大阪大学情報通信技術シンポジウム

量子暗号通信

－暗号通信と量子力学の融合－

大阪大学大学院電気電子情報工学専攻
情報通信部門極限光通信工学領域
井上　恭

平成18年2月17日

自己紹介

経歴

1984年　東京大学大学院（修）卒

1984年　ＮＴＴ研究所

（2001 – 2003年　スタンフォード大学訪問研究員）

2005年　大阪大学教授

研究歴

◆光通信、特に波長多重伝送　（1984 - 2001）

光フィルタ、光増幅、ファイバ四光波混合、光信号処理

◆量子光通信　（2001 - ）

日本経済新聞 (9/4)

朝日新聞 (12/13)

内容

[1] 量子暗号で使う量子力学

量子力学的重ね合わせ、状態と観測問題

[2] 単一光子による量子鍵配送

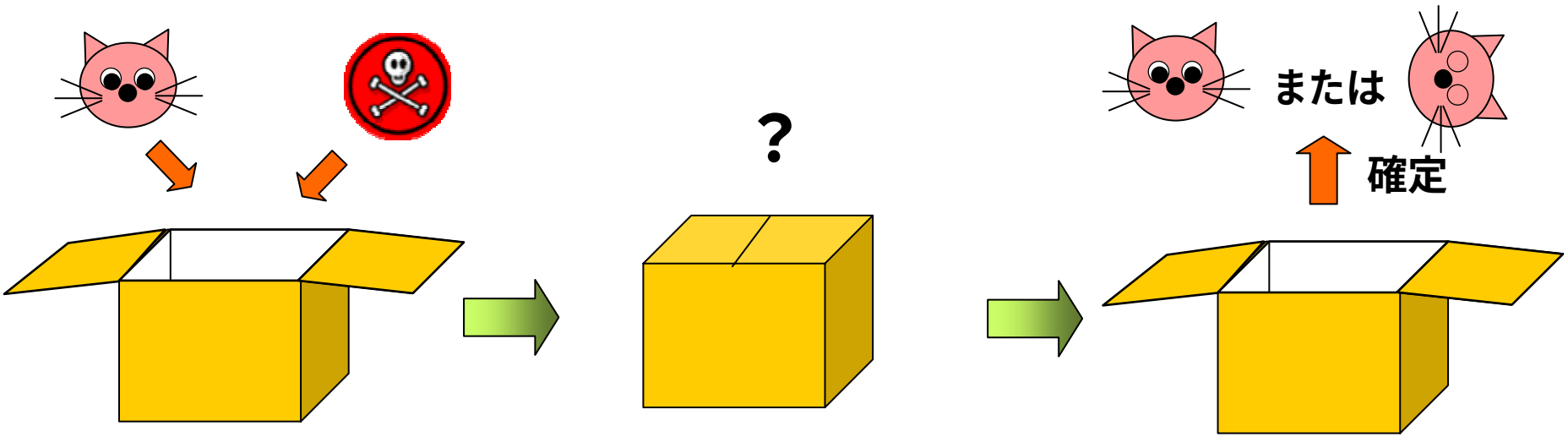
ＢＢ８４方式、差動位相シフト方式

[3] 量子もつれ光子による量子鍵配送

量子もつれとは、量子中継

量子暗号で利用する量子力学　－量子力学的重ね合わせ－

シュレディンガーの猫



問題：　箱の中の猫の状態は？

答1：　生きているか死んでいるかのどちらか。決まっているけど見えないだけ。← 古典

答2：　生きているかもしれないし、死んでいるかもしれない。
わからないのだからどちらもあり。← 量子

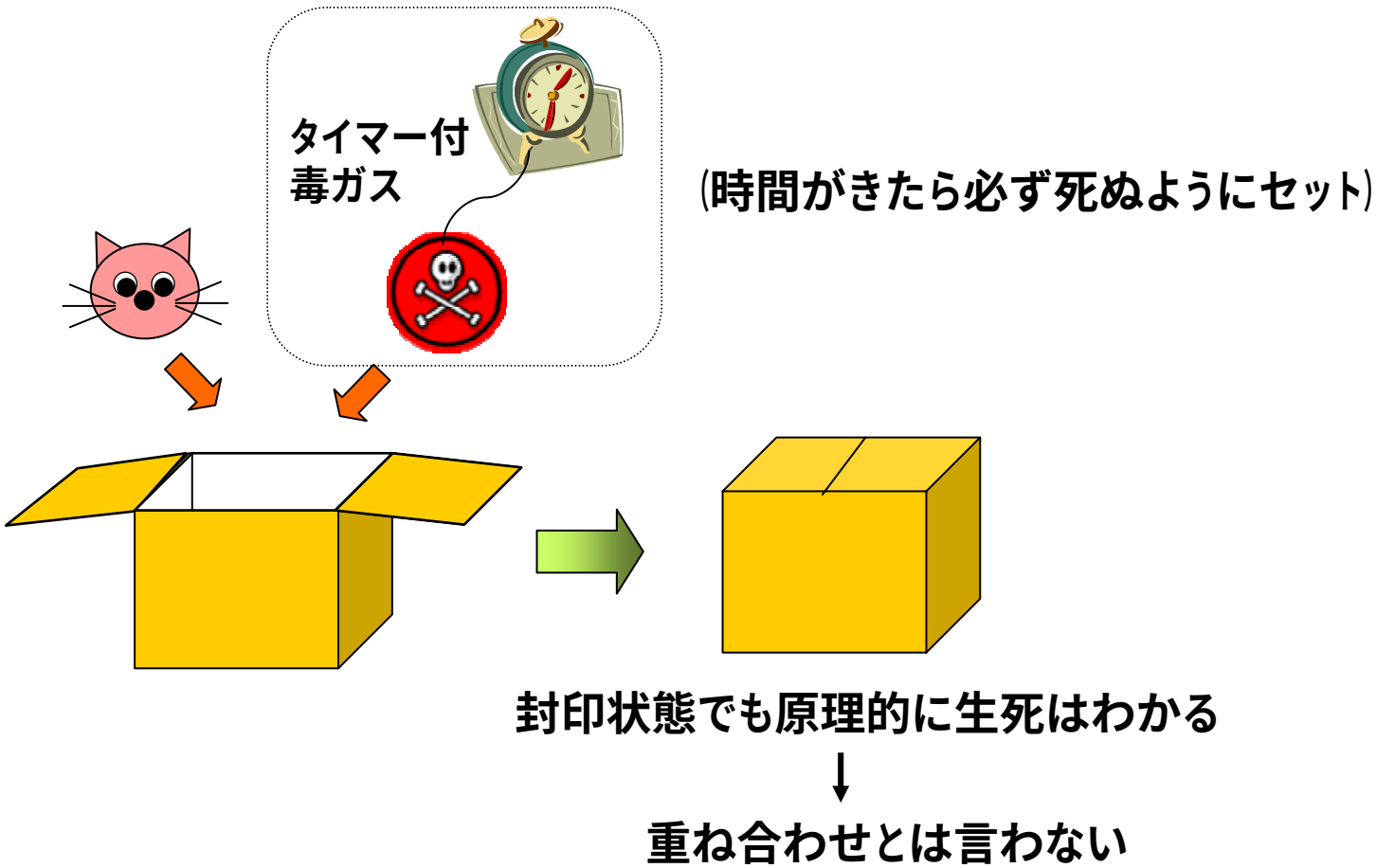
量子力学的には、どちらの状態もありとする。＝「量子力学的重ね合わせ」

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

（係数 $|a|^2$, $|b|^2$ で存在確率を表わす）

$$|a|^2 + |b|^2 = 1$$

原理的にどちらかわからない事がポイント



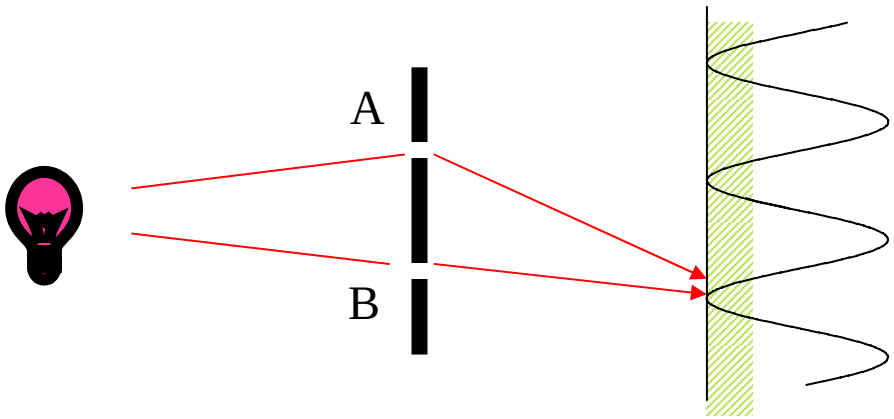
（時間がきたら必ず死ぬようにセット）

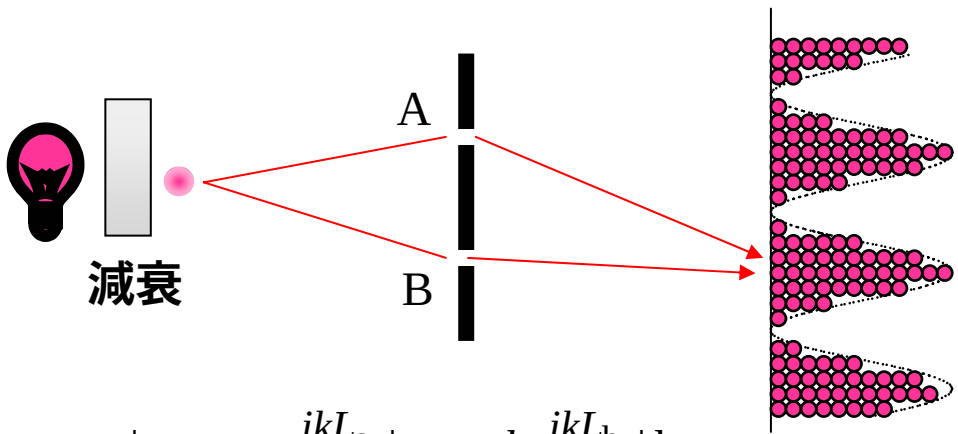
封印状態でも原理的に生死はわかる

↓

重ね合わせとは言わない

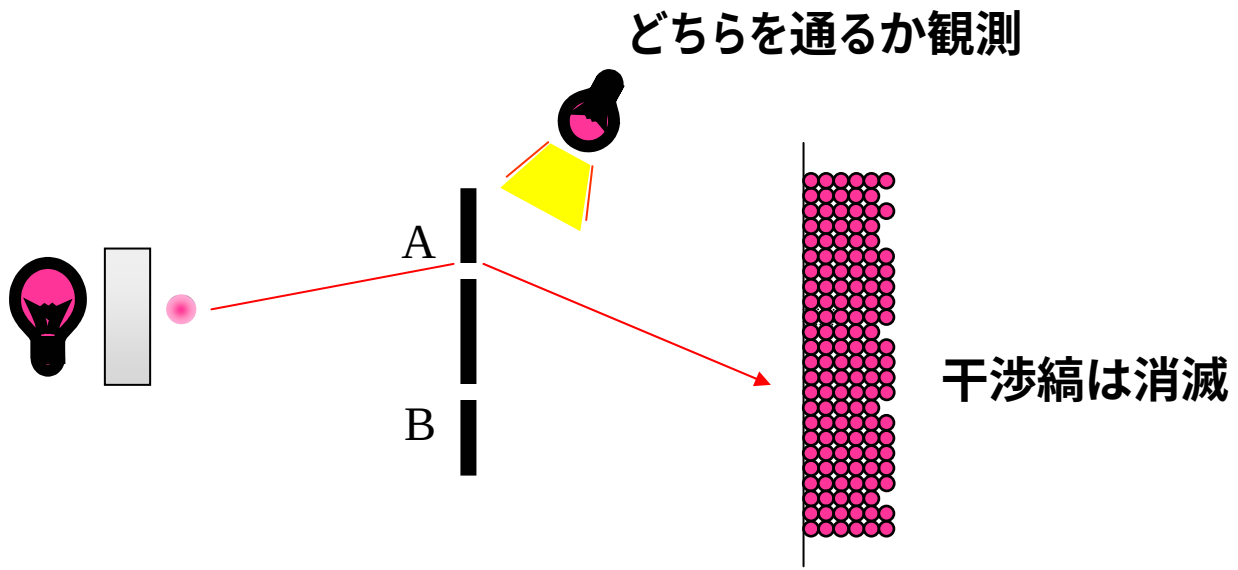
ヤングの干渉実験 -光は波であり粒子である-





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

|a>：光子がAを通った状態
|b>：光子がBを通った状態



$$|\psi>= a e^{ikL_a}|a> + b e^{ikL_b}|b>$$

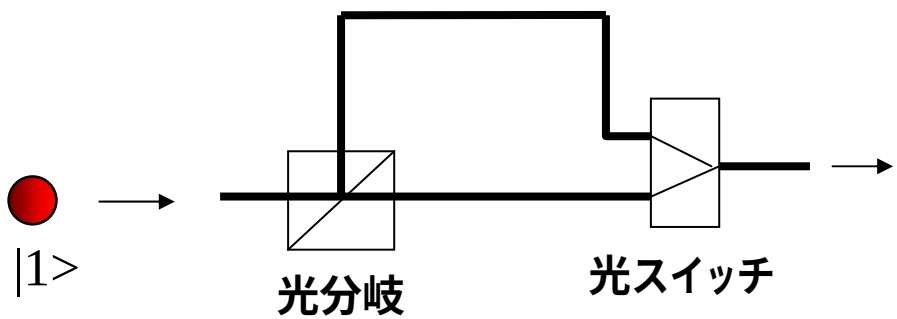
観測

$|\psi>=|a>$ or $|\psi>=|b>$

a^2 b^2

重ね合わせ状態の例1：光子の時間位置

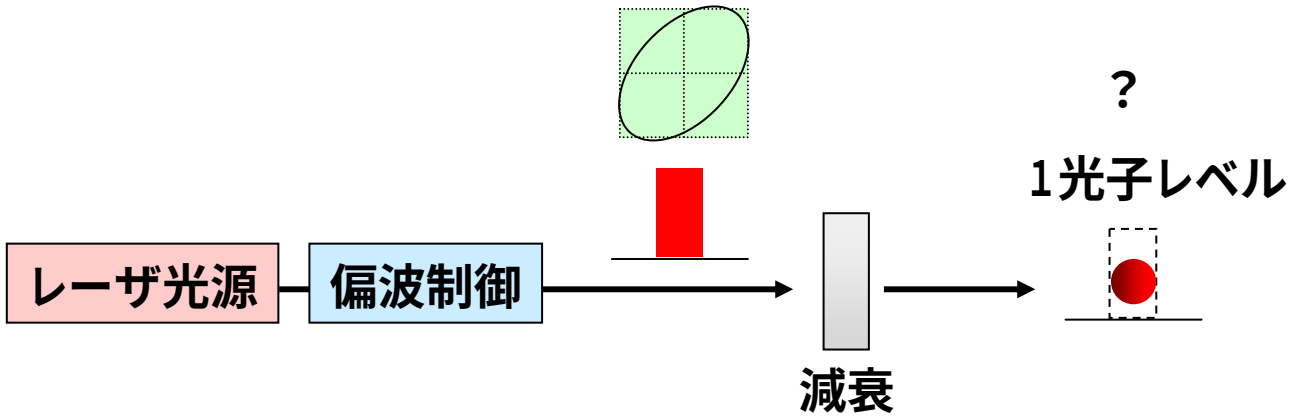
1光子を2分岐し、一方を遅延させて再び合波。

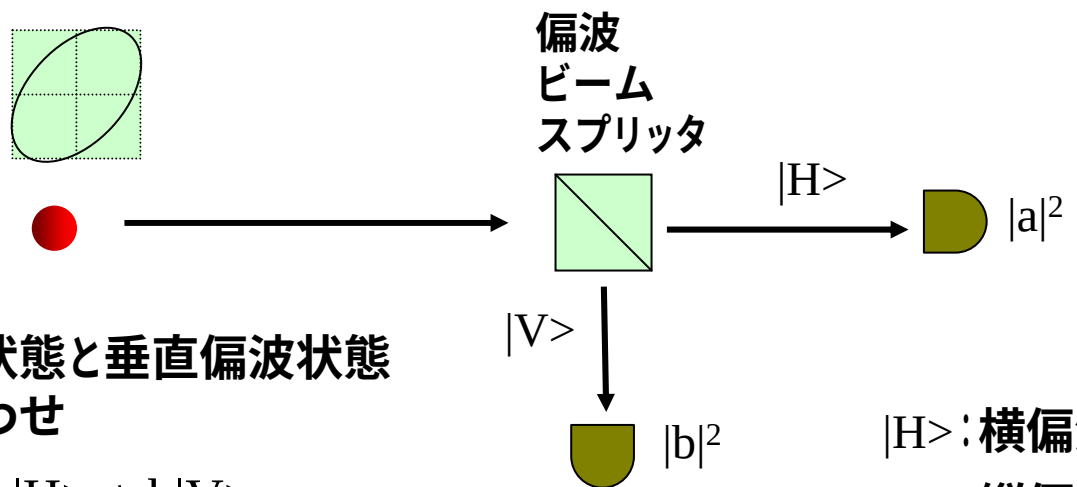


1光子状態

$$|\Psi_{out}\rangle = a_1|1\rangle_{t1} + a_2|1\rangle_{t2}$$

重ね合わせ状態の例2：光子の偏波状態





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>：横偏波光子状態

|V>：縦偏波光子状態

量子情報通信

量子力学的重ね合わせを安全な暗号鍵配布システムに利用しよう

↓

量子暗号 (量子鍵配送)

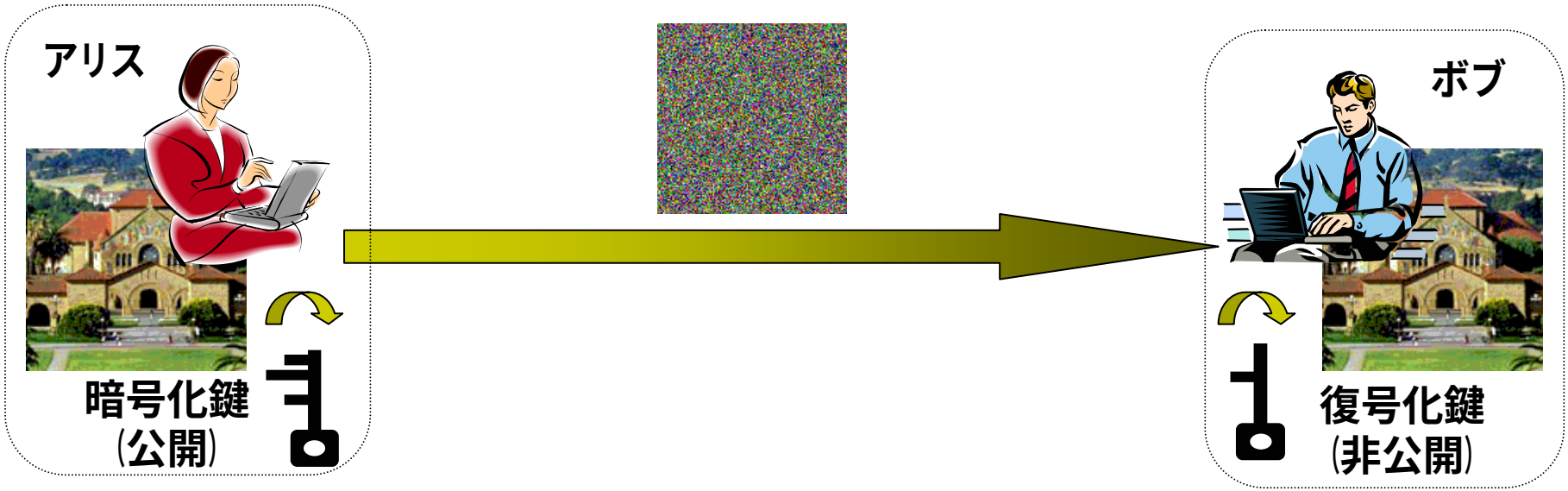
量子力学的重ね合わせを超並列計算に利用しよう

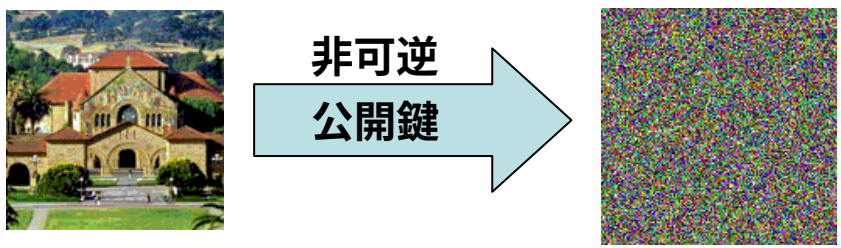
↓

量子コンピュータ

(まずは、現在の暗号方式から)

公開鍵暗号方式



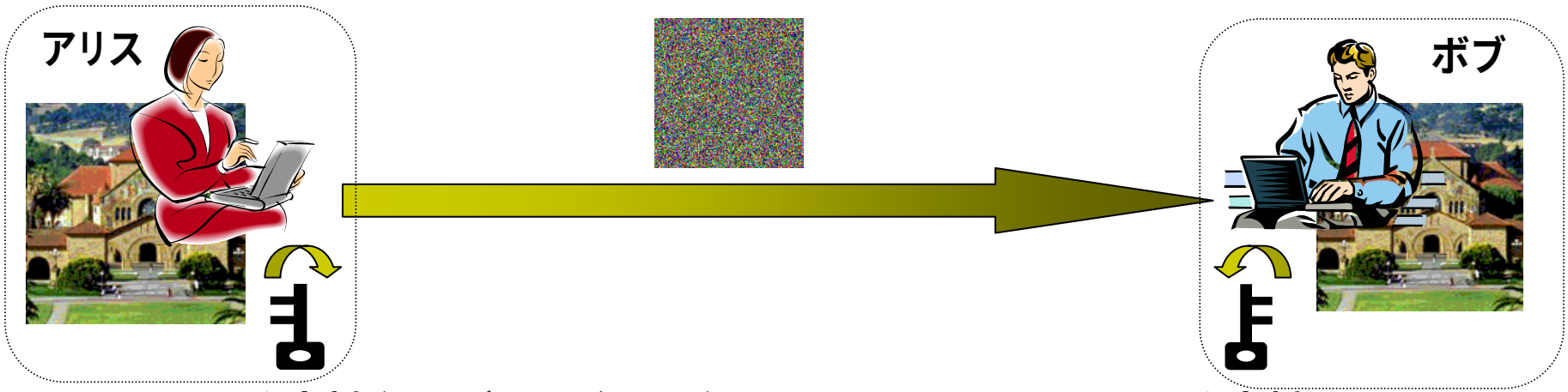


367 × 521 = Z (191207) ：easy

191207 = X × Y ：difficult

原理的には解読可能

秘密鍵暗号方式



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

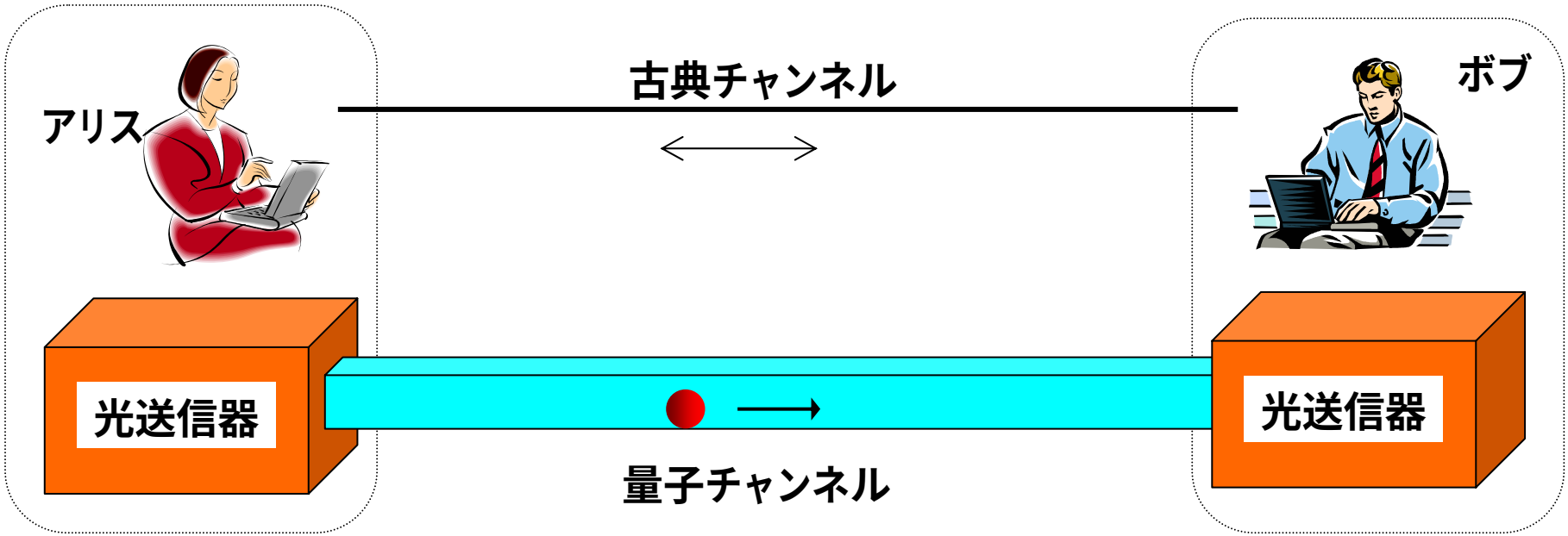
But、秘密鍵をどうやって安全に供給するか？

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　安全性は量子力学的に保証

量子鍵配送の基本構図



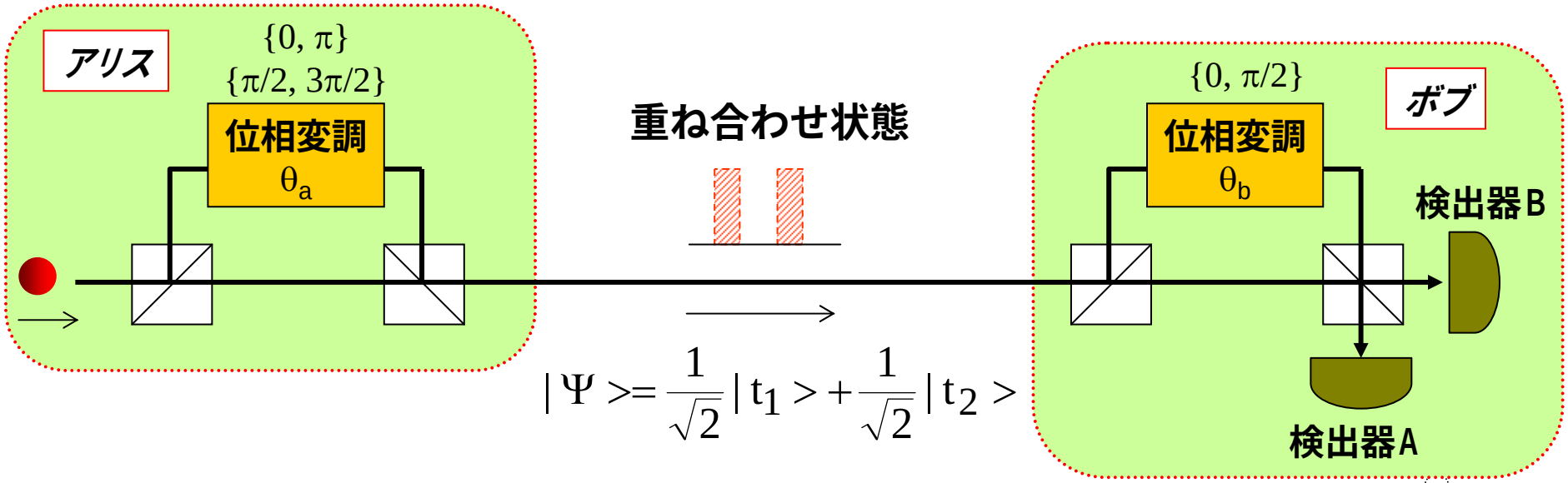
①量子チャンネルで光子を送受信

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

量子鍵配送システムの構成例1：ＢＢ８４方式



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：θ_a = {0, π} か {π/2, 3π/2}か、を通知

ボブ→アリス：θ_b = 0かπ/2か、を通知

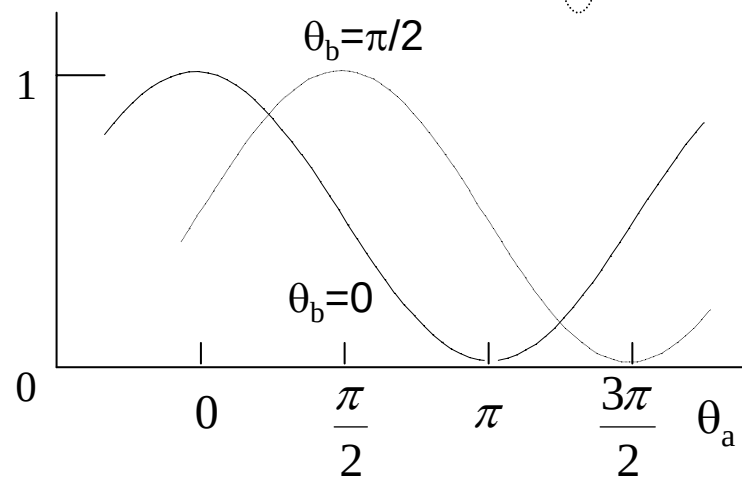
④鍵ビット生成

アリス：θ_a = 0, π/2 ⇒「0」、θ_a = π, 3π/2 ⇒「1」

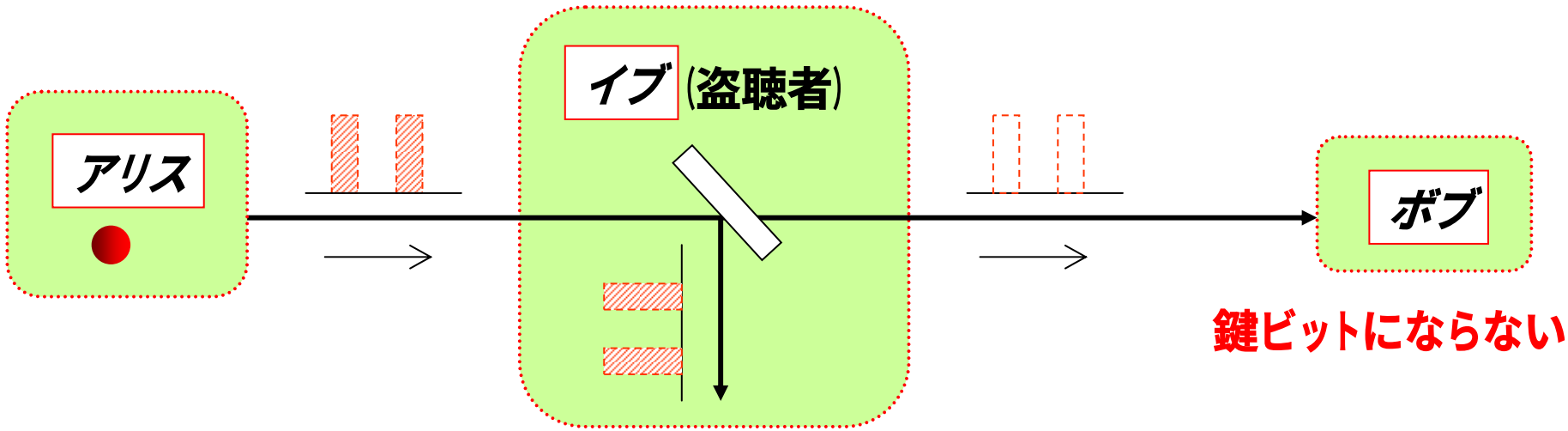
ボブ：検出器A ⇒ 「0」、検出器B ⇒ 「1」

→ 秘密鍵

検出確率
@検出器A

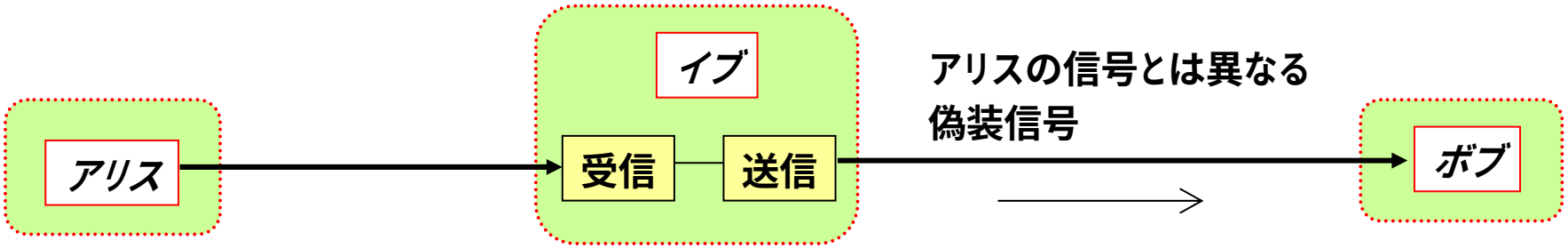


なぜ安全か（その1）–盗み聞き盗聴に対して–



伝送信号をタッピング

なぜ安全か（その2）–なりすまし盗聴に対して–



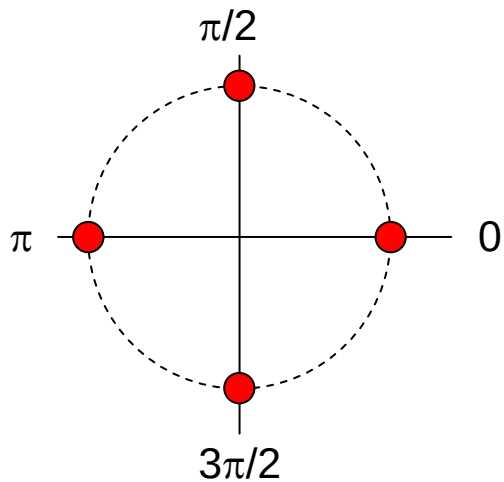
アリスの信号とは異なる
偽装信号

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。

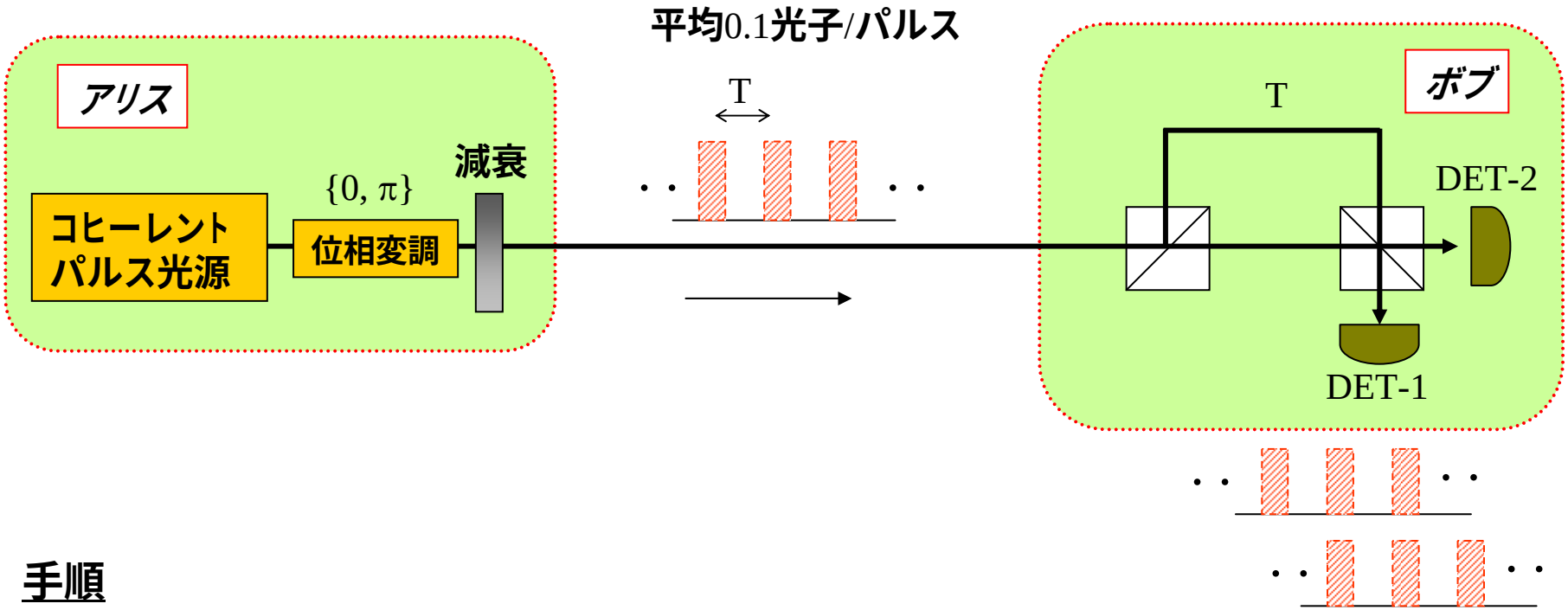


{0, π}を識別しようとすると、{π/2, 3π/2}は不定

{π/2, 3π/2}を識別しようとすると、{0, π}は不定

オリジナル提案 by Inoue

量子鍵配送システムの構成例2：差動位相シフト方式



手順

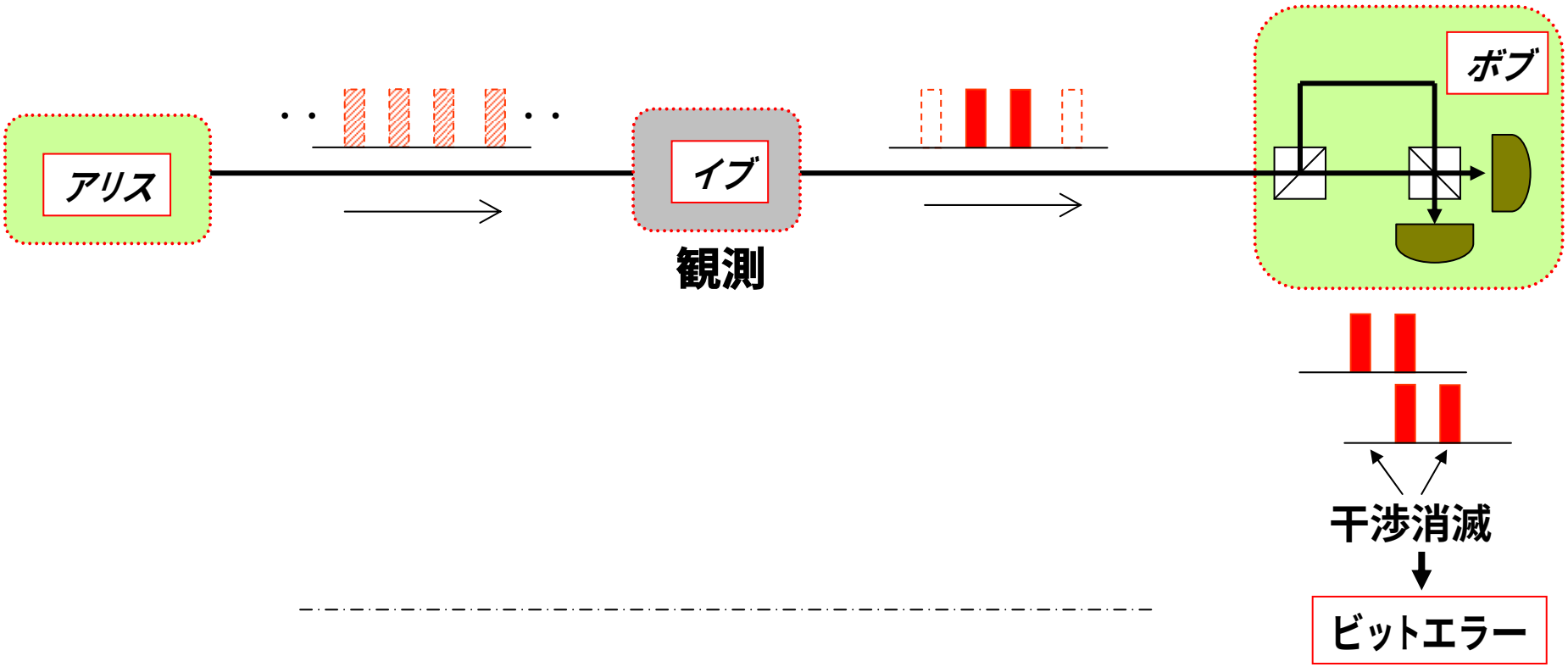
①ボブ：光子を検出した時刻と検出器を記録

②ボブ→アリス：光子検出時刻を通知

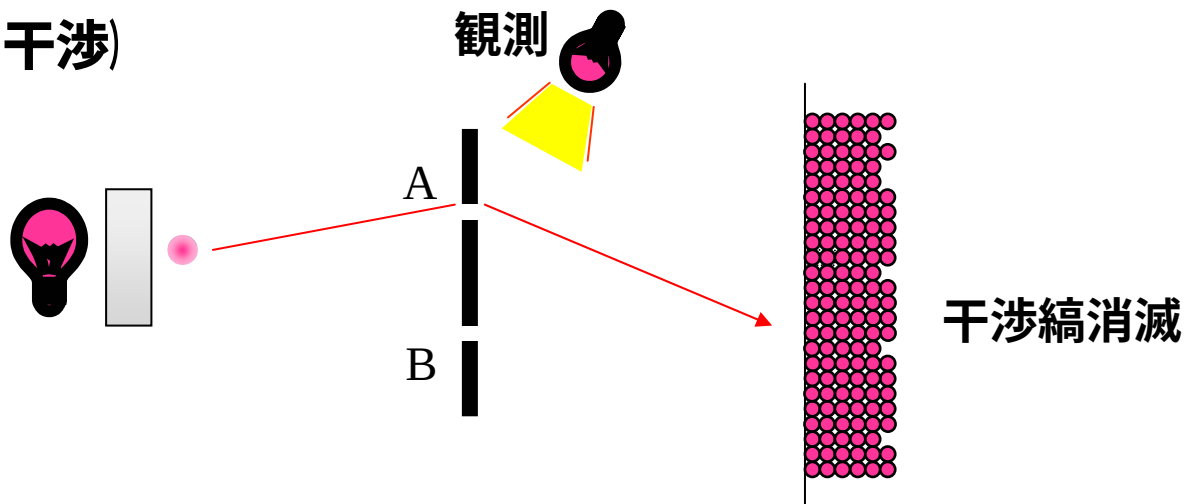
③アリス：自分の変調データから光子検出した検出器を特定

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**

なぜ安全か

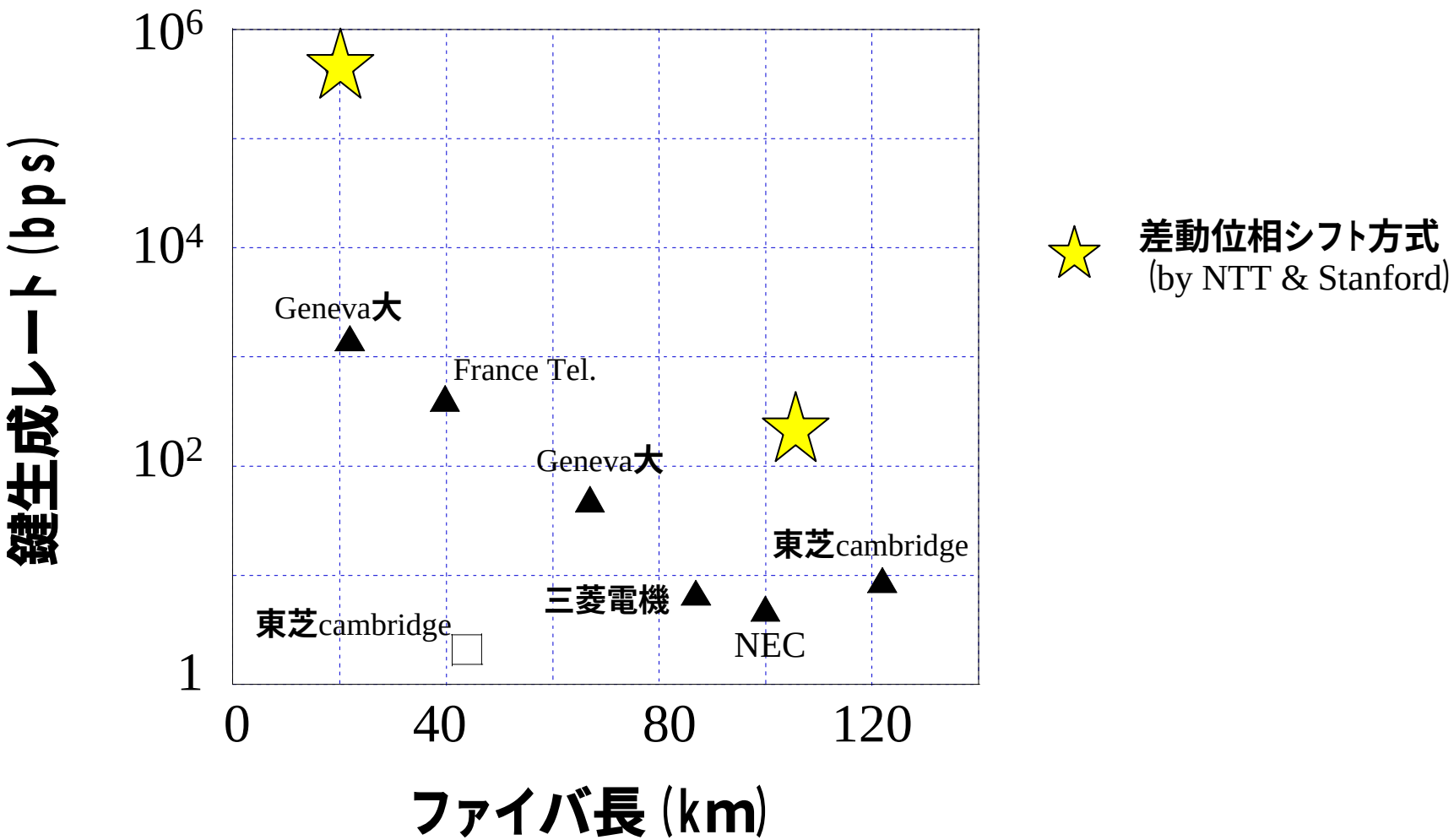


(ヤングの干渉)



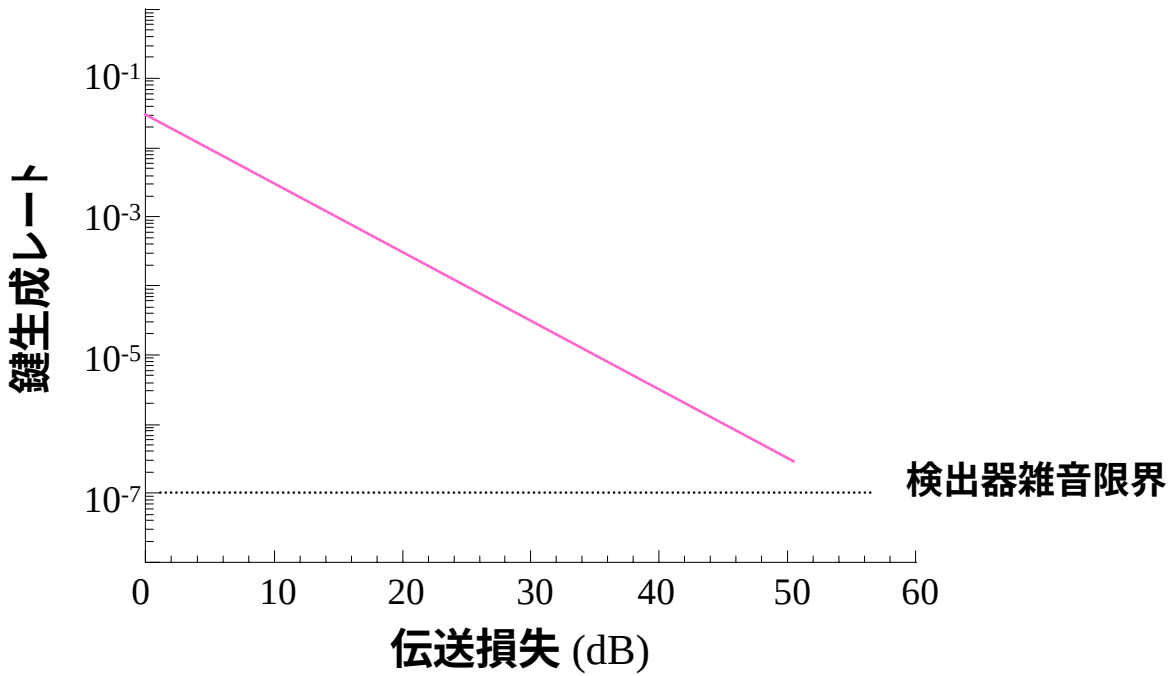
これまでの実験報告例

(但し、▲は完全に安全な鍵生成ではない)



課題：伝送距離の制限

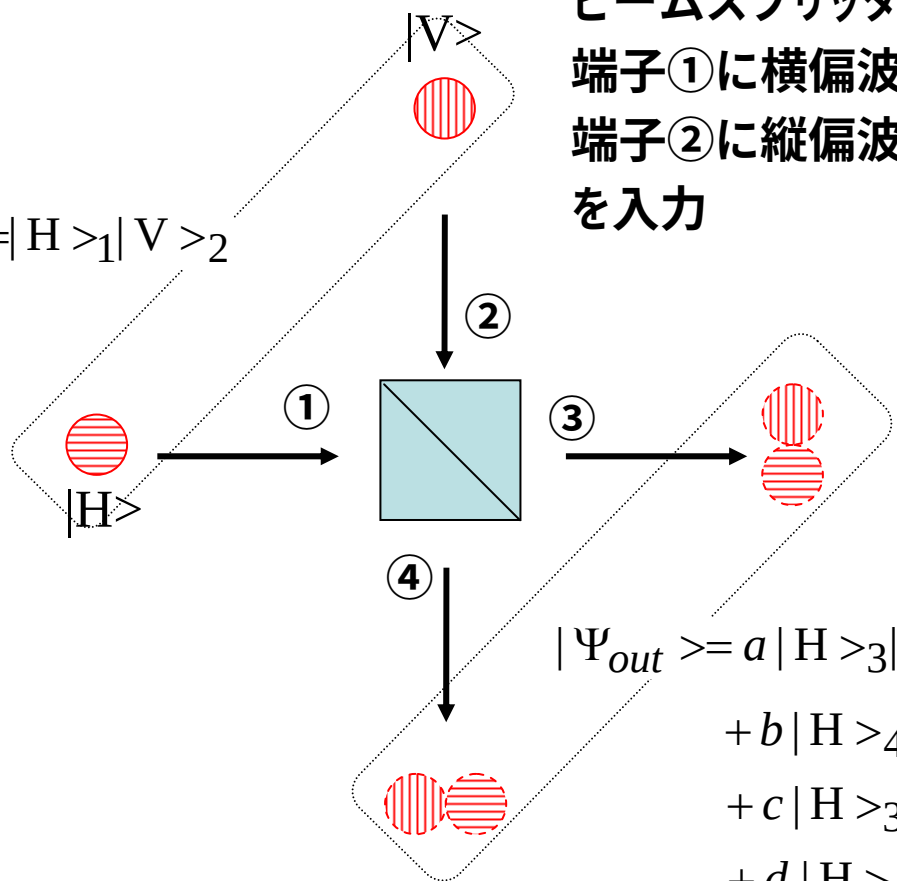
伝送距離が長くなると光子が消滅



量子もつれを利用して長距離化

量子もつれの前段階として

2光子の重ね合わせ状態



ビームスプリッタの
端子①に横偏波光子、
端子②に縦偏波光子、
を入力

$|\Psi_{in}>=|H>_1|V>_2$

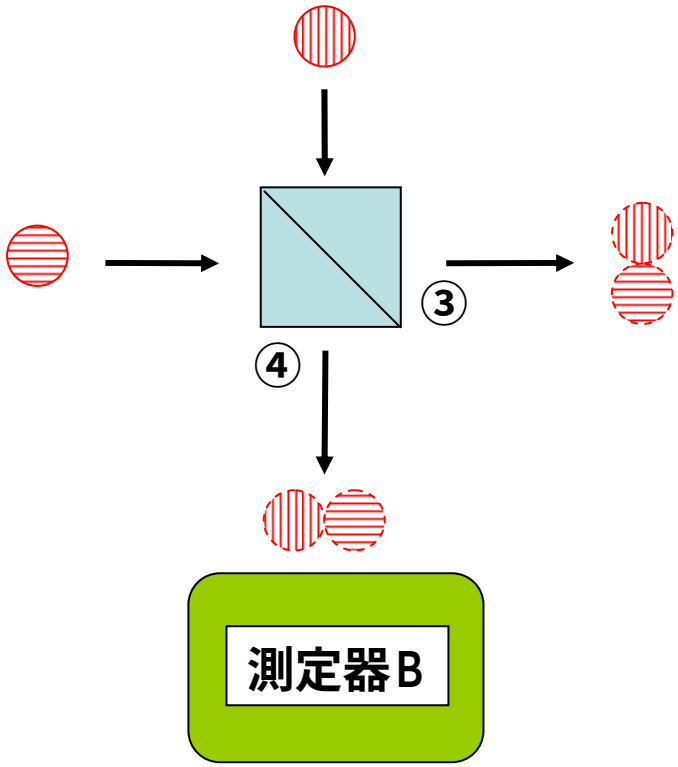
$|\Psi_{out}>= a|H>_3|V>_3$ ：2光子とも③へ

$+b|H>_4|V>_4$ ：2光子とも④へ

$+c|H>_3|V>_4$ ：横偏波は③へ、縦偏波は④へ

$+d|H>_4|V>_3$ ：横偏波は④へ、縦偏波は③へ

特殊な重ね合わせ状態：量子もつれ状態



$$|\Psi_{out}>= a\,|\mathrm{H}>_3|\mathrm{V}>_3 + b\,|\mathrm{H}>_4|\mathrm{V}>_4$$

$$+ c\,|\mathrm{H}>_3|\mathrm{V}>_4 + d\,|\mathrm{H}>_4|\mathrm{V}>_3$$

$\downarrow$ ($c = d$ とする)

$$|\Psi'>= c\{|\mathrm{H}>_3|\mathrm{V}>_4 + |\mathrm{H}>_4|\mathrm{V}>_3\}$$

量子もつれ状態

◆一方の測定器だけをみると、縦か横かは確率的。

◆両方の測定器をみると、一方が縦なら他方は必ず横。

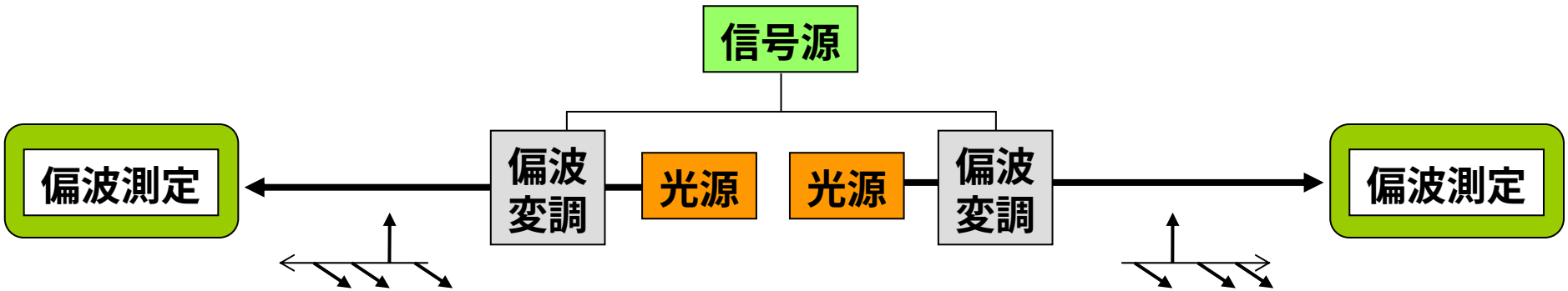
量子もつれの性質

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2) \longrightarrow$$ 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)

古典もつれとの違い



縦・横偏波系で測定 → 一方が縦 (or 横)だと他方も縦 (or 横)

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。

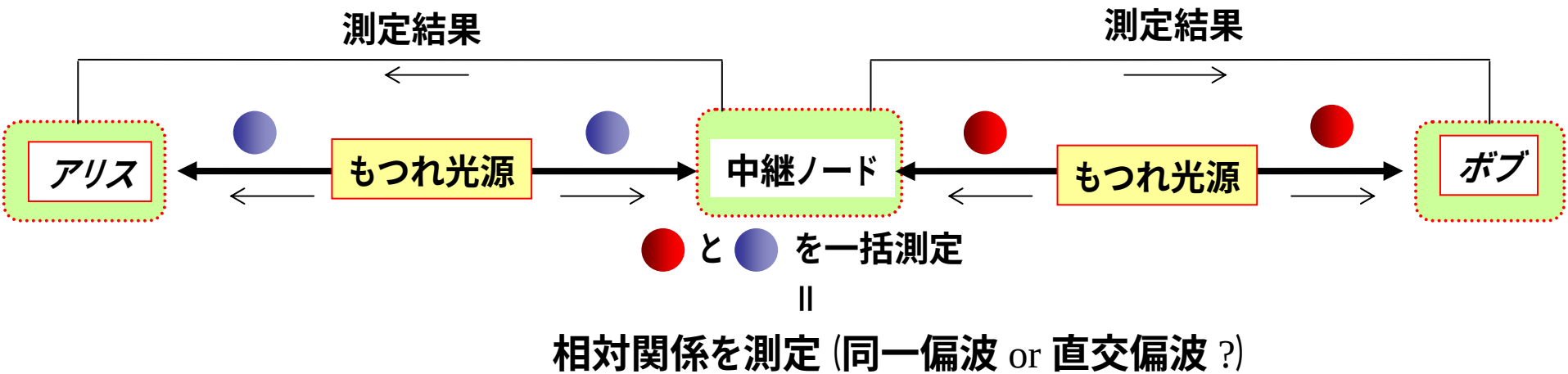
量子もつれを使う量子鍵配送

アリスとボブの測定結果に相関あり ⟶ 秘密鍵ビット生成

アリス-ボブ間距離は2倍

さらに長距離化

量子中継



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

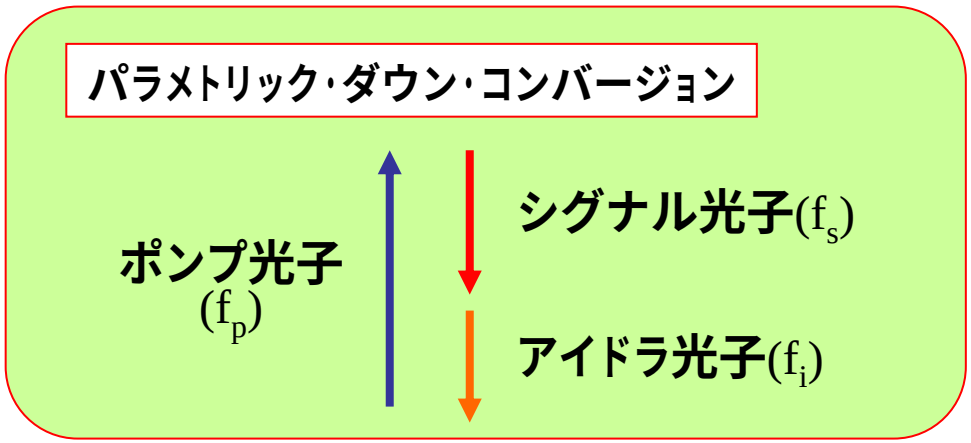
⇩

アリス-ボブで鍵生成

量子もつれ発生法

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

$|H>_s|H>_i$

非線形媒質

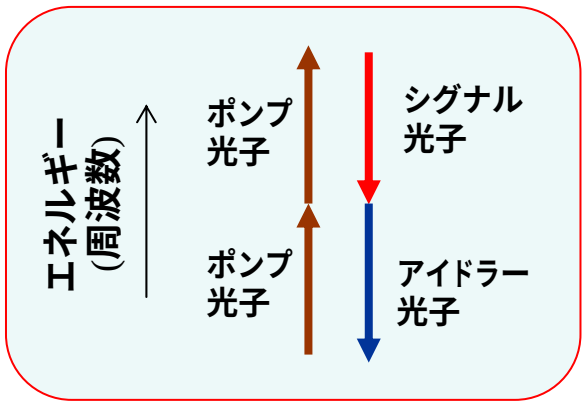
$|V>_s|V>_i$

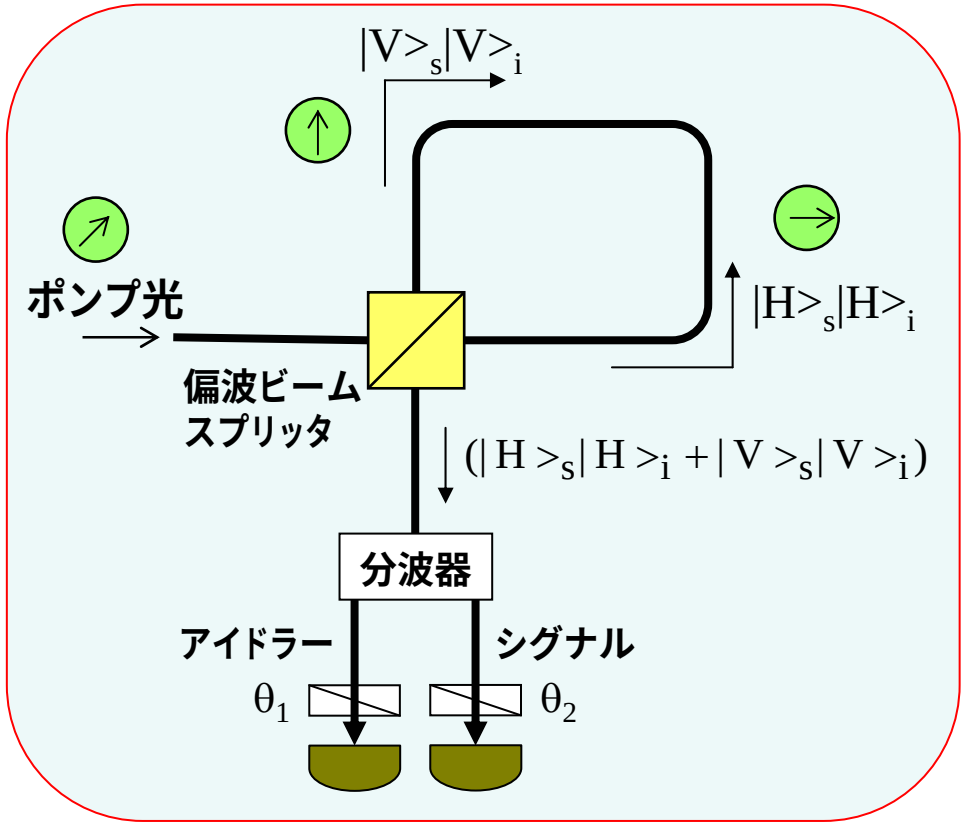
$|H>_s|H>_i$ or $|V>_s|V>_i$

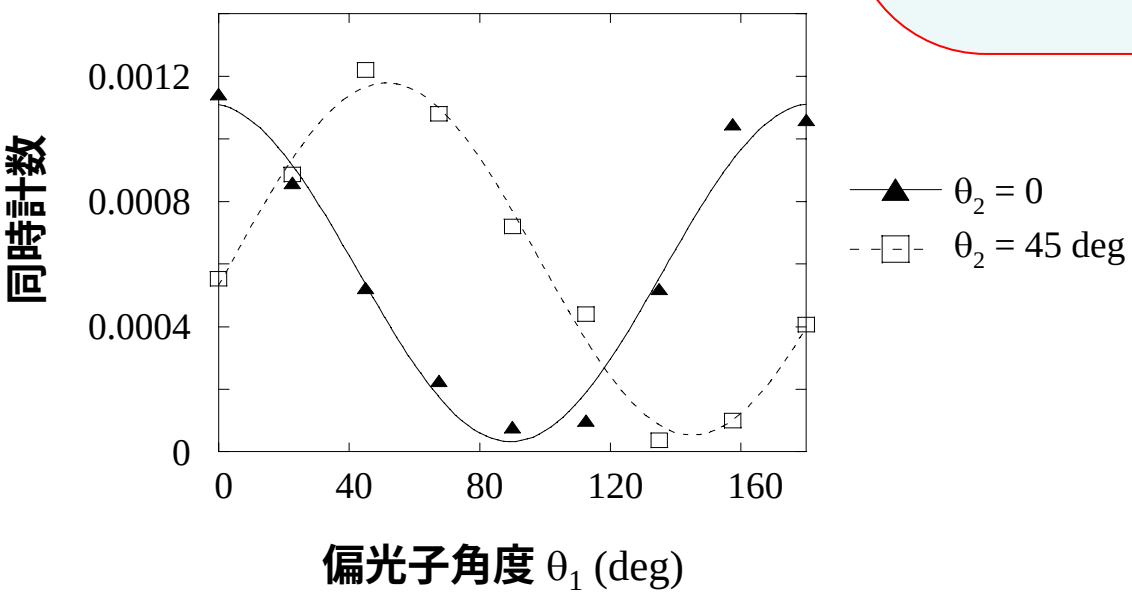
with appropriate pump power

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

ファイバ四光波混合法


エネルギー
(周波数)
ポンプ
光子
ポンプ
光子
シグナル
光子
アイドラー
光子


$|V>_s|V>_i$
ポンプ光
偏波ビーム
スプリッタ
$|H>_s|H>_i$
$(|H>_s|H>_i + |V>_s|V>_i)$
分波器
アイドラー
シグナル
θ_1
θ_2


同時計数
0.0012
0.0008
0.0004
0
0
40
80
120
160
偏光子角度 θ_1 (deg)
θ_2 = 0
θ_2 = 45 deg