

High-rate measurement-device-independent quantum cryptography

高レートでの測定装置無依存量子暗号

Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri,
Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias
Gehring, Christian S. Jacobsen, and Ulrik L. Andersen

Nature Photonics, **9**, 397-402 (2015)

平野研究室 14-041-022 柄澤真也

本論文の概要

連続変数方式(CV)で
測定装置無依存量子鍵配送(MDI-QKD)を行い、
従来のMDI-QKDよりも
3桁高い鍵生成率を実現した。

CV: Continuous Variable

MDI: Measurement Device Independent

QKD: Quantum Key Distribution

発表の流れ

1.論文の背景

- 1.1 測定装置無依存量子鍵配送 (MDI-QKD)
- 1.2 連続変数方式 (CV)
- 1.3 直交位相振幅とコヒーレント状態
- 1.4 ホモダイン検出

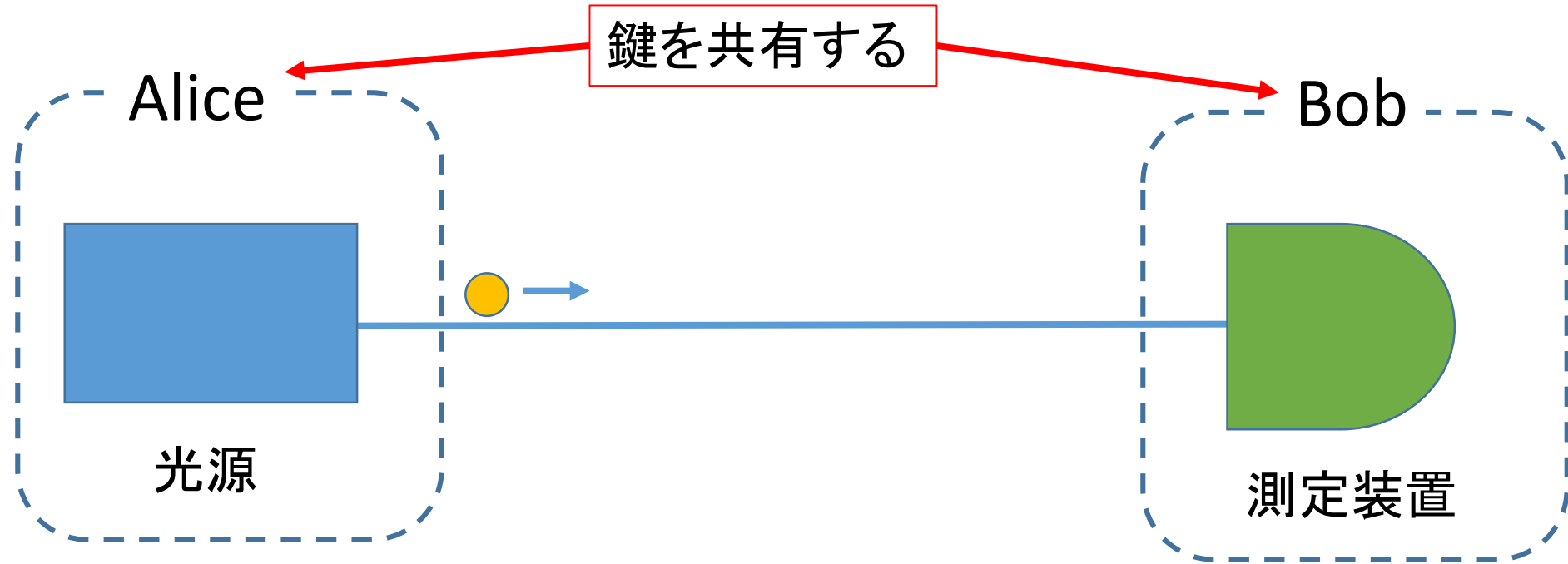
2.本論文の内容

- 2.1 プロトコル (CV MDI-QKD)
現実的なCV MDI-QKD
- 2.2 秘密鍵生成率
- 2.3 実験内容
- 2.4 実験結果

3.まとめ

1.1 測定装置無依存量子鍵配送 とは

BB84等の通常の量子鍵配送の場合

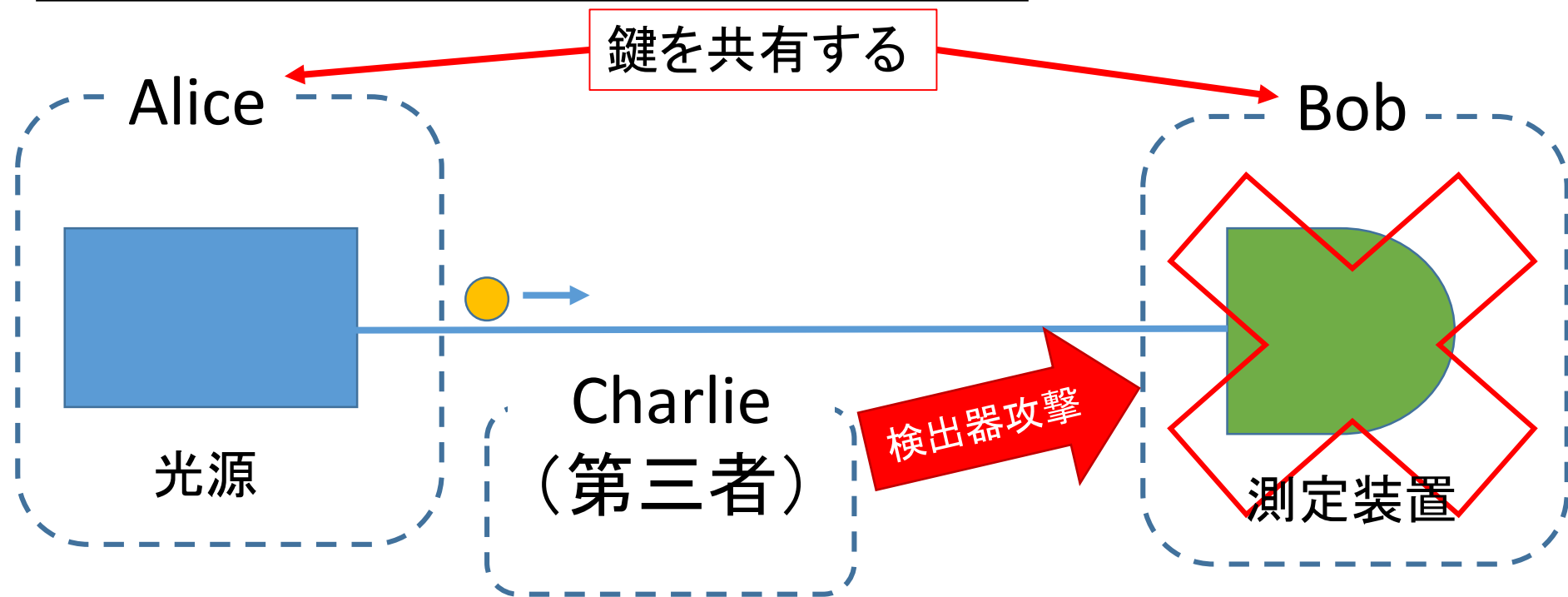


Aliceが光源を持ち、Bobが測定装置を持っている。

測定装置が正常に機能していることを仮定して
量子鍵配送の安全性は理論的に証明されている。

1.1 測定装置無依存量子鍵配送 とは

BB84等の通常の量子鍵配送の場合

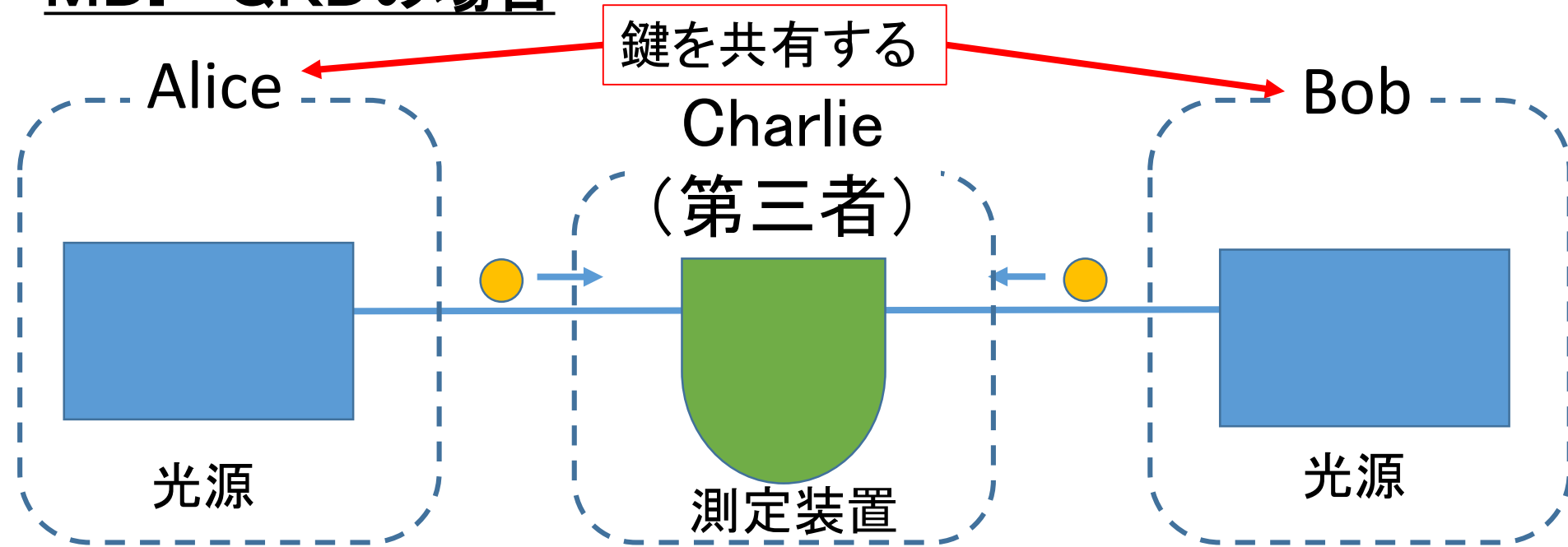


第三者に測定装置が攻撃され、予想外の方法で情報が洩れる可能性がある。

→現実の装置の安全性を理論的に証明できない

1.1 測定装置無依存量子鍵配送 とは

MDI-QKDの場合



AliceとBobは光源を持ち、
測定装置は第三者のCharlieに預けてしまう。
測定装置が正常に機能していることを仮定しなくても
量子鍵配送の安全性を理論的に証明できる。

Laser:レーザー光源
RNG:乱数生成器
EOM:電気光学変調器
BS:ビームスプリッター
PD:光検出器

測定装置無依存量子鍵配送

Measurement Device Independent-QKD:MDI-QKD

発表の流れ

1.論文の背景

1.1 測定装置無依存量子鍵配送 (MDI-QKD)

1.2 連続変数方式 (CV)

1.3 直交位相振幅とコヒーレント状態

1.4 ホモダイン検出

2.本論文の内容

2.1 プロトコル (CV MDI-QKD)

現実的なCV MDI-QKD

2.2 秘密鍵生成率

2.3 実験内容

2.4 実験結果

3.まとめ

1.2 連続変数方式

量子鍵配送の検出方法は、二つに分かれる。

- 離散変数方式 (DV)

単一光子検出を行う

- 連続変数方式 (CV)

ホモダイン検出を行う

連続変数方式は、**コヒーレント状態**の光を用い、その**直交位相振幅**の値から鍵を生成する。

発表の流れ

1.論文の背景

1.1 測定装置無依存量子鍵配送 (MDI-QKD)

1.2 連続変数方式 (CV)

1.3 直交位相振幅とコヒーレント状態

1.4 ホモダイン検出

2.本論文の内容

2.1 プロトコル (CV MDI-QKD)

現実的なCV MDI-QKD

2.2 秘密鍵生成率

2.3 実験内容

2.4 実験結果

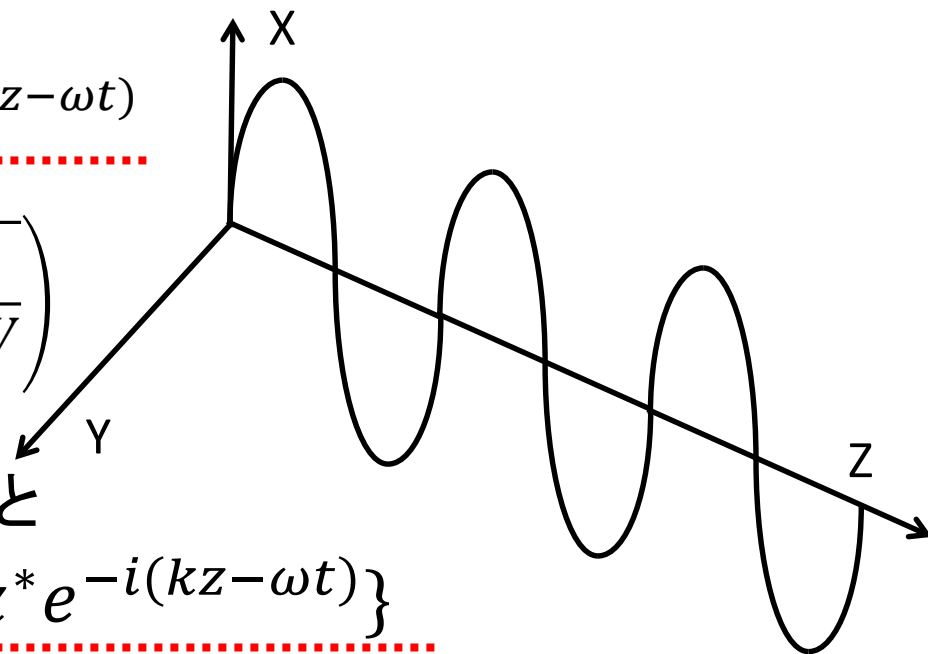
3.まとめ

電場の量子化と直交位相振幅

$$E_x(z, t) = E_0 e^{i(kz - \omega t)} + E_0^* e^{-i(kz - \omega t)}$$

A 次元を表す係数 $\left(A = \sqrt{\frac{\hbar\omega}{2\epsilon_0 V}} \right)$
 α, α^* 規格化された複素数
 とおくと

$$E_x(z, t) = A \{ \alpha e^{i(kz - \omega t)} + \alpha^* e^{-i(kz - \omega t)} \}$$



電磁場を量子力学的調和振動子の集まりとして量子化する

$$\alpha, \alpha^* \longrightarrow \hat{a}, \hat{a}^\dagger$$

$$[\hat{a}, \hat{a}^\dagger] = 1 \text{ が成立する}$$

$$\hat{E}_x(z, t) = A \{ \hat{a} e^{i(kz - \omega t)} + \hat{a}^\dagger e^{-i(kz - \omega t)} \}$$

電場を、生成演算子と消滅演算子で書き表せる

電場の量子化と直交位相振幅

直交位相振幅演算子を次のように定義する

$$\begin{cases} \hat{q} = (\hat{a} + \hat{a}^\dagger) \\ \hat{p} = -i(\hat{a} - \hat{a}^\dagger) \end{cases} \quad \begin{pmatrix} \hat{a} = \frac{1}{2}(\hat{q} + i\hat{p}) \\ \hat{a}^\dagger = \frac{1}{2}(\hat{q} - i\hat{p}) \end{pmatrix}$$

直交位相振幅演算子はエルミートである

交換関係

$$[\hat{q}, \hat{p}] = 2i$$

不確定性関係

$$\Delta q \Delta p \geq 1$$

先ほどの式を変形すると

$$\hat{E}_x(z, t) = A\{\hat{q} \cos(kz - \omega t) - \hat{p} \sin(kz - \omega t)\}$$

\hat{q} はcos成分の振幅
 \hat{p} はsin成分の振幅

コヒーレント状態と直交位相振幅

生成演算子 \hat{a}^\dagger

消滅演算子 \hat{a}

$$[\hat{a}, \hat{a}^\dagger] = 1$$

消滅演算子の固有状態をコヒーレント状態と定義する。

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \quad (\alpha \text{は複素数})$$

コヒーレント状態において直交位相振幅は

よって

$$(\Delta q)^2 = 1$$

$$(\Delta p)^2 = 1$$

$$\Delta q \Delta p = 1$$

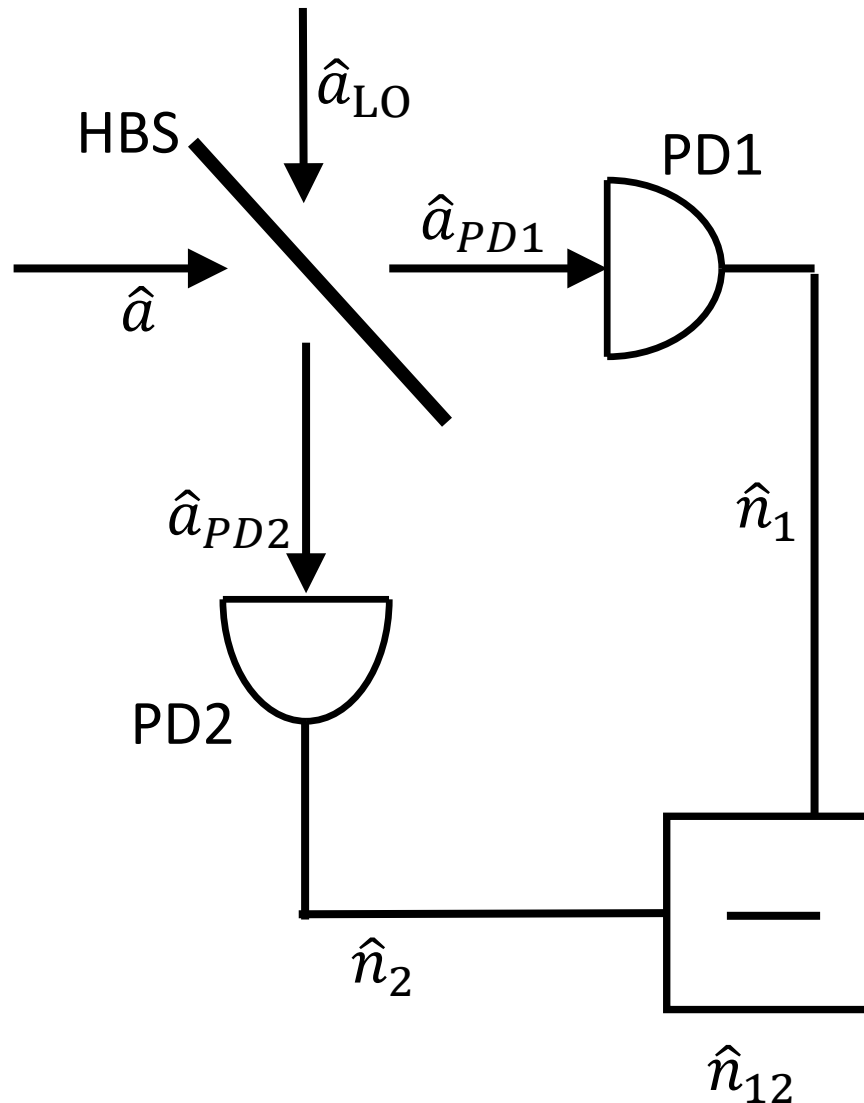
$$\begin{cases} \hat{q} = (\hat{a} + \hat{a}^\dagger) \\ \hat{p} = -i(\hat{a} - \hat{a}^\dagger) \end{cases}$$

となり、最小不確定状態となっている。

ホモダイン検出

信号光とLO光を重ね合わせてできる2つの出力の差を検出する方法

検出のために用いる光



コヒーレント状態のLO光を用いる。

LO光の状態 $|\omega\rangle$ 、位相 θ とする。

観測される光子数演算子 \hat{n}_{12} は

$$\begin{aligned}\hat{n}_{12} &= \hat{n}_1 - \hat{n}_2 \\ &= \hat{a}_{PD1}^\dagger \hat{a}_{PD1} - \hat{a}_{PD2}^\dagger \hat{a}_{PD2} \\ &= \hat{a}^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}\end{aligned}$$

$\hat{a} = \frac{1}{2}(\hat{q} + i\hat{p})$ のとき

LO光の状態 $|\omega\rangle \rightarrow \omega = |\omega|e^{i\theta}$ を用いると

$$\hat{n}_{12} = |\omega|(\hat{q} \cos \theta + \hat{p} \sin \theta)$$

$\theta = 0$ のとき \hat{q}

$\theta = \pi/2$ のとき \hat{p} を測定できる

LO光の位相を変えることで、**信号光の直交位相振幅のどちらかを測定できる**

発表の流れ

1.論文の背景

- 1.1 測定装置無依存量子鍵配送 (MDI-QKD)
- 1.2 連続変数方式 (CV)
- 1.3 直交位相振幅とコヒーレント状態
- 1.4 ホモダイン検出

2.本論文の内容

2.1 プロトコル (CV MDI-QKD)

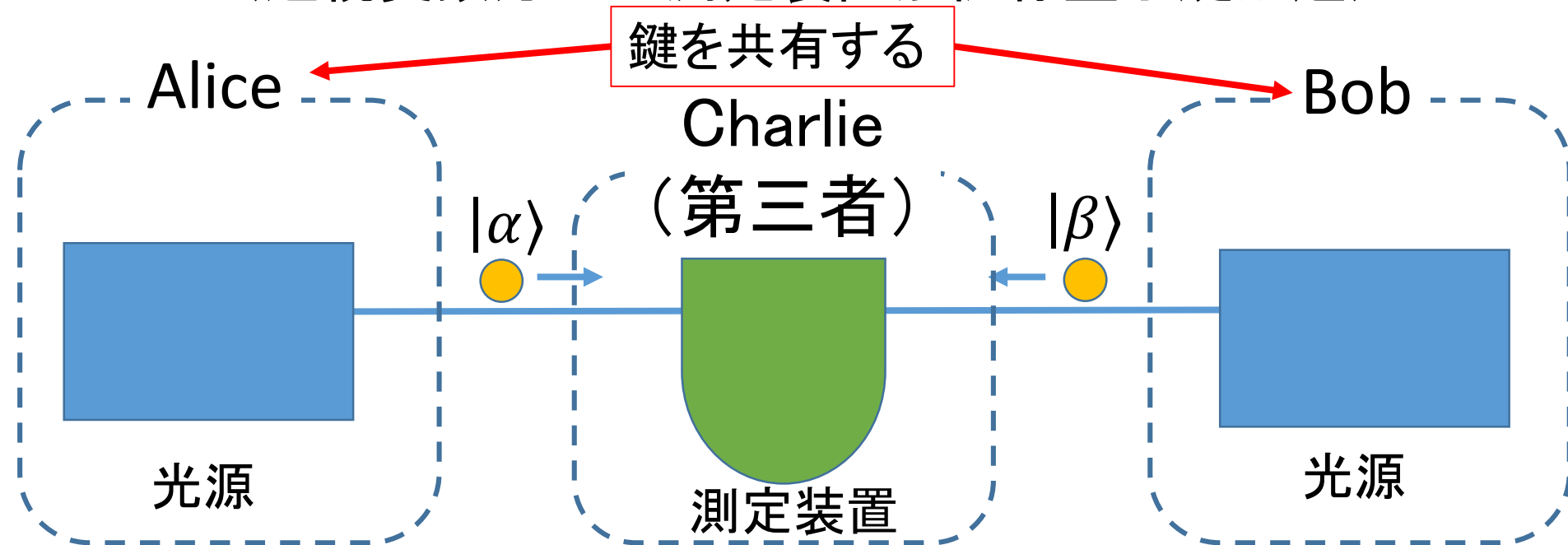
現実的なCV MDI-QKD

- 2.2 秘密鍵生成率
- 2.3 実験内容
- 2.4 実験結果

3.まとめ

2.1 プロトコル(CV MDI-QKD)

(連続変数方式の測定装置無依存量子鍵配送)

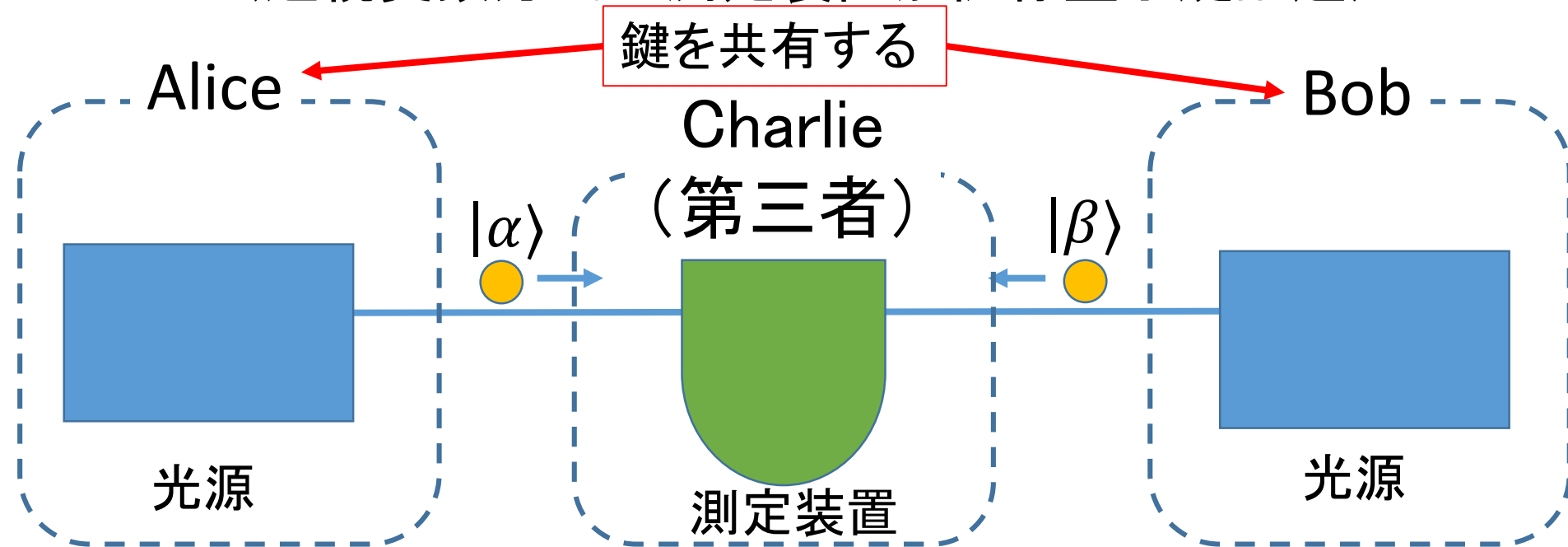


CV MDI-QKDの手順

- ① Alice、Bobはコヒーレント状態 $|\alpha\rangle$ 、 $|\beta\rangle$ をそれぞれCharlieに送る。
- ② Charlieは2つの光を干渉させ、出力の直交位相振幅(\hat{q}_- と \hat{p}_+)をホモダイン検出で観測する。
- ③ $\gamma = (q_- + ip_+)/\sqrt{2}$ をAliceとBobに教え、鍵を生成する。

2.1 プロトコル(CV MDI-QKD)

(連続変数方式の測定装置無依存量子鍵配送)



① Alice、Bobはコヒーレント状態 $|\alpha\rangle$ 、 $|\beta\rangle$ をそれぞれCharlieに送る。

①-1

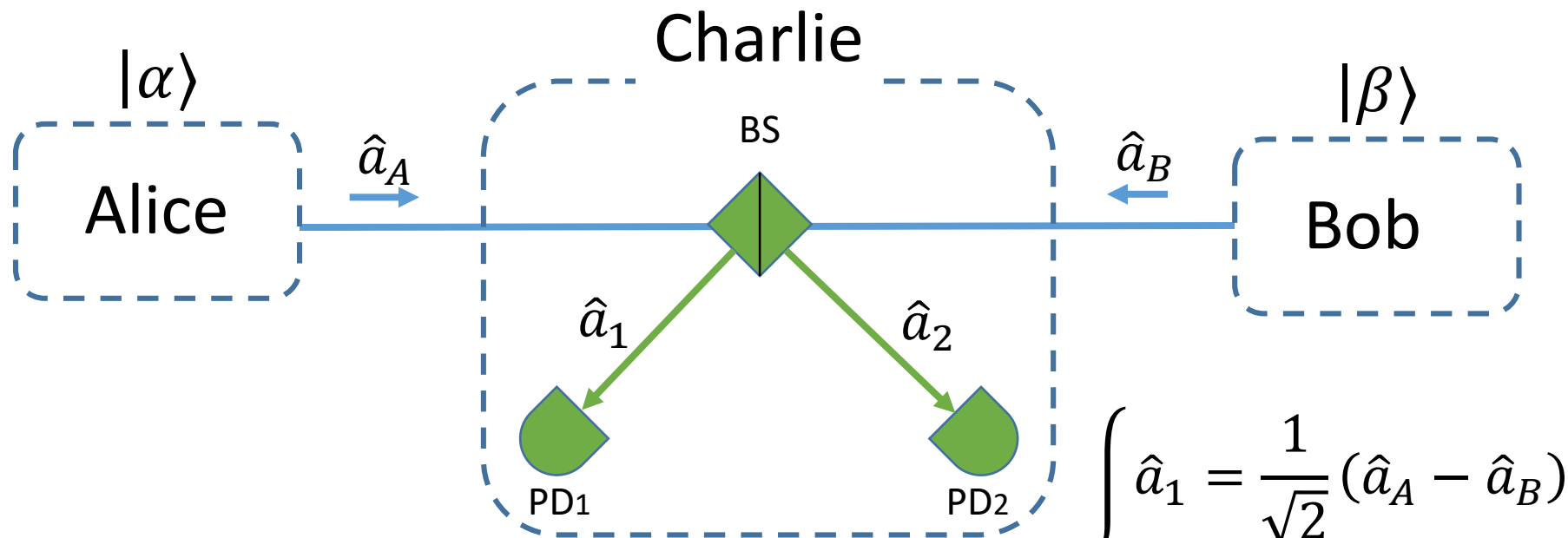
Alice、Bobは**複素数 α 、 β** をそれぞれ
ガウス分布するように**ランダムに選ぶ**

①-2

コヒーレント状態 $|\alpha\rangle$ 、 $|\beta\rangle$ をつかって、それぞれCharlieに送る

2.1 プロトコル(CV MDI-QKD)

② Charlieは2つの光を干渉させ、直交位相振幅(\hat{q}_- と \hat{p}_+)をホモダイン検出で観測する。



$$\begin{cases} \hat{a}_1 = \frac{1}{\sqrt{2}} (\hat{a}_A - \hat{a}_B) \\ \hat{a}_2 = \frac{1}{\sqrt{2}} (\hat{a}_A + \hat{a}_B) \end{cases}$$

②-1

AliceとBobから送られてきた2つの光 (消滅演算子 \hat{a}_A, \hat{a}_B)を、BSで干渉させる。

②-2

出力光(消滅演算子 \hat{a}_1, \hat{a}_2)の直交位相振幅 \hat{q}_- と \hat{p}_+ をホモダイン検出で観測する。

$$\begin{cases} \hat{a}_1 = \frac{1}{2} (\hat{q}_- + i\hat{p}_-) \\ \hat{a}_2 = \frac{1}{2} (\hat{q}_+ + i\hat{p}_+) \end{cases}$$

2.1 プロトコル(CV MDI-QKD)

③ $\gamma = (q_- + ip_+)/\sqrt{2}$ をAliceとBobに教え、鍵を生成する。

それぞれ、以下の関係で表される。

$$\begin{aligned} & (\hat{q}_- + i\hat{p}_+)/\sqrt{2} \\ &= \frac{1}{\sqrt{2}} \left\{ \frac{1}{\sqrt{2}} (\hat{q}_A - \hat{q}_B) + i \frac{1}{\sqrt{2}} (\hat{p}_A + \hat{p}_B) \right\} \\ &= \frac{1}{2} \{ (\hat{q}_A + i\hat{p}_A) - (\hat{q}_B - i\hat{p}_B) \} \\ &= \frac{1}{2} (2\hat{a}_A - 2\hat{a}_B^\dagger) \\ &= \hat{a}_A - \hat{a}_B^\dagger \end{aligned} \quad \left\{ \begin{array}{l} \hat{q}_- = \frac{1}{\sqrt{2}} (\hat{q}_A - \hat{q}_B) \\ \hat{p}_+ = \frac{1}{\sqrt{2}} (\hat{p}_A + \hat{p}_B) \\ \hat{a}_A = \frac{1}{2} (\hat{q}_A + i\hat{p}_A) \\ \hat{a}_B = \frac{1}{2} (\hat{q}_B + i\hat{p}_B) \end{array} \right.$$

$$\gamma = \alpha - \beta^* + \delta$$

δ : 測定雑音

2.1 プロトコル(CV MDI-QKD)

③ $\gamma = (q_- + ip_+)/\sqrt{2}$ を Alice と Bob に教え、鍵を生成する。

$$\gamma = \alpha - \beta^* + \delta$$

δ : 測定雑音

を Charlie は Alice と Bob に教え、Alice と Bob は γ を知る。

例えば、Bob は

$$\beta^* + \gamma = \alpha + \delta$$

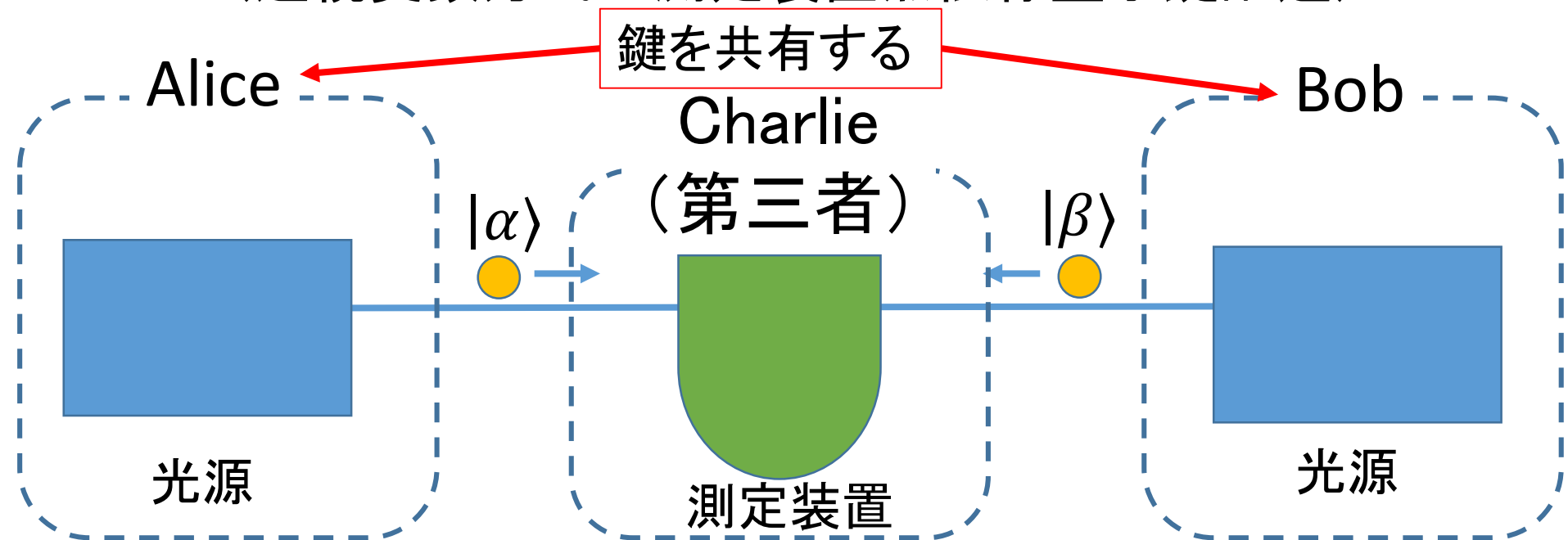
のように、Alice の変数を推定できる。

➡ Alice と Bob は相関のある変数を共有する。
例: α と $\beta^* + \gamma = \alpha + \delta$

➡ Alice と Bob で情報を共有でき、
秘密鍵を作ることができる。

2.1 プロトコル(CV MDI-QKD)

(連続変数方式の測定装置無依存量子鍵配送)



CV MDI-QKDの手順

- ① Alice、Bobはコヒーレント状態 $|\alpha\rangle$ 、 $|\beta\rangle$ をそれぞれCharlieに送る。
- ② Charlieは2つの光を干渉させ、出力の直交位相振幅 (\hat{q}_- と \hat{p}_+) をホモダイン検出で観測する。
- ③ $\gamma = (q_- + ip_+)/\sqrt{2} = \alpha - \beta^* + \delta$ をAliceとBobに教え、鍵を生成する

発表の流れ

1.論文の背景

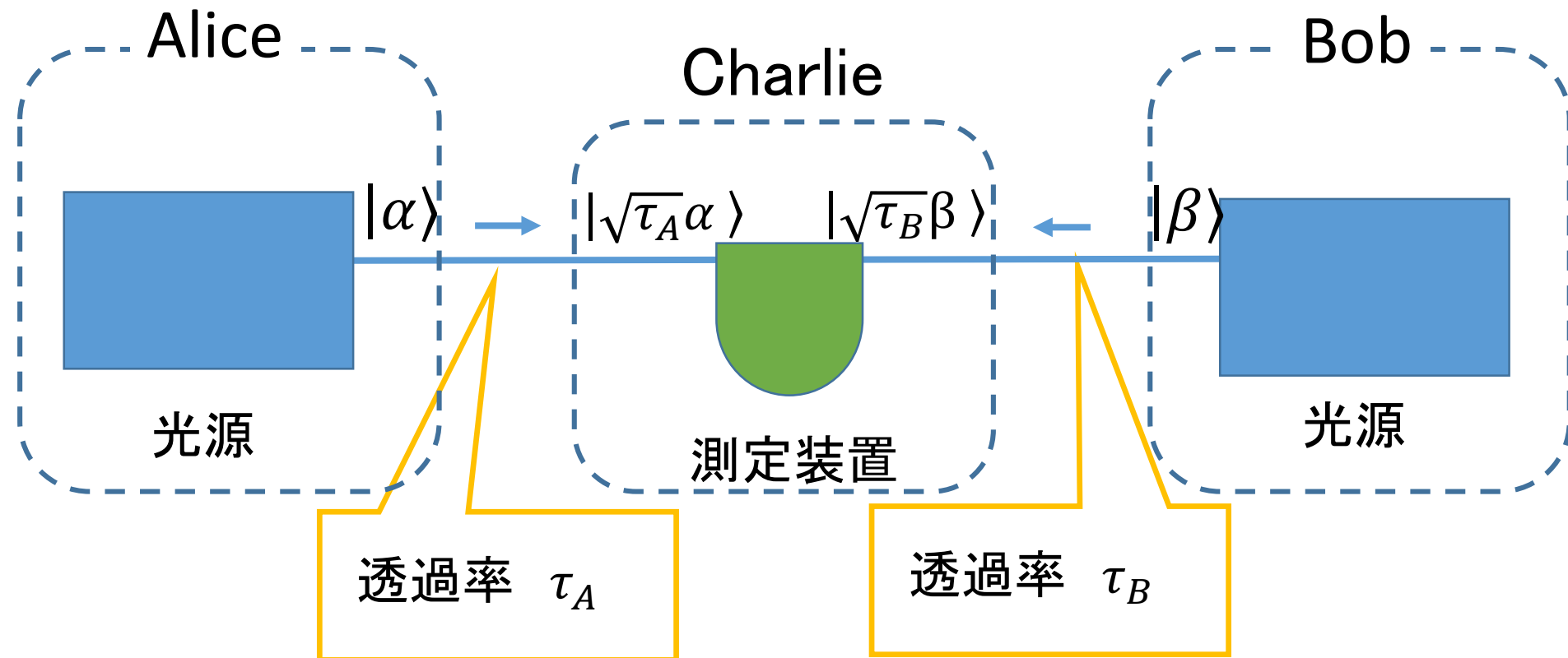
- 1.1 測定装置無依存量子鍵配送 (MDI-QKD)
- 1.2 連続変数方式 (CV)
- 1.3 直交位相振幅とコヒーレント状態
- 1.4 ホモダイン検出

2.本論文の内容

- 2.1 プロトコル (CV MDI-QKD)
 - 現実的なCV MDI-QKD
- 2.2 秘密鍵生成率
- 2.3 実験内容
- 2.4 実験結果

3.まとめ

現実的なCV MDI-QKD



一般的なファイバーでは -0.2dB/km

例：距離が1kmのとき透過率は0.935

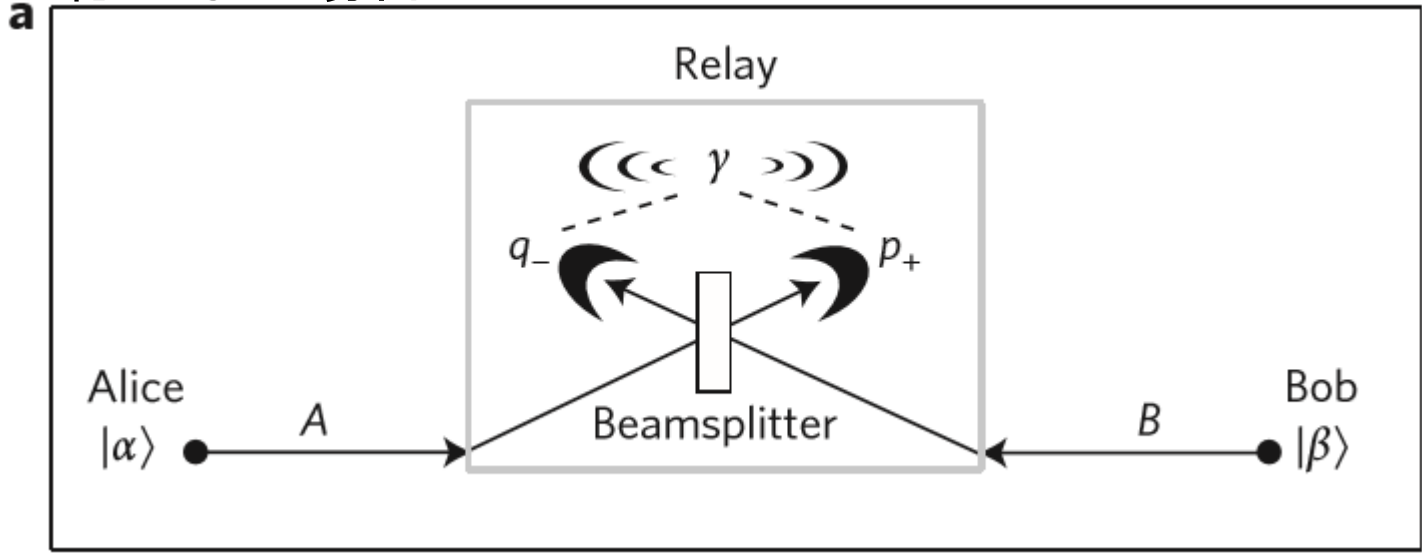
50kmのとき透過率は0.1

過剰雑音： $\varepsilon = \frac{(\Delta q)_{obs}^2}{(\Delta q)^2} - 1$ $(\Delta q)_{obs}^2 = (1 + \varepsilon)(\Delta q)^2$

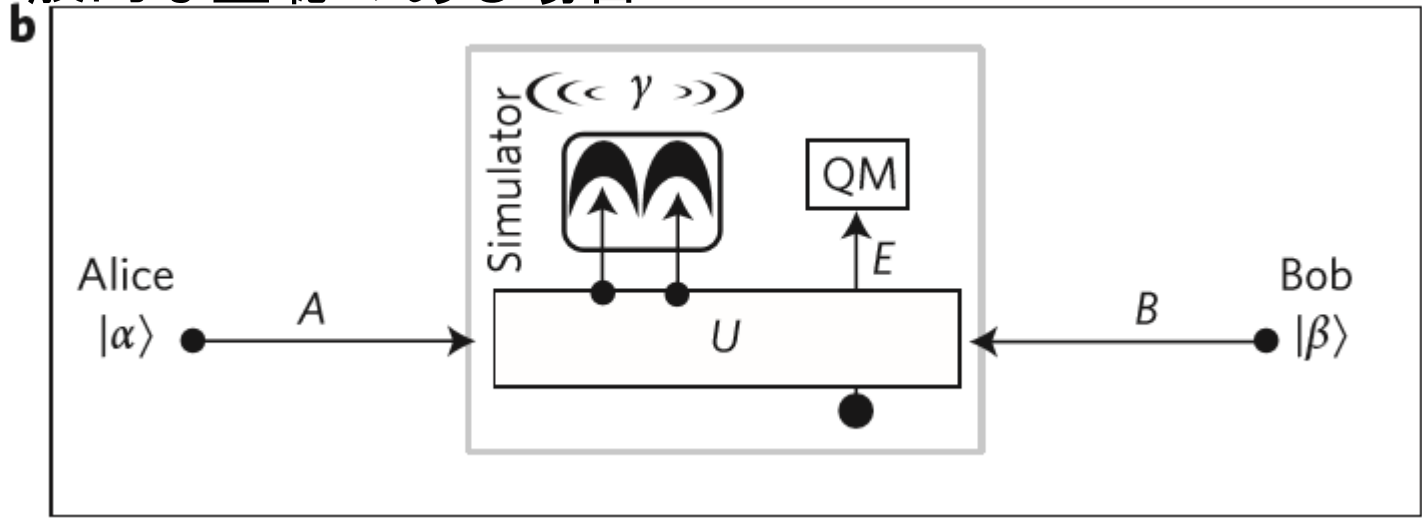
現実的なCV MDI-QKD

盗聴について

盗聴のない場合



一般的な盗聴のある場合



発表の流れ

1.論文の背景

- 1.1 測定装置無依存量子鍵配送 (MDI-QKD)
- 1.2 連続変数方式 (CV)
- 1.3 直交位相振幅とコヒーレント状態
- 1.4 ホモダイン検出

2.本論文の内容

- 2.1 プロトコル (CV MDI-QKD)
現実的なCV MDI-QKD
- 2.2 秘密鍵生成率
- 2.3 実験内容
- 2.4 実験結果

3.まとめ

秘密鍵生成率R の導入

秘密鍵生成率R

$$R = I_{AB} - I_E$$

I_{AB} : AliceとBobの相互情報量

I_E : Charlieの盗んだ情報の上限

$R > 0$ ならば、 R bitの秘密鍵を生成する

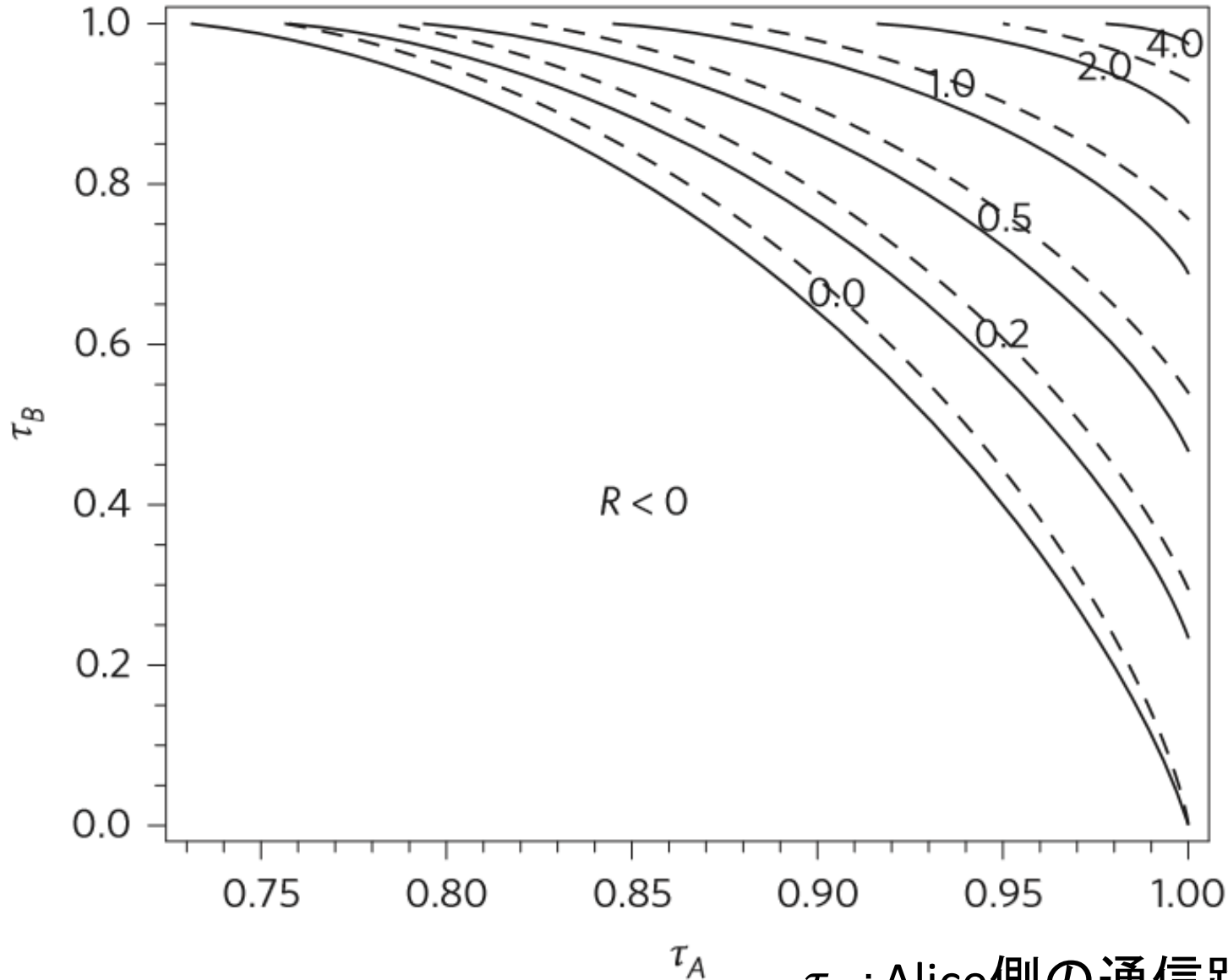
$R < 0$ ならば、秘密鍵は生成できない

ただし、AliceとBobが共有した情報(相関を持った変数)から理論的な上限で鍵を作ることは難しいので

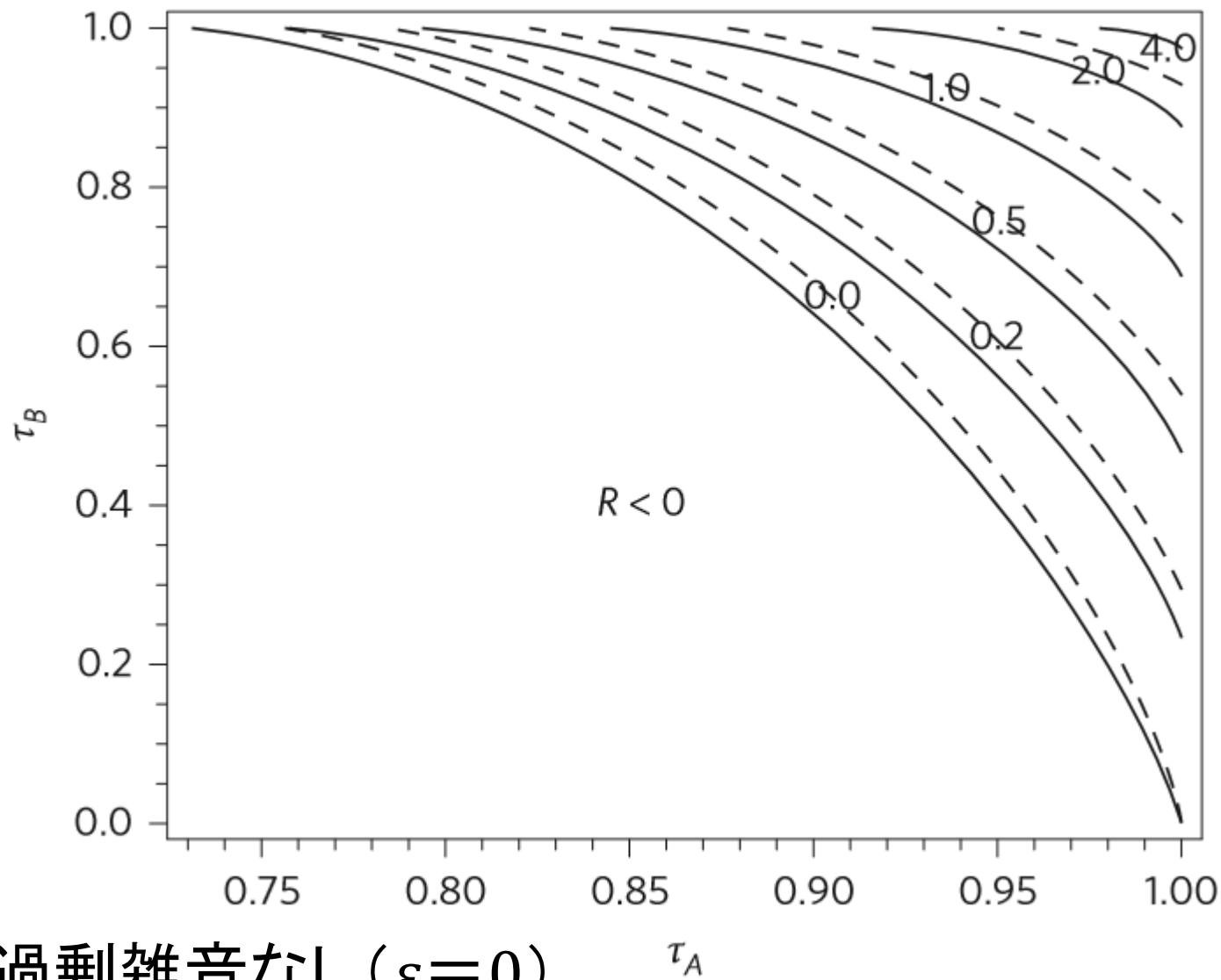
リコンシリエーション(調整)効率 $\xi \leq 1$
を導入する

$$R = \xi I_{AB} - I_E$$

1回あたりの秘密鍵生成率Rと透過率の関係



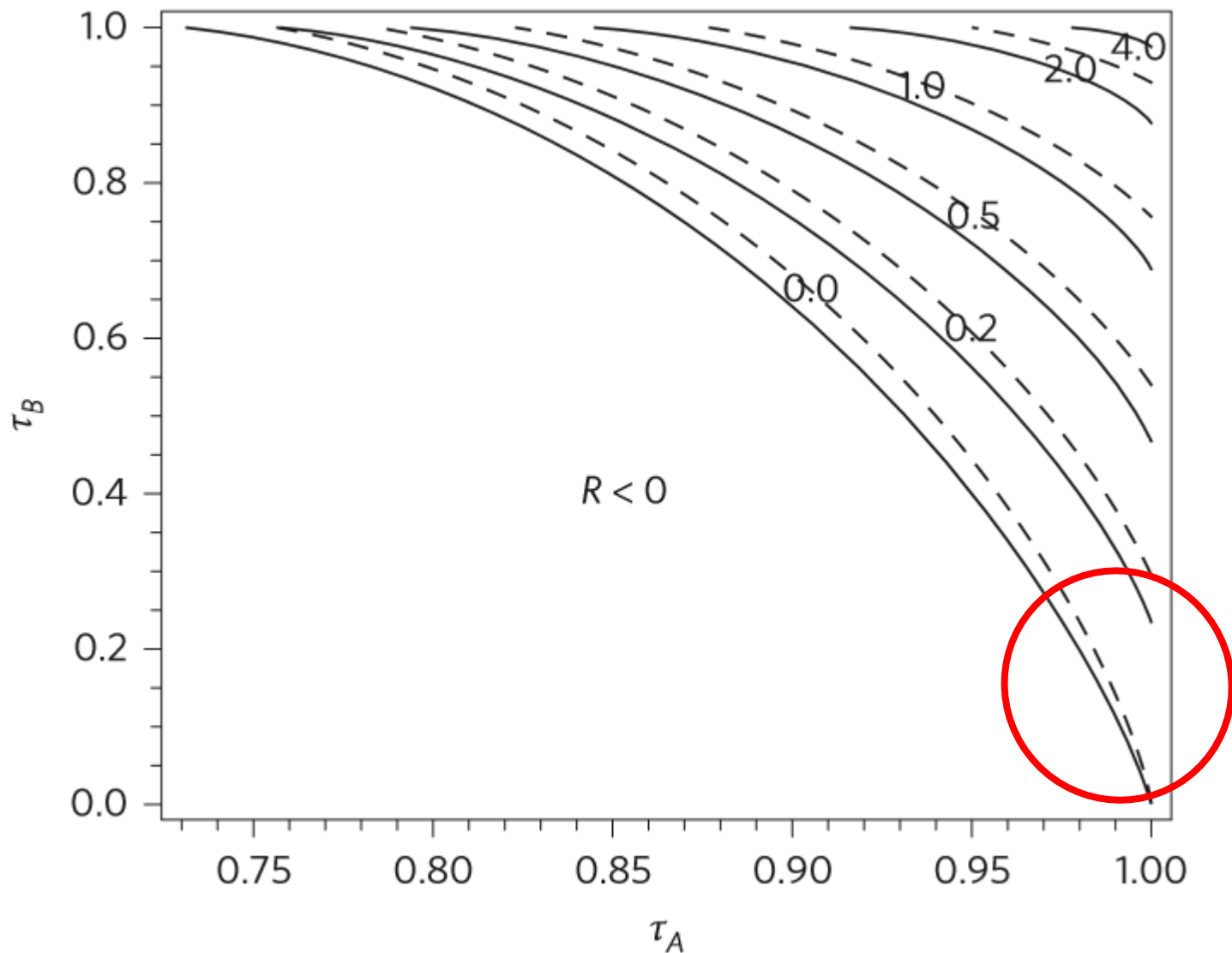
τ_A : Alice側の通信路の透過率
 τ_B : Bob側の通信路の透過率



実線：過剰雑音なし ($\varepsilon = 0$)

破線：5%過剰雑音がある場合 ($\varepsilon = 0.05$)

過剰雑音がある場合、透過率が高くないと鍵が生成できない



τ_A が1に近い値のとき τ_B が0に近い値でも鍵を生成可能
 →Alice側の通信路をできるだけ短くしたほうが良い

発表の流れ

1.論文の背景

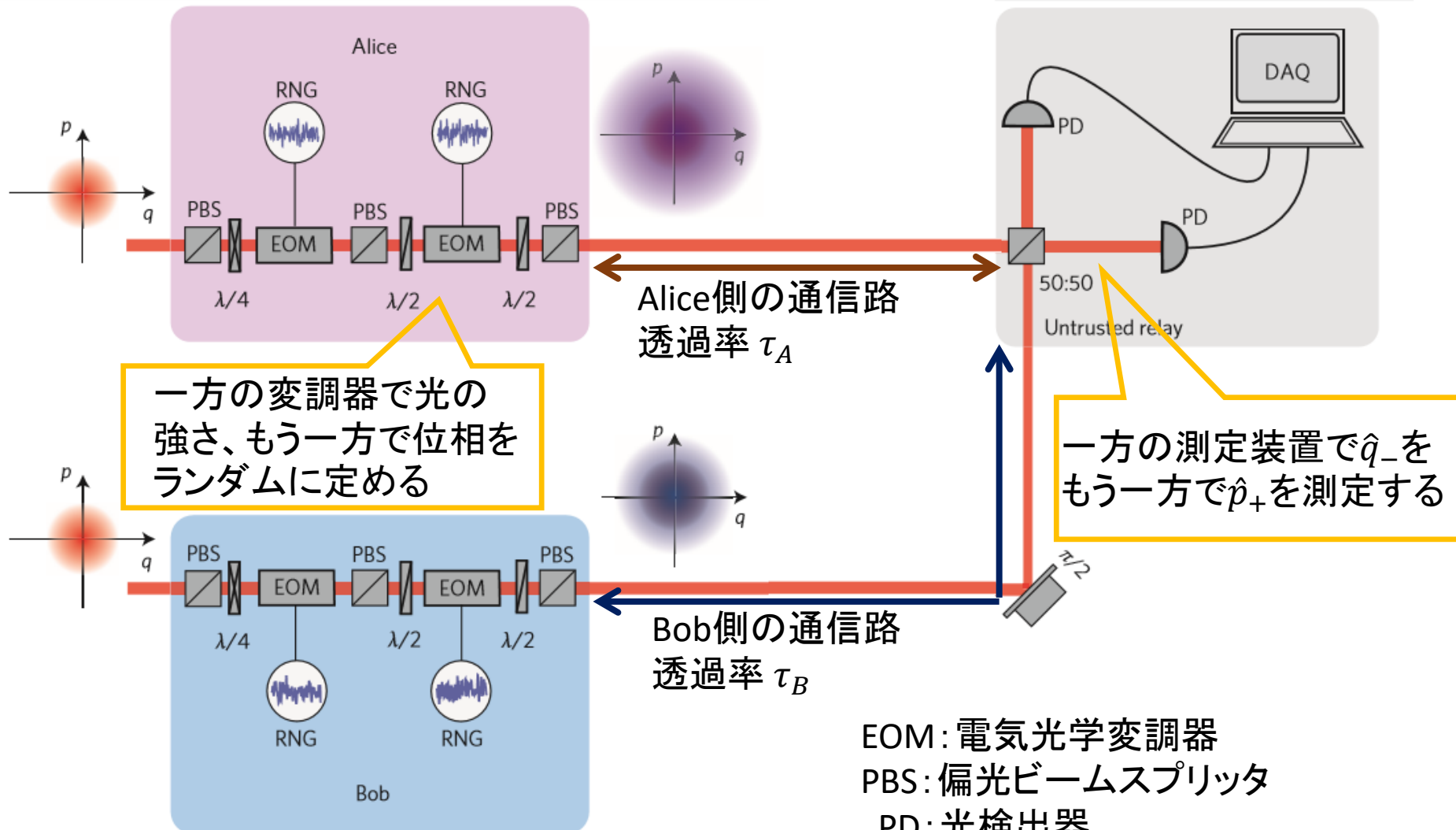
- 1.1 測定装置無依存量子鍵配送 (MDI-QKD)
- 1.2 連続変数方式 (CV)
- 1.3 直交位相振幅とコヒーレント状態
- 1.4 ホモダイン検出

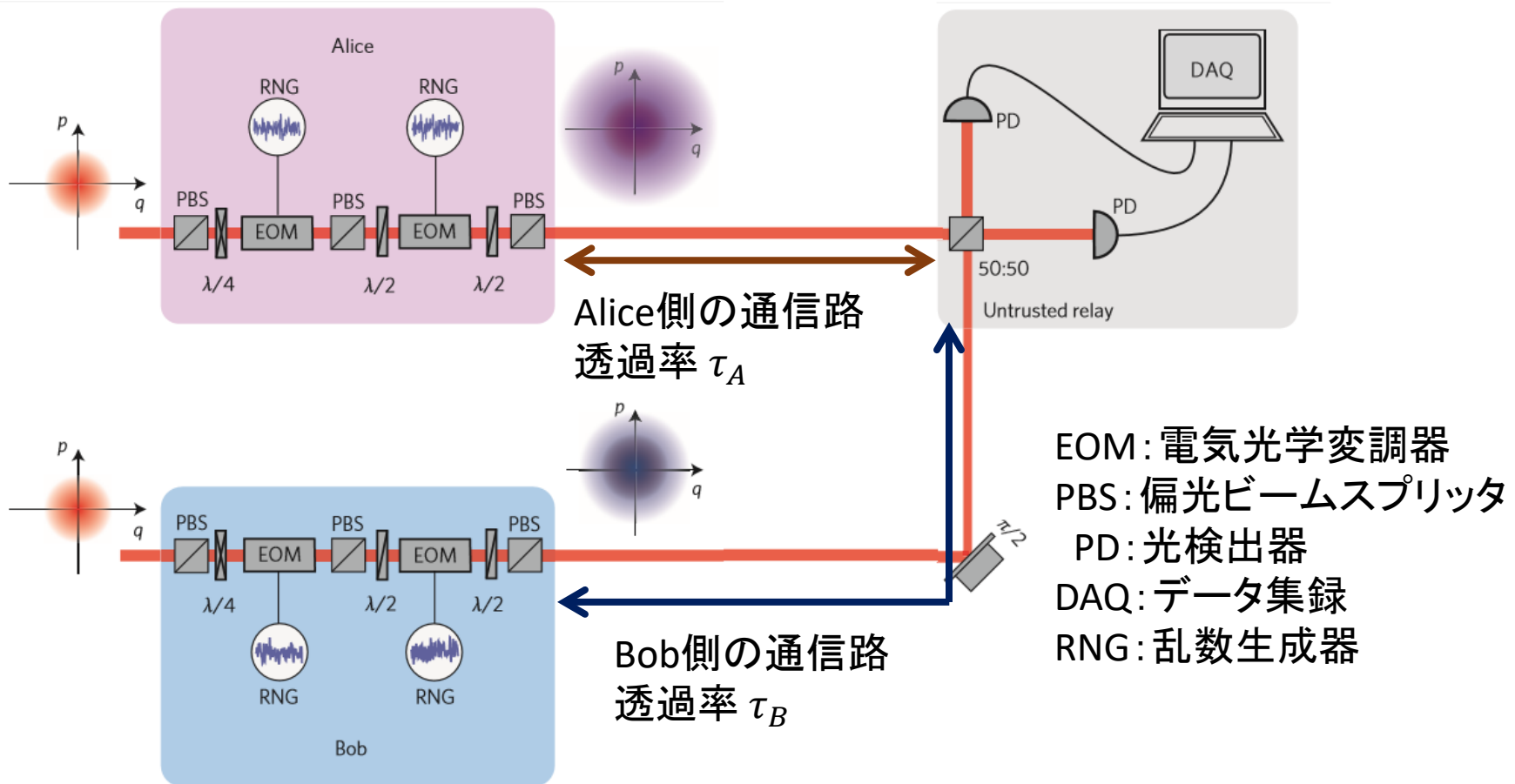
2.本論文の内容

- 2.1 プロトコル (CV MDI-QKD)
現実的なCV MDI-QKD
- 2.2 秘密鍵生成率
- 2.3 実験内容
- 2.4 実験結果

3.まとめ

2.3 実験内容





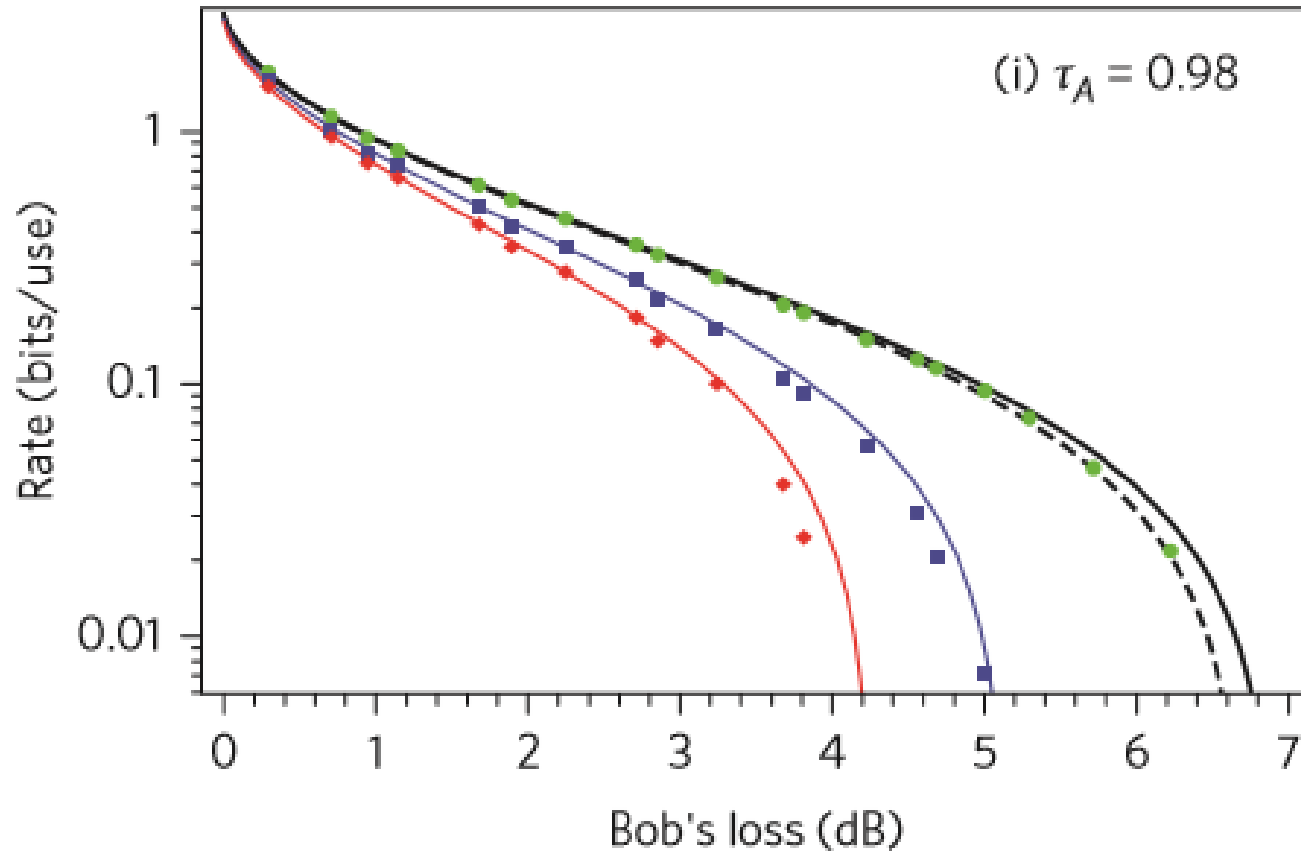
Alice側の通信路について
通信路の距離の短い場合
特に下記の3つについて実験を行う。

- (i) $\tau_A \approx 0.98$: 短い自由空間の通信路で接続
損失は中継点での検出効率によるもの
- (ii) $\tau_A \approx 0.975$: 通信路が100m相当の損失
- (iii) $\tau_A \approx 0.935$: 通信路が1km相当の損失

Bob側の通信路について
通信路の距離の長い場合
について実験を行う。

Alice側の (i) ~ (iii) それぞれ
に対して τ_B を変化させる。

2.4 実験結果



透過率 $\tau_A \approx 0.98$ の場合

実験点 (点)

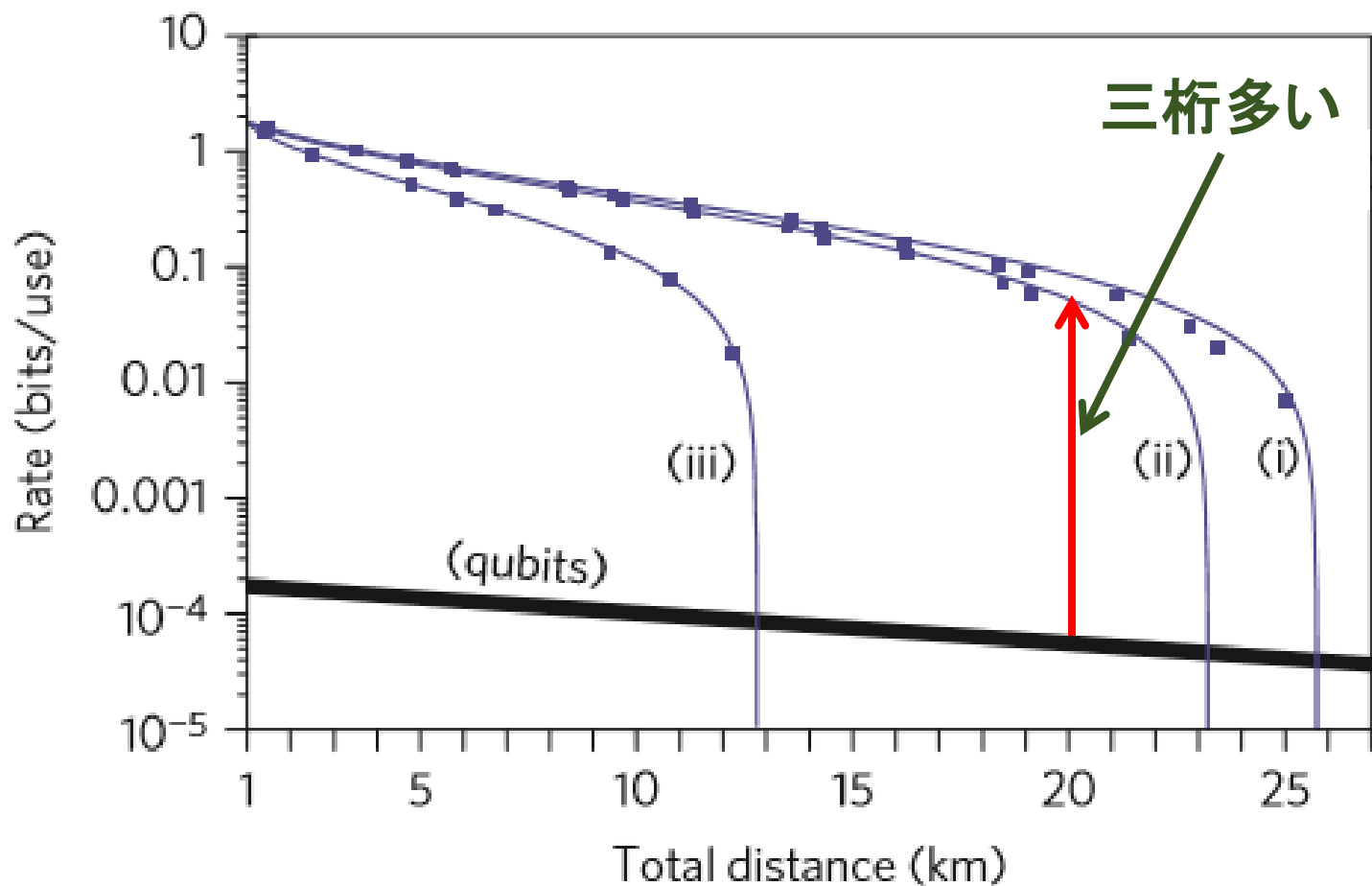
$\xi=1$ (緑色の円)、 $\xi \approx 0.97$ (青色の四角形)、 $\xi \approx 0.95$ (赤色の菱形)

理論値 R (線)

$\xi=1$ および $\epsilon=0$ (黒い実線)、 $\xi=1$ および $\epsilon \approx 0.01$ (破線の黒い線)、

$\xi \approx 0.97$ および $\epsilon=0$ (青い線)、 $\xi \approx 0.95$ および $\epsilon=0$ (赤線)。

ξ : 調整効率、 ϵ : 過剰雑音



(i) $\tau_A \approx 0.98$: 短い自由空間の通信路で接続

損失は中継点での検出効率によるもの

(ii) $\tau_A \approx 0.975$: 通信路が100m相当の損失

(iii) $\tau_A \approx 0.935$: 通信路が1km相当の損失

について、1回あたりの鍵生成率をプロット ($\xi \approx 0.97$ 、青色の四角)

・離散変数方式のMDI-QKDが達成できる鍵生成率 (太い実線)

まとめ

- ・ 測定装置無依存量子鍵配送 (MDI-QKD) は、**測定装置を第三者に預ける**ことで、**安全性を高めた**量子鍵配送の方法。
- ・ 連続変数方式 (CV) MDI-QKD は、Alice と Bob が **コヒーレント状態** $|\alpha\rangle$ 、 $|\beta\rangle$ を送り、Charlie が **$\gamma = \alpha - \beta^* + \delta$** を伝えて (δ は雑音)、鍵を生成する。
- ・ 連続変数方式で MDI-QKD を行った本論文では、離散変数方式の MDI-QKD よりも 3 桁 **高い鍵生成率** (1 回あたり) を実現した。

コヒーレント状態

消滅演算子の固有状態として定義する。

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

- ①直交位相振幅は最小不確定性状態である。
- ②直交位相振幅の不確定性はそれぞれ等しい。

CV MDI-QKD について(プロトコル)

① Alice、Bobはコヒーレント状態 $|\alpha\rangle$ 、 $|\beta\rangle$ をそれぞれCharlieに送る。

複素数 α 、 β をランダムに選ぶ

例

$$\begin{cases} \alpha = \frac{1}{2}(q_A + ip_A) \\ \beta = \frac{1}{2}(q_B + ip_B) \end{cases}$$

Alice	Bob
$\alpha_1 = 1.1 + 2.2i$	$\beta_1 = -2.3 + 1.4i$
$\alpha_2 = -2.4 + 1.1i$	$\beta_2 = 5.3 - 0.3i$
$\alpha_3 = 6.5 - 4.0i$	$\beta_3 = -1.5 - 2.1i$

CV MDI-QKD について(プロトコル)

① Alice、Bobはコヒーレント状態 $|\alpha\rangle$ 、 $|\beta\rangle$ をそれぞれCharlieに送る。

Alice	Bob	Charlie	Bobの知りうる値($\beta^* + \gamma$)
$\alpha_1 = 1.1 + 2.2i$	$\beta_1 = -2.3 + 1.4i$	$\gamma_1 = 3.6 + 3.4i$	$1.3 + 2.0i$
$\alpha_2 = -2.4 + 1.1i$	$\beta_2 = 5.3 - 0.3i$	$\gamma_2 = -8.4 + 0.9i$	$-2.7 + 1.2i$
$\alpha_3 = 6.5 - 4.0i$	$\beta_3 = -1.5 - 2.1i$	$\gamma_3 = 8.1 - 6.3i$	$6.6 - 4.2i$

δ (測定雑音)
$0.2 - 0.2i$
$-0.3 + 0.1i$
$0.1 - 0.2i$

CV MDI-QKD について(プロトコル)

③ $\gamma = (q_- + ip_+)/\sqrt{2}$ を Alice と Bob に教え、鍵を生成する。

$$\gamma = \alpha - \beta^* + \delta$$

例 Bob が $\beta^* + \gamma$ ($= \alpha + \delta$) を計算する

Bobの知りうる値 ($\beta^* + \gamma$)	Alice	Charlie
$\beta_1^* + \gamma_1 = 1.3 + 2.0i$	$\alpha_1 = 1.1 + 2.2i$	$\gamma_1 = 3.6 + 3.4i$
$\beta_2^* + \gamma_2 = -2.7 + 1.2i$	$\alpha_2 = -2.4 + 1.1i$	$\gamma_2 = -8.4 + 0.9i$
$\beta_3^* + \gamma_3 = 6.6 - 4.2i$	$\alpha_3 = 6.5 - 4.0i$	$\gamma_3 = 8.1 - 6.3i$

Alice と Bob は 相関のある変数を共有する。
Alice と Bob で情報を共有でき、
秘密鍵を作ることができる。

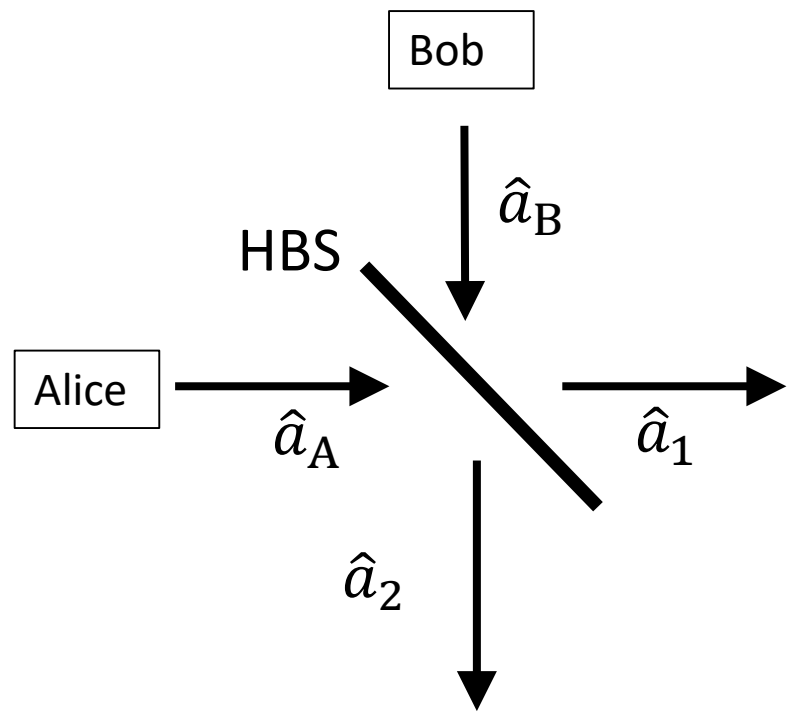
δ (測定雑音)

$$0.2 - 0.2i$$

$$-0.3 + 0.1i$$

$$0.1 - 0.2i$$

CV MDI-QKD (入射部分)



$$\begin{cases} \hat{a}_1 = \frac{1}{2}(\hat{q}_- + i\hat{p}_-) \\ \hat{a}_2 = \frac{1}{2}(\hat{q}_+ + i\hat{p}_+) \end{cases}$$

HBS: ハーフビームスプリッター

$$\begin{cases} \hat{a}_A = \frac{1}{2}(\hat{q}_A + i\hat{p}_A) \\ \hat{a}_B = \frac{1}{2}(\hat{q}_B + i\hat{p}_B) \\ \hat{a}_1 = \frac{1}{\sqrt{2}}(\hat{a}_A - \hat{a}_B) \\ \hat{a}_2 = \frac{1}{\sqrt{2}}(\hat{a}_A + \hat{a}_B) \end{cases}$$

$$\begin{aligned} \hat{a}_2 &= \frac{1}{\sqrt{2}}(\hat{a}_A + \hat{a}_B) \\ &= \frac{1}{2\sqrt{2}}(\hat{q}_A + i\hat{p}_A + \hat{q}_B + i\hat{p}_B) \\ &= \frac{1}{2} \left(\frac{1}{\sqrt{2}}(\hat{q}_A + \hat{q}_B) + i\frac{1}{\sqrt{2}}(\hat{p}_A + \hat{p}_B) \right) \\ &= \frac{1}{2}(\hat{q}_+ + i\hat{p}_+) \end{aligned}$$

ホモダイン検出と直交位相振幅

$$\hat{n}_{12} = \hat{n}_1 - \hat{n}_2 = \hat{a}_1^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}_1$$

入力の状態 $|\psi\rangle$ 、 $|\omega\rangle$ (LO光はコヒーレント状態) として

$$\begin{aligned}\langle \hat{n}_{12} \rangle &= \langle \psi | \langle \omega | (\hat{n}_{12}) | \omega \rangle | \psi \rangle \\ &= \langle \psi | \langle \omega | (\hat{a}_1^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}_1) | \omega \rangle | \psi \rangle \\ &= \langle \psi | \hat{a}_1^\dagger | \psi \rangle \cdot \langle \omega | \hat{a}_{LO} | \omega \rangle + \langle \omega | \hat{a}_{LO}^\dagger | \omega \rangle \cdot \langle \psi | \hat{a}_1 | \psi \rangle \\ &= \omega \langle \psi | \hat{a}_1^\dagger | \psi \rangle + \omega^* \langle \psi | \hat{a}_1 | \psi \rangle\end{aligned}$$

$$\hat{a}_1 = \frac{1}{2} (\hat{q}_- + i\hat{p}_-) \quad \omega = |\omega| e^{i\theta} \quad \text{を用いると}$$

$$\begin{aligned}\langle \hat{n}_{12} \rangle &= \frac{1}{2} |\omega| e^{i\theta} \langle \psi | \hat{q}_- - i\hat{p}_- | \psi \rangle + \frac{1}{2} |\omega| e^{-i\theta} \langle \psi | \hat{q}_- + i\hat{p}_- | \psi \rangle \\ &= \frac{1}{2} |\omega| (e^{i\theta} + e^{-i\theta}) \langle \psi | \hat{q}_- | \psi \rangle - \frac{i}{2} |\omega| (e^{i\theta} - e^{-i\theta}) \langle \psi | \hat{p}_- | \psi \rangle \\ &= |\omega| \langle \psi | (\hat{q}_- \cos \theta + \hat{p}_- \sin \theta) | \psi \rangle\end{aligned}$$

$$\hat{n}_{12} = |\omega| (\hat{q}_- \cos \theta + \hat{p}_- \sin \theta)$$

2.2 理論的な値

秘密鍵生成率 $R(\tau_A, \tau_B, \varepsilon)$ の式

$$R(\tau_A, \tau_B, \varepsilon) = \log_2 \left[\frac{2(\tau_A + \tau_B)}{e|\tau_A + \tau_B|\chi} \right] + h \left[\frac{\tau_A \chi}{\tau_A + \tau_B} - 1 \right] - h \left[\frac{\tau_A \tau_B \chi - (\tau_A + \tau_B)^2}{|\tau_A - \tau_B|(\tau_A + \tau_B)} \right]$$

τ_A, τ_B : 透過率 χ : 等価ノイズ
 ε : 余分なノイズ

2.2 理論的な値

秘密鍵生成率 $R(\tau_A, \tau_B, \epsilon)$ の式

$$R(\tau_A, \tau_B, \epsilon) = \log_2 \left[\frac{2(\tau_A + \tau_B)}{e|\tau_A + \tau_B|\chi} \right] + h \left[\frac{\tau_A \chi}{\tau_A + \tau_B} - 1 \right] - h \left[\frac{\tau_A \tau_B \chi - (\tau_A + \tau_B)^2}{|\tau_A - \tau_B|(\tau_A + \tau_B)} \right]$$

$$h := \frac{x+1}{2} \log_2 \frac{x+1}{2} - \frac{x-1}{2} \log_2 \frac{x-1}{2}$$