Experimental measurement-device-independent quantum digital signatures

G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor and E. Andersson

Nature Communications **8**, Article number: 1098 (2017).

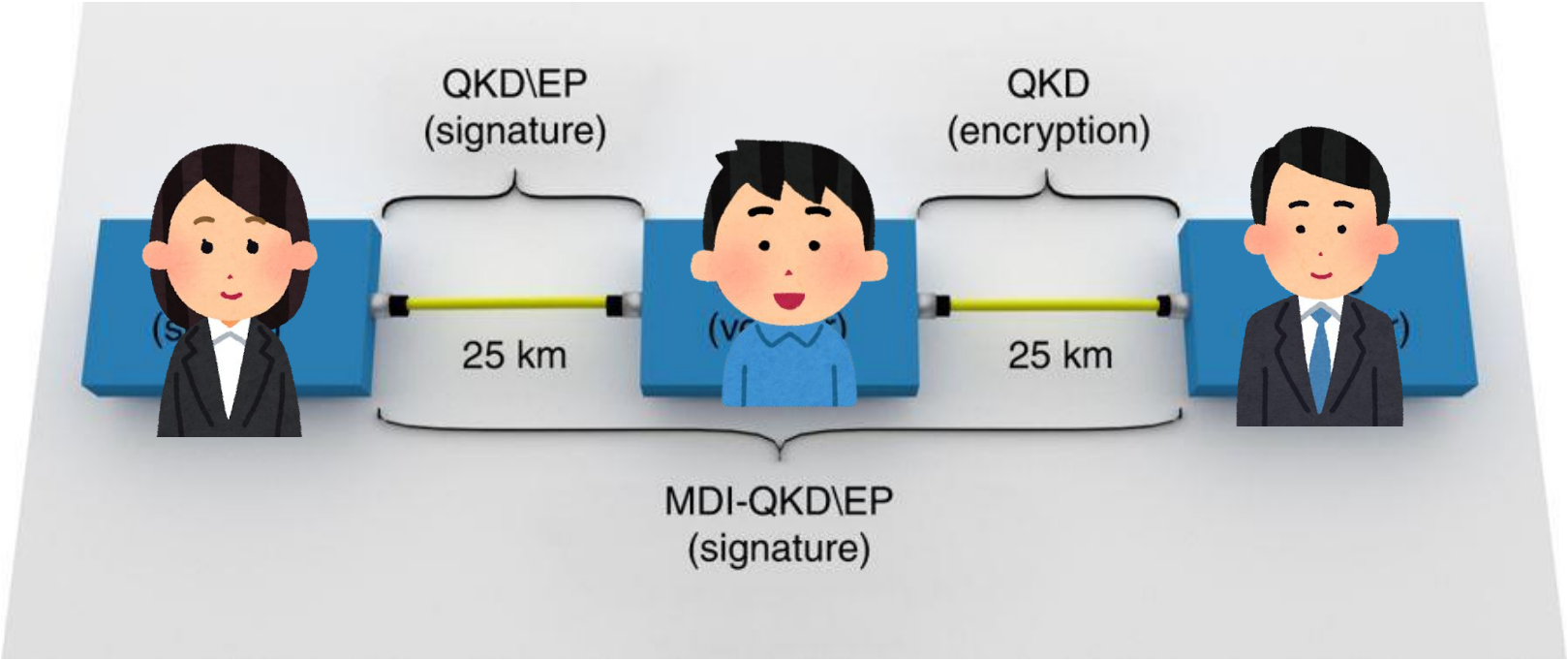
測定装置無依存の量子デジタル署名の実験

平野研究室

15-041-046 竹田ひな乃

論文の概要

- 量子鍵配送(QKD)と測定装置無依存型量子鍵配送(MDI-QKD)を用いて量子デジタル署名(QDS)を行った。

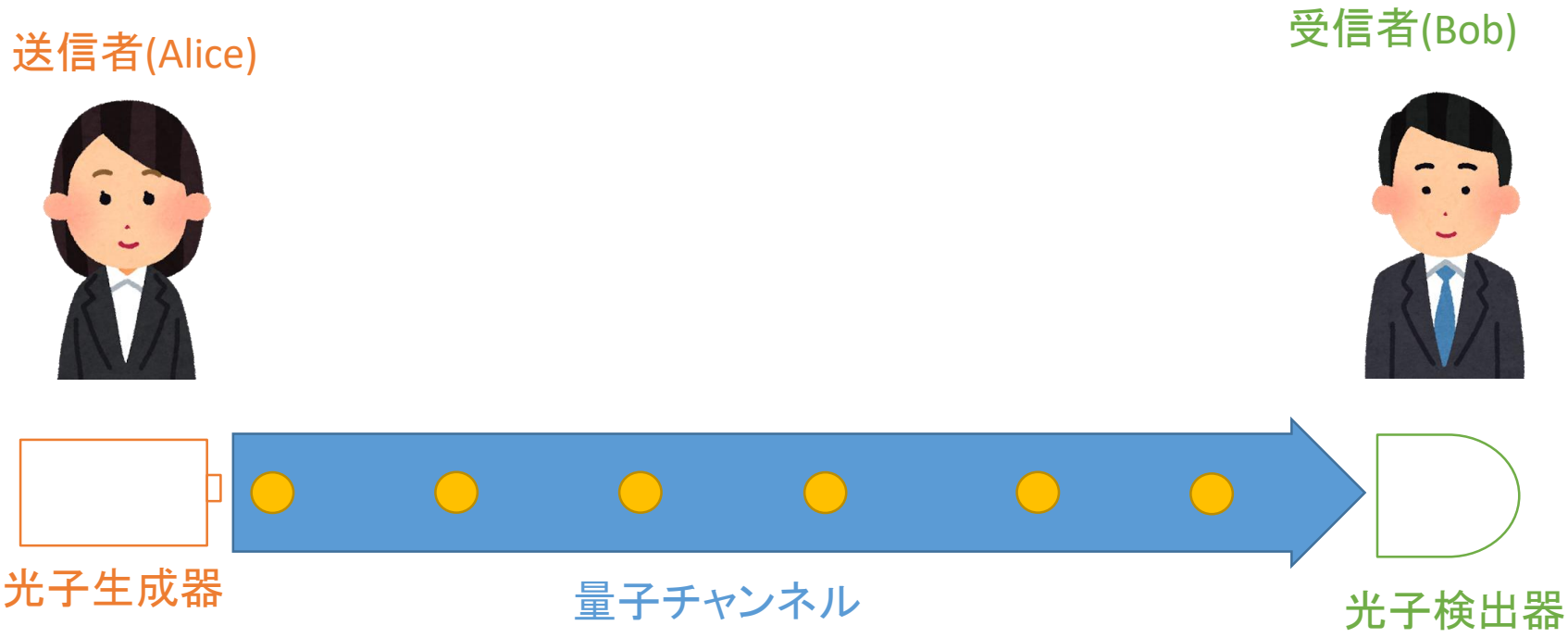


目次

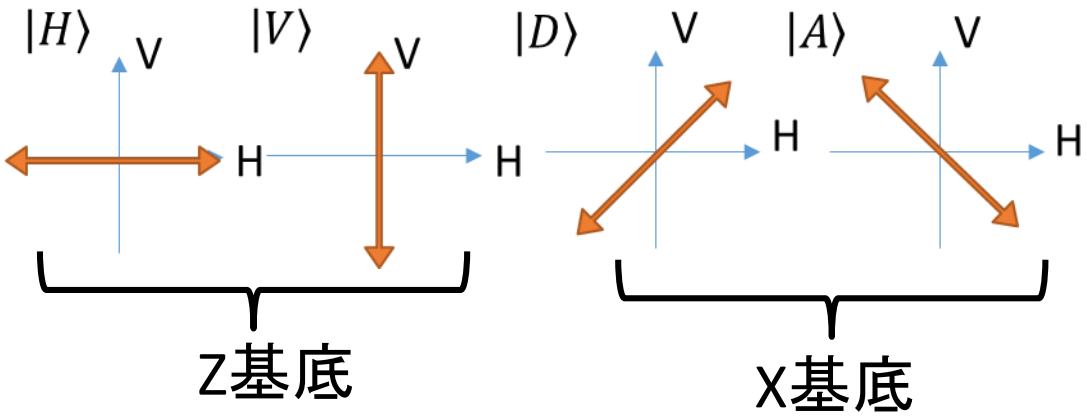
- 概要
- 第一部
  - 量子鍵配送(QKD)
  - 測定装置無依存型量子鍵配送(MDI-QKD)
    - 概要
    - プロトコル
  - 結果
- 第二部
  - 量子デジタル署名(QDS)
    - デジタル署名
    - 量子デジタル署名
    - プロトコル
  - 結果
- まとめ

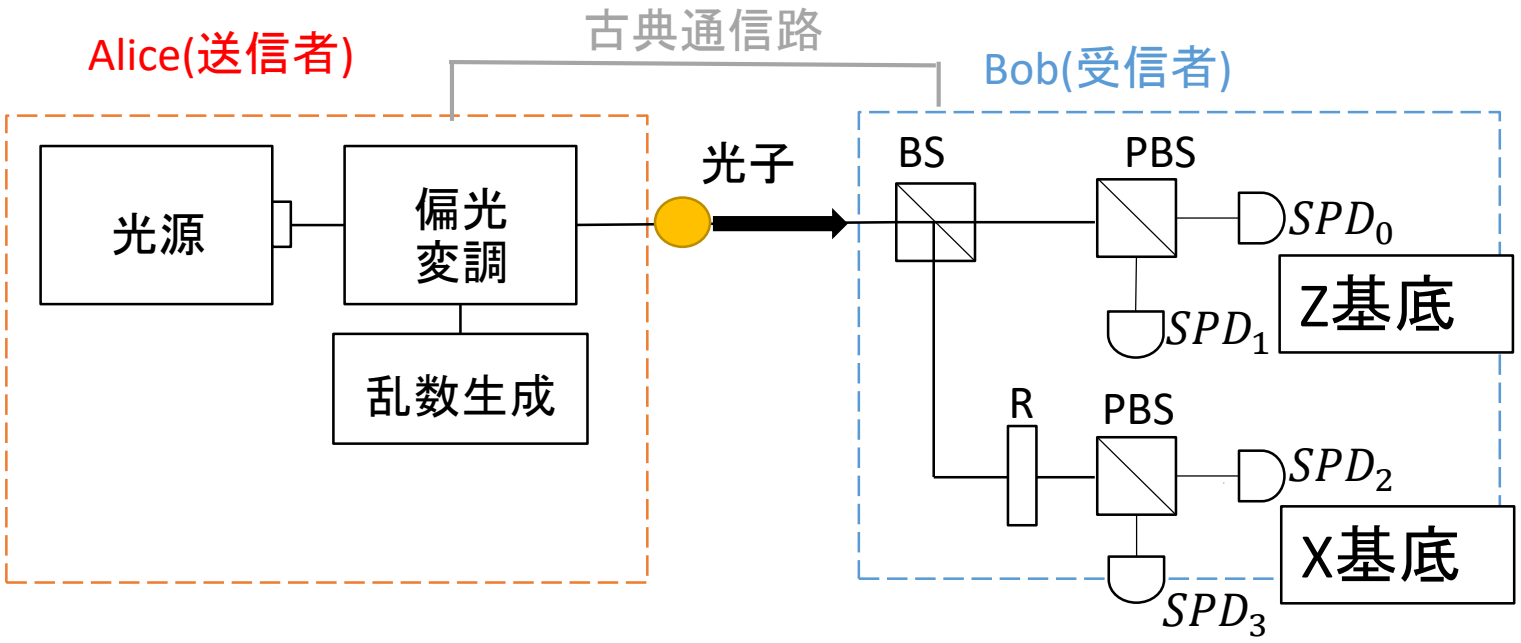
量子鍵配送(Quantum Key Distribution: QKD)とは

・量子力学の原理によって安全性を証明する、秘密鍵の共有方法



量子鍵配送(QKD)

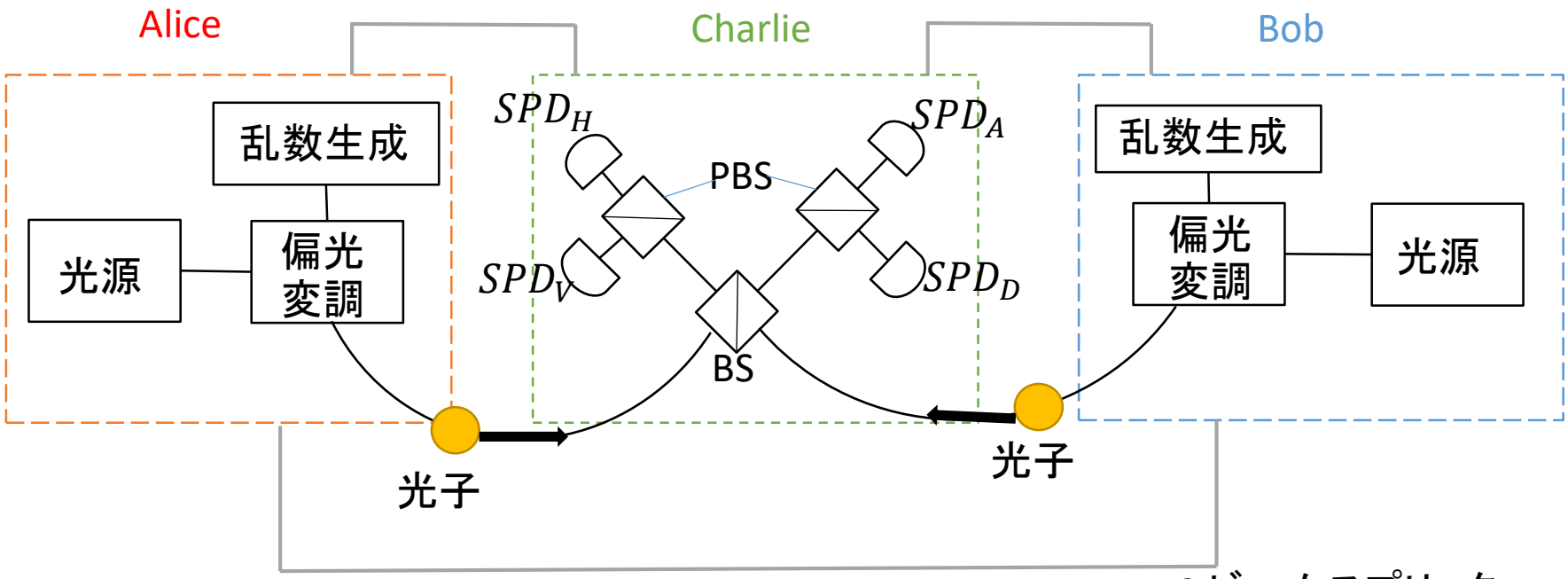




Aliceが光源を持ち、Bobが測定
Alice側は乱数で偏光を、
Bob側はBSで基底をランダムに選択

BS:ビームスプリッタ
PBS:偏光ビームスプリッタ
SPD:単一光子検出器
R:波長板

測定装置無依存型量子鍵配送
Measurement Device Independent(MDI) - QKD



BS:ビームスプリッタ
PBS:偏光ビームスプリッタ
SPD:単一光子検出器

AliceとBobが光源を持ち
Charlieが測定(4つの単一光子検出器)

測定装置無依存型量子鍵配送(MDI-QKD)の流れ

① AliceとBobはCharlieに対して4つの偏光状態から1つをランダムに選んで送る。

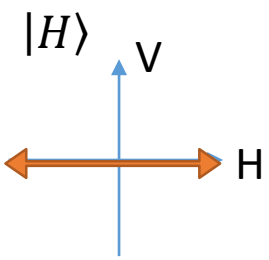
② Charlieは、AliceとBobから送られた光をビームスプリッタで干渉させ、検出器で測定。結果をAliceとBobに送る。

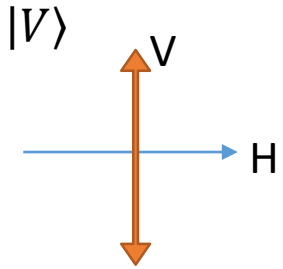
③ Charlieの結果をもとに、AliceとBobは鍵を生成する。

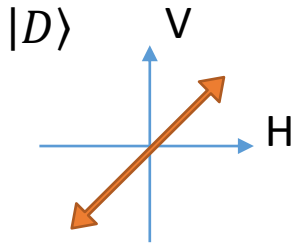
①AliceとBobはCharlieに対して4つの偏光状態から1つをランダムに選んで送る。

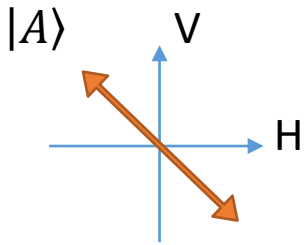
AliceとBobはそれぞれ、ビット値と基底をランダムに選ぶことによって、4状態のうち1つを選択する。

ビット値	Z基底	X基底
0	$\|H\rangle$	$\|D\rangle$
1	$\|V\rangle$	$\|A\rangle$



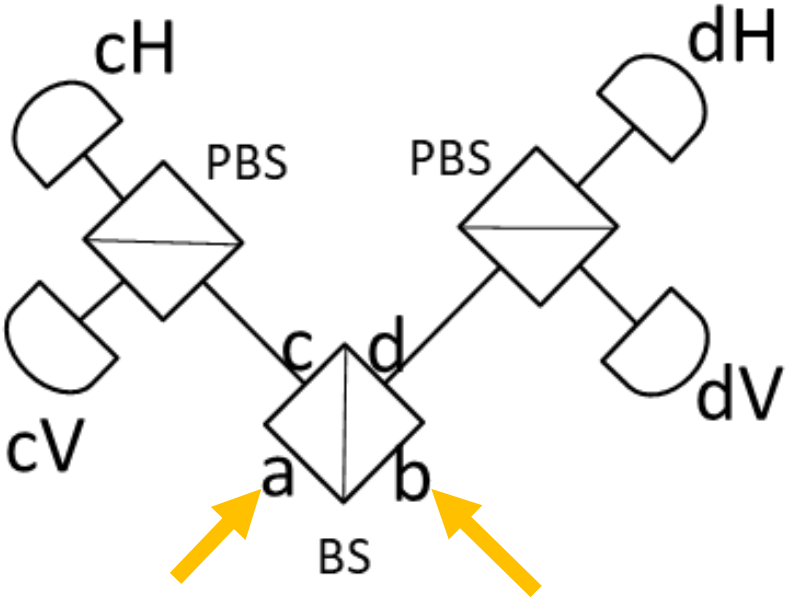






②Charlieは、AliceとBobから送られた光をビームスプリッタで干渉させ、検出器で測定。結果をAliceとBobに送る。

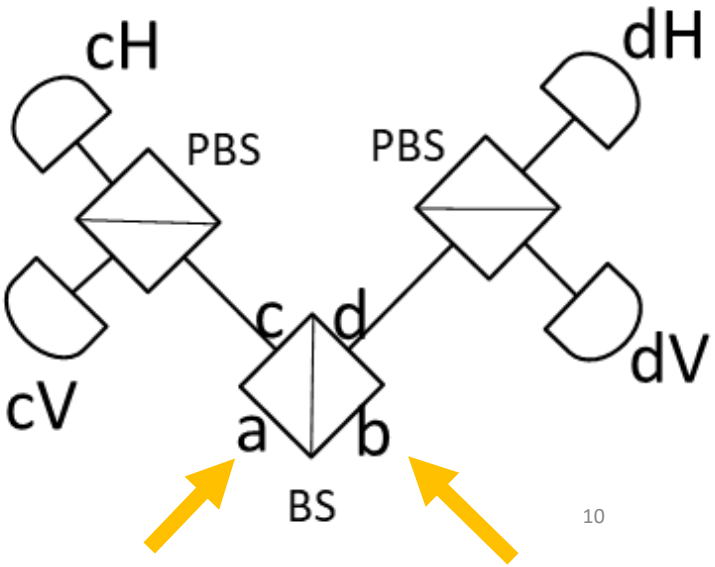
- a、bからBSに入ってきた光は、cかdどちらかから出てくる。
- Charlieは4つの単一光子検出器のどこに反応があったかを調べ、2つの検出器に反応があった場合のみ、どこの2つの検出器が反応したかAliceとbobに知らせる。



③Charlieの結果をもとに、AliceとBobは鍵を生成する。

- cHとdV あるいは dHとcV で検出→singlet
- cHとcV あるいは dHとdV で検出→triplet

この2つのみ使用



③Charlieの結果をもとに、AliceとBobは鍵を生成する。

Alice

Bit	基底	偏光
1	Z	$\|V\rangle$
1	X	$\|A\rangle$
0	Z	$\|H\rangle$
1	X	$\|A\rangle$
0	Z	$\|H\rangle$
0	X	$\|D\rangle$
⋮	⋮	⋮

Bob

Bit	基底	偏光
0	Z	$\|H\rangle$
0	X	$\|D\rangle$
1	Z	$\|V\rangle$
0	X	$\|D\rangle$
1	Z	$\|V\rangle$
1	Z	$\|V\rangle$
⋮	⋮	⋮

Charlie

反応した検出器	状態
dH/dV	triplet
cV/dV	-
cH/dV	singlet
dH/cV	singlet
dH/dV	triplet
cH/dV	singlet
⋮	⋮

同じ基底の組み合わせ　&　(Singlet or Triplet)

のみを使用

③Charlieの結果をもとに、AliceとBobは鍵を生成する。

Alice

Bit	基底	偏光
1	Z	$\|V\rangle$
0	Z	$\|H\rangle$
1	X	$\|A\rangle$
0	Z	$\|H\rangle$
⋮	⋮	⋮

Bob

Bit	基底	偏光
0	Z	$\|H\rangle$
1	Z	$\|V\rangle$
0	X	$\|D\rangle$
1	Z	$\|V\rangle$
⋮	⋮	⋮

Charlie

反応した検出器	状態
dH/dV	triplet
cH/dV	singlet
dH/cV	singlet
dH/dV	triplet
⋮	⋮

同じ基底の組み合わせ ＆ (Singlet or Triplet)

のみを使用

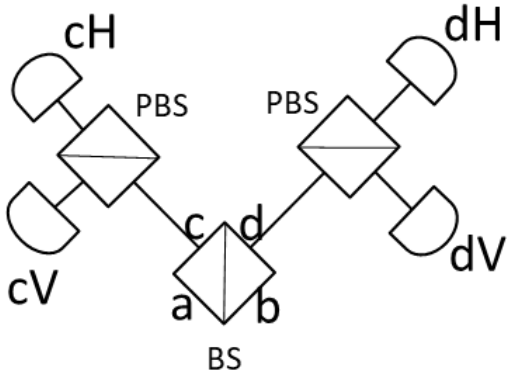
ビット反転

cHとdVあるいはdHとcV→singlet
cHとcVあるいはdHとdV→triplet

Alice,BobともZ基底で同じビットを選んだ時、つまりAlice,Bobの両方がHまたはVのとき

→singletにもtripletにもならない

<u>Z基底でsingletまたはtripletの時、両者のビットは異なる。</u>



③Charlieの結果をもとに、AliceとBobは鍵を生成する。

Alice

Bit	基底	偏光
1	Z	$\|V\rangle$
0	Z	$\|H\rangle$
1	X	$\|A\rangle$
0	Z	$\|H\rangle$
⋮	⋮	⋮

Bob

Bit	基底	偏光
0	Z	$\|H\rangle$
1	Z	$\|V\rangle$
0	X	$\|D\rangle$
1	Z	$\|V\rangle$
⋮	⋮	⋮

Charlie

反応した検出器	状態
dH/dV	triplet
cH/dV	singlet
dH/cV	singlet
dH/dV	triplet
⋮	⋮

singlet	triplet
0⇔1	0⇔1

③Charlieの結果をもとに、AliceとBobは鍵を生成する。

Alice

Bit	基底	偏光
1	Z	$\|V\rangle$
0	Z	$\|H\rangle$
1	X	$\|A\rangle$
0	Z	$\|H\rangle$
⋮	⋮	⋮

Bob

Bit	基底	偏光
1	Z	$\|H\rangle$
0	Z	$\|V\rangle$
0	X	$\|D\rangle$
0	Z	$\|V\rangle$
⋮	⋮	⋮

Charlie

反応した検出器	状態
dH/dV	triplet
cH/dV	singlet
dH/cV	singlet
dH/dV	triplet
⋮	⋮

singlet	triplet
0⇔1	0⇔1

③Charlieの結果をもとに、AliceとBobは鍵を生成する。

Alice

Bit	基底	偏光
1	Z	$\|V\rangle$
0	Z	$\|H\rangle$
1	X	$\|A\rangle$
0	Z	$\|H\rangle$
⋮	⋮	⋮

Bob

Bit	基底	偏光
1	Z	$\|H\rangle$
0	Z	$\|V\rangle$
0	X	$\|D\rangle$
0	Z	$\|V\rangle$
⋮	⋮	⋮

Charlie

反応した検出器	状態
dH/dV	triplet
cH/dV	singlet
dH/cV	singlet
dH/dV	triplet
⋮	⋮

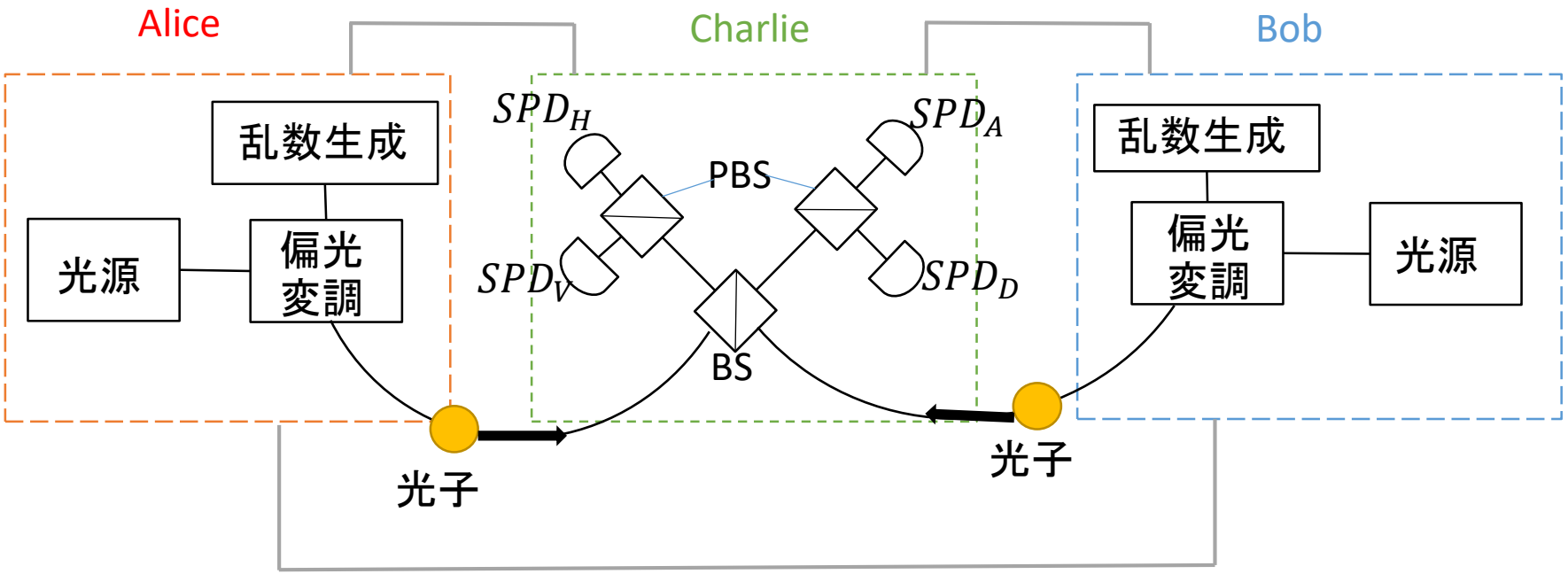
- X基底はデコイパルスとして使用
- Z基底を鍵ビットとして使用

→ シフト鍵:100・・・

その後誤り訂正、秘匿性増幅を行う → 秘密鍵(ビット列)を共有

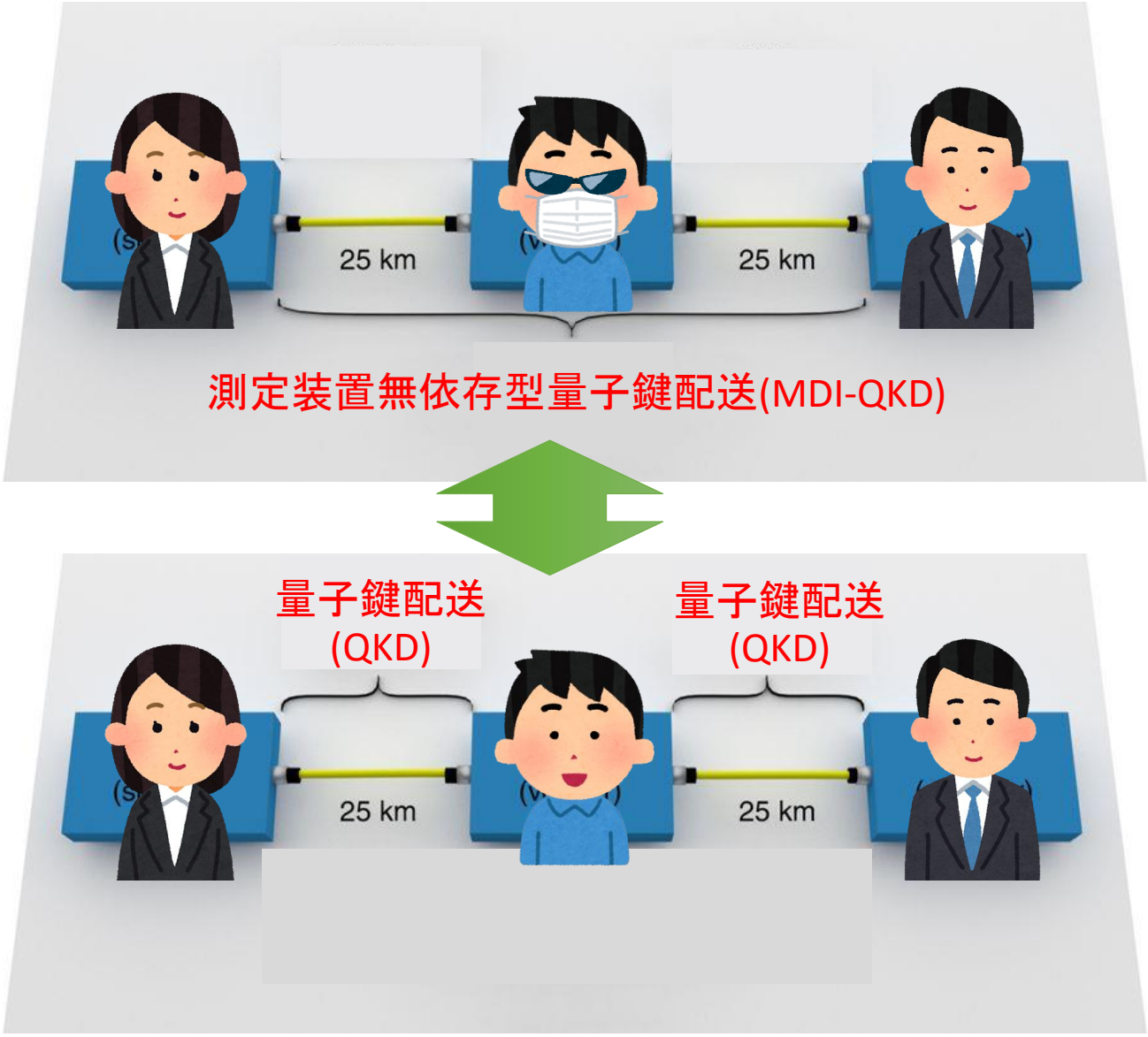
MDI-QKDまとめ

BS:ビームスプリッタ
PBS:偏光ビームスプリッタ
SPD:単一光子検出器

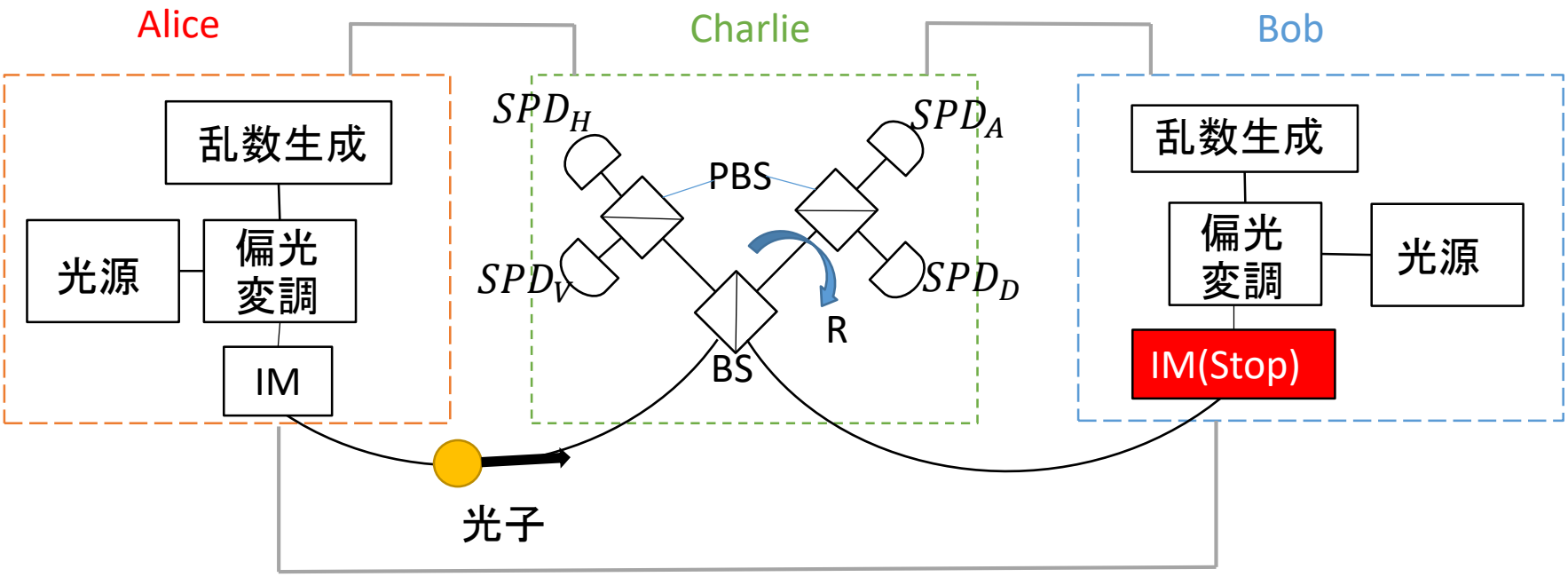


AliceとBobが光源を持ち、第三者のCharlieが測定
2箇所で光子が検出されたときに鍵を生成

MDI-QKDとQKDの切り替え

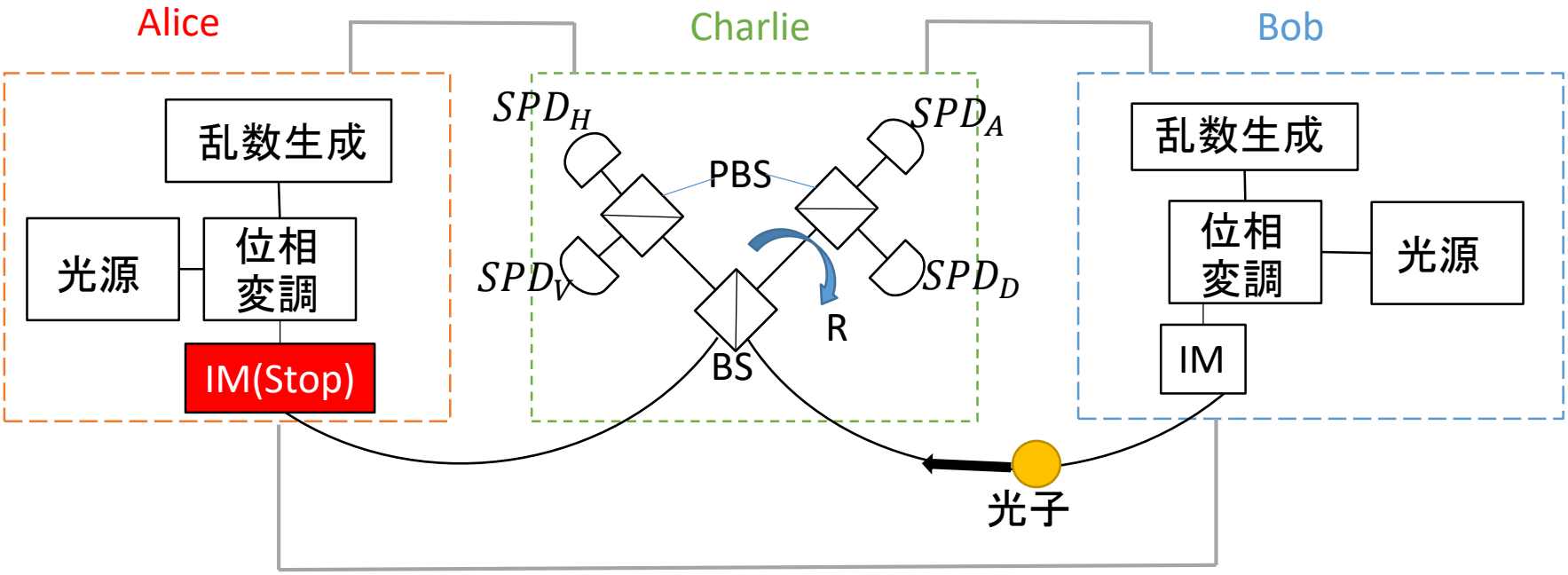


AliceとCharlie間のQKD



BS:ビームスプリッタ
PBS:偏光ビームスプリッタ
SPD:単一光子検出器
R:波長板(45度偏光面を回転させる)
IM:強度変調器

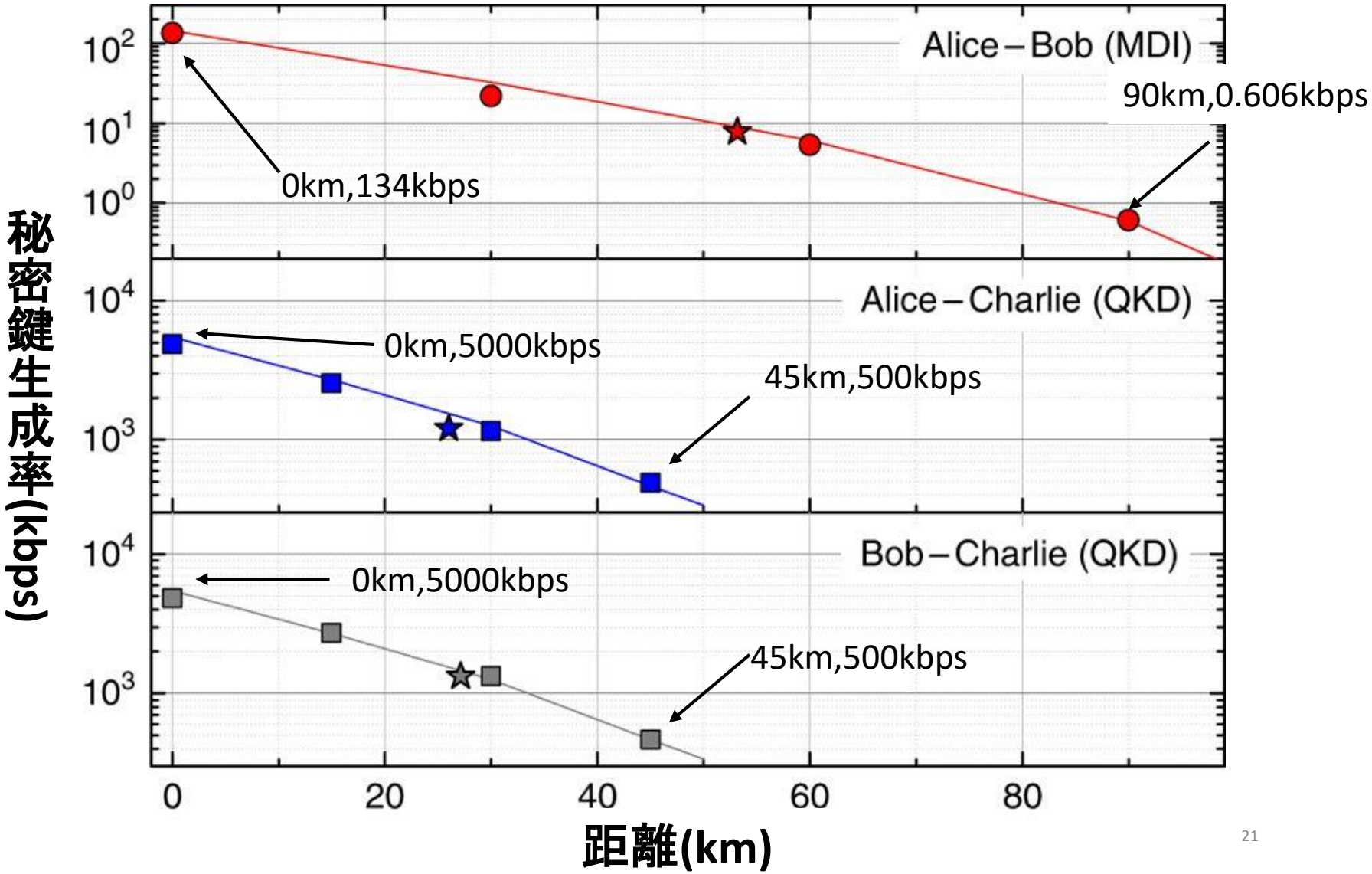
BobとCharlie間のQKD



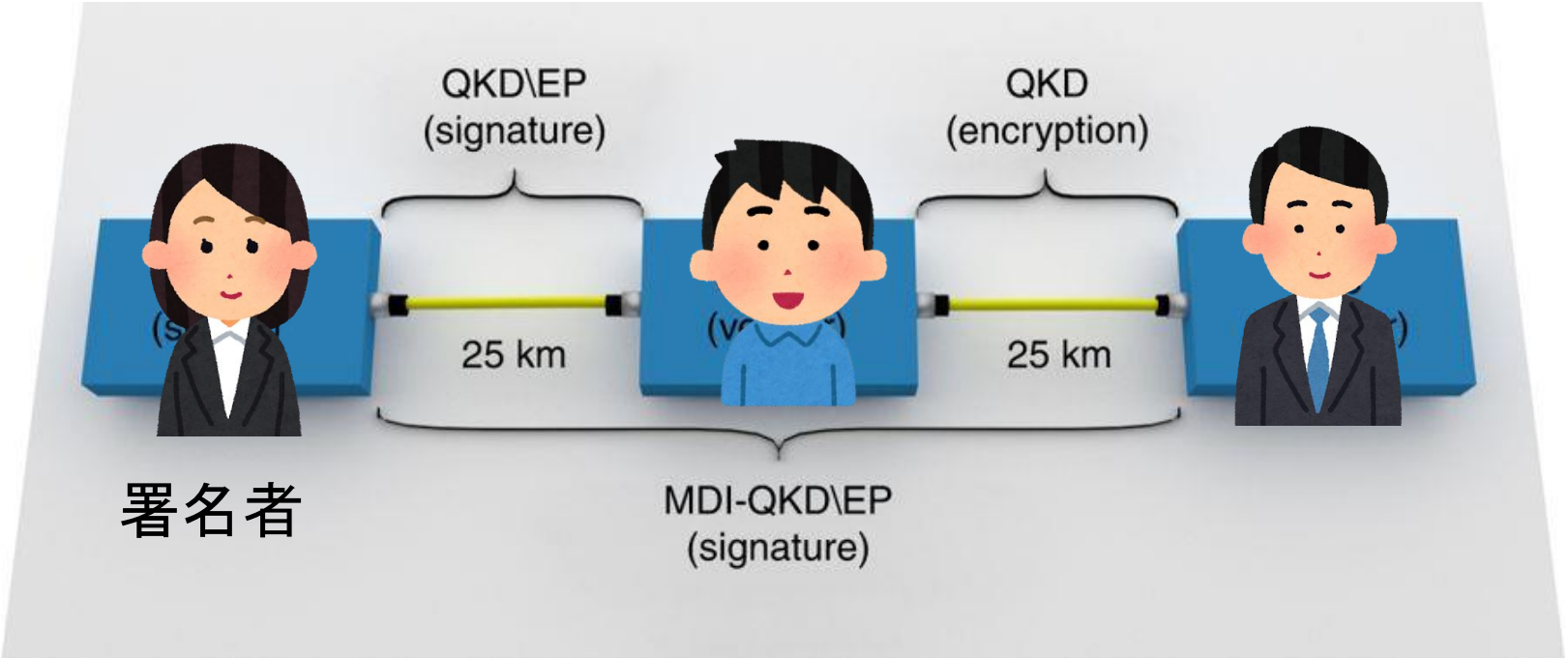
BS:ビームスプリッタ
PBS:偏光ビームスプリッタ
SPD:単一光子検出器
R:波長板(45度偏光面を回転させる)
IM:強度変調器

量子鍵配送の実験結果

☆:ファイバー
○□:光減衰器
実線:シミュレーション



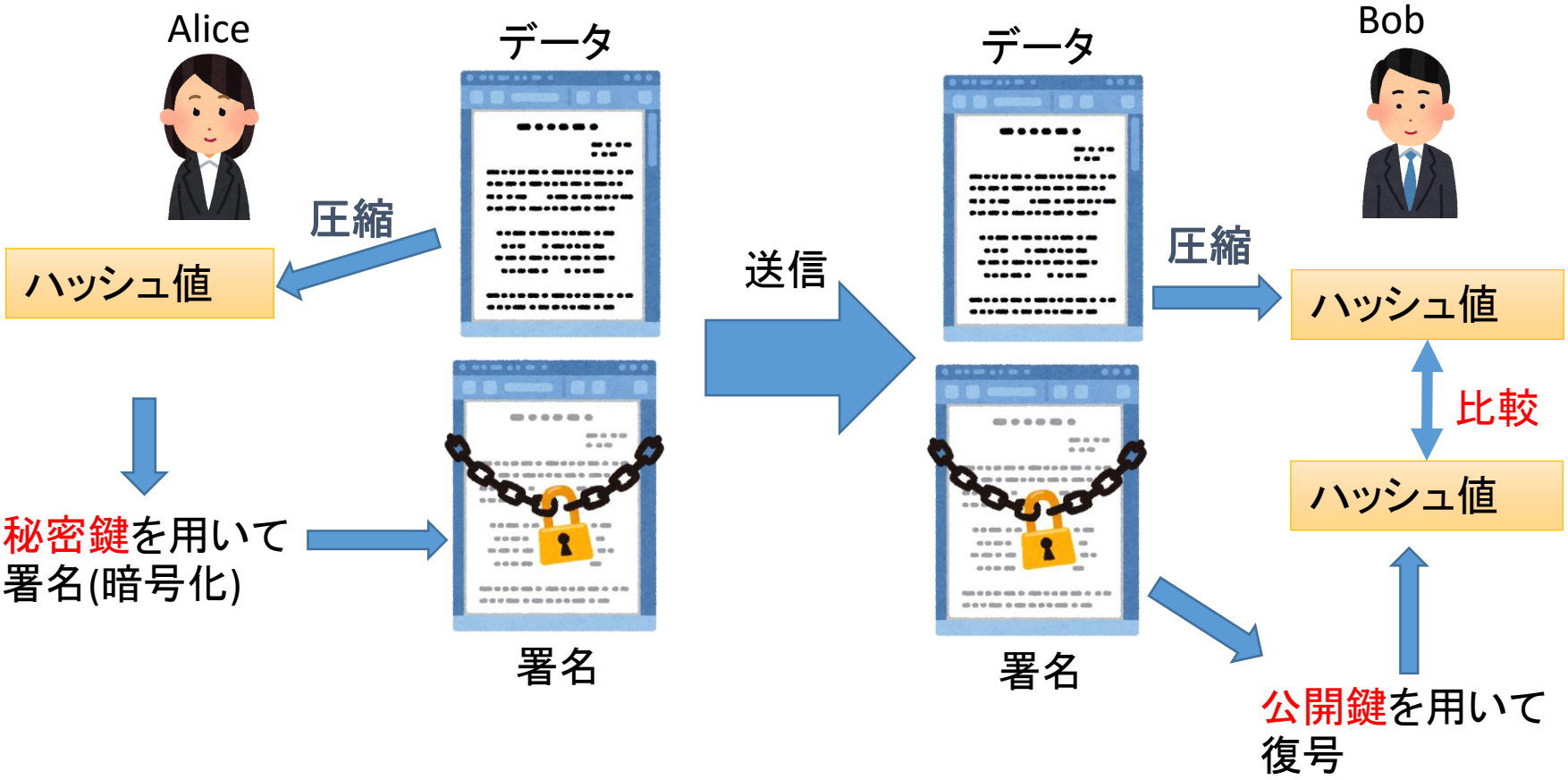
量子デジタル署名
Quantum digital signature: QDS



デジタル署名とは

ハッシュ関数→元の文が少しでも違うと異なった値を返す関数

例：ハッシュ関数を用いた署名



デジタル署名とは

例：ハッシュ関数を用いた署名

秘密鍵は署名者アリスのみが持っている

電子署名を作成できるのはアリスのみ

改ざん✖なりすまし✖

電子署名と送信データが一致すれば、送信者はアリスであり、かつ
データは改ざんされていないことが分かる

量子デジタル署名(QDS)

量子デジタル署名

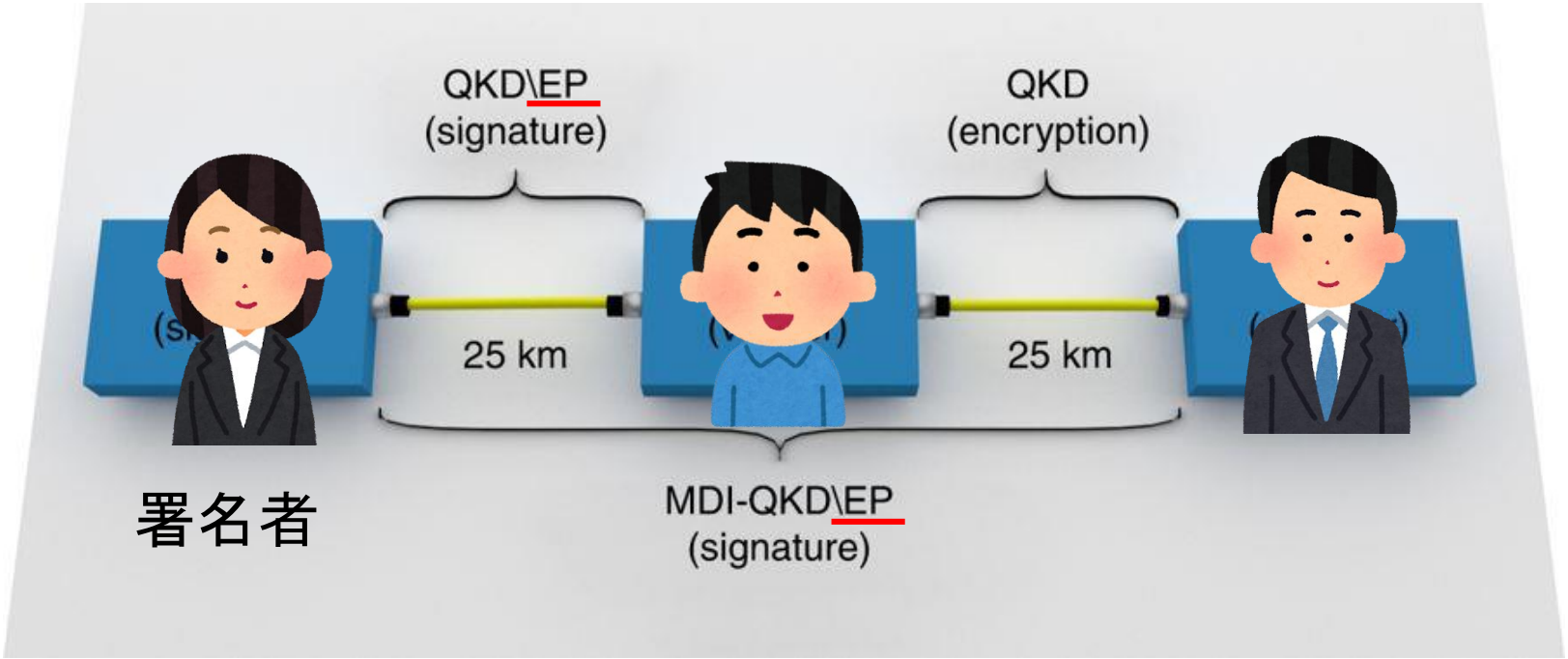
“公開鍵”→量子状態　($|H\rangle|V\rangle|D\rangle|A\rangle$のいずれか)
“秘密鍵”→量子状態を指定するビット

本論文での量子デジタル署名(QDS)

署名する人→Alice

受け取る人→BobとCharlie

Aliceが、1ビットのメッセージに署名をする状況を考える。

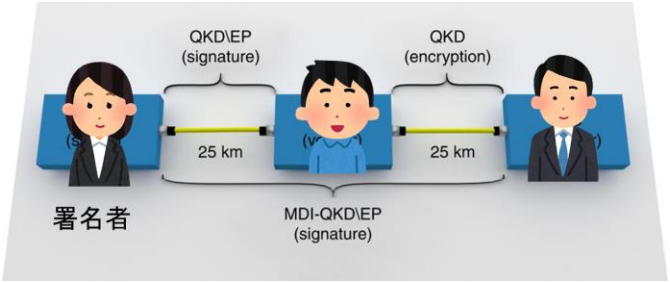


本論文での量子デジタル署名(QDS)

署名する人→Alice

受け取る人→BobとCharlie

Aliceは、1ビットのメッセージに署名をする。



・公開鍵(量子状態)の配布

A_0^B, A_1^Bというそれぞれi=0,1に対応するビット列を、MDI-QKDで量子状態としてBobに送る。

Bobが受け取るビット列をK_0^B, K_1^Bとする。

$$A_i^B \cong K_i^B$$

A_0^B, A_1^Bというそれぞれi=0,1に対応するビット列を、MDI-QKDで量子状態としてBobに送る。
Bobが受け取るビット列をK_0^B, K_1^Bとする。

Alice

Bit	基底	偏光
1	Z	$\|V\rangle$
0	Z	$\|H\rangle$
0	Z	$\|H\rangle$
⋮	⋮	⋮

Bob

Bit	基底	偏光
1	Z	$\|H\rangle$
0	Z	$\|V\rangle$
0	Z	$\|V\rangle$
⋮	⋮	⋮

Charlie

反応した検出器	状態
dH/dV	triplet
cH/dV	singlet
dH/dV	triplet
⋮	⋮

A_i^B

送信する量子状態

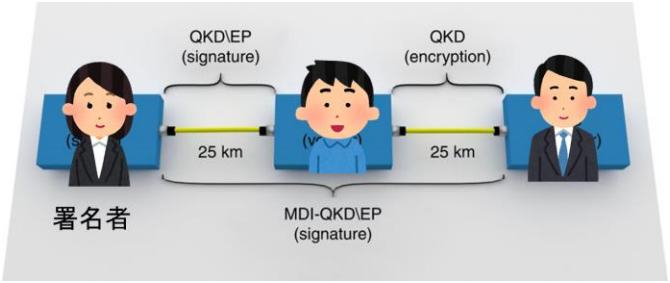
K_i^B

本論文での量子デジタル署名(QDS)

署名する人→Alice

受け取る人→BobとCharlie

Aliceは、1ビットのメッセージに署名をする。



・公開鍵の配布

A_0^B, A_1^Bというそれぞれi=0,1に対応するビット列を、MDI-QKDで量子状態としてBobに送る。

Bobが受け取るビット列をK_0^B, K_1^Bとする。

$$A_i^B \cong K_i^B$$

A_0^C, A_1^Cというそれぞれi=0,1に対応するビット列を、QKDで量子状態としてCharlieに送る。

Charlieが受け取るビット列をK_0^C, K_1^Cとする。

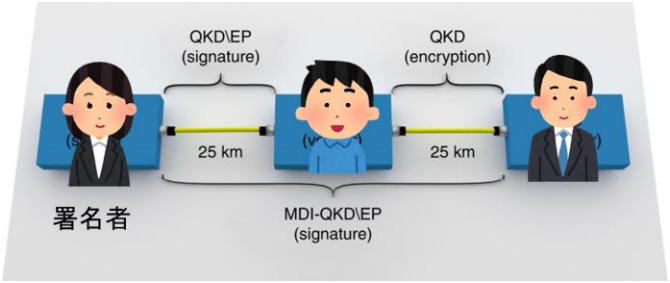
$$A_i^C \cong K_i^C$$

本論文での量子デジタル署名(QDS)

署名する人→Alice

受け取る人→BobとCharlie

Aliceは、1ビットのメッセージに署名をする。



- BobとCharlieの情報の共有

  ビット列K_i^B, K_i^Cの半分をランダムに選び、QKDを用いてBob-Charlie間で共有(両者以外には知られないように)

それぞれが持っている情報

Alice→ $A_0^B,\ A_1^B, A_0^C,\ A_1^C$

Bob→ $K_0^B, K_1^B; K_0^C, K_1^C$の半分

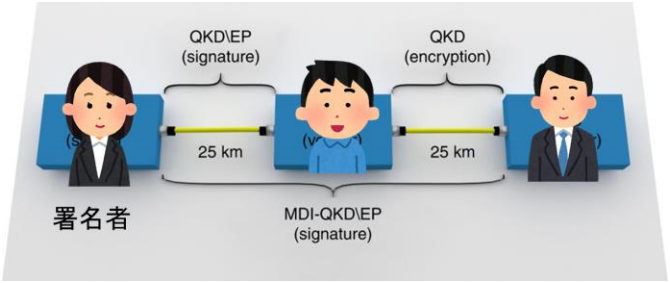
Charlie→ $K_0^C, K_1^C; K_0^B, K_1^B$の半分

本論文での量子デジタル署名(QDS)

署名する人→Alice

受け取る人→BobとCharlie

Aliceは、1ビットのメッセージに署名をする。



・メッセージの送信

i=0なら$\{0, A_0^B, A_0^C\}$を送る。

i=1なら$\{1, A_1^B, A_1^C\}$を送る。

BobとCharlieは、自分の持っている情報と送信された情報が一致しているかを確認。

本論文での量子デジタル署名(QDS)

署名する人→Alice

受け取る人→BobとCharlie

Aliceは、1ビットのメッセージに署名をする。

それぞれが持っている情報

Alice→ $A_0^B,\ A_1^B, A_0^C,\ A_1^C$

Bob→ $K_0^B, K_1^B; K_0^C, K_1^C$の半分

Charlie→ $K_0^C, K_1^C; K_0^B, K_1^B$の半分

・メッセージの送信

i=0なら$\{0, A_0^B, A_0^C\}$を送る。

i=1なら$\{1, A_1^B, A_1^C\}$を送る。

BobとCharlieは、自分の持っ

一致しているかを確認。

$A_i^B \cong K_i^B, A_i^C \cong K_i^C$なので、一致していれば送信者がAliceであることが分かる。

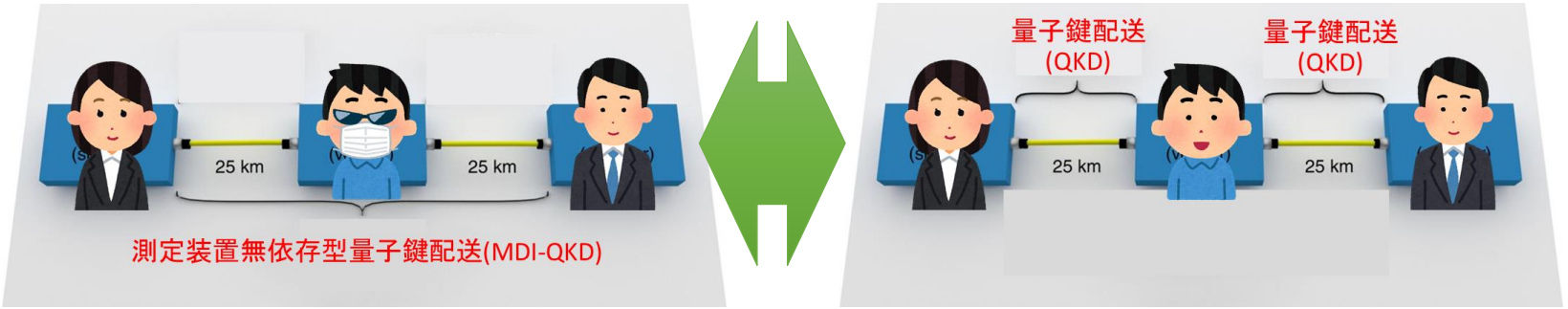
結果

$\left|A_i^B\right| = \left|A_i^C\right| = 2.5 \times 10^6\ bits$のデータを送信。

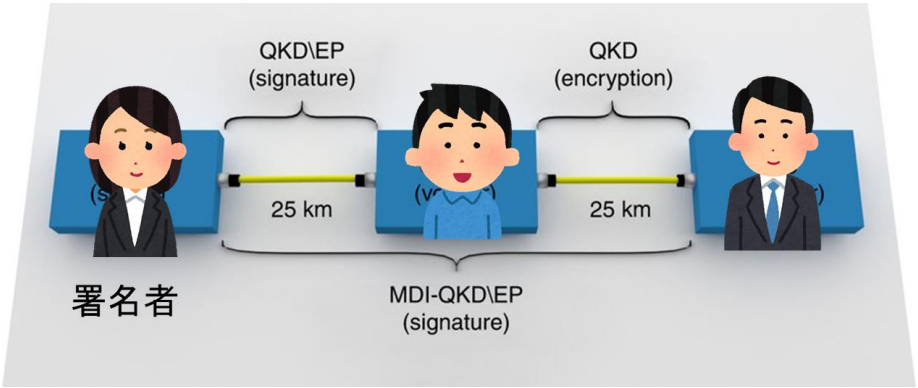
署名の失敗確率が0.5×10^{-10}となった。

まとめ

- 3者間で、測定装置無依存型量子鍵配送(MDI-QKD)と量子鍵配送(QKD)を、同一の装置を切り替えて実現した。



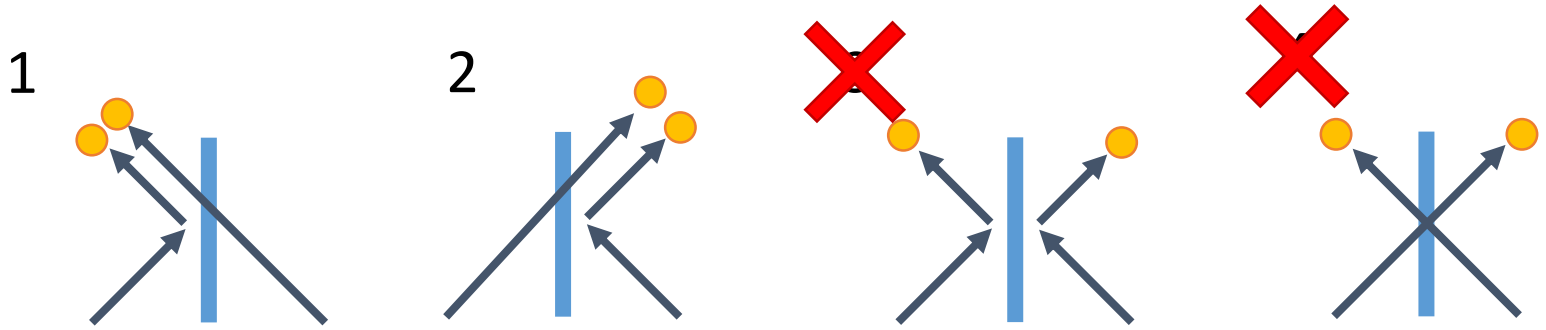
- 量子鍵配送(QKD)と測定装置無依存型量子鍵配送(MDI-QKD)を用いて量子デジタル署名(QDS)を行った。



補足↓

Hong-Ou-Mandel効果

区別のつかない2光子が同時に入射した場合、量子的な干渉によって別々の出力に1個ずつ光子が現れることがなくなる。



HOM効果によりこれらの可能性はなくなる

	Z基底	X基底
0	$\|H\rangle$	$\|D\rangle$
1	$\|V\rangle$	$\|A\rangle$

量子通信路と古典通信路

- 量子通信路
  - 光子を送る通信路(例:光ファイバー)
  - 盗聴、改ざんされる恐れあり

- 古典通信路
  - 通常の通信に使われる通信路
  - 盗聴はされるが改ざんはされない

ベル測定

・Bell測定

→Bell状態を区別する測定のこと

Bell状態

$$|\psi^-\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}} - |V\rangle_{\mathrm{A}}|\mathrm{H}\rangle_{\mathrm{B}}) \quad \text{-(1)}$$

$$|\psi^+\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}} + |V\rangle_{\mathrm{A}}|\mathrm{H}\rangle_{\mathrm{B}}) \quad \text{-(2)}$$

$$|\Phi^-\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|H\rangle_{\mathrm{B}} - |V\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}}) \quad \text{-(3)}$$

$$|\Phi^+\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|H\rangle_{\mathrm{B}} + |V\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}}) \quad \text{-(4)}$$

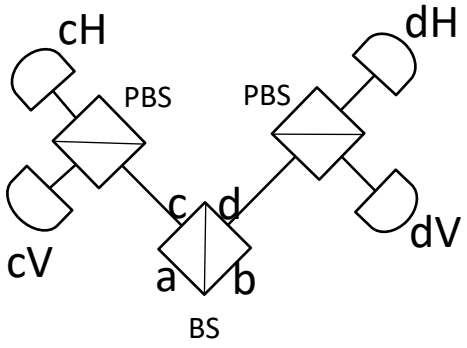
ベル測定

- $|\psi^-\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}} - |V\rangle_{\mathrm{A}}|\mathrm{H}\rangle_{\mathrm{B}})$ -(1)

  cH,dVあるいはdH,cVが反応

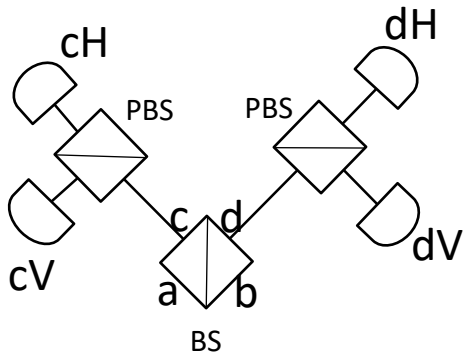
- $|\psi^+\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}} + |V\rangle_{\mathrm{A}}|\mathrm{H}\rangle_{\mathrm{B}})$ -(2)

  cH,cVあるいはdH,dVが反応



ベル測定２

- $|\Phi^-\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|H\rangle_{\mathrm{B}} - |V\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}})$ -(3)
- $|\Phi^+\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|H\rangle_{\mathrm{A}}|H\rangle_{\mathrm{B}} + |V\rangle_{\mathrm{A}}|V\rangle_{\mathrm{B}})$ -(4)
- cH,cV,dH,dVのいずれかが反応



ベル測定３

・(1)(2)の時は、測定器のうち２か所が反応する

・(3)(4)の時は、測定器のうち１か所だけが反応し、区別はできない

(1)(2)の場合だけ残し、他は廃棄する

安全性

- $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B)$ -(1)

$$= \frac{1}{\sqrt{2}}(|D\rangle_A|A\rangle_B - |A\rangle_A|D\rangle_B)$$

- $|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B)$ -(2)

$$= \frac{1}{\sqrt{2}}(|D\rangle_A|D\rangle_B - |A\rangle_A|A\rangle_B)$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

状態はXZどちらの基底でも書けるため、送信者の送った基底を知るのは不可能

また、どちらの偏光を送ったかも完全にランダムに決定されるため、偏光を知ることも不可能