Experimental demonstration of long-distance continuous-variable quantum key distribution

長距離連続変数量子鍵配送の実証実験

Paul Jouguet , Sebastien Kunz-Jacques ,
Anthony Leverrier , Philippe Grangier & Eleni Diamanti
Nature Photonics, **7**, 3678 (2013).

平野研究室10-041-045　長谷川　正義

論文の目的

従来の連続変数量子鍵配送(CVQKD)

- 長距離に向かない…複雑な誤り訂正など
- 安全性に問題…有限長の効果より

光ファイバーを用いた長距離にわたる
CVQKDの実現可能性を示す

発表の流れ

- 暗号通信
  量子暗号通信　ワンタイムパッド方式
  量子鍵配送

- 長距離連続変数量子鍵配送
  離散変数方式と連続変数方式
  量子通信：ガウス変調プロトコル
  ショット雑音と過剰雑音
  ビット値の揃え方
  有限長の効果
  秘密鍵生成率

- 実験
- まとめ

現代暗号

- 暗号の用途：電子化された情報の秘匿
- 安全性の根拠：解読に膨大な時間がかかる

例　素因数分解

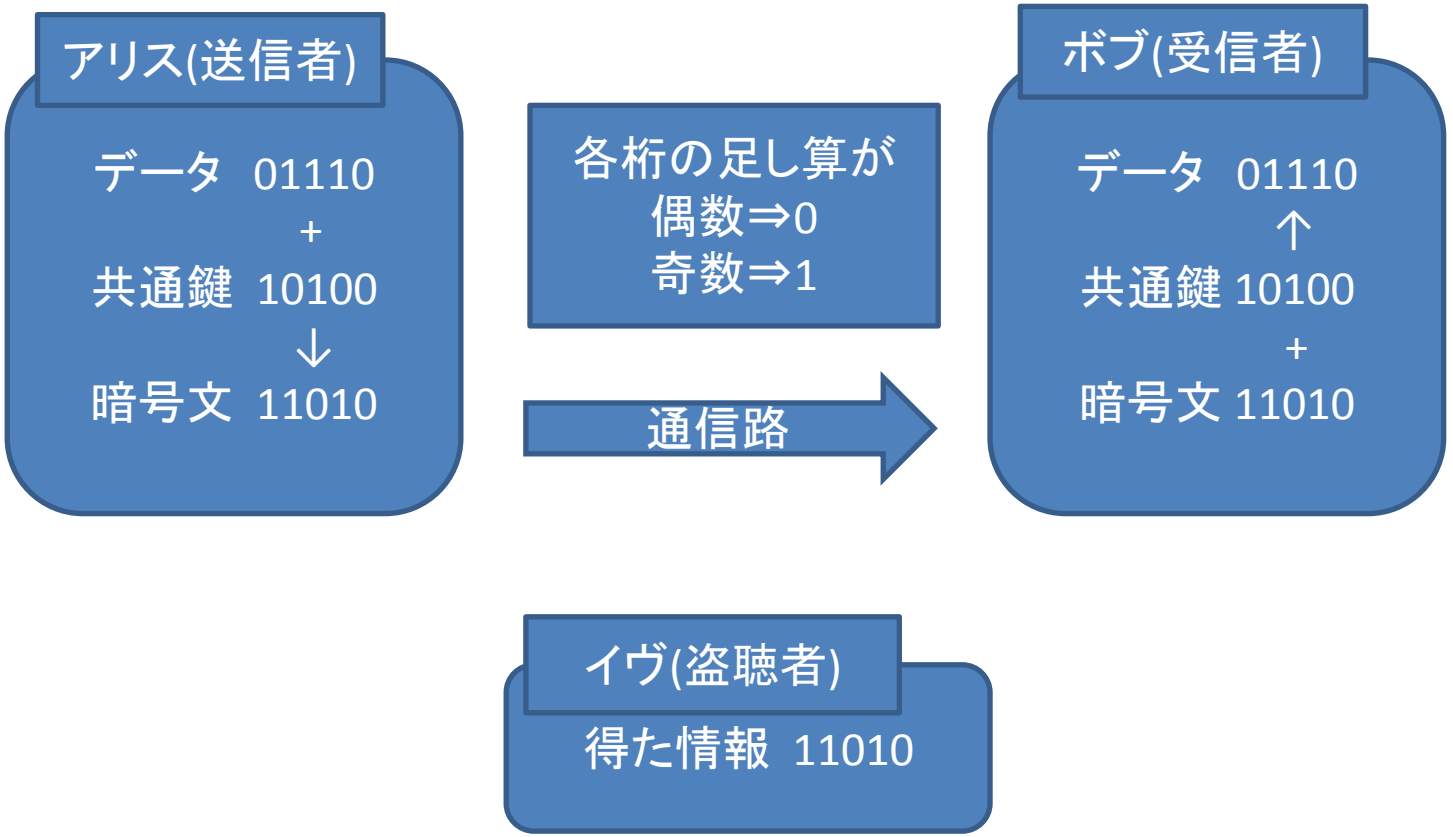
191207=367×521　　⇒時間がかかる!

しかし…

計算量的安全性は“計算能力の向上”や“効率的なアルゴリズムの開発“によって破られる可能性がある！

理論的に安全が証明されているワンタイムパッド暗号方式

ワンタイムパッド暗号方式

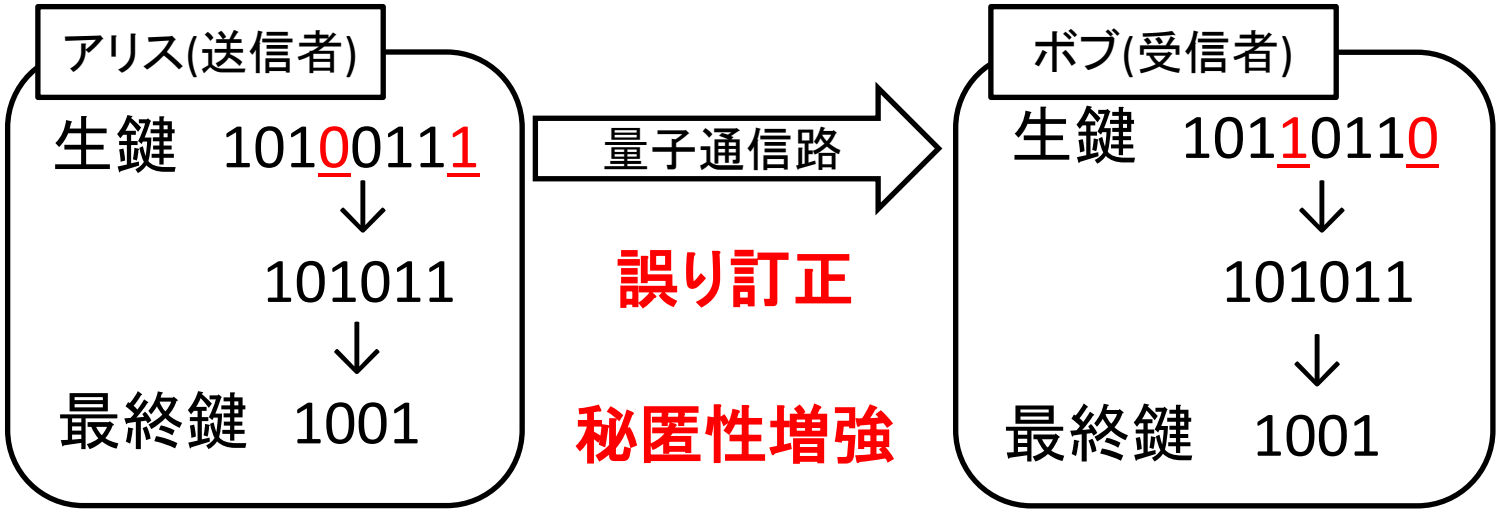


イヴは共通鍵がわからないため元の情報がわからない

その鍵を共有する方法が量子鍵配送

量子鍵配送(Quantum Key Distribution)

- 誤り訂正と秘匿性増強



雑音(量子状態の不確定性・装置の不完全さ・盗聴攻撃)

↓

ビット列に誤りがでる

量子鍵配送の種類

- 離散変数（Discrete Variable:DV）方式

BB84のように、単一光子に情報をのせ受信者は単一光子検出器にて情報を読み取る

単一光子源や単一光子検出器の実現が困難

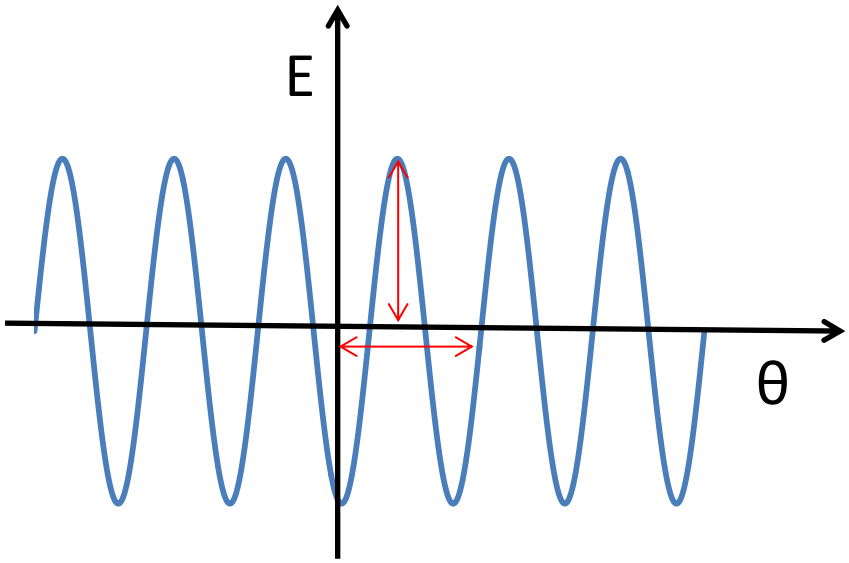
- 連続変数（Continuous Variable:CV）方式

コヒーレント光を直交振幅変調し、ホモダイン検出器により受信を行うため特殊な光源は不要

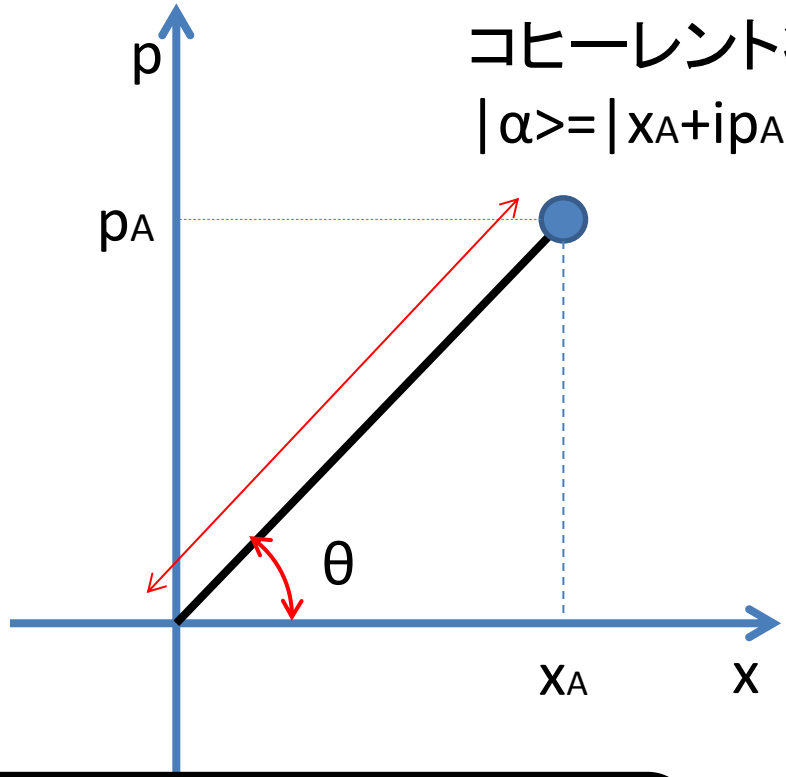
現代の一般的な技術で実装可能

連続変数方式：ガウス変調プロトコル①

送信者アリス



アリスの送信状態



コヒーレント状態

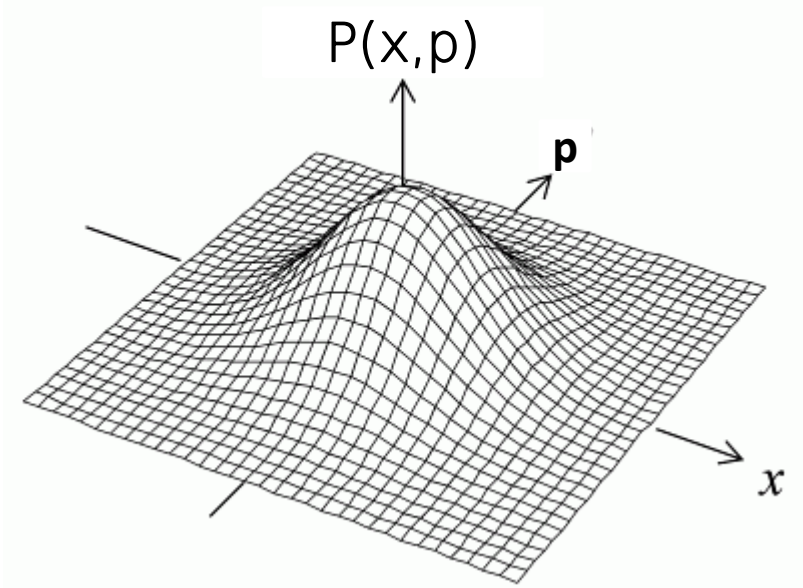
$|\alpha\rangle = |x_A + ip_A\rangle$

・パルス状のレーザーを減衰、位相と振幅を変調器で調整

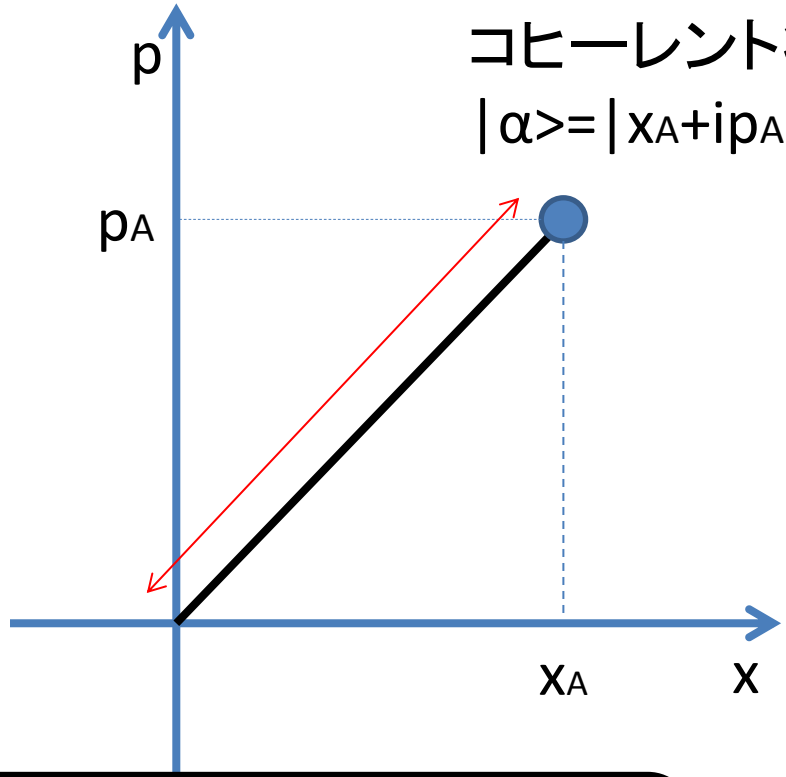
→
- 直交位相振幅値(xA,pA)の選択と同様
- コヒーレント状態$|\alpha\rangle = |x_A + ip_A\rangle$の信号光を量子通信路で送信

連続変数方式：ガウス変調プロトコル①

送信者アリス



アリスの送信状態



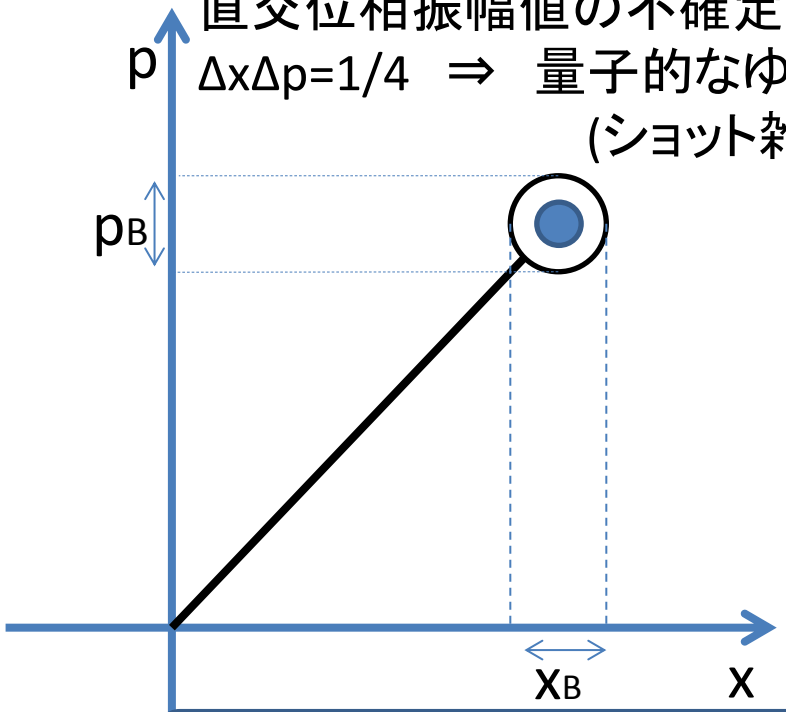
コヒーレント状態
$|\alpha\rangle = |x_A + ip_A\rangle$

・パルス状のレーザーを減衰、位相と振幅を変調器で調整
→ 直交位相振幅値(xA,pA)の選択と同様
→ コヒーレント状態$|\alpha\rangle = |x_A + ip_A\rangle$の信号光を量子通信路で送信
・原点を中心にガウス分布するように変調する

連続変数方式：ガウス変調プロトコル②

受信者：ボブ

コヒーレント状態の
直交位相振幅値の不確定性関係
$\Delta x \Delta p = 1/4$ ⇒ 量子的なゆらぎ
(ショット雑音)



送信状態　　測定

(x_A, p_A) ， x_B or p_B

(x_A, x_B) or (p_A, p_B)

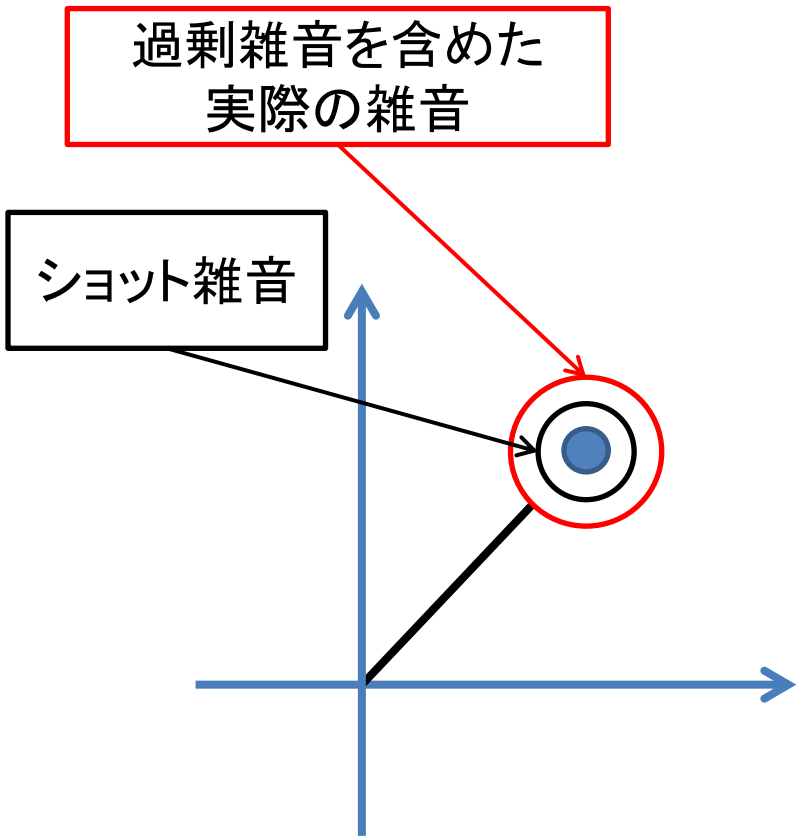
$x_B = x_A + \varepsilon$
$p_B = p_A + \varepsilon$
ε：雑音

雑音が入ってしまうため
データが一致しない

AliceとBobで相互に関連のあるデータを共有

雑音について

- ショット雑音と過剰雑音



$$(\Delta x_{\mathrm{obs}})^2 \geq (\Delta x)^2$$

実際の分散　コヒーレント状態の分散

$$(\Delta x_{\mathrm{obs}})^2 = (1+\delta)(\Delta x)^2$$

過剰雑音δ

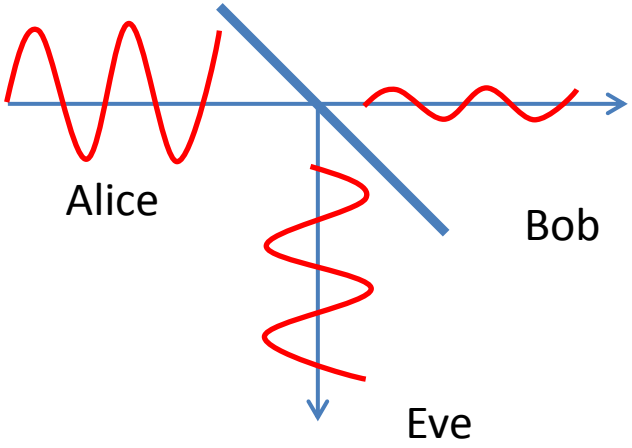
$$\delta \equiv \frac{(\Delta x_{\mathrm{obs}})^2}{(\Delta x)^2} - 1$$

ビット値の揃え方

direct reconciliation

- Aliceのビット値に合わせる方法

イヴはアリスの情報を推測する必要



reverse reconciliation

- Bobのビット値に合わせる方法

イヴはアリスとボブの情報の二つを推測する必要

有限長の効果

- なぜ有限長を考えるか…無限の精度でパラメーター推定し続けることは実際には不可能

データのパラメーターを調べる
過剰雑音がわかる
盗聴者の知りえる情報の上限がわかる
安全性の評価ができる

鍵生成率の減少

- 秘密鍵生成率

I_{AB}:アリスとボブで共有した情報
χ_{BE}:盗聴者イヴが手に入れられる情報

$$\Delta I = I_{AB} - \chi_{BE}$$

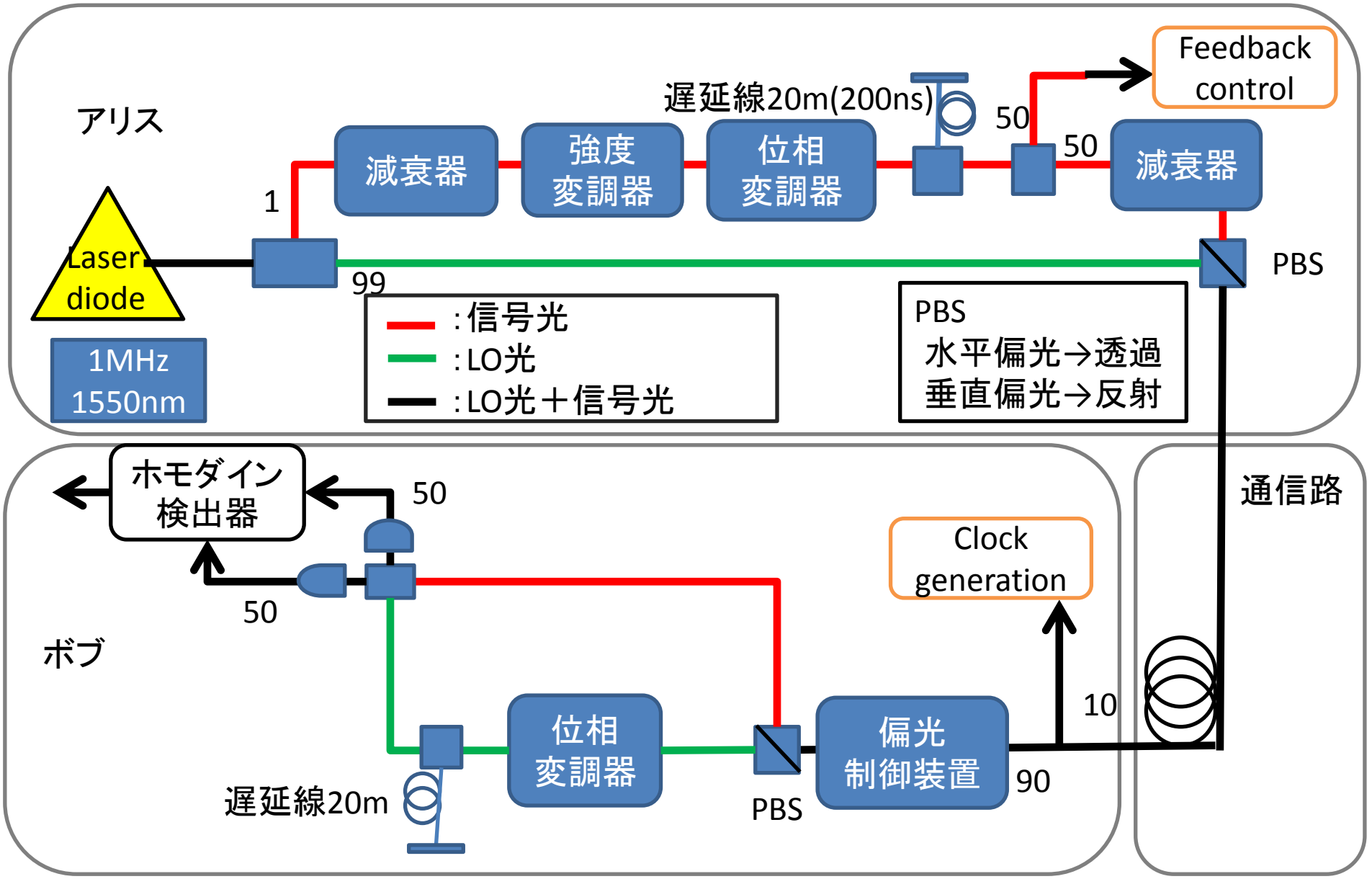
- 誤り訂正効率を考慮した秘密鍵生成率

$$\Delta I = \beta I_{AB} - \chi_{BE}$$

β:誤り訂正効率
多次元リコンシリエーションプロトコルにより　β=0.95

実験

実験装置図


アリス
Laser diode
1MHz
1550nm
1
99
減衰器
強度
変調器
位相
変調器
遅延線20m(200ns)
50
50
減衰器
Feedback
control
PBS
:信号光
:LO光
:LO光＋信号光
PBS
水平偏光→透過
垂直偏光→反射
ボブ
ホモダイン
検出器
50
50
Clock
generation
通信路
10
90
偏光
制御装置
PBS
位相
変調器
遅延線20m

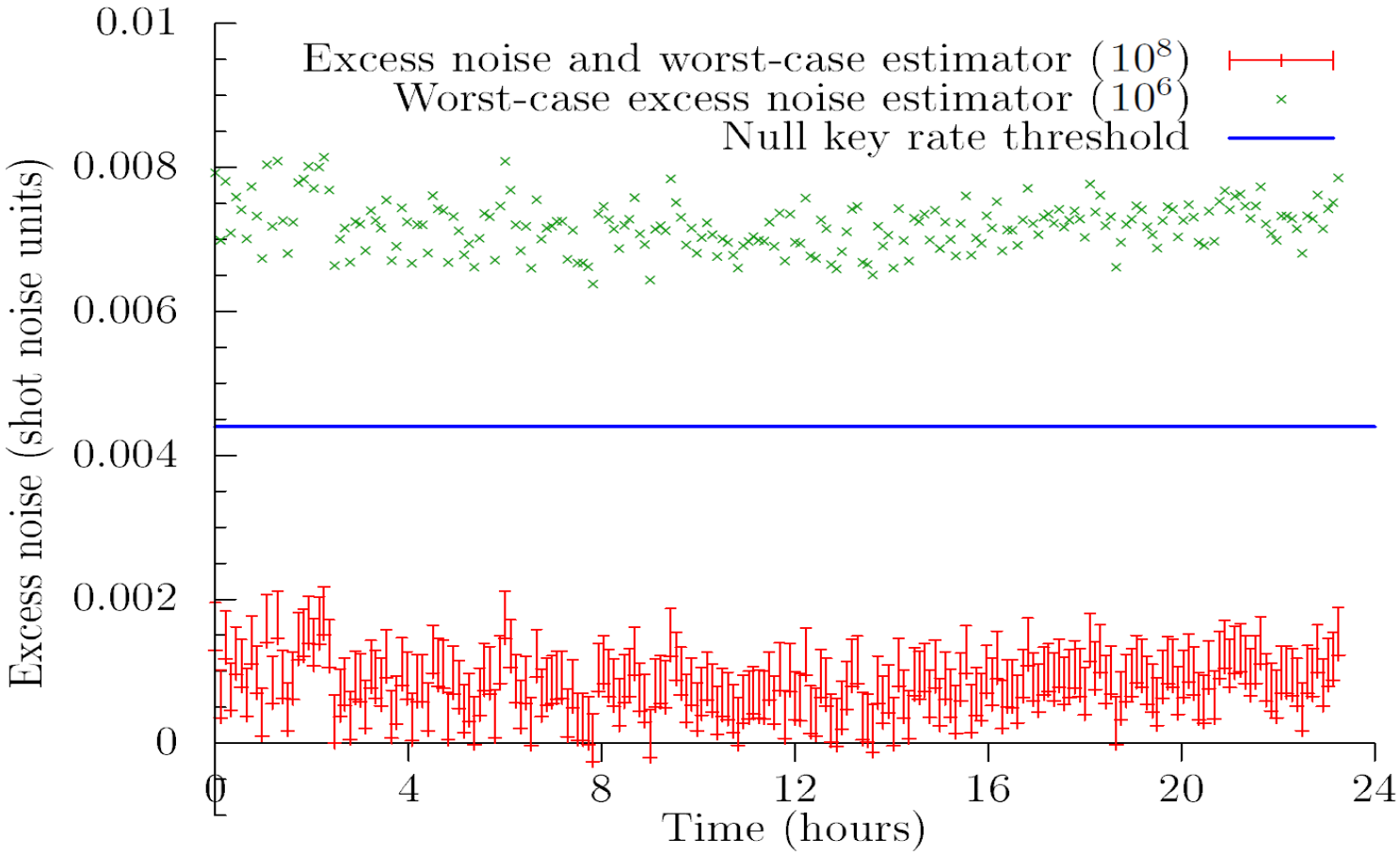
長距離実装を可能にした改善点

- 改善されたfeedback により、システムが安定

- 偏波制御により通信路後の偏波の乱れの抑制

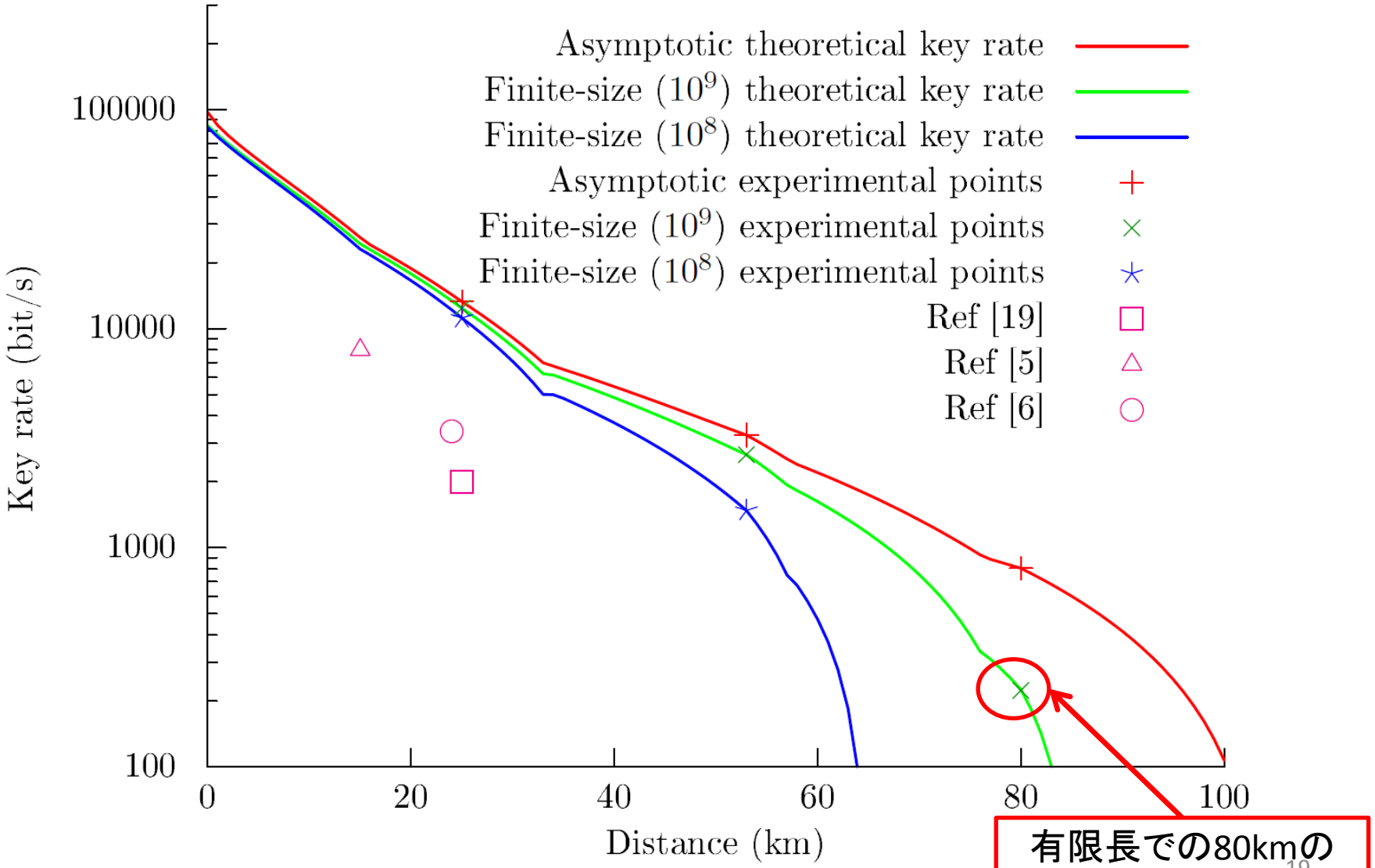
過剰雑音の低減

通信路53kmで24時間
過剰雑音を計測した結果



※データ長が10^6では鍵生成できない

誤り訂正と秘匿性増強後の鍵生成率



まとめ

有限長の効果を含んだ80kmでの連続変数量子鍵配送に成功

- ガウス変調量子鍵配送プロトコルにおいて
- 過剰雑音の低減
- 低い信号対雑音比での高い誤り訂正効率
- データ数増加による過剰雑音の推定精度向上

質問対策

アリスのとボブの共有した情報

- I_{AB}とは理論上できる鍵生成率

- $I_{AB} = 1 - H_{ER}$
- H_{ER}=h(e_{bit})
  ただし h(x):=-xlog_2x-(1-x) log_2(1-x)

- 仮想的な2値変調通信路

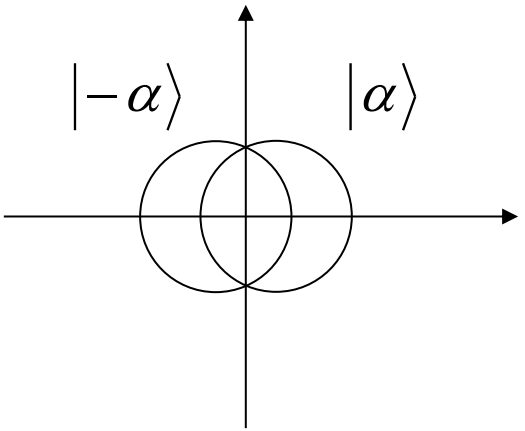
input: $x=\pm 1 \rightarrow$ output: $y = x + z \quad z \sim N(0,\sigma^2)$,

ボブはuとtを

$u=y/|y|, \quad t=|y|$ とすると

ボブは

$$v = \begin{cases} t & \text{if } x = 1 \\ -t & \text{if } x = -1 \end{cases}$$ と計算する



リバース通信路では

input: $u=\pm 1 \rightarrow$ output: $v = u + w \quad w=\mathrm{sgn}(xy)z \sim N(0,\sigma^2)$

多次元リコンシリエーションプロトコル

input: $\boldsymbol{x}$ → output: y

$\boldsymbol{u}$: ランダムな2値ベクトル, とすると

リバース通信路では、ボブ側から

input: $\mathbf{r}=\mathbf{y}\cdot\mathbf{u}$ → output: $\boldsymbol{v}=\boldsymbol{r/x}=\boldsymbol{y}\cdot\boldsymbol{u/x}$

がアリスに送られる

※ベクトルは8元数を用いる