Single Photon Quantum Cryptography

単一光子の量子暗号

Phys. Rev. Lett. **89**, 187901 (2002)

Alexios Beveratos, Rosa Brouri, Thierry Gacoin, Andre Villing, Jean-Philippe Poizat, and Philippe Grangier

平野研究室

02041025　得永　真吾

発表の流れ

1. 現代暗号の問題点
2. 量子鍵配送の方法
3. 本実験の装置図
4. 単一光子光源の有用性
5. 実験でのカギ生成
6. 本論文のまとめ

1.現代暗号の問題点

現在の暗号

安全性は素因数分解が「難しい」という事を利用。
(公開鍵暗号方式)

「難しい」とは？

例：11×41×73×101×137　＝455555551

455555551＝？？？

時間がかかる！

量子コンピュータが出来ると現在、因数分解に1000億年かかる計算が数日～数時間で出来る可能性がある。

そこで量子暗号を用いる

理論上、絶対に安全！

通信に量子状態を用いる

光子1個を送る

↓

不確定性原理により、盗聴者がいたら状態が変わってしまう。

↓

受信者が受け取るものは送信者が送ったものと違う。

↓

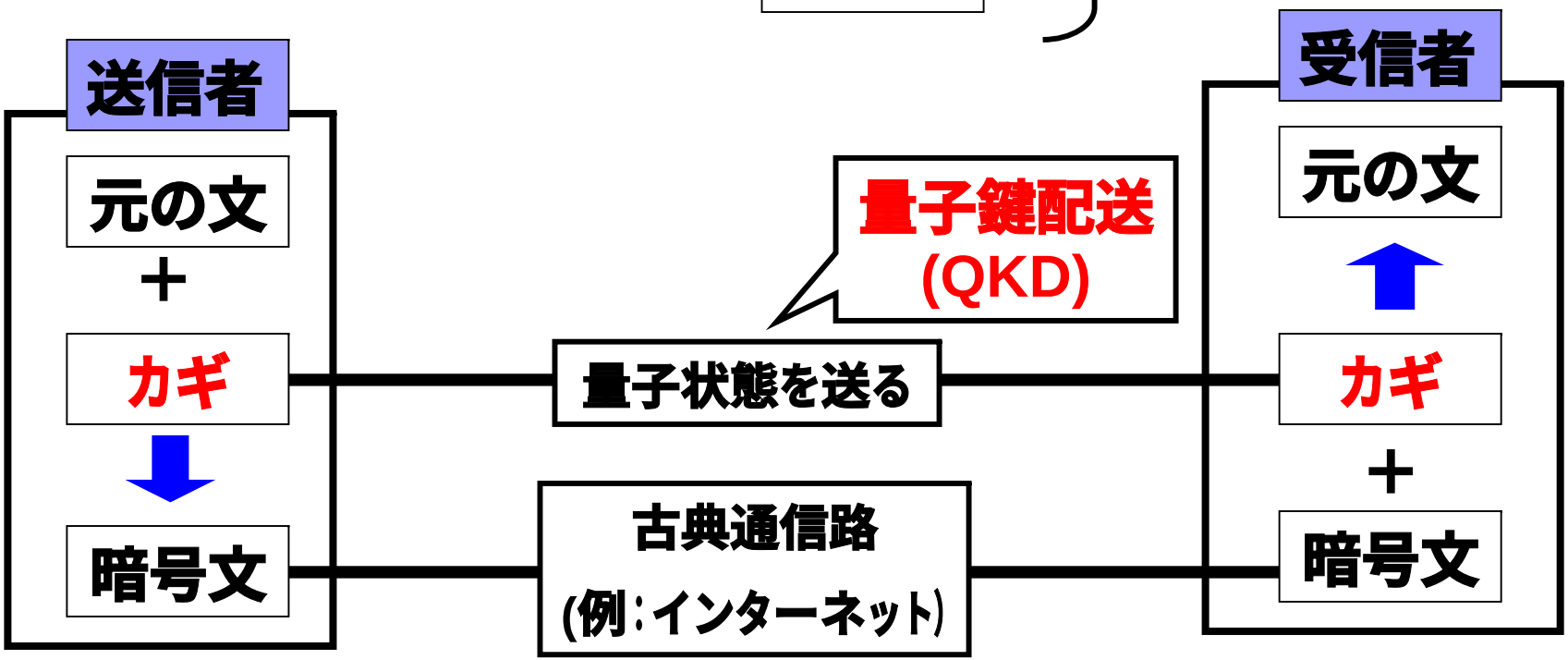
送信者と受信者の**食い違いを見る**事で**盗聴者の存在が分かる**！

通信に物理法則を用いた！

量子暗号のイメージ図

通信の話なので、ビットを扱う。

元の文
カギ
暗号文
0と1の列

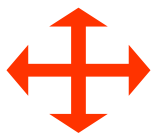


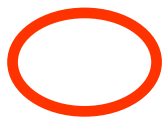
2. 量子鍵配送(QKD)の方法

準備

送信者、受信者とも2つの基底を用意。

縦横基底　　**円基底**





送信者

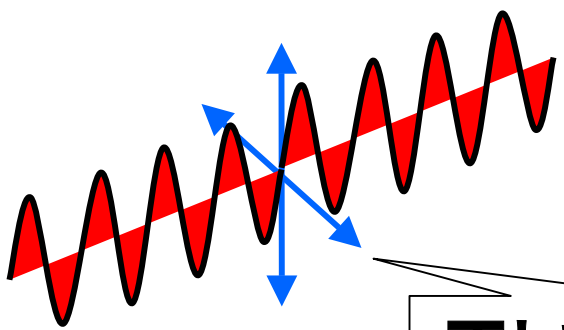
ビット＼基底		
1	↕	↻
0	↔	↺

受信者

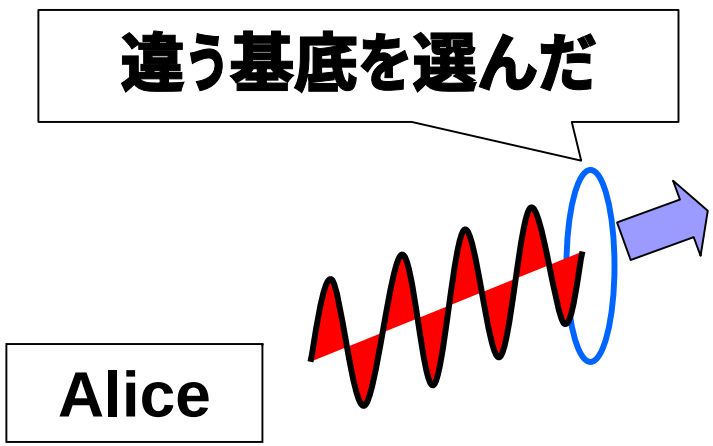
基底		
	↕	区別
	↔	
	↻	区別
	↺	

基礎知識

「1」を縦偏光で送ろう



Bobは「1」という正しい情報を**確実**に得られる。

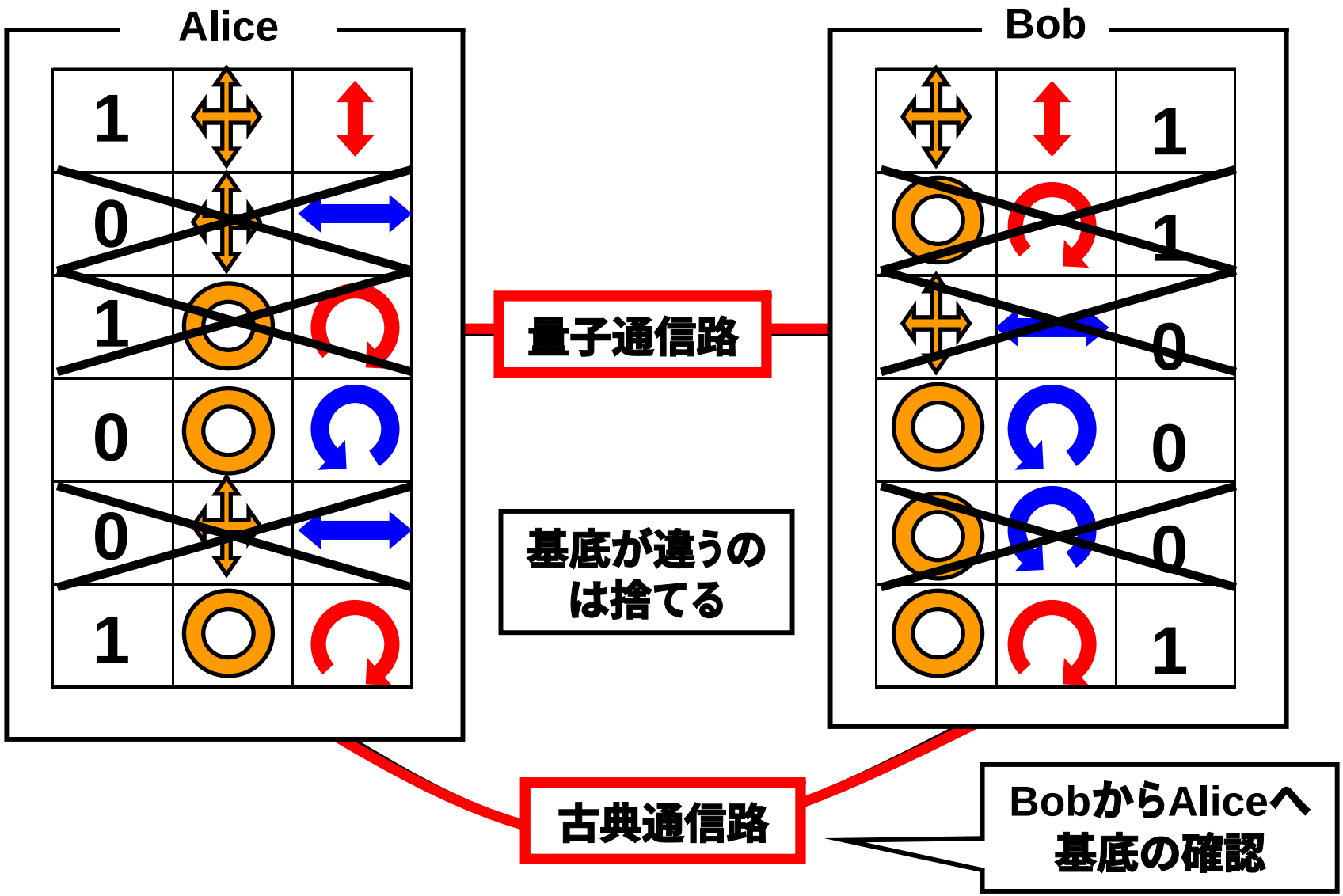


Bobは「1」、「0」を確率**50%**ずつで得る。

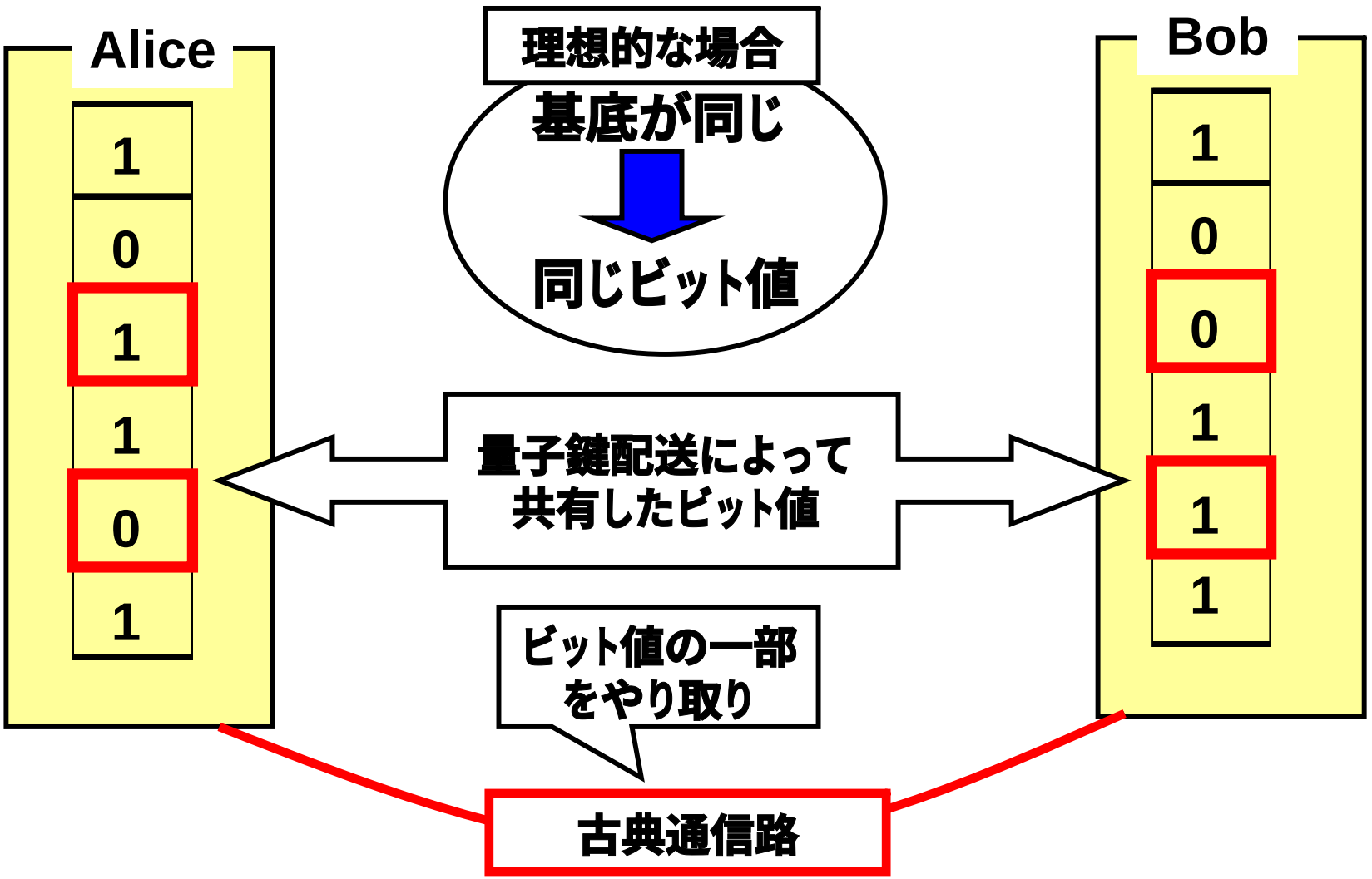
量子力学では状態を

重ね合わせで書き表すから。

量子鍵配送(QKD)の手順



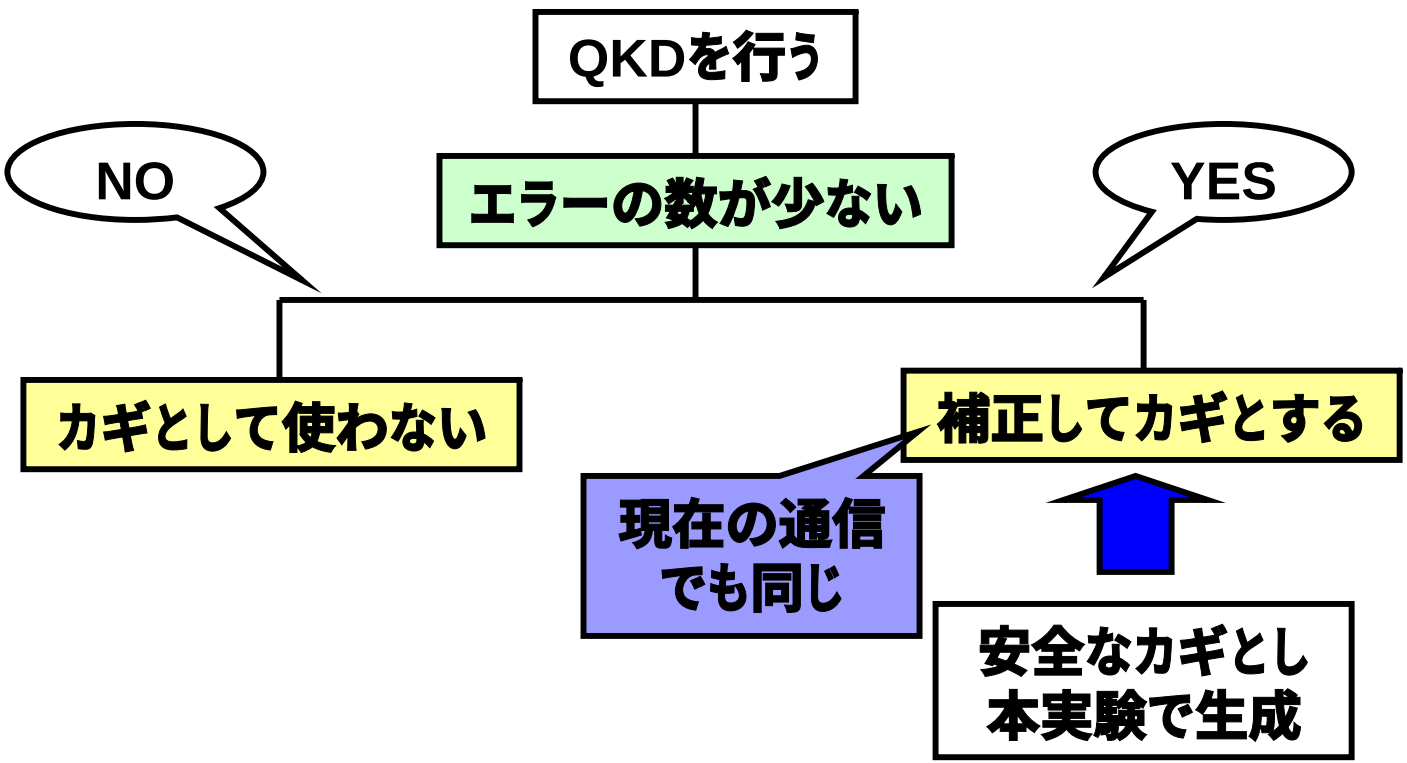
現実の量子鍵配送


Alice
1
0
1
1
0
1
理想的な場合
基底が同じ
同じビット値
量子鍵配送によって
共有したビット値
ビット値の一部
をやり取り
古典通信路
Bob
1
0
0
1
1
1

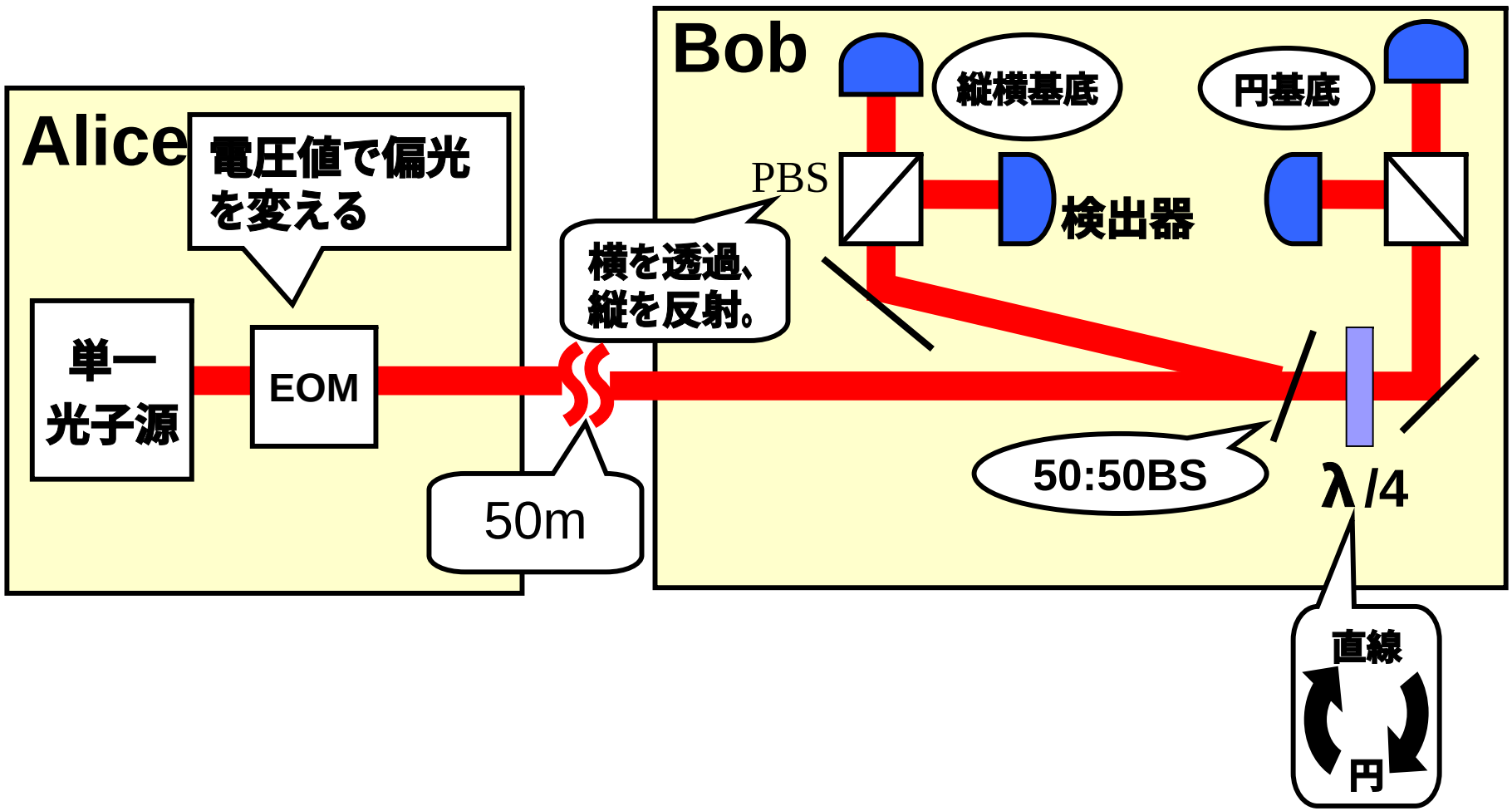
何故ビットが食い違うのか？

通信路のエラー、雑音 ⇒ 検出器、機械のためだが、盗聴者の影響とする

QKDの後どうする？

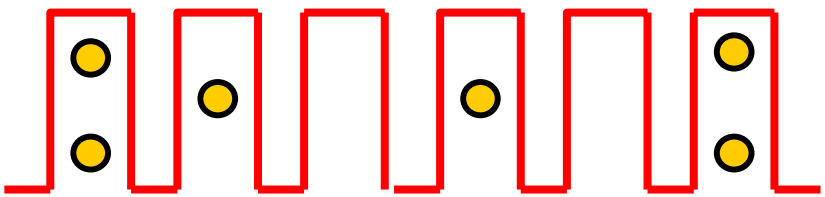


3.本実験の装置図

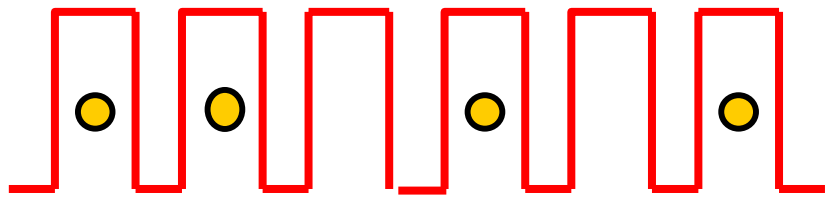

Alice
電圧値で偏光を変える
単一光子源
EOM
50m
横を透過、縦を反射。
Bob
縦横基底
円基底
PBS
検出器
50:50BS
λ/4
直線
円

4.単一光子光源の有用性

既存のパルスレーザー



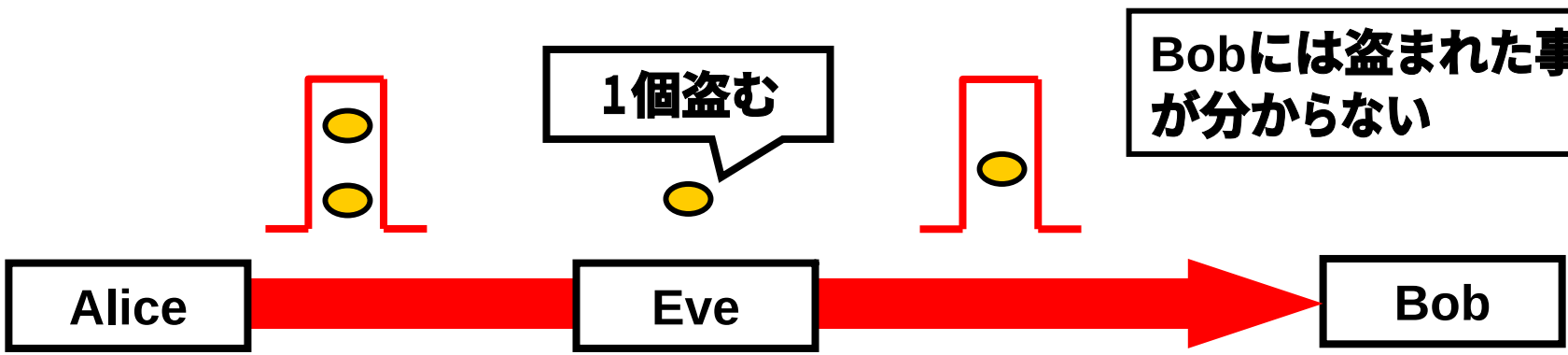
パルス単一光子源



量子暗号では1パルスあたり1個の光子にする必要がある。

➡ 何故なら、盗聴の危険性があるから。

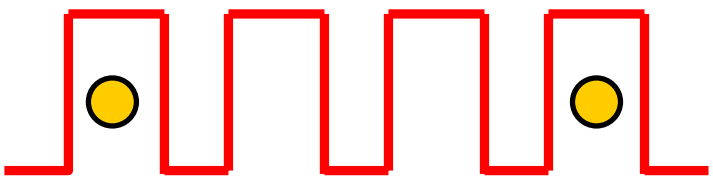
2光子あった場合に考えられる盗聴法



さらに

弱いレーザーを用いる場合、平均光子数μを小さくするしか、1パルス内に2光子になる確率を小さく出来ない。

しかし μを下げると伝送速度が遅くなってしまう！



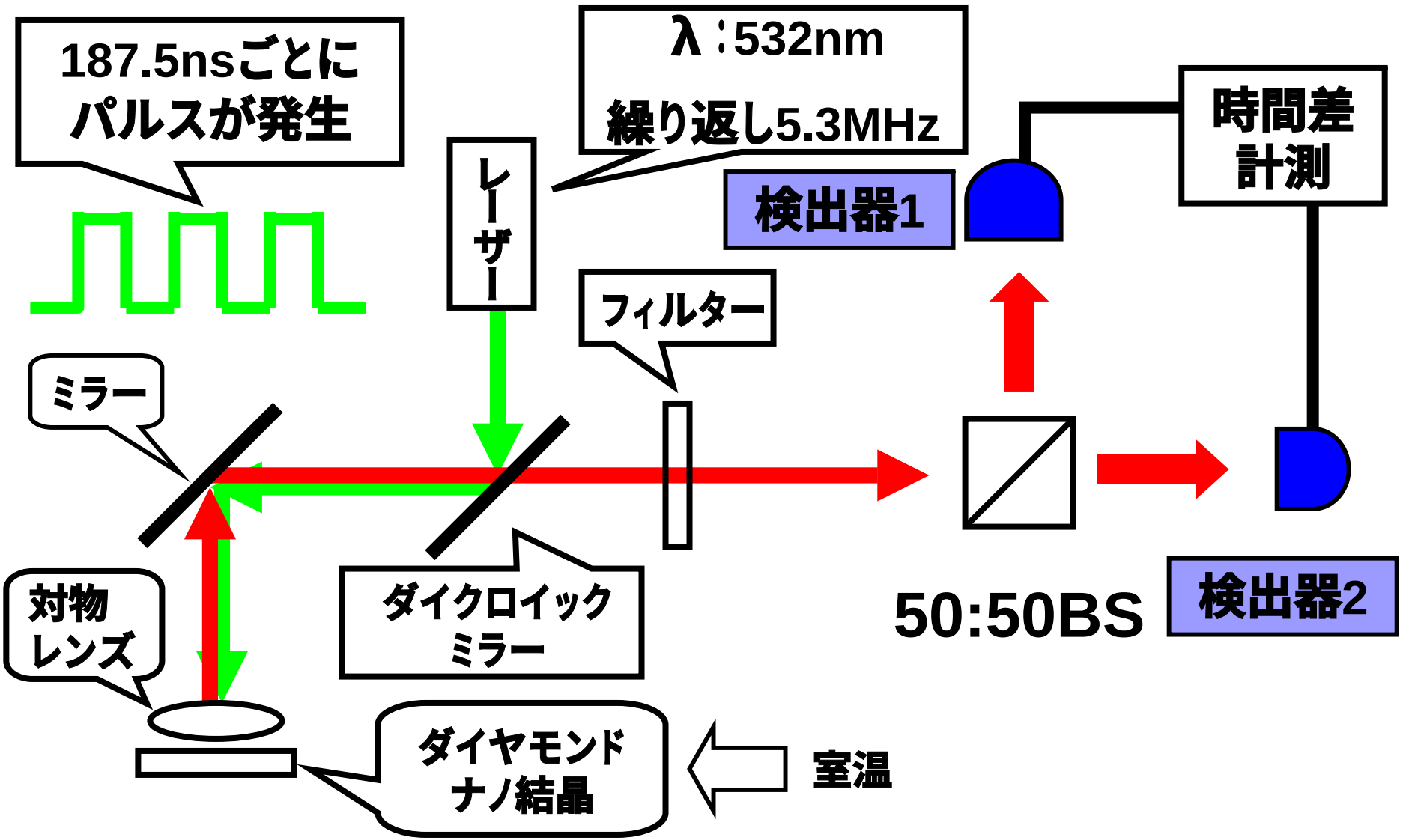
平均光子数：μ=0.5

平均光子数:1パルス中に含まれる光子の数の平均

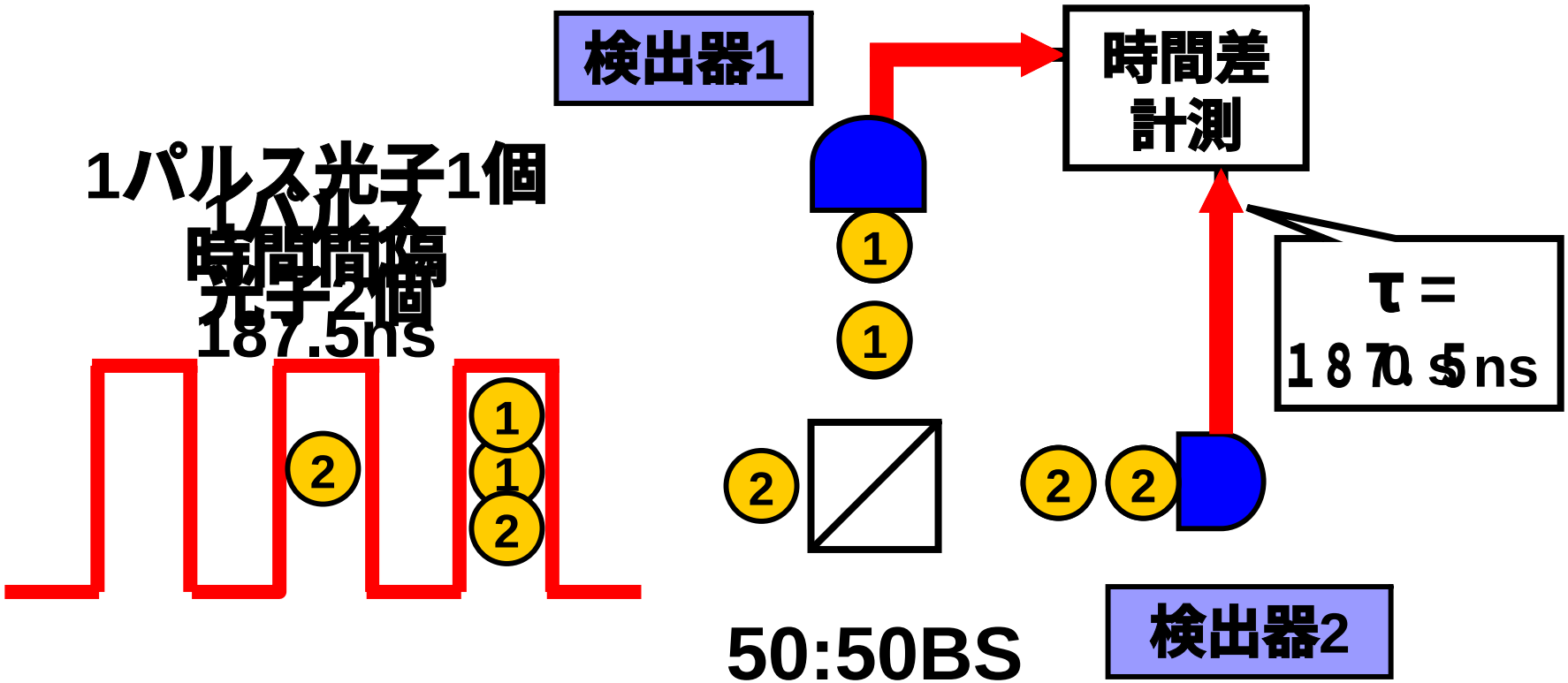
単一光子光源を使う！

1. **盗聴される確率を小さくできる。**
2. **伝送速度が速い！！**

単一光子光源の生成、確認

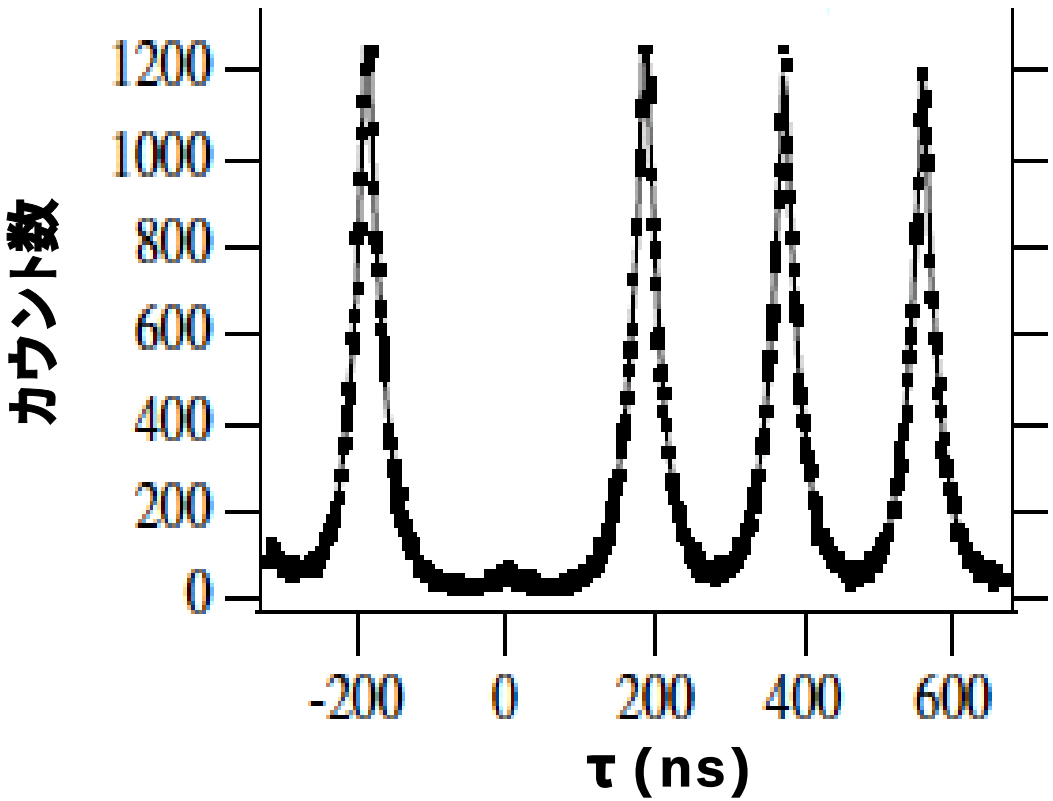


時間差のカウント法


検出器1
時間差
計測
1パルス光子1個
1パルス
時間間隔
光子2個
187.5ns
τ =
187.5ns
1
1
2
1
1
2
2
2
2
50:50BS
検出器2

実験での確認

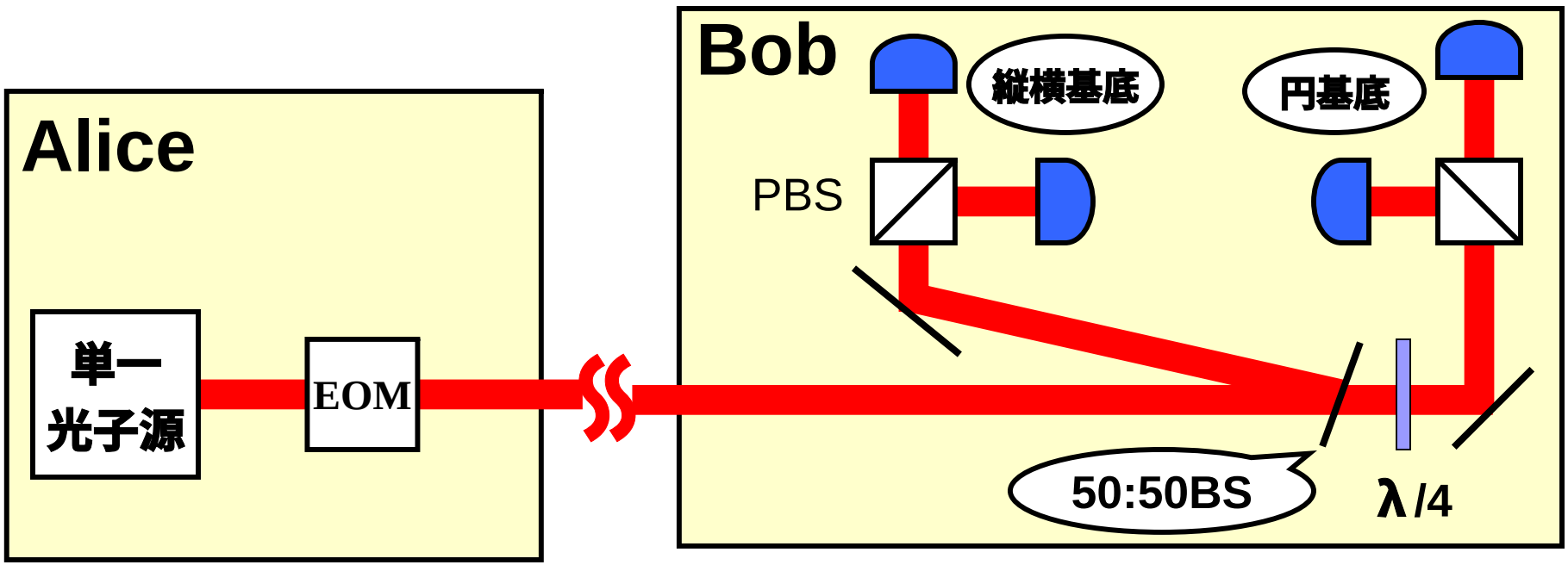
1パルス内に2個の光子ならば，τ=0でカウントする。



パルスの発生間隔は187.5ns。

τ=0でカウントされてない。187.5nsごとにカウントの山が見られる。

5.実験でのカギ生成



QKDを行う

$17700\ s^{-1}$

エラーの数が少ない

カギとして使わない

補正してカギとする

安全なカギの見積り

1パルスあたり安全なビット数Gを見積もる。

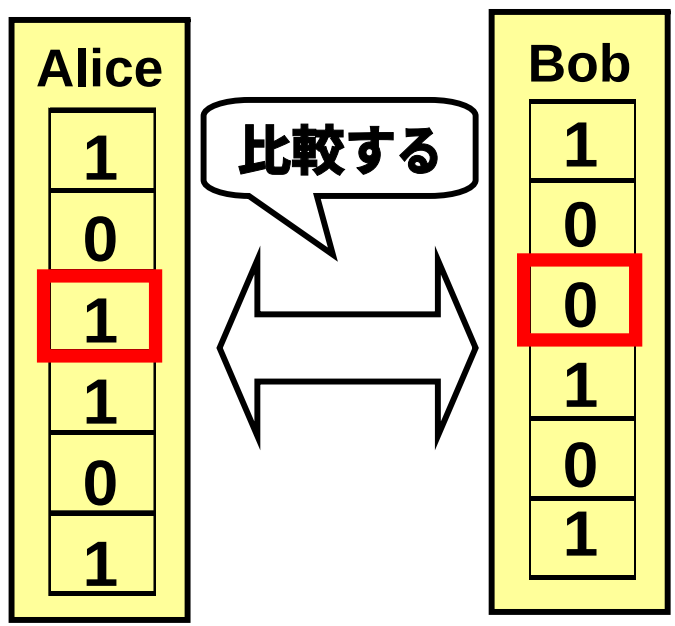
Gを算出するために必要な値が3つ

1. Bobが信号を検出する確率

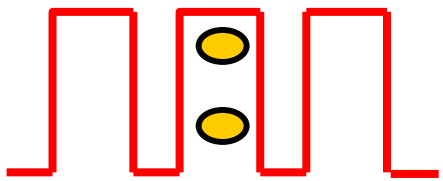
$$p_{\exp} = 0.74\%$$

2. Bobの検出が間違う確率

$$e = 4.6\%$$



3. Aliceが1パルス2光子以上を出す確率



μ=0.014 ⇨ $S_m = 0.0007\%$

μ=0.014で弱いレーザー(WCP)を用いた場合は

$$S_m^{WCP} = 0.01\%$$

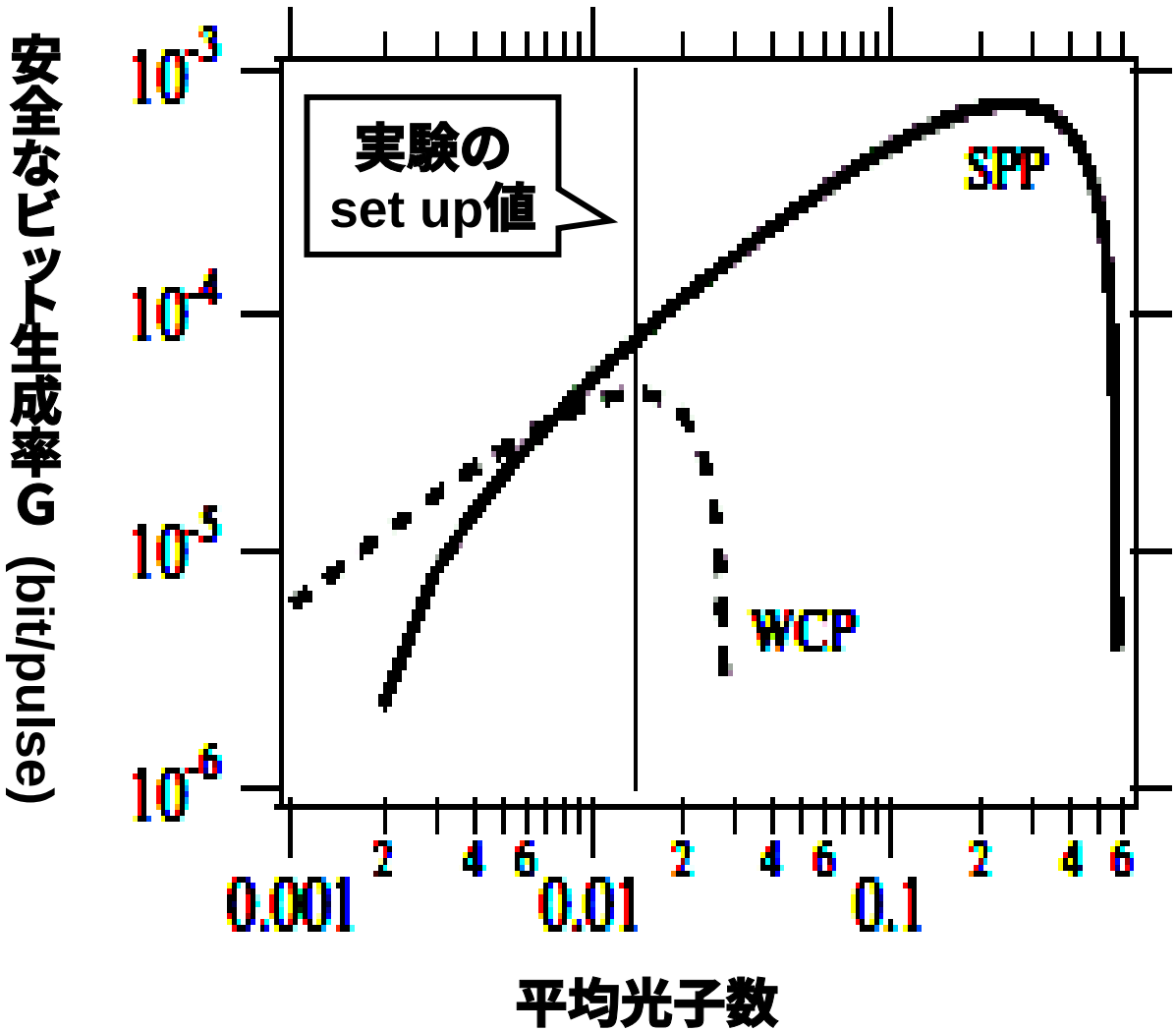
$S_m < S_m^{WCP}$ なので単一光子を用いた方が良い事が分かる。

上の3つの値で実験をした場合に得られる見積り値は

$$G = 1.68 \times 10^{-3} (\text{bit/pulse})$$

となる。

計算値をグラフ化



SPP (単一光子光源)の方がWCPよりも鍵生成の効率が良い。

1秒間に何ビット(N_{QKD})のやり取りが出来るかに見積もると

$$N_{QKD} = 1.68 \times 10^{-3} \times 5.3MHz$$

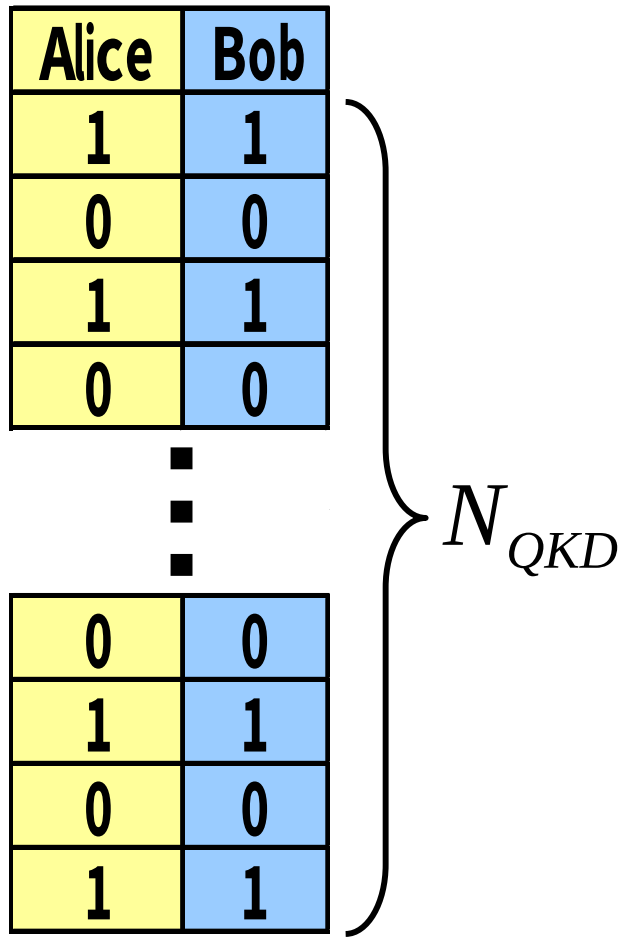
$$\approx 8900\, s^{-1}$$

レーザーの繰り返し周波数

実験値

実験で実際に補正をして得た1秒間あたりのビット数

$$N'_{QKD} = 7700\ s^{-1}$$



6.本論文のまとめ

単一光子光源で4つの偏光状態を用いた量子暗号実験を行った。

1.室温で動作する**単一光子光源**を用いた。

2.**空間50m**を伝送し、秘密鍵の生成率は

$$N'_{QKD} = 7700s^{-1}$$

この実験によって単一光子光源を用いる**長距離(地上と衛星)**の量子暗号の可能性が示された。

計算結果

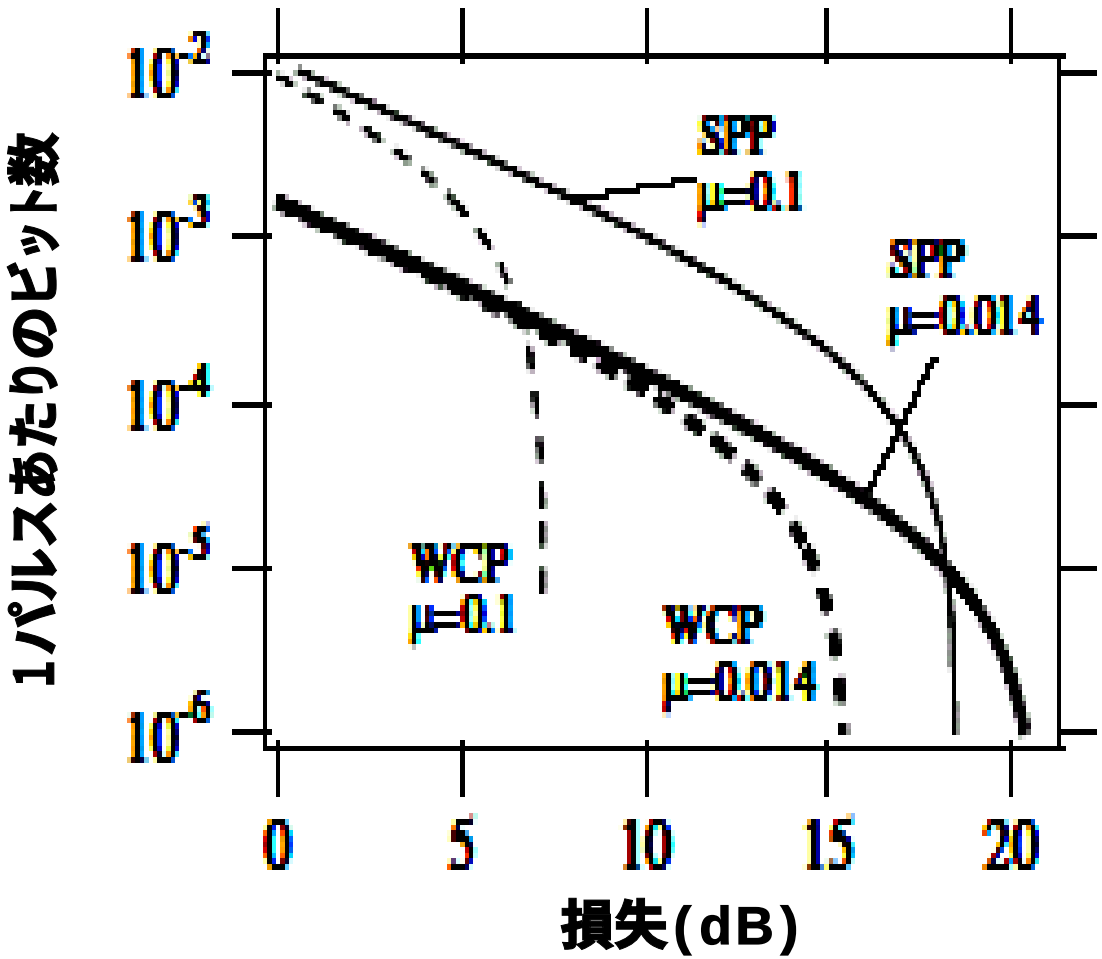
SPP:単一光子パルスレーザー

WCP:強度の弱いパルスレーザー

今回の実験結果から得られる値を理論値に代入し、グラフを書いた。

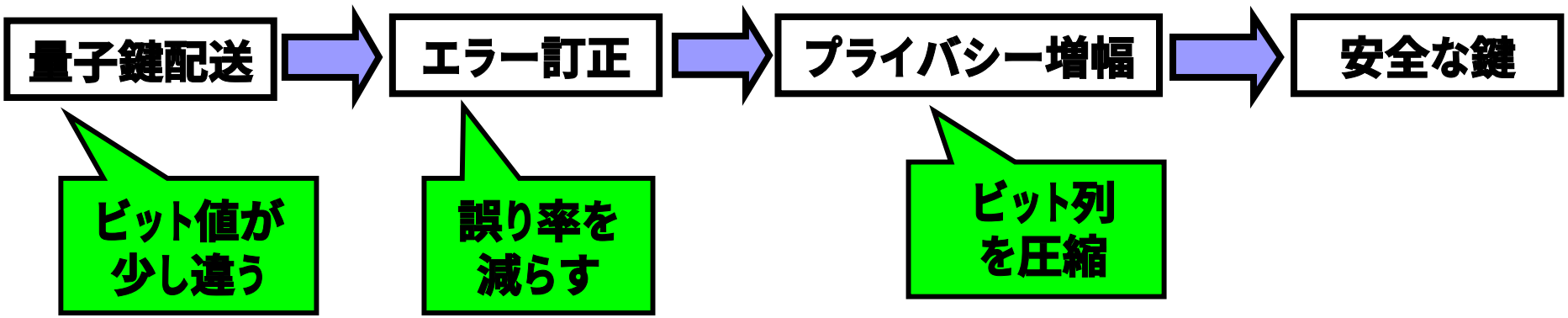
①の結果比較1

鍵生成は落ちるが、SPPの方が遠くに伝送できる事が分かる。



実験の前に

ビット値の乱れ
1．盗聴者
2．通信路エラー、雑音
➡ 補正してから評価する



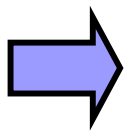
AliceとBobで1秒間に共有出来る安全なビット数を計算値と実験値の比較。

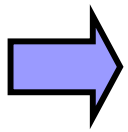
2.QKD（量子鍵配送）の方法

準備

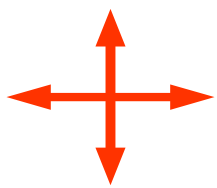
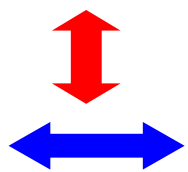
送信者「Alice」

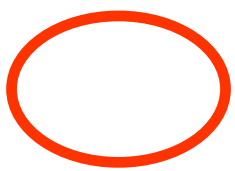
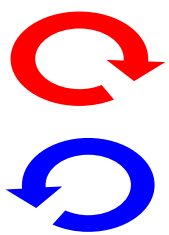
縦偏光 	右回り円偏光 
横偏光 	左回り円偏光 

 1と符号化する

 0と符号化する

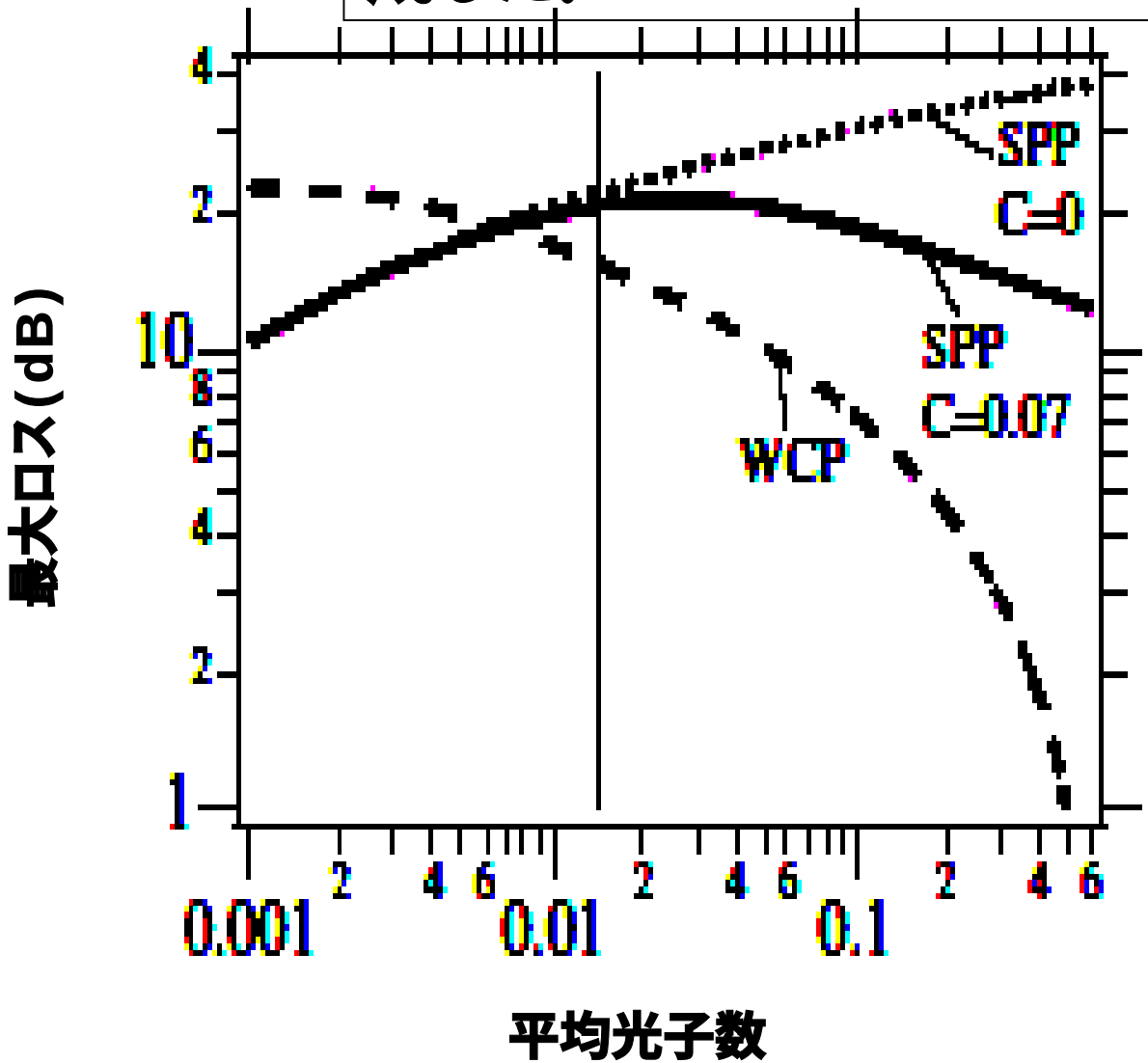
受信者「Bob」

縦横基底    区別出来る

円基底    区別出来る

比較2

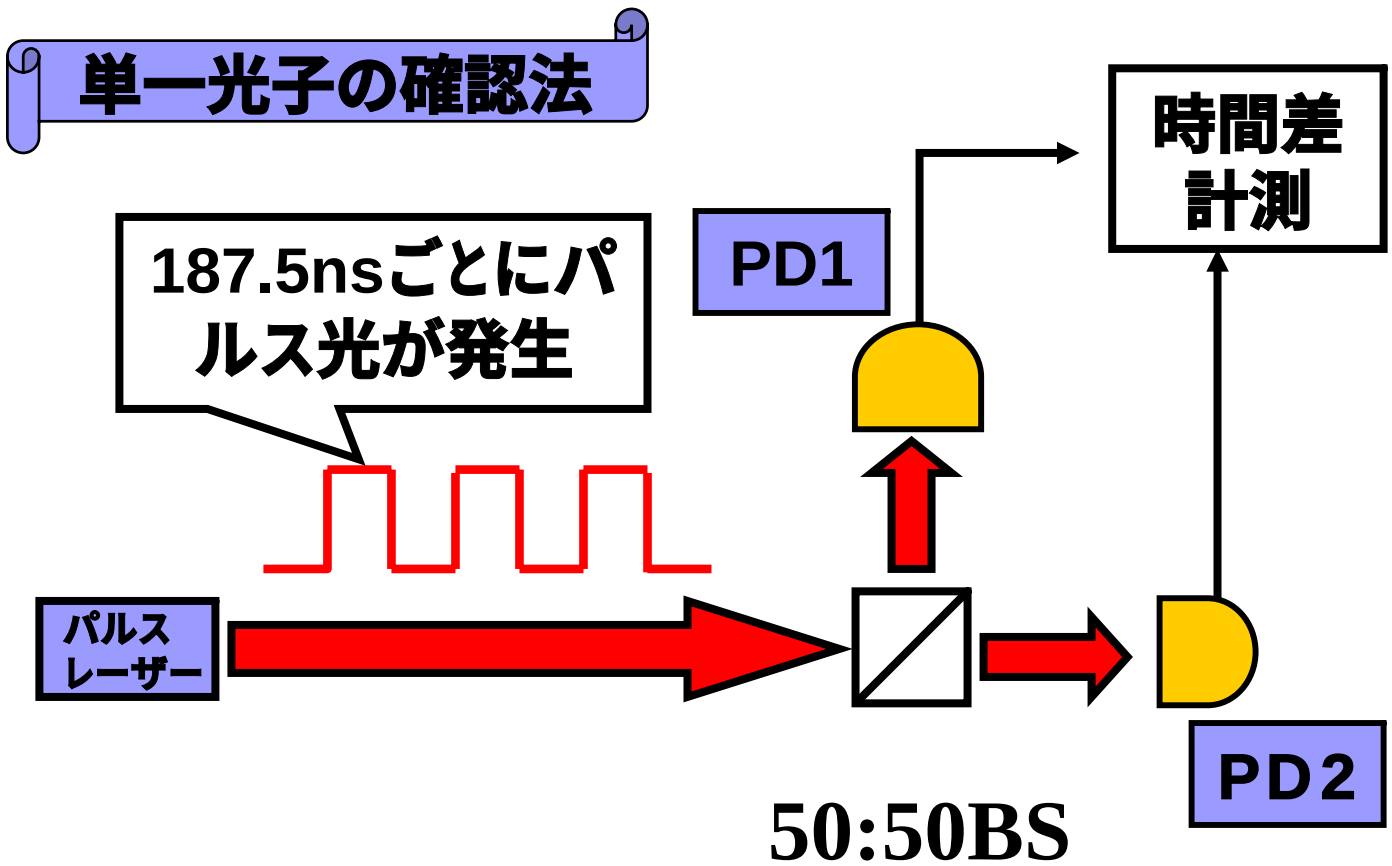
AliceとBobの間で共有する安全なカギを実成した。



平均光子数を
下げた時に
SPPの方が
ロスが小さくなる。

単一光子の確認

ダイヤモンドナノ結晶に波長532nmのレーザー光(繰り返し5.3MHz)を当てて発生した蛍光を単一光子光源として使用している。



Gの計算式

$$G = \frac{1}{2} p_{\exp} \left\{ \frac{p_{\exp} - S_m}{p_{\exp}} \left(1 - \log_2 \left[\right. \right. \right.$$

$$\left. \left. \left. 1 + 4e \frac{p_{\exp}}{p_{\exp} - S_m} - 4 \left(e \frac{p_{\exp}}{p_{\exp} - S_m} \right)^2 \right] \right) \right.$$

$$\left. + f[e][e \log_2 e + (1-e) \log_2 (1-e)] \right\}$$