量子鍵配送 - BB84 プロトコルについて

Hirotsugu Seike

2026 年 1 月 23 日

1　導入

量子状態はヒルベルト空間 $\mathcal{H} = \mathbb{C}^2$ のベクトルと考えられる. 標準基底 (Z 基底) を次式で定義する.

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

この時, 任意の 1 量子ビット状態 $|\psi\rangle$ は, 次式で書ける (ただし, 確率振幅 $\alpha, \beta \in \mathbb{C}$ かつ $|\alpha|^2 + |\beta|^2 = 1$ である.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{2}$$

Z 基底で測定した時, 量子ビットが $|0\rangle, |1\rangle$ (つまり 0, 1) と測定される確率はそれぞれ以下のようになる (内積は $\langle 0|0\rangle = \langle 1|1\rangle = 1$, $\langle 1|0\rangle = \langle 0|1\rangle = 0$ となるため).

$$\begin{cases} P(|0\rangle) & = |\langle 0|\psi\rangle|^2 = |\alpha|^2, \\ P(|1\rangle) & = |\langle 1|\psi\rangle|^2 = |\beta|^2. \end{cases} \tag{3}$$

この性質は, 量子力学における基本原理の一つであり, ボルン則 (Born rule) と呼ばれる. 特に $\alpha = 1$ または $\beta = 1$ の場合, Z 基底で測定すると決定論的に量子ビットの値が定まる. つまり, 測定時に選択した基底に応じて, 測定結果が確率 1 で定まる場合と確率的に分布する場合が生じる. 一定条件下で測定結果が決定論的に定まる特徴を利用することで, 盗聴を検知することが可能である.

2　BB84 プロトコル

BB84 プロトコルとは, 1984 年に C. H. Bennett, G. Brassard によって提案された量子鍵配送 (QKD: Quantum Key Distribution) 方式である [1]. Alice を送信者, Bob を受信者, Carol を盗聴者とする. Alice は, ヒルベルト空間 $\mathcal{H}$ 上に, 次の 2 つの正規直交基底を定義する.

$$Z = \{\, |0\rangle, |1\rangle \,\}, \quad X = \{\, |+\rangle, |-\rangle \,\}, \tag{4}$$

ここで,

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{5}$$

である. Alice は, ランダムなビット $a \in \{0, 1\}$ とランダムな正規直交基底 $B_a \in \{Z, X\}$ を選択し, 次式のような量子ビット $|\psi_a\rangle$ を Bob に送信する.

$$|\psi_a\rangle = \begin{cases} |a\rangle, & (B_a = Z), \\ \dfrac{|0\rangle + (-1)^a|1\rangle}{\sqrt{2}}, & (B_a = X). \end{cases} \tag{6}$$

Bob は正規直交基底 $B_b \in \{Z, X\}$ をランダムに選択して, $|\psi_a\rangle$ を測定する. つまり, 運よく $B_a = B_b$ となった場合, 以下のようになる.

$$\begin{cases} P(|0\rangle) & = |\langle 0|\psi_a\rangle|^2 = 1, (a = 0, B_a = Z, B_b = Z) \\ P(|1\rangle) & = |\langle 1|\psi_a\rangle|^2 = 1, (a = 1, B_a = Z, B_b = Z) \end{cases} \tag{7}$$

$$\begin{cases} P(|+\rangle) & = |\langle +|\psi_a\rangle|^2 = 1, (a = 0, B_a = X, B_b = X) \\ P(|-\rangle) & = |\langle -|\psi_a\rangle|^2 = 1, (a = 1, B_a = X, B_b = X) \end{cases} \tag{8}$$

一方で, $B_a \neq B_b$ の場合, 以下のように量子ビットは 0, 1 として, ランダムに観測されることになる.

$$\begin{cases} P(|+\rangle) & = |\langle +|\psi_a\rangle|^2 = 1/2, (a = 0, B_a = Z, B_b = X) \\ P(|-\rangle) & = |\langle -|\psi_a\rangle|^2 = 1/2, (a = 1, B_a = Z, B_b = X) \end{cases} \tag{9}$$

$$\begin{cases} P(|0\rangle) & = |\langle 0|\psi_a\rangle|^2 = 1/2, (a = 0, B_a = X, B_b = Z) \\ P(|1\rangle) & = |\langle 1|\psi_a\rangle|^2 = 1/2, (a = 1, B_a = X, B_b = Z) \end{cases} \tag{10}$$

BB84 では, 上記のように Alice がランダムに送信した量子ビットを Bob が観測する. その後, 古典的な通信路で, 各量子ビットを生成する際に Alice が用いた正規直交基底 B_a の情報を Bob に送る. そして, $B_a \neq B_b$ となる量子ビットは全て捨てる. 残った量子ビット m 個の情報 $\{0, 1\}^m$ を用いて, 共有鍵を作成することができる.

仮に, Carol が Man in the middle attack を仕掛けて, 量子通信を傍受したとする. その場合, 古典的通信と異なり, 観測する前の量子ビットを再現して Bob に送信することはできない. Carol が選択した基底 $B_c \in \{Z, X\}$ が Alice の基底と一致しているかどうかは不明であり, Alice が量子ビットを作成するために必要だった $a \in \{0, 1\}, B_a \in \{Z, X\}$ に関する情報を一切保持していないためである.

従って, Carol が Alice と同じ基底を用いて測定できていない $B_c \neq B_a$ 上で, Bob が Alice と同じ基底を用いたにも関わらずビットを測定できていないパターンで盗聴を検知できる. その確率は 1 量子ビットにつき, 次式で与えられる.

$$\mathrm{QBER} = \Pr(b_E \neq b_A) \Pr(\mathrm{error} \mid b_E \neq b_A) \tag{11}$$

$$= \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}. \tag{12}$$

従って, 測定用の基底が等しい $(B_a = B_b)$, 十分に大きな m が与えられれば, 次式より盗聴を検知できない確率は指数関数的に下がる.

$$P_{\mathrm{undetected}} = (1 - \mathrm{QBER})^m = \left(\frac{3}{4}\right)^m. \tag{13}$$

参考文献

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179, 1984.

付録 A　特になし