実験物理屋がどのように物理研究を行っているか

堀切　智之
国立情報学研究所 (NII), 東京大学
tomoyuki-horikiri@nii.ac.jp

自己紹介

- 2002-2007　東大理学系研究科物理学専攻　小林孝嘉研究室
  大学院に進んだ動機：量子コンピュータを作りたい

  博士研究：量子鍵配送のSPDCと光子数識別器による秘密鍵生成率向上

- 2007-　国立情報学研究所、スタンフォード大学　山本研
  2007-2008　Si結晶中不純物P束縛励起子線の分光実験（目標：量子メモリーのためのP核スピンの超微細構造による分光読み出し）
  2008-　半導体マイクロ共振器量子井戸構造における励起子ポラリトン凝縮の研究

- 2011-　東大光量子科学センター五神研究室に
  山本グループ実験室を立ち上げ。

Outline

1. 実験：ある量子光学の実験屋が、普段どんな事を、どんな装置で、どういう風に研究しているか

2. 特殊？な例：量子情報

量子暗号（量子鍵配送）の

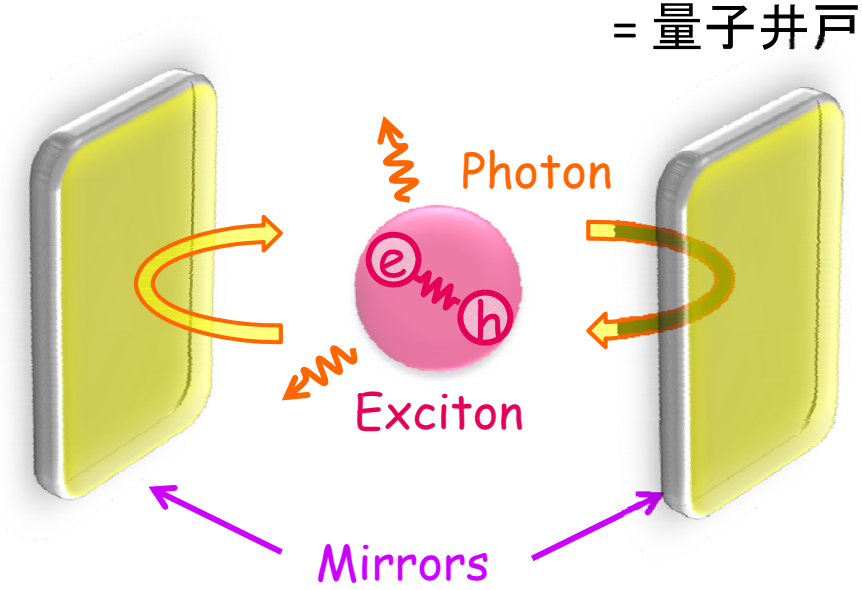
研究を例にして

1. 実験
現在のテーマ：励起子ポラリトン凝縮の研究

ポラリトン(polariton)　= polarization + photon

半導体量子井戸マイクロ共振器系

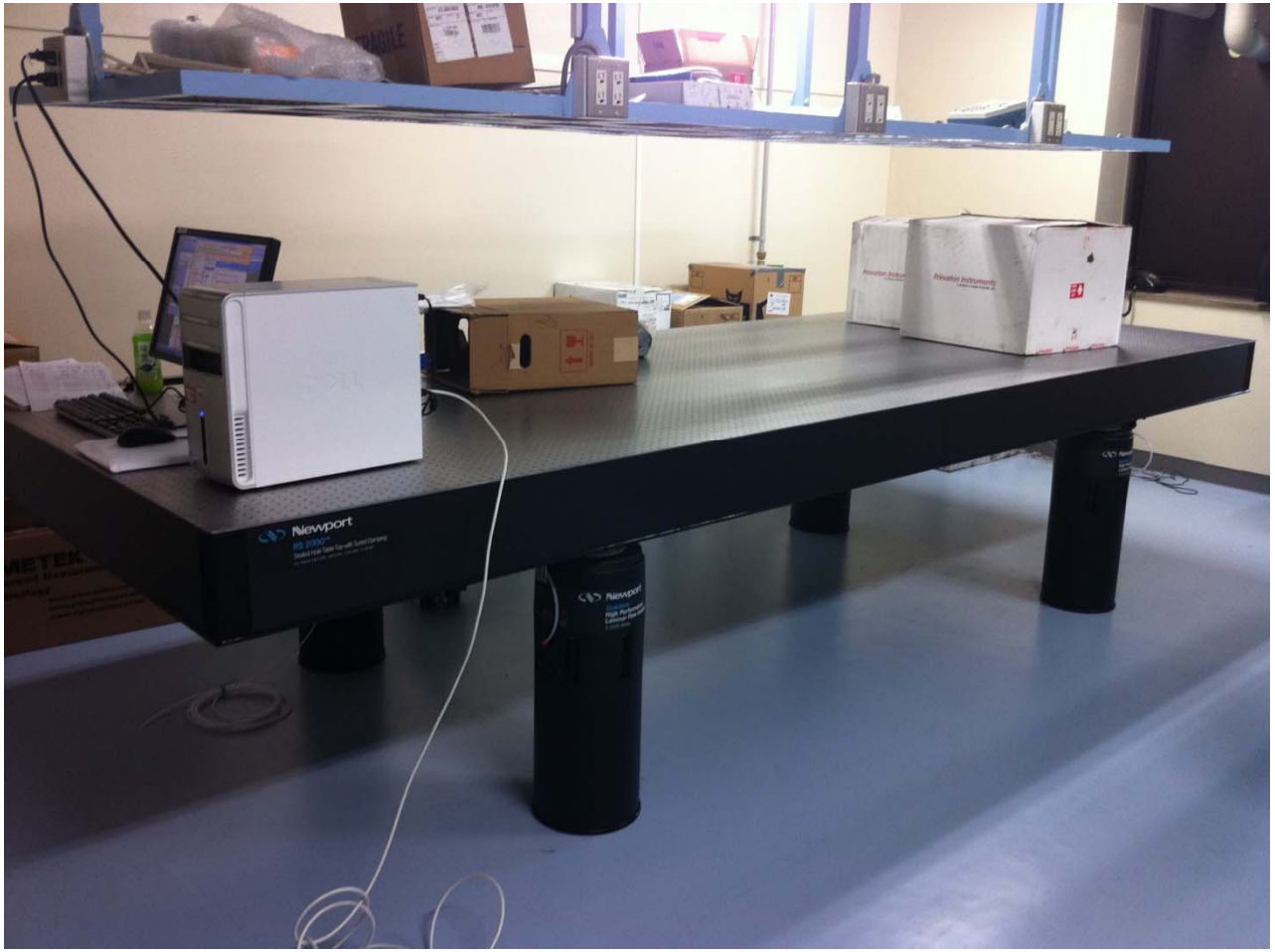
= 量子井戸励起子+ マイクロ共振器光子



共振器光と共鳴する励起子との間で
コヒーレントなエネルギーのやりとりが
行われている強結合状態➔
準粒子：ポラリトン

実験室

光学テーブル：この上にレーザー、光学素子（ミラー、BSなど）、
分光器など様々な機器を載せて実験を行う。
多くの光学テーブルには除振機能がついている
実験機材がほとんど納入されていない2011年5月16日。

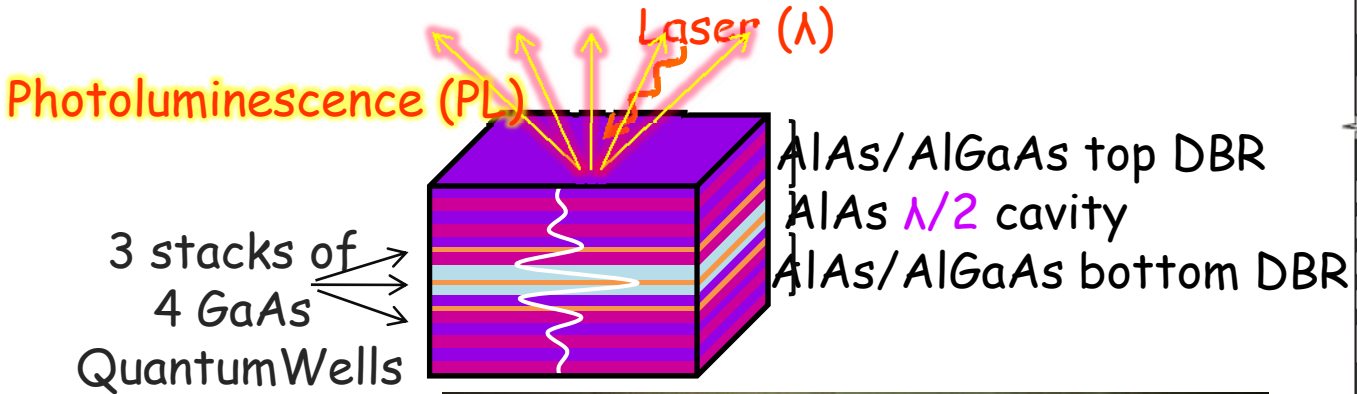


実験系

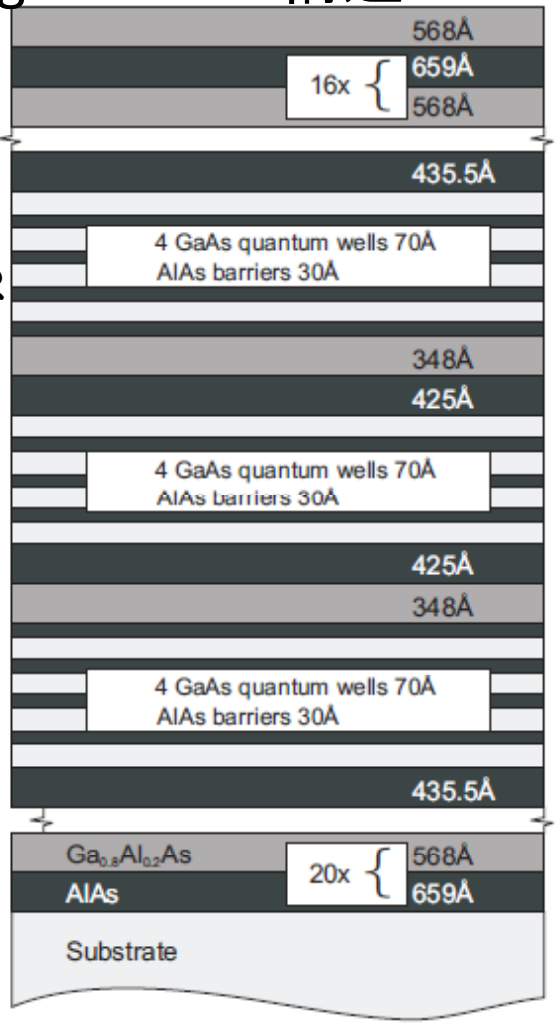
サンプル

ガリウム砒素GaAs 量子井戸(QW)

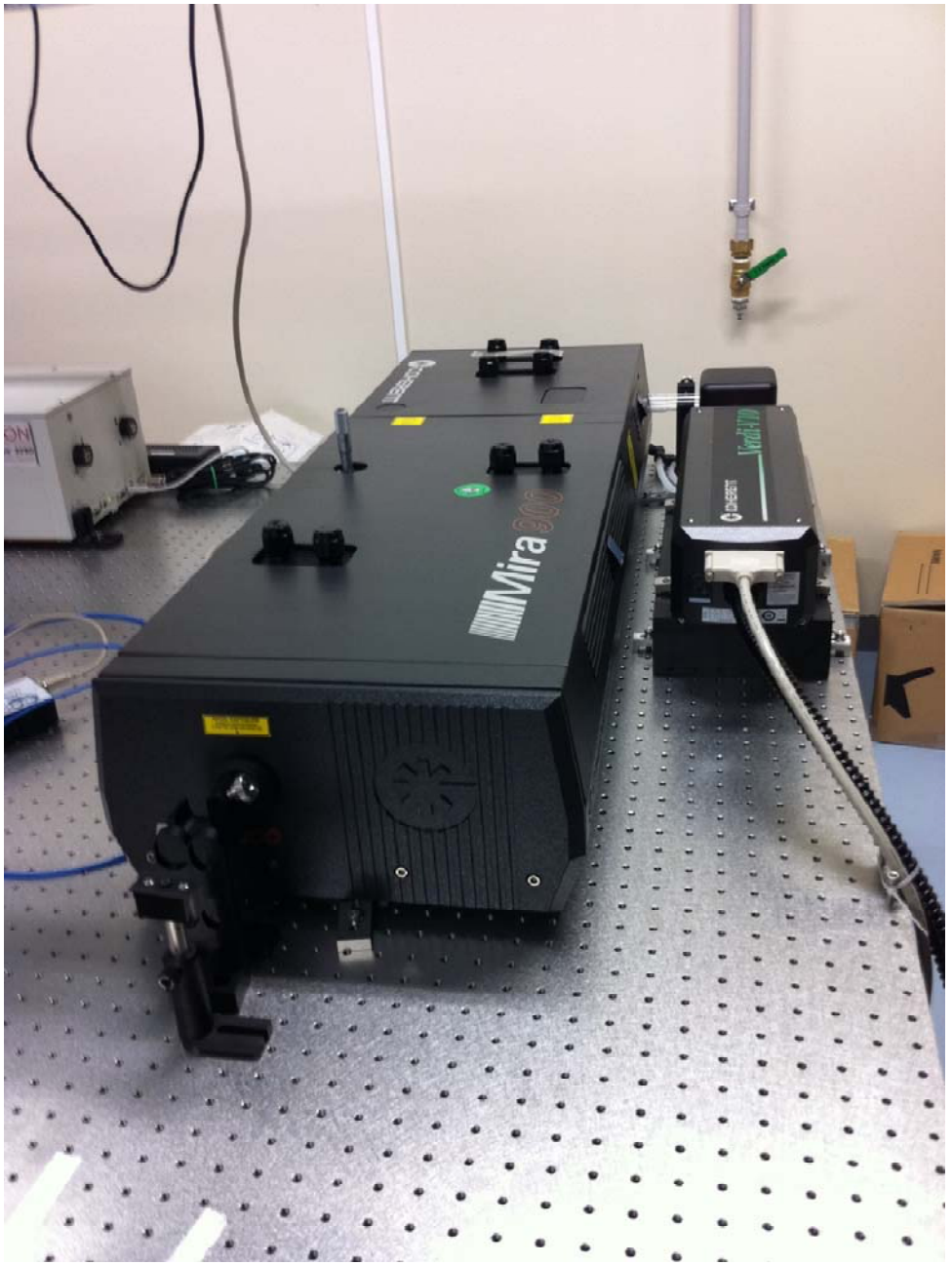
マイクロ共振器：AlAs/AlGaAs distributed Bragg reflector 構造



サンプル写真

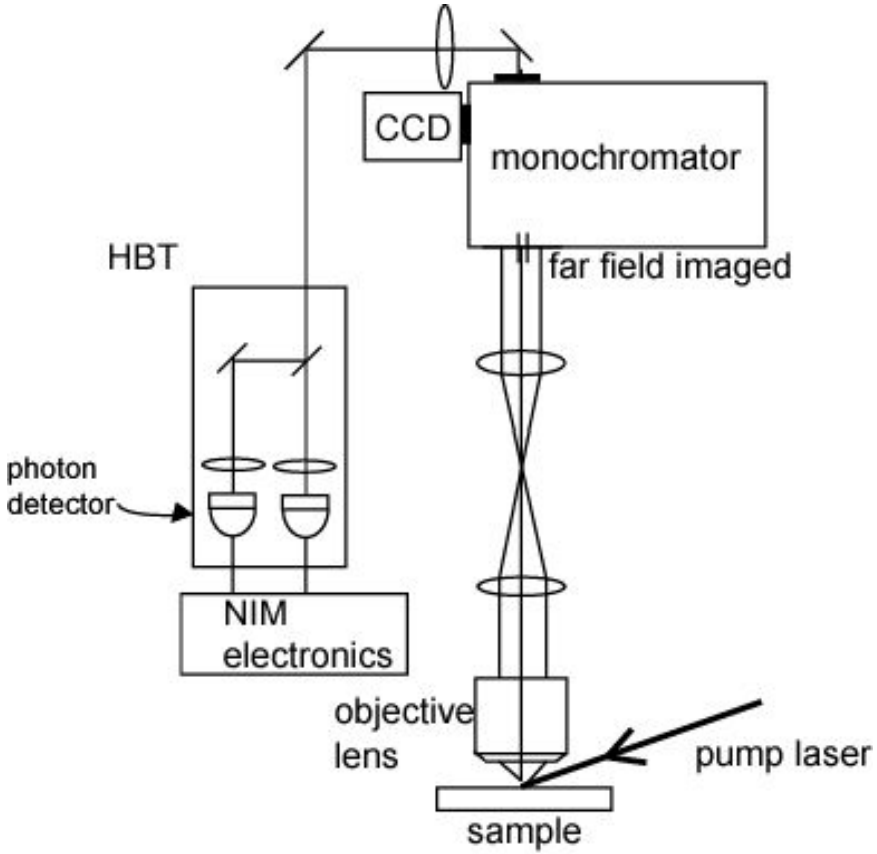


レーザー



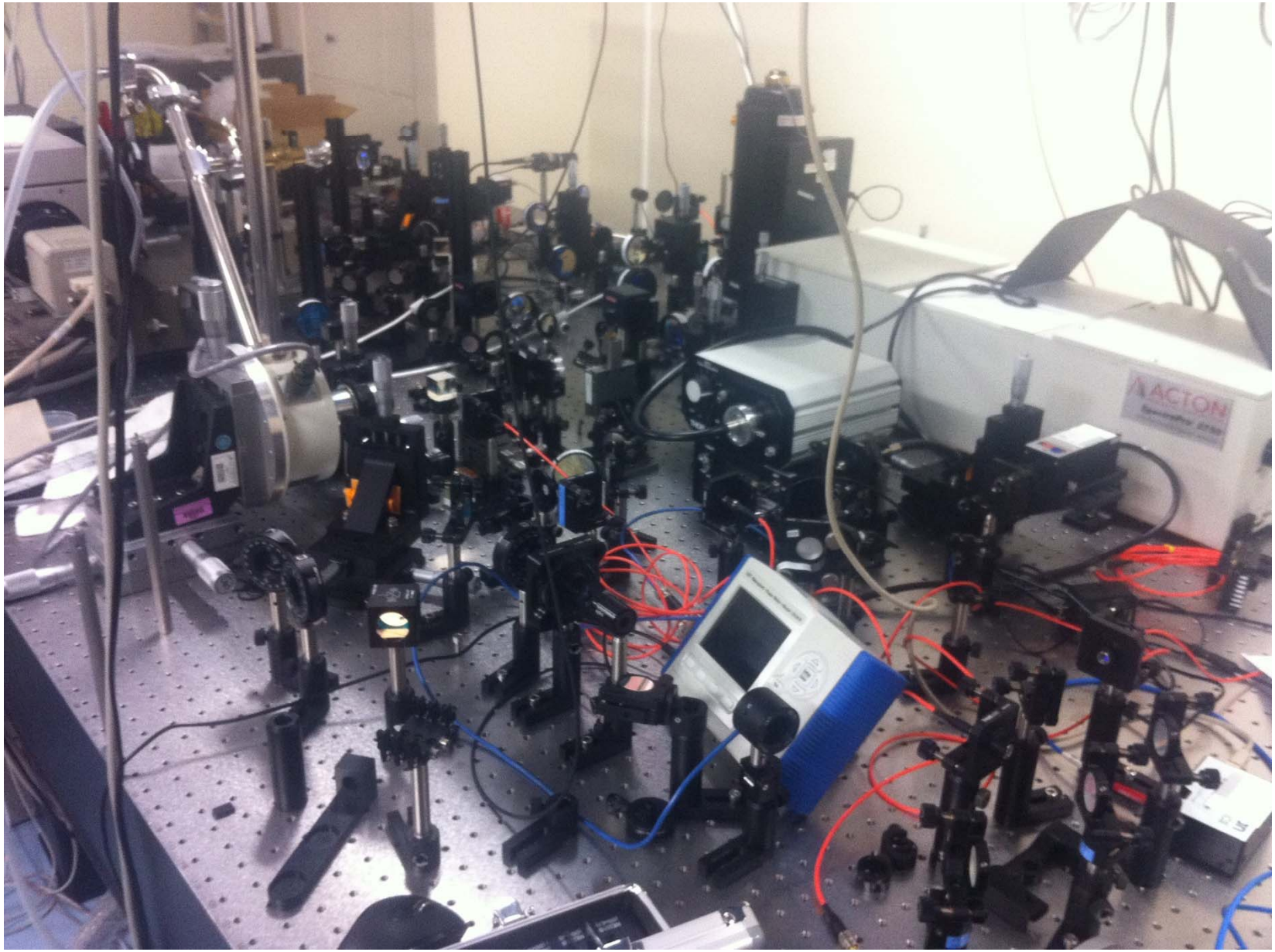
Coherent社　verdi 10 (10W, 532nm)
MIRA (Ti:S laser, 3ps pulse laser)

光学測定系
概略図



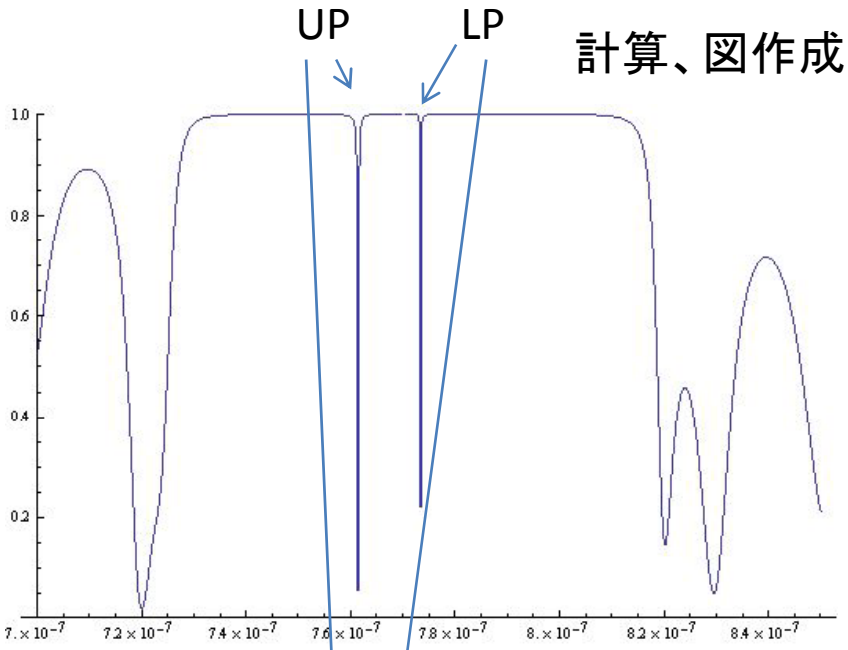
クライオスタット
(サンプル冷却用)

光学テーブル上の光学系



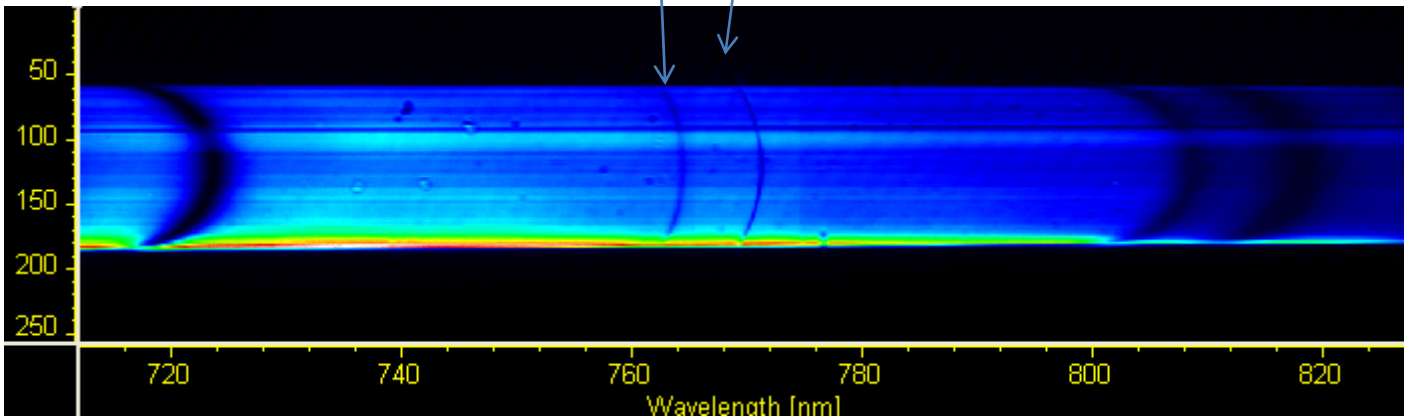
測定例：DBR構造サンプルによる反射率の変調

マイクロ共振器量子井戸サンプル
の反射率計算(k=0)

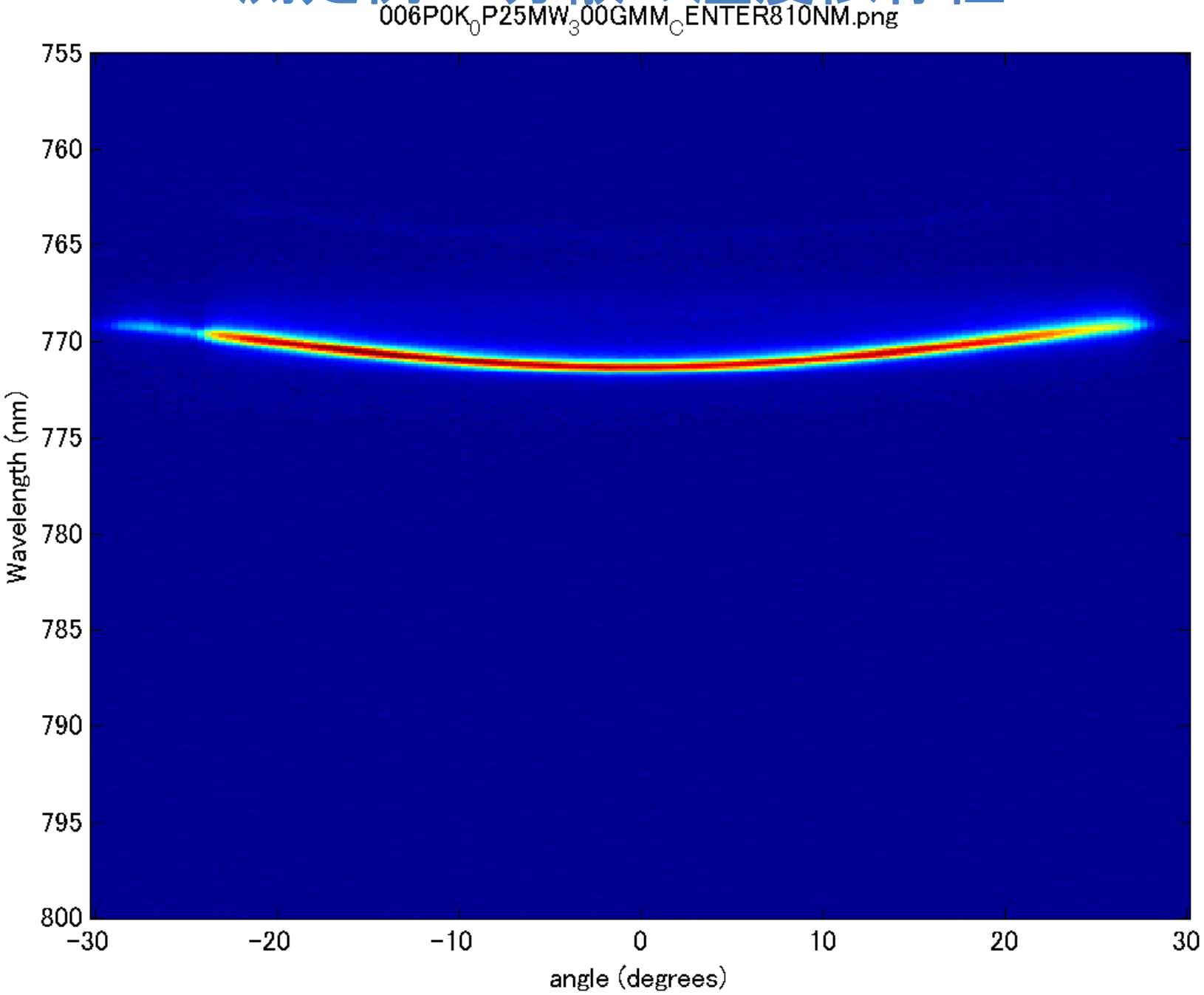


計算、図作成：松尾康弘

白色光による
反射率測定結果
縦軸：k

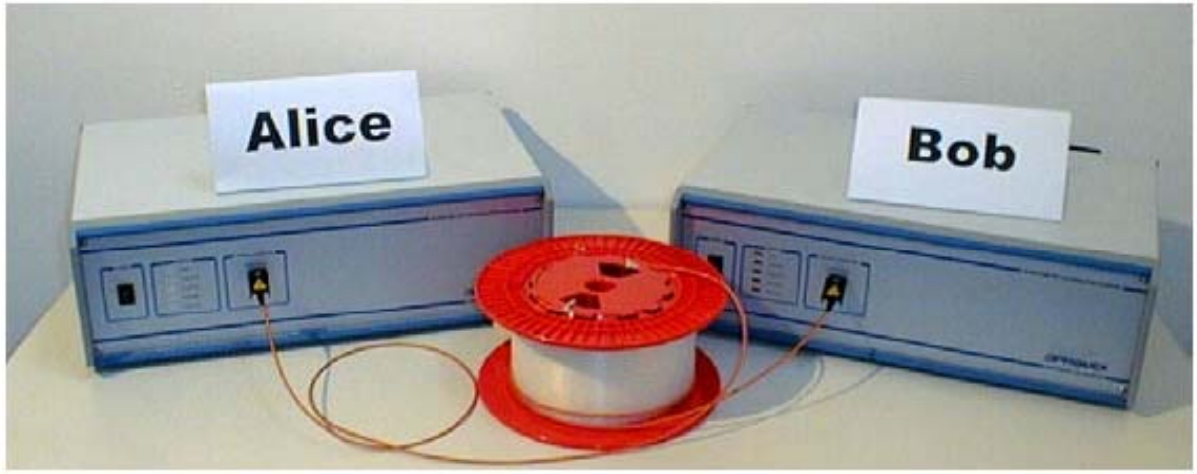


測定例2：分散の温度依存性



2：量子情報
例：量子暗号（量子鍵配送）

- 離れた場所の2人(Alice, Bob)が安全に情報伝達を行うため秘密鍵を共有したい。
- 鍵 = ランダムビット列(1011100…)
- 利点：絶対的な安全性が得られる
- 様々なプロトコルが提案され,多くの実験が行われており、販売されている量子鍵配送システムもある。



Clavis , id-Quantique社

量子鍵配送：
量子性を用いた特殊な応用技術

現在では多くの鍵配送の方法（プロトコル）が存在するが、
原点はBB84プロトコル（Bennett,Brassard）

1光子に1ビット符号化➔受信者に送信。
符号化には2組の符号用グループのどちらか用いる
例：偏光符号化　　直線{0=H(水平),1=V(鉛直)},
　　円 {0=L(左円),1=R(右円)}
その後で、どのグループを各ビットに用いたか
古典通信で教え合う。➔暗号鍵の生成

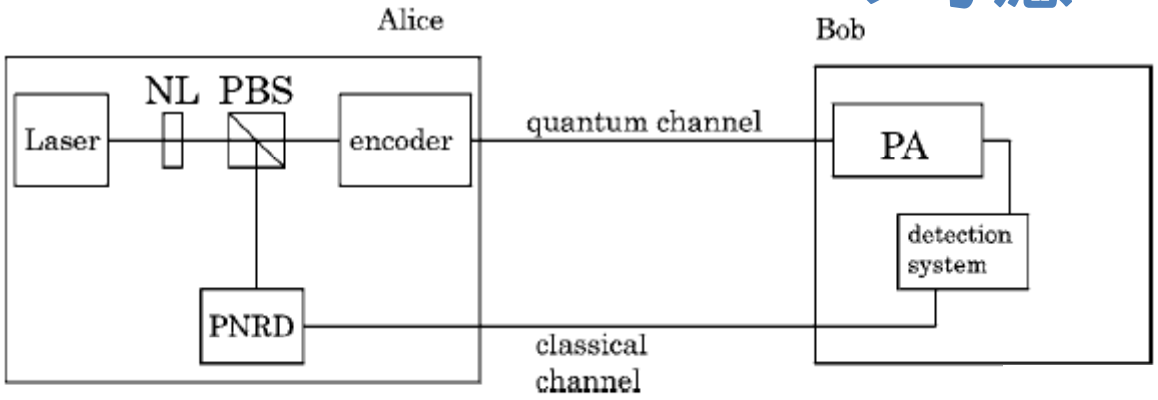
BB84を始めとする量子鍵配送プロトコルは
理想的な状況（光子透過率＝１、検出確率＝１、１光子確率＝１）での安全性を保証する。
⇒通信路中での損失（透過率<1）
　検出器の非効率（検出確率<1）
　光源からの複数光子確率（1光子確率<1, 複数光子確率>0)
といった**実際の状況下での安全性は自明ではない**。
⇒盗聴者の能力を仮定した上で、
　　（かなり強力な盗聴能力でも）安全性証明がなされている。

盗聴攻撃の例：photon number splitting attack
１．あるビット情報が複数の光子に対して符号化されてしまう
２．（原理的に）盗聴者はその内の1つを自分で保持し残りを受信者に送る事ができる
３．送信者が受信者に用いた基底情報を聞いた後なら、
盗聴者は100%の確率で正しいビット値を得られる。

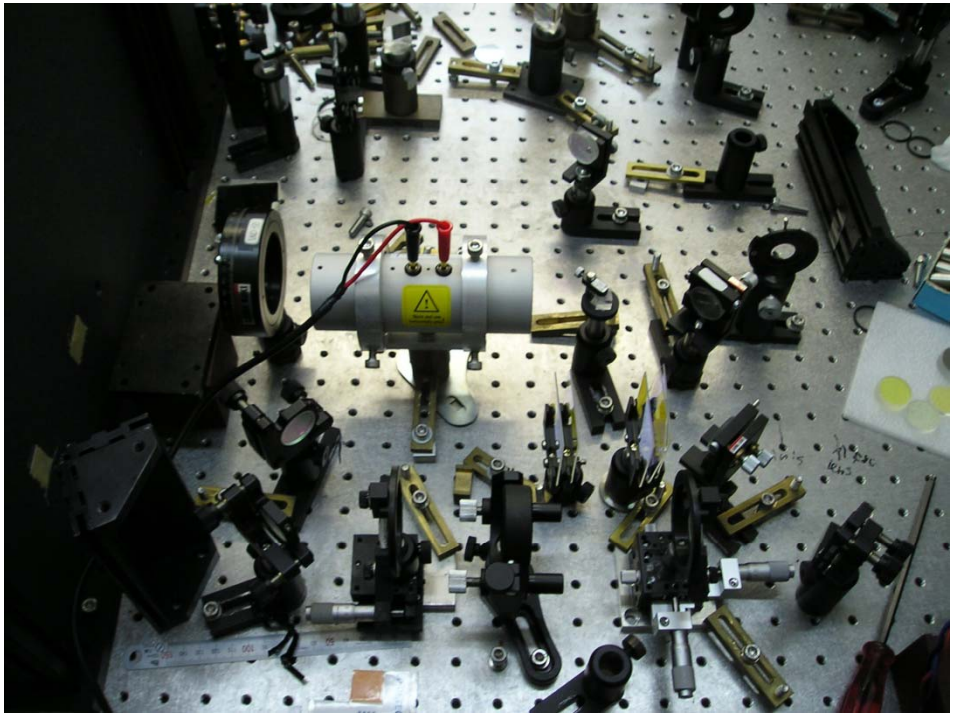
⇒**現在使用できる光源**では複数光子を除去しきれない

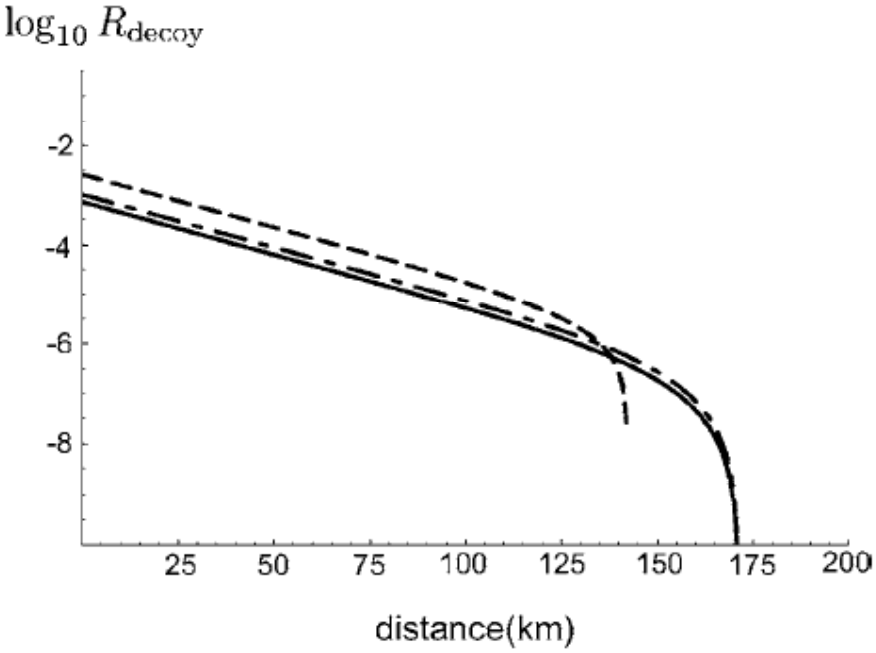
博士研究では、複数光子確率を減らすシステムの考案と実証実験を行った。

研究立案と実施：分野現況と自分に出来る事の考慮



自分の考える量子鍵配送のスキーム提案

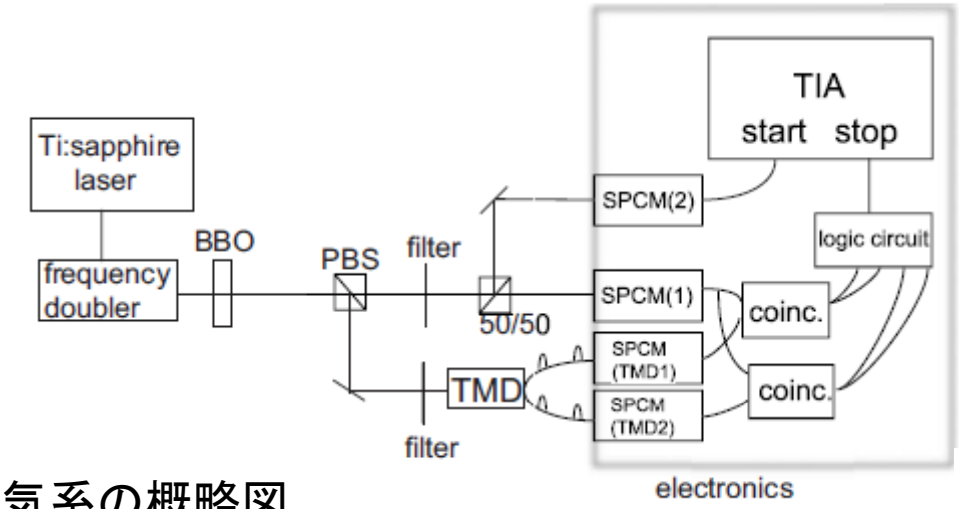




秘密鍵生成率の向上を計算により示す

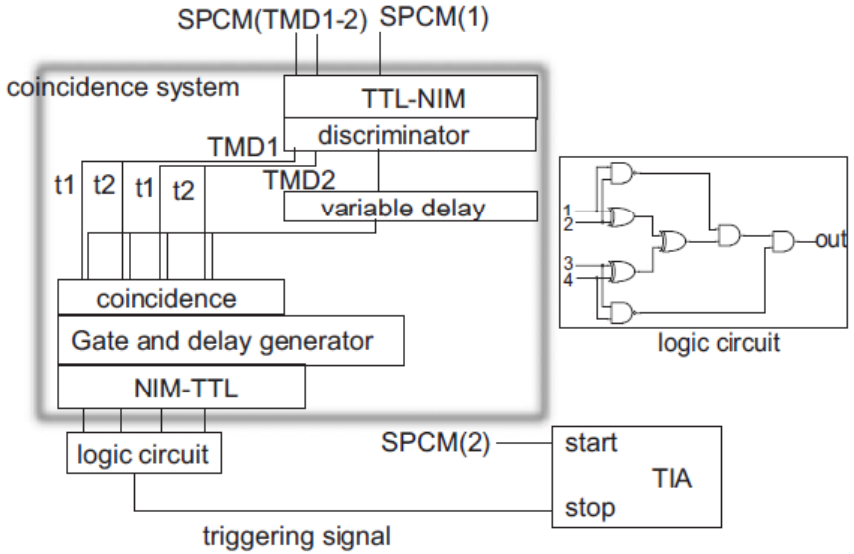
Physical Review A 73, 032331 (2006)

簡易光子数識別器の製作と測定による量子鍵配送システム向上可能性の実証

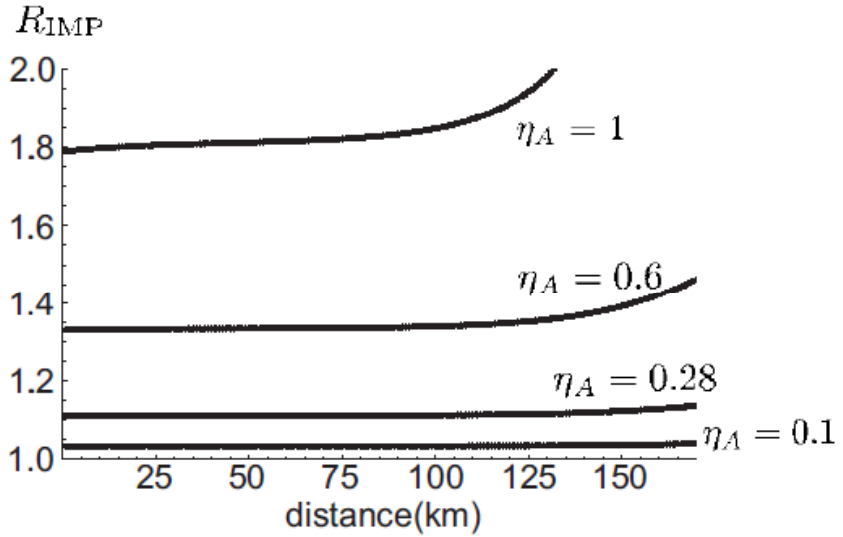


実験系：光学系＋電気系

電気系の概略図



実験で示せた秘密鍵生成率の向上率



Physical Review A 76, 012306 (2007)

まとめ

実験研究の一例紹介

量子情報：非常に特殊な研究領域
➔量子状態の重ね合わせ、量子の分割不可能性などマクロには知覚できないが、20世紀の量子論（や情報理論）の膨大な積み上げを利用した、新しい技術・役に立つものを作ろうと目指す研究領域

実際の研究：分野の進展に重要な寄与したいとの（多分多くの研究者がもっている）思いと、
自分の能力・環境における限界との兼ね合いからやれる事が決まる（おそらくこの制約は実験屋の方が大きい）

鍵を共有した時の情報伝達方法

送信者（Alice）

情報	0010100…..
鍵	1011100…..
XOR 出力	1001000…..

出力を受信者に送る.

受信者（Bob）

送られてきたビット列	1001000…..
鍵	1011100…..
復号化された情報	0010100…..

例：BB84 protocol

光子に4状態をランダムに符号化する

- 1. 送信者Aliceはランダムビット列を決める。
  00101101…….
- 2. 2組の基底を用いて、各々のビットをどちらで符号化するか選択する.
  例：偏光符号化　直線{0=H(水平),1=V(鉛直)},
  円 {0=L(左円),1=R(右円)}

送信者が始めに選ぶビット列	0	0	1	0	1	1	0	1
送信者が始めに選ぶ基底	○	↔↕	○	○	↔↕	↔↕	○	○
符号化に用いる偏光	L	V	R	L	H	H	L	R
受信者が始めに選ぶ基底	○	↔↕	↔↕	○	↔↕	○	↔↕	○
送受信者共通の基底	○	↔↕		○	↔↕			○
受信者が誤りなしに得られるビット列	0	0		0	1			1

- 3. 偏光した光子を受信者Bobに送る.
- 4. Bobはそれぞれの光子をどちらの基底で測定するかランダムに選ぶ.
- 5. 送信者と受信者の基底が一致した場合、復号化されたビットは必ず一致する.

（Alice,Bobの基底が一致する確率は1/2なので、最初にAliceが選んだビット列の半分の長さの鍵が得られる）

受信者が始めに選ぶ基底	○	↔↕	↔↕	○	↔↕	○	↔↕	○
送受信者共通の基底	○	↔↕		○	↔↕			○
受信者が誤りなしに得られるビット列	0	0		0	1			1

- 6.　送信者はそれぞれのビットの符号化に使用した基底を受信者に知らせる.
- 7.最後に符号化と復号化に同じ基底を使用したビットのみを取ることで鍵の共有が完成する。

(この場合, 1,2,4,5,8番目のビットが鍵として使える.)

送信者が始めに選ぶビット列	0	0	1	0	1	1	0	1
送信者が始めに選ぶ基底	○	↔↕	○	○	↔↕	↔↕	○	○
符号化に用いる偏光	L	V	R	L	H	H	L	R
受信者が始めに選ぶ基底	○	↔↕	↔↕	○	↔↕	○	↔↕	○
送受信者共通の基底	○	↔↕		○	↔↕			○
受信者が誤りなしに得られるビット列	0	0		0	1			1

安全な理由

盗聴者がいる場合を考える

符号化に用いられた基底はわからない（光を受信した後で
基底情報を伝える）ので、
盗聴者：ランダムに円偏光か直線偏光かを選び測定する。
→Alice,Bobの通信で、同じ基底を用いた一致するべき
ビット値に誤りが生じる。
例：Alice={直線偏光, 0}, Bob={直線偏光}→0 のはずだが、
盗聴者がいると
Alice={直線偏光,0}, Eve={円偏光}→0と1
それぞれ1/2の確率で得られるので¼の確率で誤りを生じる。
盗聴者Eveは光を盗んだ事がばれないように、Bob
に自分の測定結果に基づく光を作って送る
Bob={直線偏光}→ 0 p=3/4
1 p=1/4
→1/4の確率で盗聴がばれる
→検査するビットの数を増やせば、盗聴を見過ごす確率は
任意に0に近づける。