Introduction to Quantum Information, Quantum Computation, and Its Application to Cryptography

D. J. Guan

Abstract

The development of quantum algorithms and quantum information theory, as well as the design and construction of experimental quantum computers, are the most exciting events in the scientific community in the last two decades. In this talk, I will briefly introduce quantum computation and quantum information. I will also discuss the influences of these developments on information security and our recent research results on the design of cryptographic protocol by using quantum information.

Quantum Computers

In 1982 Richard Feynman observed that certain quantum mechanical effects cannot be simulated *efficiently* on a traditional computer.

It is speculated that computations may be done more efficiently by using these quantum effects.

In 1980 Benioff introduced a quantum Turing machine model.

In 1989 Deutch proposed the quantum circuit model.

In 1993 Yao showed that the *uniform* quantum circuit model of computation is equivalent to the quantum Turing machine model.

Classical bits and Quantum Bits

classical bits:

$$0,\ 1$$

quantum bits, *qubit*: a superposition of $|0\rangle$ and $|1\rangle$

$$\alpha|0\rangle + \beta|1\rangle,$$

1. The ability of a qubit to be in a superposition state runs counter to our *common sense* of physical world around us.
2. Despite this strangeness, qubits are decidedly real. Their existence and behavior have been extensively validated by experiments.

Quantum System and Hilbert Space

A quantum system can be represented by a vector in a Hilbert space $\mathcal{H}$.

The concept of a Hilbert space generalizes the notion of Euclidean space in a way that extends methods of vector algebra from the finite-dimensional spaces to infinite-dimensional spaces.

A finite dimensional Hilbert space $\mathcal{H}$ is a vector space over the complex numbers $\mathbf{C}$ with a complex valued inner product

$$\mathcal{H} \times \mathcal{H} \mapsto \mathbf{C}$$

which is complete with respect to the norm

$$||v|| = \sqrt{(v, v)},$$

where (v, v) is the inner product.

Qubit

A *qubit* is a quantum system Q whose state is in a 2-dimensional Hilbert space $\mathcal{H}$.

Many different quantum systems can be used to realize qubits, for example,

1. polarizations of photons,
2. alignment of a nuclear spin in a uniform magnetic field,
3. ground and excited states of an electron orbiting a single atom.

Notations

ket-vector

An element of a Hilbert space $\mathcal{H}$ will be called a *ket-vector*, and denoted by $|\phi\rangle$, which is a column vector

$$|\phi\rangle = \begin{bmatrix} x \\ y \end{bmatrix}$$

Two vectors $|\phi\rangle$ and $|\varphi\rangle$ in a Hilbert space $\mathcal{H}$ represent the same state if they differ by a non-zero multiplicative constant,

$$|\phi\rangle = \lambda|\varphi\rangle.$$

Therefore, we will choose those vectors which are unit length.

Representation of Qubits

Let $|0\rangle$ and $|1\rangle$ be a basis of the Hilbert space $\mathcal{H}$.

Elements of $\mathcal{H}$ is usually denoted by

$$\alpha|0\rangle + \beta|1\rangle,$$

where α and β are complex numbers with

$$|\alpha|^2 + |\beta|^2 = 1.$$

When measured with $\{|0\rangle, |1\rangle\}$,

the probability of obtaining $|0\rangle$ is $|\alpha|^2$, and

the probability of obtaining $|1\rangle$ is $|\beta|^2$.

Bloch Sphere Representation

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = e^{ir}\left(\left(\cos\frac{z}{2}\right)|0\rangle + e^{ix}\left(\sin\frac{z}{2}\right)|1\rangle\right)$$

where z is the angle between z-axis and $|\phi\rangle$,
and x is the angles between x-axis and the projection of $|\phi\rangle$ onto the x-y-plane.

The Lie algebra $\mathbf{su}(2)$ is isomorphic to the Lie algebra $\mathbf{so}(3)$.

Observations

- Infinite many information can be represented by a qubit.
- However, when measured, it will give only one bit of information, either 0 or 1.
- After measurement, the qubit will change its superposition state to either $|0\rangle$ or $|1\rangle$, depending on the outcome of the measurement.
- It is impossible to examine a qubit to determine its quantum state. (Only if infinite many identical qubits are measured would one be able to determine the values of α and β.)

Notations

bra-vector

Let $\mathcal{H}^*$ denote the Hilbert space of all Hilbert space homomorphisms of $\mathcal{H}$ into the Hilbert space of the complex number $\mathbf{C}$

$$\mathcal{H}^* = \mathrm{Hom}(\mathcal{H}, \mathbf{C}).$$

An element of $\mathcal{H}^*$ will be called a *bra-vector*, and denoted by $\langle\varphi|$ which is a row vector

$$\langle\varphi| = [x, y]\,.$$

Note that $\langle\varphi||\phi\rangle$ is a complex number.

If $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} x \\ y \end{bmatrix}$, then $\langle\varphi| = [x^*, y^*]$.

Quantum Operators

A linear quantum operator A on Hilbert spaces $\mathcal{H}$ is denoted by a matrix A.

Evolution

The evolution of a closed quantum system is described by a *unitary* transformation.

$$|\phi_t\rangle = U|\phi_0\rangle$$

A matrix U is unitary if $U^\dagger U = I$,

where $U^\dagger = \left(U^T\right)^*$ is the adjoint of U.

Summary of Notations

1. z^*: complex conjugate,
2. $|\phi\rangle$: ket-vector, a vector in $\mathcal{H}$,
3. $\langle\varphi|$: bra-vector, a vector in $\mathcal{H}^*$, dual to $|\phi\rangle$,
4. $\langle\varphi||\phi\rangle$: inner product of $\langle\varphi|$ and $|\phi\rangle$,
5. $|\phi\rangle|\varphi\rangle = |\phi\rangle \otimes |\varphi\rangle$: tensor product of $|\phi\rangle$ and $|\varphi\rangle$,
6. A^*: complex conjugate of the matrix A,
7. A^T: transpose of the matrix A,
8. $A^\dagger = \left(A^T\right)^*$: the Hermitian conjugate or the adjoints of A.
9. $\langle\varphi|A|\phi\rangle = (|\varphi\rangle, A|\phi\rangle) = (A^\dagger|\varphi\rangle, |\phi\rangle)$

Quantum Measurement

Quantum measurements are described by a collection $\{M_r\}$ of measurement operators, where r represents the outcome of the measurement.

Assume that the state before the measurement is $|\phi\rangle$.

1. The probability that the result r occurs is

$$p(r) = \langle\phi|M_r^\dagger M_r|\phi\rangle.$$

2. The state of the quantum system after measurement is

$$\frac{M_r|\phi\rangle}{\sqrt{\langle\phi|M_r^\dagger M_r|\phi\rangle}}.$$

3. The measurement operators satisfy the completeness equation

$$\sum_r M_r^\dagger M_r = I.$$

An Example

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, and $M = \{M_0, M_1\}$

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

completeness: $M_0^\dagger M_0 + M_1^\dagger M_1 = I$

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$p(0) = \langle\phi|M_0^\dagger M_0|\phi\rangle = |\alpha|^2$$

$$p(1) = \langle\phi|M_1^\dagger M_1|\phi\rangle = |\beta|^2$$

An Example

The outcome of measuring

$$|\phi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

with $\{|0\rangle, |1\rangle\}$ will be 50% $|0\rangle$ and 50% $|1\rangle$.

$$|\phi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Composite Systems

The state space of a composite quantum system is the *tensor* product of the state space of the component quantum systems.

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$$

$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle$ is usually denoted by $|\phi_1\phi_2 \cdots \phi_n\rangle$

Quantum Entanglement

Let $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_n$ be quantum systems with underlying Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2 \ldots, \mathcal{H}_n$, respectively.

The global quantum system $\mathcal{Q}$ is *entangled* if its state

$$|\phi\rangle \in \mathcal{H} = \bigotimes_{j=1}^{n} H_j$$

cannot be written in the form

$$|\phi\rangle = \bigotimes_{j=1}^{n} |\phi_j\rangle$$

An Example

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |\phi\rangle \otimes |\varphi\rangle$ for any $|\phi\rangle$ and any $|\varphi\rangle$.

$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle)$
$= (\alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle)$

Observations

- The measurement outcome of entangled qubits are correlated.
- Entanglement is defined only for pure ensembles, entanglement for mixed ensembles has not been well understood yet.

Quantum Computation

Quantum computation is a composition of a sequence of sufficiently local unitary transformations.

$$U = U_n U_{n-1} \cdots U_1$$

Single qubit operations

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Examples

1. $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$,
2. $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$
3. $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}; \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{aligned} X(\alpha|0\rangle + \beta|1\rangle) &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \left(\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \\ &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \left(\begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} \right) \\ &= \begin{bmatrix} 0 \\ \alpha \end{bmatrix} + \begin{bmatrix} \beta \\ 0 \end{bmatrix} = \alpha \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \beta|0\rangle + \alpha|1\rangle \end{aligned}$$

Two-qubit Operations

CNOT: $(a, b) \mapsto (a, a + b)$.

a	b	x	y
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

CNOT

CNOT gate can be described by the following unitary transformation.

$$A_C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$A_C^\dagger A_C = I$$

Three-qubit operations

Toffoli: $(a, b, c) \mapsto (a, b, ab + c)$.

a	b	c	x	y	z
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Toffoli Gate

Toffoli gate can be described by the following unitary transformation.

$$A_T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$A_T^\dagger A_T = I$$

Universality

$\mathrm{NOT}(x) = X(x) = \mathrm{CNOT}(1, x) = \mathrm{Toffoli}(1, 1, x)$

$\mathrm{OR}(x, y) = \mathrm{CNOT}(x, y) = \mathrm{Toffoli}(1, x, y)$

$\mathrm{AND}(x, y) = \mathrm{Toffoli}(x, y, 0)$

[Theorem] Any Boolean function that can be computed by a Turing machine can also be computed by a quantum computer.

Reversible Computations

Since any quantum evolution can be described by a unitary transformation, any quantum computation must be *reversible*.

$$|\phi\rangle = U|\varphi\rangle$$

Since U is unitary,

$$U^\dagger U = I$$

Therefore,

$$|\varphi\rangle = U^\dagger|\phi\rangle$$

Quantum Computation

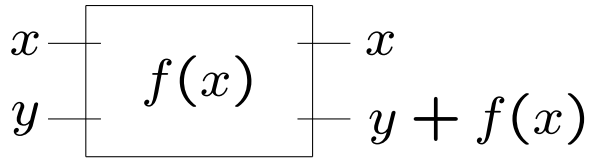
Many traditional computations are not reversible.

For example, knowing $x + y = 1$ cannot deduce the values of x and y.

We overcome this difficulty by adding extra qubits to the input and the output to make all computations reversible.

In fact, we can show that any Boolean function $f(x)$ computable by a Turing machine can be computed by a quantum computer.

$$(x, y) \mapsto (x, y + f(x))$$



Landauer's Principle

Suppose a computer erases one bit of information. Then the amount of energy dissipated into the environment is at least

$$k_B T \log 2,$$

where k_b is the Boltzmann's constant, T is the temperature of the environment.

Computers in the year 2000 dissipate roughly $500 k_B T \log 2$ in energy for each elementary logical operation.

Reversible computations dissipate minimum amount of energy, since they do not erase information.

Quantum Parallelism

By preparing each input qubit in the state

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

then n qubits will be in a state such that all the 2^n possible states

$$|00\ldots0\rangle, |00\ldots01\rangle, |00\ldots10\rangle, \ldots, |11\ldots1\rangle$$

are equally likely.

Therefore, a single application of the circuit for $f(x)$ can be used to evaluate the function f for all possible values of x. This is called *quantum parallelism*.

Quantum Parallelism

Although quantum parallelism enable all possible values of $f(x)$ to be evaluated in a single step, this is not immediately useful.

Measurement of the resulting state gives only one possible value of $f(x)$.

Computational Complexity

Turing machine is a mathematical model of classical computation.

[Church-Turing Thesis] Any model of computation can be effectively simulated on a Turing machine with at most a polynomial increase in the number of elementary operations.

Probabilistic Algorithm

In cryptography, probabilistic algorithms play an important role.

1. Miller-Rabin's primality testing algorithm
2. number fields sieve integer factoring algorithm

[Strong Church-Turing Thesis] Any model of computation can be effectively simulated on a probabilistic Turing machine with at most a polynomial increase in the number of elementary operations.

Computational Power of Quantum Computer

Can a quantum computer efficiently solve computational problems which have no efficient algorithms on a classical computer?

Efficient Quantum Algorithms

1. (1992) Deutsch-Jozsa's algorithm for testing whether a Boolean function is constant or balanced needs only 1 evaluation of the function.
   A classical algorithm needs $2^{n-1}+1$ evaluations of the function.

2. (1997) Bernstein-Vazirani's algorithm for determining the value of $a \in \mathbf{Z}_2^n$ in $f_a(x) = a \cdot x$ needs only 1 evaluation of the function.
   A classical algorithm needs n evaluations of the function.

3. (1994) Simon's algorithm for determining the period of a function $f : \mathbf{Z}_2^n \mapsto \mathbf{Z}_2^n$ needs only $O(n)$ (expected) evaluation of the function.
   A classical algorithm needs 2^n evaluations of the function.

4. (1994) Peter Shor's integer factorization algorithm runs in $O(\log^3 n)$ time.

The best-known classical algorithm needs $O\left(e^{(64/9)(\log n)^{1/3}(\log\log n)^{2/3}}\right)$ time.

5. (1995) Lov Grover's search algorithm needs only $\sqrt{n}$ queries. Traditional algorithm needs n queries.

Computational Power of Quantum Computers

1. What class of problems can be solved more efficiently on quantum computers?
2. Can quantum computational model break the strong Church-Turing thesis?

Complexity Classes

L problems which can be solved by a Turing machine in logarithmic space.

P problems which can be solved by a Turing machine in polynomial time.

NP problems which can be solved by a non-deterministic Turing machine in polynomial time.

PSpace problems which can be solved by a Turing machine in polynomial space.

ETime problems which can be solved by a Turing machine in exponential time.

Complexity Classes

$$\mathsf{L} \subseteq \mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSpace} \subseteq \mathsf{ETime}$$

Time Hierarchy Theorem:

$$\mathsf{Time}(f(n)) \subset \mathsf{Time}(f(n)\log^2(f(n))).$$

Space Hierarchy Theorem:

$$\mathsf{Space}(f(n)) \subset \mathsf{Space}(f(n)\log(f(n))).$$

$$\mathsf{L} \subset \mathsf{PSpace}$$

$$\mathsf{P} \subset \mathsf{ETime}$$

BPP problems which can be solved by a probabilistic Turing machine in polynomial time.

BQP problems which can be solved by a quantum computer in polynomial time.

$$\mathrm{P} \subseteq \mathrm{BPP} \subseteq \mathrm{BQP} \subseteq \mathrm{PSpace}$$

$$\mathrm{P} \subset \mathrm{BQP} \quad \Rightarrow \quad \mathrm{P} \subset \mathrm{PSpace}$$

Therefore, it may be *difficult/possible* to show that quantum computers are more powerful then classical computers.

Shor's algorithm

Shor's algorithm for factoring integers on a quantum computer can be briefly described as follows.

1. Choose an even integer m, $1 < m < n$, at random.
   If $\gcd(m, n) > 1$, then $\gcd(m, n)$ is a factor of n.

2. Use a *quantum computer* to determine the period r of the function
$$f(x) = m^x \bmod n.$$

3. If r is odd then repeat from step 1. Otherwise,
$$(m^{r/2})^2 \equiv 1 \pmod{n}.$$

4. If $m^{r/2} \not\equiv \pm 1 \pmod{n}$ then $\gcd(m^{r/2} + 1, n)$ is a factor of n.

Factor a Large Integer

A technique for factoring a composite integer n, which is a product of two large primes, involves finding a pair of *congruent* squares

$$x^2 \equiv y^2 \pmod{n}.$$

$$x^2 \equiv y^2 \pmod{n} \quad \Rightarrow \quad x^2 - y^2 \equiv 0 \pmod{n} \quad \Rightarrow$$

$$n \mid (x+y)(x-y).$$

If $x \not\equiv \pm y \pmod{n}$, then

$$n \not\mid (x+y) \text{ and } n \not\mid (x-y).$$

Therefore, $\gcd(x+y, n)$ and $\gcd(x-y, n)$ are the two prime factors of n.

Shor's algorithm

Finding the period of $f(x) = m^x \bmod n$ is the only step in Shor's algorithm which needs a QUANTUM COMPUTER.

This is done as follows.

1. transform each input qubit from $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
2. apply the function $f(x)$ where x is the input qubits.
3. perform the discrete Fourier transform on the data $f(x)$, $x = 0, 1, \ldots, 2^k - 1$.
4. measure the phase of the qubits to determine the period of the function f.

The Hidden Subgroup Problem

Given a group G, a subgroup $H \subseteq G$, and a set X.

A function $f : G \mapsto X$ hides the subgroup H if for all $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ if and only if $g_1 H = g_2 H$ for the cosets of H.

Equivalently, the function f is constant on the cosets of H, while it is different between the different cosets of H.

Hidden subgroup problem: Let G be a group, X a finite set, and $f : G \mapsto X$ a function that hides a subgroup $H \subseteq G$.

The function f is given via an oracle, which uses $O(\log |G| + \log |X|)$ bits.

Using information gained from evaluations of f via its oracle, determine a generating set for H.

The Hidden Subgroup Problem

G: a finitely generated group

X: a finite set

f: a function from G to X:

1. f is constant on the cosets of a subgroup H
2. f is distinct on each coset

Given a black box for performing the unitary transformation

$$U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle, \quad \text{for } g \in G \text{ and } h \in X,$$

find a generating set for H.

1. period of a function:
   $G = (\mathbf{Z}, +)$; $X =$ any finite set; $K = \{0, r, 2r, \ldots\}$; $f(x + r) = f(x)$.

2. order of an element:
   $G = (\mathbf{Z}, +)$; $X = \{a^j\}$; $a^r = 1$; $K = \{0, r, 2r, \ldots\}$; $f(x) = a^x$, $f(x + r) = f(x)$.

3. discrete logarithm:
   $G = \mathbf{Z}_r \times \mathbf{Z}_r$; $X = \{a^j\}$; $a^r = 1$; $K = \{l - ls\}$; $f(x_1, x_2) = a^{kx_1 + x_2}$, $f(x_1 + l, x_2 - ls) = f(x_1, x_2)$.

Are Quantum Computers More Powerful Then Classical Computers?

Super Dense Coding

Assume that Alice wants to send 2 classical bits to Bob.

$$\text{Alice} \xrightarrow{xy} \text{Bob}$$

This can be done by sending only 1 qubit, provided that they share two qubits in advance.

$$\text{Alice} \xrightarrow{q} \text{Bob}$$

Super Dense Coding

Let the two qubits q_0 and q_1 be in the entangled state

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

(q_0 and q_1 are also called an EPR pair.)

Initially, Alice has possession of q_0 and Bob has q_1.

1. Alice transforms her qubit by the following rules.

   $$00 : I|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad 01 : Z|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
   $$10 : X|\phi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \qquad 11 : iY|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

   and then sends her qubit to Bob.

2. Bob can recover the information sent by Alice by measuring the two qubits by using Bell basis.

Bell Basis

The Bell basis is a basis for the (2-dimensional) Hilbert space where the basis vectors are defined in terms of the computational basis as

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\bar{\phi}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \qquad |\bar{\varphi}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

The quantum states represented by these vectors are called Bell states and are maximally entangled.

In general, there are no effective ways to distinguish a quantum state by using a finite number of measurements.

The Bell states from an orthonormal basis and can, therefore, be distinguished by an appropriate quantum measurement.

No-Cloning Theorem

[Theorem] There cannot be a device that produces exact copies of a quantum state.

However, we can send a quantum object from one location to another by extracting sufficient information and then reassemble the original object at the intended destination. This is called *quantum teleportation*.

The no-cloning theorem is not violated since the original object is destroyed during the process.

Quantum Teleportation

1. Prepare two qubits q_1 and q_2 in Bell state.

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

2. Send q_2 to Bob.

3. Let the qubit to be transported be q_0 and it is in the state

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

We express the state $|\varphi\rangle$ in terms of the following basis.

$$|\phi_A\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle), \quad |\phi_B\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle),$$
$$|\phi_C\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\phi_D\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

The result is

$$\begin{aligned}|\varphi\rangle &= \frac{1}{2}[|\phi_A\rangle(-\alpha|0\rangle - \beta|1\rangle) + |\phi_B\rangle(-\alpha|0\rangle + \beta|1\rangle) \\ &\quad +|\phi_C\rangle(\alpha|1\rangle + \beta|0\rangle) + |\phi_D\rangle(\alpha|1\rangle - \beta|0\rangle)]\end{aligned}$$

4. Let U be the unitary transformation defined by

$$\begin{aligned}|\phi_A\rangle &\mapsto |00\rangle, \quad & |\phi_B\rangle &\mapsto |01\rangle, \\ |\phi_C\rangle &\mapsto |10\rangle, \quad & |\phi_D\rangle &\mapsto |11\rangle.\end{aligned}$$

Apply U to q_0 and q_1, the resulting state is

$$\begin{aligned}|\varphi\rangle &= \frac{1}{2}[|00\rangle(-\alpha|0\rangle - \beta|1\rangle) + |01\rangle(-\alpha|0\rangle + \beta|1\rangle) \\ &\quad +|10\rangle(\alpha|1\rangle + \beta|0\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]\end{aligned}$$

5. Alice measures the qubits q_0 and q_1. The results will be two classical bits 00, 01, 10, or 11. Send the two classical bits to Bob.

6. After receiving the two classical bits from Alice, Bob performs a transformation on the qubit q_2 according to the following rules.

$$00 : U = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}; \qquad 01 : U = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix};$$

$$10 : U = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}; \qquad 11 : U = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

It can be check that after the transformation, the third qubit q_2 is at the state $\alpha|0\rangle + \beta|1\rangle$.

Quantum Key Distribution

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |\phi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad |\varphi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

	$\|0\rangle$	$\|1\rangle$	$\|\phi\rangle$	$\|\varphi\rangle$
$\{\|0\rangle, \|1\rangle\}$	$\|0\rangle$	$\|1\rangle$	(1)	(1)
$\{\|\phi\rangle, \|\varphi\rangle\}$	(2)	(2)	$\|\phi\rangle$	$\|\varphi\rangle$

(1) 50%: $|0\rangle$; 50%: $|1\rangle$.

(2) 50%: $|\phi\rangle$; 50%: $|\varphi\rangle$.

In general, non-orthogonal quantum states cannot be reliably distinguished.

BB84 Key Distribution Protocol

Let $R = \{|0\rangle, |1\rangle\}$, $D = \{|\phi\rangle, |\varphi\rangle\}$.

1	1	1	0	1	1	0	0	1	0	1	1	0	0	1	0
2	R	D	R	R	R	R	R	D	D	R	D	D	D	R	D
3	$\|1\rangle$	$\|\varphi\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|\varphi\rangle$	$\|\phi\rangle$	$\|0\rangle$	$\|\varphi\rangle$	$\|\phi\rangle$	$\|\phi\rangle$	$\|0\rangle$	$\|1\rangle$
4	D	D	R	R	D	D	R	D	R	D	D	D	D	R	R
5	0	1	0	1	0	0	0	1	1	1	1	0	0	1	1
6	D	D	R	R	D	D	R	D	R	D	D	D	D	R	R
7		Y	Y	Y			Y	Y			Y	Y	Y	Y	
8				1				1			1		0		
9				Y				Y			Y		Y		
10		1	0				0					0		1	

1. Alice randomly chooses a key.
2. Alice randomly chooses a sequence of basis to encode the bit string of the key, e.g., 0: $|0\rangle$ or $|\phi\rangle$; 1: $|1\rangle$ or $|\varphi\rangle$.
3. Alice sends the qubit string to Bob.
4. Bob randomly chooses a sequence of basis to measure the qubits.

5. The information obtained by Bob.
6. Bob sends his measurement basses to Alice.
7. Alice checks the basis.
8. Bob sends some of his measurement results to Alice.
9. Alice check the correctness of these bits.
10. Alice and Bob use the other bits as the key.

Theorem. In any attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance to the signal.

Authentication Scheme

A user U wants to login to the system S.

The password for U is p.

Simple method:

1. $U \xrightarrow{u} S$
2. $U \xrightarrow{p} S$

Challenge and response:

1. $U \xrightarrow{u} S$
2. $S \xrightarrow{c} U$
3. $U \xrightarrow{h(p+c)} S$

Communication cost for step (2) and (3): $2n$ bits.

A Quantum Authentication Scheme

1. $U \xrightarrow{u} S$
2. S and U establish a secret random binary string c by using BB84 protocol.
3. $U \xrightarrow{p+c} S$

Communication cost: $4n$ qubits, plus $12n$ bits.

Another Quantum Authentication Scheme

Two sets of basis:

$$B_0 = \{|0\rangle, |1\rangle\} \qquad B_1 = \{|x\rangle, |y\rangle\}$$

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle) \\ |1\rangle &= \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle) \\ |x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |0\rangle) \\ |y\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |1\rangle) \end{aligned}$$

$p = p_1, p_2, \ldots, p_n$, $p_i \in \{0, 1\}$

$h : \mathbf{Z}_2^n \mapsto \mathbf{Z}_2^{n/2}$, a universal hash function

1. $U \xrightarrow{u} S$
2. S randomly select an integer $c = c_1, c_2, \ldots, c_n$.
3. S encodes c_i by a quantum bit q_i,

	$p_i = 0$	$p_i = 1$
$c_i = 0$	$\|0\rangle$	$\|x\rangle$
$c_i = 1$	$\|1\rangle$	$\|y\rangle$

   and sends the quantum bits to U.
4. U decodes the message c, and sends $h(c)$ to S.
5. S checks if $h(c)$ is correct or not.

Communication cost: n qubits, plus $n/2$ bits.

Key Evolution

After a successful run, S and U need to update their password from p to $f(p, c)$, where $f : \mathbf{Z}_2^{2n} \mapsto \mathbf{Z}_2^n$ is chosen randomly from a class of universal$_2$ hash functions.

Universal Hash Functions

Let A and B be two finite sets. A class of hash functions H from A to B is called universal$_2$ if for each $x, y \in A$, $x \neq y$, and a function h chosen uniformly in H at random, we have

$$\Pr[h(x) = h(y)] \leq \frac{1}{|B|}.$$

Let $A = \{1, 2, \ldots, p-1\}$, for some prime p, and $B = \{1, 2, \ldots, m-1\}$. Then

$$H = \{h_{a,b}(x) = ((ax + b) \bmod p) \bmod m \mid a, b \in A\}$$

is a class of universal$_2$ hash functions.

Privacy Amplification

Two types of communication channels:

1. perfect authenticity but no privacy.
2. imperfect privacy but no authenticity.

Privacy amplification: use a channel with perfect authenticity but no privacy to repair the defects of a channel with imperfect privacy but no authenticity.

Assume that an n-bit binary string x is shared by A and B.

Let the attacker learns at most d-bits of information about x.

Let $s < n - d$ be a safety parameter.

Let $r \leq n - d - s$, and $h : \mathbf{Z}_2^n \to \mathbf{Z}_2^R$ be a function randomly chosen from a class of universal$_2$ hash functions.

The expected amount of information the attacker has on $h(x)$ is less than $2^{-s}/\ln 2$ bits.

Conclusions

1. The rules of quantum mechanics are simple, but even experts find them counter-intuitive.

2. No *effective* quantum information processing systems have been built yet.
   Only very small quantum computers capable of doing a few operations on few quantum bits represent the state of the art in quantum computation.

3. Quantum communications seems very promising. Communication systems using quantum mechanics have been built.

4. The impact of quantum information science on information security will be revolutionary.
   New cryptosystems should be designed based on the properties of quantum mechanics to ensure the security of the systems.

References

1. Charles H. Bennett and Gilles Brassars. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, System and Singal Processing*, December 1984.

2. Charles H. Bennett, Gilles Brassars, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

3. Ranee K. Brylinski and Goong Chen, editors. *Mathematics of Quantum Computation*. CRC Press, 2002.

4. Goong Chen, David A. Church, Berthold-George Englert, Carsten Henkel, Bernd Rohwedder, Marlan O. Scully, and M. Suhail Zbairy. *Quantum Computing Devices: Principles, Designs, and Analysis*. Chapman and Hall/CRC press, 2006.

5. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.