量子情報数理特論

（第1回）イントロダクション

2021年4月7日

電気通信大学 大学院情報理工学研究科

小川朋宏

講義内容（進度は適宜調整します）

（第2〜7回）量子系に関する基礎事項

Hilbert空間，リースの表現定理とブラケット記法，エルミート作用素，非負定値作用素，トレース，量子系の状態と測定，混合状態と純粋状態，オブザーバブルと同時測定，射影子，スペクトル分解，合成系，テンソル積空間，部分トレース，極分解，特異値分解，Schmidt分解，エンタングルメント，完全正値性と量子通信路，Stinespring表現，Kraus表現

（第8〜11回）量子系の情報量

von Neumann エントロピー，量子相対エントロピー，量子 f −ダイバージェンス，CPTP単調性，Holevo相互情報量，トレース距離，忠実度とUhlmannの定理

（第12〜14回）量子仮説検定理論

量子Steinの補題，量子Neyman-Pearson検定，Audenaertの不等式とHoefding型指数レート，サンドイッチ型の量子相対レニーエントロピー，量子仮説検定における強逆指数レート

（第15回）アドバンスト・トピック　（下記いずれかのトッピックを紹介）

古典・量子通信路符号化 (Holevo-Shumacher-Westmoreland theorem)
量子通信路resolvability
量子盗聴通信路符号化定理 (Devetak Theorem)
量子・量子通信路符号化定理 (Shor-Devetak Theorem)

参考文献の紹介

☆ 量子情報理論の教科書

・石坂智, 小川朋宏, 河内亮周, 木村元, 林正人, 量子情報科学入門, 共立出版, 2012.
（英訳）M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, T. Ogawa,
Introduction to Quantum Information Science, Springer, 2014.
・M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge, 2000.
・林正人, 量子情報理論入門, サイエンス社, 2004.
（英訳増強）M. Hayashi, Quantum Information: An Introduction, Springer, 2006.

☆ 線形代数

・川久保勝夫, 線形代数学, 日本評論社, 1999. （初心者向け）
・日合文雄, 柳研二郎, ヒルベルト空間と線型作用素, 牧野書店, 1995.
・竹内外史, 線形代数と量子力学, 裳華房, 1981. （復刊版が出ている）

☆ 情報理論

・T. M. Cover and J. A. Thomas, Elements of Information Theory, Wiley, 1991.

☆ 量子力学

・J. J. Sakurai, Modern Quantum Mechanics, Addison Wesley, 1985.
（日本語訳）J. J. サクライ, 現代の量子力学, 吉岡書店, 1989.
・清水明, 新版: 量子論の基礎, サイエンス社, 2003.

講義の進め方と成績評価

（１）ZoomとSlackを使います．講義では資料について理解のポイントを主に説明していきます．
- 講義中に質問があれば，Slack「教員への質問」チャンネルに書き込んで下さい．
- マイクをオンにして質問しても結構です．

（２）毎回，簡単な課題（講義を聴けば分かる程度）を出します．
- 講義の翌日までに，Slack の DM（ダイレクトメール）で，レポートとして提出して下さい．
- レポートの形式は自由です．Slack に文章で直接書いて頂いても，
  紙に書いて写真を取るでも，LaTeXをPDFに変換したものでもOKです．
- 事情があって講義に参加出来なかった人は，DMで相談して下さい．

（３）中間レポート，最終レポートとして，１～２回程度，本格的な課題を出します．
- 写真をPDFに変換したり，LaTeXからPDFにしたりして提出をして下さい．

（４）成績評価は（１）（２）による出席評価，（２）（３）によるレポートで行います．
- レポートを重視しますので，すべて出席しても不可になることがあります．

量子力学の導入

（課題 1）偏光フィルターを通過する光の強度について，以下を説明せよ．

(1-1) 古典的電磁波による説明

(1-2) 量子力学による説明

(1-3) 古典的電磁波による説明はなぜ実験事実を説明することが出来ないか？

（課題 2）ディラックのブラケット記法

(2-1) ケットベクトル

$$|\psi\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad |\varphi\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

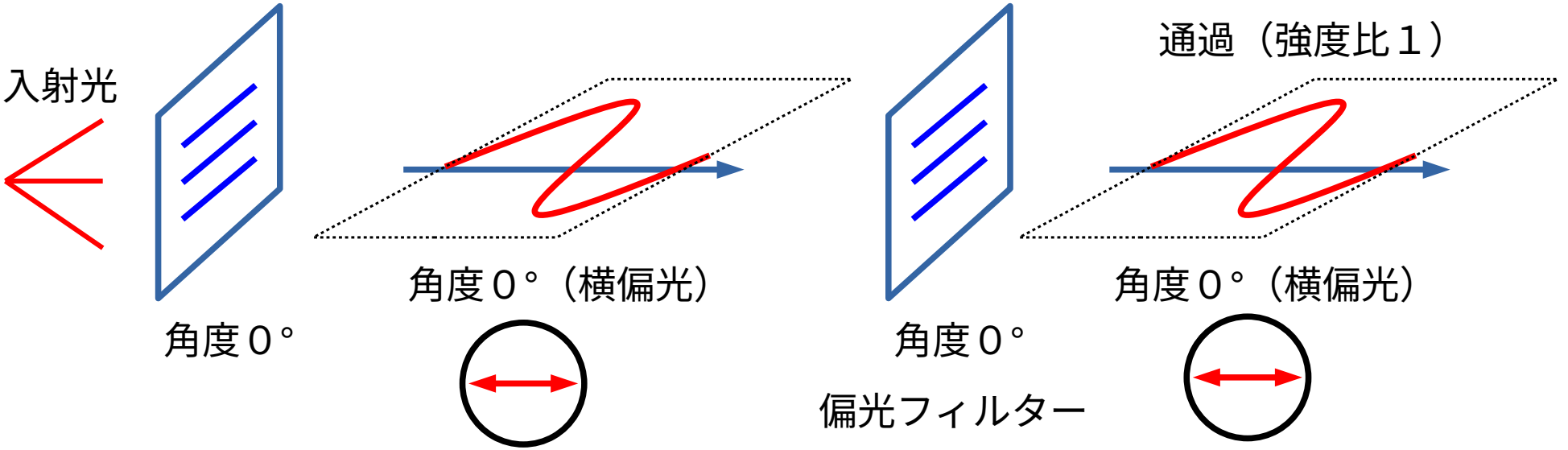
について，ブラベクトル $\langle\psi|$, $\langle\varphi|$ を求めよ．

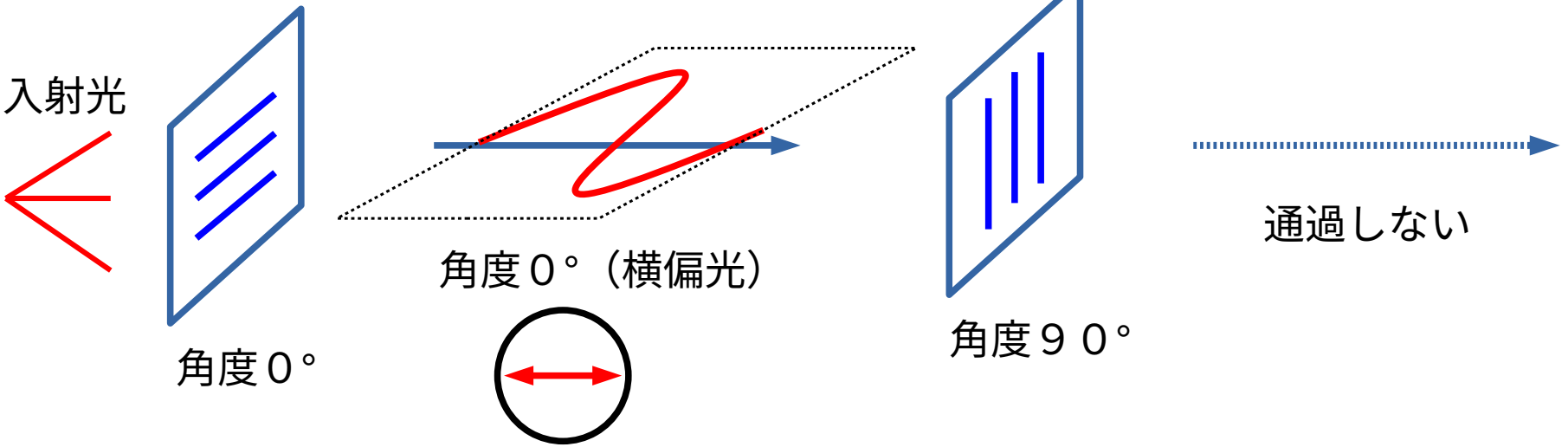
(2-2) 内積 $\langle\psi\,|\,\psi\rangle$, $\langle\psi\,|\,\varphi\rangle$ を求めよ．

光の偏光と偏光フィルター

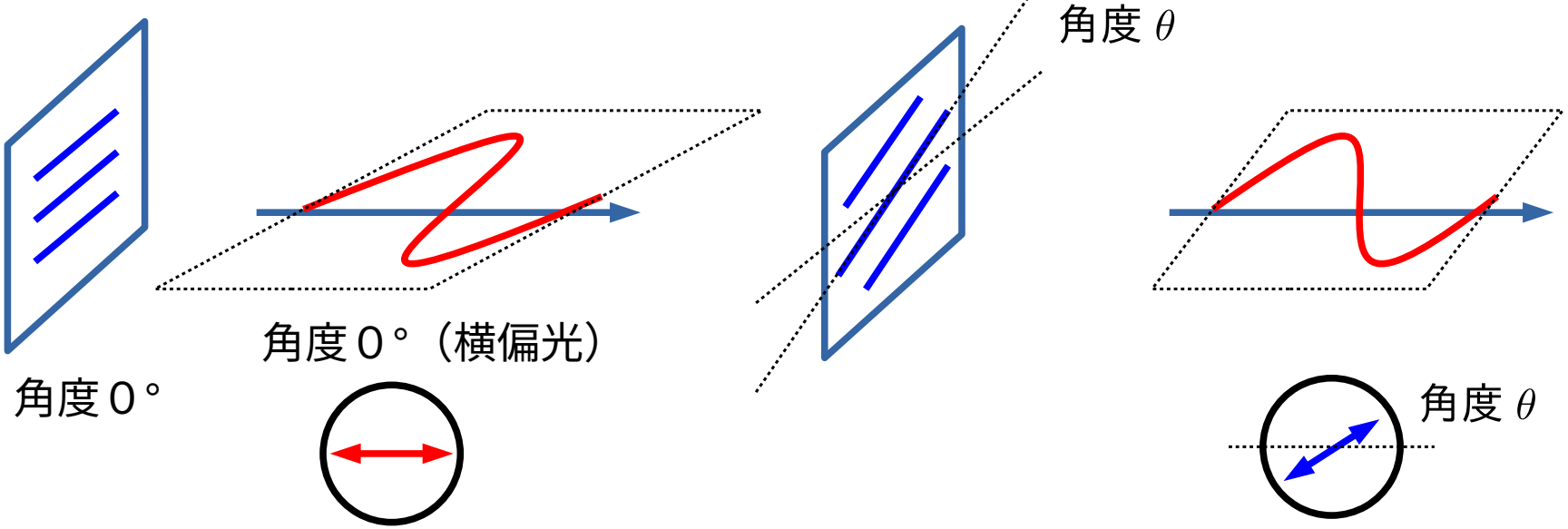
☆ 光は電磁波の一種で，横波である．
（進行方向に垂直な方向に，電場と磁場が互いに振動しながら伝播する）

☆ 偏光フィルターは特定の振動方向を選択的に通過させる性質を持つ．



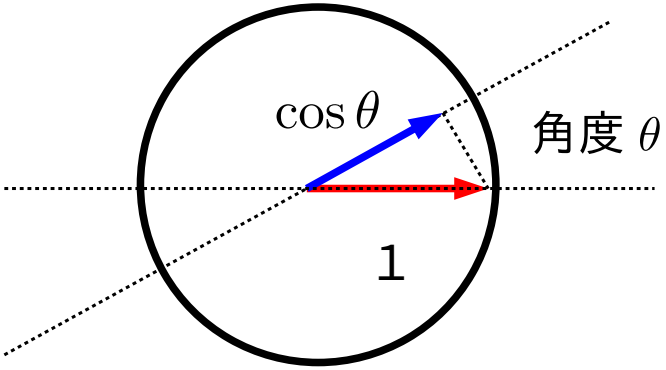


一般の角度に置いた偏光フィルター



振動方向ベクトルの射影成分は $\cos\theta$ ⟶ 強度比は 2 乗 $\cos^2\theta$

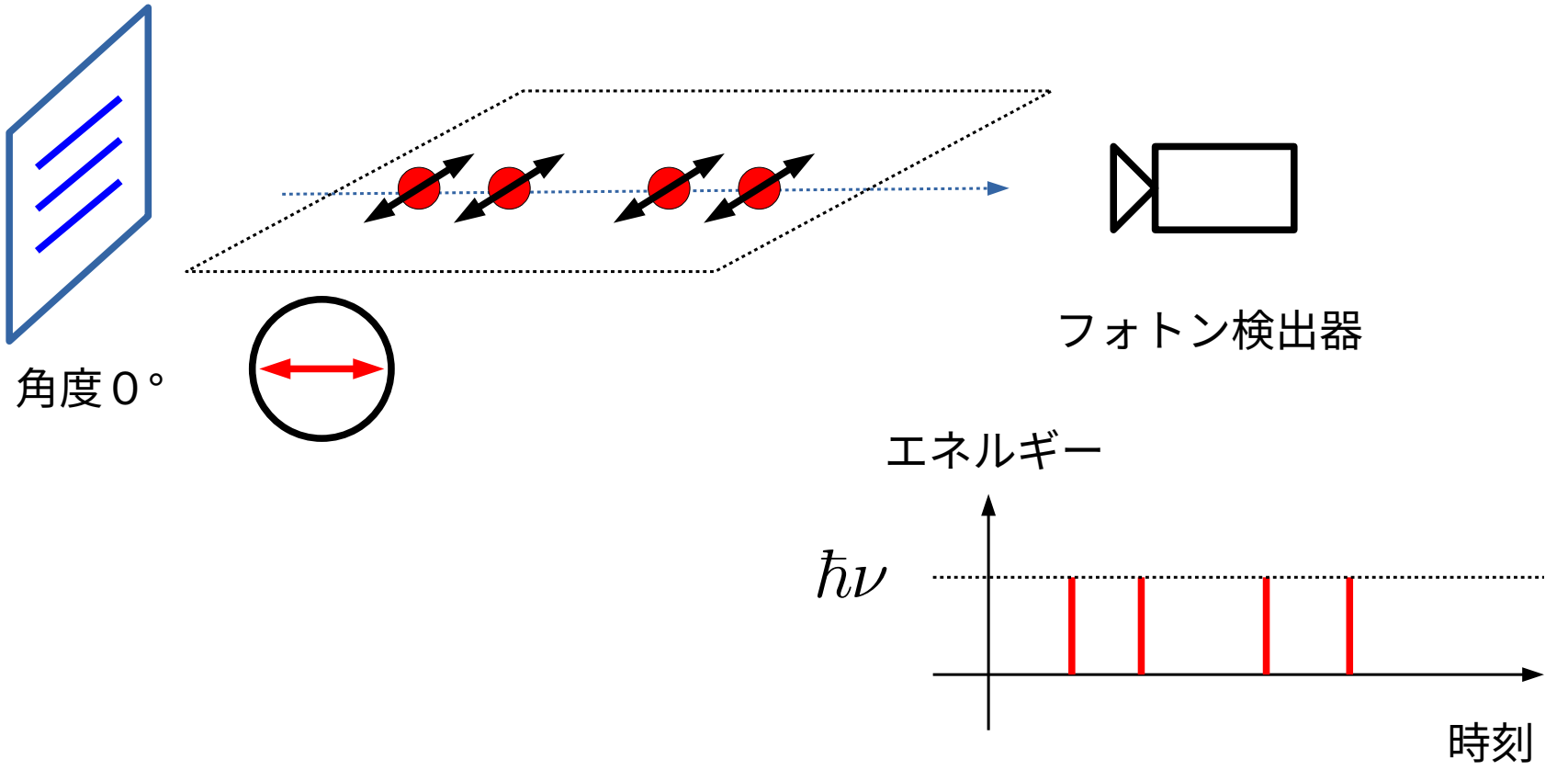
（Wikipediaより）



（偏光フィルターの応用）
自動車のフロントガラス，
サングラス，カメラのフィルター

☆ 偏光フィルターと同じ方向の「波の射影成分」だけ通過する，と考えて良いか？

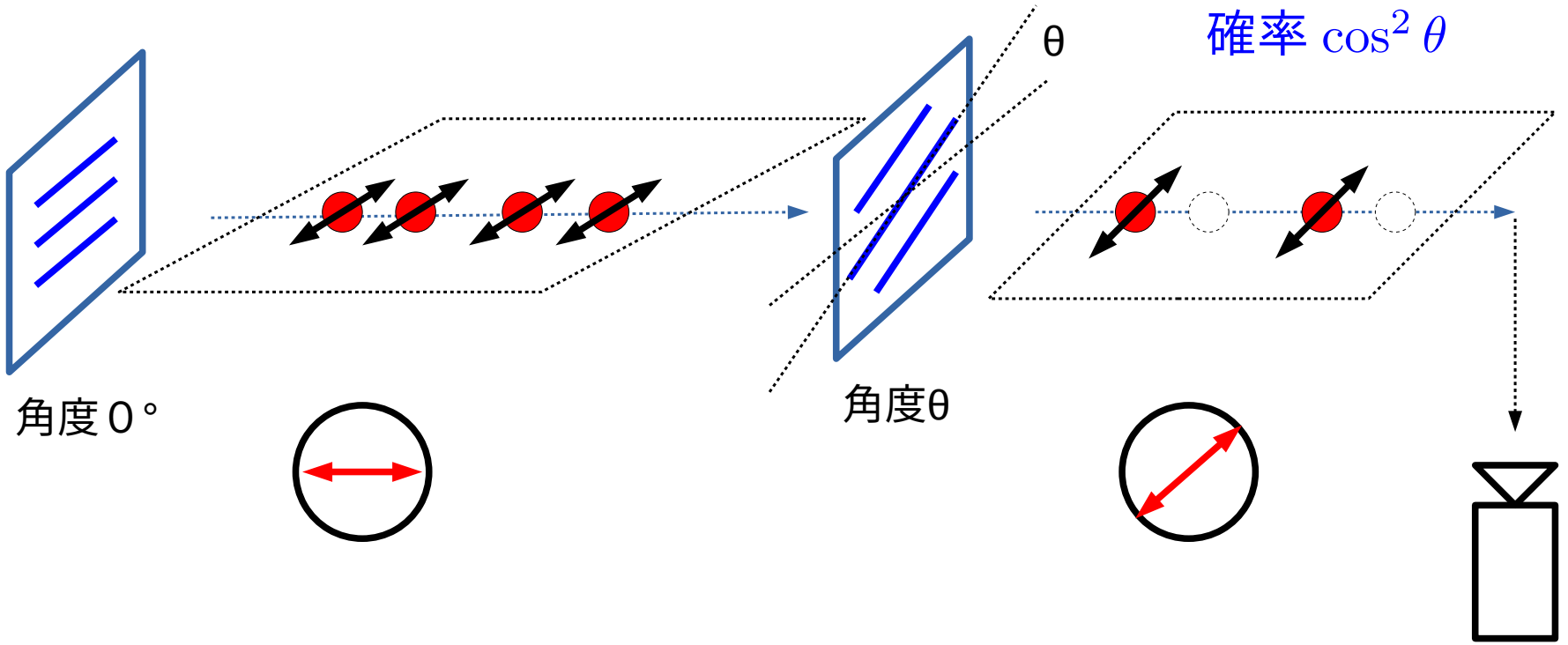
微弱なレーザーはフォトンとして振る舞う



☆ 光には分割が不可能なエネルギー単位（プランク定数×振動数）がある

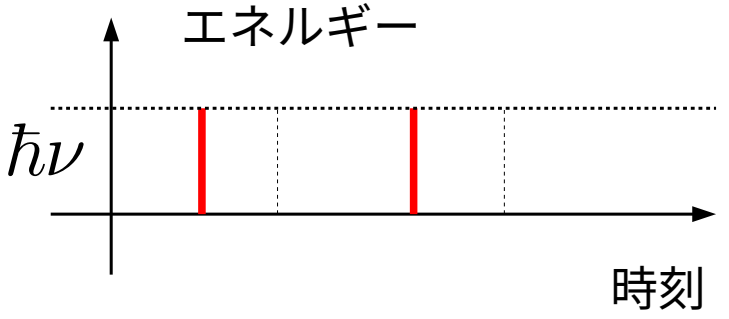
☆ 光の性質を調べたり，光を利用するには量子力学が必要

偏光フィルターの量子力学による説明



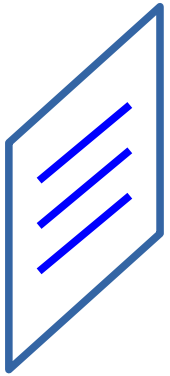
☆ 一つのフォトンが通過するか，通過しないかは，
確率的にしか予言することが出来ない．

通過する確率は $\cos^2\theta$

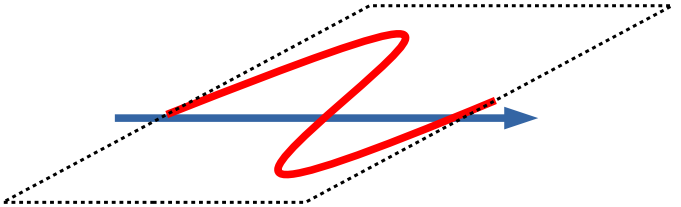


☆ 偏光フィルターを通過したフォトンの偏光状態は？

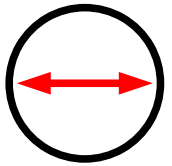
古典的な実験事実と考察

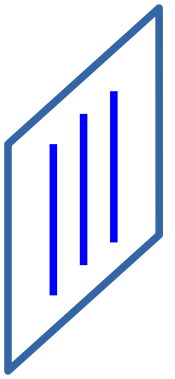


角度０°



角度０°（横偏光）

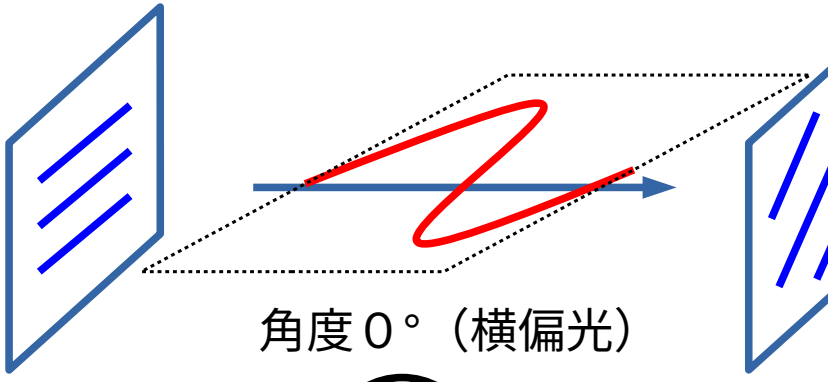




通過しない

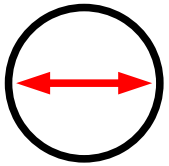
角度９０°

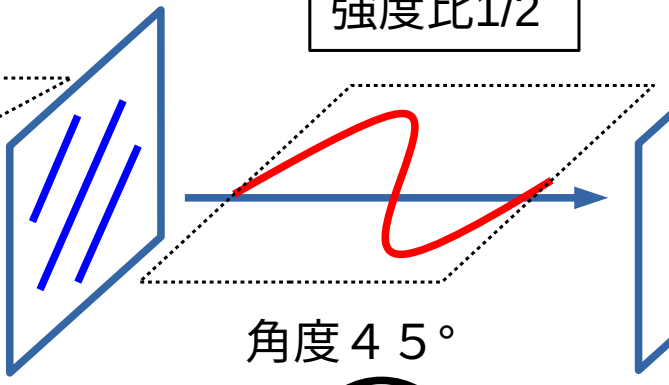
☆ 間に角度４５°の偏光フィルターを入れると？



角度０°

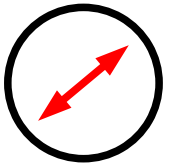
角度０°（横偏光）



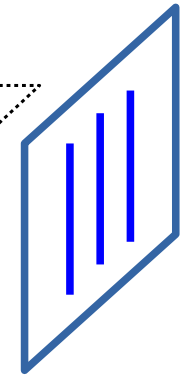


角度45°

角度４５°

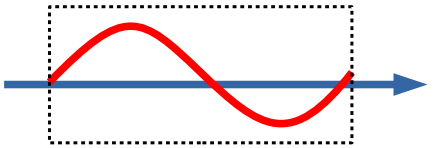


強度比1/2

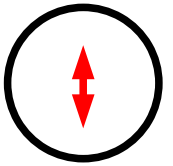


角度９０°

強度比さらに1/2

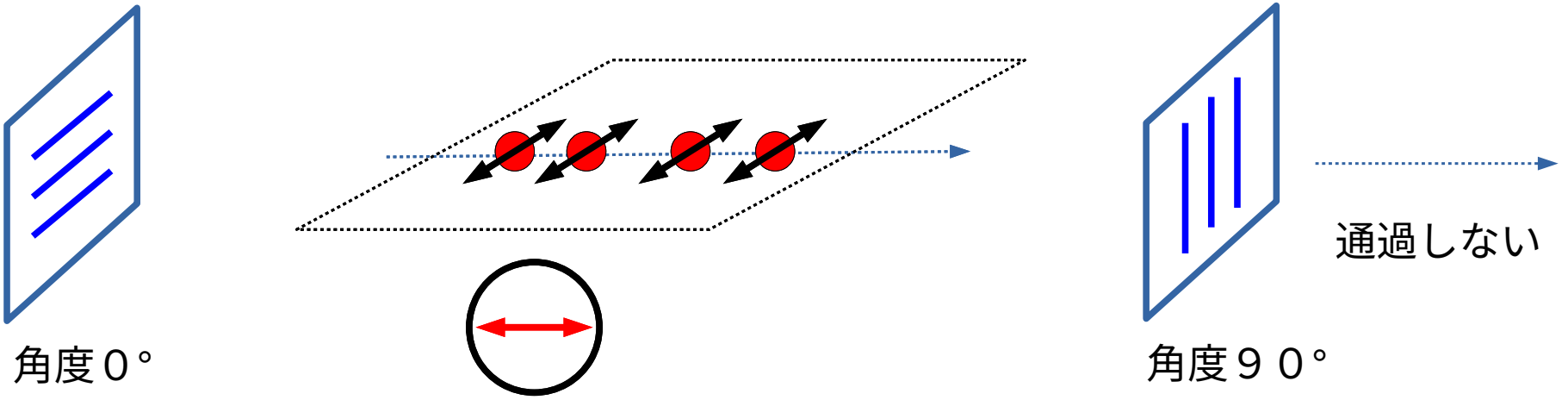


角度９０°（縦偏光）

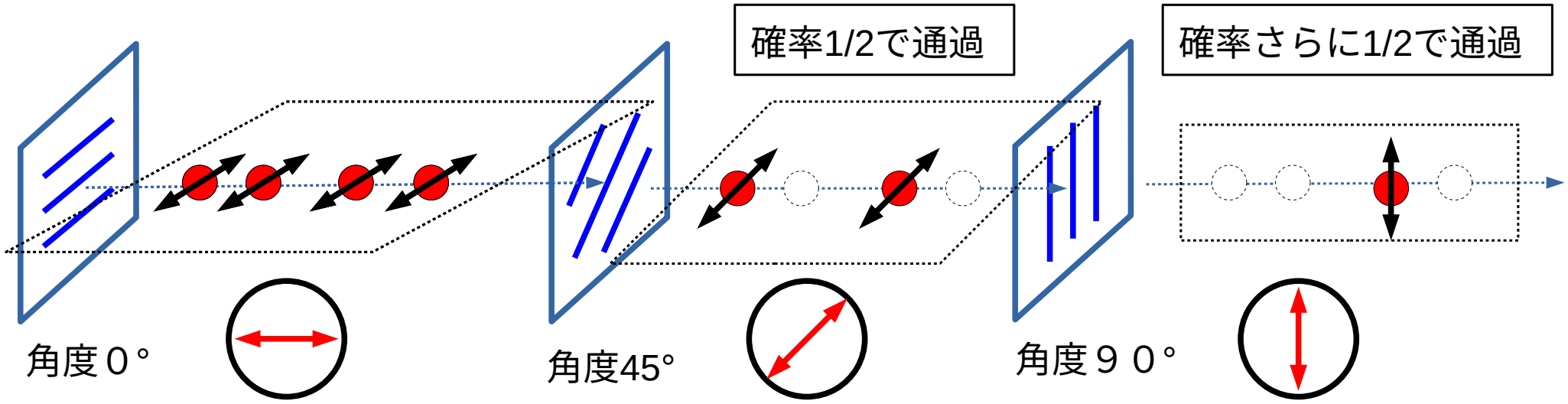


☆ １つのフォトンは分割できないので「波の射影成分」では説明できない！

微弱なレーザーの実験事実と量子状態



☆ 間に角度４５°の偏光フィルターを入れると？

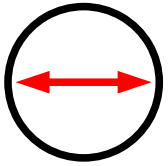


☆ 偏光フィルターと同じ向きに，通過したフォトンの偏光状態が変化する！

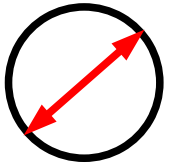
☆ 通過以前の情報は失われる！

量子力学の数学的記述方法

1）フォトンの偏光状態を，長さ1の2次元ベクトルで表す（状態ベクトル）



$$\psi(0) = \begin{pmatrix} \cos 0 \\ \sin 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$



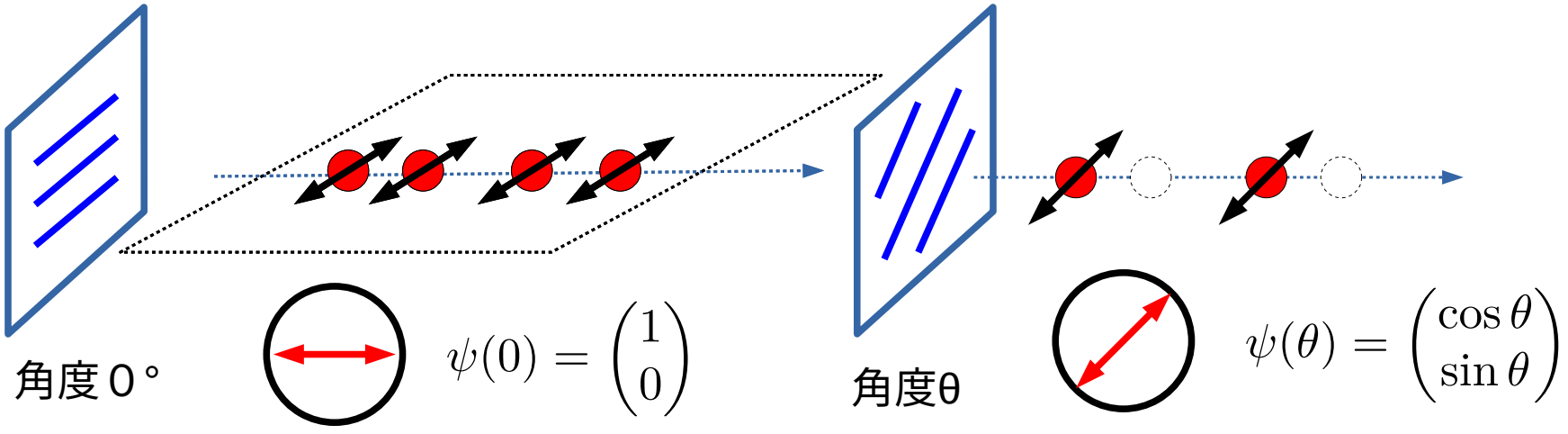
$$\psi(\theta) = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$

2）偏光フィルターの向きを，長さ1の 2次元ベクトルで表す ← 下の例では $\psi(\theta) = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$

3）通過する確率は，状態ベクトルと偏光フィルタの向きの内積の2乗

$$\left| \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \right|^2 = \cos^2\theta$$

4）フィルター通過直後，フィルターと同じ向きに偏光状態が変化する（射影公理）



ディラックのブラケット記法 (Dirac braket notation)

- 英語でカギカッコ $\langle \quad \rangle$ をブラケット (bracket) という
- 複素数成分をもつ縦ベクトルを $|\psi\rangle$, $|\varphi\rangle$ で表し，ケットベクトルと呼ぶ

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \quad |\varphi\rangle = \begin{pmatrix} c \\ d \end{pmatrix} \quad a, b, c, d \in \mathbb{C}$$

- $|\psi\rangle$, $|\varphi\rangle$ の複素共役転置（横ベクトル）を $\langle\psi|$, $\langle\varphi|$ で表し，ブラベクトルと呼ぶ
- ブラベクトル $\langle\varphi|$ とケットベクトル $|\psi\rangle$ の掛け算は内積になる

$$\langle\varphi\,|\,\psi\rangle = \begin{pmatrix} c^*, d^* \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = c^*a + d^*b$$

- 偏光状態 $|\psi\rangle$ のフォトンが，$|\varphi\rangle$ で表される偏光フィルターを通過する確率は，

$$|\,\langle\varphi\,|\,\psi\rangle\,|^2 = |c^*a + d^*b|^2$$

内積 $\langle\varphi\,|\,\psi\rangle$ は複素数であることに注意
複素数 $z = x + iy$ $(x, y \in \mathbb{R})$ について，$|z| = \sqrt{x^2 + y^2}$

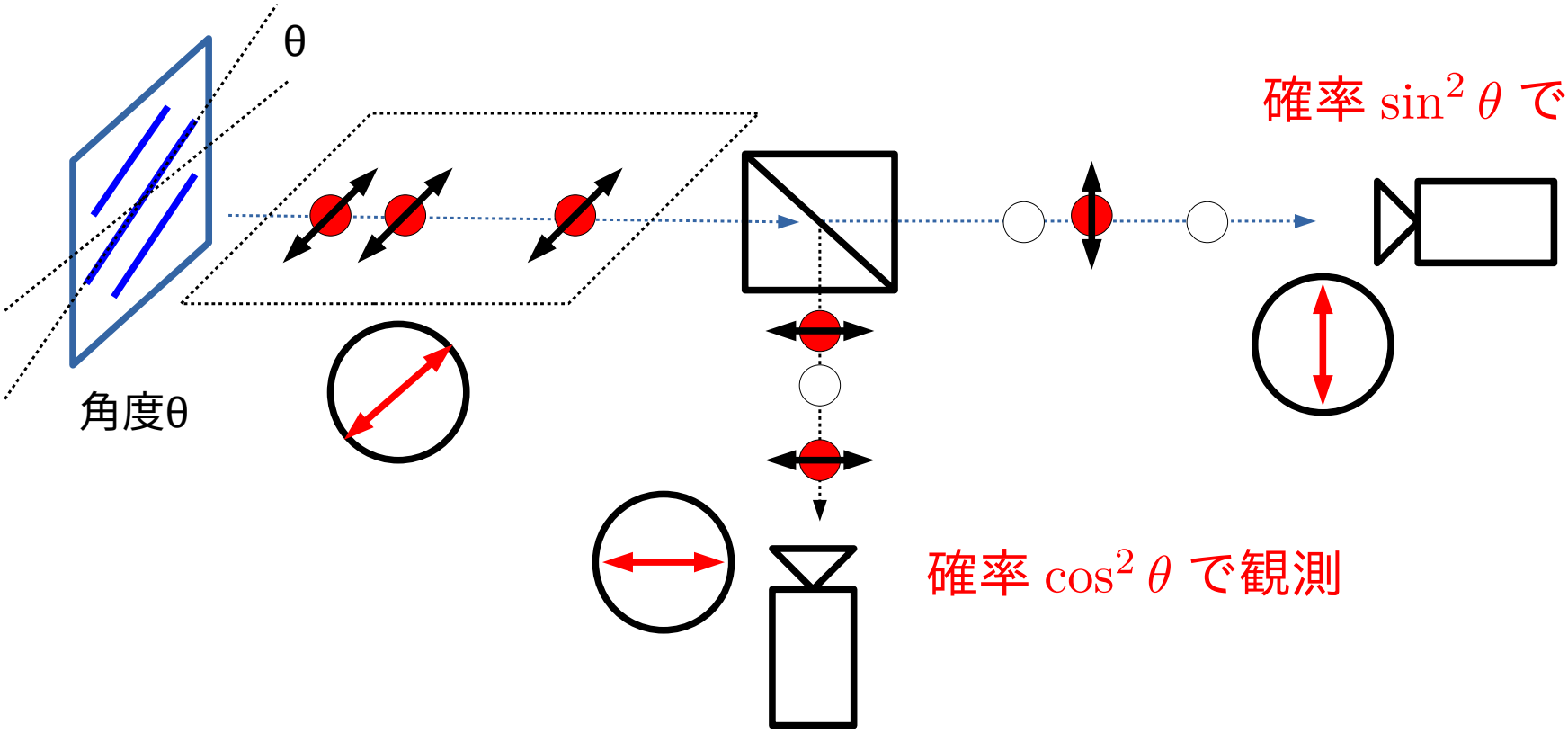
量子測定と偏光ビームスプリッター

☆ 量子測定：状態ベクトルを２つの直交する成分に分け，どちらかに射影する

$$|\psi(\theta)\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \cos\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \sin\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

☆ 測定後の状態が各成分に見出される確率＝係数（振幅）の２乗

☆ 偏光ビームスプリッターによる量子測定はそのような状況を実現している



量子暗号プロトコル BB84

（課題 3）量子暗号について以下の設問に答えよ（回答は本資料中の記号を使って良い）

(3-1) 量子暗号の目的を説明せよ

(3-2) プラス基底を用いるとき，$0, 1$ に割り当てる量子状態をそれぞれ答えよ

(3-3) クロス基底を用いるとき，$0, 1$ に割り当てる量子状態をそれぞれ答えよ

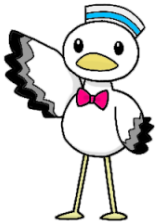
(3-4) $|e_0\rangle$ をクロス基底で測定する場合の測定結果とその確率を答えよ（簡潔に理由も述べよ）

ワンタイムパッドと無条件安全性

送信者アリス

送信メッセージ
“HELLO”
$a = 11010000\cdots$

受信者ボブ



受信メッセージ
“HELLO”
$a = 11010000\cdots$

共有鍵　　ランダムなビット列を事前に共有　　共有鍵
$b = 01101010\cdots$　　$b = 01101010\cdots$

⇓ ⊕ 暗号化

復号 ⊕ ⇑

暗号文
$c = 10111010\cdots$

公開通信路 ⟶

暗号文
$c = 10111010\cdots$

盗聴者イブ ↘
暗号文を盗聴　$c = 10111010\cdots$

メッセージをランダムに反転したものなので，元が分からない

→無条件安全性，情報理論的安全性

☆ ただし，遠隔で離れているため，鍵共有の問題が生じる

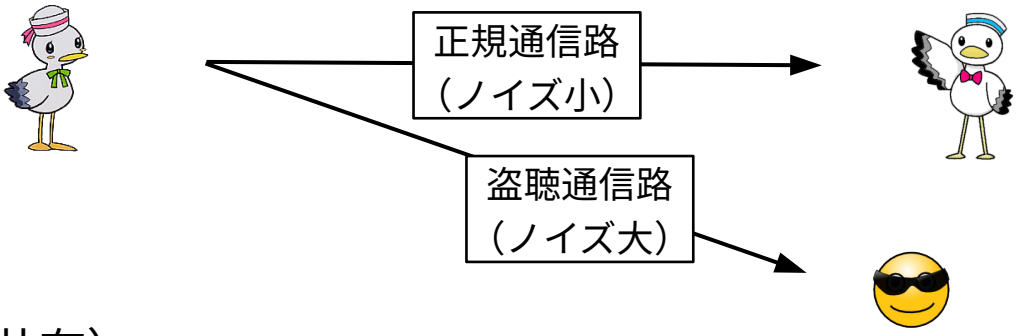
ワンタイムパッドの鍵共有はどうするの？

☆ 公開鍵暗号

- Diffie-Hellman-Merkle 鍵共有，RSA暗号, 楕円暗号など
- 現在主流の暗号方式，現行計算機の計算量理論が安全性の根拠
- 素因数分解の効率的な解法や，量子コンピュータの実現により安全性が崩れる

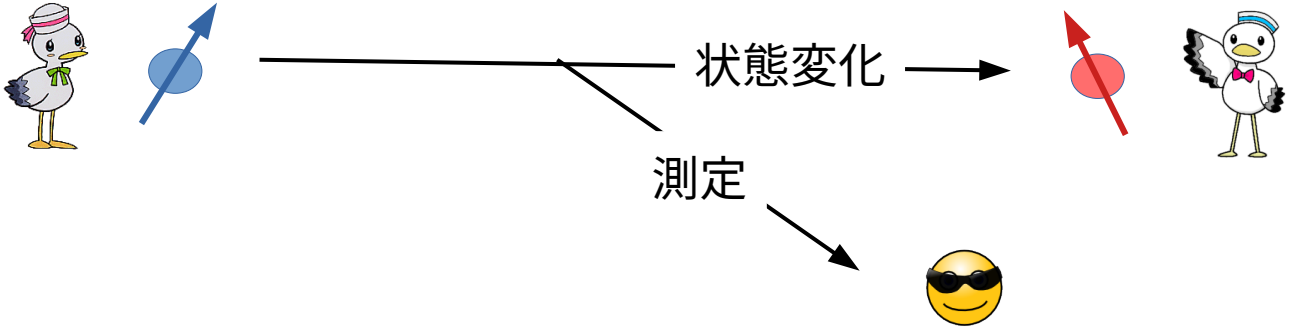
☆ 盗聴通信路符号化

- ”正規通信路のノイズ＜盗聴通信路のノイズ”であるとき，ノイズ差を利用して符号化
- 符号化を上手く行うことで，盗聴者に送信メッセージに関する情報を一切与えない



☆ 量子暗号（量子鍵共有）

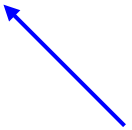
- 量子状態を送受信することで乱数（秘密鍵）を共有する方法
- 量子力学における測定による状態変化（射影公理）が安全性を保証する



量子状態の送受信に使う，プラス基底とクロス基底

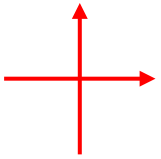
☆ 0, 1 のビット列を以下の2種類の方向（４種類の状態）により送信，受信を行う

☆ ４種類の送信状態

	プラス基底（”＋”で表す）	クロス基底（”×”で表す）
送信ビット０	$\|e_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$	 $\|f_0\rangle = \frac{\|e_0\rangle + \|e_1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
送信ビット１	 $\|e_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	 $\|f_1\rangle = \frac{\|e_0\rangle - \|e_1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

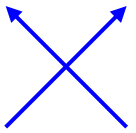
☆ ２種類の測定

$$|\psi\rangle = \alpha_0 |e_0\rangle + \alpha_1 |e_1\rangle$$



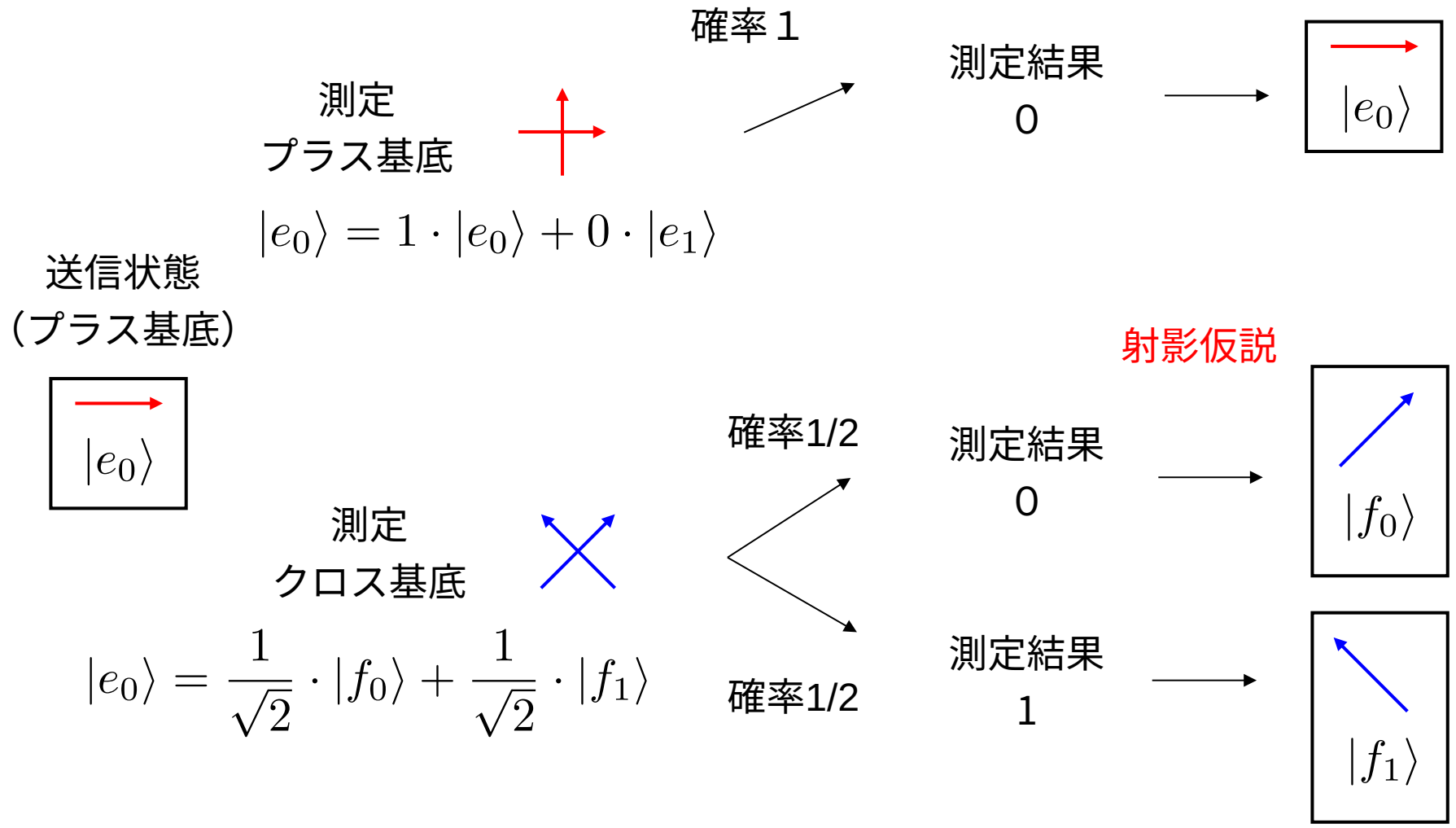
状態が $|\psi\rangle$ のとき，
確率 $|\alpha_0|^2$ で $|e_0\rangle$ に，
確率 $|\alpha_1|^2$ で $|e_1\rangle$ に変化

$$|\psi\rangle = \beta_0 |f_0\rangle + \beta_1 |f_1\rangle$$



状態が $|\psi\rangle$ のとき，
確率 $|\beta_0|^2$ で $|f_0\rangle$ に，
確率 $|\beta_1|^2$ で $|f_1\rangle$ に変化

受信方向と測定結果の例



Remember:

$$|e_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |f_0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |f_0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

量子鍵共有プロトコル（BB84プロトコル）

☆ 送信者：Alice

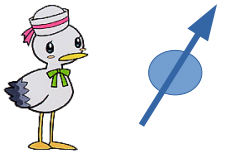
1）ランダムなビット列を用意する

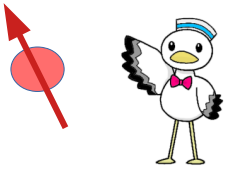
2）ランダムな送信方向を用意してビット列を送信

☆ 受信者：Bob

3）ランダムな受信方向を用いて受信量子状態を測定

1) ランダムビット列
10110011001110





2) ランダムな送信方向で送信

＋×＋＋××＋＋×＋××＋＋

3) ランダムな受信方向で受信

＋＋×＋×××＋×＋＋××＋

☆ 双方：公開通信路で事後にチェック

4）送信方向と受信方向を互いに伝え合い，両者が一致したビットを残す

5）残ったビット列からランダムにテストビットを伝え合い，一致を確認

量子鍵配送プロトコル (BB84) の例

送信者
Alice

送信 bit 列	1	0	1	1	0	0	1	1	0	0	1	1	1	0
送信方向	+	×	+	+	×	×	+	+	×	+	×	×	+	+
送信偏光	↑	↗	↑	↑	↗	↗	↑	↑	↗	→	↖	↖	↑	→

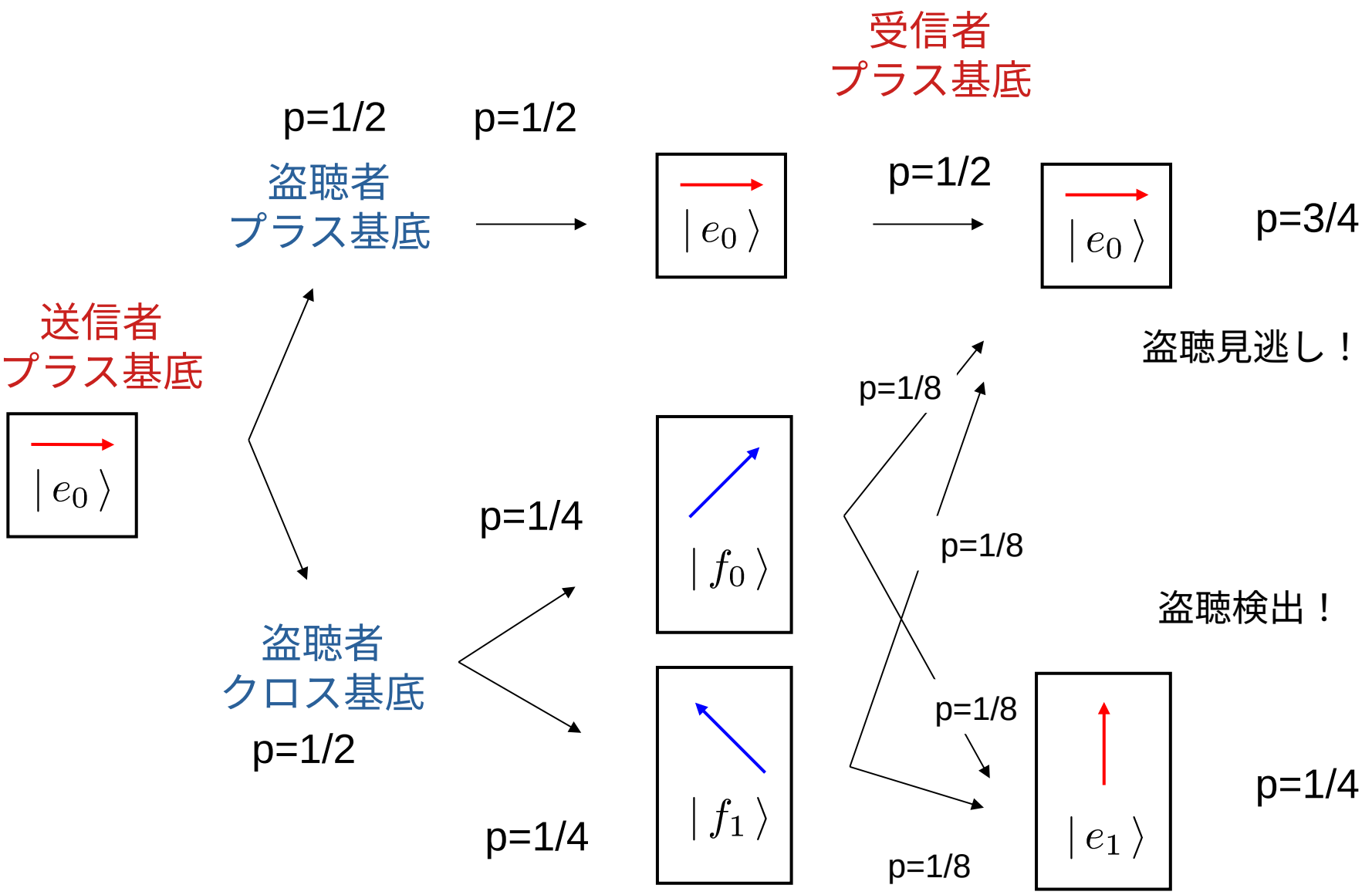
受信者
Bob

測定方向	+	+	×	+	×	×	×	+	×	+	+	×	×	+
受信偏光	↑	↑	↖	↑	↗	↗	↖	↑	↗	→	↓	↖	↗	→
受信 bit 列	1			1	0	0		1	0	0		1		0

盗聴
チェック

テスト bit	○				○					○				
完成 bit 列				1		0		1	0			1		0

盗聴者を検出する確率



盗聴を見逃す確率：$(3/4)^n \to 0$ （テストビット数 $\to \infty$）