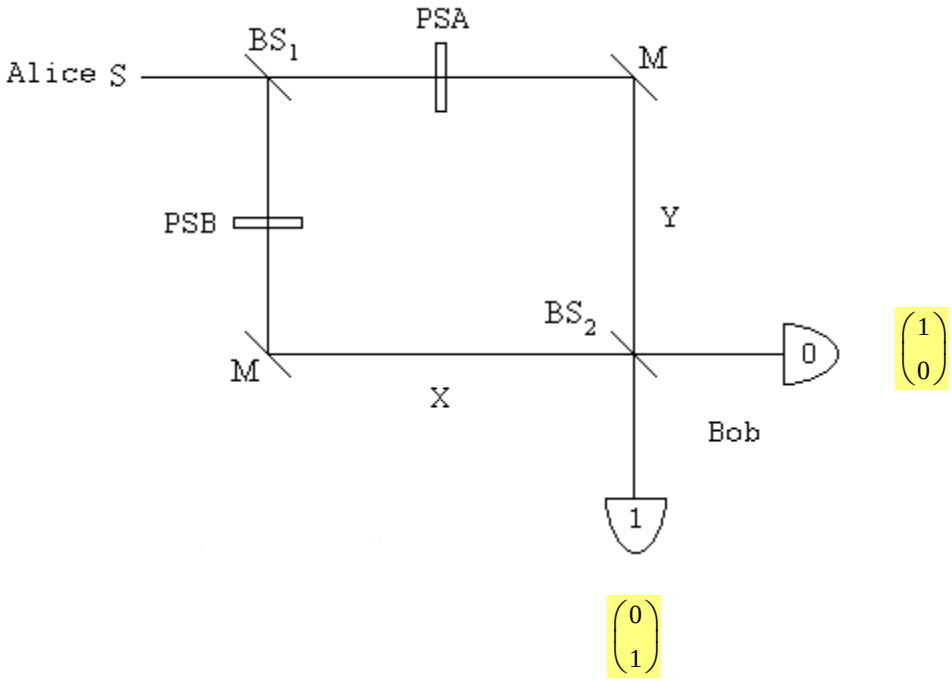
Quantum Key Distribution Using a Mach-Zehnder Interferometer

Frank Rioux

Charles H. Bennett proposed the following Mach-Zehnder interferometer for quantum key distribution (*Physical Review Letters* **68**, 3121 (1992)).



$\begin{pmatrix}1\\0\end{pmatrix}$

$\begin{pmatrix}0\\1\end{pmatrix}$

Alice's source at the left supplies single-photon states, which are split by a symmetric beam splitter BS_1 into a superposition being present in both arms of a Mach-Zehnder interferometer (MZI). Alice (PSA) applies a random 0-, 90-, 180-, or 270-degree phase shift in one arm and Bob (PSB) applies a random 0- or 90-degree phase shift in the other arm. Mirrors direct the photon to a second beam splitter creating two photon paths to each detector and thereby allowing for interference between the paths. After photon detection by Bob, Alice and Bob agree publicly to keep only those results for which their phase shifts differ by 0 or 180 degrees, settings for which the photons behave deterministically at the second beam splitter.

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

Matrix operators for the interferometer components:

Beam splitter: $BS := \frac{1}{\sqrt{2}} \cdot \begin{pmatrix}1 & i\\ i & 1\end{pmatrix}$ Mirror: $M := \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ Phase shift: $\begin{pmatrix}e^{i\cdot PSA} & 0\\ 0 & e^{i\cdot PSB}\end{pmatrix}$

Construct a Mach-Zehnder interferometer using these components.

$$MZI(PSA, PSB) := BS \cdot M \cdot \begin{pmatrix}e^{i\cdot PSA} & 0\\ 0 & e^{i\cdot PSB}\end{pmatrix} \cdot BS$$

Probability Detector 0 will fire:

$$Detector\_0(PSA, PSB) := \left(\left|x^T \cdot MZI(PSA, PSB) \cdot x\right|\right)^2$$

Probability Detector 1 will fire:

$$Detector\_1(PSA, PSB) := \left(\left|y^T \cdot MZI(PSA, PSB) \cdot x\right|\right)^2$$

For each of eight possible phase shift settings calculate the probability that detectors |0> and |1> will register the arrival of a photon.

The PSA/PSB settings for which a photon behaves deterministically are highlighted.

		Detector = $\begin{pmatrix}1\\0\end{pmatrix}$ = 0	Detector = $\begin{pmatrix}0\\1\end{pmatrix}$ = 1
PSA := 0·deg	PSB := 0·deg	Detector_0(PSA, PSB) = 1	Detector_1(PSA, PSB) = 0
PSA := 0·deg	PSB := 90·deg	Detector_0(PSA, PSB) = 0.5	Detector_1(PSA, PSB) = 0.5
PSA := 90·deg	PSB := 0·deg	Detector_0(PSA, PSB) = 0.5	Detector_1(PSA, PSB) = 0.5
PSA := 90·deg	PSB := 90·deg	Detector_0(PSA, PSB) = 1	Detector_1(PSA, PSB) = 0
PSA := 180·deg	PSB := 0·deg	Detector_0(PSA, PSB) = 0	Detector_1(PSA, PSB) = 1
PSA := 180·deg	PSB := 90·deg	Detector_0(PSA, PSB) = 0.5	Detector_1(PSA, PSB) = 0.5
PSA := 270·deg	PSB := 0·deg	Detector_0(PSA, PSB) = 0.5	Detector_1(PSA, PSB) = 0.5
PSA := 270·deg	PSB := 90·deg	Detector_0(PSA, PSB) = 0	Detector_1(PSA, PSB) = 1

Demonstrate that the detection results at each detector are completely random. In other words, that if someone was monitoring Bob's detectors he or she would see no pattern in the results.

The settings of phase shifters PSA and PSB are changed randomly by Alice and Bob. So given a large number of runs, each pair of settings shown above will occur with probability 1/8 or 12.5%. Overall each detector will register a photon in half the runs.

Detector = $\begin{pmatrix}1\\0\end{pmatrix}$ $\dfrac{1+\frac{1}{2}+\frac{1}{2}+1+0+\frac{1}{2}+\frac{1}{2}+0}{8} \to \frac{1}{2}$ Detector = $\begin{pmatrix}0\\1\end{pmatrix}$ $\dfrac{0+\frac{1}{2}+\frac{1}{2}+0+1+\frac{1}{2}+\frac{1}{2}+1}{8} \to \frac{1}{2}$

Demonstrate the use of a secret key to exchange a secure message between a sender and a receiver.

Coding and Decoding a Message

As an example, a binary key and message are generated using a truncated random number generator. A coded message is created by adding the key to the message modulo 2. The coded message is sent to the receiver who decodes it by adding the key to it modulo 2.

$j := 1 .. 25$ $Key_j := trunc(rnd(2))$ $Key^T = (0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1)$

$Mes_j := trunc(rnd(2))$ $Mes^T = (1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1)$

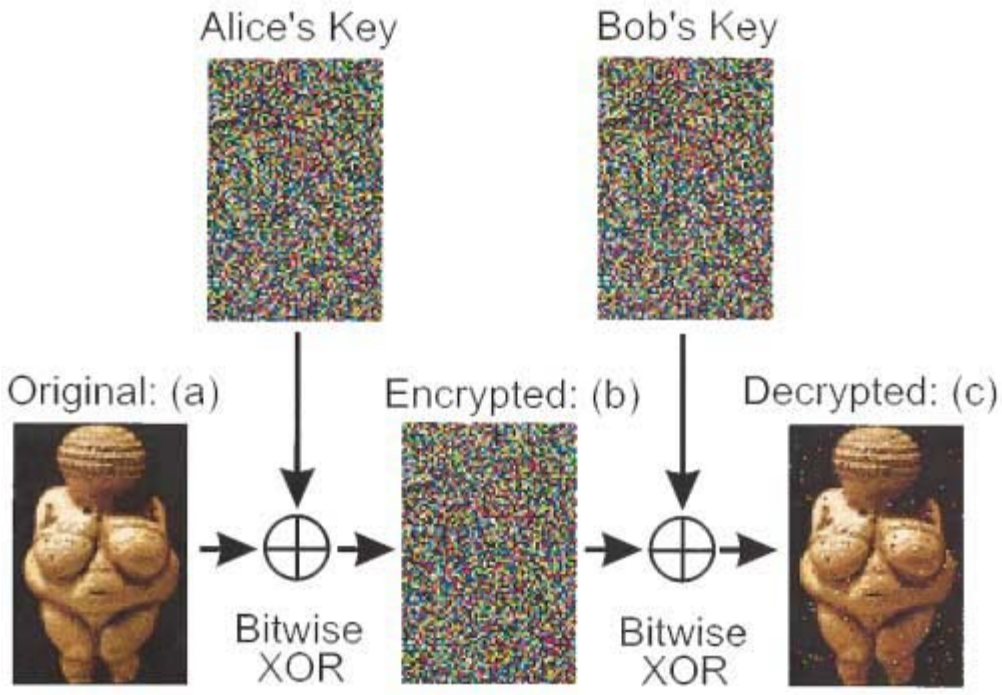
$CMes_j := Mes_j \oplus Key_j$ $CMes^T = (1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0)$

$DMes_j := CMes_j \oplus Key_j$ $DMes^T = (1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1)$

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.

$(DMes - Mes)^T = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$

In 2000 Anton Zeilinger and his research team sent an encrypted photo of the fertility goddess Venus of Willendorf from Alice to Bob, two computers in two buildings about 400 meters apart. The figure summarizing this achievement first appeared in *Physical Review Letters* and later in a review article in *Nature*.



By extending the previous example to two dimensions, it easy to produce a rudimentary simulation of the experiment. Bitwise XOR is nothing more than addition modulo 2. (XOR = CNOT)

The original Venus and the shared key are represented by the following matrices, where the matrix elements are pixels that are either off (0) or on (1).

$$\text{Venus} := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad \text{Key} := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

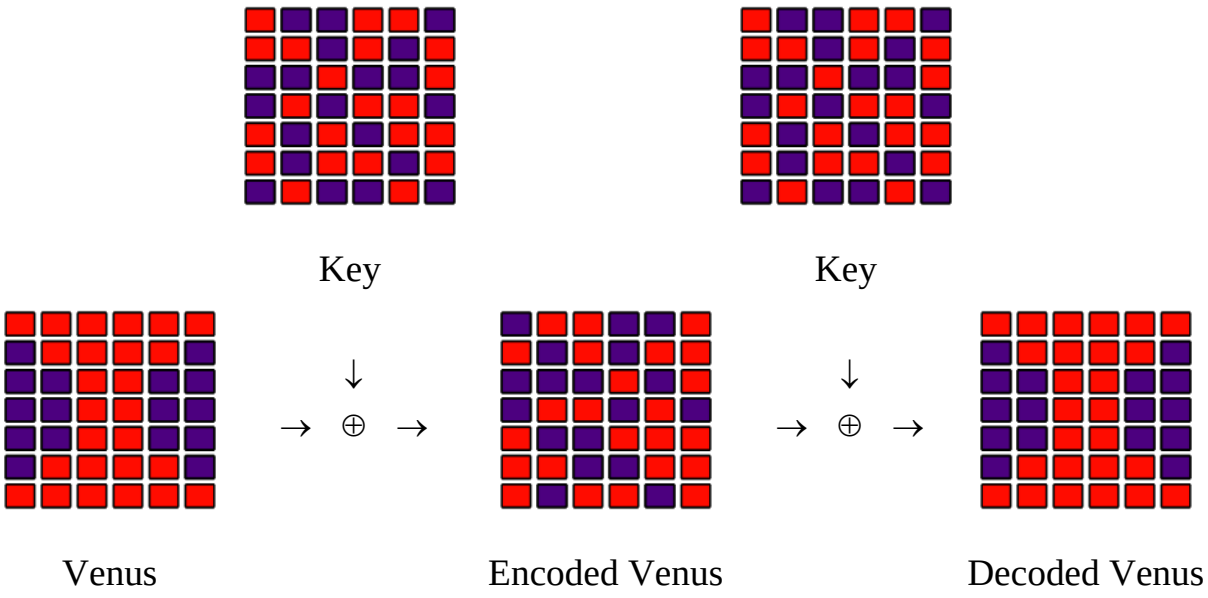
A coded version of Venus is prepared by adding Venus and the Key modulo 2 and sent to Bob.

$$i := 1 .. 7 \qquad j := 1 .. 6 \qquad \text{CVenus}_{i,j} := \text{Venus}_{i,j} \oplus \text{Key}_{i,j} \qquad \text{CVenus} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Bob adds the key to CVenus modulo 2 and sends the result to his printer.

$$DVenus_{i,j} := CVenus_{i,j} \oplus Key_{i,j} \qquad DVenus = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

A graphic summary of the simulation:



Appendix

Random key production can be implemented as follows:

$$j := 1 \,..\, 20 \qquad PSA_j := trunc(rnd(4)) \cdot 90 \cdot deg \qquad PSB_j := trunc(rnd(2)) \cdot 90 \cdot deg$$

$$Det0_j := \left[\left| x^T \cdot BS \cdot M \cdot \begin{pmatrix} e^{i \cdot PSA_j} & 0 \\ 0 & e^{i \cdot PSB_j} \end{pmatrix} \cdot BS \cdot x \right| \right]^2 \qquad Det1_j := \left[\left| y^T \cdot BS \cdot M \cdot \begin{pmatrix} e^{i \cdot PSA_j} & 0 \\ 0 & e^{i \cdot PSB_j} \end{pmatrix} \cdot BS \cdot x \right| \right]^2$$

$\frac{PSA_j}{deg}$ =	$\frac{PSB_j}{deg}$ =	$Det0_j$ =	$Det1_j$ =
0	0	1	0
0	90	0.5	0.5
180	0	0	1
90	90	1	0
270	90	0	1
0	0	1	0
270	90	0	1
0	90	0.5	0.5
270	0	0.5	0.5
0	90	0.5	0.5
180	90	0.5	0.5
90	90	1	0
180	90	0.5	0.5
180	90	0.5	0.5
0	0	1	0
...	...	...	...