量子暗号の盗聴はバレる！ ── 波動関数の収縮が起きてしまうのだ

ここではパウリ行列 σ_z，σ_x を，簡単のため Z，X で表すことにしよう。すなわち

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1}$$

である。Z の固有状態 $|\pm\rangle$ と X の固有状態 $|\pm'\rangle$ の間には，以下の関係がある：

$$|+'\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \quad |-'\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \tag{2}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|+'\rangle + |-'\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|+'\rangle - |-'\rangle) \tag{3}$$

以下では，量子ビット $|+\rangle$，$|+'\rangle$ は「ビット 0」，$|-\rangle$，$|-'\rangle$ は「ビット 1」に対応させる。

暗号キー　A が演算子 $\{Z, X\}$，およびビット値 $\{0, 1\}$ を無作為に選び，対応する量子ビット[1]，$\{Z0 \to |+\rangle,\ Z1 \to |-\rangle,\ X0 \to |+'\rangle,\ X1 \to |-'\rangle\}$ の列を B に送る。B は受取った量子ビット列を，こちらも無作為に選んだ $\{Z, X\}$ で観測し，測定値のビット列 $0, 0, 1, 0, 1, \ldots$ を得る。A と B の選んだ演算子 $\{Z, X\}$ が一致する場合は，B の観測で状態は変化せず，B の測定値は A の選んだビット値と同じである。一致しない場合は，(2)，(3) の右辺の，A とは異なる方の演算子の固有状態の いずれか がランダムに観測されるから，A と B でビット値が同じになるとは限らない。

一連の量子ビット列を送った後で，A と B それぞれで選んだ「Z か X か」の古典情報列を交信して照合すれば，半分くらいは一致しているはずである。そこで，一致した位置のビット情報だけを各自で拾えば，これは交信して一致を確かめる必要はない。したがって，部外者に漏れる機会はなく当事者だけで秘かに共有されるので，安全な暗号キー（BB84）として利用できる。

盗聴者　第三者 E がいて A が送る量子ビットを盗聴しているとする。E は「量子ビット信号が送られている」こと以上に詳しい仕掛けは知らず，ひたすら Z を観測[2]する。E は盗聴できた $\{|+\rangle, |-\rangle\}$ と同じ量子ビットを，内心「得たり！」と B へ送る。A が Z を選んでいた場合は，A が送り出したのと同じものを B に転送することになる。一方，【半々の確率で】X であった場合にも，それが $|+'\rangle$ であれ，$|-'\rangle$ であれ，ちゃんと (2) の右辺の $|+\rangle$ か $|-\rangle$ が観測されるから，E は仕掛けに気づかず，それを B に送る。この場合，B が A と同じ X を観測しても，再び $|+\rangle$ であれ，$|-\rangle$ であれ，(3) により【さらに半々の確率で】ランダムに $|+'\rangle$ か $|-'\rangle$ になるから，半分くらいは A が送った X のビットとは一致しない。A と B で $\{Z, X\}$ を照合して一致した位置だけ，双方で拾い集めたビット列も，その半分の半分，つまり **1/4** くらいは食い違う可能性がある。

安全確認　まず，必要とする暗号キーの長さの 2 倍よりは十分に長い量子ビット列を A から送った後，A，B で選んだ $\{Z, X\}$ 情報を交信して一致した位置のビット値だけ，各自で拾っておく。この中からキーとして必要な長さのビット列は各自でキープした上で，残りのビット列を開けて**試し**に両者で照合する。1ヶ所でも合わないなら，盗聴されていることになる。合わない確率が 1/4 もあるなら，ある程度長いテストビット列を照合すれば，ほぼ確実に盗聴を検出できる。[3]

要するに，E が盗聴（＝観測）を行うことで**波動関数の収縮**が起きるのである。例えば A で $X0$ を選んで $|+'\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ を送り出し，E が A の選択を知らずに Z を観測すると，状態は半々の確率で $|+\rangle$ か $|-\rangle$ に**非可逆的に変質**してしまう。A の送り出した任意の状態を観測した上で，それと同じ状態を再生し B に送ることは不可能なのだ（**No cloning theorem**→[**226**]）。

---

[1] 例えば，{$Z0$：x-偏光，$Z1$：y-偏光，$X0$：+45 度偏光，$X1$：−45 度偏光 } の光子。→ [**228**]

[2] そもそも知っておれば盗聴を試みない。仕掛けを知っていても $\{Z, X\}$ を当てずっぽうに選ぶしかなく，結論は同じである。A と B が**事後に**交信する $\{Z, X\}$ 列の情報を知っても，観測を終えてしまった E には何の役にも立たない。

[3] E が盗聴をあきらめて意図的な攪乱（例えば数ヶ所だけを改ざん）を企てたような場合は，この限りではない。**量子コンピュータ**は，厳密に解を得るのではなく，この例のように重ね合わせの状態を利用して，**確率的にほぼ確実**という判定により，実用目的に応えられる解を求めることが多い。