井上研究室の紹介

研究題目:

量子暗号

光伝送システム(特に光信号再生)

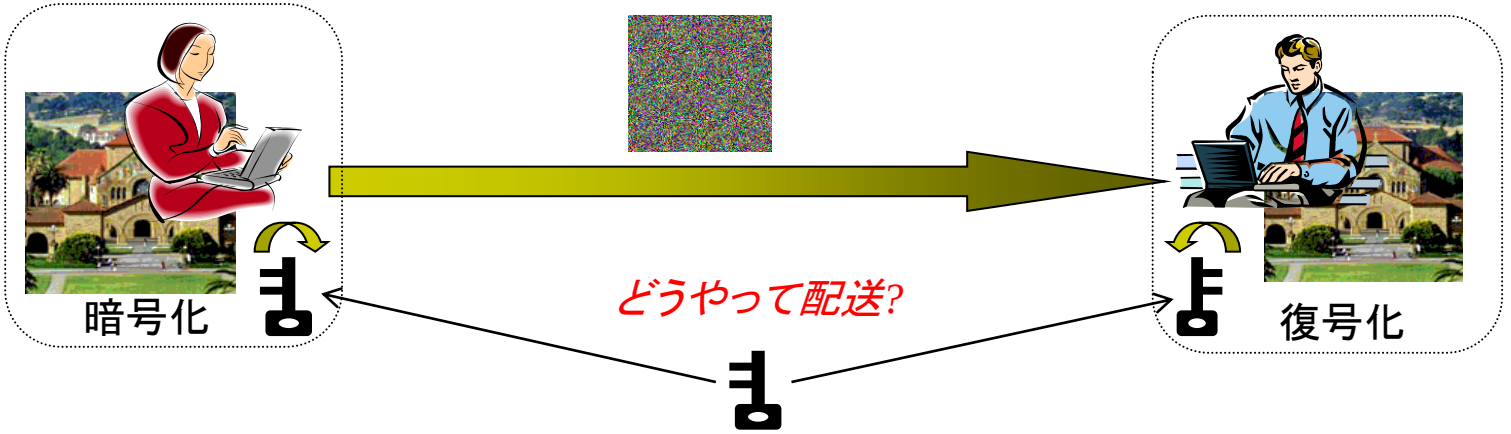
量子暗号

秘匿通信では、秘密鍵によってデータを暗号化/復号化する

◆現行システムは公開鍵によって暗号化、秘密鍵によって復号

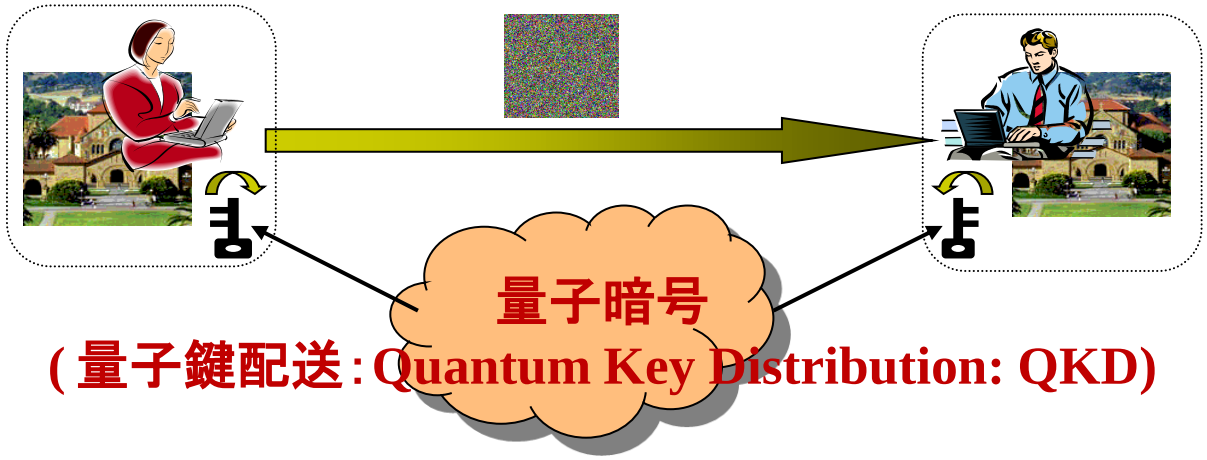
安全性は、公開鍵による解読には莫大な計算量がかかることに基づくが、
原理的には盗聴可能

◆暗号化と復号化の両方に秘密鍵を用いるシステムは絶対に安全
ただし、いかに離れた二者に安全に秘密鍵を供給するかが課題



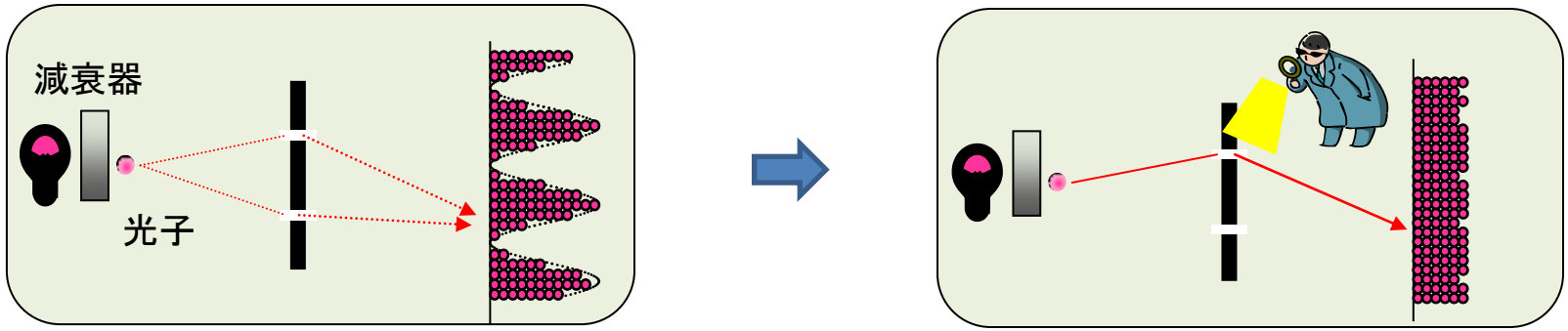
量子暗号は、暗号化/復号化のための秘密鍵を供給するシステム。

システムの安全性は量子力学に基づく。→原理的に安全



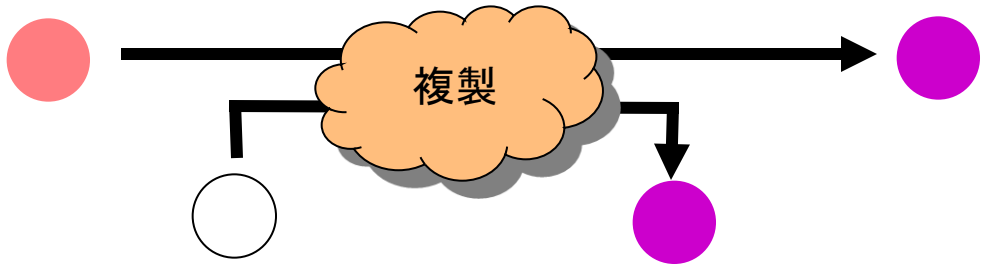
量子力学の基本定理

重ね合わせ: 量子システムは重ね合わせ状態である
重ね合わせ状態は観測されると崩壊する



不確定性原理: 共役二つの物理量は正確には測定できない

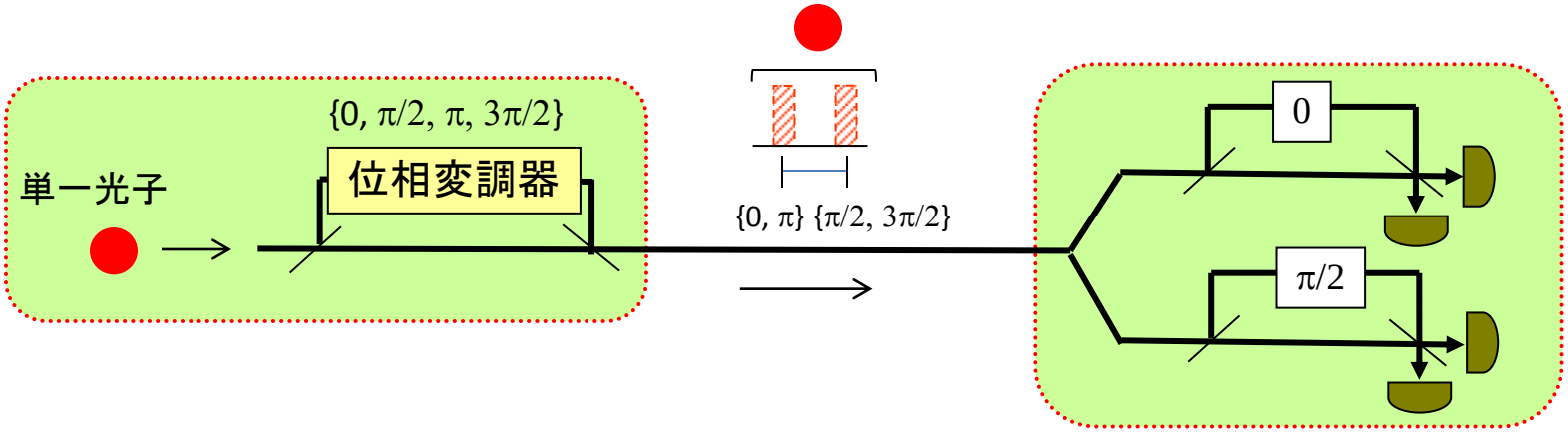
複製不可定理: いかなる量子状態も攪乱なしではコピーできない



QKDプロトコル

QKDには様々なプロトコルがある; BB84, B92, E91, BBM92, *DPS-QKD*, etc.

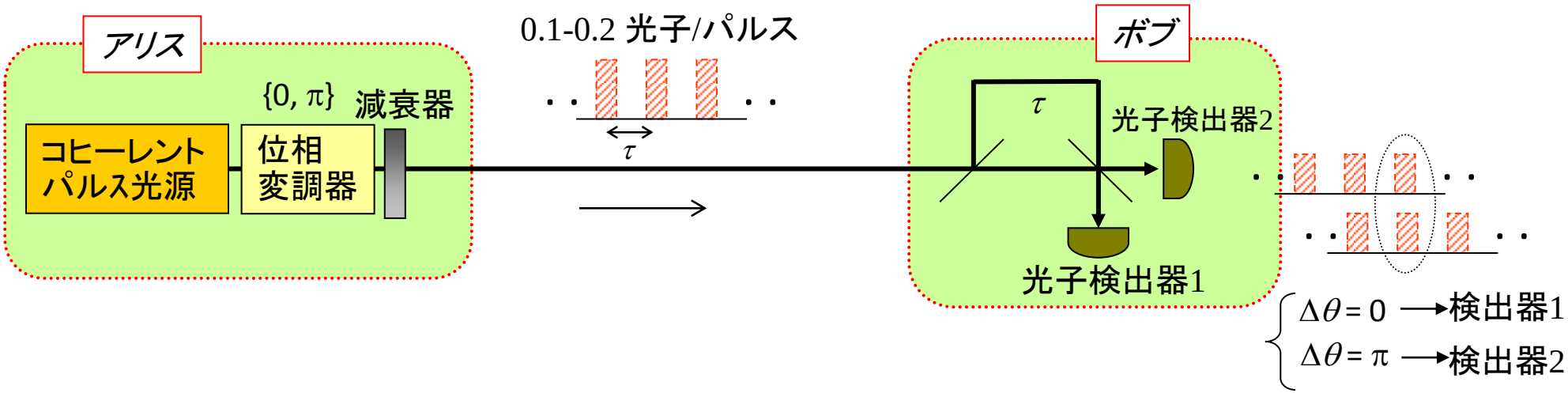
位相エンコードBB84



BBM92

DPS (Differential-Phase-Shift) QKD

井上研オリジナルプロトコル



手順

(1) 光子伝送を行う。この際、光子は時々かつランダムに検出される

(2) 光子伝送後、ボブはアリスに光子検出時刻を通知する

(3) アリスは、検出時刻情報と自分の変調データから、どちらの検出器で光子を検出したかを知る

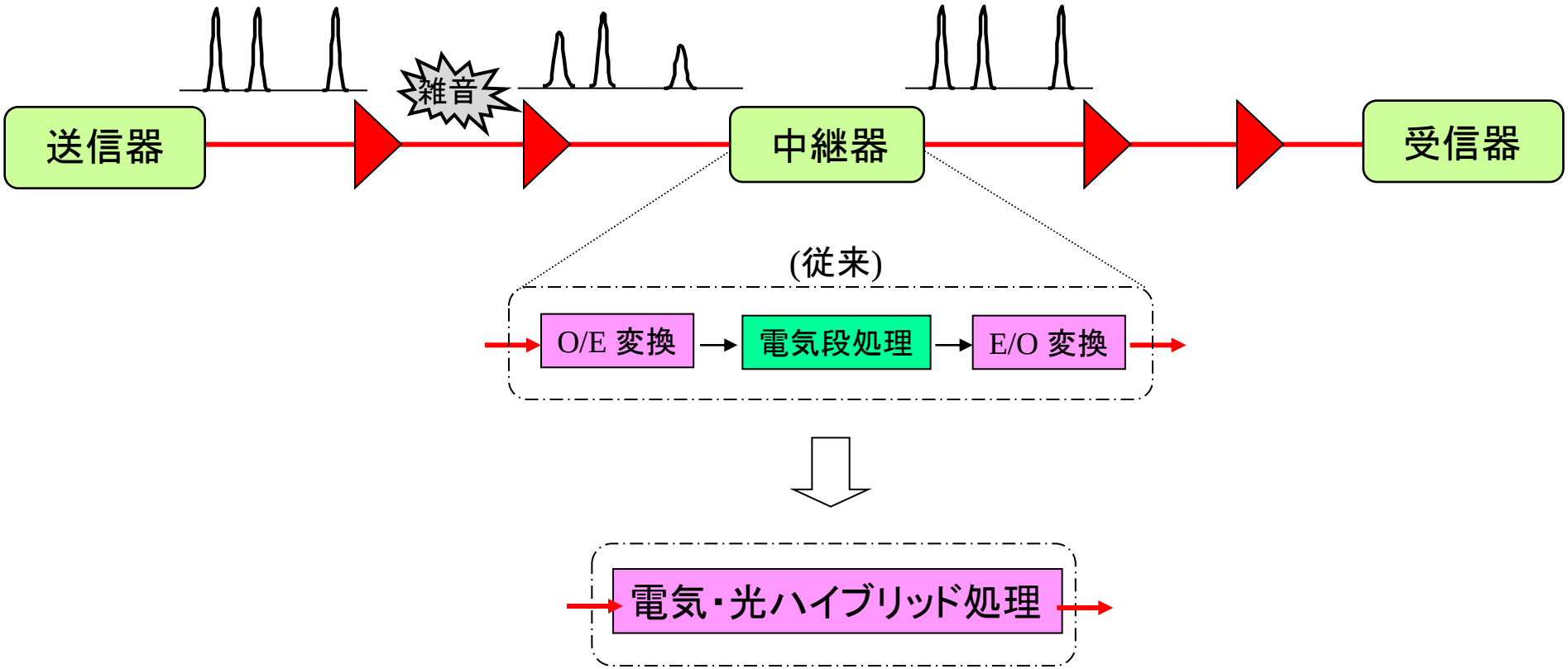
(4) 検出器1での検出をビット0、検出器2での検出をビット1とすると、アリスとボブは同一のビットを共有する

秘密鍵

特徴

- 簡便な構成
- 時間領域の効率的利用
- 光子数分割攻撃に対して頑強

光信号再生



フィードフォワード型強度再生器