8.91: A Shorter Version of the Quantum Math Behind Ekert's Key Distribution Scheme

Alice and Bob share an entangled photon (EPR) pair in the following state.

$$|\Psi = \frac{1}{\sqrt{2}}[|R\rangle_A|R\rangle_B + |L\rangle_A|L\rangle_B] = \frac{1}{2\sqrt{2}}\left[\begin{pmatrix}1\\ i\end{pmatrix}_A \otimes \begin{pmatrix}1\\ i\end{pmatrix}_B + \begin{pmatrix}1\\ -i\end{pmatrix}_A \otimes \begin{pmatrix}1\\ -i\end{pmatrix}_B\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\\ 0\\ -1\end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}[|V\rangle_A|V\rangle_B - |H\rangle_A|H\rangle_B]$$

They agree to make random polarization measurements in the rectilinear and circular polarization bases. When a measurement is made on a quantum system the result is always an eigenstate of the measurement operator. The eigenstates in the circular and rectilinear bases are:

$$R = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix} \quad L = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix} \quad V = \begin{pmatrix}1\\ 0\end{pmatrix} \quad H = \begin{pmatrix}0\\ 1\end{pmatrix}$$

Pertinent superpositions:

$$V = \tfrac{1}{\sqrt{2}}(R+L) \quad H = \tfrac{i}{\sqrt{2}}(L-R) \quad R = \tfrac{1}{\sqrt{2}}(V+iH) \quad L = \tfrac{1}{\sqrt{2}}(V-iH)$$

Alice's random measurement effectively sends a random photon to Bob due to the correlations built into the entangled state of their shared photon pair. Alice's four measurement possibilities and their consequences for Bob are now examined.

Alice's photon is found to be right circularly polarized, |R>. If Bob measures circular polarization he is certain to find his photon to be |R>. But if he chooses to measure in the rectilinear basis the probability he will observe |V> is 0.5 and the probability he will observe |H> is 0.5.

$$\frac{1}{\sqrt{2}}RR = \frac{1}{\sqrt{2}}R\left[\frac{1}{\sqrt{2}}(V+iH)\right]$$

If Alice observes |L>, Bob will also if he measures circular polarization. But if he measures in the rectilinear basis the probability he will observe |V> is 0.5 and the probability he will observe |H> is 0.5.

$$\frac{1}{\sqrt{2}}LL = \frac{1}{\sqrt{2}}L\left[\frac{1}{\sqrt{2}}(V-iH)\right]$$

The same kind of reasoning applies to measurements Alice makes in the rectilinear basis.

$$\tfrac{1}{\sqrt{2}}VV = \tfrac{1}{\sqrt{2}}V\left[\tfrac{1}{\sqrt{2}}(R+L)\right] \quad \tfrac{1}{\sqrt{2}}HH = \tfrac{1}{\sqrt{2}}H\left[\tfrac{1}{\sqrt{2}}(L-R)\right]$$

Alice and Bob keep the results for the experiments for which they measured in the same basis (blue in the table below), and make the following bit value assignments: |V> = |R> = 0 and |H> = |L> = 1. This leads to the secret key on the bottom line.

Alice	*R*	V	*V*	*L*	H	L	*H*	*R*	*V*	L	*H*
Bob	*R*	L	*V*	*L*	R	H	*H*	*R*	*V*	V	*H*
Key	0		0	1		1	0	0		1	

The following demonstrates how a binary message is coded and subsequently decoded using a shared binary secret key and modulo 2 arithmetic.

$$\underset{\text{Message}}{\text{Mes}} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \quad \underset{\text{Key}}{\text{Key}} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad \underset{\text{Coded Message}}{\text{CMes} = \text{mod}(\text{Mes} + \text{Key}, 2) =} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \underset{\text{Decoded Message}}{\text{DMes} = \text{mod}(\text{CMes} + \text{Key}, 2) =} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

It is clear by inspection that the message has been accurately decoded. This is confirmed by calculating the difference between the message and the decoded message.

$$(\text{Mes} - \text{DMes})^T = (0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0)$$
