

1.7: Quantum Computation- A Short Course

As can be seen in the previous tutorials, teleportation involves entanglement transfer. Alice projects her photons onto one of the entangled Bell states and Bob receives a photon state which using information provided via the classical communication channel can be transformed into the teleportee state. Given the importance of entanglement in quantum computing a more elaborate example of entanglement transfer is provided in the following tutorial.

An Entanglement Swapping Protocol

In the field of quantum information interference, superpositions and entangled states are essential resources. Entanglement, a non-factorable superposition, is routinely achieved when two photons are emitted from the same source, say a parametric down converter (PDC). Entanglement swapping involves the transfer of entanglement to two photons that were produced independently and never previously interacted. The Bell states are the four maximally entangled two-qubit entangled basis for a four-dimensional Hilbert space and play an essential role in quantum information theory and technology, including teleportation and entanglement swapping. The Bell states are shown below.

$$\begin{aligned}\Phi_p &= \frac{1}{\sqrt{2}} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] & \Phi_p &:= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} & \Phi_m &= \frac{1}{\sqrt{2}} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] & \Phi_m &:= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \\ \Psi_p &= \frac{1}{\sqrt{2}} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] & \Psi_p &:= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} & \Psi_m &= \frac{1}{\sqrt{2}} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] & \Psi_m &:= \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}\end{aligned}$$

A four-qubit state is prepared in which photons 1 and 2 are entangled in Bell state Φ_p , and photons 3 and 4 are entangled in Bell state Ψ_m . The state multiplication below is understood to be tensor vector multiplication.

$$\begin{aligned}\Psi &= \Phi_p \cdot \Psi_m = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \\ \Psi &:= \frac{1}{2} \cdot (0 \ 1 \ -1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ -1 \ 0)^T \quad I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\end{aligned}$$

Four Bell state measurements are now made on photons 2 and 3 which entangles photons 1 and 4. Projection of photons 2 and 3 onto Φ_p projects photons 1 and 4 onto Ψ_m .

$$\begin{aligned}& (\text{kronecker}(I, \text{kronecker}(\Phi_p \cdot \Phi_p^T, I)) \cdot \Psi)^T \\ &= (0 \ 0.25 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0.25 \ -0.25 \ 0 \ 0 \ 0 \ 0 \ 0 \ -0.25 \ 0) \\ &= \frac{1}{2\sqrt{2}} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]^T \\ &= \frac{1}{4} \cdot (0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ -1 \ 0 \ 0 \ 0 \ 0 \ 0 \ -1 \ 0)\end{aligned}$$

Projection of photons 2 and 3 onto Φ_m projects photons 1 and 4 onto Ψ_p .

$$\begin{aligned}& (\text{kronecker}(I, \text{kronecker}(\Phi_m \cdot \Phi_m^T, I)) \cdot \Psi)^T \\ &= (0 \ 0.25 \ 0 \ 0 \ 0 \ 0 \ 0 \ -0.25 \ 0.25 \ 0 \ 0 \ 0 \ 0 \ 0 \ -0.25 \ 0) \\ &= \frac{1}{2\sqrt{2}} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]^T \\ &= \frac{1}{4} \cdot (0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ -1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ -1 \ 0)\end{aligned}$$

Projection of photons 2 and 3 onto Ψ_p projects photons 1 and 4 onto Φ_m .

$$\begin{aligned}& (\text{kronecker}(I, \text{kronecker}(\Psi_p \cdot \Psi_p^T, I)) \cdot \Psi)^T \\ &= (0 \ 0 \ -0.25 \ 0 \ -0.25 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0.25 \ 0 \ 0.25 \ 0) \\ &= \frac{1}{2\sqrt{2}} \cdot \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]^T \\ &= \frac{1}{4} \cdot (0 \ 0 \ -1 \ 0 \ -1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0)\end{aligned}$$

Finally, projection of photons 2 and 3 onto Ψ_m projects photons 1 and 4 onto Ψ_p .

$$\begin{aligned}& (\text{kronecker}(I, \text{kronecker}(\Psi_m \cdot \Psi_m^T, I)) \cdot \Psi)^T \\ &= (0 \ 0 \ -0.25 \ 0 \ 0.25 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ -0.25 \ 0 \ 0.25 \ 0 \ 0) \\ &= \frac{-1}{2\sqrt{2}} \cdot \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]^T \\ &= \frac{1}{4} \cdot (0 \ 0 \ -1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ -1 \ 0 \ 1 \ 0 \ 0)\end{aligned}$$

In our earlier examination of the quantum computer we saw that a quantum circuit can calculate all the values of $f(x)$ simultaneously, but we can only retrieve one value due to the collapse of the superposition of answers on observation. To achieve a quantum advantage in computation requires more subtle programming techniques which exploit the effects of quantum interference. The following tutorials reveal how the quantum advantage can be achieved in several areas of practical importance.

While quantum mechanics could spell disaster for public-key cryptography, it may also offer salvation. This is because the resources of the quantum world appear to offer the ultimate form of secret code, one that is guaranteed by the laws of physics to be unbreakable. Julian Brown, *The Quest for the Quantum Computer*, page 189.

In other words, "The quantum taketh away and the quantum giveth back!" Asher Peres

We begin with Shor's algorithm which demonstrates how quantum entanglement and interference effects can facilitate the factorization of large integers into their prime factors. The inability of conventional computers to do this is essential to the integrity of public-key cryptography.

Factoring Using Shor's Quantum Algorithm

This tutorial presents a toy calculation dealing with quantum factorization using Shor's algorithm. Before beginning that task, traditional classical factorization is reviewed with the example of finding the prime factors of 15. As shown below the key is to find the period of $a^x \text{ modulo } 15$, where a is chosen randomly.

$$a := 4 \quad N := 15 \quad f(x) := \text{mod}(a^x, N) \quad Q := 8 \quad x := 0 \dots Q-1$$

x	f(x)
0	1
1	4
2	1
3	4
4	1
5	4
6	1
7	4

Seeing that the period of $f(x)$ is two, the next step is to use the Euclidian algorithm by calculating the greatest common denominator of two functions involving the period and a , and the number to be factored, N .

$$\text{period} := 2 \quad \gcd\left(a^{\frac{\text{period}}{2}} - 1, N\right) = 3 \quad \gcd\left(a^{\frac{\text{period}}{2}} + 1, N\right) = 5$$

We proceed by ignoring the fact that we already know that the period of $f(x)$ is 2 and demonstrate how it is determined using a quantum (discrete) Fourier transform. After the registers are loaded with x and $f(x)$ using a **quantum** computer, they exist in the following **superposition**.

$$\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle = \frac{1}{2} [|0\rangle|1\rangle + |1\rangle|4\rangle + |2\rangle|1\rangle + |3\rangle|4\rangle + \dots]$$

The next step is to find the period of $f(x)$ by performing a quantum Fourier transform (QFT) on the input register $|x\rangle$.

$$Q := 4 \quad m := 0 \dots Q-1 \quad n := 0 \dots Q-1 \quad \text{QFT}_{m,n} := \frac{1}{\sqrt{Q}} \cdot \exp\left(i \cdot \frac{2 \cdot \pi \cdot m \cdot n}{Q}\right)$$

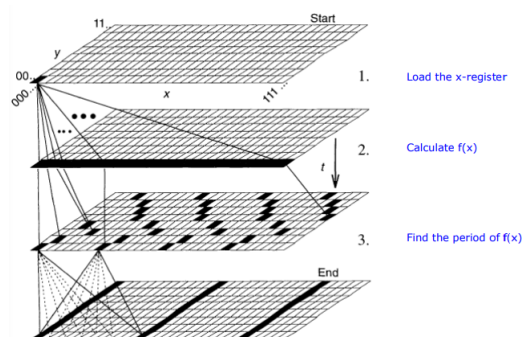
$$\text{QFT} = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

$$\begin{aligned} x=0 \quad \text{QFT} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0.5 \\ 0.5 \\ 0.5 \\ 0.5 \end{pmatrix} & x=1 \quad \text{QFT} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0.5 \\ 0.5i \\ -0.5 \\ -0.5i \end{pmatrix} \\ x=2 \quad \text{QFT} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0.5 \\ -0.5 \\ 0.5 \\ -0.5 \end{pmatrix} & x=3 \quad \text{QFT} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 0.5 \\ -0.5i \\ -0.5 \\ 0.5i \end{pmatrix} \end{aligned}$$

The operation of the QFT on the x -register is expressed algebraically in the middle term below. Quantum interference in this term yields the result on the right which shows a period of 2 on the x -register.

$$\begin{aligned} & \frac{1}{4} [|0\rangle + |1\rangle + |2\rangle + |3\rangle] |1\rangle \\ & + \\ & \frac{1}{4} [|0\rangle + i|1\rangle - |2\rangle - i|3\rangle] |4\rangle \\ & + \\ & \frac{1}{4} [|0\rangle - |1\rangle + |2\rangle - |3\rangle] |1\rangle \\ & + \\ & \frac{1}{4} [|0\rangle - i|1\rangle - |2\rangle + i|3\rangle] |4\rangle \\ \text{QFT}(x) \frac{1}{2} [|0\rangle|1\rangle + |1\rangle|4\rangle + |2\rangle|1\rangle + |3\rangle|4\rangle] &= \frac{1}{2} [|0\rangle(|1\rangle + |4\rangle) + |2\rangle(|1\rangle - |4\rangle)] \end{aligned}$$

Figure 5 in "Quantum Computation," by David P. DiVincenzo, *Science* **270**, 258 (1995) provides a graphical illustration of the steps of Shor's factorization algorithm.



How quantum theory gives back is demonstrated by an examination of Ekert's quantum secret key proposal.

The Quantum Math Behind Ekert's Key Distribution Scheme

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

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

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:

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

Pertinent superpositions:

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

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, $|R\rangle$. If Bob measures circular polarization he is certain to find his photon to be $|R\rangle$. But if he chooses to measure in the rectilinear basis the probability he will observe $|V\rangle$ is 0.5 and the probability he will observe $|H\rangle$ is 0.5.

$$\frac{1}{\sqrt{2}} \cdot R \cdot R = \frac{1}{\sqrt{2}} \cdot R \cdot \left[\frac{1}{\sqrt{2}} \cdot (V + i \cdot H) \right]$$

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

$$\frac{1}{\sqrt{2}} \cdot L \cdot L = \frac{1}{\sqrt{2}} \cdot L \cdot \left[\frac{1}{\sqrt{2}} \cdot (V - i \cdot H) \right]$$

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

$$\frac{1}{\sqrt{2}} \cdot V \cdot V = \frac{1}{\sqrt{2}} \cdot V \cdot \left[\frac{1}{\sqrt{2}} \cdot (R + L) \right] \quad \frac{1}{\sqrt{2}} \cdot H \cdot H = -\frac{1}{\sqrt{2}} \cdot H \cdot \left[\frac{i}{\sqrt{2}} \cdot (L - R) \right]$$

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: $|V\rangle = |R\rangle = 0$ and $|H\rangle = |L\rangle = 1$. 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.

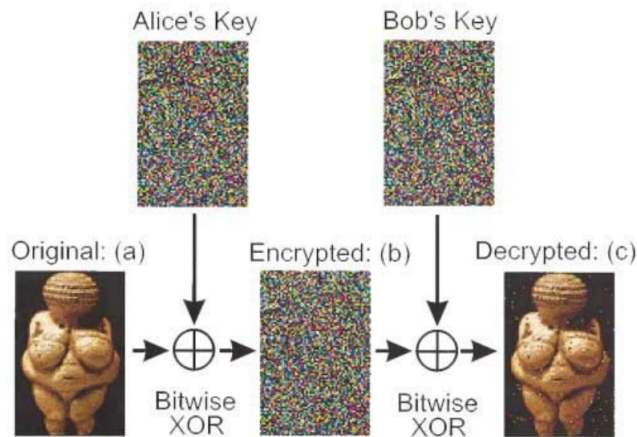
Message	Key	Coded Message	Decoded
$\text{Mes} := \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \quad (1.7.1)$	$\text{Key} := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \quad (1.7.2)$	$\text{CMes} := \text{mod}(\text{Mes} + \text{Key}, 2) \quad (1.7.3)$	$\text{DMes} := \text{mod}(\text{CMes}, 2)$

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.

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

Coding and Decoding Venus

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*.



It is easy to produce a rudimentary simulation of the experiment. Bitwise XOR is nothing more than addition modulo 2. 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).

$$i = 1..7 \quad j = 1..6 \quad \text{Key}_{i,j} := \text{trunc}(\text{md}(2))$$

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

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

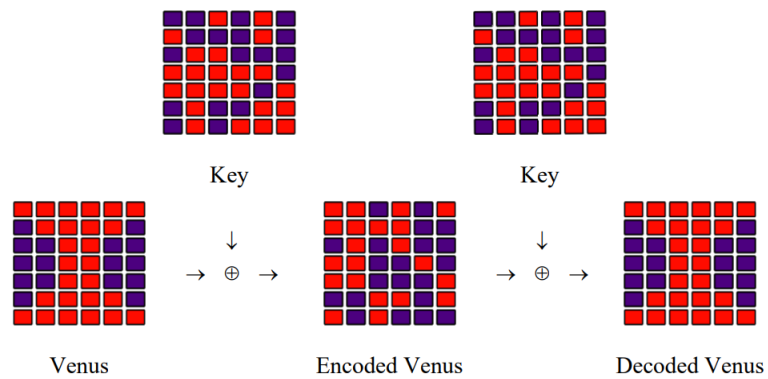
A coded version of Venus is prepared by adding Venus and the Key modulo 2 and sent to Bob.

$$C_{i,j} := \text{Venus}_{i,j} \oplus \text{Key}_{i,j} \quad \text{CVenus} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

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

$$\text{DVenus}_{i,j} := \text{CVenus}_{i,j} \oplus \text{Key}_{i,j} \quad \text{DVenus} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

A graphic summary of the simulation:



This page titled [1.7: Quantum Computation- A Short Course](#) is shared under a [CC BY 4.0](#) license and was authored, remixed, and/or curated by [Frank Rioux](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.