解答

作成者：吾妻広夫

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 $|0\rangle$ を検出する確率は次で与えられる。まず、途中の Eve が正しく $|0\rangle$ を検出する確率は 1 である。従って、Eve は正しく $|0\rangle$ を Bob に送る。結局、Bob が正しく $|0\rangle$ を検出する確率は 1 である。また、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も 1 である。

   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 $|1\rangle$ を検出する確率は次で与えられる。まず、途中の Eve が正しく $|1\rangle$ を検出する確率は 1 である。従って、Eve は正しく $|1\rangle$ を Bob に送る。結局、Bob が正しく $|1\rangle$ を検出する確率は 1 である。また、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も 1 である。

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 $|+\rangle$ を検出する確率は次で与えられる。まず、途中の Eve は、$|0\rangle$ または $|1\rangle$ をそれぞれ 1/2 の確率で検出する。Eve が Bob に $|0\rangle$ を送信した場合、Bob が正しく $|+\rangle$ を検出する確率は 1/2 である。また、Eve が Bob に $|1\rangle$ を送信した場合、Bob が正しく $|+\rangle$ を検出する確率は 1/2 である。結局、Bob が正しく $|+\rangle$ を検出する確率は 1/2 である。また、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も 1/2 である。

   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 $|-\rangle$ を検出する確率は次で与えられる。まず、途中の Eve は、$|0\rangle$ または $|1\rangle$ をそれぞれ 1/2 の確率で検出する。Eve が Bob に $|0\rangle$ を送信した場合、Bob が正しく $|-\rangle$ を検出する確率は 1/2 である。また、Eve が Bob に $|1\rangle$ を送信した場合、Bob が正しく $|-\rangle$ を検出する確率は 1/2 である。結局、Bob が正しく $|-\rangle$ を検出する確率は 1/2 である。また、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も 1/2 である。

3. 前の二つの問いの結果から、以下が得られる。

   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は以下で与えられる。

   $$\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4} \tag{1}$$

   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は以下で与えられる。

   $$\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4} \tag{2}$$

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 $|0\rangle$ を検出する確率は次で与えられる。まず、途中の Eve は、$|+\rangle$ または $|-\rangle$ をそれぞれ 1/2 の確率で検出する。Eve が Bob に $|+\rangle$ を送信した場合、Bob が正しく $|0\rangle$ を検出する確率は 1/2 である。また、Eve が Bob に $|-\rangle$

を送信した場合、Bob が正しく $|0\rangle$ を検出する確率は 1/2 である。結局、Bob が正しく $|0\rangle$ を検出する確率は 1/2 である。また、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も 1/2 である。

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 $|1\rangle$ を検出する確率を検出する確率はは次で与えられる。まず、途中の Eve は、$|+\rangle$ または $|-\rangle$ をそれぞれ 1/2 の確率で検出する。Eve が Bob に $|+\rangle$ を送信した場合、Bob が正しく $|1\rangle$ を検出する確率は 1/2 である。また、Eve が Bob に $|-\rangle$ を送信した場合、Bob が正しく $|1\rangle$ を検出する確率は 1/2 である。結局、Bob が正しく $|1\rangle$ を検出する確率は 1/2 である。また、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も 1/2 である。

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 $|+\rangle$ を検出する確率は次で与えられる。まず、途中の Eve が正しく $|+\rangle$ を検出する確率は 1 である。従って、Eve は正しく $|+\rangle$ を Bob に送る。結局、Bob が正しく $|+\rangle$ を検出する確率は 1 である。また、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も 1 である。

   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 $|-\rangle$ を検出する確率は次で与えられる。まず、途中の Eve が正しく $|-\rangle$ を検出する確率は 1 である。従って、Eve は正しく $|-\rangle$ を Bob に送る。結局、Bob が正しく $|-\rangle$ を検出する確率は 1 である。また、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も 1 である。

6. 前の二つの問いの結果から、以下が得られる。

   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は以下で与えられる。

$$\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4} \tag{3}$$

   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は以下で与えられる。

$$\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4} \tag{4}$$