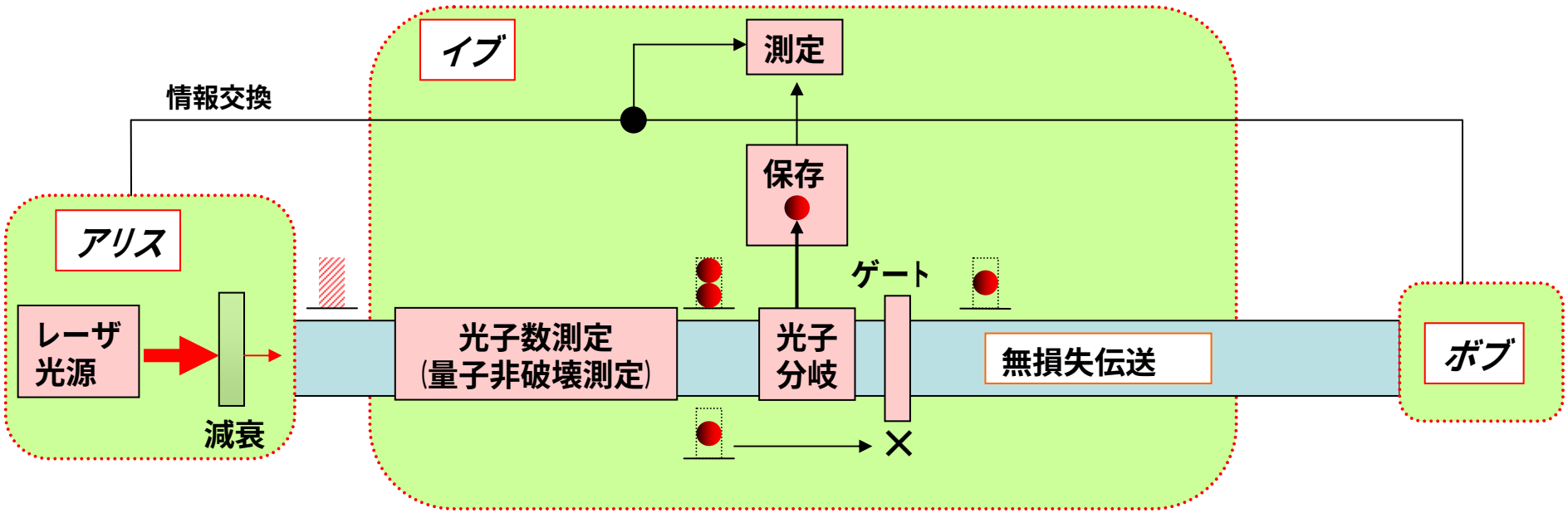


実際には減衰レーザ光を
擬似的に単一光子として使用

一部盗聴成功

イブが万能とすると
特にやっかい

光子数分岐盗聴

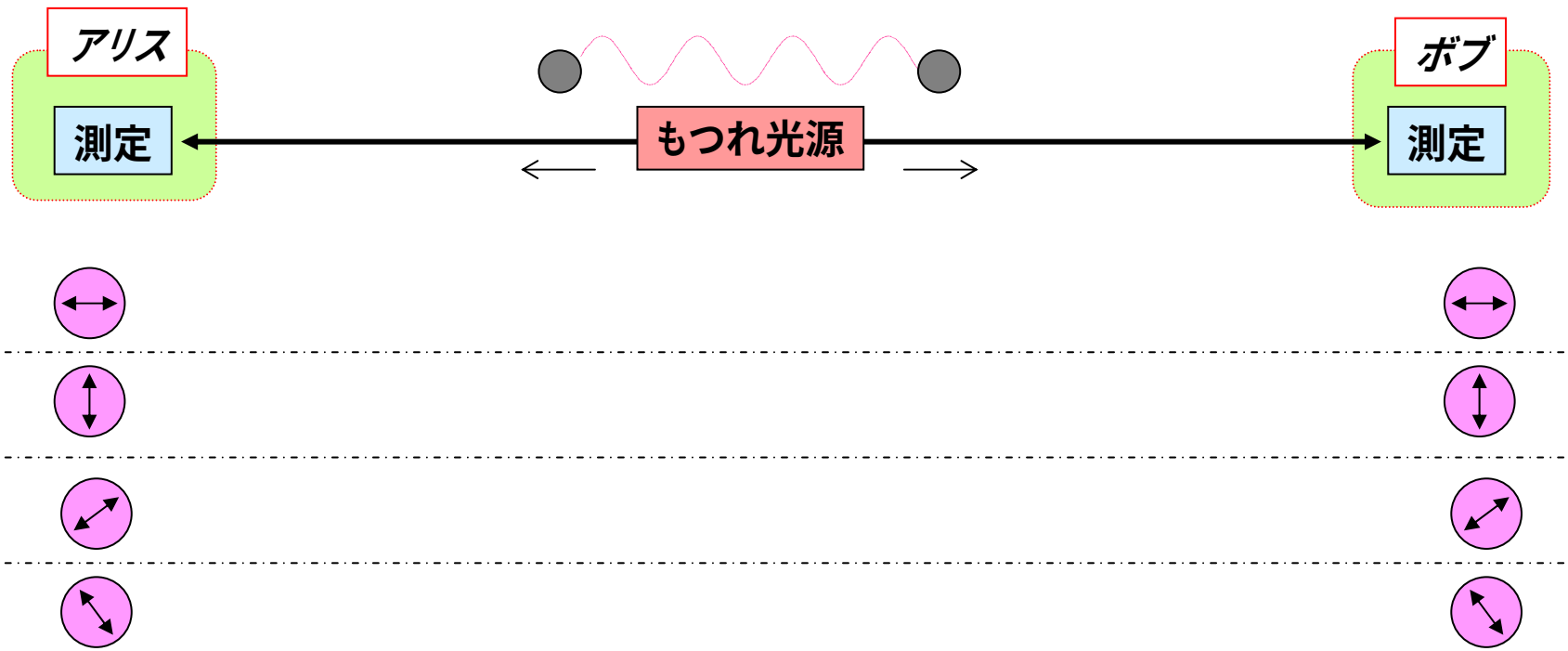


①光子数を非破壊で測定
②2光子あるパルスから1光子だけ分岐
③分岐した光子を保存
④残りの光子は無損失伝送路でボブへ送信
⑤1光子/パルスの場合はブロック
⑥アリス-ボブの基底情報を盗み聞く
⑦モード情報に基づいて保存しておいた光子を測定

2光子パルスの確率＝伝送路損失の場合 ⇒ *100%盗聴*

そこで

量子もつれ光子を使う鍵配送



アリスとボブの測定結果には相関あり

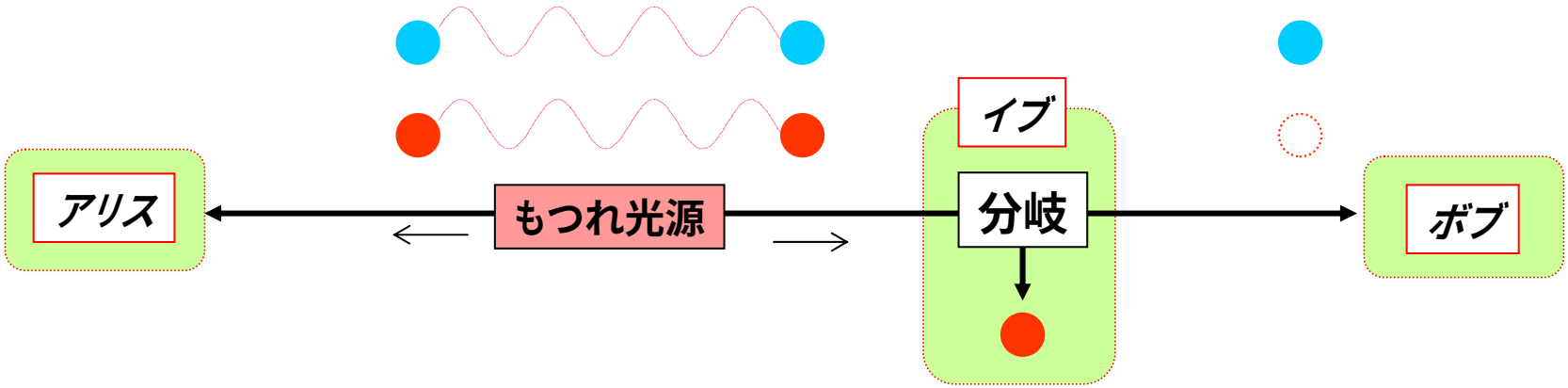
↓

同じビットを生成＝秘密鍵

システム長は光子伝送距離の2倍

課題2に対して

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

↓

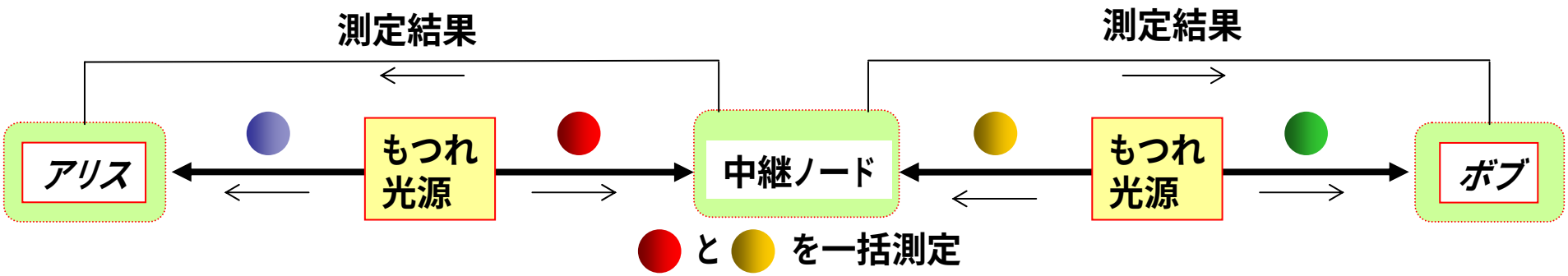
分岐しても盗聴にはならない

↓

高い安全性

さらに進んで

量子リレー鍵配送



● と ● を一括測定

||

相対関係を測定（同一偏波 or 直交偏波 ?）

アリス：● の測定結果＋中継ノード情報 → ● の状態がわかる

ボブ：● の測定結果＋中継ノード情報 → ● の状態がわかる

⇩

アリス-ボブで鍵生成

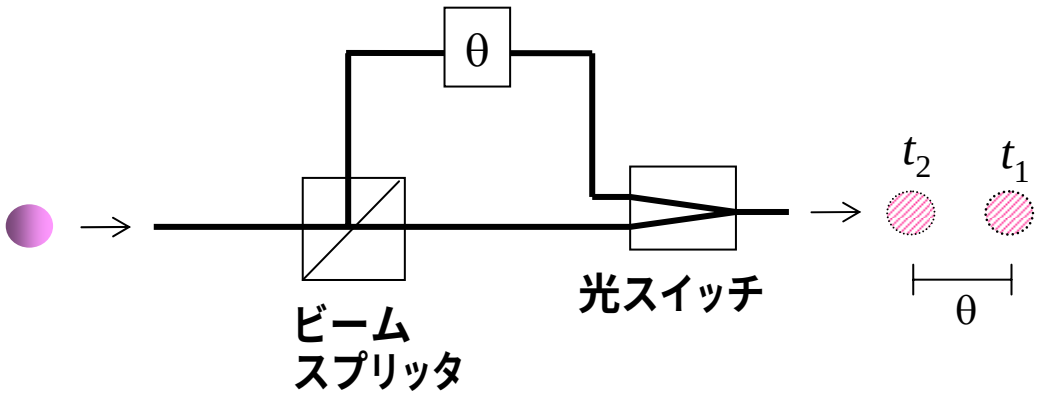
さらに長距離化

では具体的に

量子鍵配送に用いる量子もつれ状態

(ファイバ伝送を意識して)

時間位置重ね合わせ状態 (1光子)

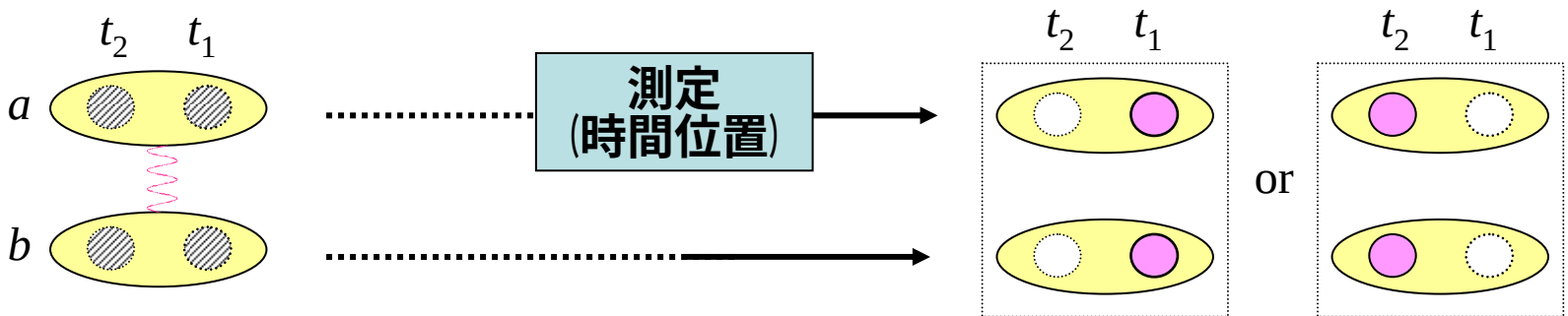


$$|\Psi>=\frac{1}{\sqrt{2}}\{|t_1>+e^{i\theta}|t_2>\}$$

測定
(時間位置)

$$|\Psi>=|t_1> \quad \text{or} \quad |t_2>$$

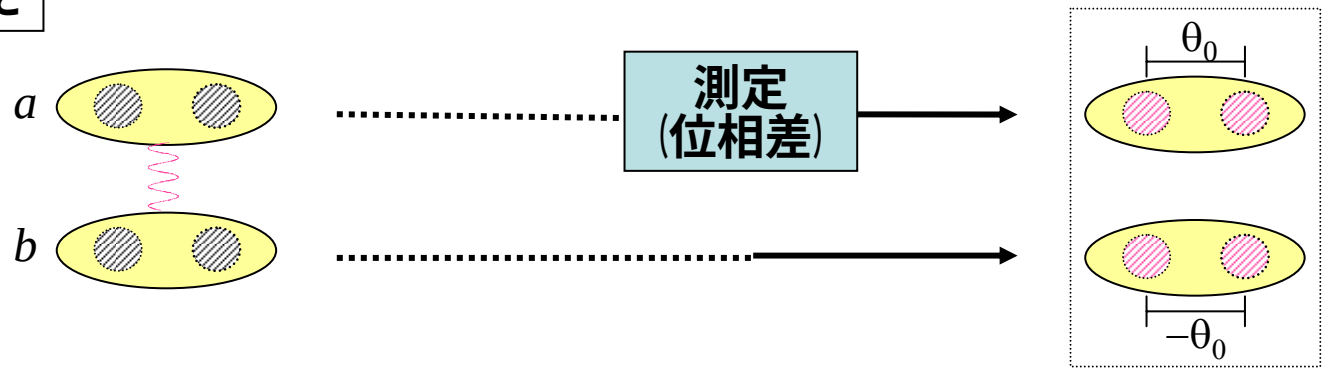
時間位置もつれ状態 (2光子)



$$|\Psi>=\frac{1}{\sqrt{2}}\{|t_1>_a|t_1>_b+|t_2>_a|t_2>_b\} \longrightarrow |t_1>_a|t_1>_b \qquad |t_2>_a|t_2>_b$$

もつれ状態

測定法を変えると



$$|\Psi>=\frac{1}{\sqrt{2}}(|t_1>_a|t_1>_b+|t_2>_a|t_2>_b)$$

$$=\frac{1}{\sqrt{2}}\{|\phi_+(\theta)>_a|\phi_+(-\theta)>_b+|\phi_-(\theta)>_a|\phi_-(-\theta)>_b\}$$

(θ は任意)

$$|\phi_+(\theta_0)>_a|\phi_+(-\theta_0)>_b$$

or

$$|\phi_-(\theta_0)>_a|\phi_-(-\theta_0)>_b$$

一方が$|\phi_+(\theta_0)>$なら他方は必ず$|\phi_+(-\theta_0)>$

一方が$|\phi_-(\theta_0)>$なら他方は必ず$|\phi_-(-\theta_0)>$

where

$$|\phi_+(x)>=\frac{1}{\sqrt{2}}(|t_1>+e^{ix}|t_2>)$$: **位相差 x の時間位置重ね合わせ状態**

$$|\phi_-(x)>=\frac{1}{\sqrt{2}}(|t_1>-e^{ix}|t_2>)$$: **位相差$(x+\pi)$の時間位置重ね合わせ状態**

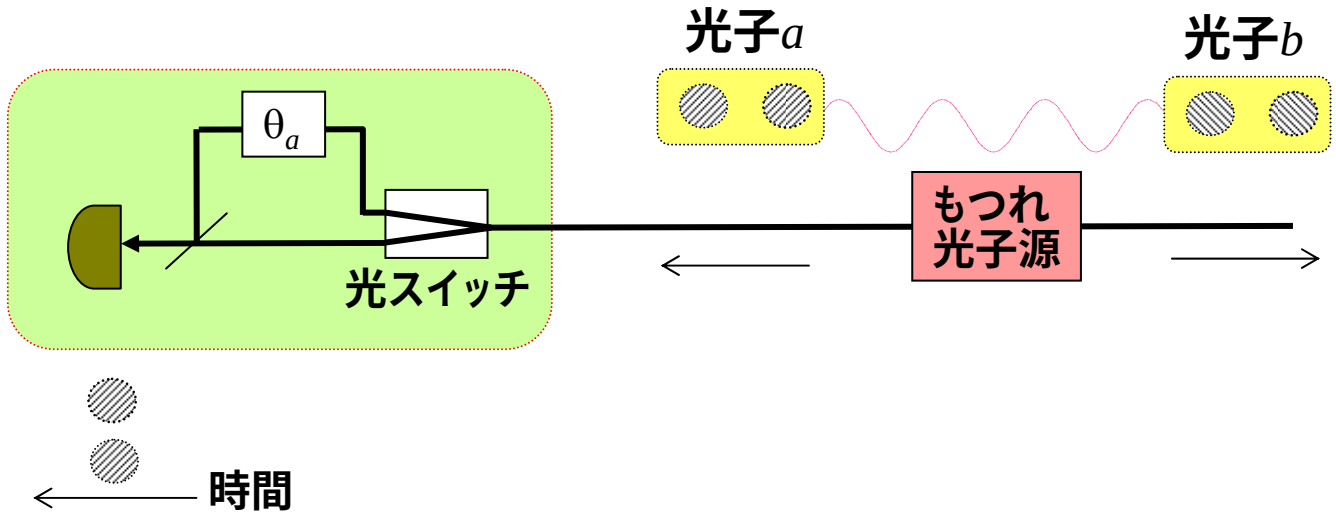
ポイント

測定前の位相は不確定

測定した瞬間に相関のある値に確定

測定法をもう少し具体的に

時間位置重ね合わせ状態の位相差測定

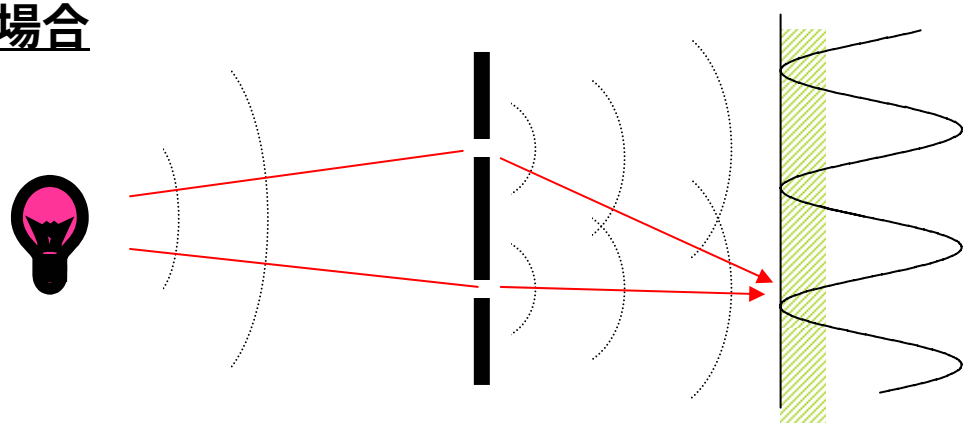


重ね合わせ2状態を時間位置を合わせて合波　→　2状態が干渉

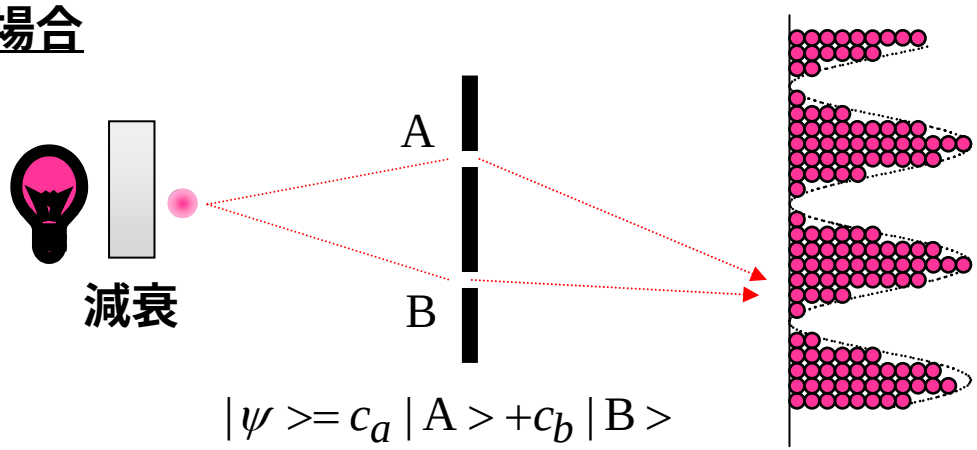
ここで、重ね合わせ状態の干渉について

ヤングの干渉実験

通常光の場合



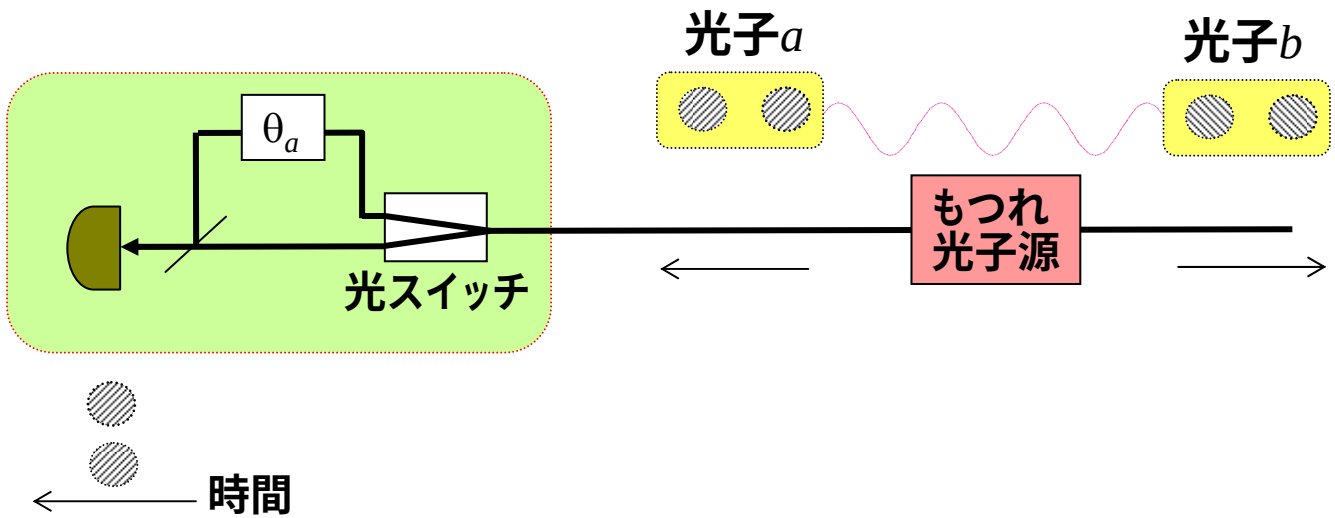
1光子の場合



$$|\psi>=c_a|\mathrm{A}>+c_b|\mathrm{B}>$$

確率振幅が干渉

さて、光子aを測定すると



重ね合わせ2状態が干渉

2状態が同位相なら強め合い、逆位相なら弱め合う

↓

検出器において、同位相なら光子検出、逆位相なら不検出。

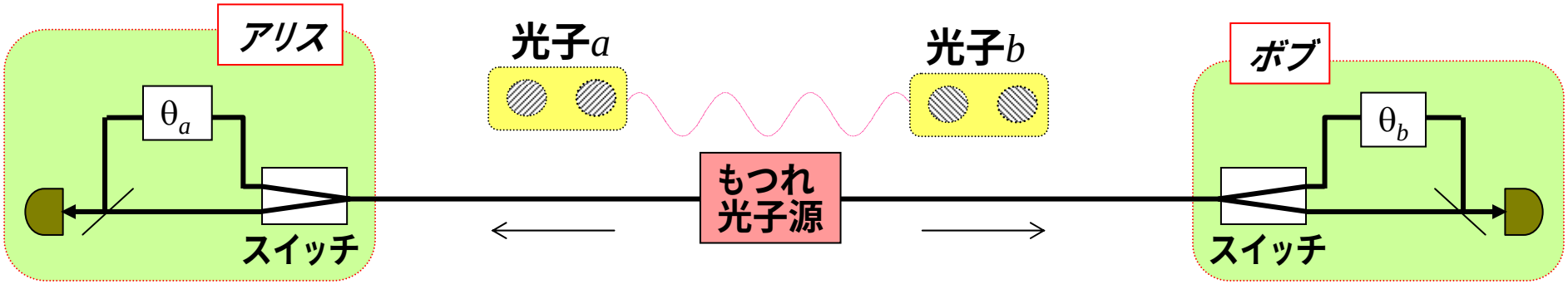
↓

光子検出 ⇔ 干渉計出力段で同位相 ⇔ 干渉計入力段の位相差＝$\theta_a + \pi/2$

(註：ビームスプリッタの反射は位相$\pi/2$シフト)

一方、光子bは

時間位置もつれ光子対の相関特性



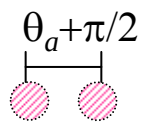
もつれ光源出力

$$|\Psi>=(|t_1>_a|t_1>_b+|t_2>_a|t_2>_b)/\sqrt{2}$$

$$=\{|\phi_+(\theta)>_a|\phi_+(-\theta)>_b+|\phi_-(\theta)>_a|\phi_-(-\theta)>_b\}/\sqrt{2}$$

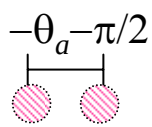
$$\begin{pmatrix} |\phi_+(x)>=(|t_1>+e^{ix}|t_2>)/\sqrt{2} \\ |\phi_-(x)>=(|t_1>-e^{ix}|t_2>)/\sqrt{2} \end{pmatrix}$$

アリス光子検出 ⇒ 光子a ：$|\phi_-(\theta_a+\pi/2)>_a$

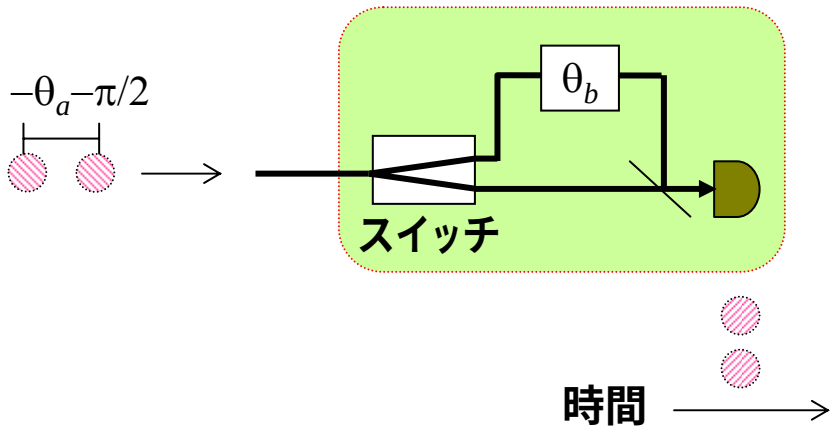


光子対の状態

$$|\Psi>=|\phi_+(\theta_a+\pi/2)>_a|\phi_+(-\theta_a-\pi/2)>_b \Rightarrow \text{光子}b：|\phi_-(-\theta_a-\pi/2)>_b$$



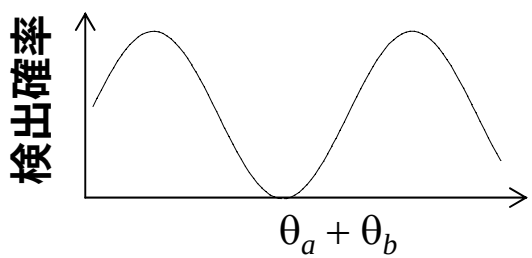
ボブ測定



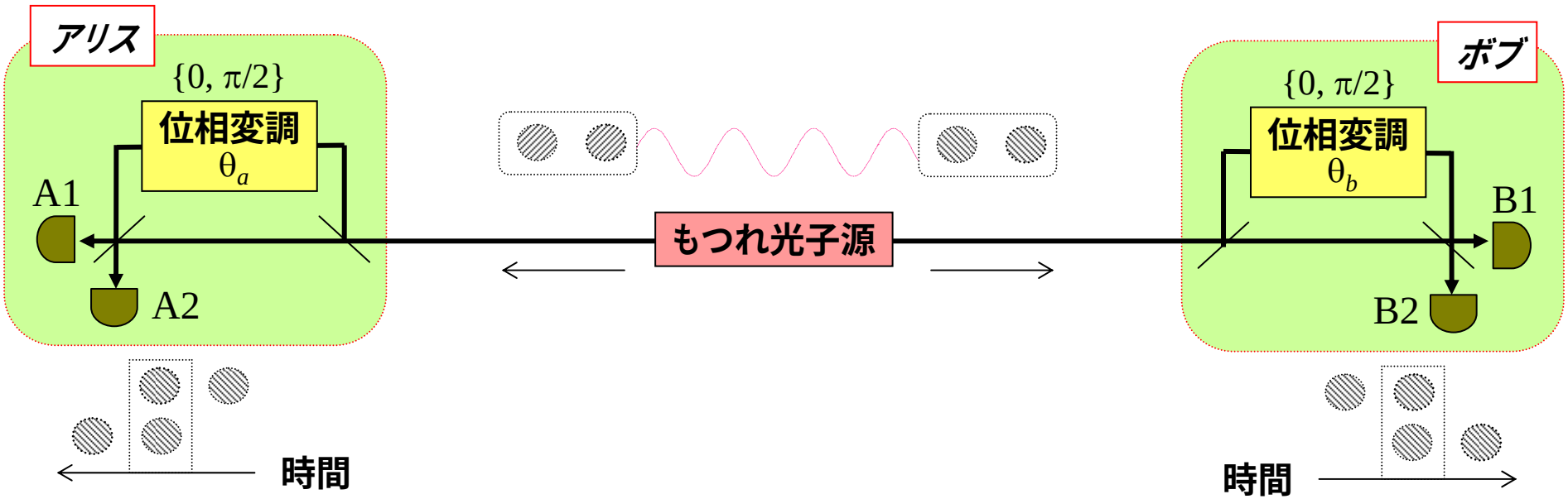
$$\begin{cases} (-\theta_a - \pi/2) - (\theta_b + \pi/2) = 0 \text{ だと同位相} \Rightarrow \text{光子検出} \\ (-\theta_a - \pi/2) - (\theta_b + \pi/2) = \pi \text{ だと逆位相} \Rightarrow \text{光子検出せず} \end{cases}$$

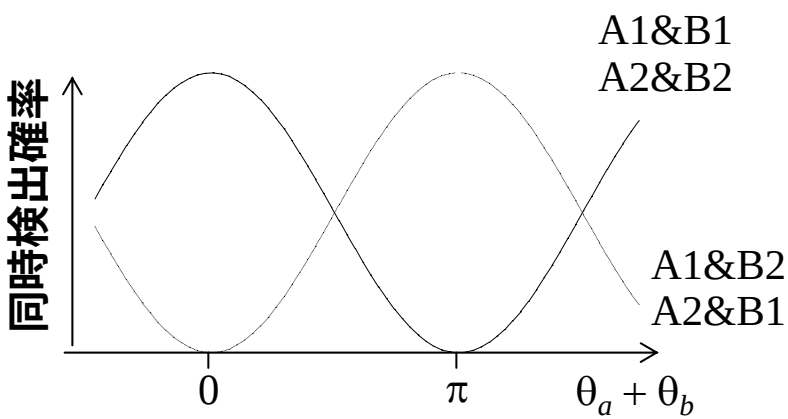
$$\Vert$$

$$\begin{cases} \theta_a + \theta_b = \pi \Rightarrow \text{光子検出} \\ \theta_a + \theta_b = 0 \Rightarrow \text{光子検出せず} \\ \text{中間状態} \Rightarrow \text{検出したりしなかったり} \end{cases}$$



時間位置もつれ光子による秘密鍵生成





光子検出の相関関係

	$\theta_a + \theta_b$		
アリス検出	0	π/2	π
A1	B1	B1/B2	B2
A2	B2	B1/B2	B1

秘密鍵生成手順

① 遅延位相を $\{0, \pi/2\}$ でランダムに変調しながら光子を検出。

② 光子検出時刻及びその光子に対する遅延位相を互いに通知。

③ 両方ともが真ん中の時刻で光子を検出し、
かつ、
遅延位相が $\theta_a + \theta_b = 0$ または π である検出結果からビット生成。

$\theta_a + \theta_b = 0$：$\{A1, B1\} \Leftrightarrow$「0」、 $\{A2, B2\} \Leftrightarrow$「1」
$\theta_a + \theta_b = 0$：$\{A1, B2\} \Leftrightarrow$「0」、 $\{A2, B1\} \Leftrightarrow$「1」

⇒ 秘密鍵

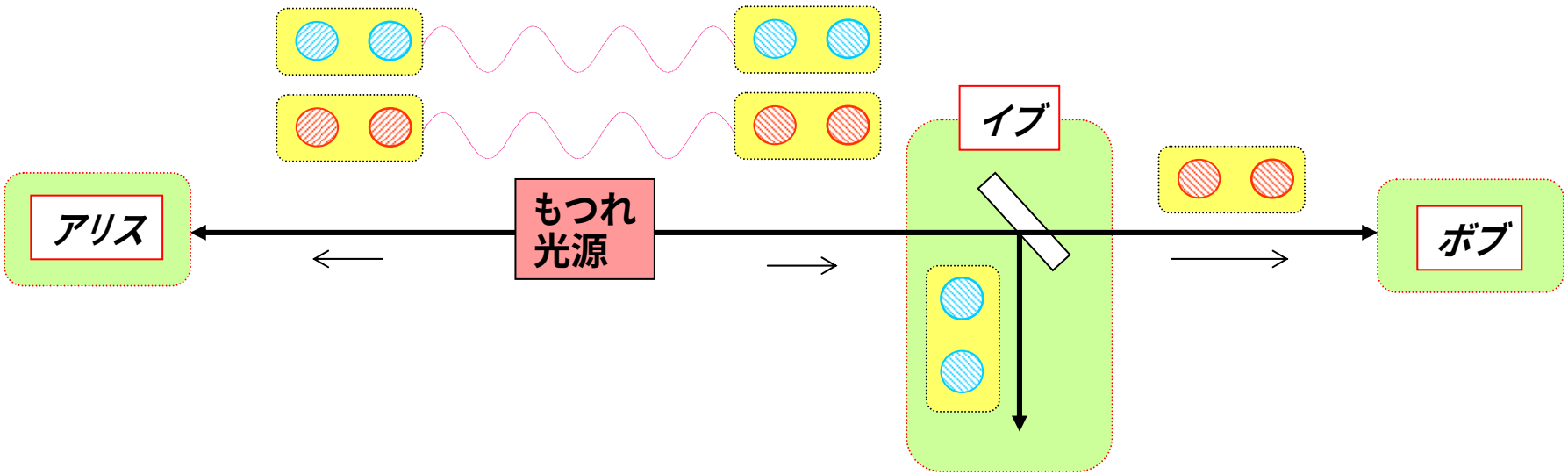
④ 上記以外の検出結果は無視。

アリス検出	$\theta_a + \theta_b$ 0	$\pi/2$	π
A1	B1	B1/B2	B2
A2	B2	B1/B2	B1

安全性1

盗聴に対して－ビームスプリット攻撃－

伝送信号を一部分岐



分岐光子はアリス/ボブの受信光子とは無関係

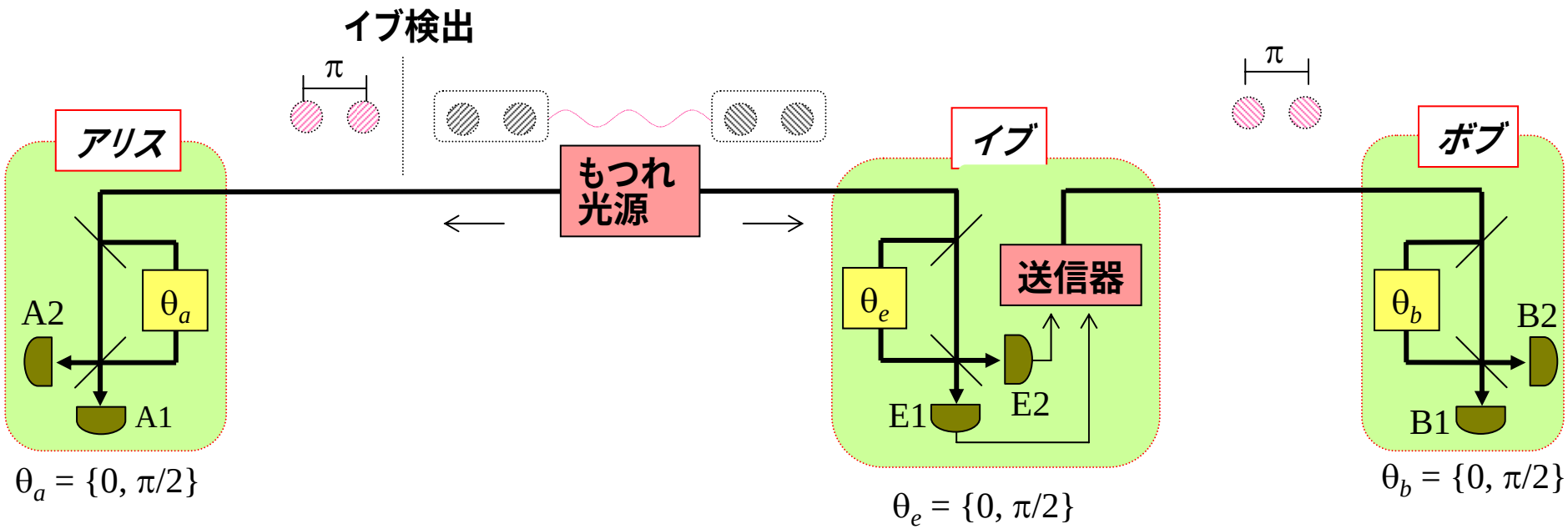
↓

盗聴にはならない

安全性2

盗聴に対して－なりすまし攻撃－

伝送信号を全て受信し、受信結果に基づいて偽装信号を送信。



イブが$\theta_e = 0$ の時にE1で光子検出すると、

アリス行き光子の位相差＝π に確定。

イブは位相差π の光子をボブに送信。

アリス/ボブが$\theta_a = \theta_b = \pi/2$ でこれを受信すると、

どちらの検出器で光子検出するかはランダム。

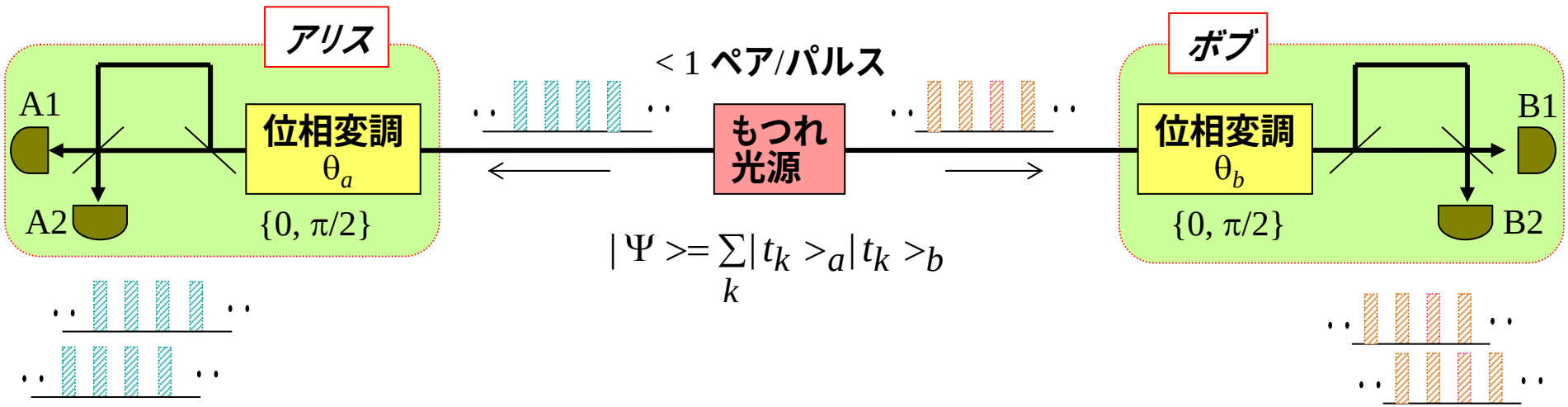
アリス検出	$\theta_a + \theta_b$ 0	π/2	π
A1	B1	B1/B2	B2
A2	B2	B1/B2	B1

ところが、$\theta_a + \theta_b = \pi$ なので、アリス/ボブは確定的検出だと思い、鍵ビット生成。

⟶ ビット不一致 ⟶ *盗聴発覚！*

より実際的には

もつれパルス列鍵配送



光子検出の相関関係

アリス検出	$\Delta\theta_a + \Delta\theta_b$		
	0	π/2	π
A1	B1	B1/B2	B2
A2	B2	B1/B2	B1

⇨

鍵ビット生成

$\Delta\theta_a + \Delta\theta_b = 0$: {A1, B1} = 「0」, {A2, B2} = 「1」

$\Delta\theta_a + \Delta\theta_b = \pi$: {A1, B2} = 「0」, {A2, B1} = 「1」

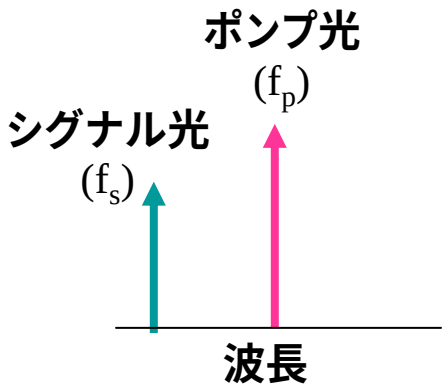
$\Delta\theta_a + \Delta\theta_b = \pi/2$: **無視**

- 時間領域の有効利用 → 高データレート
- 位相変調が干渉計の外側 → 高安定動作

1. 量子鍵配送とは
    - 単一光子システムとその課題
2. 量子もつれ光子による鍵配送
    - 概略
    - ファイバ伝送向け量子もつれ状態
    - システム構成
3. **実験**
    - 光ファイバによるもつれ光子発生
    - 鍵配送実験

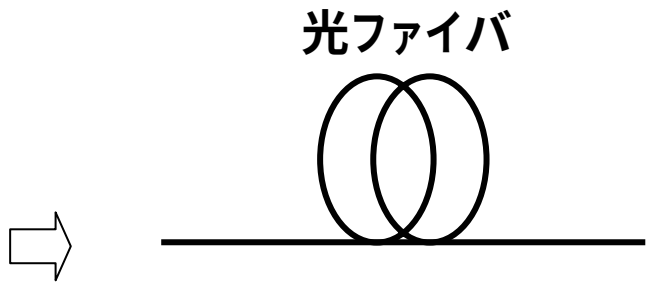
量子もつれ光子発生が何より基本

四光波混合 in 光ファイバ



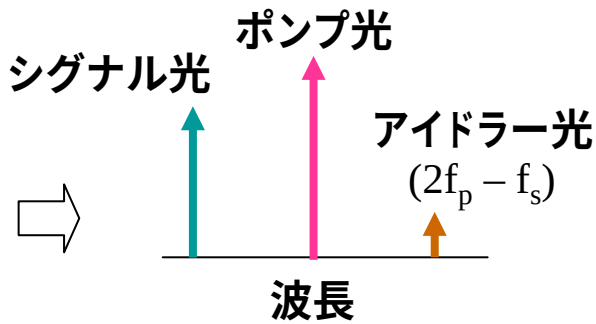
入力光電場

$E_p \exp(i\omega_p t) + E_s \exp(i\omega_s t) + c.c.$

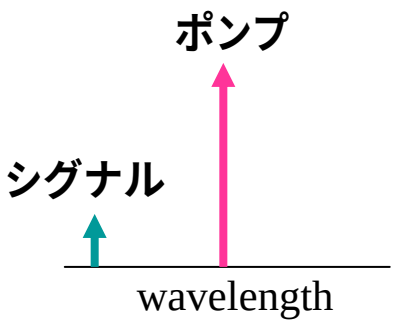


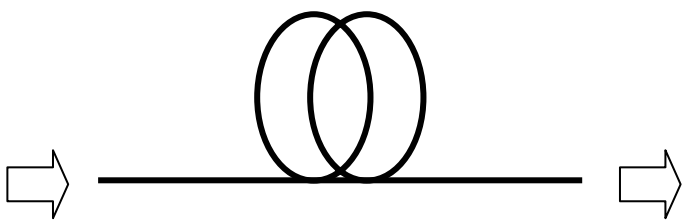
分極

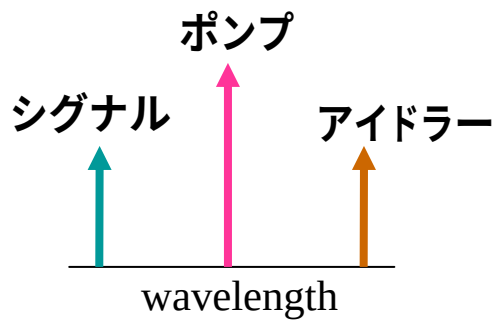
$P = \varepsilon_0 \chi_1 E + \varepsilon_0 \chi_2 EE + \varepsilon_0 \chi_3 EEE + \cdots$



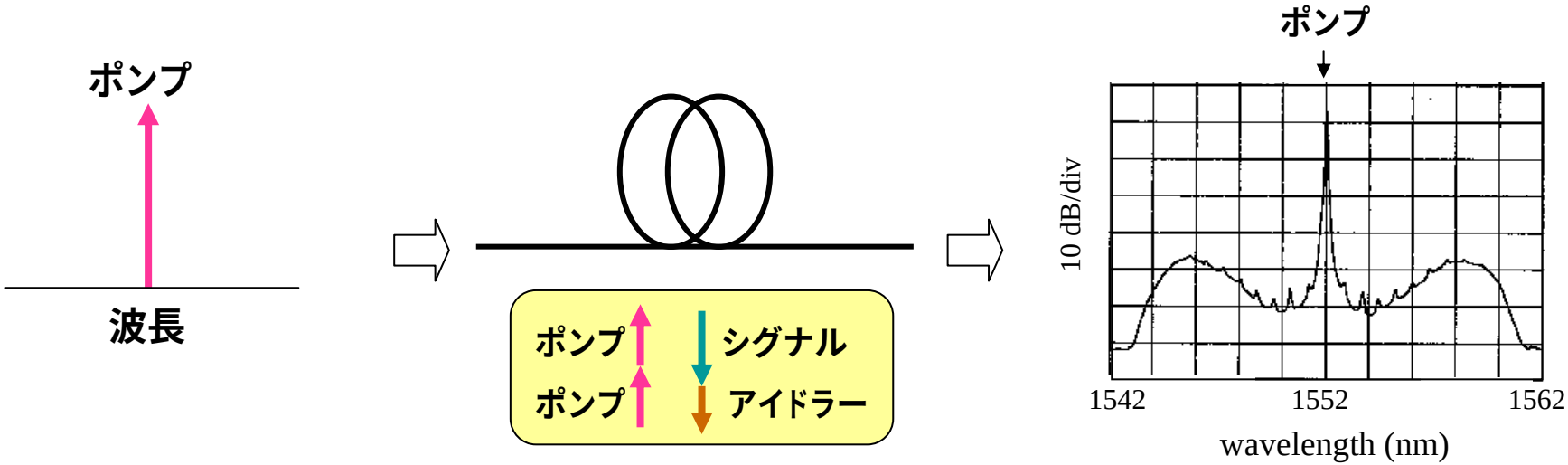
ファイバ光パラメトリック増幅







自然四光波混合



シグナル光子とアイドラー光子は必ずペアで発生

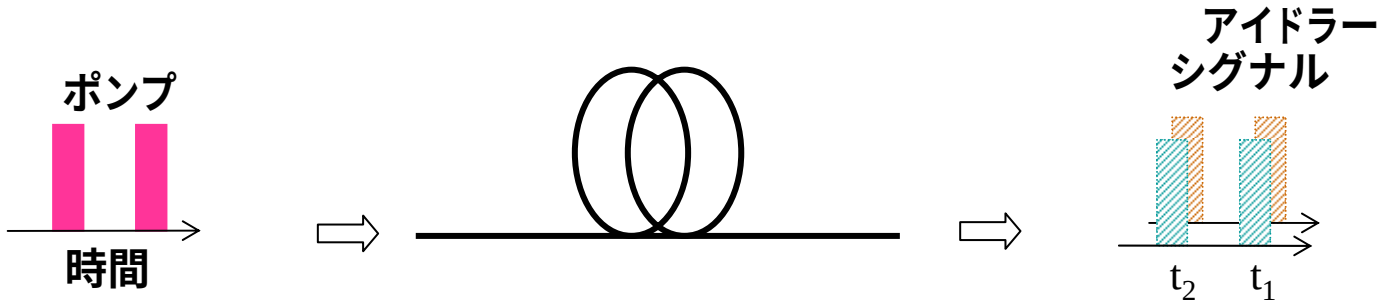
かつポンプ光と同じ偏波

‖

相関光子対： $|1\rangle_s|1\rangle_i$

これをタネに量子もつれ状態を作ろう

時間位置もつれ光子発生



ポンプ光パワーにより光子対発生確率を調整

（2ペア発生確率）<<（1ペア発生確率）

$r^2 << r(1-r)$　　（r: 光子対発生確率）

⇩

シグナル/アイドラーが1ペア発生した時に、それがt_1なのかt_2なのか不明。

⇩

シグナル/アイドラーがt_1にいる状態とt_2にいる状態との重ね合わせ状態

$$|\Psi>=|t_1>_s|t_1>_i + e^{i\phi}|t_2>_s|t_2>_i \quad (\phi = 2\Delta\phi_p、\ \Delta\phi_p：\text{ポンプ光位相差})$$

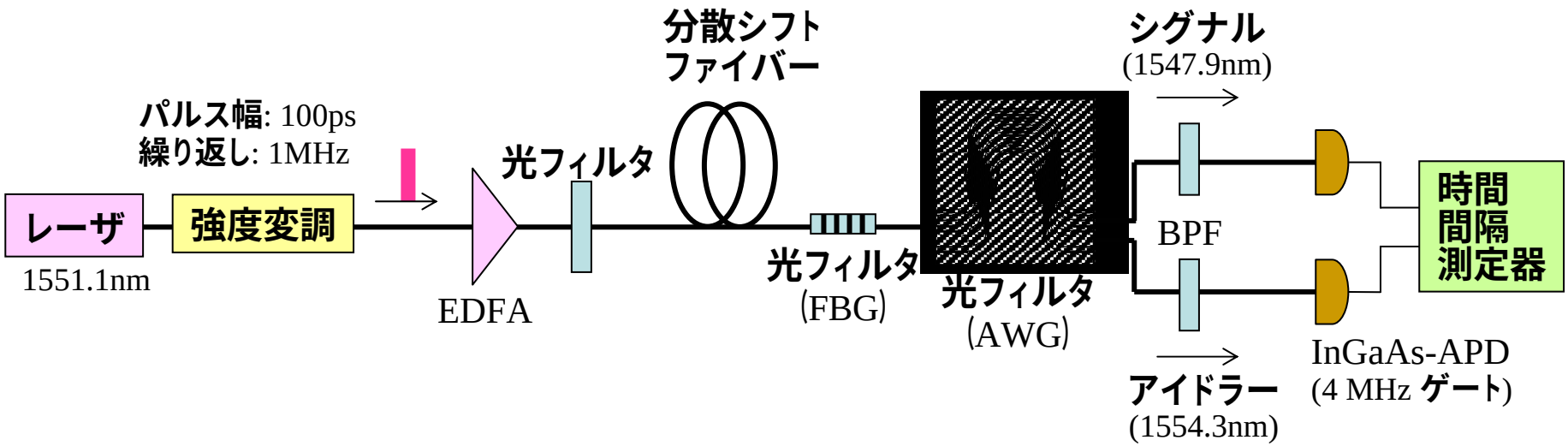
⇩ $(\Delta\phi_p = 0)$

$$|\Psi>=|t_1>_s|t_1>_i + |t_2>_s|t_2>_i$$

時間位置もつれ状態

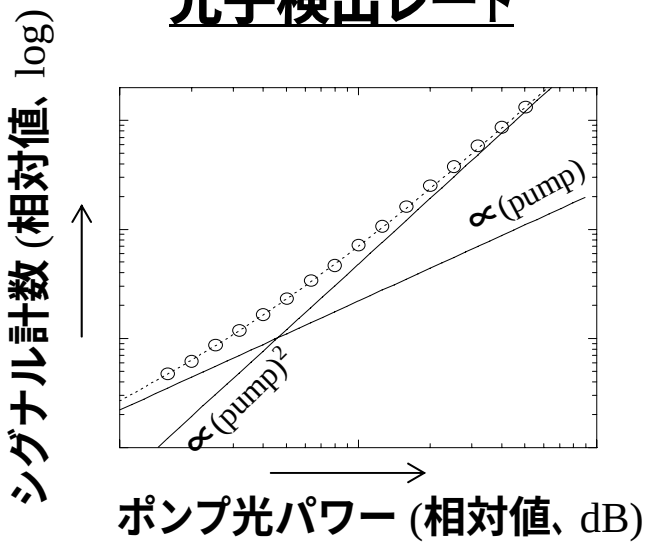
まずは、相関光子対発生

シグナル/アイドラー同時発生実験



測定結果

光子検出レート

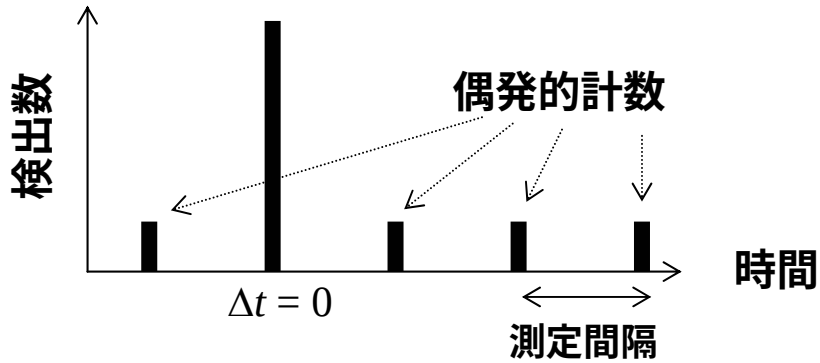


出力は、

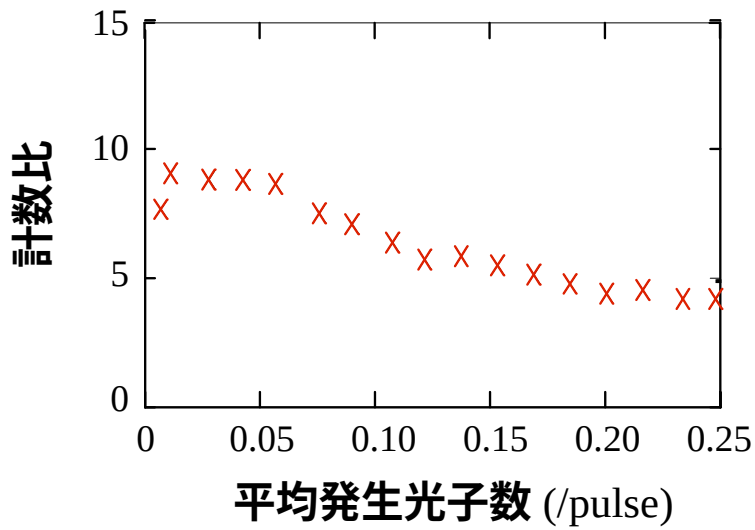
(ポンプ光パワー) ^{2}に比例する成分 **相関光子対**

(ポンプ光パワー) に比例する成分 **?**

時間間隔測定器の測定データ



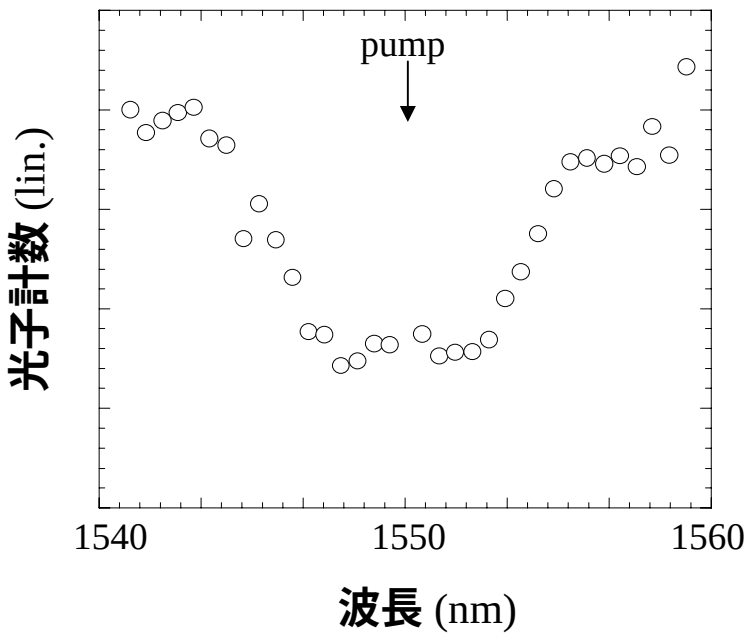
同時計数と偶発計数との比



相関光子対発生、
が相関の無い光子も発生 → 雑音光子

雑音光子の正体は？

線形成分の波長依存性

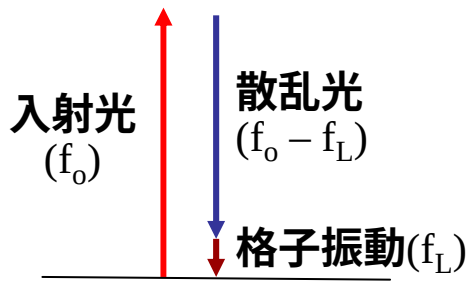


このスペクトル形状は、自然ラマン散乱光っぽい。

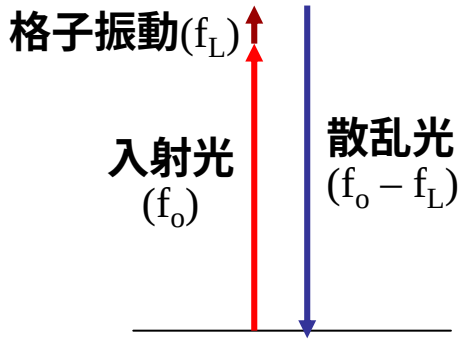
ラマン散乱

格子振動（フォノン）による光の散乱現象

ストークス散乱



反ストークス散乱

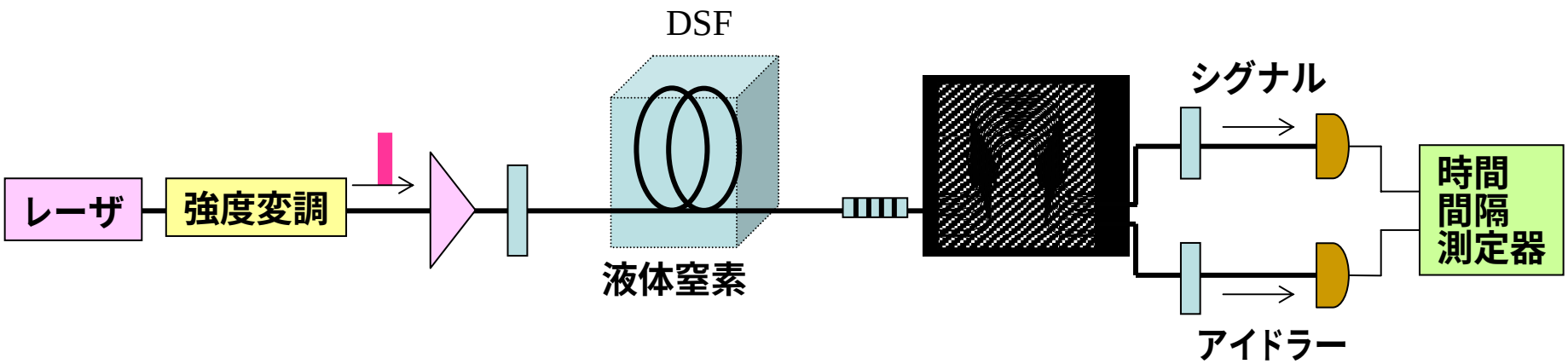


格子振動は冷却すれば鎮静化（フォノン数小）

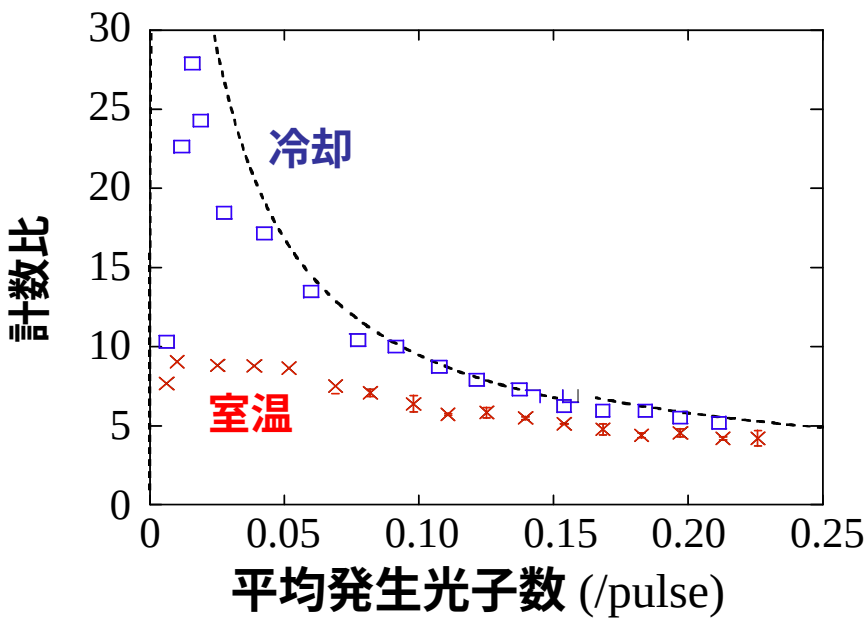
⇩

冷却すればラマン散乱は抑制

ファイバ冷却によるラマン散乱抑圧

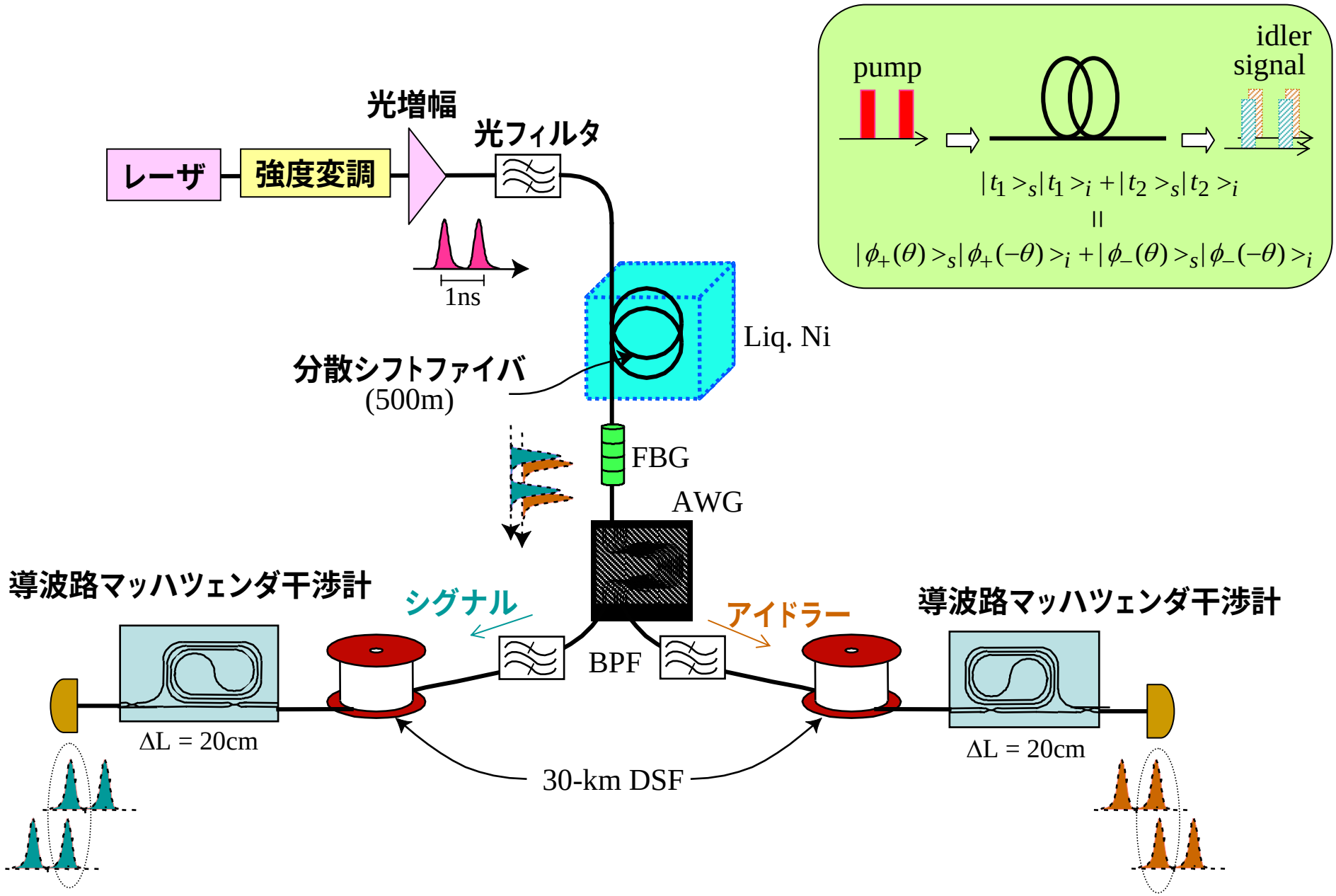


同時計数と偶発計数との比

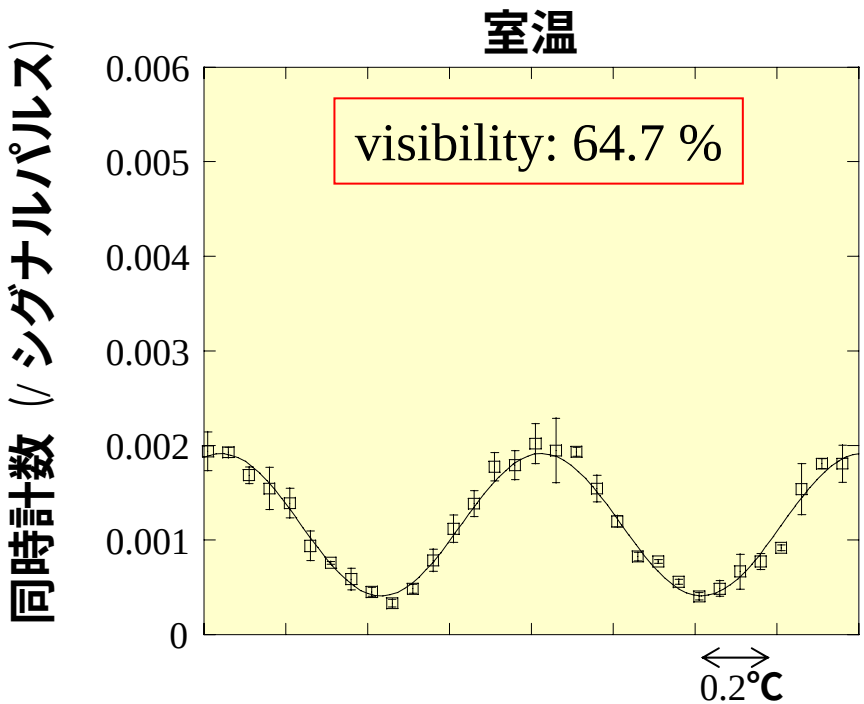


雑音光子減少

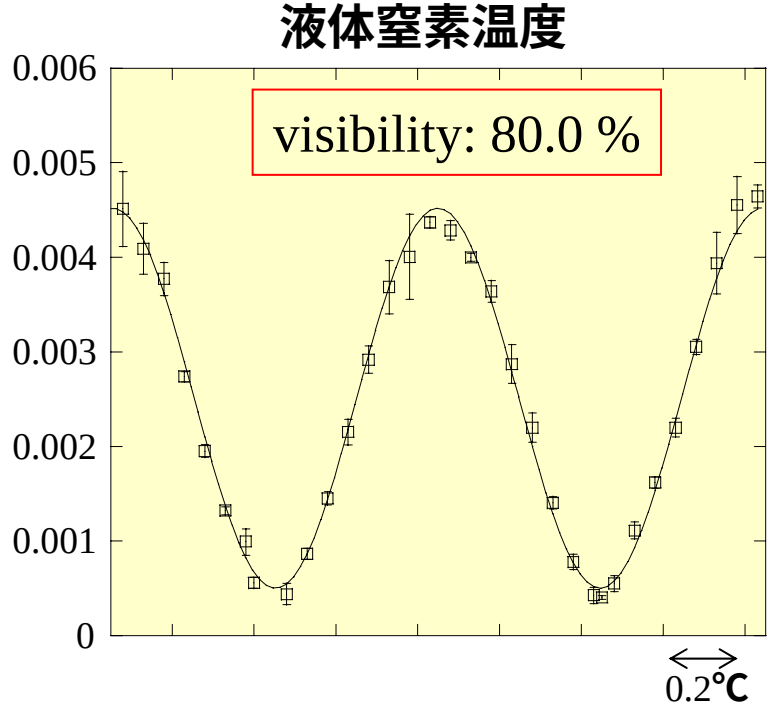
時間位置もつれ光子発生実験



測定結果



干渉計温度 for シグナル

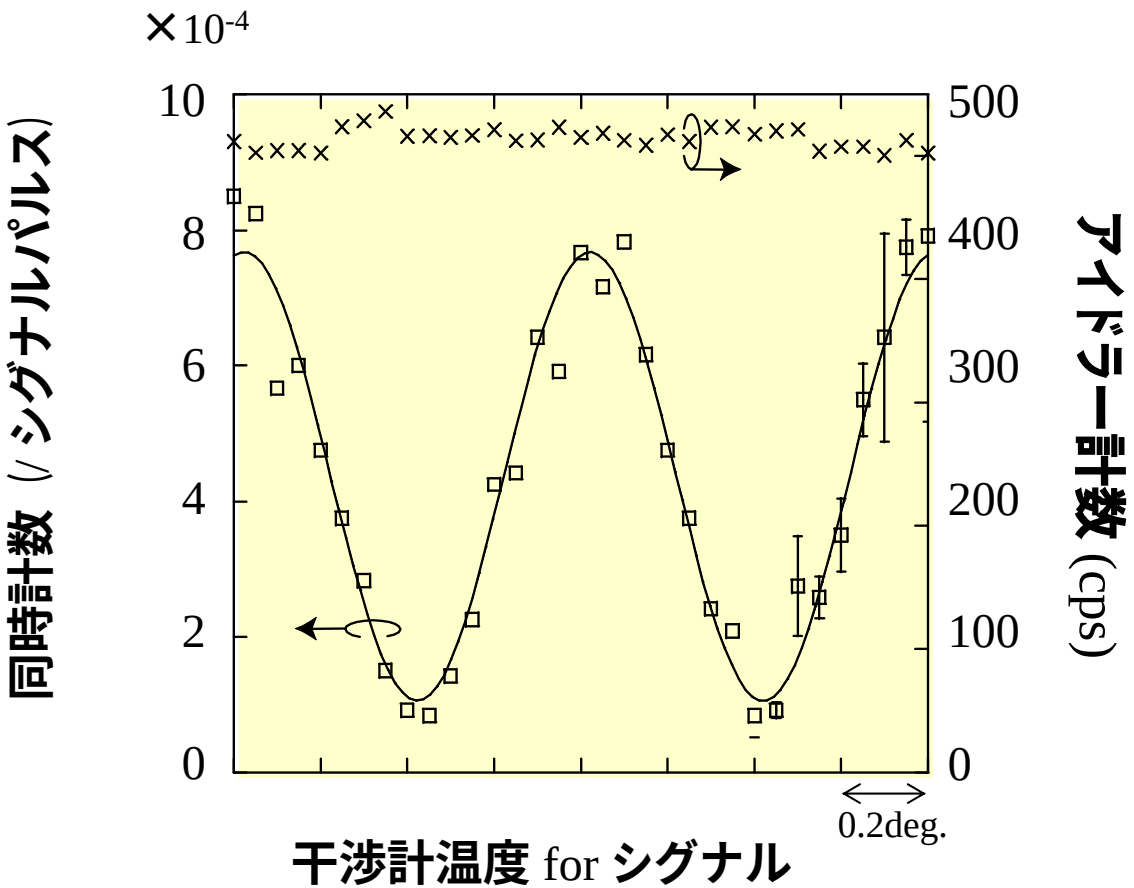


干渉計温度 for シグナル

干渉計温度 for アイドラーは固定

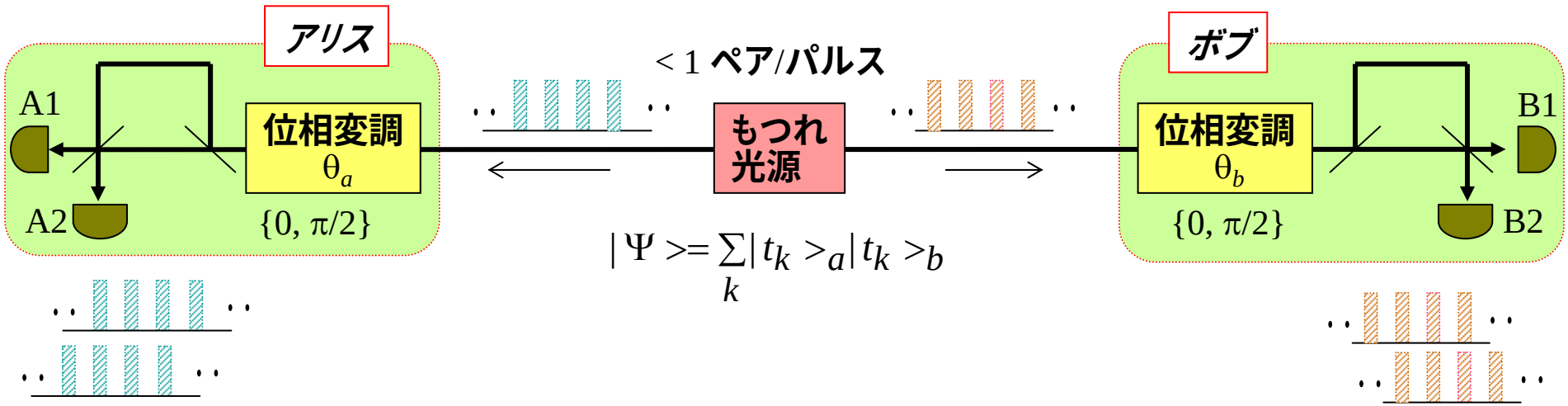
平均光子対数：: 0.06 /パルス with pump power of 140mW

測定結果
– (30km×2)-ファイバ伝送 –



では鍵配送実験

もつれパルス列鍵配送システム



光子検出の相関関係

アリス検出	$\Delta\theta_a + \Delta\theta_b$		
	0	π/2	π
A1	B1	B1/B2	B2
A2	B2	B1/B2	B1

⇨

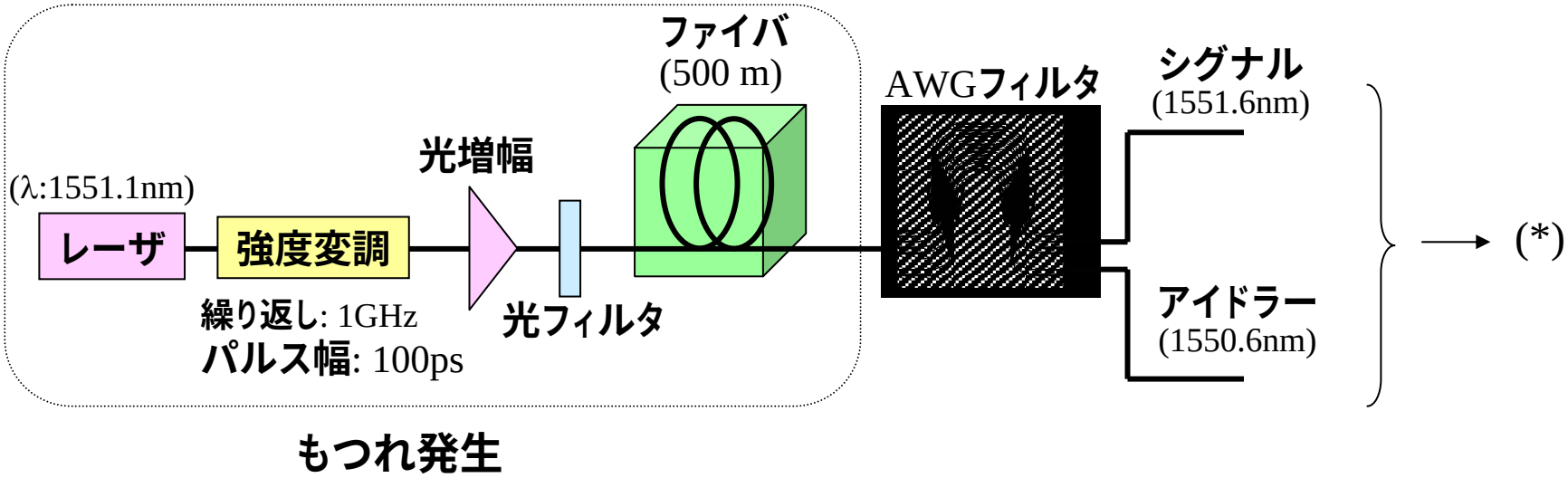
鍵ビット生成

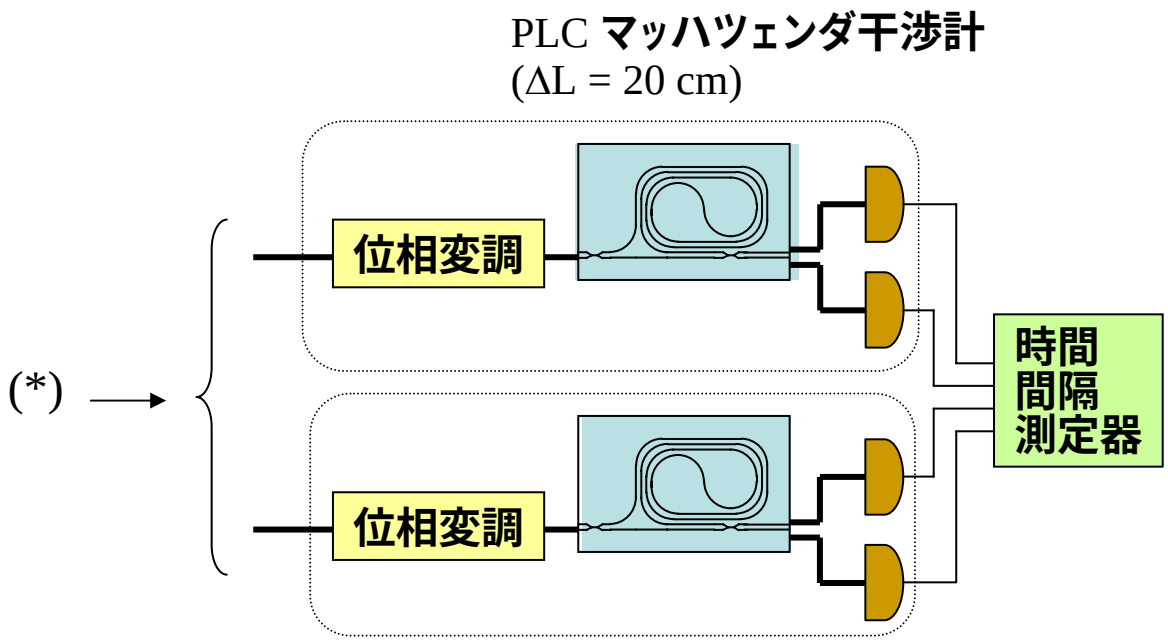
$\Delta\theta_a + \Delta\theta_b = 0$: {A1, B1} = 「0」, {A2, B2} = 「1」

$\Delta\theta_a + \Delta\theta_b = \pi$: {A1, B2} = 「0」, {A2, B1} = 「1」

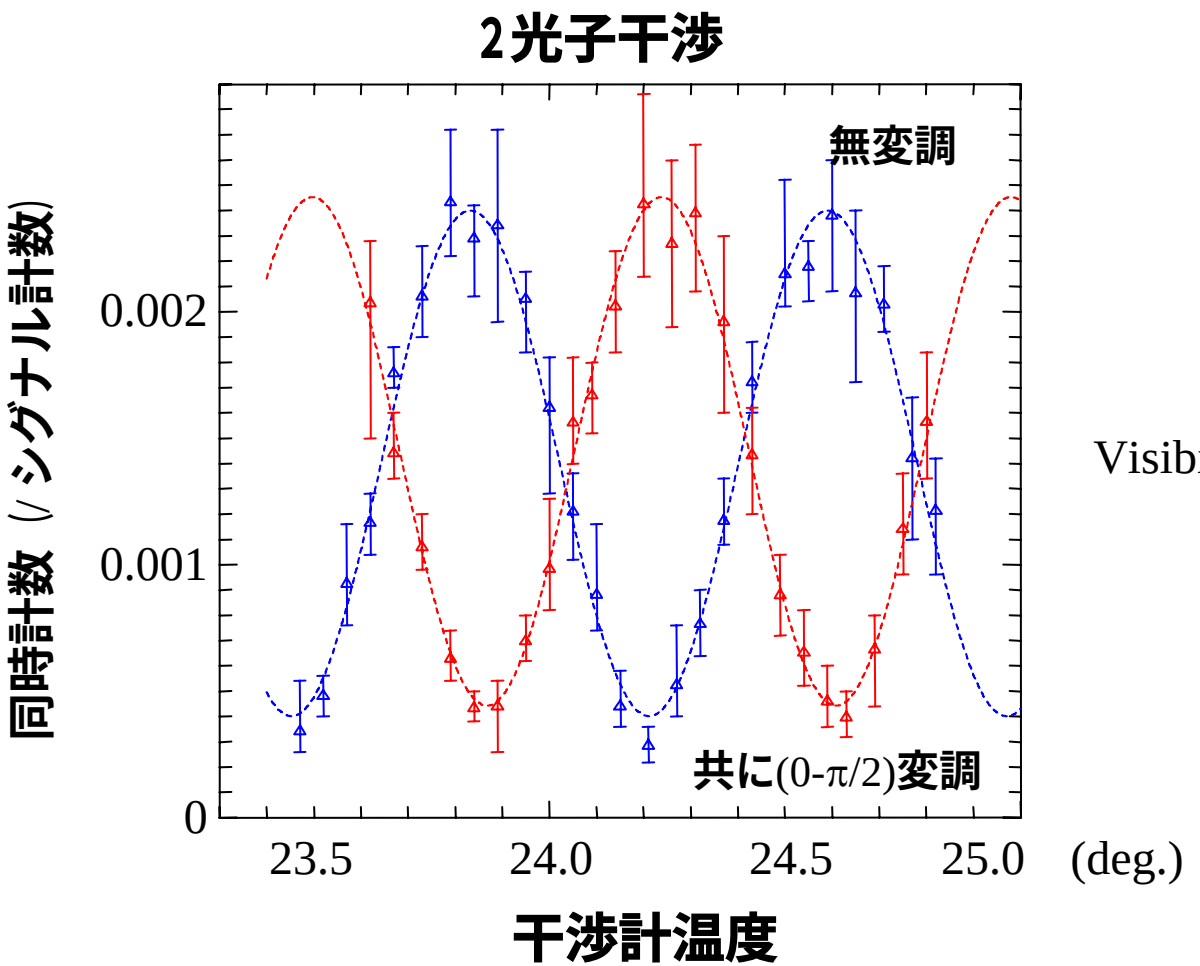
$\Delta\theta_a + \Delta\theta_b = \pi/2$: **無視**

鍵配送実験


ファイバ
(500 m)
AWGフィルタ
シグナル
(1551.6nm)
光増幅
(λ:1551.1nm)
レーザ
強度変調
繰り返し: 1GHz
パルス幅: 100ps
光フィルタ
アイドラー
(1550.6nm)
(*)
もつれ発生


PLC マッハツェンダ干渉計
(ΔL = 20 cm)
(*)
位相変調
位相変調
時間
間隔
測定器

実験結果



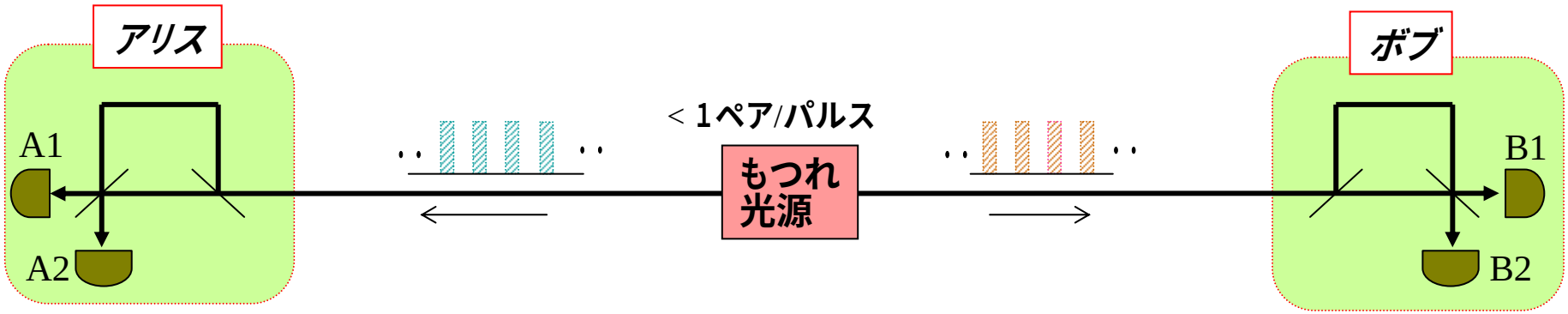
Visibility: 70 %

秘密鍵生成　データレート：0.34 bps

誤り率：8.6%

追加

差動位相量子もつれ鍵配送



位相変調が不要

鍵ビット生成

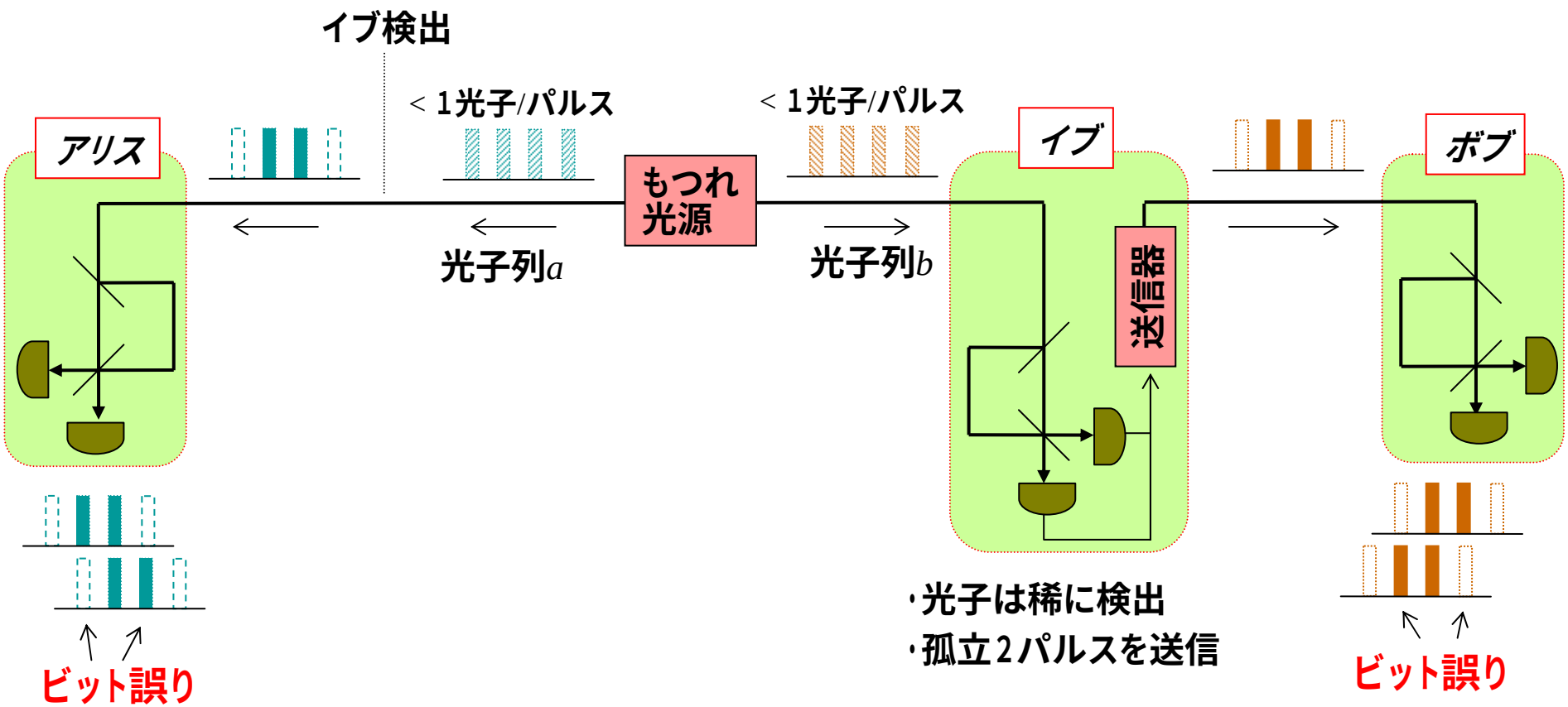
{A1, B1} = 「0」

{A2, B2} = 「1」

安全性1

盗聴に対して－なりすまし攻撃－

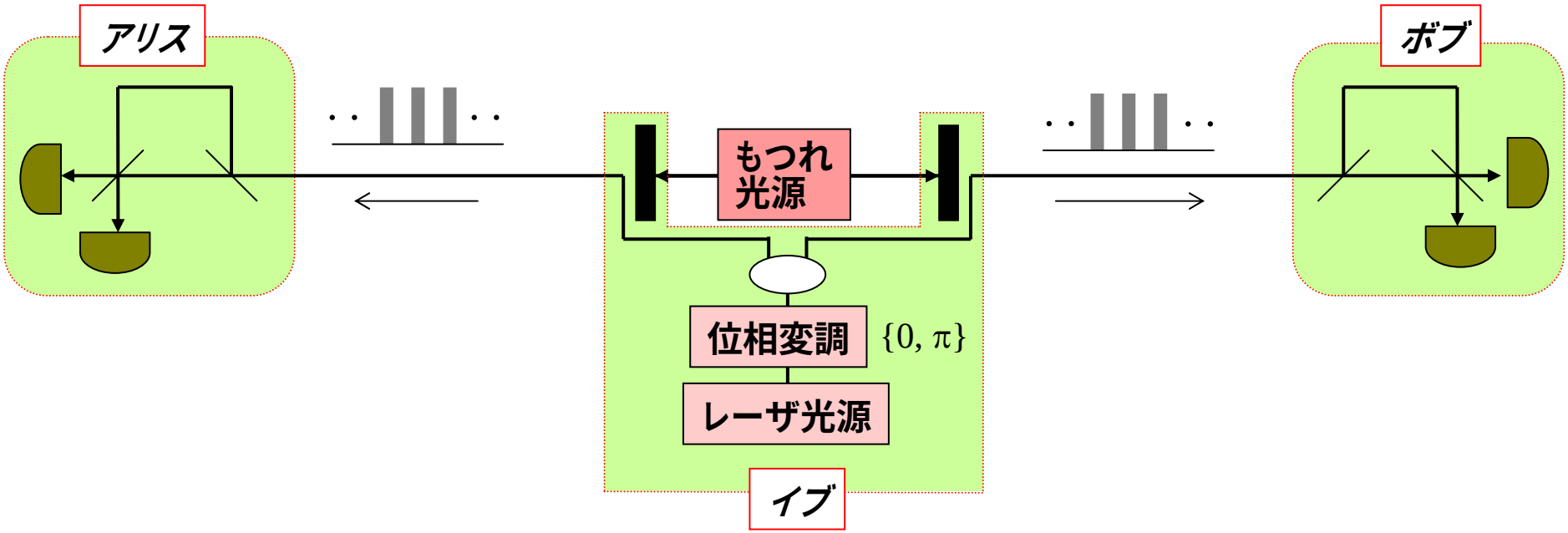
伝送信号を全て受信し、受信結果に基づいて偽装信号を送信。



安全性2

盗聴に対して－光源置き換え攻撃－

もつれ光子列をブロックし、代わりに位相変調光を送信。



レーザ光：AとBで光子検出時刻は独立
もつれ光：AとBで光子検出時刻に相関

⇒ 同時検出レートに違い

⇓

盗聴発覚！

量子鍵配送システム
-量子もつれ光子対-

1．量子鍵配送とは
　　単一光子システムとその課題
2．量子もつれ光子による鍵配送
　　概略
　　ファイバ伝送向け量子もつれ状態
　　システム構成
3．実験
　　光ファイバによるもつれ光子発生
　　鍵配送実験