Fundamentals

Qubits

A single qubit is a two–state system, such as a two–level atom we denote two orthogonal states of a single qubit as

\[ \{ |0\rangle, |1\rangle \} \]

Any state of this system can be in arbitrary superposition:

\[ \alpha |0\rangle + \beta |1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1. \]

\(n\) qubits

more generally, a system of \(n\) qubits represents a Hilbert space of dimension \(2^n\), and the state of the “system” is a superposition of the basic states

\[
\sum_{i=1}^{2^n} \alpha_i |\psi_i\rangle, \quad \sum_{i=1}^{2^n} |\alpha_i|^2 = 1
\]

\[ |\psi_i\rangle = |a_1 a_2 \cdots a_n\rangle, \quad a_i \in \{0, 1\} \]
Entangled States

Example 1: product state

$$\frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

Example 2: EPR (Einstein–Podolsky–Rosen) pair

$$\frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$
Unitary Operations

\[ S_1 \xrightarrow{\mathcal{U}} S_2 \]

Hadamard transformation

A 1-qubit operation, denoted by \( H \), and performs the following transform

\[
|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),
|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).
\]

NOT

A 1-qubit operation

\[
|0\rangle \mapsto |1\rangle,
|1\rangle \mapsto |0\rangle.
\]
Measurement

Example 1:

\[ |S\rangle = \sqrt{\frac{1}{3}} |00\rangle + \sqrt{\frac{2}{3}} |11\rangle \]

measurement \[\rightarrow\] \[\begin{cases} |00\rangle \text{ with probability } \frac{1}{3} \\ |11\rangle \text{ with probability } \frac{2}{3} \end{cases}\]

Example 2: partial measurement

\[ \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \]

first system measured \[\rightarrow\] \[\begin{cases} |0\rangle \text{ with probability } \frac{1}{2} \text{ and the system collapses to } |1\rangle \\ |1\rangle \text{ with probability } \frac{1}{2} \text{ and the system collapses to } |0\rangle \end{cases}\]

Example 3:

\[ \frac{1}{2} |0\rangle_1 (|0\rangle_2 - |1\rangle_2) + \frac{1}{2} |1\rangle_1 (|0\rangle_2 + |1\rangle_2) \]

first system measured \[\rightarrow\] \[\begin{cases} |0\rangle \text{ the system collapses to } \frac{1}{\sqrt{2}} (|0\rangle_2 - |1\rangle_2) \\ |1\rangle \text{ the system collapses to } \frac{1}{\sqrt{2}} (|0\rangle_2 + |1\rangle_2) \end{cases}\]
Quantum Teleportation

There are two players: *Alice* and *Bob*.

*Alice* is given a quantum system $|\varphi\rangle_1$ unknown to her.

*Alice* wants to send sufficient information about $|\varphi\rangle_1$ so that *Bob* is able to make an accurate copy of it. *Alice* is not allowed to transform the original particle.
Suppose Alice and Bob each has a particle of an EPR pair:

\[
\begin{aligned}
& |\varphi\rangle_1 = \alpha |0\rangle_1 + \beta |1\rangle_1, \quad |\alpha|^2 + |\beta|^2 = 1 \\
\text{EPR pair: } |\Psi\rangle_{23} = \frac{1}{\sqrt{2}} (|0\rangle_2 |1\rangle_3 - |1\rangle_2 |0\rangle_3)
\end{aligned}
\]
the state of the three particles:

\[
|\varphi\rangle_1 |\Psi\rangle_{23} = \\
(\alpha |0\rangle_1 + \beta |1\rangle_1) \frac{1}{\sqrt{2}} (|0\rangle_2 |1\rangle_3 - |1\rangle_2 |0\rangle_3) \\
= \frac{\alpha}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 |1\rangle_3 - |0\rangle_1 |1\rangle_2 |0\rangle_3) \\
+ \frac{\beta}{\sqrt{2}} (|1\rangle_1 |0\rangle_2 |1\rangle_3 - |1\rangle_1 |1\rangle_2 |0\rangle_3)
\]

It can be written as

\[
= \frac{1}{2} |A\rangle_{12} (-\alpha |0\rangle_3 - \beta |1\rangle_3) \\
+ \frac{1}{2} |B\rangle_{12} (-\alpha |0\rangle_3 + \beta |1\rangle_3) \\
+ \frac{1}{2} |C\rangle_{12} (\beta |0\rangle_3 + \alpha |1\rangle_3) \\
+ \frac{1}{2} |D\rangle_{12} (-\beta |0\rangle_3 + \alpha |1\rangle_3)
\]
where

\[ |A\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2) \]

\[ |B\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2) \]

\[ |C\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2) \]

\[ |D\rangle_{12} = \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 - |1\rangle_1 |1\rangle_2) \]

The four states

\[ |A\rangle_{12}, \quad |B\rangle_{12}, \quad |C\rangle_{12}, \quad |D\rangle_{12} \]

are a complete orthonormal basis for particles 1 and 2.
Alice measures in Bell operator basis of 
\{ |A\rangle_{12}, |B\rangle_{12}, |C\rangle_{12}, |D\rangle_{12} \} the joint system 
consists of the particle 1 (i.e., |φ⟩_1) and the particle 2 
(her EPR particle).

Regardless of the unknown state |φ⟩_1, the four 
measurement outcomes are equally likely.

After Alice’s’s measurement, Bob’s particle 3 will be 
projected into one of the following four pure states:

<table>
<thead>
<tr>
<th>result of Alice’s measurment</th>
<th>Bob’s particle 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A⟩_{12}</td>
</tr>
<tr>
<td></td>
<td>B⟩_{12}</td>
</tr>
<tr>
<td></td>
<td>C⟩_{12}</td>
</tr>
<tr>
<td></td>
<td>D⟩_{12}</td>
</tr>
</tbody>
</table>

Alice, via the classical channel, sends the result of the 
measurement. Then Bob performs the corresponding 
unitary operation on his particle.
Alice and Bob are provided with binary strings $x$ and $y$.

**goal:** Alice has to determine $f(x, y)$, where

$$f(x, y) : \{0, 1\}^n \times \{0, 1\}^n \longrightarrow \{0, 1\},$$

with as little communication between Alice and Bob as possible.
**trivial solution:** Bob sends all his $n$ bits to Alice.

**nontrivial question:** Can this be done with communicating less than $n$ bits?

Two–party **communication complexity** of the function $f$ is the minimum number of bits that must be communicated between Alice and Bob in order for Alice to compute $f(x, y)$.

Generalization to more than two parties is straightforward.
**Example 1:** The parity function

\[ f(x, y) = x_1 \oplus \cdots \oplus x_n \oplus y_1 \oplus \cdots \oplus y_n \]

\(\oplus\): addition modulo two.

It suffices for Bob to send a single bit (i.e., \(y_1 \oplus \cdots \oplus y_n\)) to Alice.

**Example 2:** The inner product modulo two

\[ IP(x, y) = (x_1 \cdot y_1) \oplus \cdots \oplus (x_n \cdot y_n) \]

It is proved that \(n\) bits of communication is necessary. That is, there is no communication protocol that allows Alice to compute \(IP(x, y)\) if the total number of bits communicated is less than \(n\).

**Question:** If Alice and Bob share quantum entangled particles, is it possible to reduce the communication complexity?
There are $k$ parties. The party $P_i$ receives $x_i \in \{0, 1, \ldots, 2^n - 1\}$. The inputs satisfy

$$\left(\sum_{i=1}^{k} x_i\right) \mod 2^{n-1} = 0.$$  

The goal is to compute

$$F(x_1, \ldots, x_k) = \frac{1}{2^{n-1}} \left[ \left(\sum_{i=1}^{k} x_i\right) \mod 2^n \right]$$

which is always is 0 or 1.

The classical communication complexity of $F$ is

$$\approx k \log_2 k.$$  

If parties share entangled particles then $F$ can be computed by communicating $k$ bits.
The parties share the cat state

\[ |q_1 \cdots q_k \rangle = \frac{1}{\sqrt{2}}(|00 \cdots 0\rangle + |11 \cdots 1\rangle) , \]

where the party \( P_i \) holds the qubit \( q_i \).
the protocol:

(1) Each party $P_i$ applies the phase–change operator

$$|0\rangle \mapsto |0\rangle$$
$$|1\rangle \mapsto e^{\frac{2\pi i \omega_i}{2^n}} |1\rangle$$
on his qubit $q_i$.

(2) Each $P_i$ applies the Hadamard transform

$$|0\rangle \mapsto \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$
$$|1\rangle \mapsto \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$
on his qubit $q_i$.

(3) $P_i$ measures his qubit $q_i$ in the basis $\{|0\rangle, |1\rangle\}$, and sends the outcoming bit $b_i$ to the others.

Then $F(x_1, \ldots, x_k) = b_1 \oplus \cdots \oplus b_k$. 
Why is this protocol correct?

After applying the phase-change operator, the entangled state becomes

$$\frac{1}{\sqrt{2}} (|00\cdots0\rangle + e^{\frac{2\pi i}{2^n}(x_1+\cdots+x_k)} |11\cdots1\rangle)$$

The Hadamard transform results in (with factor $\frac{1}{\sqrt{2^{n+1}}}$)

$$\sum_{z \in \{0,1\}^n} |z\rangle + e^{\frac{2\pi i}{2^n}(x_1+\cdots+x_k)} \sum_{z \in \{0,1\}^n} (-1)^{z \cdot 1} |z\rangle$$

or

$$\sum_{z \in \{0,1\}^n} |z\rangle + (-1)^{F(x_1,\ldots,x_k)} \sum_{z \in \{0,1\}^n} (-1)^{z \cdot 1} |z\rangle$$

which is $\sum_{z \text{ even}} |z\rangle$ if $F(x_1, \ldots, x_k) = 0$, and $\sum_{z \text{ odd}} |z\rangle$ otherwise.
The RSA public key cryptosystem

Alice
plain message → $E_B$ → open channel → $D_B$ → plain message

Bob
private file

Eve
public file

$E_B$

private file

<table>
<thead>
<tr>
<th>prime numbers: ( p ) and ( q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N = p \cdot q )</td>
</tr>
<tr>
<td>integers ( e ) and ( d ) such that ( d \cdot e \equiv 1 \pmod{\gamma(N)} )</td>
</tr>
<tr>
<td>where ( \gamma(N) ) = least common multiple ((p - 1, q - 1))</td>
</tr>
</tbody>
</table>

public file

| \( N \) and \( e \) |

\[
E_B(x) = x^e \pmod{N} \\
D_B(x) = x^d \pmod{N}
\]

It holds that

\[
D_B(E_B(x)) = x^{e \cdot d} \pmod{N} = x
\]
Example:

\[ p = 5, \quad q = 7, \quad \text{then } N = 35 \]

\[ \gamma(N) = \text{l.c.m.}(4, 6) = 12 \]

chose \( e = 17 \), then \( 17d \equiv 1 \pmod{12} \implies d = 5 \)

public file: \( N = 35 \) and \( e = 17 \)

If the plaintext is \( P = 33 \) then the ciphertext is

\[ E_B(33) = 33^{17} \pmod{35} = 3. \]

Bob uses \( D_B(3) = 3^5 \pmod{35} = 33 \) to obtain the plain text \( P \).
Quantum Cryptography

Alice

plain message
encryption
open channel
key
Eve

Bob

decryption
plain message

Quantum channel
Generating quantum key distribution:

*Alice* and *Bob* generate their own independent sets of random numbers:

<table>
<thead>
<tr>
<th>Alice</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Bob</em></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>...</td>
</tr>
</tbody>
</table>

They try to find a subset of identical bits in their sets of random bits.

<table>
<thead>
<tr>
<th>Alice</th>
<th>*</th>
<th>0</th>
<th>*</th>
<th>*</th>
<th>1</th>
<th>*</th>
<th>*</th>
<th>1</th>
<th>*</th>
<th>*</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Bob</em></td>
<td>*</td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>1</td>
<td>*</td>
<td>*</td>
<td>1</td>
<td>*</td>
<td>*</td>
<td>...</td>
</tr>
</tbody>
</table>

The result is their common key:

```
0 1 1 ... 
```
How to find the common bits securely?

*Alice* sends, through a quantum channel, the following quantum states for each bit in her set

<table>
<thead>
<tr>
<th>bit</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$</td>
</tr>
<tr>
<td>1</td>
<td>$</td>
</tr>
</tbody>
</table>

*Bob* makes a measurement on each state he receives. The measurement depends on his corresponding bit.

<table>
<thead>
<tr>
<th>bit</th>
<th>measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$P_{</td>
</tr>
<tr>
<td>1</td>
<td>$P_{</td>
</tr>
</tbody>
</table>
Measurement $P_{\left|x\right>}$ is a projection operator

$$P_{\left|x\right>} = \left|x\right> \left<x\right|.$$  

The result of this measurement on state $\left|\varphi\right>$ is

$$\frac{P_{\left|x\right>}\left|\varphi\right>}{\|P_{\left|x\right>}\left|\varphi\right>\|}, \text{ with probability } \left<\varphi\left|P_{\left|x\right>}\right|\varphi\right>, \quad \frac{(1 - P_{\left|x\right>})\left|\varphi\right>}{\|(1 - P_{\left|x\right>})\left|\varphi\right>\|}, \text{ with probability } \left<\varphi\left|1 - P_{\left|x\right>}\right|\varphi\right>, \quad \frac{(1 - P_{\left|x\right>})\left|\varphi\right>}{\|(1 - P_{\left|x\right>})\left|\varphi\right>\|}, \text{ with probability } \left<\varphi\left|1 - P_{\left|x\right>}\right|\varphi\right>,$$
The probability of Bob’s measurement results:

<table>
<thead>
<tr>
<th>Alice’s bit</th>
<th>Bob’s bit</th>
<th>measurement result</th>
<th>probability</th>
<th>decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>$</td>
<td>b_0\rangle$</td>
<td>$\frac{1}{2}$</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>$</td>
<td>a_1\rangle$</td>
<td>$\frac{1}{2}$</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>$</td>
<td>a_0\rangle$</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>$</td>
<td>a_1\rangle$</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>$</td>
<td>b_1\rangle$</td>
<td>$\frac{1}{2}$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>$</td>
<td>a_0\rangle$</td>
<td>$\frac{1}{2}$</td>
</tr>
</tbody>
</table>

Y=“pass”; Bob observes $|\varphi\rangle$ when he makes the projection $P_{|\varphi\rangle}$.

N=“fail”.

If the bits are different, the decision is always “N”. If Bob and Alice have the same bit then with probability $\frac{1}{2}$ the decision is “Y”.

25
Bob sends the sequence of Y–N decisions to Alice over a public channel.
They keep only the bits for which the decision is “Y”.
The result becomes the shared key.
A Boolean function $f: \{0, 1\}^n \rightarrow \{0, 1\}$ is given. It is known that either $f$ is constant or balanced (i.e., takes values 0 and 1 an equal number of times). The problem is to decide whether $f$ is constant or balanced.

$$U_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
Step 1: prepare the state

\[ |00 \cdots 0\rangle (|0\rangle - |1\rangle), \]

where the first register consists of \( n \) qubits.

Step 2: perform the Hadamard transform on the first \( n \) qubits

\[
\sum_{x \in \{0,1\}^n} |x\rangle (|0\rangle - |1\rangle).
\]

\[
= \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle - \sum_{x \in \{0,1\}^n} |x\rangle |1\rangle.
\]
Step 3: apply

\[ \mathcal{U}_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle \]

\[
\sum_{x \in \{0,1\}^n} |x\rangle |0 \oplus f(x)\rangle - \sum_{x \in \{0,1\}^n} |x\rangle |1 \oplus f(x)\rangle .
\]

Note that for \(a \in \{0,1\}\)

\[
|0 \oplus a\rangle - |1 \oplus a\rangle = (-1)^a (|0\rangle - |1\rangle).
\]

So the result of this step is

\[
\left[ \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right] (|0\rangle - |1\rangle).
\]

Note that

\[
\sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle
\]

\[
= \begin{cases} |A\rangle = \pm \sum_{x \in \{0,1\}^n} |x\rangle & \text{if } f \text{ is constant,} \\ |B\rangle & \text{if } f \text{ is balanced,} \end{cases}
\]

Where \(|B\rangle\) is orthogonal to \(|A\rangle\).
Step 4: apply the Hadamard transform $H$ on the first $n$ qubits

note that

$$H |A\rangle = \pm |00 \cdots 0\rangle$$

because $H^{-1} = H$

$H |B\rangle$ is orthogonal to $H |A\rangle = \pm |00 \cdots 0\rangle$, because the unitary operation $H$ maps orthogonal states to orthogonal ones.

the final result

if $f$ is constant $\pm |00 \cdots 0\rangle (|0\rangle - |1\rangle)$

if $f$ is balanced $|C\rangle (|0\rangle - |1\rangle)$

where $|C\rangle$ is orthogonal to $|00 \cdots 0\rangle$

measure the first $n$ qubits

$f$ is constant if and only if we observe $n$ zeros
Grover’s algorithm: Quantum search

A Boolean function $T: \{0, 1\}^n \rightarrow \{0, 1\}$ such that $T(x) = 1$ for only one value $x = x_0$.

Find: $x_0$.

We assume that $T$ can be evaluated in unit time.

Any classical algorithm (deterministic or probabilistic) for this problem needs to check at least $\frac{1}{2} 2^n$ vectors of $\{0, 1\}^n$.

Grover’s algorithm shows the quantum computer can solves this problem in time $O(\sqrt{2^n})$. 

Fix \( c \in \{0, 1\}^n \), we define the unitary operator \( S_c \) as

\[
S_c(|x\rangle) = \begin{cases} -|x\rangle & \text{if } x = c, \\ |x\rangle & \text{otherwise.} \end{cases}
\]

We will apply \( S_0 \), for \( c = 0 \), and \( S_{x_0} \). The operator \( S_0 \) can be computed efficiently (in time polynomial in \( n \));

In the beginning we do not know \( x_0 \), but still it is possible to compute \( S_{x_0} \) efficiently, if we assume that \( T(x) \) can be computed efficiently on each given input \( x \in \{0, 1\}^n \).

The algorithm is based on iteration of the following transform:

\[
G = -H^\otimes n \ S_0 \ H^\otimes n \ S_{x_0} ,
\]
First we prepare the uniform superposition

$$|A\rangle = 2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle$$

Then we apply the transform $G$ on $|A\rangle$ repeatedly.

The operator $G$ maps each superposition of the form

$$k|x_0\rangle + \ell \sum_{x \neq x_0} |x\rangle$$

to itself.
Initially

\[ k_0 = \ell_0 = \frac{1}{\sqrt{2^n}} \]

and after \( j \) iteration of \( G \), for \( \sin \theta = \frac{1}{\sqrt{2^n}} \),

\[ k_j = \sin((2j + 1)\theta), \]
\[ \ell_j = \frac{1}{\sqrt{2^n - 1}} \cos((2j + 1)\theta), \]

After \( m \) iterations the probability of measuring \( x_0 \), i.e. \( k_m^2 \), is very close to 1 if

\[ m = \left\lfloor \frac{\pi}{4} \sqrt{2^n} \right\rfloor \]
Computing the unitary operator $S_{x_0}$
Computing the unitary operator $G$