Quantum Cryptography Based on Bell's Theorem

Bellの定理を用いた量子暗号

Artur K. Ekert

Phys. Rev. Lett. **67**, 661 (1991).

10-041-005
石井　伴旺

・発表の概要

エンタングルしたスピン対を用いて秘密鍵を共有し

盗聴者の有無を判断するのにBellの定理を用いるような

量子暗号方式　E91プロトコルの紹介をする

・発表の流れ

1) 導入

・秘密鍵とは

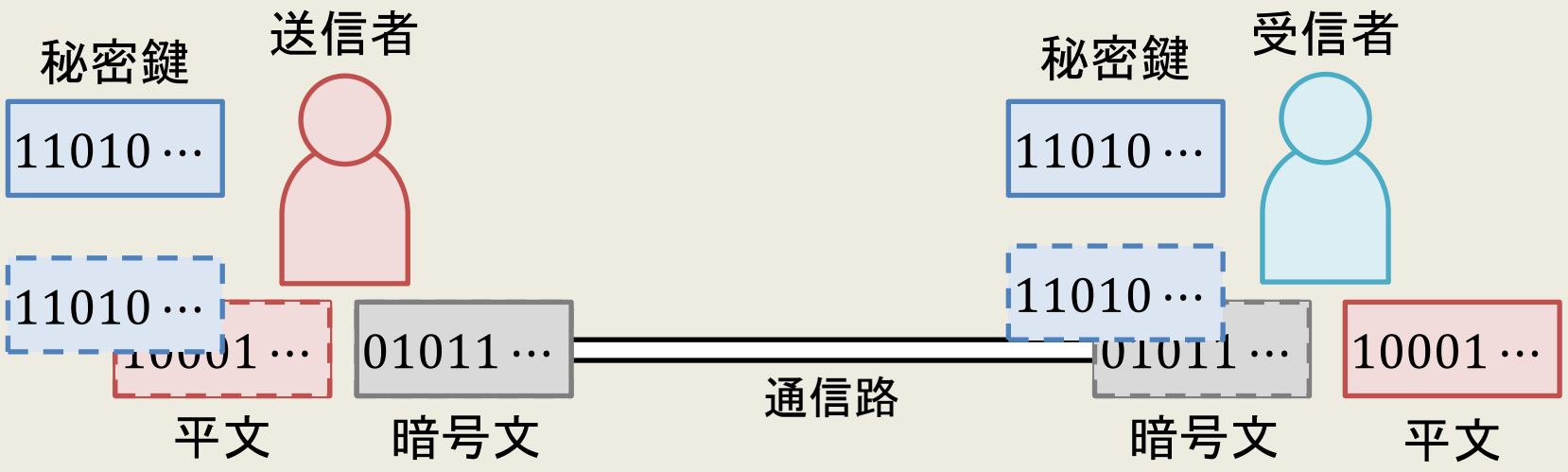
・エンタングルしたスピン対

2) E91プロトコルの操作

3) E91プロトコルの安全性

4) まとめ

・導入(秘密鍵とは)



秘密鍵とは 0 と 1 がランダムに並んだビット列のこと

暗号通信を行う送信者と受信者が共有をし

平文（送る情報）から暗号文を生成　したり　暗号文から平文を復号

する際に使う

第三者に秘密鍵が知られていなければ安全な暗号通信を行うことができる

送信者と受信者は第三者に知られないよう
秘密鍵を共有する必要がある

・導入(エンタングルしたスピン対)

2つのスピン1/2の粒子から成り

x軸方向のスピンの固有状態 $|\uparrow_x\rangle, |\downarrow_x\rangle$ を用いて

$$\frac{1}{\sqrt{2}}\left[\ \underbrace{|\uparrow_x\rangle_a \otimes |\downarrow_x\rangle_b}_{①} \ - \ \underbrace{|\downarrow_x\rangle_a \otimes |\uparrow_x\rangle_b}_{②}\ \right]$$

と表せるような状態のこと

2つの粒子に対して同じ方向のスピン成分を測定したときの結果は

粒子aが up なら 粒子bは $down$ に …①

粒子aが $down$ なら 粒子bは up に …②

なるという相関がある

スピンの測定値が up or $down$ で観測される確率はそれぞれ $1/2$

・発表の流れ

1) 導入

・秘密鍵とは

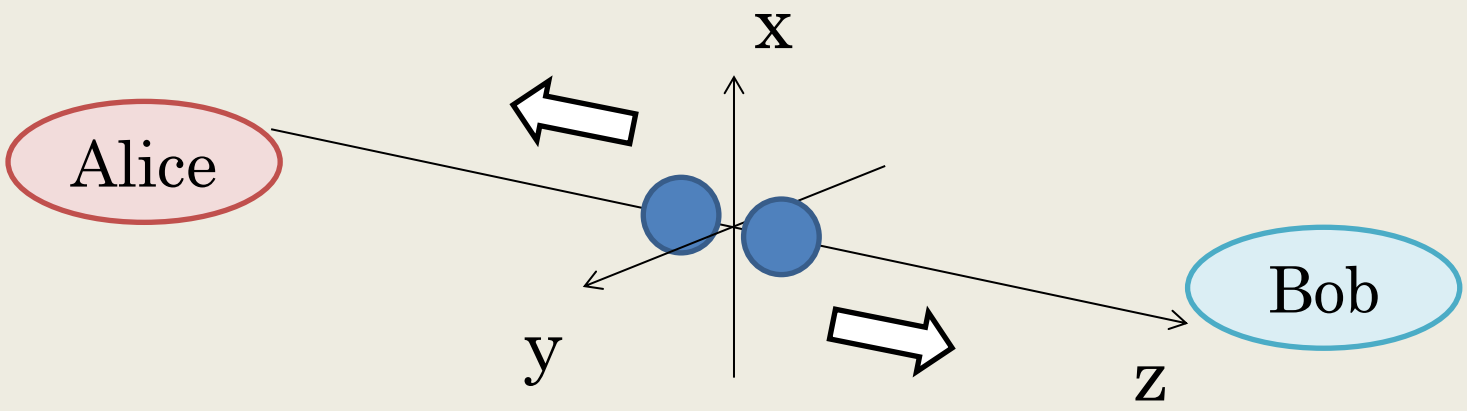
・エンタングルしたスピン対

2) E91プロトコルの操作

3) E91プロトコルの安全性

4) まとめ

・E91プロトコル(操作①)

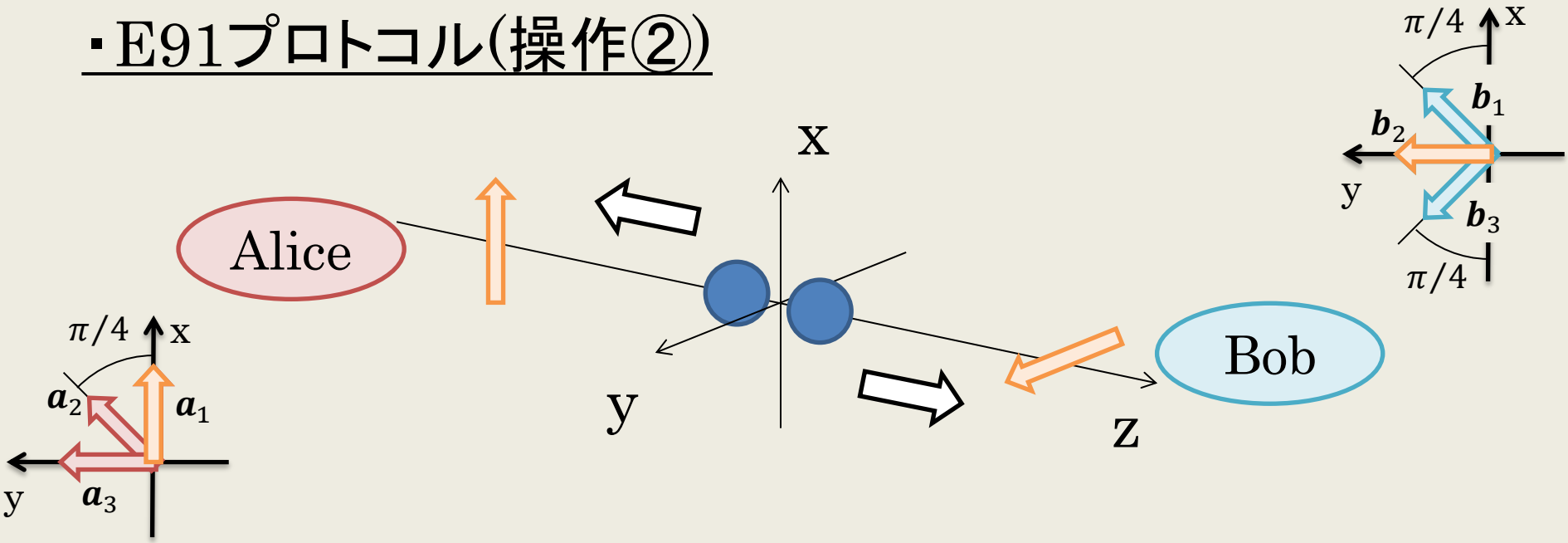


エンタングルしたスピン対を生成し

片方の粒子をAliceへ　　もう片方の粒子をBobへ

次々と送るような系を考える

・E91プロトコル(操作②)



やってきた粒子に対し

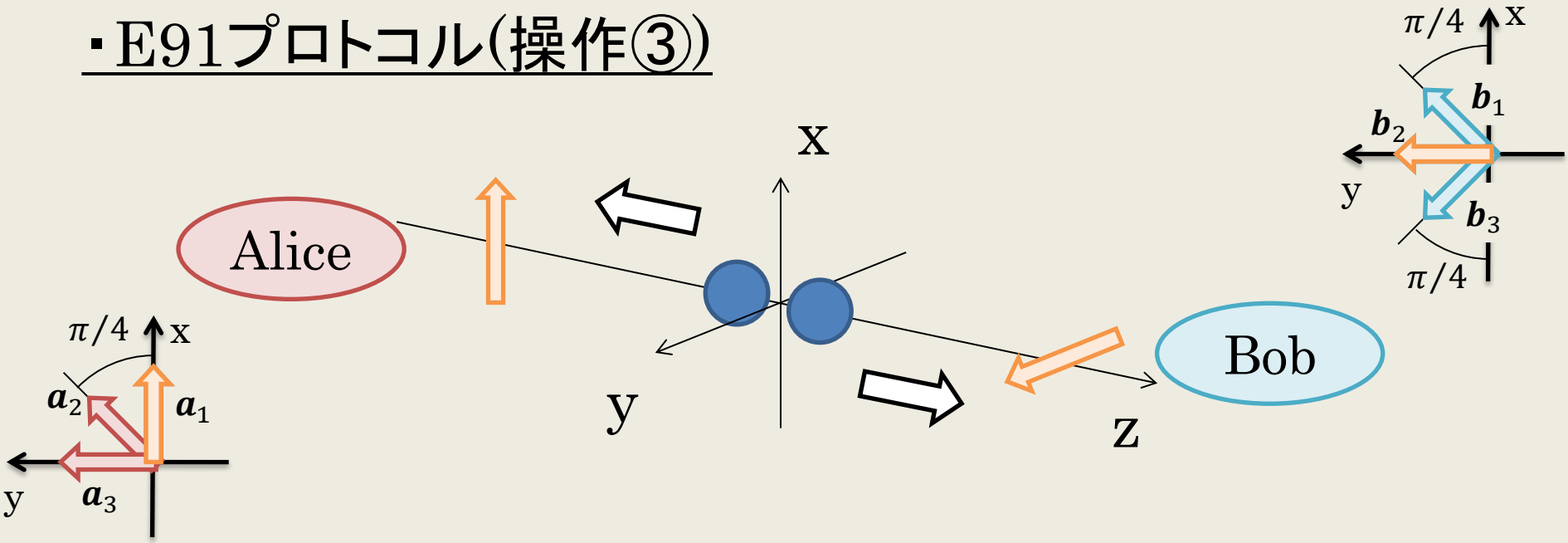
Aliceは　$\boldsymbol{a}_i$ (i = 1 , 2 , 3) の中から　　Bobは　$\boldsymbol{b}_j$ (j = 1 , 2 , 3) の中から

それぞれランダムに1つの方向を選びその方向のスピン成分を測る

測定したスピン成分の方向 $\boldsymbol{a}_i$, $\boldsymbol{b}_j$	と	測定値が　up か　$down$ か

を記録する

・E91プロトコル(操作③)



a_i , b_j からランダムに1つの方向を選ぶ

↓

その方向の粒子のスピン成分を測定する

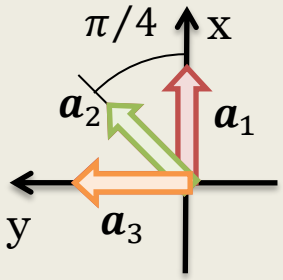
↓

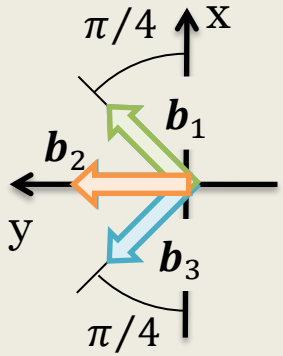
スピン成分の方向 と *up* か *down* か を記録する

以上の操作を送られてくる
粒子にくり返し行う

・E91プロトコル(操作④)

	Alice		Bob	
	スピン成分の方向	*up* or *down*	スピン成分の方向	*up* or *down*
1回目	$\boldsymbol{a}_2$	*down*	$\boldsymbol{b}_2$	*down*
2回目	$\boldsymbol{a}_1$	*down*	$\boldsymbol{b}_2$	*up*
3回目	$\boldsymbol{a}_2$	*up*	$\boldsymbol{b}_1$	*down*
⋮	⋮	⋮	⋮	⋮





AliceとBobは各粒子に対して測ったスピン成分の方向だけを公開する

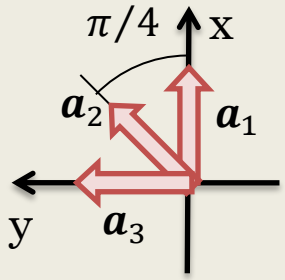
公開したスピン成分の方向に着目し

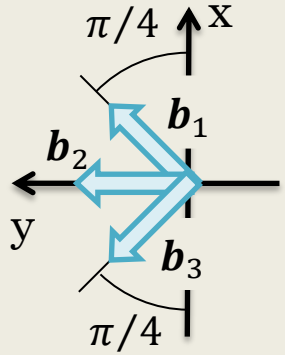
AliceとBobが同じ方向のスピン成分を測定したとき 以外 の*up or down* を公開する

($(\boldsymbol{a}_2, \boldsymbol{b}_1)$ または $(\boldsymbol{a}_3, \boldsymbol{b}_2)$ のとき)

・E91プロトコル(操作)

	Alice		Bob	
	スピン成分の方向	*up* or *down*	スピン成分の方向	*up* or *down*
1回目	$\boldsymbol{a}_2$		$\boldsymbol{b}_2$	
2回目	$\boldsymbol{a}_1$		$\boldsymbol{b}_2$	
3回目	$\boldsymbol{a}_2$		$\boldsymbol{b}_1$	
⋮	⋮		⋮	

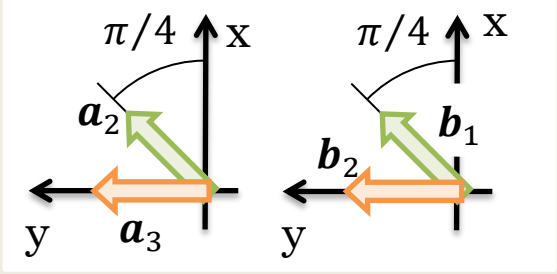




AliceとBobは各粒子に対して測ったスピン成分の方向だけを公開する

秘密鍵 (ビット列) を共有する

・E91プロトコル(操作⑤)



AliceとBobが 同じ方向 のスピン成分を測ったときの *up or down* に着目し

Aliceが *up* のときビットを 1　　Aliceが *down* のときビットを 0

Bobが *down* のときビットを 1　　Bobが *up* のときビットを 0

とすれば 0と1 がランダムにならんだビット列が手に入る

	Alice			Bob		
	スピン成分の方向	*up or down*	ビット	スピン成分の方向	*up or down*	ビット
3回目	a_2	*up*	1	b_1	*down*	1
m回目	a_3	*down*	0	b_2	*up*	0
n回目	a_3	*down*	0	b_2	*up*	0

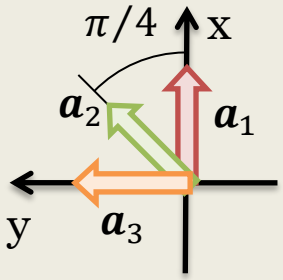
ビット列 (秘密鍵)

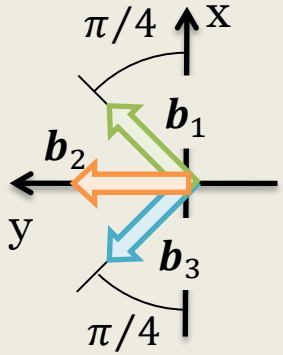
1 … 0 … 0 …

が共有できた

・E91プロトコル(操作)

	Alice		Bob	
	スピン成分の方向	*up* or *down*	スピン成分の方向	*up* or *down*
1回目	$\boldsymbol{a}_2$	*down*	$\boldsymbol{b}_2$	*down*
2回目	$\boldsymbol{a}_1$	*down*	$\boldsymbol{b}_2$	*up*
3回目	$\boldsymbol{a}_2$		$\boldsymbol{b}_1$	
⋮	⋮	⋮	⋮	⋮





公開したスピン成分の方向に着目し

AliceとBobが同じ方向のスピン成分を測定したとき 以外 の*up or down* を公開する

⇨ 公開したデータからBellの定理を検証し盗聴の有無を調べる

・発表の流れ

1) 導入

・秘密鍵とは

・エンタングルしたスピン対

2) E91プロトコルの操作

3) E91プロトコルの安全性

4) まとめ

・E91プロトコルの安全性

エンタングルしたスピン対が送られる

盗聴者が操作できる

AliceとBobが送られた粒子に対しスピン成分を測定する

AliceとBobが測定したスピン成分の方向と ,測定結果の一部を公開する

秘密鍵が共有される

盗聴者は操作できない
（と仮定する）

送られる途中の粒子から測定結果を得ることは出来ないか

盗聴者が粒子を送ることで秘密鍵の情報を得ることは出来ないか

ということが考えられる

・E91プロトコルの安全性

AliceとBobに送られる粒子から盗聴者はAliceとBobの測定結果を得ることが出来るか

盗聴者がAliceとBobに定まったスピンの状態を送るような盗聴は可能か

という2つについて考える

・E91プロトコルの安全性

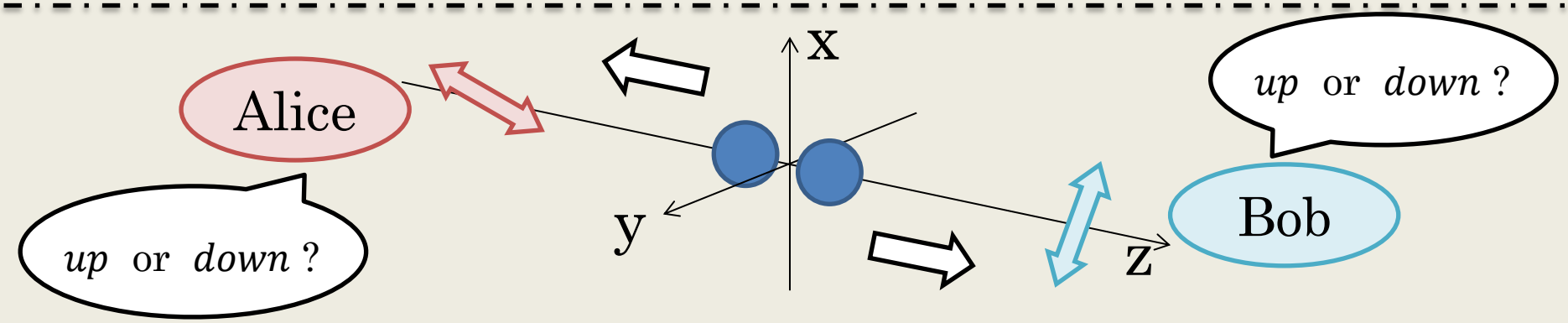
AliceとBobに送られる粒子から盗聴者はAliceとBobの測定結果を得ることが出来るか

盗聴者がAliceとBobに定まったスピンの状態を送るような盗聴は可能か

という2つについて考える

・E91プロトコルの安全性

AliceとBobに送られる粒子から盗聴者はAliceとBobの測定結果を得ることが出来るか



系の状態はx軸方向のスピンの固有状態 $|\uparrow_x\rangle, |\downarrow_x\rangle$ を用いて

$$\frac{1}{\sqrt{2}}\left[\ |\uparrow_x\rangle \otimes |\downarrow_x\rangle \ - \ |\downarrow_x\rangle \otimes |\uparrow_x\rangle\ \right]$$

と表される

AliceとBobがそれぞれ粒子のスピンを測定したときの結果は

1/2の確率で　　up or down　　となる

測定結果は完全にランダム　⇒　測定結果の情報は状態の中に含まれない

⇒　盗聴者は情報を得ることはできない

・E91プロトコルの安全性

AliceとBobに送られる粒子から盗聴者はAliceとBobの測定結果を得ることが出来るか

得ることはできない

盗聴者がAliceとBobに定まったスピンの状態を送るような盗聴は可能か

という2つについて考える

・E91プロトコルの安全性

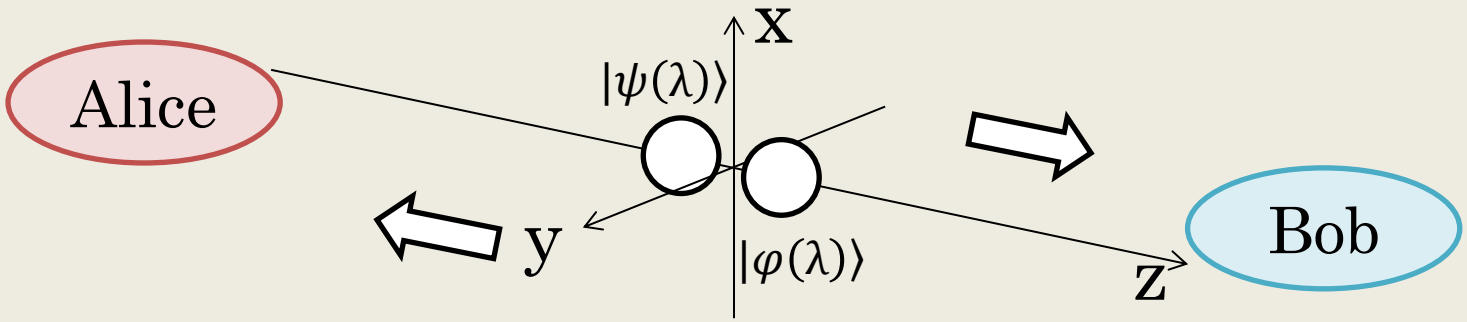
AliceとBobに送られる粒子から盗聴者はAliceとBobの測定結果を得ることが出来るか

盗聴者がAliceとBobに定まったスピンの状態を送るような盗聴は可能か

という2つについて考える

・E91プロトコルの安全性

盗聴者がAliceとBobに定まったスピンの状態を送るような盗聴は可能か



盗聴者がAliceに$|\psi(\lambda)\rangle$　Bobに$|\varphi(\lambda)\rangle$　のスピン状態が定まった粒子を送ったとする

そのとき系の状態は　　$|\psi(\lambda)\rangle \otimes |\varphi(\lambda)\rangle$　と表せる

λ は系の振る舞いを表すパラメーターで　λ が定まると

・AliceとBobに送られる状態

・AliceとBobのスピン成分の測定値の確率分布　　が決まる

・E91プロトコルの安全性

$a_i\,, b_j\quad (i\,, j = 1\,, 2\,, 3)$ を

Aliceが粒子の $\boldsymbol{a}_i$ 方向のスピン成分を測定した結果が

up なら　$a_i = 1$　　$down$ なら　$a_i = -1$

Bobが粒子の $\boldsymbol{b}_j$ 方向のスピン成分を測定した結果が

up なら　$b_j = 1$　　$down$ なら　$b_j = -1$

と定義する

パラメーター λ が決まると測定結果も定まるので $a_i\,, b_j$ は $a_i(\lambda)\,, b_j(\lambda)$ と表せる

盗聴者が粒子を送った際　パラメーターが λ となる確率を$p(\lambda)$ とすると

積 $a_i b_j$ の期待値 $\langle a_i b_j \rangle$ は　$\langle a_i b_j \rangle = \sum_{\lambda} p(\lambda)\, a_i(\lambda)\, b_j(\lambda)$　となる

・E91プロトコルの安全性

$$\langle a_i b_j \rangle = \sum_{\lambda} p(\lambda)\, a_i(\lambda)\, b_j(\lambda)$$

ここで次のような値 S を考える

$$S = \langle a_1\, b_1 \rangle - \langle a_1\, b_3 \rangle + \langle a_3\, b_1 \rangle + \langle a_3\, b_3 \rangle$$

$$= \sum_{\lambda} p(\lambda) \{ a_1(\lambda)\, b_1(\lambda) - a_1(\lambda)\, b_3(\lambda) + a_3(\lambda)\, b_1(\lambda) + a_3(\lambda)\, b_3(\lambda) \}$$

$$| a_1(\lambda)\, b_1(\lambda) - a_1(\lambda)\, b_3(\lambda) + a_3(\lambda)\, b_1(\lambda) + a_3(\lambda)\, b_3(\lambda) |$$

$$= | \{ a_1(\lambda) + a_3(\lambda) \} b_1(\lambda) + \{ a_3(\lambda) - a_1(\lambda) \} b_3(\lambda) |$$

$$\leq | a_1(\lambda) + a_3(\lambda) | + | a_3(\lambda) - a_1(\lambda) | = 2$$

となる

（量子力学3 参照）

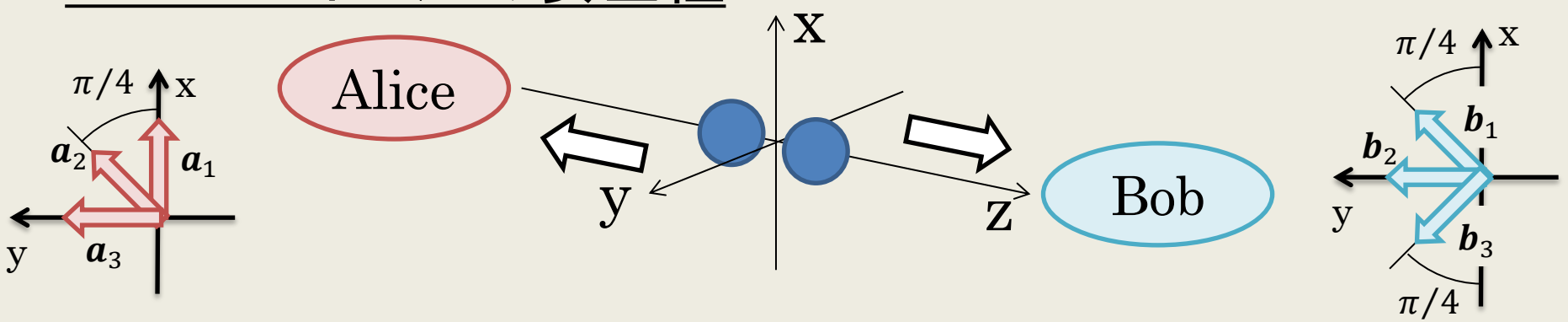
ここで $p(\lambda)$ は確率密度なので

$$-2 \leq S \leq 2$$

となることがわかる

Bellの不等式

・E91プロトコルの安全性

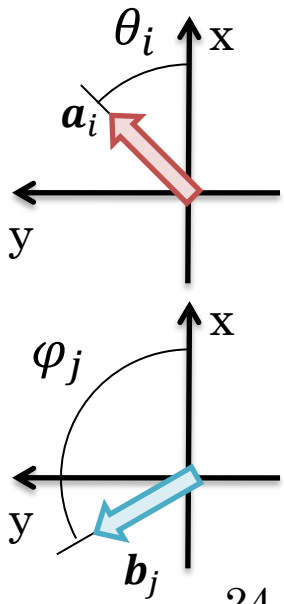


エンタングルしたスピン対からなる系において粒子がそれぞれAliceとBobに送られるとき

Aliceが $\boldsymbol{a}_i$ Bobが $\boldsymbol{b}_j$ 方向のスピンを測定したときの積 $a_i\, b_j$ の期待値 $\langle a_i\, b_j \rangle$ は

$$\langle a_i\, b_j \rangle = -\cos(\theta_i - \varphi_j)$$

（量子力学3 参照）

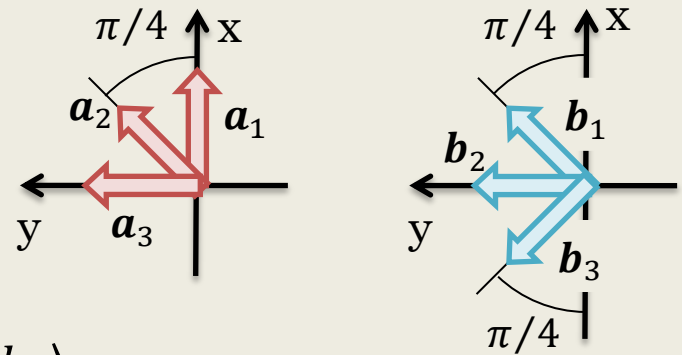


$$S = \langle a_1\, b_1 \rangle - \langle a_1\, b_3 \rangle + \langle a_3\, b_1 \rangle + \langle a_3\, b_3 \rangle$$

$$= -\cos(-\pi/4) + \cos(-3\pi/4) - \cos(\pi/4) - \cos(-\pi/4)$$

$$= -2\sqrt{2}$$

・E91プロトコルの安全性



$$S = \langle a_1\, b_1\rangle - \langle a_1\, b_3\rangle + \langle a_3\, b_1\rangle + \langle a_3\, b_3\rangle$$

について考えると

盗聴者が定まったスピンの状態を送るとき　$-2 \le S \le 2$

2つのエンタングルしたスピンから成る系のとき　$S = -2\sqrt{2}$

AliceとBobがお互いに公開した測定値から上の値 S を計算し

$S < -2$ となったら ⇒ 盗聴者が状態を送っていないことがわかる

⇒ スピンの状態を送るような盗聴は不可能である

・E91プロトコルの安全性

AliceとBobに送られる粒子から盗聴者はAliceとBobの測定結果を得ることが出来るか

盗聴者がAliceとBobに定まったスピンの状態を送るような盗聴は可能か

⇨ 不可能である

という2つについて考える

・E91プロトコルの安全性

AliceとBobに送られる粒子から盗聴者はAliceとBobの測定結果を得ることが出来るか

⇨ 得ることはできない

盗聴者がAliceとBobに定まったスピンの状態を送るような盗聴は可能か

⇨ 不可能である

という2つについて考える

・発表の流れ

1) 導入

・秘密鍵とは

・エンタングルしたスピン対

2) E91プロトコルの操作

3) E91プロトコルの安全性

4) まとめ

・まとめ

エンタングルしたスピン対から成る系を用いることで秘密鍵を共有することが出来ることを示した

・盗聴者が粒子からAliceとBobの測定結果を得ようとしても

⇨ エンタングルしたスピン対から成る系なので得ることはできない

・盗聴者が定まったスピンの状態を送るような盗聴を行うことを考えても

⇨ 測定値からBellの不等式が破れていることが分かればそのような盗聴が無いことが分かる

エンタングルしたスピン対と量子暗号の安全性の関連性が示された