QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett, Gilles Brassard

Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, pp 175-179, December 1984.

量子暗号 : 公開鍵配送とコイン投げ

11-041-061
松原　多玖人

- 量子暗号:量子力学の原理を使った暗号
- 「BB84」と呼ばれている暗号の手順を世界で初めて提案した論文

  →東芝、NECなどで製品化に向けた研究が進行中(後日平川がNECの論文を紹介)
- 本発表:量子暗号の最初の論文をなるべく忠実に紹介
- Coin Tossingは時間の関係で紹介しません

目次

1. 論文の概要
2. 本論文で提案された暗号の特徴
3. この暗号で利用する量子状態
4. 鍵配送の具体的な手順
   ① 鍵配送とは
   ② 量子通信路上での手順
   ③ 古典通信路上での手順
5. まとめ

論文の概要

- 量子系を使ってデジタル情報を送信

  →不確定性原理により、従来は不可能であった新しい暗号が可能に

  本論文では、偏光した光子を用いて、盗聴を検知できる通信を提案

- 量子通信路と古典通信路との組合わせ

  →安全に乱数鍵を2者間で配送可能

  (事前の秘密情報の共有も不要)

目次

本論文で提案する暗号

	従来の暗号 (ENIGMA, DES, RSA)	本論文の暗号
原理	推量と数学の組み合わせ	不確定性原理
安全性	公開鍵暗号は証明なし	盗聴者の存在を検出可能
通信内容の読み取り、コピー	可能	不可能

本論文の暗号の特徴

- 安全に鍵を共有できる
  - 改ざんできない古典通信路があると
    →事前に秘密情報を共有しなくても安全に鍵を共有できる　→公開鍵暗号と同じ機能
  - 改ざん可能な古典通信路でも
    →事前に秘密情報を共有していれば安全
- 盗聴者が超技術や無限の計算能力を持っていても量子力学が正しければ安全

本論文の暗号の特徴

- 実用上の困難
  - ✓信号強度を弱くする必要がある
  - ✓送信中に増幅できない
- 公開鍵暗号にはできても、量子暗号ではできないことがある

  →デジタル署名など

論文の概要

- 量子系を使ってデジタル情報を送信

  →不確定性原理により、従来は不可能であった新しい暗号が可能に

  本論文では、偏光した光子を用いて、盗聴を検知できる通信を提案

- 量子通信路と古典通信路との組合わせ

  →安全に乱数鍵を2者間に配送可能

  (事前の秘密情報の共有も不要)

後に証明される量子暗号の特徴を述べている

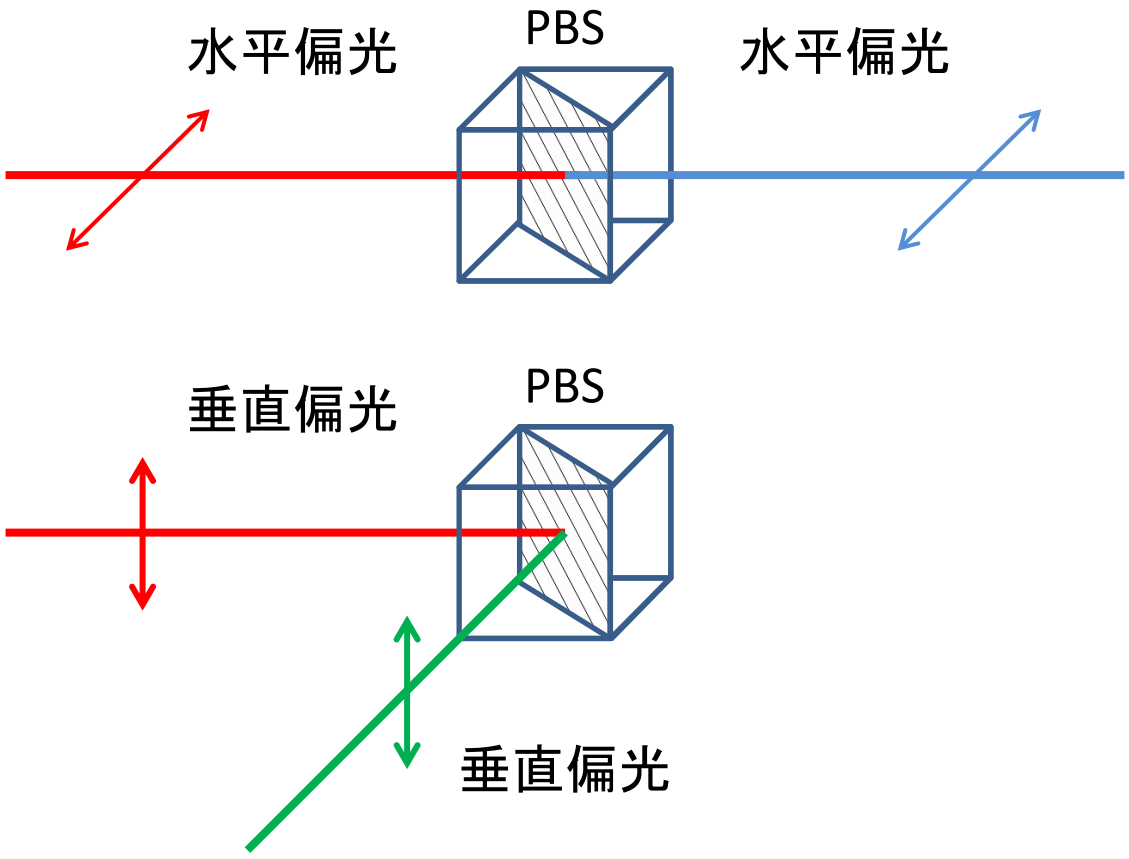
目次

偏光した光子

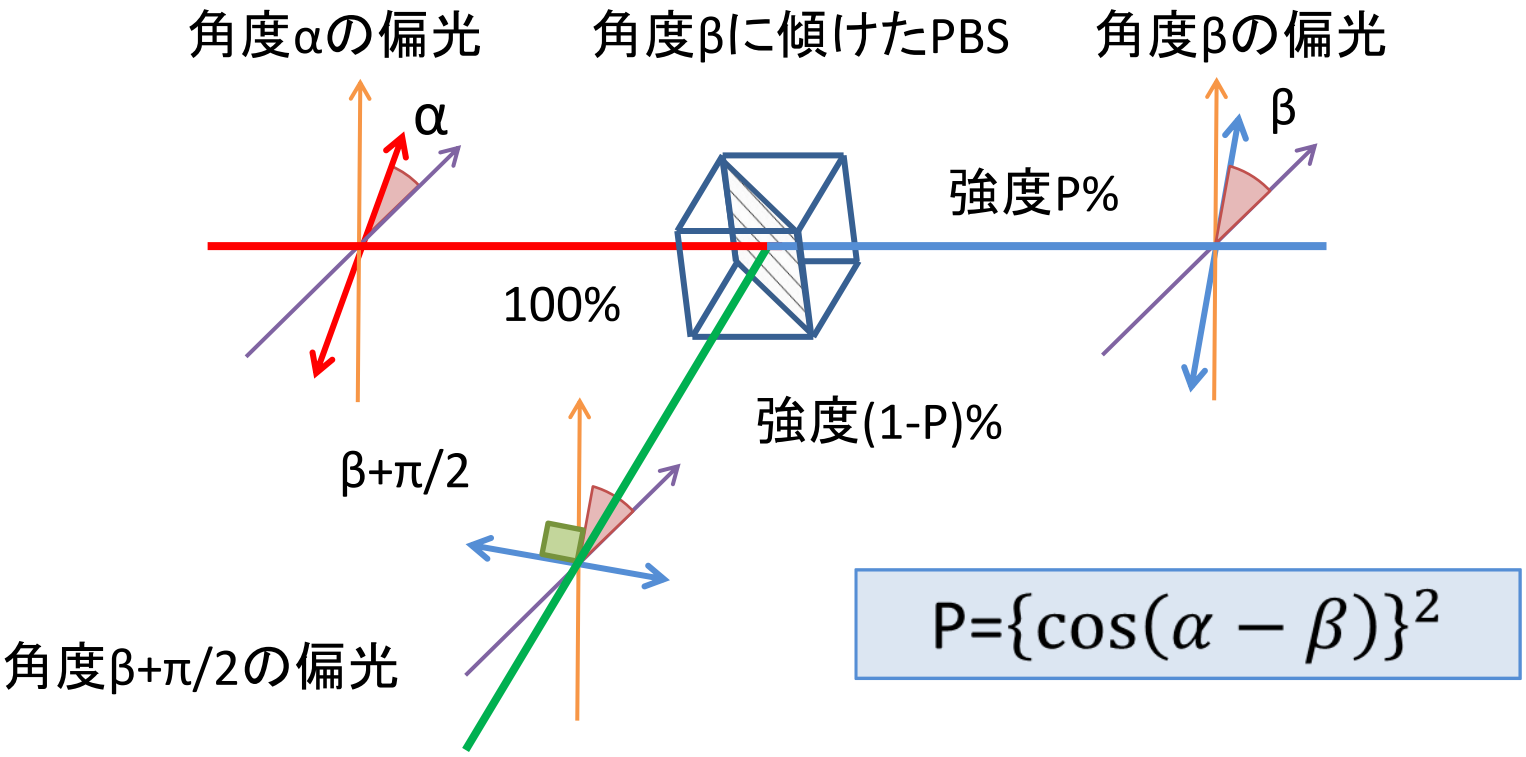
- 普通の光線を偏光板、又は方解石結晶へ
  →直線偏光した光線に
- 直線偏光の偏光面
  →偏光光線を発生する装置の向きによる
- 1個の偏光した光子も作れる
  →原理的には、偏光光線から光子を1個持ってくればよい
  →実験的にも可能(単一の原子からの放出)

PBSについての補足

- PBS(polarized beam splitter)
- 水平偏光を透過し、垂直偏光を反射する

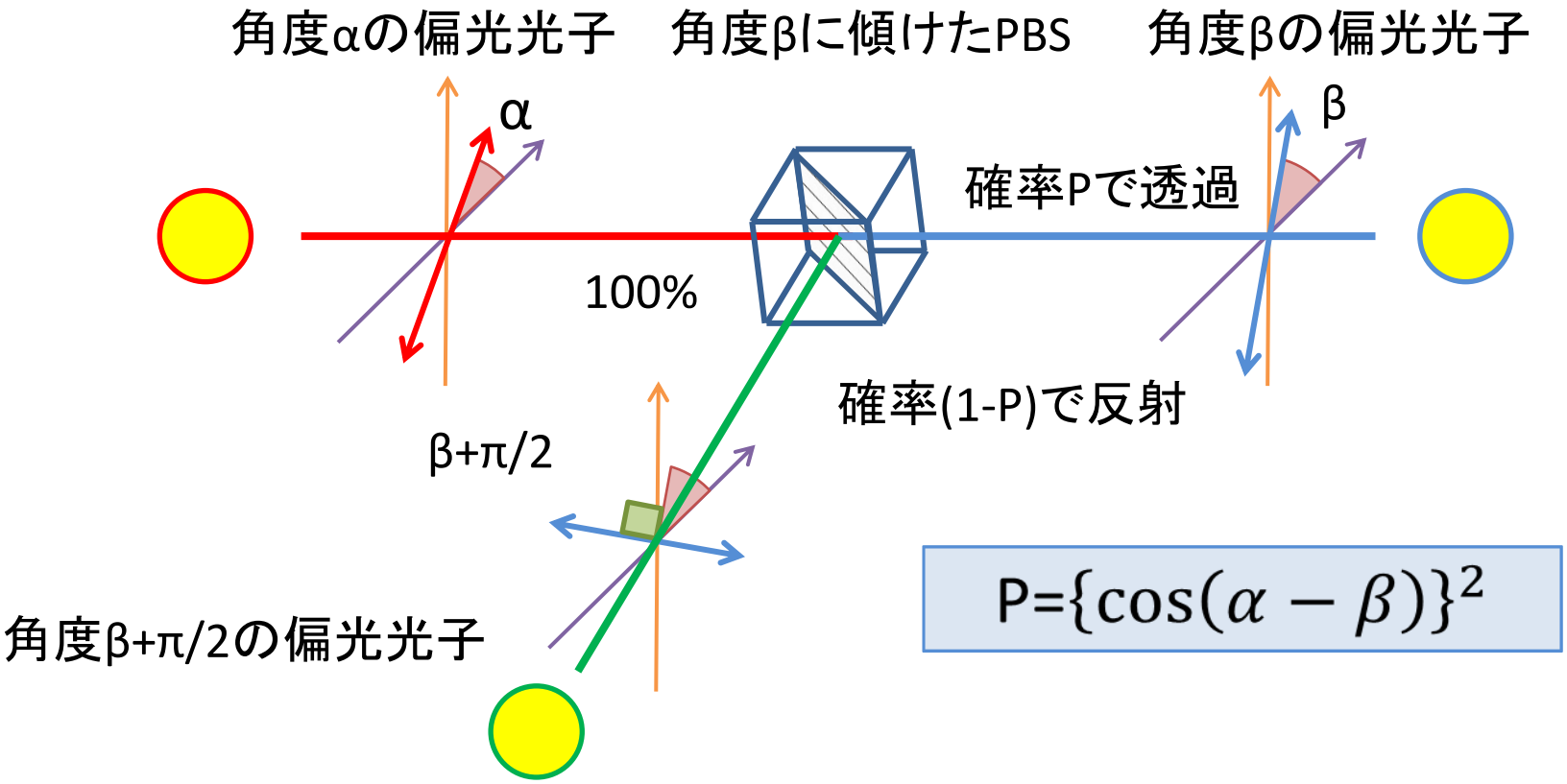


偏光した光線の振る舞い



$$P=\{\cos(\alpha-\beta)\}^2$$

偏光した光子の振る舞い



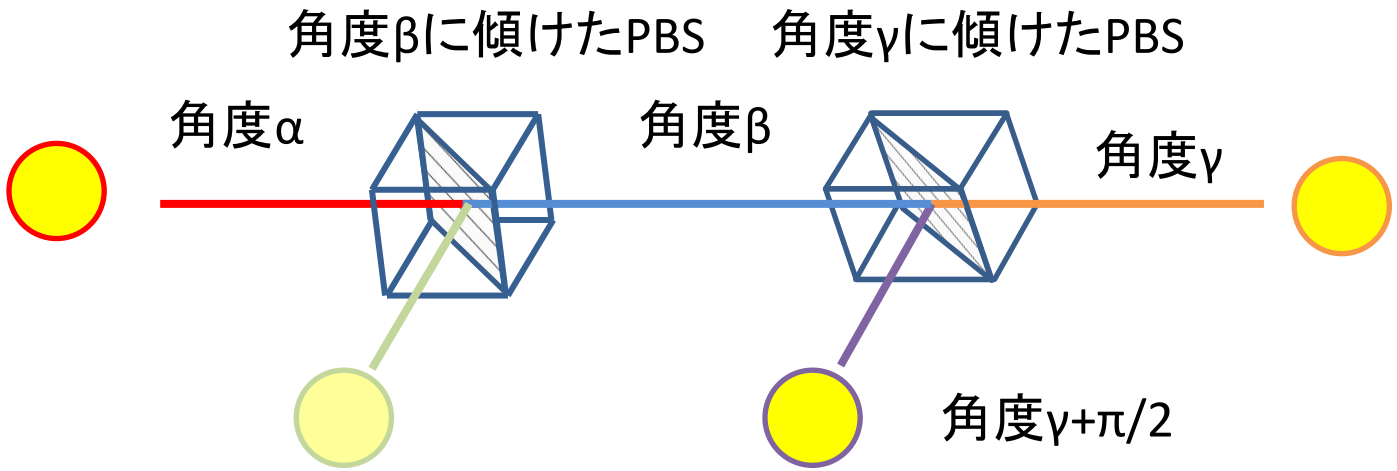
$$P=\{\cos(\alpha-\beta)\}^2$$

光子の持つ情報

- βのPBSを通った後、別の角度を向いたPBSでαについての情報を知りたい　→不可能

  理由:偏光板を通った偏光はちょうど角度βに

  →角度αの偏光の情報は全て失う



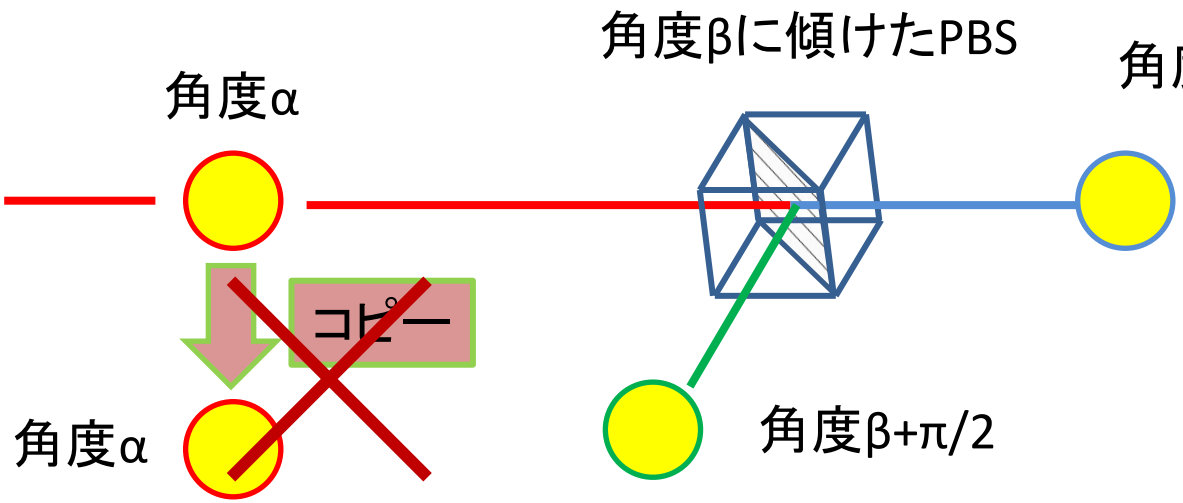
光子の持つ情報

- 捕まえた光子を複製してから測定する

  →光子1つから1bit以上の情報を引き出そう

  →しかし、これも不可能

  理由:未知の量子状態の複製は、量子力学の基本と矛盾する(複製不可能定理)



目次

目次

鍵配送とは

- 量子通信路では意味のある情報は送らない
- 送るのはランダムなビット列の情報
- ビット列の送信者がアリス、受信者がボブ
- 通信が妨害されなかった場合

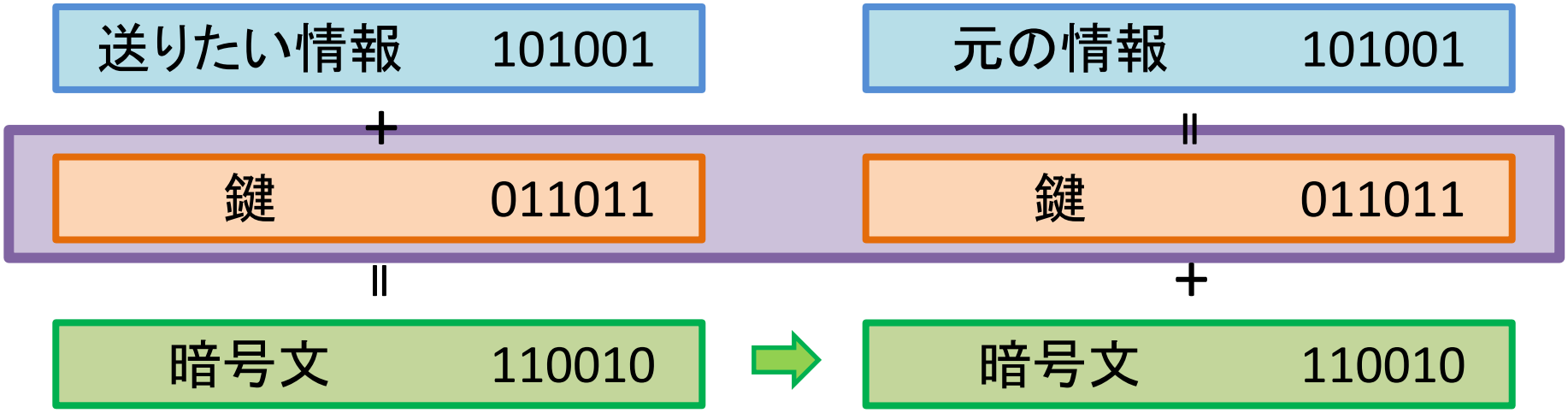
  →共有された鍵を使って意味のある通信を安全に行える
- 通信が妨害された場合

  →最初からやり直す

鍵についての補足

- 鍵は0と1のビット列
- 情報理論によると
  - ✓ 少なくとも平文より長い事
  - ✓ 使用するのは1度のみ

  の2条件を満たせば安全な通信ができる



目次

アリス側の手順

基底とビット列の準備

- まずアリスはビット列をランダムに用意する
  0 または 1
- 送信する偏光の基底もランダムに選ぶ
  R基底 または D基底

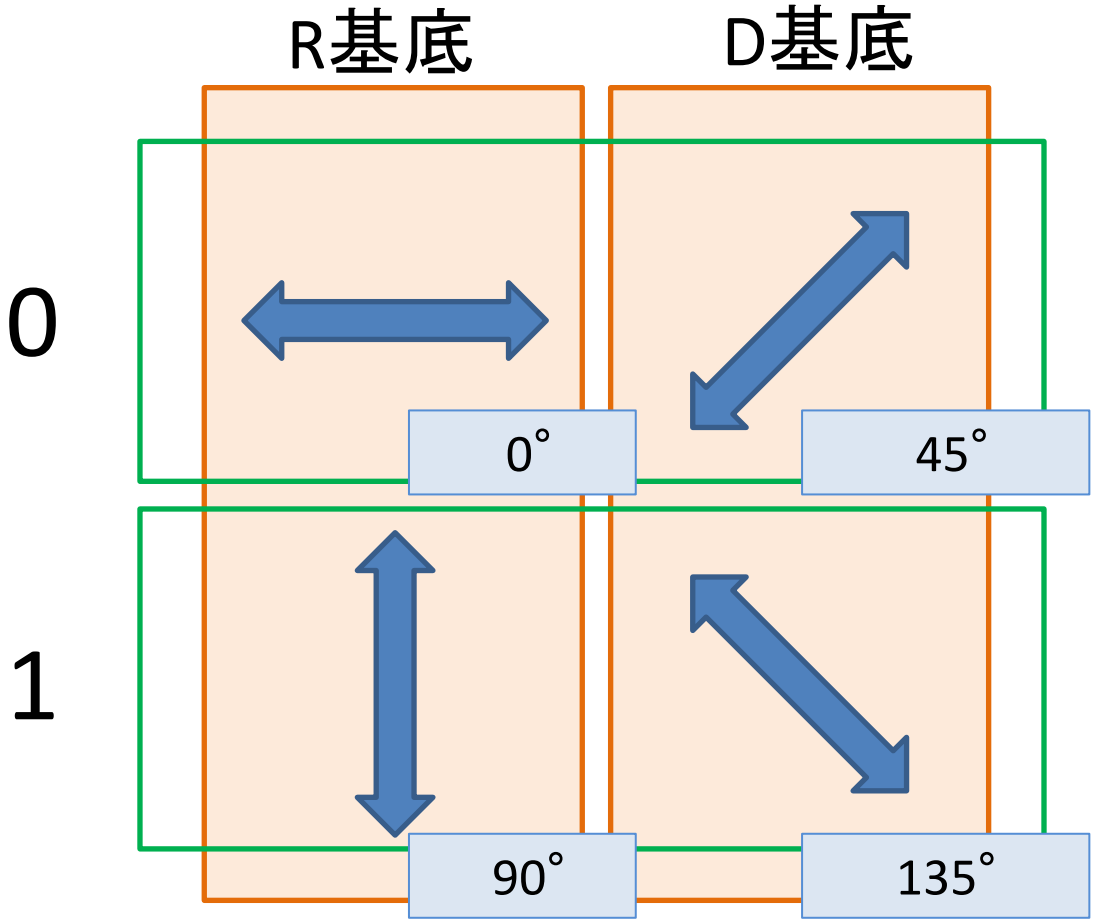
例

選んだビット	0	1	1	0	1	1
選んだ基底	D	R	D	R	R	R

アリス側の手順

基底とビット列の準備

- ビットと偏光の向きの対応
  - ➢偏光面の向きは2進数の0,1に対応している

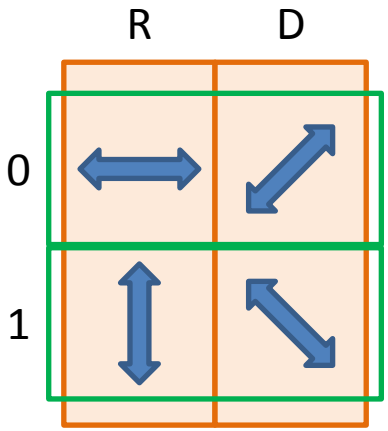


アリス側の手順

基底とビット列の準備

- アリスは、選んだビットと基底から、送信する光子の偏光を決定する

選んだビット	0	1	1	0	1	1
選んだ基底	D	R	D	R	R	R
偏光の角度	↗	↕	↘	↔	↕	↕



ボブ側の手順

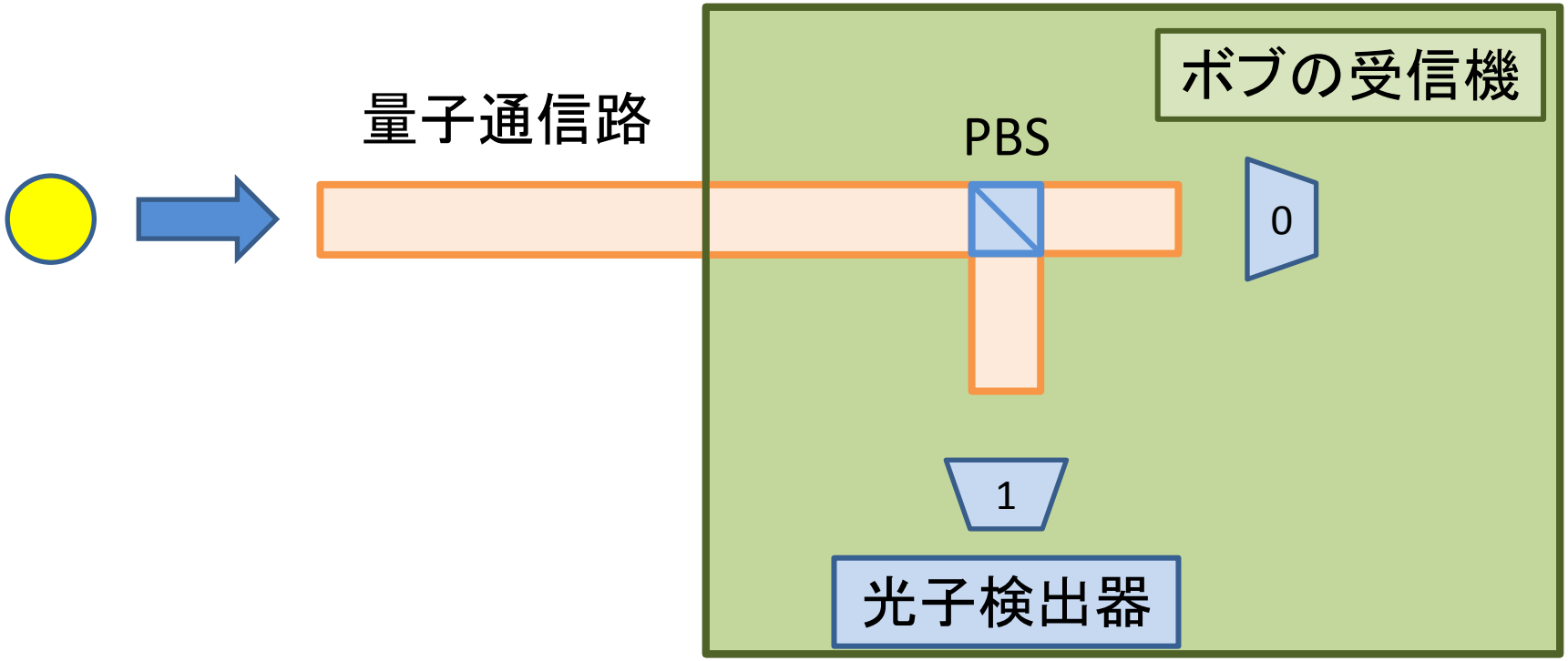
ボブの受信と基底の選択

- ボブはR基底かD基底に切り替え可能な受信機を持っている。
- ボブは受信する度にどちらを使うかをランダムに選択

アリスが選んだビット	0	1	1	0	1	1
アリスが選んだ基底	D	R	D	R	R	R
アリスが送った状態						
ボブが選んだ基底	R	D	D	R	R	D

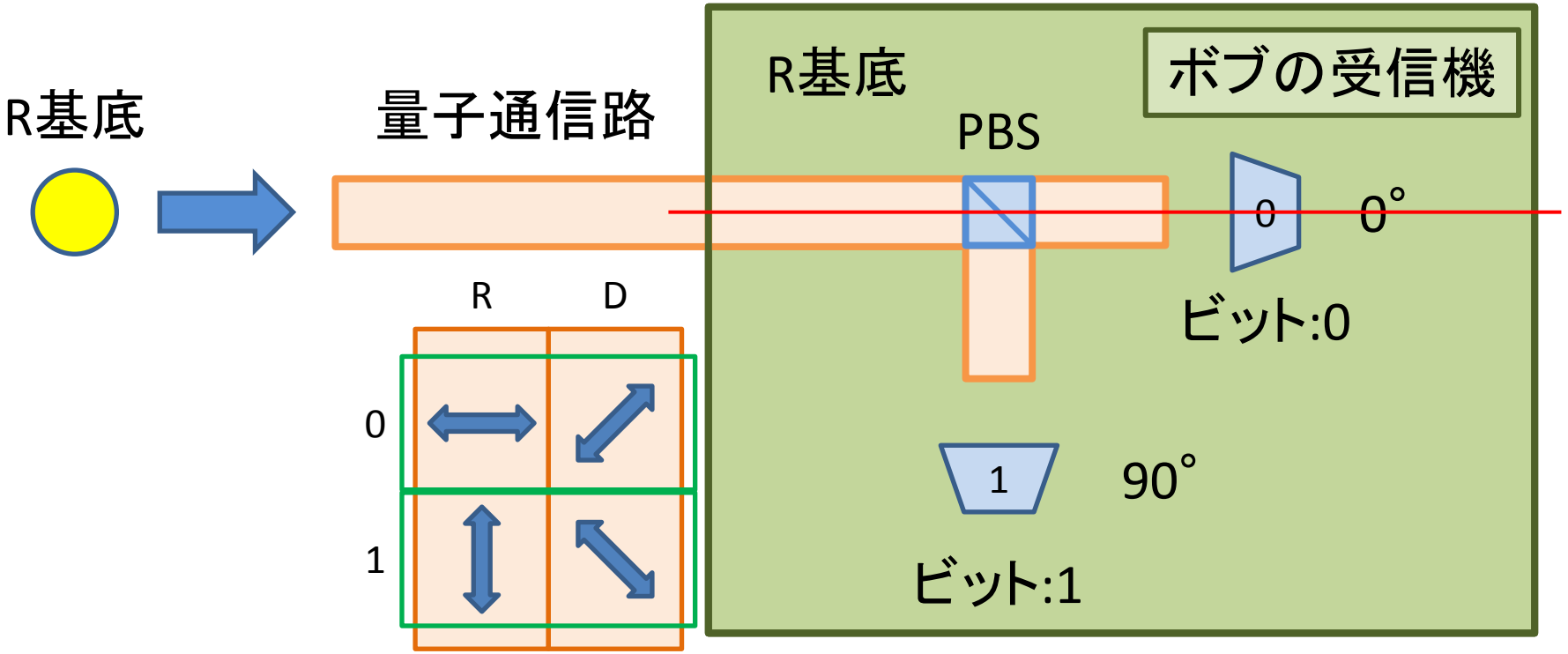
ボブの受信と基底の選択

- ボブの受信機のイメージ
  - 光子がどちらに入るかで光子の持つビットを判断する



ボブの受信と基底の選択

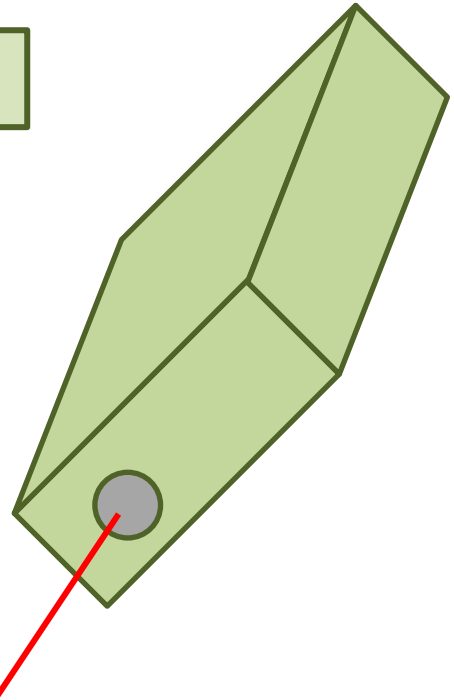
- ボブの受信機のイメージ
  - 二人が同じ基底を選べばビットも一致する
  - 基底の切り替えは受信機を45°傾ける



ボブの受信と基底の選択

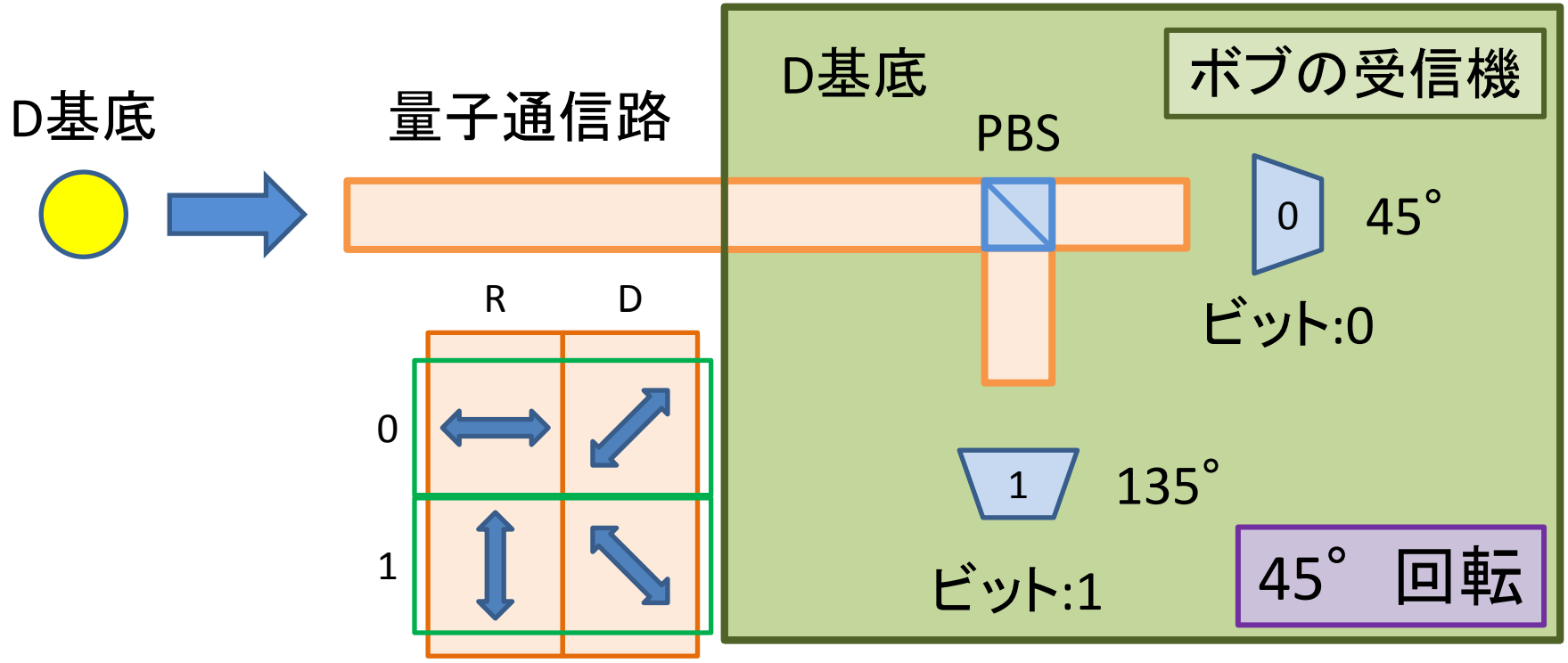
- ボブの受信機のイメージ
  - 受信機を傾けるのはPBSを傾ける意味がある

ボブの受信機



ボブの受信と基底の選択

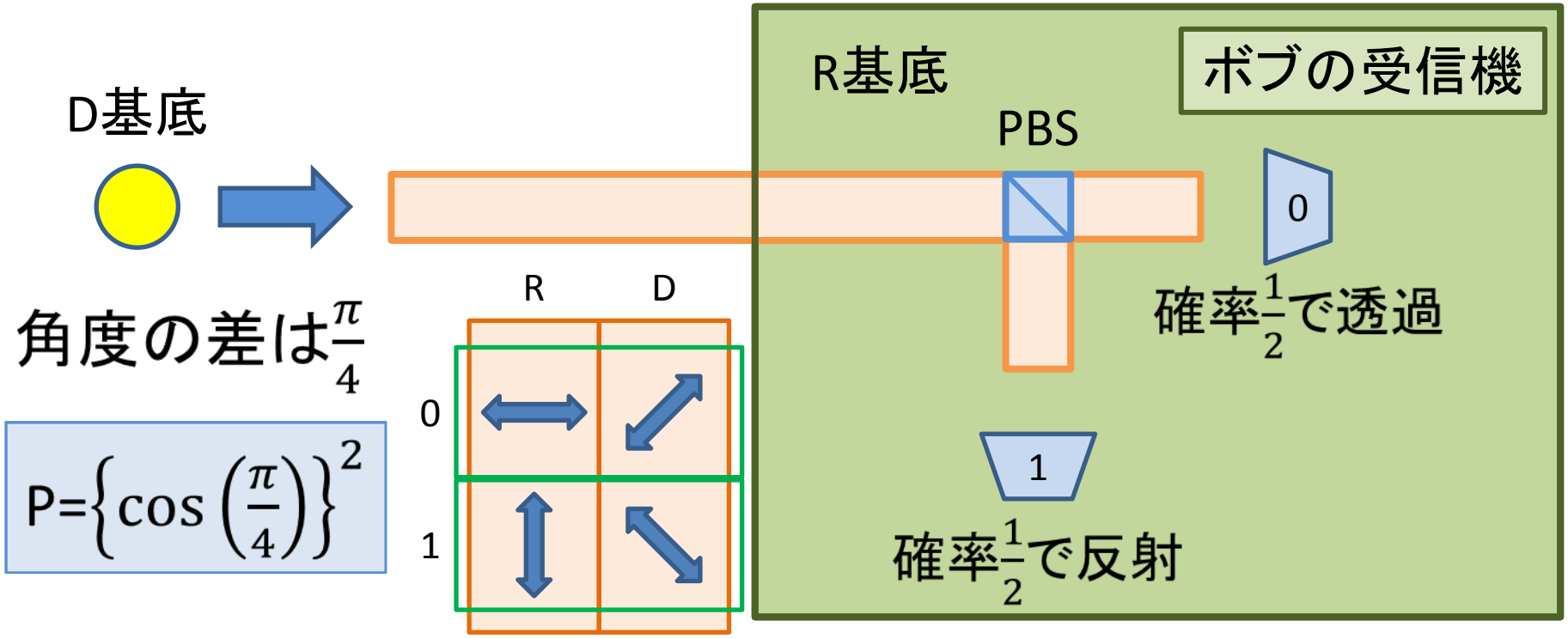
- ボブの受信機のイメージ
  - 傾けたことによりD基底に切り替わった



ボブ側の手順

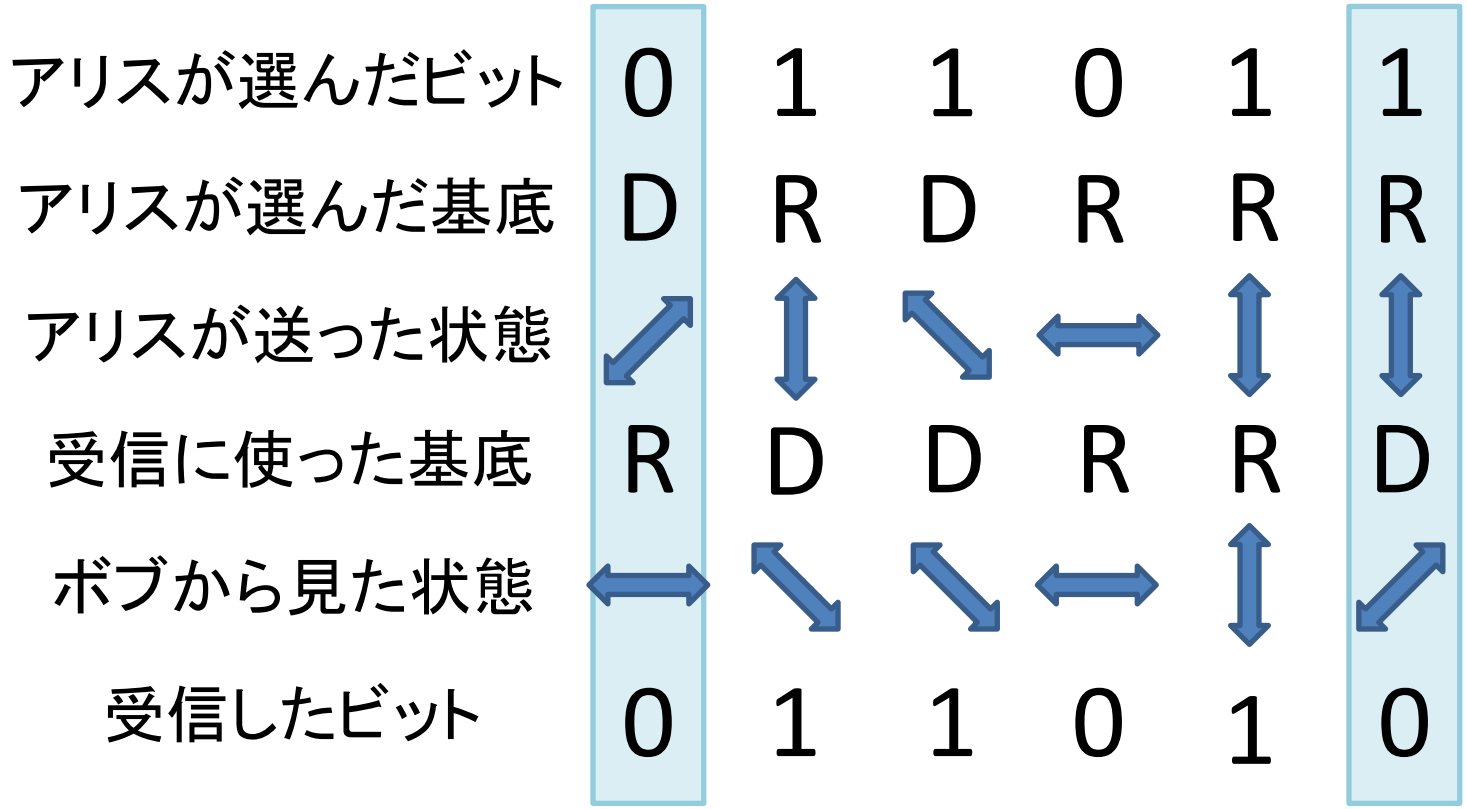
ボブの受信と基底の選択

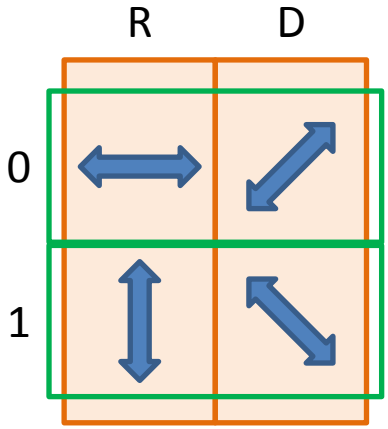
- 二人が選んだ基底が違うと$\frac{1}{2}$の確率でビットが変わる



ボブの受信と基底の選択

- 今までの流れのまとめ

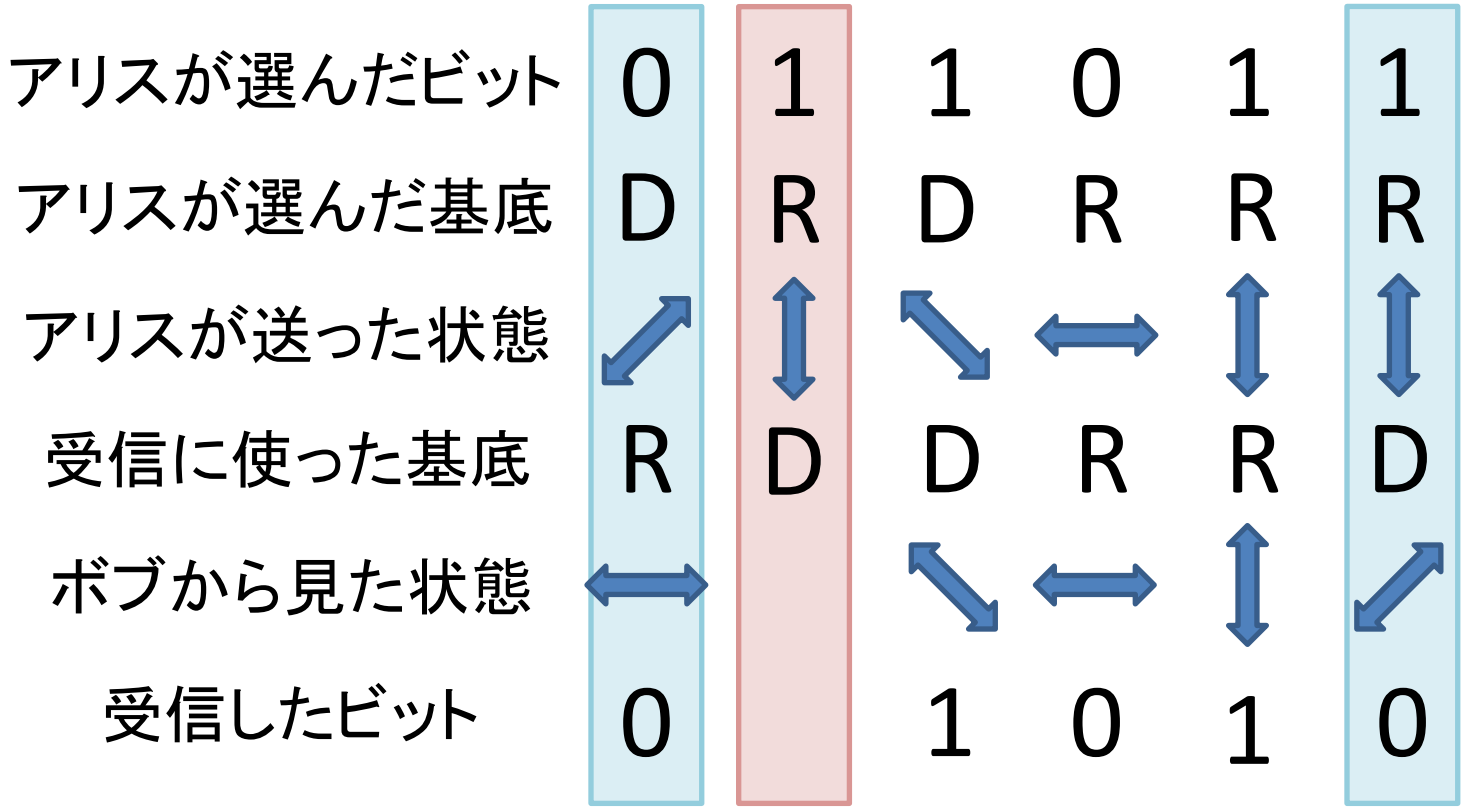


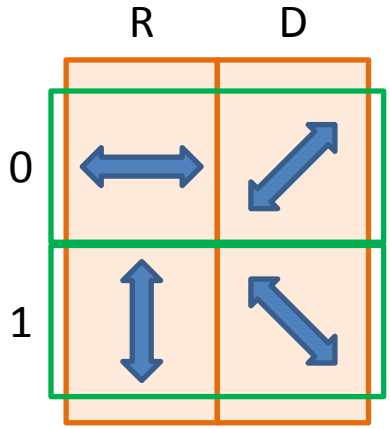


ボブ側の手順

ボブの受信と基底の選択

- 光子そのものが検出できないこともある
  →検出器が見逃す、通信路中で失われる





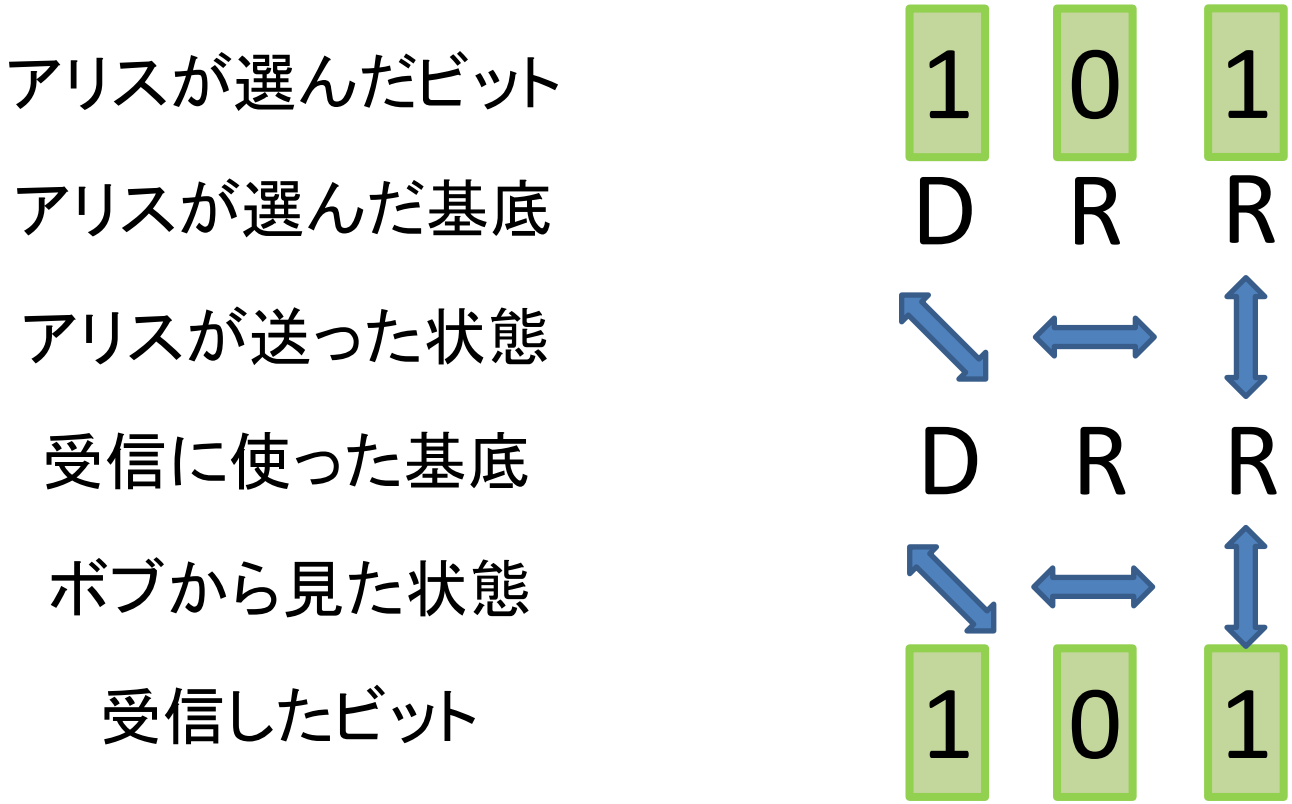
目次

基底の照合

- ボブは受信に使った基底をアリスに報告
  - 報告するのはボブが受信できたもののみ
- アリスは正しい基底で受信された信号をボブに教える
  - ここで基底が違うものは除外

基底の照合

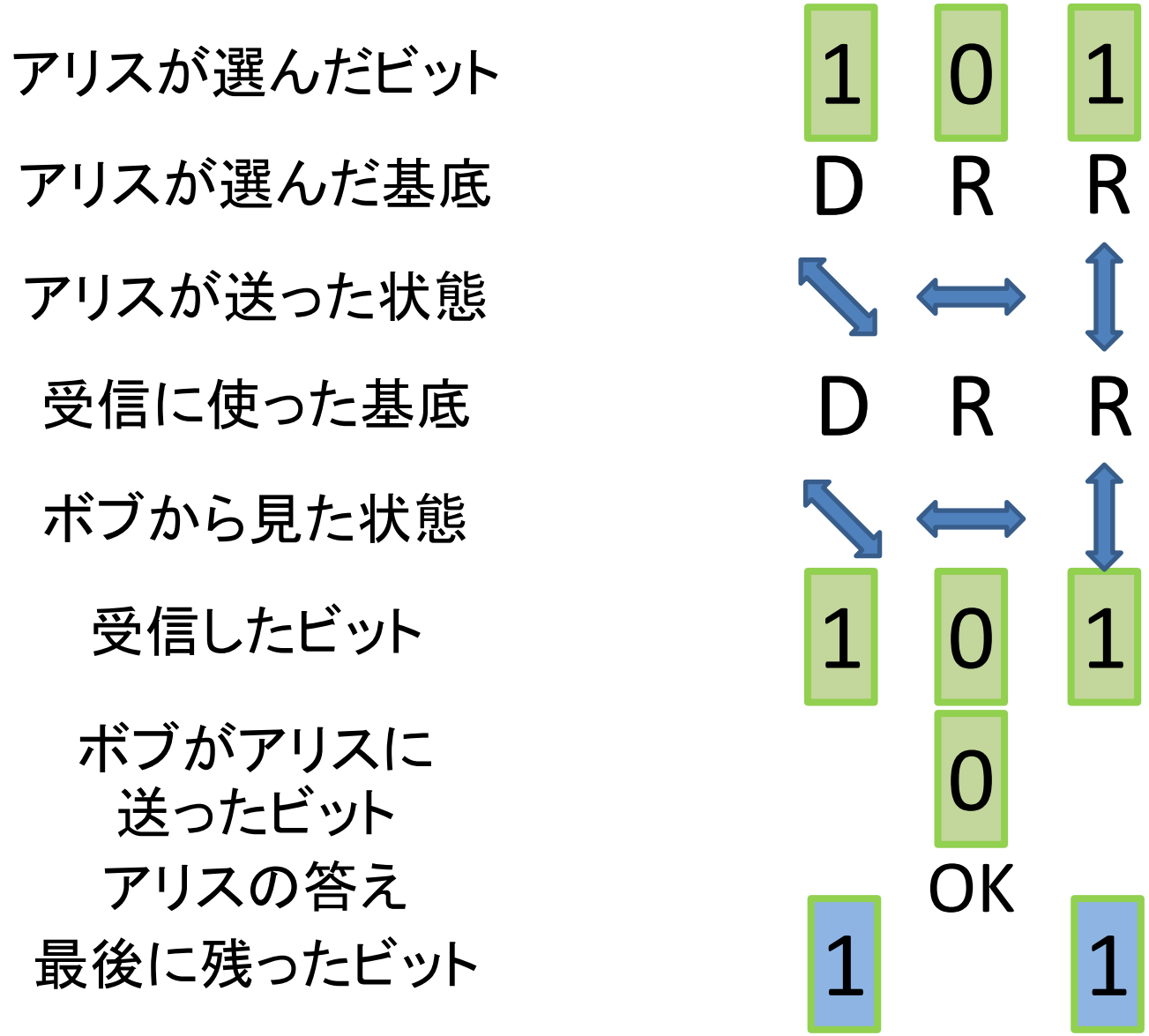
- 生き残ったビット



鍵の照合

- 基底を照合した時点で両者は鍵を共有できたことになる
- しかし、機械の不完全性や盗聴により、鍵の不一致が生じることがある
  - 「基底は同じだがビットは違う」
- よってアリスとボブは鍵の1部を古典通信路上にて照合する
  - 照合に使うビットはランダムに決める
  - 照合につかったビットは破棄する

鍵の照合


アリスが選んだビット
1
0
1
アリスが選んだ基底
D
R
R
アリスが送った状態
受信に使った基底
D
R
R
ボブから見た状態
受信したビット
1
0
1
ボブがアリスに
送ったビット
0
アリスの答え
OK
最後に残ったビット
1
1

結果

- 一致しないビットが多すぎる場合、盗聴者がいると判断して、その量子通信路での通信をあきらめる。
- 一致しないビットが少ない場合、安全が確保されたと判断できる

  →**秘密鍵を共有できる**

まとめ

- 鍵配送の手順(BB84プロトコル)を説明
- 量子系を使ってデジタル情報を送信
  →盗聴を検知できる量子通信路を実現
- 量子、古典通信路の組み合わせ
  →安全に秘密鍵を共有できる
  →共有した秘密鍵を用いた安全な情報通信

以下補足スライド

イブの攻撃

- 基底は同じだがビットは違う