Quantum Key Distribution

- No radically new encryption schemes emerge from our studies of quantum information
- But QM can make our existing methods provably secure, in particular:
- We can use qubits to securely distribute private keys
- Quantum Key Distribution is provably secure
- There are several protocols: BB84, B92, EPR
- We will focus on BB84, due to Bennett and Brassard (in 1984!)

The BB84 Protocol

This is perhaps the simplest of QKD protocols

- Alice generates a random bit string b (could be classical, must be private). Say, $b = 10110101$
- Alice then forms the equivalent quantum string $|10110101\rangle$ and "encodes" it by passing each bit through either an identity or a Hadamard gate, chosen at random
- Say Alice chooses $HIHIHIHI$
- This gives the quantum state $|q\rangle = |-0 - 1 + 1 + 1\rangle$
- Alice then sends this state to Bob—not by teleportation, but using polarised photons down a fibre
- When Bob receives the state he randomly chooses whether to pass each qubit through an identity or a Hadamard gate, say $HHIIHHII$
- Bob then measures the state—where he chose the same "encoding" as Alice, the result of his measurement is certain
- In this case, Bob will measure $1??10??1$

The BB84 Protocol

- Alice and Bob then publicly announce the *encodings* they chose: Alice: HIHIHIHI; Bob: HHIIHHII
- They retain only those qubits for which they chose the same encoding, in this case, the first, fourth, fifth and eighth bits
- Alice publicly announces the values of a subset of the retained bits: e.g. bits 4 and 5: 10
- Bob checks to see whether his measurements were the same
- If so, they use the undisclosed bits as a private key for message exchange
- If not, they abort the communication
- How does this help us detect an eavesdropper?
- The key is that Eve must guess the encodings that Alice and Bob chose
- An incorrect choice will lead to Alice and Bob's checkbits failing to match

Detecting Eve

- Say Alice transmits $|q'\rangle = |-0-1+1+1\rangle$, encoded using $HIHIHIHI$
- Eve cannot know Alices encoding and must guess - say $HHHHIIII$
- Eve "decodes the intercepted signal", getting $|1+1-+1+1\rangle$ and then measures
- Eve will measure $1?1??1?1$—say 10100111
- Eve then reencodes with $HHHHIIII$, getting $|q'\rangle = -+-+0111$
- Where Eve's encoding matches Alice's, the measurement does not change the state and Eve's re-encoding reproduces $|q\rangle$
- When Eve's and Alice's encodings do not match, the quantum string that Bob receives will not be the one Alice sent
- Bob receives $|q'\rangle$, and decodes using $HHIIHHII$
- Bob measures $10????11$, for example 10111011
- Alice and Bob then publicly compare bits 4 and 5— Alice: 10; Bob: 11
- Eve's interception has corrupted the key, and Alice and Bob know it has not been transmitted securely

4.5.1 Dense Coding

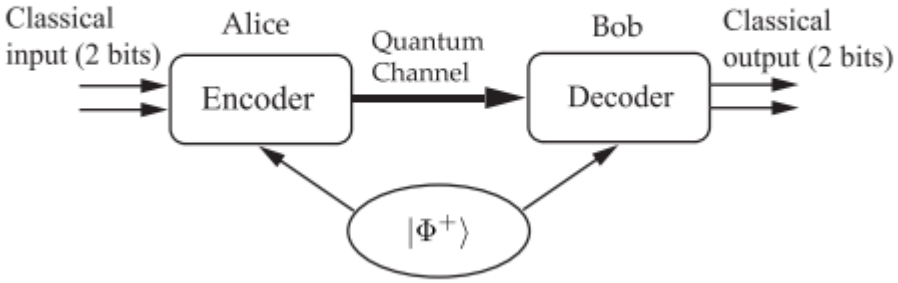

FIGURE 4.1
Communication from Alice to Bob using dense coding. Each qubit of the Bell state $|\Phi^+\rangle$ has been distributed to each of them beforehand. Then two bits of classical information can be transmitted by sending a single qubit through the quantum channel.

Alice: Alice wants to send Bob a binary number $x \in \{00, 01, 10, 11\}$. She picks up one of $\{I, X, Y, Z\}$ according to x she has chosen and applies the transformation on her qubit (the first qubit of the Bell state). Applying the transformation to only her qubit means she applies an identity transformation

to the second qubit which Bob keeps with him. This results in

$$\begin{array}{lll} x & \text{transformation } U & \text{state after transformation} \\ 0 = 00 & I \otimes I & |\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ 1 = 01 & X \otimes I & |\psi_1\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ 2 = 10 & Y \otimes I & |\psi_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \\ 3 = 11 & Z \otimes I & |\psi_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \end{array} \tag{4.39}$$

Alice sends Bob her qubit after the transformation given above is applied. Note that the set of four states in the rightmost column is nothing but the four Bell basis vectors.

Bob: Bob applies CNOT to the entangled pair in which the first qubit, the received qubit, is the control bit, while the second one, which Bob keeps, is the target bit. This results in a tensor-product state:

$$\begin{array}{llll} \text{Received state} & \text{Output of CNOT} & \text{1st qubit} & \text{2nd qubit} \\ |\psi_0\rangle & \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & |0\rangle \\ |\psi_1\rangle & \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) & \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) & |1\rangle \\ |\psi_2\rangle & \frac{1}{\sqrt{2}}(|11\rangle - |01\rangle) & \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) & |1\rangle \\ |\psi_3\rangle & \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & |0\rangle \end{array} \tag{4.40}$$

Note that Bob can measure the first and second qubits independently since the output is a tensor-product state. The number x is either 00 or 11 if the measurement outcome of the second qubit is $|0\rangle$, while it is either 01 or 10 if the meansurement outcome is $|1\rangle$.

Finally, a Hadamard transformation H is applied on the first qubit. Bob obtains

$$\begin{array}{lll} \text{Received state} & \text{1st qubit} & U_{\mathrm{H}}|\text{1st qubit}\rangle \\ |\psi_0\rangle & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & |0\rangle \\ |\psi_1\rangle & \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) & |0\rangle \\ |\psi_2\rangle & \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) & -|1\rangle \\ |\psi_3\rangle & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & |1\rangle \end{array} \tag{4.41}$$

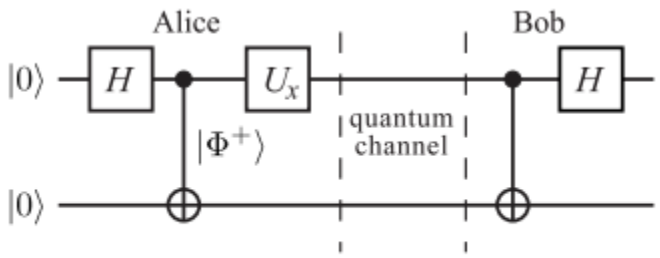

FIGURE 4.2
Quantum circuit implementation of the dense coding system. The leftmost Hadamard gate and the next CNOT gate generate the Bell state. Then a unitary gate U, depending on the bits Alice wants to send, is applied to the first qubit. Bob applies the rightmost CNOT gate and the Hadamard gate to decode Alice's message.

The number x is either 00 or 01 if the measurement of the first qubit results in $|0\rangle$, while it is either 10 or 11 if it is $|1\rangle$. Therefore, Bob can tell what x is in every case.

Quantum circuit implementation for the dense coding is given in Fig. 4.2

4.5.2 Quantum Teleportation

The purpose of **quantum teleportation** is to transmit an unknown quantum *state* of a qubit using two classical bits such that the recipient reproduces exactly the same state as the original qubit state. Note that the qubit itself is not transported but the information required to reproduce the quantum state is transmitted. The original state is destroyed such that quantum teleportation should not be in contradiction with the no-cloning theorem. Quantum teleportation has already been realized under laboratory conditions using photons [6, 7, 8, 9], coherent light field [10], NMR [11], and trapped ions [12, 13]. The teleportation scheme introduced in this section is due to [11]. Figure 4.3 shows the schematic diagram of quantum teleportation, which will be described in detail below.

Alice: Alice has a qubit, whose state she does not know. She wishes to send Bob the quantum state of this qubit through a classical communication channel. Let

$$|\phi\rangle = a|0\rangle + b|1\rangle \tag{4.42}$$

be the state of the qubit. Both of them have been given one of the qubits of the entangled pair

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

as in the case of the dense coding.

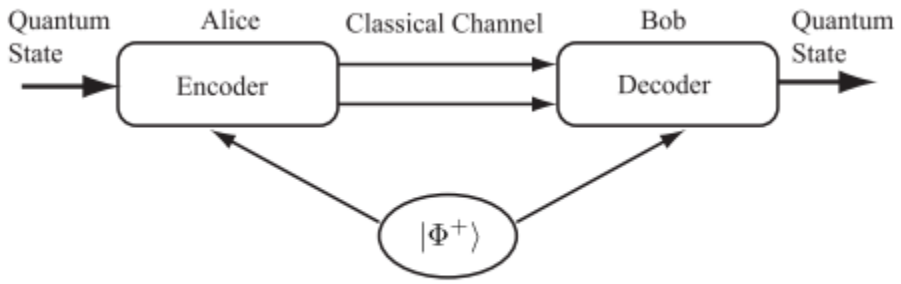

FIGURE 4.3
In quantum teleportation, Alice sends Bob two classical bits so that Bob reproduces a qubit state Alice used to have.

Alice applies the decoding step in the dense coding to the qubit $|\phi\rangle = a|0\rangle + b|1\rangle$ to be sent and her qubit of the entangled pair. They start with the state

$$\begin{aligned} |\phi\rangle \otimes |\Phi^+\rangle &= \frac{1}{\sqrt{2}}\left[a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)\right] \\ &= \frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right), \end{aligned} \tag{4.43}$$

where Alice has the first two qubits while Bob has the third. Alice applies $U_{\text{CNOT}} \otimes I$ followed by $U_{\text{H}} \otimes I \otimes I$ to this state, which results in

$$\begin{aligned} &(U_{\text{H}} \otimes I \otimes I)(U_{\text{CNOT}} \otimes I)(|\phi\rangle \otimes |\Phi^+\rangle) \\ &= (U_{\text{H}} \otimes I \otimes I)(U_{\text{CNOT}} \otimes I)\frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right) \\ &= \frac{1}{2}\left[a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\right] \\ &= \frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) \\ &\qquad + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)]. \end{aligned} \tag{4.44}$$

If Alice measures the two qubits in her hand, she will obtain one of the states $|00\rangle, |01\rangle, |10\rangle$ or $|11\rangle$ with equal probability 1/4. Bob's qubit (a qubit from the Bell state initially) collapses to $a|0\rangle + b|1\rangle, a|1\rangle + b|0\rangle, a|0\rangle - b|1\rangle$ or $a|1\rangle - b|0\rangle$, respectively, depending on the result of Alice's measurement. Alice then sends Bob her result of the measurement using two classical bits.

Notice that Alice has totally destroyed the initial qubit $|\phi\rangle$ upon her measurement. This makes quantum teleportation consistent with the no-cloning theorem.

Bob: After receiving two classical bits, Bob knows the state of the qubit in

his hand;

Received bits	Bob's state	Decoding
00	$a\|0\rangle + b\|1\rangle$	I
01	$a\|1\rangle + b\|0\rangle$	X
10	$a\|0\rangle - b\|1\rangle$	Z
11	$a\|1\rangle - b\|0\rangle$	Y

(4.45)

Bob reconstructs the intial state $|\phi\rangle$ by applying the decoding process shown above. Suppose Alice sends Bob the classical bits 10, for example. Then Bob applies Z to his state to reconstruct $|\phi\rangle$ as follows:

$$Z: \ (a|0\rangle - b|1\rangle) \mapsto (a|0\rangle + b|1\rangle) = |\phi\rangle.$$

Figure 4.4 shows the actual quantum circuit for quantum teleportation.

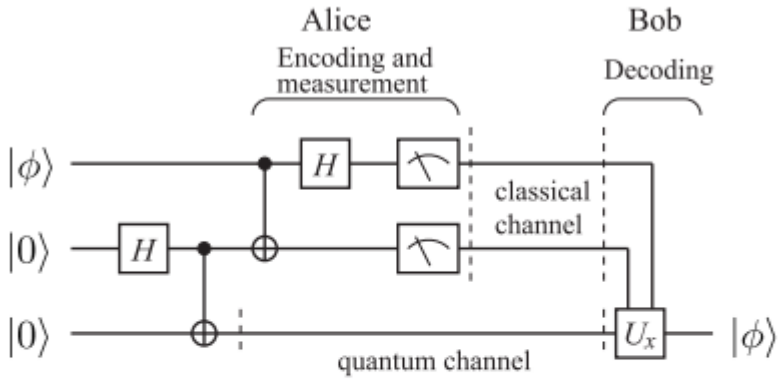

FIGURE 4.4
Quantum circuit implementation of quantum teleportation. Alice operates gates in the left side. The first Hadamard gate and the next CNOT gates generate the Bell state $|\Phi^+\rangle$ from $|00\rangle$. The bottom qubit is sent to Bob through a quantum channel while the first and the second qubits are measured after applying the second set of the CNOT gate and the Hadamard gate on them. The measurement outcome x is sent to Bob through a classical channel. Bob operates a unitary operation U_x, which depends on the received message x, on his qubit.

The Fourier Transform

- FT allows us to extract the underlying periodic behaviour of a function
- Period finding is the basis for Shor's factoring algorithm, and wewill use the QFT in this important application of quantum computing
- We must begin by defining the discrete version of the Fourier Transform, which will form the basis for the quantum algorithm

Discrete Fourier Transform

- The DFT is a version of the FT which works on discrete data sets
- Mathematically, the DFT is written as

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N}$$

- Looks formidable, but isn't too hard to calculate
- x_j are complex numbers, with $j = 0 \ldots N-1$
- y_k are complex numbers, with $k = 0 \ldots N-1$
- $\mathrm{i} = \sqrt{-1}$; j and k are indices
- An example will show us how to calculate this in practice

An Example Calculation

- Given $x_j = \{1, 2\}$, calculate y_k
- $x_0 = 1$, $x_1 = 2$, and $N = 2$
- So $y_k = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} x_j e^{2\pi i j k/2}$
- For $k = 0$, $y_0 = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} x_j = \frac{1}{\sqrt{2}} + \frac{2}{\sqrt{2}} = \frac{3}{\sqrt{2}}$
- For $k = 1$, $y_1 = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} x_j e^{2\pi i j/2} = \frac{1}{\sqrt{2}} \left(1 + 2e^{\pi i}\right) = -\frac{1}{\sqrt{2}}$
- So it's really not that hard to calculate
- The Fast Fourier Transform (FFT) algorithm of Cooley and Tukey allows us to compute the DFT very rapidly
- The FFT is often use in sound and image processing for the removal of noise
- In general, the FT is useful when there is underlying periodicity
- We will later see that the FT allows us to manipulate quantum state vectors to allow us to measure the result of quantum computations

The Quantum Fourier Transform

Since our state vectors for qubits are just vectors of complex numbers, we should not be surprised to learn that the DFT can be applied to them

Given a state vector $|\psi\rangle = \sum_{j=0}^{N-1} a_j |j\rangle = \begin{pmatrix} a_0 \\ \vdots \\ a_{N-1} \end{pmatrix}$

We can compute the DFT of this state as

$$F|\psi\rangle = \sum_{k=0}^{N-1} b_k |k\rangle$$

$$\text{where} \quad b_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{2\pi i j k/N}$$

It can be shown that this is unitary, and so can be implemented

Example of a QFT

- Consider the 2-qubit state $|\psi\rangle = a_{00}|00\rangle + a_{01}|00\rangle + a_{10}|10\rangle + a_{11}|11\rangle$, which has $N = 4$.
- Then $b_k = \frac{1}{2}\sum_{j=0}^{3} a_j e^{2\pi i jk/4}$, and we have

$$
\begin{aligned}
b_0 &= \frac{1}{2}\sum_{j=0}^{3} a_j = \frac{1}{2}(a_{00} + a_{01} + a_{10} + a_{11}) \\
b_1 &= \frac{1}{2}\sum_{j=0}^{3} a_j e^{2\pi ij/4} = \frac{1}{2}\left(a_{00} + a_{01}e^{i\pi/2} + a_{10}e^{i\pi} + a_{11}e^{3i\pi/2}\right) \\
b_2 &= \frac{1}{2}\sum_{j=0}^{3} a_j e^{4\pi ij/4} = \frac{1}{2}\left(a_{00} + a_{01}e^{i\pi} + a_{10}e^{2i\pi} + a_{11}e^{3i\pi}\right) \\
b_3 &= \frac{1}{2}\sum_{j=0}^{3} a_j e^{6\pi ij/4} = \frac{1}{2}\left(a_{00} + a_{01}e^{3i\pi/2} + a_{10}e^{3i\pi} + a_{11}e^{9i\pi/2}\right)
\end{aligned}
$$

Example of a QFT

- Writing $\omega = e^{\pi i/2}$, and noting that $\omega^4 = e^{2\pi i} = 1$ and so, e.g. $e^{9i\pi/2} = e^{i\pi/2} = i$, we can write the 2-qubit QFT in matrix form:

$$
F = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & 1 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}
$$

- This can easily be shown to be a unitary operator
- We can build a fairly simple quantum circuit that performs this transformation

4.7 Quantum Parallelism and Entanglement

Given an input x, a typical quantum computer computes $f(x)$ in such a way as

$$U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle, \tag{4.61}$$

where U_f is a unitary matrix that implements the function f.

Suppose U_f acts on the input which is a superposition of many states. Since U_f is a linear operator, it acts simultaneously on all the vectors that constitute the superposition. Thus the output is also a superposition of all the results;

$$U_f : \sum_x |x\rangle|0\rangle \mapsto \sum_x |x\rangle|f(x)\rangle. \tag{4.62}$$

Namely, when the input is a superposition of n states, U_f computes n values $f(x_k)$ $(1 \leq k \leq n)$ simultaneously. This feature, called the *quantum parallelism*, gives a quantum computer an enormous power. A quantum computer is advantageous compared to a classical counterpart in that it makes use of this quantum parallelism and also entanglement.

A unitary transformation acts on a superposition of all possible states in most quantum algorithms. This superposition is prepared by the action of the Walsh-Hadamard transformation on an n-qubit register in the state $|00\ldots0\rangle = |0\rangle \otimes |0\rangle \otimes \ldots \otimes |0\rangle$ resulting in

$$\frac{1}{\sqrt{2^n}}(|00\ldots0\rangle + |00\ldots1\rangle + \ldots |11\ldots1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \tag{4.63}$$

This state is a superposition of vectors encoding all the integers between 0 and $2^n - 1$. Then the linearity of U_f leads to

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f|x\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle. \tag{4.64}$$

5.1 Deutsch Algorithm

The **Deutsch algorithm** is one of the first quantum algorithms which showed quantum algorithms may be more efficient than their classical counterparts. In spite of its simplicty, full use of the superposition principle has been made here.

Let $f : \{0,1\} \to \{0,1\}$ be a binary function. Note that there are only four possible f, namely

$$f_1 : 0 \mapsto 0,\ 1 \mapsto 0, \quad f_2 : 0 \mapsto 1,\ 1 \mapsto 1,$$
$$f_3 : 0 \mapsto 0,\ 1 \mapsto 1, \quad f_4 : 0 \mapsto 1,\ 1 \mapsto 0.$$

The first two cases, f_1 and f_2, are called *constant*, while the rest, f_3 and f_4, are *balanced*. If we only have classical resources, we need to evaluate f twice to tell if f is constant or balanced. There is a quantum algorithm, however, with which it is possible to tell if f is constant or balanced with a single evaluation of f, as was shown by Deutsch [2].

Let $|0\rangle$ and $|1\rangle$ correspond to classical bits 0 and 1, respectively, and consider the state $|\psi_0\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$. We apply f on this state in terms of the unitary operator $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$, where $\oplus$ is an addition mod 2. To be explicit, we obtain

$$\begin{aligned}
|\psi_1\rangle &= U_f|\psi_0\rangle \\
&= \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle) \\
&= \frac{1}{2}(|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle),
\end{aligned}$$

where $\neg$ stands for negation. Therefore this operation is nothing but the CNOT gate with the control bit $f(x)$; the target bit y is flipped if and only if

$f(x) = 1$ and left unchanged otherwise. Subsequently we apply a Hadamard gate on the first qubit to obtain

$$\begin{aligned}|\psi_2\rangle &= (U_{\mathrm{H}} \otimes I)|\psi_1\rangle \\ &= \frac{1}{2\sqrt{2}}\left[(|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle)\right].\end{aligned}$$

The wave function reduces to

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle(|f(0)\rangle - |\neg f(0)\rangle) \tag{5.1}$$

in case f is constant, for which $|f(0)\rangle = |f(1)\rangle$, and

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |\neg f(0)\rangle) \tag{5.2}$$

if f is balanced, for which $|\neg f(0)\rangle = |f(1)\rangle$. Therefore the measurement of the first qubit tells us whether f is constant or balanced.

Let us consider a quantum circuit which implements the Deutsch algorithm. We first apply Walsh-Hadamard transformation $W_2 = U_{\mathrm{H}} \otimes U_{\mathrm{H}}$ on $|01\rangle$ to obtain $|\psi_0\rangle$. We need to introduce a conditional gate U_f, i.e., the controlled-NOT gate with the control bit $f(x)$, whose action is $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$. Then a Hadamard gate is applied on the first qubit before it is measured. Figure 5.1 depicts this implementation.

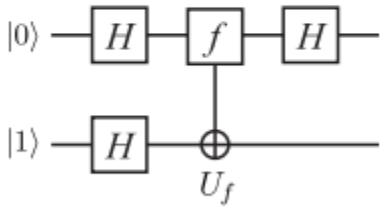

FIGURE 5.1
Implementation of the Deutsch algorithm.