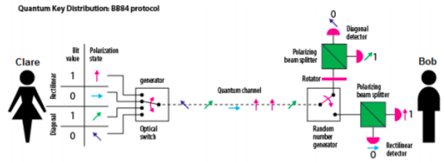
8.89: Matrix Mechanics Analysis of the BB84 Key Distribution

The figure below (www.nsa.gov/research/tnw/tnw201/article6.shtml) illustrates an implementation of the BB84 public key distribution protocol. Clare randomly sends Bob single photons in either the rectilinear or diagonal basis. Bob randomly chooses to measure the photons he receives in either the rectilinear or diagonal basis. The table below the figure displays typical results and how Clare and Bob use them to create a secret key.

While the key distribution protocol is clear enough from the graphic alone, the purpose of this tutorial is to show the details of its operation using the methods of matrix mechanics.



Quantum transmission & detection	Clare's photons	↖	↗	→	↑	↑	↗	↖	↑
	Clare's random bits	0	1	0	1	1	1	0	1
	Bob's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	Bob's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	Bob's measurement basis	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	Clare tells Bob which bits to keep		✔		✔		✔	✔	
	Shared secret key	–	1	–	1	–	1	0	–

Direction of motion and polarization states are represented by the following vectors. The x-direction is horizontal in the figure above.

$$\text{Direction of propagation states:} x = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad y = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\text{Photon polarization states:} \qquad v = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad h = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad d = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad s = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

There are eight propagation-polarization states which are created by tensor multiplication of the appropriate vectors.

$$xv = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad xv = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad xh = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad xh = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad yv = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad yv = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad yh = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad yh = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$xd = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad xd = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad xs = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad xs = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

$$yd = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad yd = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \quad ys = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad ys = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$$

The operators required for the BB84 implementation shown above are matrices representing the identity, mirror, rotator and polarization beam splitter, PBS.

$$\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \mathrm{M} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{Rotator} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{PBS} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

The rotator, which prepares photons for measurement in the diagonal basis, rotates the photon polarization state clockwise by 45 degrees.

$$\text{Rotator v} = \begin{pmatrix} 0.707 \\ 0.707 \end{pmatrix} = |d\rangle \quad \text{Rotator h} = \begin{pmatrix} -0.707 \\ 0.707 \end{pmatrix} = -|s\rangle \quad \text{Rotator d} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |h\rangle \quad \text{Rotator s} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |v\rangle$$

The PBS transmits vertical and reflects horizontal photons. For example,

$$\text{PBS xv} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |xv\rangle \quad \text{PBS xh} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = yh\rangle \quad \text{PBS yv} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |yv\rangle \quad \text{PBS yh} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |xh\rangle$$

Interpreting Measurement Results

Suppose Bob measures Clare's photons (|v>, |h>, |d> and |s>) in the rectilinear basis. Note that the rectilinear detector is in the same direction as the photons are propagating. For |v> and |h> he correctly measures the polarization of Clare's photons. However, |d> and |s> are not eigenstates of the PBS, but superpositions of |v> and |h>, so for these photons half the time Bob will observe |v> and half the time |h>. According to quantum principles he always observes one of the eigenstates of the measurement operator. When Clare and Bob publicly discuss the result she will tell him for which events he chose the correct measurement basis.

$$\text{PBS xv} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = xv \quad \text{PBS xh} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = yh \quad \text{PBS xd} = \begin{pmatrix} 0.707 \\ 0 \\ 0 \\ 0.707 \end{pmatrix} \quad \frac{1}{\sqrt{2}}(\text{xv} + \text{yh}) = \begin{pmatrix} 0.707 \\ 0 \\ 0 \\ 0.707 \end{pmatrix}$$

$$\text{PBS xs} = \begin{pmatrix} 0.707 \\ 0 \\ 0 \\ -0.707 \end{pmatrix} \quad \frac{1}{\sqrt{2}}(\text{xv - yh}) = \begin{pmatrix} 0.707 \\ 0 \\ 0 \\ -0.707 \end{pmatrix}$$

Suppose Bob measures Clare's photons in the diagonal basis. The diagonal detector is reached in the vertical direction via a mirror. The rotator causes a basis change so that the |d> and |s> photons become eigenvectors of the PBS. Thus for |d> or |s> Bob always gets the correct result because they have been transformed to |h> or |v>. The states |v> and |h> are transformed by the rotator into superpositions of |v> and |h>, indicating that half the time he will observe |d> and half the time |s>. When Clare and Bob publicly discuss the result she will tell him which events he chose the correct measurement basis.

$$\text{PBS kronecker(M, Rotator) xd} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = xh \qquad \text{PBS kronecker(M, Rotator) xs} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = yv$$

$$\text{PBS kronecker(M, Rotator) xv} = \begin{pmatrix} 0 \\ 0.707 \\ 0.707 \\ 0 \end{pmatrix} \qquad \frac{1}{\sqrt{2}}(\text{xh} + \text{yv}) = \begin{pmatrix} 0 \\ 0.707 \\ 0.707 \\ 0 \end{pmatrix} \qquad \text{PBS kronecker(M, Rotator) xh} = \begin{pmatrix} 0 \\ 0.707 \\ -0.707 \\ 0 \end{pmatrix} \qquad \frac{1}{\sqrt{2}}(\text{xh - yv}) = \begin{pmatrix} 0 \\ 0.707 \\ -0.707 \\ 0 \end{pmatrix}$$

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

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

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.

$$(\text{Mes} - \text{DMes})^T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Here's a graphical representation of the coding and decoding mechanism.