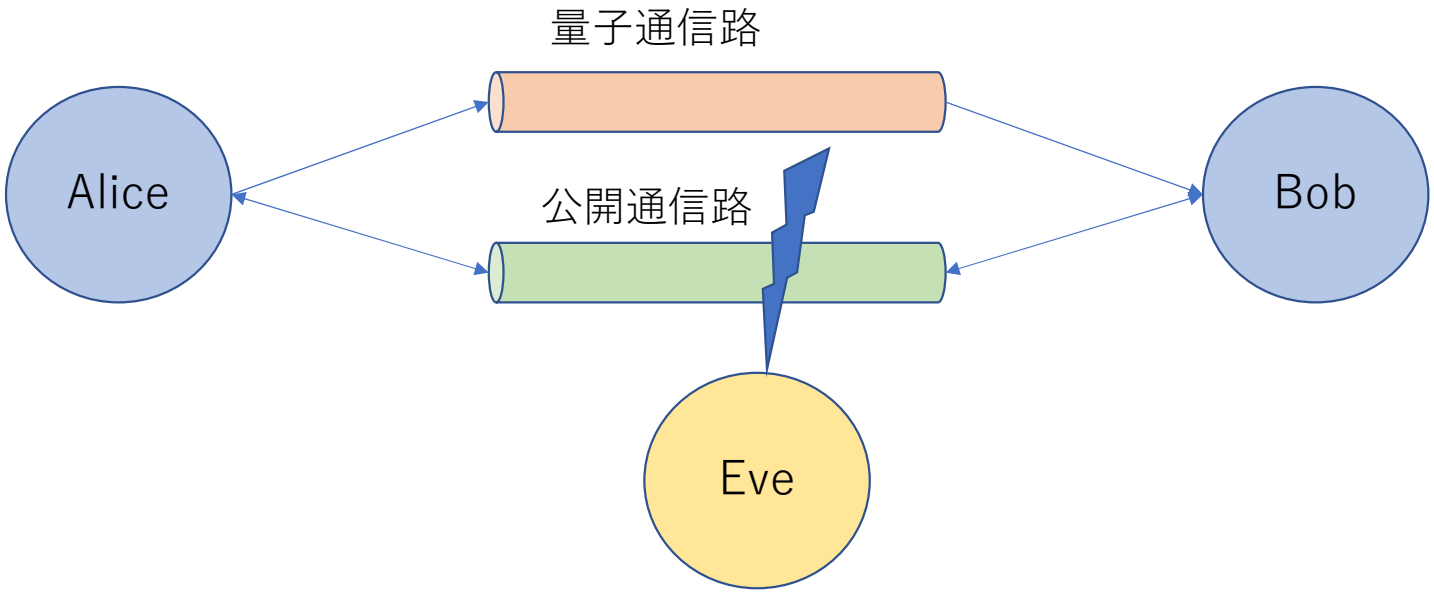
量子鍵配送

量子鍵配送(QKD)とは

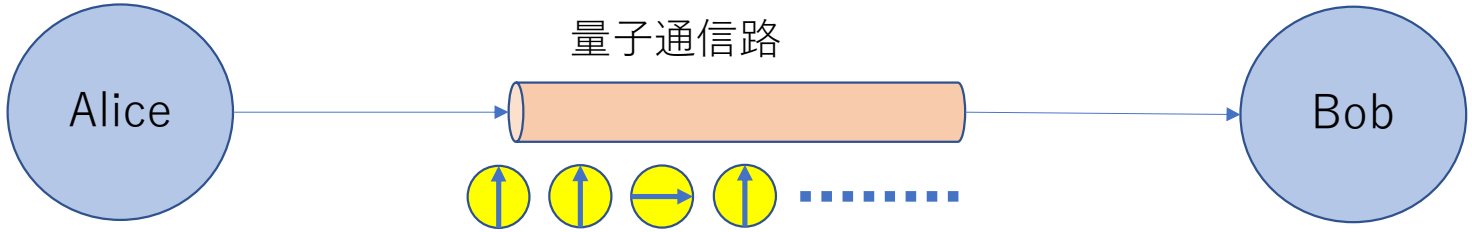
- 量子力学の原理を利用する鍵配送プロトコル
  - 量子の性質（コピーできない、状態を変化させずに観測できない等）を利用し、情報理論的に安全な鍵配送を実現できる
  - DH方式等と異なり計算困難性に依存しないため、コンピュータの高速化や量子コンピュータの実用化によって危殆化するおそれがない
  - [BB84]Bennett and Brassard(1984)、[B92]Bennett(1992)、[E91]Ekert(1991)等、いくつかの方式が提案されている
  - いくつかの企業、研究機関が実証実験を行っており、製品化もされている（日本では、NICTや東芝、NECなど）

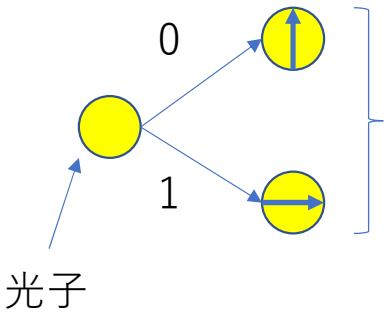
BB84プロトコル

- 最初に提案された量子鍵配送プロトコル
  - 送信者(Alice)と受信者(Bob)間に、量子通信路（専用光ケーブル）と通常の通信路（インターネット等）があるとする。
  - 盗聴者(Eve)は、両方の通信路を好きなだけ盗聴できる

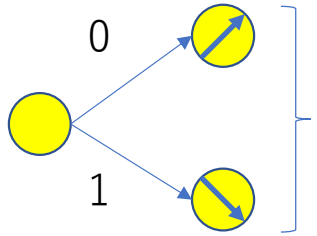


量子光通信

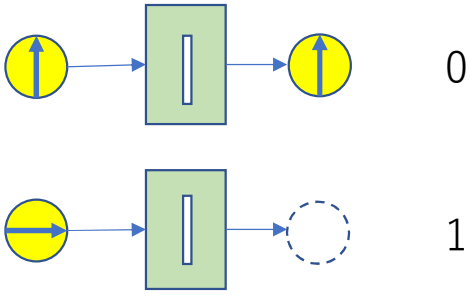


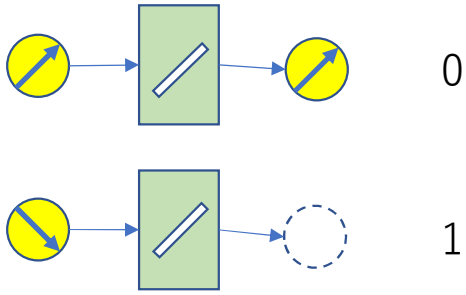


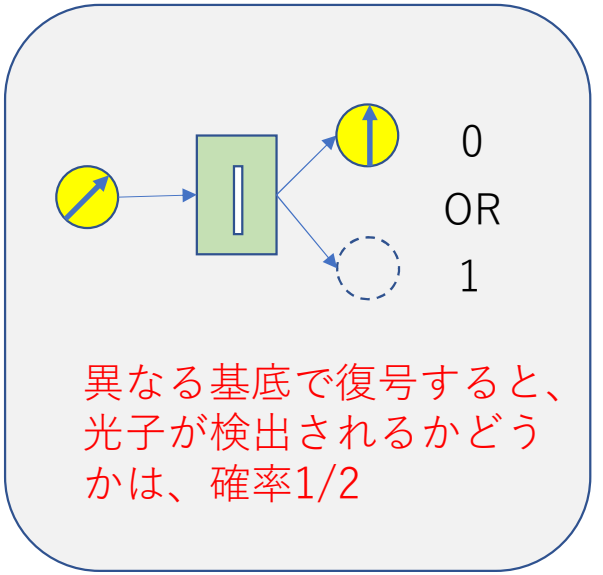
互いに直交する偏光状態



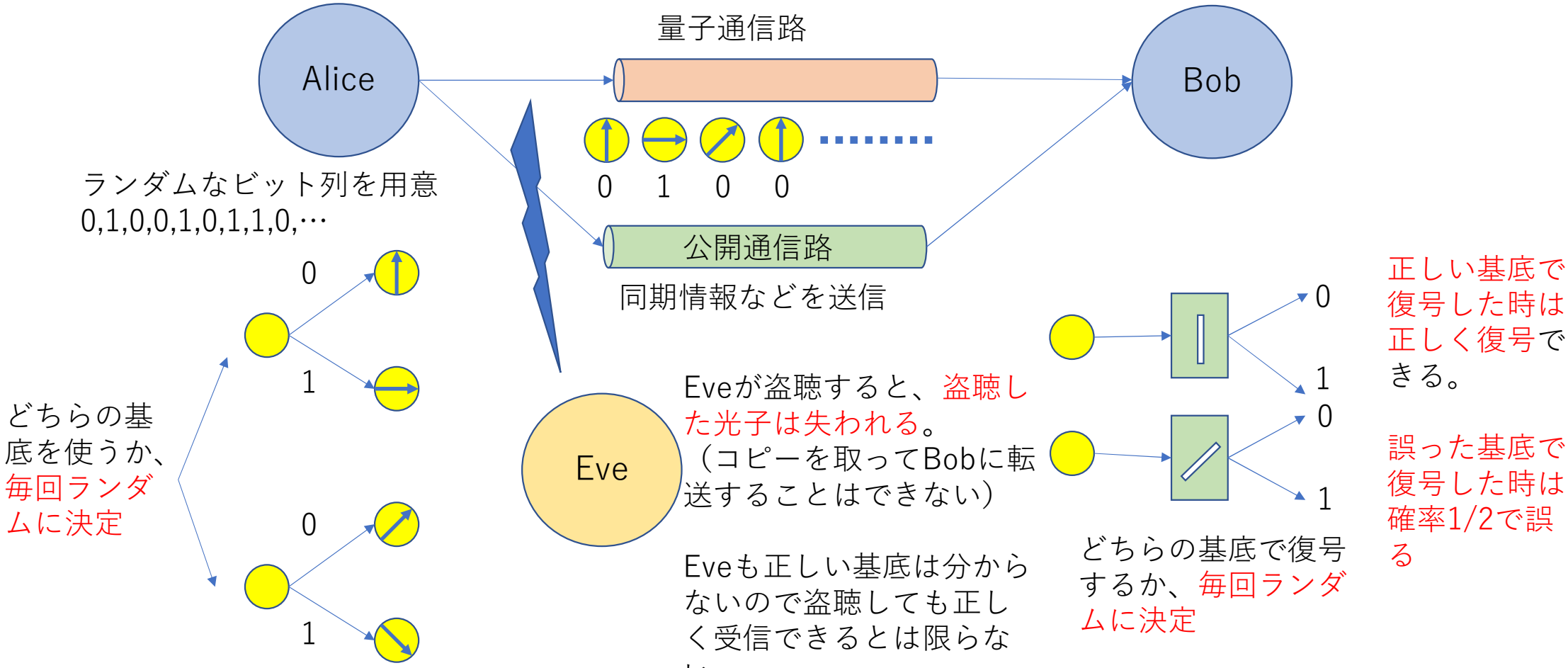
直交していれば他の基底でもOK



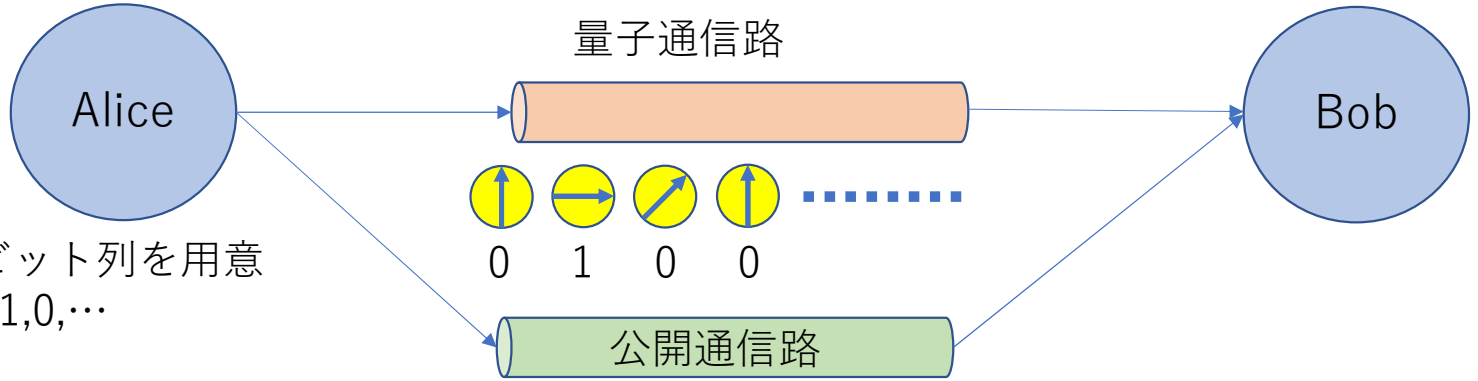




BB84プロトコル（１）


Alice
量子通信路
Bob
0 1 0 0
公開通信路
同期情報などを送信
ランダムなビット列を用意
0,1,0,0,1,0,1,1,0,…
0
1
0
1
どちらの基底を使うか、毎回ランダムに決定
Eve
Eveが盗聴すると、盗聴した光子は失われる。（コピーを取ってBobに転送することはできない）
Eveも正しい基底は分からないので盗聴しても正しく受信できるとは限らない
0
1
0
1
どちらの基底で復号するか、毎回ランダムに決定
正しい基底で復号した時は正しく復号できる。
誤った基底で復号した時は確率1/2で誤る

BB84プロトコル（2）



ランダムなビット列を用意
0,1,0,0,1,0,1,1,0,…

公開通信路で基底の一致/不一致を答え合わせ

送信ビット列	0	1	0	0	1	1	0	1
Aliceの基底	↕	↕	⤡	↕	⤡	⤡	↕	⤡
Bobの基底	↕	⤡	⤡	↕	↕	⤡	⤡	↕
受信ビット列	0	1	0	0	0	1	1	0

基底の一致	○	×	○	○	×	○	×	×
共有ビット列	0	-	0	0	-	1	-	-

基底が一致した箇所だけを共有ビット列として残す

基底が一致しなかった場合は、0と1を確率1/2で受信

ノイズや盗聴者の影響により、基底が一致していてもエラーが生じる

BB84プロトコル（３）

- 送受信者間で基底が一致していても共有ビットが食い違うことがある
  - 通信路のノイズによるエラー
  - 盗聴者の存在（盗聴者は光子の状態をコピーできないので、盗聴者を経由して送られた光子は1/2の確率でエラーになる）
- 共有ビット列に対して公開通信路を介してパリティ情報を交換することにより誤り訂正を行う
  - 訂正したビット数から盗聴者の有無（どのくらいの情報が漏洩したか）が推定できる
- 漏洩した分の情報を圧縮して安全性を高める（秘匿性増強）

量子鍵配送の利点と今後の課題

- 量子鍵配送により、共有したビット列を用いてワンタイムパッド暗号化（平文系列に共有した鍵系列を加えて（排他的論理和）暗号化）することにより、情報理論的に安全な通信が可能
- 鍵の共有速度が遅いので、高速、大容量通信には不向き（共有した鍵系列を種にして一般的な共通鍵暗号の鍵を作れば解決できるが、情報理論的に安全とはいえなくなる）
- 実現のためには、専用の光回線が必要
- 長距離の伝送（数十Km～）はできないので中継点が必要になるが、中継点のセキュリティに留意する必要がある