作成者：吾妻広夫

練習問題 3

量子鍵配布プロトコル BB84 における、盗聴者 Eve の攻撃を考える。

図 1 は、Eve が $Z$ 基底 $\{|0\rangle, |1\rangle\}$ で光子を盗聴する様子を表している。Eve は Alice から送られてきた光子を、経路 P0 については検出器 ED0 で、経路 P1 については検出器 ED1 で検出する。そして、検出器 ED0 がヒットした場合は、光子源 S0 から経路 P0 に光子を放出し、検出器 ED1 がヒットした場合は、光子源 S1 から経路 P1 に光子を放出する。

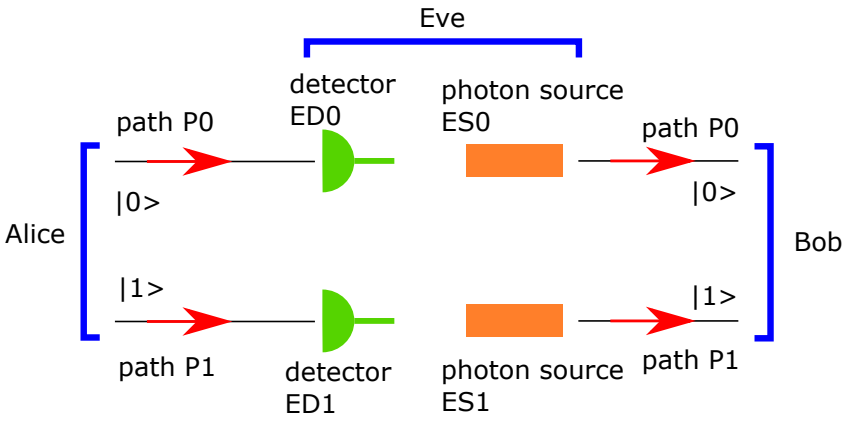


Figure 1: Eve が $Z$ 基底 $\{|0\rangle, |1\rangle\}$ で光子を盗聴する様子

図 2 は、Eve が $X$ 基底 $\{|+\rangle, |-\rangle\}$ で光子を盗聴する様子を表している。この攻撃で、Eve はビームスプリッタ EBSa、EBSb を使用する。ビームスプリッタ EBSa、EBSb が引き起こすユニタリ変換 $B$ は、次の行列で表されるとする。

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1}$$

ただし、この表示では、$\{|0\rangle, |1\rangle\}$ は次の 2 成分ベクトルで与えられるとする。

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2}$$

図 2 において、Eve は Alice から送られてきた光子に対してユニタリ変換 $B$ を作用させる。次に、Eve は検出器 ED0、ED1 で光子を検出する。そして、検出器 ED0 がヒットした場合は、光子源 S0 から経路 P0 に光子を放出し、検出器 ED1 がヒットした場合は、光子源 S1 から経路 P1 に光子を放出する。さらに、Eve は光子源から放出した光子に対してユニタリ変換 $B$ を作用させる。こうして処理された光子は Bob に送られる。

ここで、次の点に注意する。Alice が $Z$ 基底、$X$ 基底のどちらで光子を送信したか、Bob が $Z$ 基底、$X$ 基底のどちらで光子を受信したか、プロトコルの最後の段階で公表される。従って、Eve は盗聴する際、Alice と Bob がどの基底を使用したか分からない。そのため、Eve は図 1 と図 2 の攻撃を、状況に応じて使い分けることができない。基本的に、Eve は、図 1 または図 2 の攻撃を、プロトコル全体を通じて使い続けなくてはならない。

1. Eve が図 1 の攻撃方法を採用したとする。Alice が $|0\rangle$ を送信して、Bob が $Z$ 基底で受信する場合、Bob が正しく $|0\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。さらに、Alice が $|1\rangle$ を

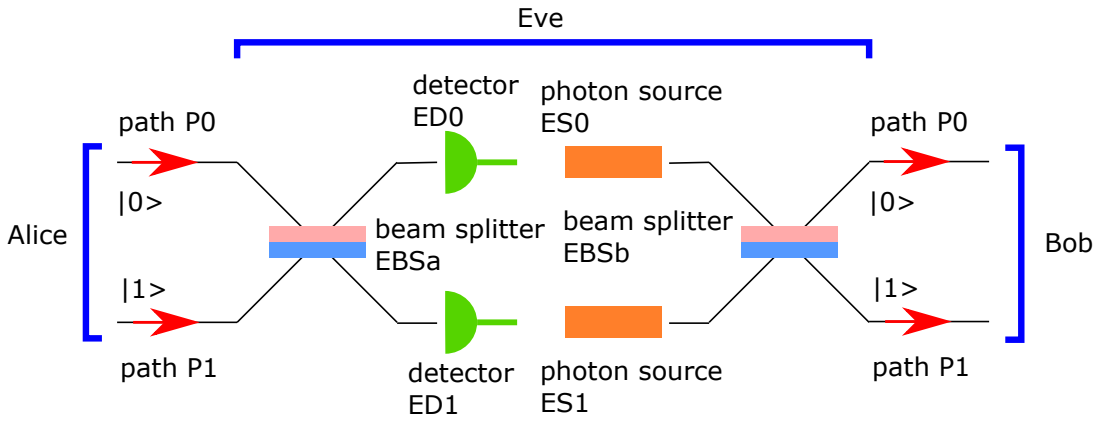


Figure 2: Eve が $X$ 基底 $\{|+\rangle, |-\rangle\}$ で光子を盗聴する様子

送信して、Bob が $Z$ 基底で受信する場合、Bob が正しく $|1\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。

2. Eve が図 1 の攻撃方法を採用したとする。Alice が $|+\rangle$ を送信して、Bob が $X$ 基底で受信する場合、Bob が正しく $|+\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。さらに、Alice が $|-\rangle$ を送信して、Bob が $X$ 基底で受信する場合、Bob が正しく $|-\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。

3. Alice と Bob は共通の基底をランダムに選択したとする。すなわち、Alice と Bob が $Z$ 基底で通信する確率は 1/2、Alice と Bob が $X$ 基底で通信する確率も 1/2 とする。このとき、Eve が図 1 の攻撃方法を採用したとすると、Alice と Bob が正しく送受信して共通のビット値を得る確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。ただし、この問題では、Alice と Bob が異なる基底で送受信した場合、そのデータは捨て去ることを前提にしていることに注意しなさい。

4. Eve が図 2 の攻撃方法を採用したとする。Alice が $|0\rangle$ を送信して、Bob が $Z$ 基底で受信する場合、Bob が正しく $|0\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。さらに、Alice が $|1\rangle$ を送信して、Bob が $Z$ 基底で受信する場合、Bob が正しく $|1\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。

5. Eve が図 2 の攻撃方法を採用したとする。Alice が $|+\rangle$ を送信して、Bob が $X$ 基底で受信する場合、Bob が正しく $|+\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。さらに、Alice が $|-\rangle$ を送信して、Bob が $X$ 基底で受信する場合、Bob が正しく $|-\rangle$ を検出する確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。

6. Alice と Bob は共通の基底をランダムに選択したとする。すなわち、Alice と Bob が $Z$ 基底で通信する確率は $1/2$、Alice と Bob が $X$ 基底で通信する確率も $1/2$ とする。このとき、Eve が図 2 の攻撃方法を採用したとすると、Alice と Bob が正しく送受信して共通のビット値を得る確率、および、Eve が Alice の送信しようとしたビット値情報を正しく推測する確率を求めなさい。ただし、この問題では、Alice と Bob が異なる基底で送受信した場合、そのデータは捨て去ることを前提にしていることに注意しなさい。