A 24km fiber-based discretely signaled continuous variable quantum key distribution system

24kmのファイバーを用いた、
離散変調された連続変数量子鍵配送

2009 / Vol. 17, No. 26 / OPTICS EXPRESS 24244
Quyen Dinh Xuan, Zheshen Zhang, and Paul L. Voss

平野研究室
07-041-011 川副 僚介

目次

- 暗号通信の予備知識
- 本論文の量子鍵配送について
- 本論文の実験について
- まとめ

暗号について

暗号：送りたい情報を第三者（盗聴者）に知られないようにする技術

- 身近な暗号の用途例
  - インターネットでの個人情報保護

- 今の暗号の安全性根拠→解読に膨大な計算が必要
  - 効率的な計算方法の発見
  - コンピューターの計算速度の飛躍的向上

  ⇨ 短時間で解読される可能性がある！

- 新しい暗号技術、量子鍵配送が研究されている
  - 確実に安全な通信を行うことが出来る

鍵とは何か

平文（送りたいメッセージ）⟷暗号文で変換する道具

例）

平文：hiranoken

↓鍵で暗号文に

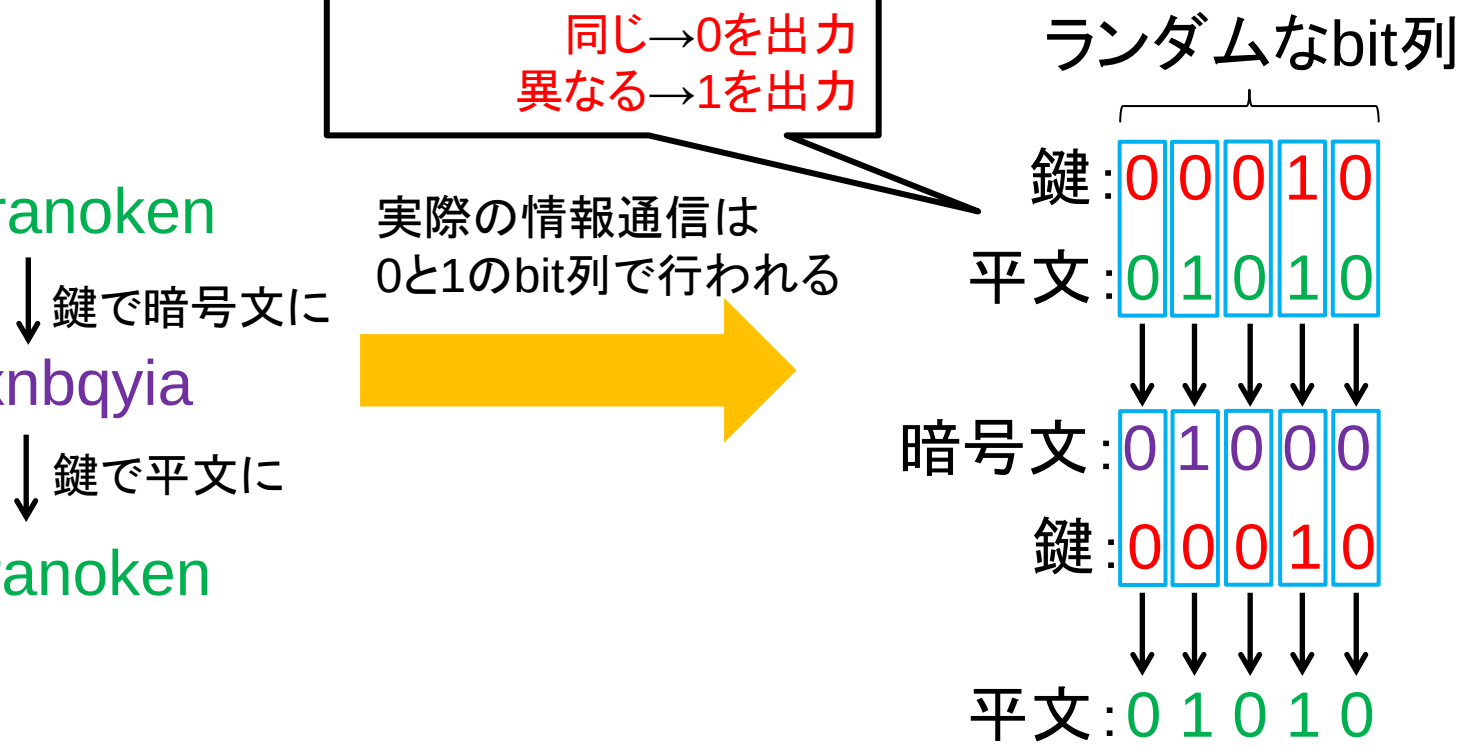
暗号文：elxnbqyia

↓鍵で平文に

平文：hiranoken

鍵と平文の値を比較して
同じ→0を出力
異なる→1を出力

実際の情報通信は
0と1のbit列で行われる



鍵を使った通信

Alice(送信者)

鍵

平文:0 1 0 1 0

鍵:0 0 0 1 0

↓

暗号文:**0 1 0 0 0**

0 1 0 0 0　　**0 1 0 0 0**

通信路

Eve(盗聴者)

暗号文: 0 1 0 0 0

鍵がないので解読できない！

Bob(受信者)

鍵

暗号文:0 1 0 0 0

鍵:0 0 0 1 0

↓

平文: 0 1 0 1 0

AliceからBobへ
平文を送信できた！

AliceとBobのみが共通の鍵を持っていれば
安全な通信を行うことが出来る

どのようにして共通の鍵を持つかが問題

量子鍵配送！

- 本論文の量子鍵配送について
  - 量子鍵配送の概要
  - 量子状態の説明
  - 鍵共有方法
  - 実験での操作
  - 量子鍵配送の安全性

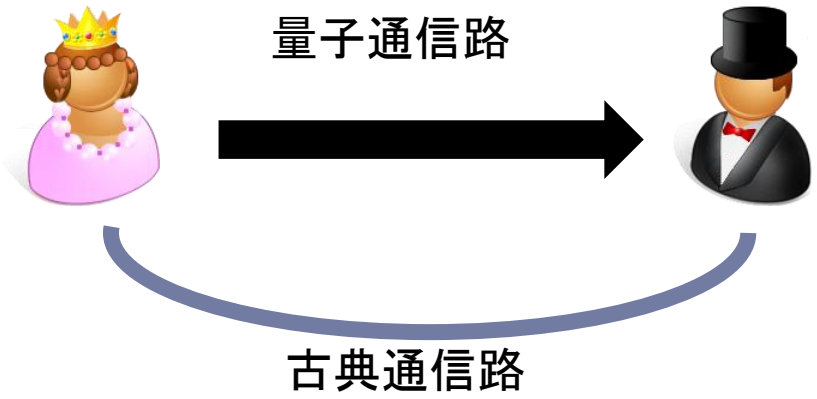
量子鍵配送の概要

目的

最終的に、AliceとBobのみが知る鍵を共有すること

鍵共有の方法

- Aliceは量子状態を量子通信路を使ってBobに送り、Bobは量子状態を測定する
- 古典通信路を使って相談し、安全な鍵を作る



本実験でAliceが送る状態と、Bobの測定する物理量

本実験でAliceは微弱なレーザー光の位相を
変化させ、4種類の量子状態（コヒーレント状態）
のひとつを送る

Bobは直交位相振幅xまたはpを測定する

コヒーレント状態$|\alpha\rangle$と直交位相振幅x,p

レーザー光はコヒーレント状態として扱うことが出来る

コヒーレント状態$|\alpha\rangle$は消滅演算子の固有状態として定義できる

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$$

αは複素数で、電場の複素振幅に比例

$\hat{x}, \hat{p}$：直交位相振幅,実部と虚部に対応

$$\hat{x} = \frac{1}{2}\left(\hat{a} + \hat{a}^{\dagger}\right), \hat{p} = \frac{i}{2}\left(\hat{a}^{\dagger} - \hat{a}\right)$$

$$[\hat{x}, \hat{p}] = \frac{i}{2} \qquad \boxed{\Delta x \Delta p \geq \frac{1}{4}}$$

コヒーレント状態に対する直交位相振幅x,pの不確定さ

$$\langle x\rangle = \tfrac{1}{2}\left\langle \alpha \left| \hat{a} + \hat{a}^{\dagger} \right| \alpha \right\rangle = \tfrac{1}{2}(\alpha + \alpha^{*})$$

$$\langle p\rangle = \tfrac{i}{2}\left\langle \alpha \left| \hat{a}^{\dagger} - \hat{a} \right| \alpha \right\rangle = \tfrac{i}{2}(\alpha^{*} - \alpha)$$

$$\left\langle x^{2}\right\rangle = \tfrac{1}{4}\left(\alpha^{2} + 2|\alpha|^{2} + (\alpha^{*})^{2} + 1\right)$$

$$\left\langle p^{2}\right\rangle = -\tfrac{1}{4}\left(\alpha^{2} + (\alpha^{*})^{2} - 2\,|\alpha|^{2} - 1\right)$$

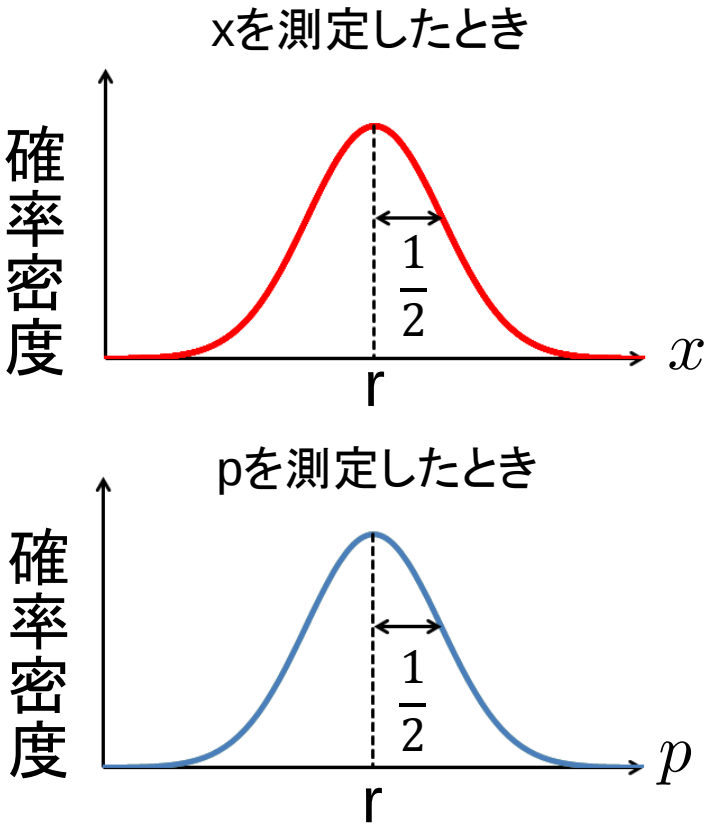
$$(\Delta x)^{2} = \left\langle x^{2}\right\rangle - \langle x\rangle^{2} = \tfrac{1}{4}$$

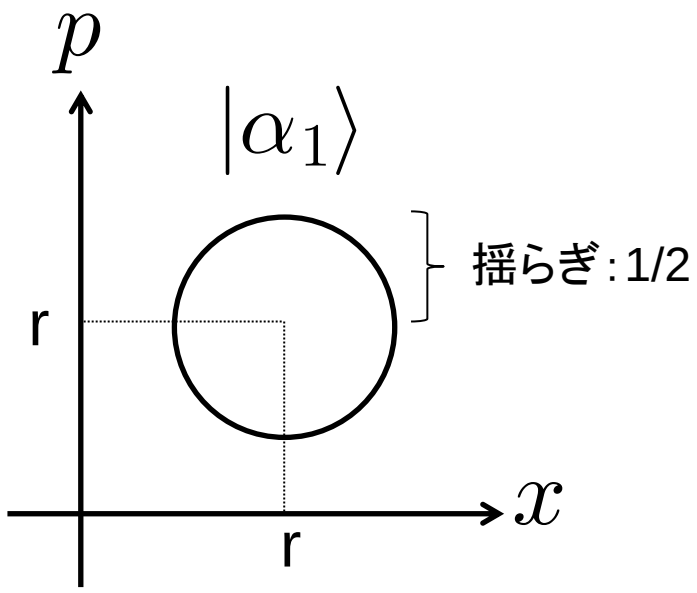
$$(\Delta p)^{2} = \left\langle p^{2}\right\rangle - \langle p\rangle^{2} = \tfrac{1}{4}$$

$$(\Delta x) = (\Delta p) = \frac{1}{2}$$

x,pの測定結果には不確定性関係に起因する量子揺らぎがある

x,pの複素表示



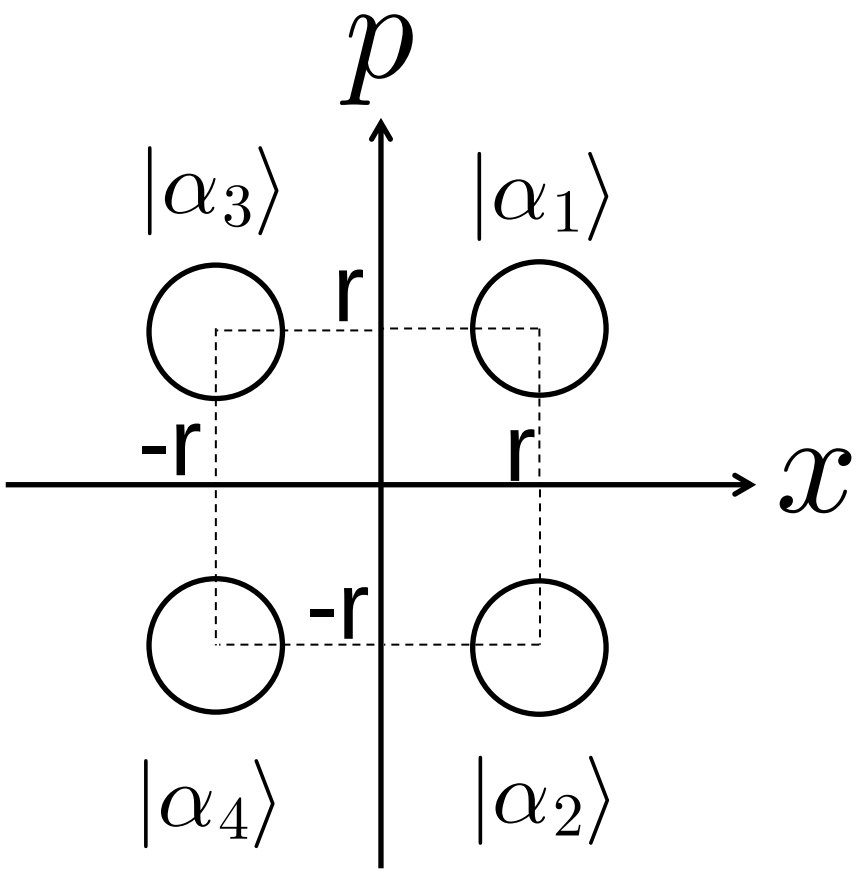


x.pの測定結果がばらつく

本実験でAliceが送る状態と、Bobの測定する物理量

本実験ではAliceは
微弱なレーザー光の位相を
変化させ、4種類の量子状態
（コヒーレント状態）のひとつ
を送る

Bobは直交位相振幅
xまたはpを測定する

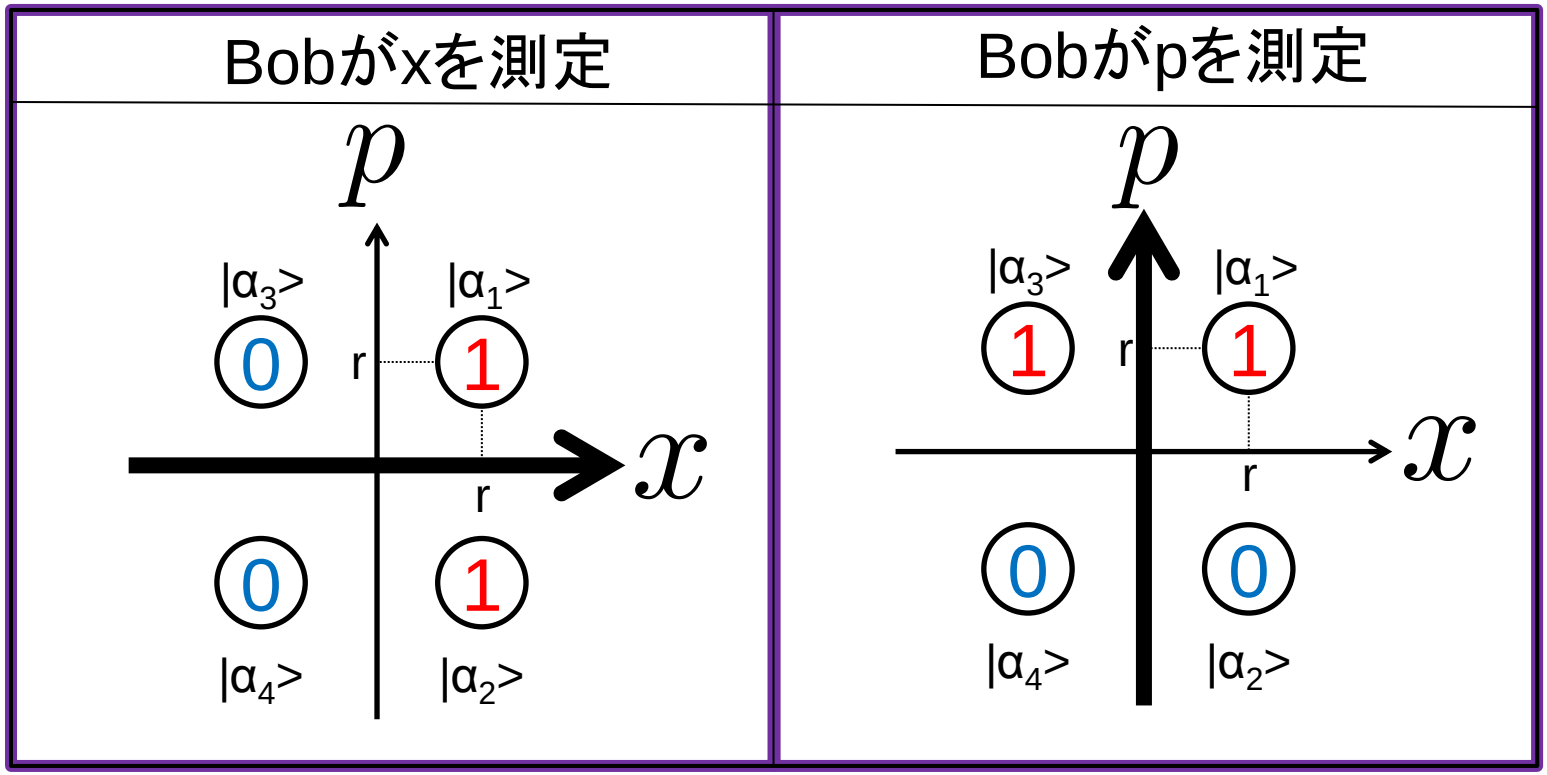


- 本論文の量子鍵配送について
  - 量子鍵配送の概要
  - 量子状態の説明
  - 鍵共有方法
  - 実験での操作
  - 量子鍵配送の安全性

鍵共有の方法(Alice)

1:4種類の量子状態のひとつをランダムに選んで送る

2:Bobがx,pどちらを測定したかを聞き、下図のように鍵bit値0,1に対応させる



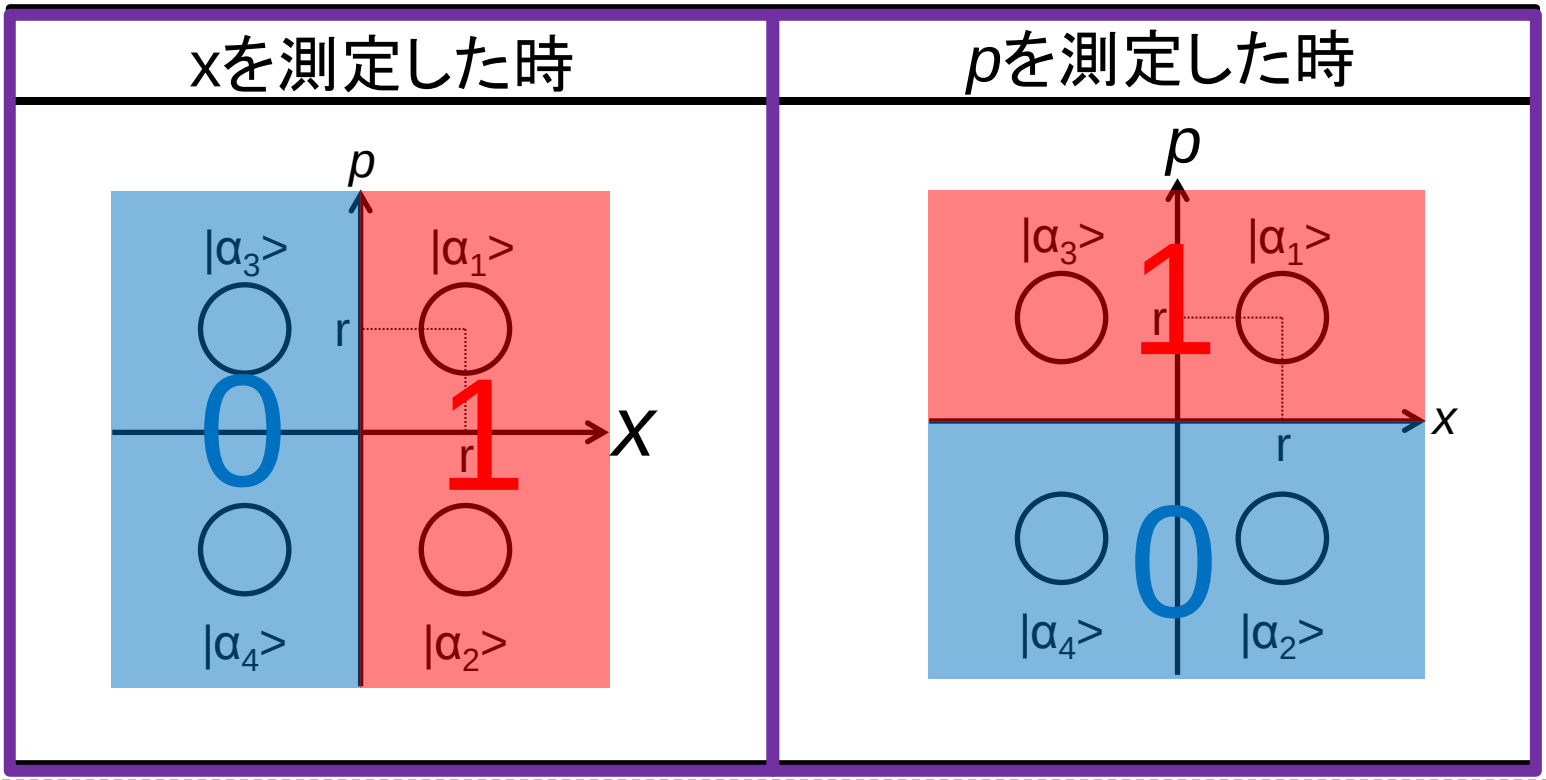
鍵共有の方法(Bob)

BobはAliceが送った状態を判別して同じbit値を得たい

1:受け取った量子状態のx,pどちらかを測定する

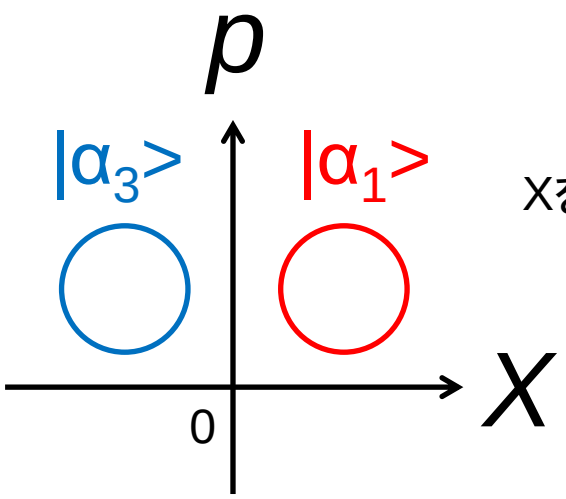
2:x,pのどちらを測定したかをAliceに伝える

3:測定した値が負なら鍵bit値0,正ならbit値1とする

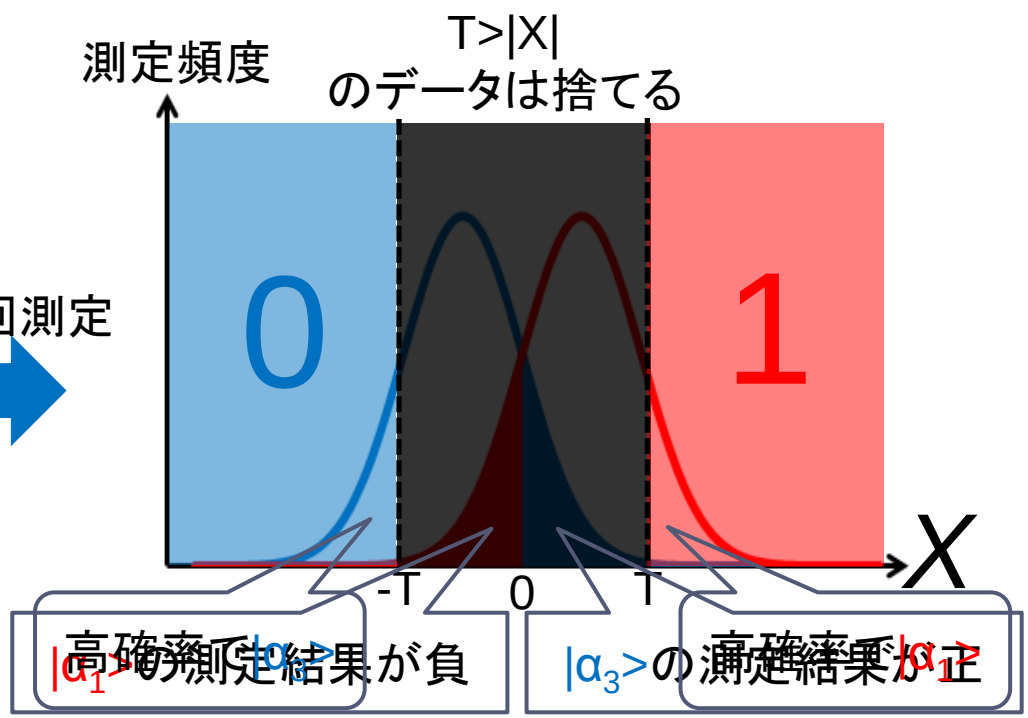


判別ミスを減らす操作：ポストセレクション

簡単のため、2つの状態で考える



Xを多数回測定



Bobは正負だけで$|\alpha_1\rangle$と$|\alpha_3\rangle$を区別できない

$|\alpha_1\rangle$と$|\alpha_3\rangle$を高確率で判別出来る

この操作をポストセレクションと呼ぶ！

鍵共有の方法まとめ

Alice 

	1		3		5
状態	$\|\alpha_2\rangle$		$\|\alpha_1\rangle$		$\|\alpha_4\rangle$
測定軸	x		x		p
測定結果					
鍵bit	**1**		**1**		**0**

Bob 

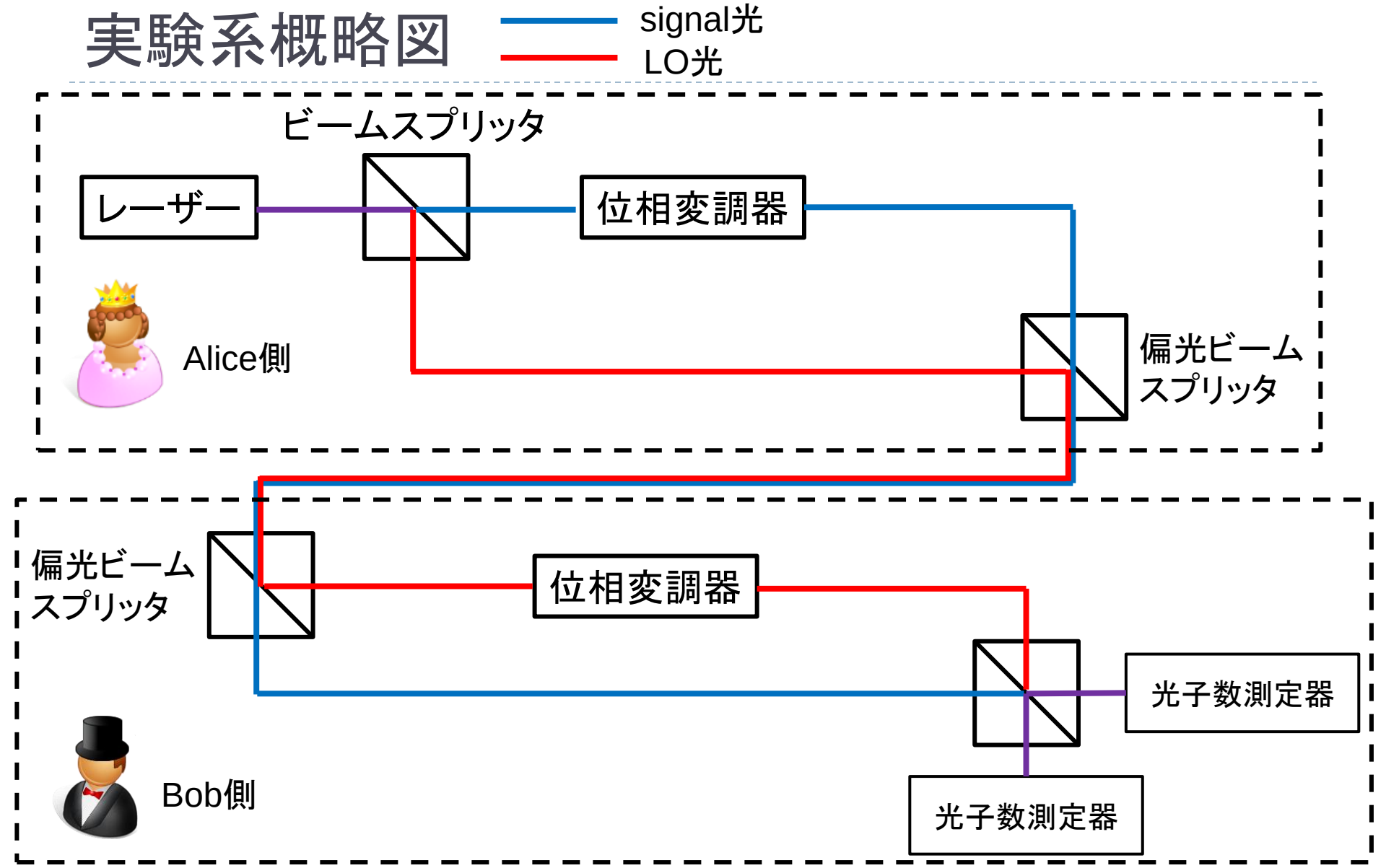
	1		3		5
状態					
測定軸	x		x		p
測定結果	1.3		1.1		-1.5
鍵bit	**1**		**1**		**0**

Alice:4つの量子状態をランダムに送る
Bob:測定軸x,pを選んで測定する
Bob:ポストセレクションを行ない、測定結果がしきい値以下のデータを捨てる
Bob:測定値が負ならbit値を0,正ならbit値を1とする
Bob:ポストセレクションによって捨てたデータ番号と測定した軸をAliceに教える
Alice:規則によって、状態を0と1に対応させる

鍵を共有！

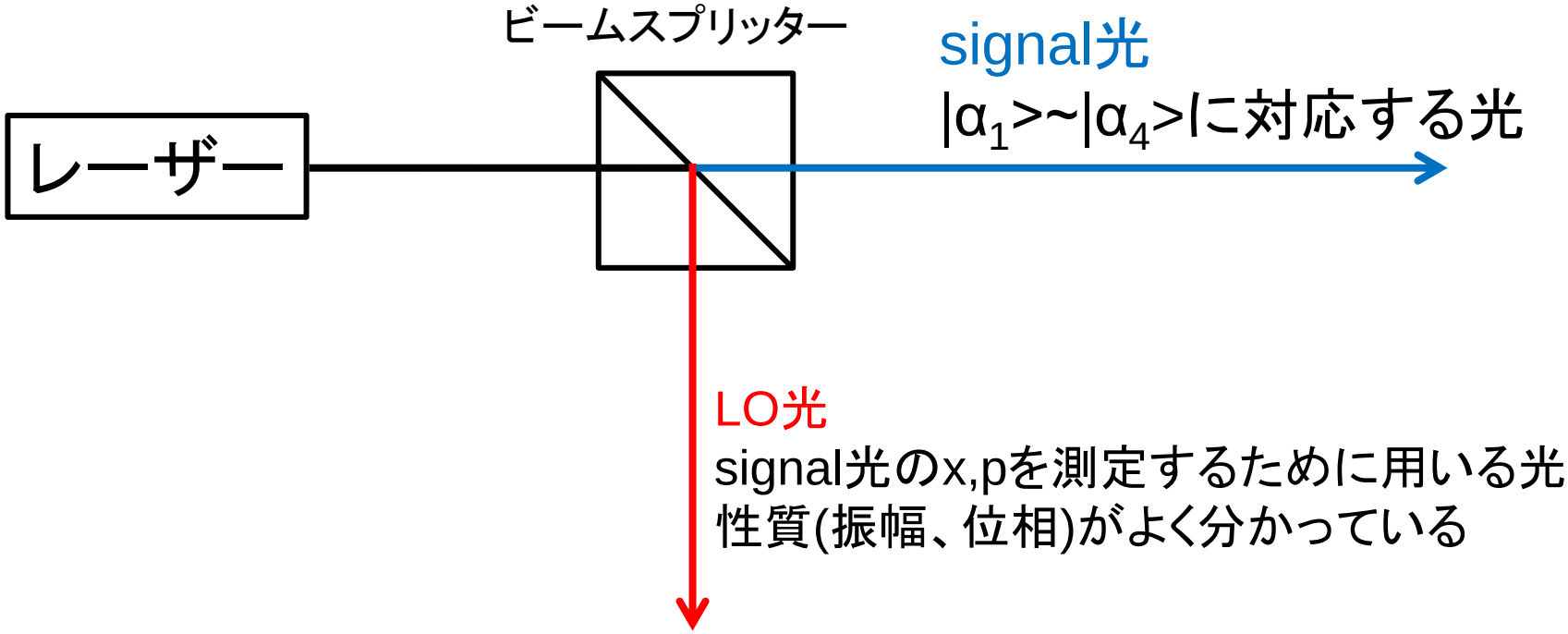
- 本論文の量子鍵配送について
  - 量子鍵配送の概要
  - 量子状態の説明
  - 鍵共有方法
  - 実験での操作
  - 量子鍵配送の安全性

実験系概略図


signal光
LO光
ビームスプリッタ
レーザー
位相変調器
Alice側
偏光ビーム
スプリッタ
偏光ビーム
スプリッタ
位相変調器
光子数測定器
Bob側
光子数測定器

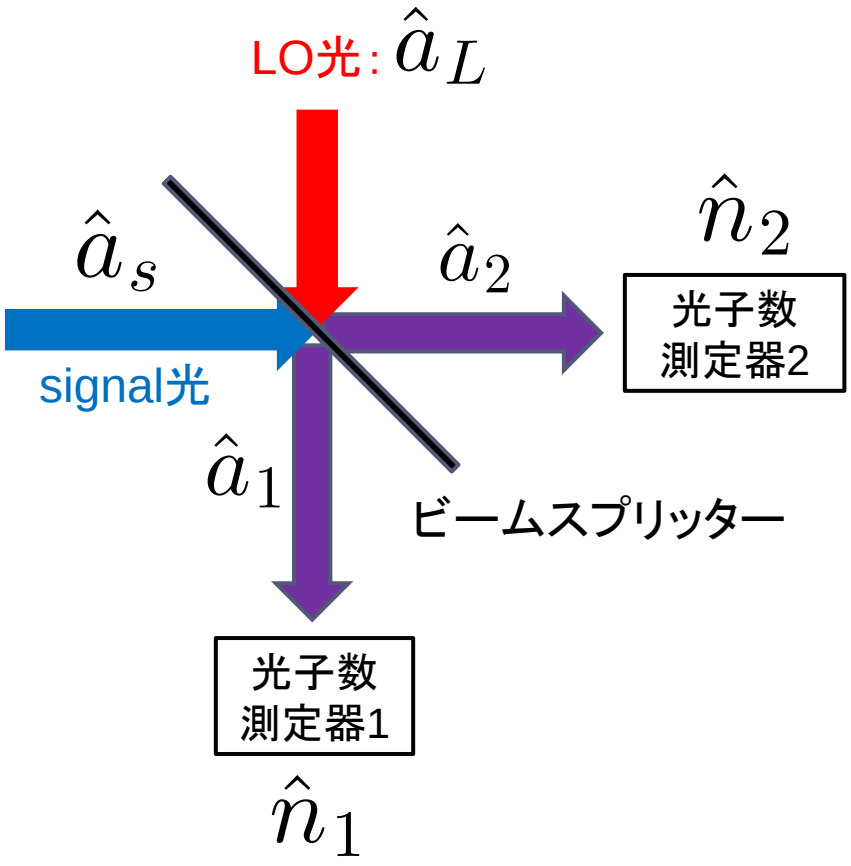
x,pの測定方法：ホモダイン検出法

Bobがx,pをホモダイン検出法で測定するためには、
測定したい光の他にもう一本光が必要
本実験ではレーザーから出射された光を分割して用いる



x,pの測定方法：ホモダイン検出法

ホモダイン検出法：signal光とLO光を混ぜ、その混ぜた光の光子数の差をとることで
signal光の直交位相振幅x,p測定が可能



$$\hat{n}_1 - \hat{n}_2 = \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2$$

$$\hat{a}_1 = (\hat{a}_S + \hat{a}_L)/\sqrt{2}$$

$$\hat{a}_2 = (\hat{a}_S - \hat{a}_L)/\sqrt{2}$$

$$\hat{n}_1 - \hat{n}_2 = \hat{a}_s^\dagger \hat{a}_L + \hat{a}_L^\dagger \hat{a}_s$$

$$\hat{a}_L = \langle a_L \rangle + \Delta \hat{a}_L$$

$$\rightarrow \langle a_L \rangle = |\alpha_L| e^{i\phi_L}$$

$$\hat{n}_1 - \hat{n}_2$$
$$= \hat{a}_s^\dagger \hat{a}_L + \hat{a}_L^\dagger \hat{a}_s$$
$$\rightarrow 2|\alpha_L|(\hat{x}_S \cos\phi_L + \hat{p}_S \sin\phi_L)$$

実験との対応

$$\hat{n}_1 - \hat{n}_2 = 2|\alpha_L|(\hat{x}_S \cos\phi_L + \hat{p}_S \sin\phi_L)$$

LO光の位相 ϕ_L =0の時 $\hat{x}_S = \frac{\hat{n}_1 - \hat{n}_2}{2|\alpha_L|}$

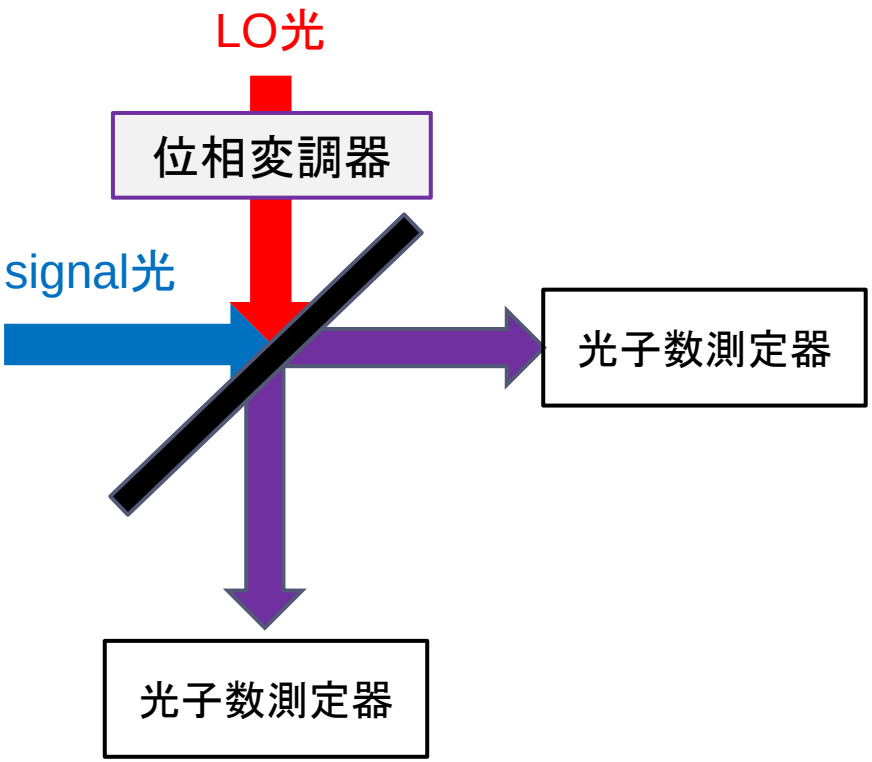
$\phi_L = \frac{\pi}{2}$の時 $\hat{p}_S = \frac{\hat{n}_1 - \hat{n}_2}{2|\alpha_L|}$

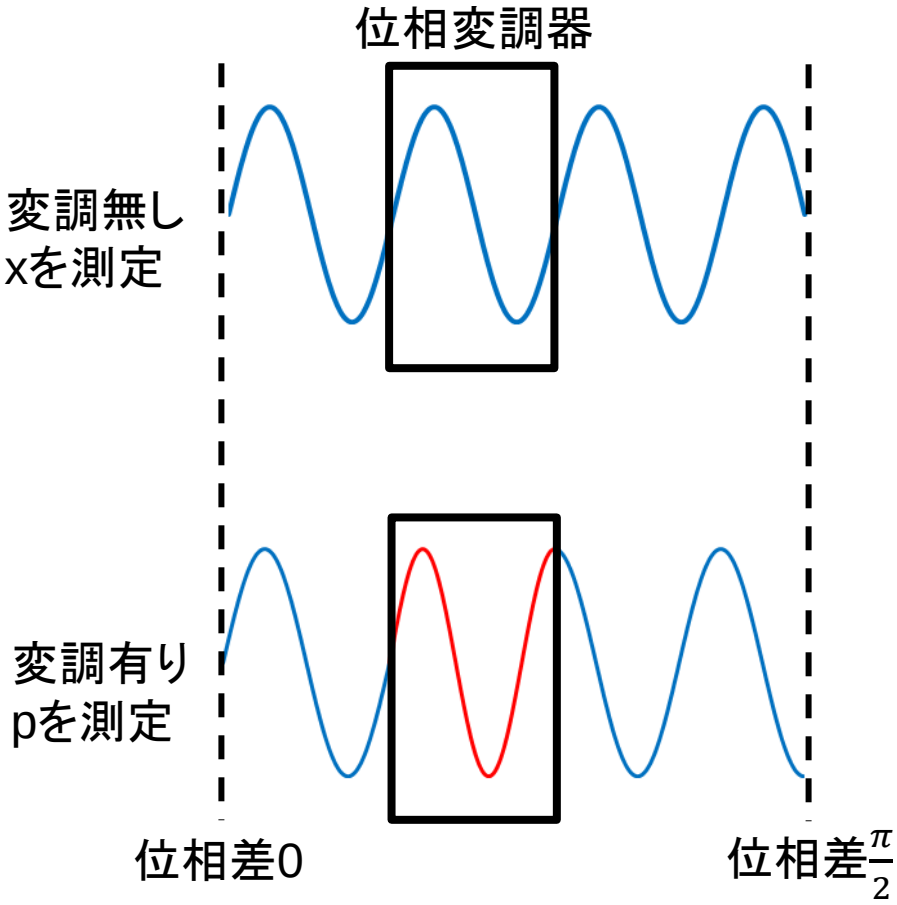
Bobが測定軸
x or p
を選んで測定

LO光の位相を
0 or $\frac{\pi}{2}$
で測定するか

LO光の位相変調で測定軸を選ぶ

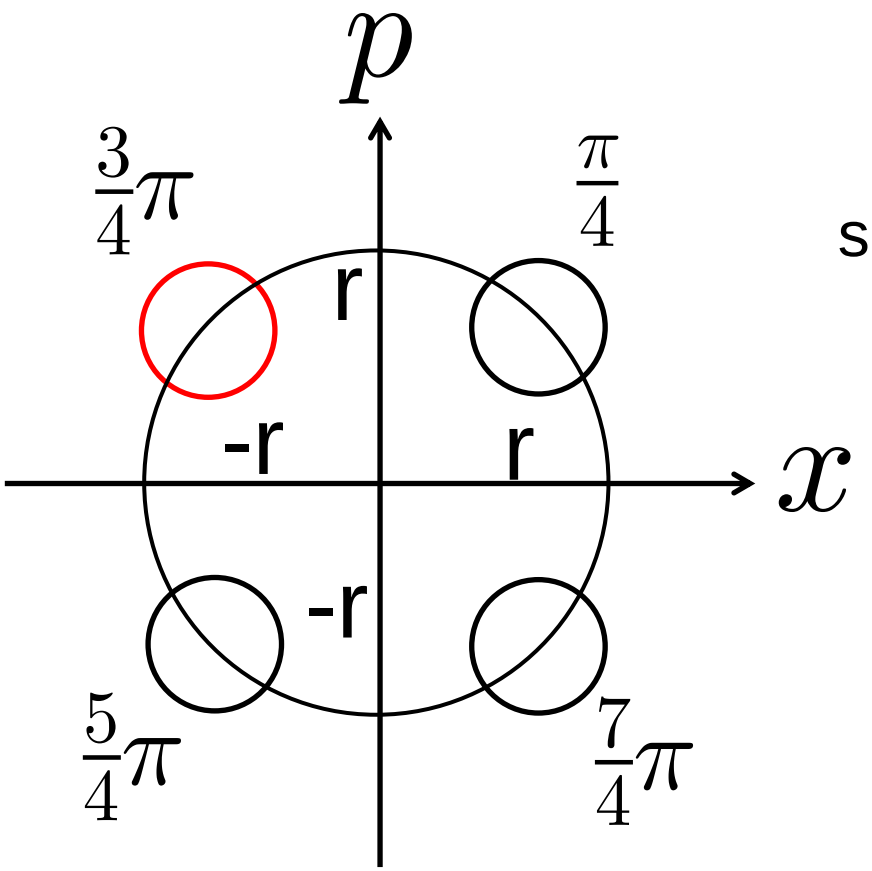
位相変調器：電圧を加えることで屈折率を操作できる装置

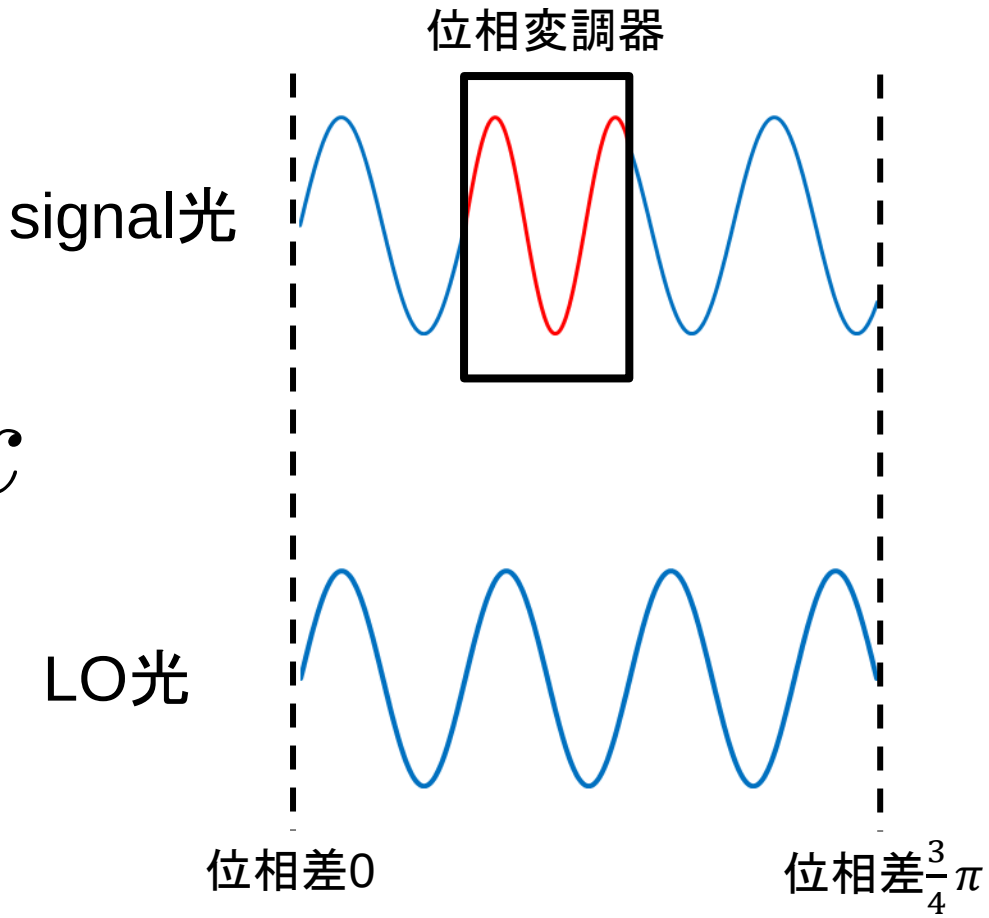




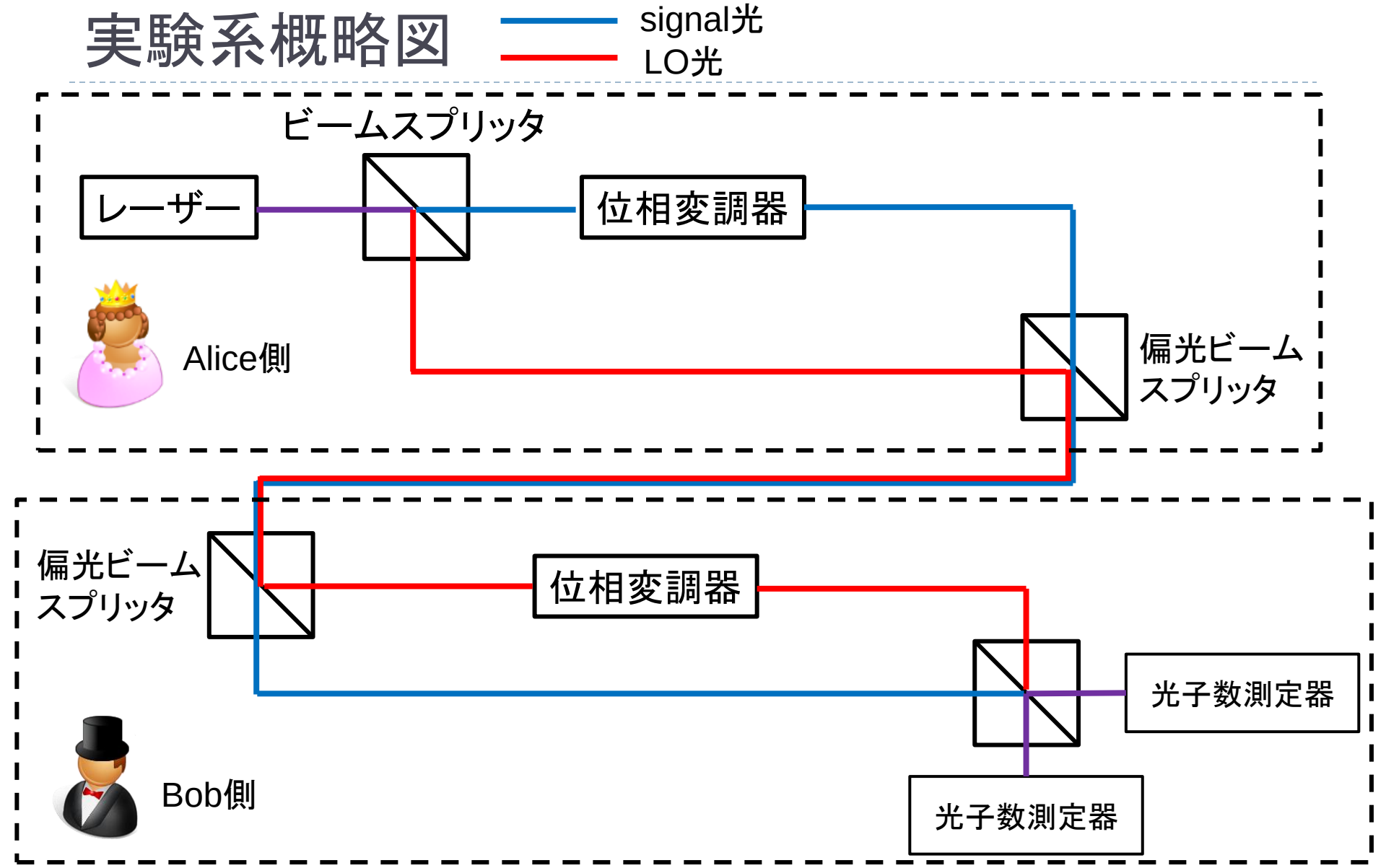
4つの量子状態の作り方

4つの状態を、signal光とLO光の相対的な位相によって状態を区別する





実験系概略図


signal光
LO光
ビームスプリッタ
レーザー
位相変調器
Alice側
偏光ビーム
スプリッタ
偏光ビーム
スプリッタ
位相変調器
光子数測定器
Bob側
光子数測定器

- 本論文の量子鍵配送について
  - 量子鍵配送の概要
  - 量子状態の説明
  - 鍵共有方法
  - 実験での操作
  - 量子鍵配送の安全性（安全な鍵を得るためには）

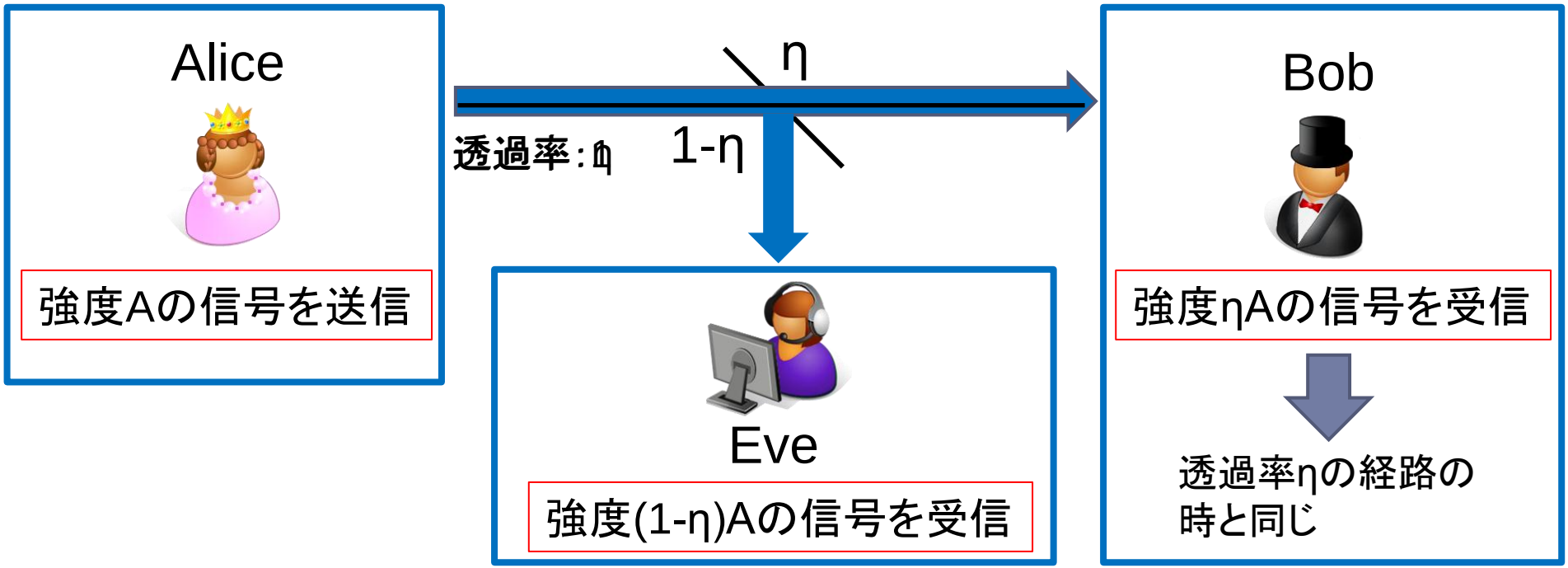
安全な鍵を得るためには

- AliceとBobは量子状態を送受信して、鍵の候補を得る
- Eveも盗聴行為を行うことで、鍵の候補についての情報を知っているかもしれない
  beam splitting attack

Eveの盗聴行為

透過率η：Aliceが送った信号の強度が、Bobに届いたときにどれだけの値になっているか
例）η=0.7:強度が70%になって届く　(η≦1)

Eve(盗聴者)：物理学に矛盾しない範囲で、理想的な盗聴行為を行えると仮定する
例)透過率1の通信路を用いることが可能



通信路に損失があるとEveは気付かれずに盗聴を行うことが出来る

安全な鍵を得るために

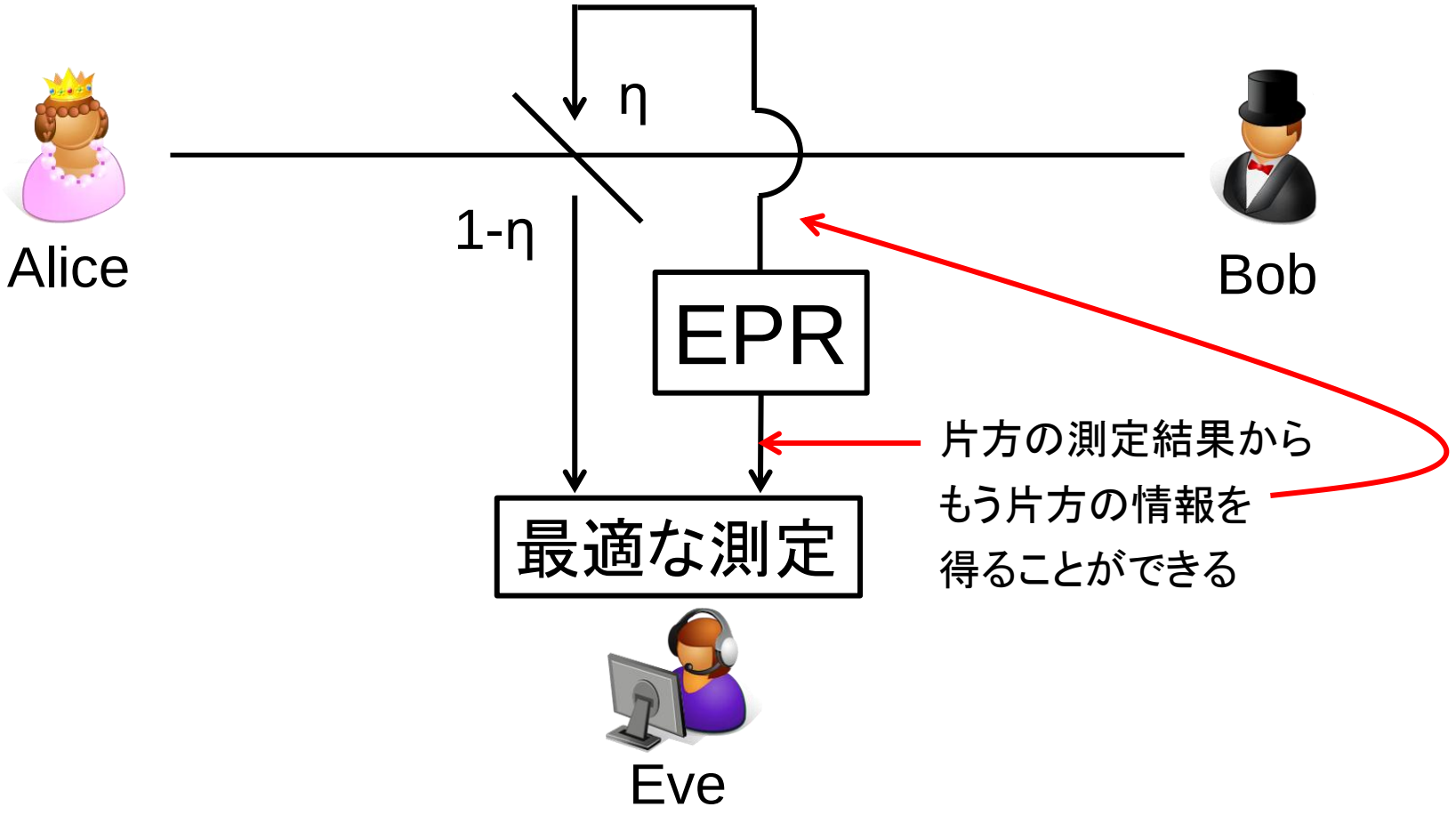
- 量子状態を送受信して、鍵の候補を得る
- Eveも盗聴行為を行うことで、鍵の候補についての情報を知っているかもしれない
  beam splitting attack
- 鍵の候補についてのEveの情報量の上限を見積もる（量子鍵配送の特徴）

Eveが最適な測定を行ったときに得る情報

entangling cloner attack

Eveの攻撃:entangling cloner attack

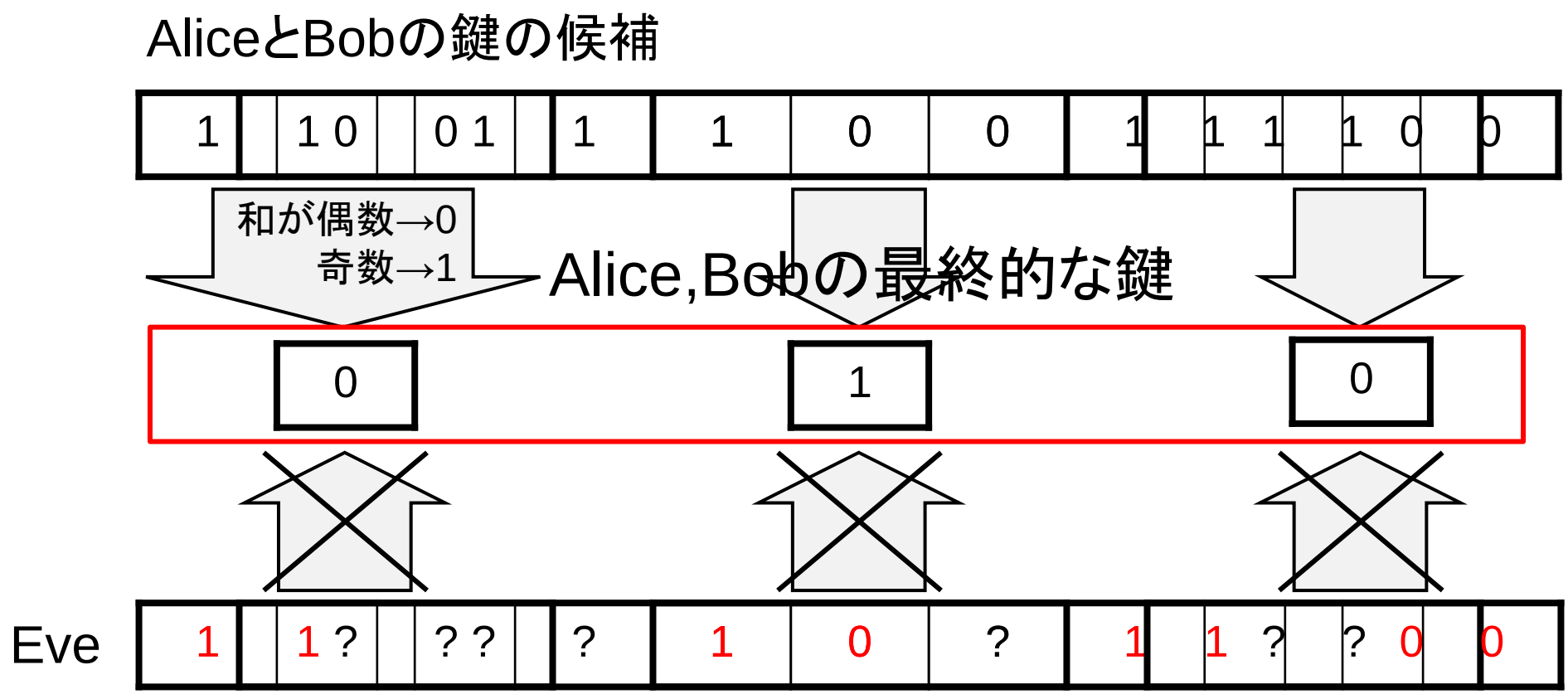
現実的な通信路(光ファイバ)では、信号が減衰するだけでなく雑音が乗ってしまう
これにより、量子的な揺らぎとは別に揺らぎが増えてしまう。その雑音を過剰雑音と呼ぶ



安全な鍵を得るために

- 量子状態を送受信して、鍵の候補を得る
- Eveも盗聴行為を行うことで、鍵の候補についての情報を知っているかもしれない
  beam splitting attack
- Eveが持つ鍵の候補についての情報量の上限を見積もる（量子鍵配送の最大の特徴）
  entangling cloner attack
- AliceとBobの情報量が、Eveの情報量より大きければ、秘匿性増強を行い、最終的な鍵についてEveの持つ情報量を任意に小さくすることが出来る。
- AliceとBobのみが知る安全な鍵を得る

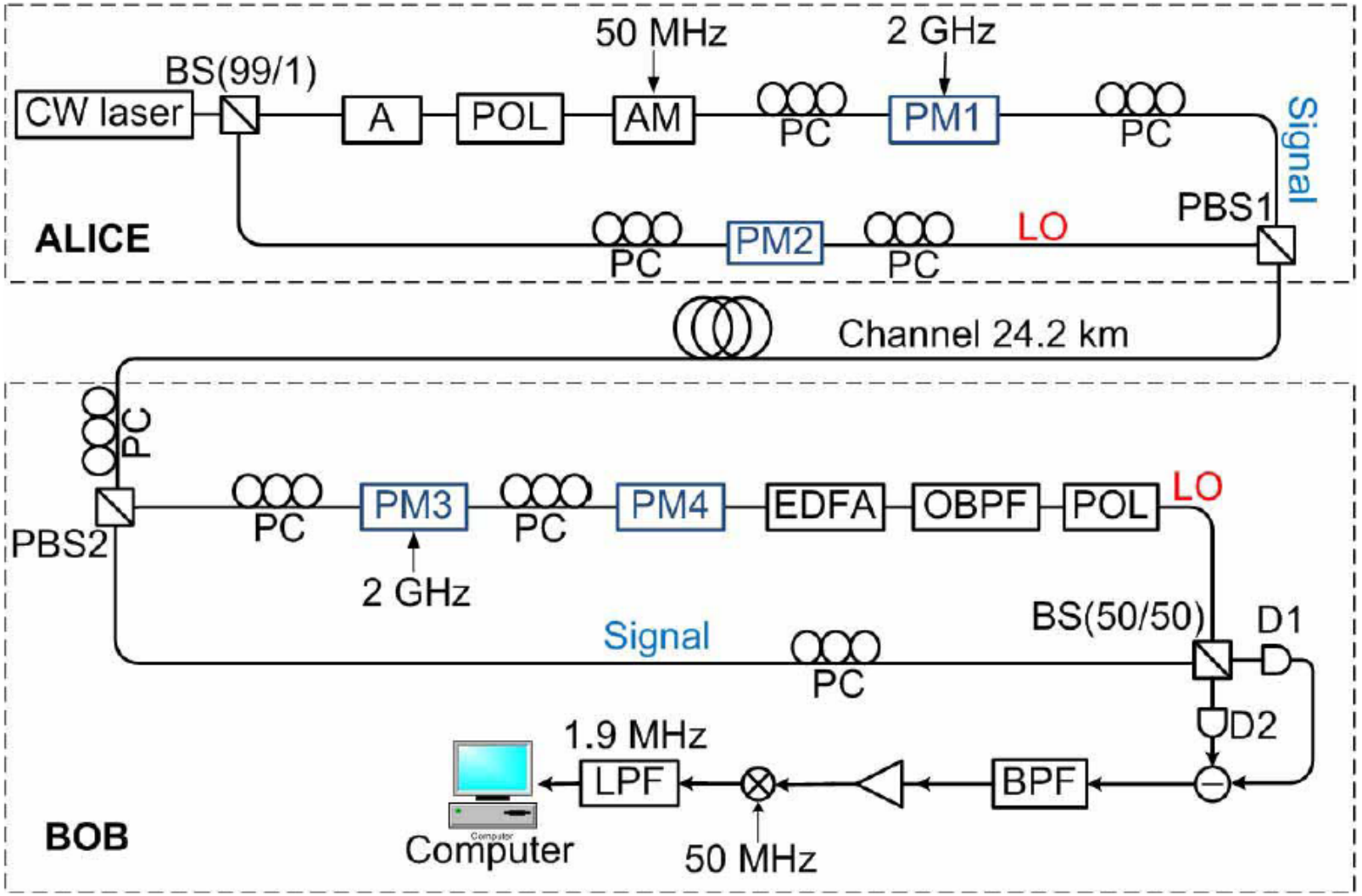
秘匿性増強の簡単な例


AliceとBobの鍵の候補
1 1 0 0 1 1 0 1 1 0 0 1 1 1 1 0 0
和が偶数→0
奇数→1
Alice,Bobの最終的な鍵
0 1 0
Eve
1 1 ? ? ? ? 1 0 ? 1 1 ? ? 0 0

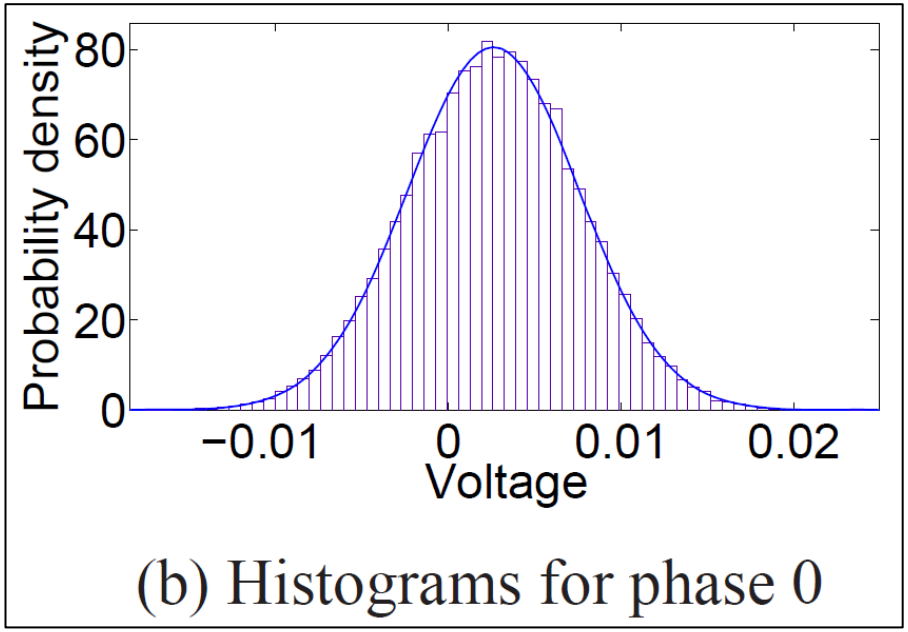
目次

- 暗号通信の予備知識
- 本論文の量子鍵配送について
- 本論文の実験について
- まとめ

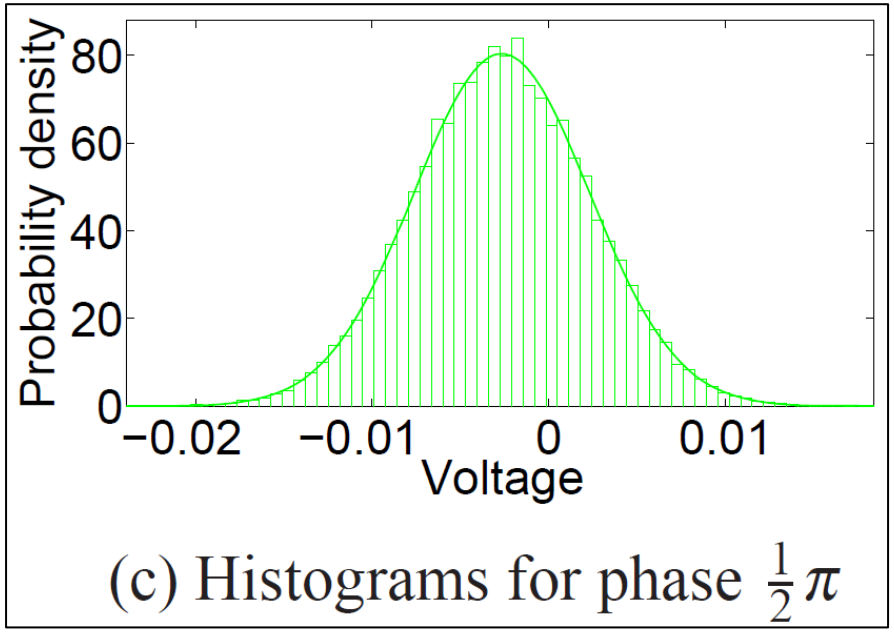
実験系


50 MHz
2 GHz
BS(99/1)
CW laser
A
POL
AM
PC
PM1
PC
Signal
ALICE
PC
PM2
PC
LO
PBS1
Channel 24.2 km
PC
PBS2
PC
PM3
PC
PM4
EDFA
OBPF
POL
LO
2 GHz
Signal
PC
BS(50/50)
D1
D2
1.9 MHz
LPF
BPF
BOB
Computer
50 MHz

実験結果：測定で得られた頻度分布



(b) Histograms for phase 0



(c) Histograms for phase $\frac{1}{2}\pi$

過剰雑音0.0024(コヒーレント状態の量子揺らぎで規格化)
経路透過率:0.327

鍵生成率

- 経路透過率:0.327
- 過剰雑音:0.0024
- Eveの攻撃:entangling cloner attackを仮定

秘匿性増強

安全な鍵を得た

鍵生成率:3.45kilobits/sec

まとめ

・量子鍵配送を用いると安全な通信ができる
・4つのコヒーレント状態を送り、鍵を共有した

実験結果
・通信距離:24.2km
・経路透過率:0.327
・過剰雑音:0.0024
・鍵生成率3.45kilobits/sec

ホモダイン検出を用いる実験では、最も良い結果
長距離通信が成功したことにより、実用化が期待されている