Journal of International Technology and Information Management

Volume 29 | Issue 2 Article 3

2020

Quantum Computing: Principles and Applications

Yoshito Kanamori
University of Alaska Anchorage, ykanamori@alaska.edu

Seong-Moo Yoo
University of Alabama in Huntsville, yoos@uah.edu

Recommended Citation

Kanamori, Yoshito and Yoo, Seong-Moo (2020) "Quantum Computing: Principles and Applications," *Journal of International Technology and Information Management*: Vol. 29: Iss. 2, Article 3.
DOI: https://doi.org/10.58729/1941-6679.1410
Available at: https://scholarworks.lib.csusb.edu/jitim/vol29/iss2/3

Quantum Computing: Principles and Applications

Yoshito Kanamori
(University of Alaska Anchorage)

Seong-Moo Yoo
(University of Alabama in Huntsville)

ABSTRACT

The development of quantum computers over the past few years is one of the most significant advancements in the history of quantum computing. D-Wave quantum computer has been available for more than eight years. IBM has made its quantum computer accessible via its cloud service. Also, Microsoft, Google, Intel, and NASA have been heavily investing in the development of quantum computers and their applications. The quantum computer seems to be no longer just for physicists and computer scientists, but also for information system researchers. This paper introduces the basic concepts of quantum computing and describes well-known quantum applications for non-physicists. The current status of the developments in quantum computing is also presented.

Keywords: Quantum computer, Quantum gate, QKD, Shor, Grover

INTRODUCTION

Quantum computers seem to have a significant impact on business. Various quantum algorithms were developed since quantum computing was proposed in the 1980s (Benioff, 1980; Coles et al., 2018; Feynman, 1982; Montanaro, 2016). The most well-known quantum algorithms are Glover's database search algorithm and Shor's integer factoring algorithm. Both quantum algorithms are known to outperform the algorithms for classical computers significantly and also be used for cracking the encryption systems (e.g., AES, RSA, ECC), which have globally used on the Internet (e.g., online shopping sites.) Governments have been increasing the funding for quantum computing research and development not only for the advancement of computing technology but also for their national security. However, after the Canadian company D-wave unveiled a commercial annealer-based

ISSN: 1941-6679-On-line Copy

quantum computer in 2012, quantum computing has attracted much more increasing attention from enterprises ("D-Wave: Quantum Computing Applications," 2019; Robert Hackett, 2019).

JPMorgan Chase and Goldman Sacks have been evaluating algorithms and applications that may utilize the power of quantum computing. Their research teams have found that quantum computing could significantly reduce the time of option-pricing and risk-assessment calculations (Sara Castellanos, 2019). ExxonMobil has explored practical applications in the area of energy and chemical manufacturing, such as optimizing a country's power grid, developing more predictable environmental modeling, and discovering new materials. Daimler Mercedes-Benz has been using a quantum computer to develop a new battery for electric vehicles. Volkswagen has investigated the use of quantum computers to find a solution for the optimization of traffic flows in Beijing, China.

IBM, which owns 53-qubit gate-based quantum computers, has been collaborating with more than 100 organizations, including the companies mentioned above, across industries and made their 5-qubit and 20-qubit quantum computers available via their cloud service called "IBM Q Experience" (IBM, n.d.). More than 200 third party research papers on practical applications have been published with IBM quantum computers. This cloud service provides a graphical user interface in a browser to build quantum circuits on IBM's simulators or real quantum computers by dragging and dropping the icons, which represent quantum logic gates (e.g., NOT gate), on the lines connected to inputs and outputs. Also, the quantum circuits can be built and run remotely by using Python with the Qiskit library installed on the user's desktop computer. In January 2019, IBM unveiled the first commercial general-purpose 20-qubit gate-based quantum computer called "IBM Q System one" ("IBM Unveils World's First Integrated Quantum Computing System for Commercial Use - Jan. 8, 2019," 2019). This system enables a company to operate a gate-based quantum computer on its premises.

The commercial annealing-based quantum computer D-Wave 2000Q has about 2000 qubits (Gibney, 2017). The quantum-annealing-based quantum computer is not a universal computer but designed to solve optimization problems. NASA uses 2000Q to explore the potential for quantum computers to solve their optimization problems for applications such as air traffic control, mission planning and scheduling, machine autonomy, fault diagnosis, and robust system design (National Aeronautics and Space Administration, 2015).

D-Wave has announced its 5000-qubit system, which will be released in mid-2020, has been sold to Los Alamos National Laboratory (Wheatley, n.d.).

In 2019, Google announced its quantum computer with 53 qubits needed only 200 seconds to perform a highly technical and specialized computation that would have taken a state-of-art classical supercomputer approximately10,000 years (Arute et al., 2019). Google claimed their quantum computer had demonstrated "quantum

ISSN: 1941-6679-On-line Copy

.

supremacy," where we could perform tasks with controlled quantum systems going beyond what could be achieved with ordinary digital computers (Preskill, 2012). However, IBM claimed that Google's quantum computer did not reach quantum supremacy because the same task could be done with an ideal algorithm on a classical computer in 2.5 days (Pednault, Gunnels, Maslov, & Gambetta, 2019).

Intel, Rigetti, and IonQ also have been developing a quantum computer in their laboratories (Gomes, 2018). Microsoft has released the quantum development kit (QDK) and the quantum programming toolkit Q# for Visual Studio ("Quantum Development Kit | Microsoft," 2019), which allows users to simulate quantum circuits on a classical computer. Microsoft also started Azure Quantum, which provides Internet cloud access to their quantum computer simulators and the real quantum hardware supplied by Honeywell, IonQ, and QCI. Similarly, Amazon started a quantum computing service via AWS, called Amazon Braket, where users can remotely use the quantum computer hardware of the partners: D-wave, IonQ, and Rigetti.

Although everyone in business may not need a quantum computer for their tasks, many business applications can be improved by quantum computing, as mentioned above ((Bo) Ewald, 2019; Chalmers Brown, 2018; Cusumano, 2018; "D-Wave: Quantum Computing Applications," 2019; Robert Hackett, 2019). It seems that the time has come for researchers who are not necessarily physicists to design new business applications for quantum computers and communications.

This paper introduces the basic concepts of quantum computing, particularly for a general-purpose gate-based quantum computer, and describes the well-researched applications of quantum computing for non-experts. The next section provides the fundamentals of quantum computing. Section 3 describes three applications: Glover's quantum search algorithm, Shor's quantum integer factoring algorithm, and Quantum key distribution protocol. In section 4, a brief survey of the current status and research challenges in quantum computing is presented.

PRINCIPLES OF QUANTUM COMPUTING

Qubit

Computation is a process of manipulating the states of a physical system to solve a problem. Quantum computing uses a microscopic object (e.g., electron, photon, ion) as the medium to store and transfer digital information. One-bit information (i.e., zero or one) can be encoded using two orthogonal states of a microscopic object. This quantum two-state system is called a quantum bit (or qubit). A quantum computer solves a problem by setting qubits in initial states and then manipulating the states so that an expected result appears on the qubits. In order to

ISSN: 1941-6679-On-line Copy

.

design such a quantum circuit, quantum mechanics is used to describe the states since those microscopic objects do not follow the rules of classical physics. The state of a qubit can be written as a vector $|\psi\rangle$.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \{\alpha, \beta \in \mathbb{C}\} \quad (1)$$

where α and β are complex numbers $\mathbb{C}$, called probability amplitude, and satisfy $|\alpha|^2 + |\beta|^2 = 1$. $|\alpha|^2$ is the probability of getting the state $|0\rangle$ as the result of the measurement on the qubit $|\psi\rangle$ while $|\beta\rangle^2$ is the probability of getting $|1\rangle$. "$|\ \rangle$" is a standard notation for specifying states in quantum mechanics, called column vector or ket vector in the Dirac notation. The orthonormal basis $|0\rangle$ and $|1\rangle$ can be written as

$$|0\rangle = [1,0]^{\mathrm{T}}, \qquad |1\rangle = [0,1]^{\mathrm{T}} \quad (2)$$

Quantum states combine through the tensor product. For instance, two qubits state can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$, where "$\otimes$" indicates a tensor product, or more compactly $|\psi_1\rangle|\psi_2\rangle$ or $|\psi_1\psi_2\rangle$. For example,

$$\begin{aligned} |\psi_1\rangle \otimes |\psi_2\rangle &= \left[\psi_{1,0}, \psi_{1,1}\right]^T \otimes \left[\psi_{2,0}, \psi_{2,1}\right]^T \\ &= [\psi_{1,0}\psi_{2,0}, \psi_{1,0}\psi_{2,1}, \psi_{1,1}\psi_{2,0}, \psi_{1,1}\psi_{2,1}]^T \end{aligned} \quad (3)$$

where $|\psi_i\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha[1,0]^T + \beta[0,1]^T = [\alpha, \beta]^T = [\psi_{i,0}, \psi_{i,1}]^T$.

Thus, an n-qubit state can be represented by a column vector with 2^n elements.

Superposition State

Superposition State is an essential ingredient of quantum computing. In this section, a photon is used as an example of a qubit for the sake of ease. The polarization (i.e., the geometric orientation of the photon) represents one-bit information. A horizontally polarized photon represents classical bit 0, and a vertically polarized photon represents bit 1. In Figure 1, photons are fired at the emitter and going through the Filter-V, which allows only vertically polarized photons to go through. We assume only a single photon goes into Polarization Beam Splitter (PBS) at a time to make the example simpler. PBS transmits vertically polarized photons (measured at the detector DV) while the PBS deflects horizontally polarized photons (measured at the detector DH). Thus, all photons will be measured at DV in Figure 1.

.

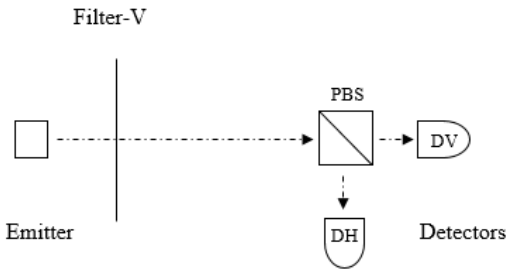

Figure 1: All photons are detected at DV

If a filter that only transmits diagonally polarized photons called "Filter-45°", however, is placed between Filter-V and PBS (Figure 2), a vertically or horizontally polarized photon is found at each detector with the probability of ½.

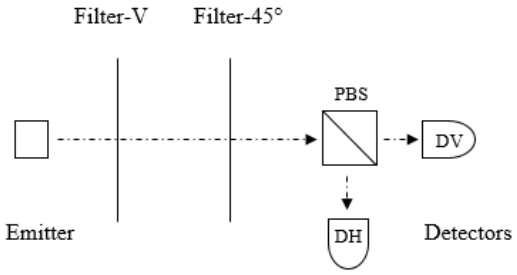

Figure 2: The half of photons are found at DV, and the rest are at DH

Since the probability of finding the horizontally polarized photon $|\psi\rangle = |H\rangle$ or vertically polarized photon $|\psi\rangle = |V\rangle$ at the PBS is ½, the probability amplitudes α and β should be $1/\sqrt{2}$. Thus, the state of a photon just before PBS can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle \tag{4}$$

Since $|\mathrm{H}\rangle$ is used to represent a classical bit "0" and $|\mathrm{V}\rangle$ is used for "1", the expression (4) is written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{5}$$

When a photon is prepared in this state, the digital information encoded in the photon is "0" or "1". We can interpret the equation (5) as meaning the states "0" and "1" exist at the same time. This unique state is called a *superposition state.* When two qubits are both in the superposition state (5), the state can be written as

.

$$
\begin{aligned}
|\psi_1\rangle|\psi_2\rangle &= \left\{\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\right\}\left\{\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\right\} \\
&= \frac{1}{2}\{[1,1]^T \otimes [1,1]^T\} = \frac{1}{2}[1,1,1,1]^T \\
&= \frac{1}{2}\{[1,0,0,0]^T + [0,1,0,0]^T + [0,0,1,0]^T + [0,0,0,1]^T\} \\
&= \frac{1}{2}|0\rangle|0\rangle + \frac{1}{2}|0\rangle|1\rangle + \frac{1}{2}|1\rangle|0\rangle + \frac{1}{2}|1\rangle|1\rangle \qquad (6)
\end{aligned}
$$

This two-qubit state represents four classical binary states (00, 01, 10, 11) at the same time. When a quantum computer prepares *n* qubits in a superposition state as its input for a quantum circuit (Figure 3), 2^n possible inputs can be processed simultaneously. This quantum parallelism is one of the significant advantages of quantum computers.

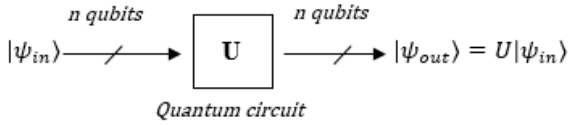

Figure 3: n-qubit quantum circuit

Quantum Circuit and Measurement

As mentioned earlier, computation is a process of manipulating the states of a physical system. A quantum computer takes a quantum state as the input and controls the state to increase the probability of finding the answer in the output state for the computation. For instance, Shor's algorithm manipulates the quantum states to find prime factors of a large number. A significant difference between a classical (electronic) circuit and a quantum circuit is the intermediate states in the circuits. In a classical electronic circuit, we can measure the intermediate state since zero and one in binary is represented by the voltages (e.g., 0 volts and 5 volts) on a node in the circuit. Thus, it is possible to find an error (e.g., 2.5 volts) by measuring the voltage in the circuit. However, in a quantum circuit, the intermediate states are likely to be in a superposition state. If the superposition state is measured, the quantum state is corrupted and becomes one of the two orthogonal base states (i.e., $|0\rangle$ or $|1\rangle$) at the time of the measurement with the probabilities $|\alpha|^2$ and $|\beta\rangle^2$.
For example, when the photons in the equation (6) are measured, one of the four states (e.g., $|\psi_1\rangle|\psi_2\rangle = |0\rangle|1\rangle$) is observed with an equal probability (i.e., $1/4,$) but all other information about the original state (6) are lost by the measurement. In other words, the measurement is a one-way operation that does not allow us to

.

find the original state from the measured result similar to classical one-way function (e.g., hash.)

Quantum Gate and Reversibility

The basic operations to manipulate an input state for a quantum circuit is called quantum gates. Each gate operation can be mathematically represented with a matrix. For instance, the Filter-45° in Figure 2 converts from one of the orthogonal base states (i.e., $|0\rangle$) to a superposition state (i.e., $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.) This operation can be expressed with the following matrix U_H, called Hadamard gate (Nielsen & Chuang, 2010).

$$U_H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (7)$$

Another example of the quantum gate is the controlled-NOT (cNOT) gate (Figure 4), which behaves like a classical XOR gate, as shown in Table 1.

Table 1: A truth table for the quantum XOR gate with two inputs and two outputs

ψ_{in1}	ψ_{in2}	ψ_{out1}	ψ_{out2}
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

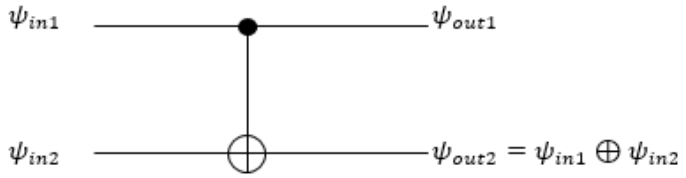

Figure 4: Controlled-Not gate behaves like a classical XOR

This quantum gate negates the state of the second qubit $|\psi_{in2}\rangle$ only when the first qubit $|\psi_{in1}\rangle$ is $|1\rangle$ while $|\psi_{in1}\rangle$ itself is unchanged by the gate (i.e., $|\psi_{in1}\rangle = |\psi_{out1}\rangle$). This operation can be written as:

.

$$|\psi_{out1}\rangle|\psi_{out2}\rangle = U_{cNOT}|\psi_{in1}\rangle|\psi_{in2}\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}\psi_{1,0}\psi_{2,0}\\ \psi_{1,0}\psi_{2,1}\\ \psi_{1,1}\psi_{2,0}\\ \psi_{1,1}\psi_{2,1}\end{bmatrix} = \begin{bmatrix}\psi_{1,0}\psi_{2,0}\\ \psi_{1,0}\psi_{2,1}\\ \psi_{1,1}\psi_{2,1}\\ \psi_{1,1}\psi_{2,0}\end{bmatrix} (8)$$

If we can construct a NAND gate with quantum gates, any logic gate (e.g., AND, OR, NOT) can be built since the NAND gate is universal (Mano, 1995). The classical NAND gate's truth table is given in Table 2.

Table 2: A truth table for the classical NAND gate with two inputs

IN_1	IN_2	Out
0	0	1
0	1	1
1	0	1
1	1	0

If the NAND gate is built based on the truth table above and the inputs are two qubits $|0\rangle|1\rangle = [1,0]^{\mathrm{T}} \otimes [0,1]^{\mathrm{T}} = [0,1,0,0]^{\mathrm{T}}$, the operation can be written as following (Yanofsky & Mannucci, 2008),

$$NAND: \begin{bmatrix}0 & 0 & 0 & 1\\ 1 & 1 & 1 & 0\end{bmatrix} \quad (9)$$

$$U_{NAND}|0\rangle|1\rangle = \begin{bmatrix}0 & 0 & 0 & 1\\ 1 & 1 & 1 & 0\end{bmatrix}[0,1,0,0]^T = [0,1]^T = |1\rangle \quad (10)$$

However, this NAND gate cannot be realized with quantum gates because two-bit information before the gate becomes one bit after the gate in (10). Quantum mechanics does not allow the system (e.g., quantum circuit) to lose information unless the quantum states in the system are measured. Therefore, quantum gates must have the same number of inputs as the outputs and must be *reversible* with no information loss by the gates. In contrast, classical gates except NOT gate are one-way functions and lose some of the input information at the exit of the gate. This requirement is another significant difference from classical computing.

Table 3: Truth table for Quantum NAND gate

ψ_{in1}	ψ_{in2}	ψ_{in3}	ψ_{out1}	ψ_{out2}	ψ_{out3}
0	0	1	0	0	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

.

A quantum NAND gate can be made of a *Toffoli* gate, also known as the controlled-controlled-NOT (ccNOT) gate (Figure 5, Table 4). The revised truth table for the quantum NAND gate is given in Table 3.

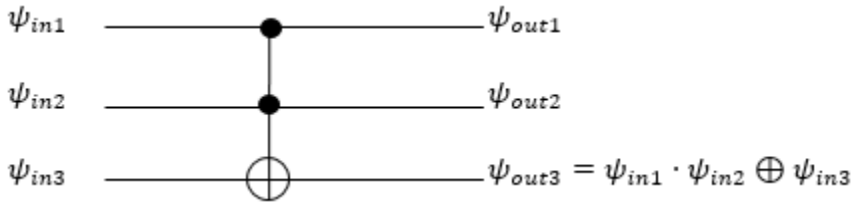

Figure 5: Controlled-Controlled-NOT (*Toffoli* gate)

Table 4: Truth table for Controlled-Controlled-NOT

ψ_{in1}	ψ_{in2}	ψ_{in3}	ψ_{out1}	ψ_{out2}	ψ_{out3}
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

When the Toffoli gate with $\psi_{in3} = 1$, the *ccNOT* gate works as a NAND gate.

$$\psi_{out3} = \neg(\psi_{in1} \wedge \psi_{in2}) \tag{11}$$

Thus, we can build any digital logic with the quantum gates theoretically.

No-Cloning Theorem and Entangled State

When ψ_{in2} is zero in Table 1, the *cNOT* gate keeps the ψ_{out2} to be zero for $\psi_{in1} = 0$ and changes ψ_{out2} to be one for $\psi_{in1} = 1$. Thus, it seems that *cNOT* gate copies the classical bit information in ψ_{in1} to ψ_{out2} when $\psi_{in2} = 0$.

$$\begin{aligned} |\psi_{out1}\rangle|\psi_{out2}\rangle &= cNOT|0\rangle|0\rangle = |0\rangle|0\rangle \\ |\psi_{out1}\rangle|\psi_{out2}\rangle &= cNOT|1\rangle|0\rangle = |1\rangle|1\rangle \end{aligned} \tag{12}$$

If *cNOT* gate can copy an arbitrary state in a qubit to the other qubit, it should be valid for a superposition state. When the input ψ_{in1} is $\alpha|0\rangle + \beta|1\rangle$, the output ψ_{out2} should be $\alpha|0\rangle + \beta|1\rangle$.

.

$$|\psi_{out1}\rangle|\psi_{out2}\rangle = \text{cNOT}(\alpha|0\rangle + \beta|1\rangle)|0\rangle$$
$$\longrightarrow (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$
$$= \alpha^2|0\rangle|0\rangle + \alpha\beta|1\rangle|0\rangle + \beta\alpha|0\rangle|1\rangle + \beta^2|1\rangle|1\rangle \quad (13)$$

However, from (12), the output from the *cNOT* gate for the superposition state turns out to be $\alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$.

$$|\psi_{out1}\rangle|\psi_{out2}\rangle = cNOT(\alpha|0\rangle + \beta|1\rangle)|0\rangle$$
$$= cNOT(\alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle)$$
$$= \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \quad (14)$$

Obviously, the equation (13) is not equal to (14). In quantum mechanics, the replication of an arbitrary quantum state is not possible. This restriction is known as the ***no-cloning theorem*** (Nielsen & Chuang, 2010; Wootters & Zurek, 1982). Even if *cNOT* gate seems to copy the classical bit information in $|\psi_{in1}\rangle$ to $|\psi_{out2}\rangle$, this is not a classical meaning of "copy". The results in (12) are the special cases for $\alpha = 1$ or $\beta = 1$ ($|\alpha|^2 + |\beta|^2 = 1$).

Also, the resulting states in (14) is quite impressive. The equation says, when we observe zero in ψ_{out1} by measurement, we know ψ_{out2} is also zero with no additional measurement. Similarly, when we find one in ψ_{out1}, we know ψ_{out2} is also one without measuring ψ_{out2}. In other words, the quantum state in ψ_{out2} depends on the value observed in $|\psi_{out1}\rangle$. Thus, the outputs ψ_{out1} and ψ_{out2} cannot be described independently. This bizarre states, where the individual states of qubits are intimately related to one another, is called the ***entangled state***. There is no way to express the entangled states as separable states like the expression $|\psi_{out1}\rangle = (\alpha|0\rangle + \beta|1\rangle)$ and $|\psi_{out2}\rangle = (\alpha|0\rangle + \beta|1\rangle)$ in (13). The use of entangled states is another essential ingredient of quantum computing.

APPLICATIONS

Quantum Computations

As mentioned earlier, one of the significant advantages of quantum computation is the ability of massively parallel computation. By using a quantum superposition state, 2^n inputs can be stored in *n* qubits simultaneously. Since universal quantum gates allow us to design an arbitrary quantum circuit, the *n* qubits can be used as the input for a quantum circuit, which performs an arbitrary computation.

.

For example, four classical values {0, 1, 2, and 3} can be stored in two qubits simultaneously, which can be written as the state (6). For example, a circuit can be designed to compute $f(x) = x + 5$. It seems that four computations can be performed with only one step by placing the qubits in the superposition states in the circuit. However, the output state is a superposition state of four possible output values {5, 6, 7, and 8}. The result of the measurement on the output qubits is one of the four possible outputs. In short, when a classical logic is implemented as a quantum circuit, the output qubits are the superposition of 2^n outputs for 2^n inputs.

The measurement result is one of 2^n possible output states with the probability $1/2^n$. Therefore, a quantum circuit needs to be designed to manipulate the probability amplitudes of the qubits so that an expected result can be found by the measurement with the probability higher than $1/2^n$. In this section, two well-known quantum algorithms that significantly outperform classical algorithms are introduced.

Grover's algorithm

This database search algorithm is designed to find an item in an unordered list. For example, it can be used for speeding up brute force key search on symmetric key encryption such as AES (Bernstein, 2010). It is known that this algorithm requires $O(\sqrt{N})$ operations to search an unsorted array of size *N*, which requires $O(N)$ operations for classical algorithms (Grover, 1996).

The idea of Grover's algorithm is the following. When the number x_a that satisfies $f(x_a) = 1$ needs to be found in a large unsorted database, the qubits are set to be in a superposition state of all possible ID numbers $\{x = 0,1,2, \dots, N-1\}$ as the initial state. To simplify the expression, the decimal notation is used for *n*-qubit. For example,$|1\rangle|0\rangle|0\rangle$ is written as $|4\rangle$. The initial state (Figure 6) can be written as

$$|\psi\rangle = \sum_{x=0}^{N-1} \rho_x |x\rangle = \rho_0|0\rangle + \rho_1|1\rangle + \rho_2|2\rangle + \cdots \rho_{N-1}|N-1\rangle \qquad (15)$$

where the initial values of ρ_x are $1/\sqrt{2^n}$ when $N = 2^n$. Thus, $\sum_{x=0}^{N-1} \rho_x^2 = 1$.

ISSN: 1941-6679-On-line Copy

.

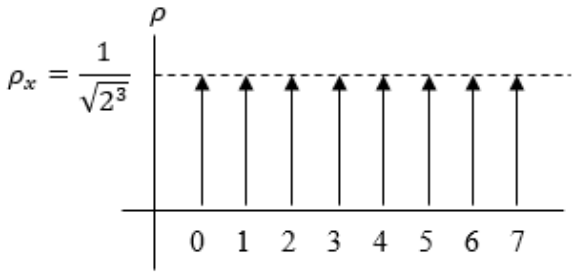

Figure 6: Initial States for N = 8 (n = 3)

Next, a quantum circuit is used to flip the phase of the state where x is equal to x_a (Figure 7).

$$|\psi'\rangle = (-1)^{f(x)} \sum_{x=0}^{N-1} \rho_x |x\rangle$$
$$= \rho_0|0\rangle + \rho_1|1\rangle + \cdots + (-1)\rho_{x_a}|x_a\rangle + \cdots + \rho_{N-1}|N-1\rangle \qquad (16)$$

where $f(x) = \begin{cases} 0 & x \neq x_a \\ 1 & x = x_a \end{cases}$.

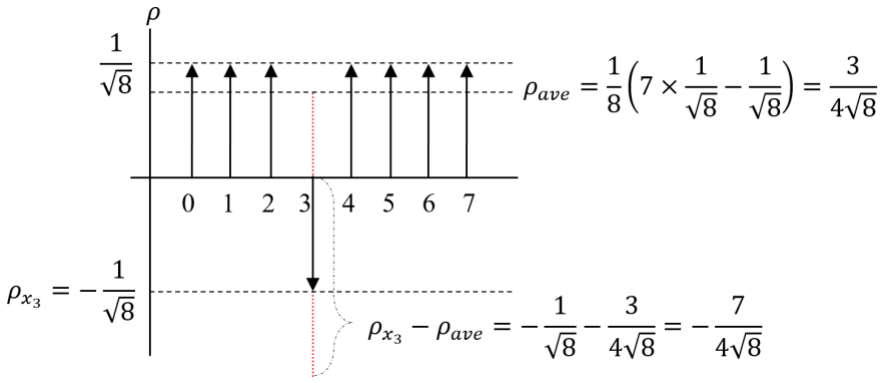

Figure 7: Flip the phase of the state x_a for N = 8 (n = 3), *assuming $f(x_a = 3) = 1$ in this example*

Then, the difference between the average of the probability amplitudes ρ_{ave} and the amplitude ρ_x is subtracted from the amplitude ρ_{ave} (Figure 8)

$$|\psi''\rangle = \sum_{x=0}^{N-1} \{\rho_{ave} - (\rho_x - \rho_{ave})\}|x\rangle = \sum_{x=0}^{N-1} (2\rho_{ave} - \rho_x)|x\rangle \qquad (17)$$

where $\rho_{ave} = \frac{1}{N}\sum_{x=0}^{N-1} \rho_x$.

.

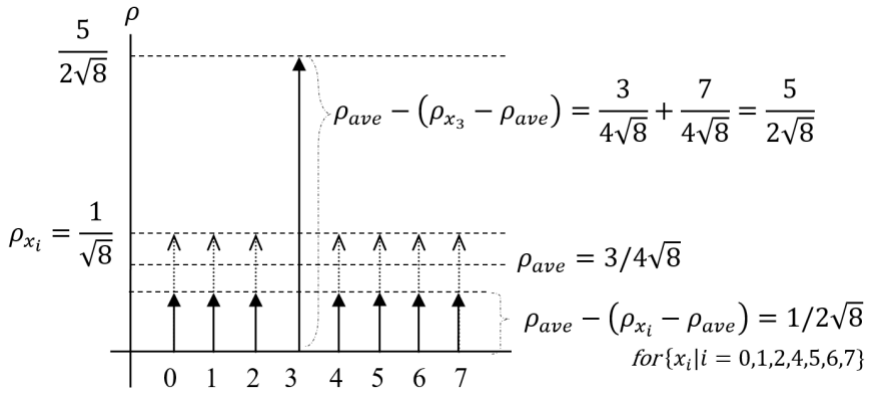

Figure 8: Difference between ρ_{ave} and ρ_x is subtracted from ρ_{ave} for N = 8 (n = 3)

This operation is called *inversion about the average.* As shown in the example with N = 8 (n = 3), the probability amplitude of the target state $|3\rangle$ goes up to $5/2\sqrt{8}$ from $1/\sqrt{8}$ after the operation, while the amplitudes for the rest of the states is reduced to $1/2\sqrt{8}$. This result still satisfies $\sum_{x=0}^{N-1} \rho_x^2 = \left(5/2\sqrt{8}\right)^2 + 7 \times \left(1/2\sqrt{8}\right)^2 = 1$. Thus, the probability of finding the target state $|3\rangle$ by measurement is increased from 12.5% to 78.1%. If the operation is repeated one more time, $\rho_{ave} = 1/8\sqrt{8}$ and $2\rho_{ave} - \rho_{x_3} = 11/4\sqrt{8}$. Thus, the probability $\left(2\rho_{ave} - \rho_{x_3}\right)^2$ is increased to 94.5%.

By performing *inversion about the average* multiple times, the probability of yielding the targeted ID x_a by measurement can be boosted from the initial probability of $1/N$. Since finding an item from N items takes $N/2$ operations on average, when N is small, the quantum algorithm does not substantially exceed the performance of classical algorithms.

$$O\left(\sqrt{N}\right) < O(N/2) \tag{18}$$

However, when N is large, the advantage is quite distinct. For example, when a database has 10^6 items (e.g., for biometric authentications), Grover's algorithm only needs 1000 steps to search an item while a classical algorithm needs 50,000 steps (Morsch, 2008).

.

Shor's Algorithm

In 1994, Peter Shor showed that a quantum computer could be used to factor a large integer in polynomial time (Shor, 1994). His algorithm attracted a great deal of attention from security agencies since, if a quantum computer is developed, it can break the RSA encryption algorithms (Van Meter & Horsman, 2013), which is the most widely used public-key encryption algorithm.
Shor's algorithm consists of classical parts and quantum parts. This section explains how quantum computation is utilized with the classical computation in Shor's algorithm after the RSA algorithm is briefly introduced.

Summary of the RSA encryption algorithm

A receiver of a secret message, Alice, chooses two large prime numbers (p, q) and computes $N = pq$. Also, she randomly chooses a number e, which is coprime to $(p-1)(q-1)$. (i.e., $\gcd\{e, (p-1)(q-1)\} \equiv 1$) and finds the number d, which satisfies

$$ed \equiv 1 \; mod\{(p-1)(q-1)\} \tag{19}$$

She makes those two numbers (N, e) available as her public key and keeps the number d as her private key. To encrypt a message M, a sender, Bob, computes $C = M^e \; mod \; N$. For decryption, Alice computes $M = C^d mod \; N$.
In order to break the security of the RSA, the eavesdropper, Eve, needs to find the private key d. Since N and e are in public, all she has to do is to find p and q from N to compute (19). However, there is no classical algorithm that can factor a large integer in polynomial time. The security of the RSA encryption relies on the difficulty of factoring a large integer (e.g., 200 digits)(Schneier, 1996).

Classical computations in Shor's algorithm

According to the number theory (Stallings, 1999), if a randomly chosen integer a that satisfies $0 < a < N$, is coprime to N, the function

$$f_{a,N}(m) = a^m \; mod \; N \tag{20}$$

is periodic and there is at least one integer m that satisfies the condition

$$a^m \equiv 1 \; mod \; N \tag{21}$$

For example, when $a = 7$ and $N = 15$,

$$f_{7,15}(1) = 7^1 \; mod \; 15 = 7$$
$$f_{7,15}(2) = 7^2 \; mod \; 15 = 4$$

ISSN: 1941-6679-On-line Copy

.

$$\begin{aligned} f_{7,15}(3) &= 7^3 \; mod \; 15 = 13 \\ f_{7,15}(4) &= 7^4 \; mod \; 15 = 1 \\ f_{7,15}(5) &= 7^5 \; mod \; 15 = 7 \\ f_{7,15}(6) &= 7^6 \; mod \; 15 = 4 \\ f_{7,15}(7) &= 7^7 \; mod \; 15 = 13 \end{aligned} \tag{22}$$

Therefore, when $m = 4,8,12, \ldots$, the function $f_{7,15}(m)$ is equal to 1. The least positive exponent is the length of the period generated by $f_{a,N}(m)$. In this example, the period *r* is 4.

The condition (21) can be revised by subtracting one from both sides of the equivalence.

$$a^r - 1 \equiv 0 \; mod \; N \tag{23}$$

When the period *r* is an even number,

$$\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) \equiv 0 \; mod \; N \tag{24}$$

Thus, when the integer N is a divisor of $\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right)$, the remainder is zero. There is a good chance that one of two factors $\left(a^{r/2} - 1\right)$ or $(a^{r/2} + 1)$ is a factor for N. By using the classical Euclidean algorithm, a factor for N can be found with $gcd\,\{a^{r/2} - 1, N\}$ and $gcd\,\{a^{r/2} + 1, N\}$ except for the case where $a^{r/2} = \pm 1 \; mod \; N$. In the example, when $m = 4$, the factors 3 and 5 for $N = 15$ can be found calculating $gcd\{7^2 - 1, 15\} = gcd\{48, 15\} = 3$ and $gcd\{7^2 + 1, 15\} = gcd\{50, 15\} = 5$.

Quantum computations in Shor's algorithm

When the integer *N* is large (e.g., 200 digits), finding the period of $f_{a,N}(m)$ is very time-consuming with a classical computer (if possible.) Thus, a quantum superposition state is used to find the period by computing $f_{a,N}(m)$ for $m = 0$ to, at least, $m = N^2$.

In Grover's algorithm, only one set of qubits in the superposition state is manipulated to increase the probability of finding the targeted index by measurement on the qubits. In Shor's algorithm, two sets of qubits are used: $|\psi_1\rangle$ for the input *m* and $|\psi_2\rangle$ for the output of $f_{a,N}(m)$ in (20). The number of qubits for $|\psi_2\rangle$ is $k = \log N$ since $f_{a,N}(m)$ is always less than N while the number of qubits for $|\psi_1\rangle$ is, at least, $\log N^2 = 2k$ (Yanofsky & Mannucci, 2008). Similar to (15), the initial state of the qubits for *m* is

$$|\psi_1\rangle = \sum_{m=0}^{N^2-1} \rho_m |m\rangle = \rho_0|0\rangle + \rho_1|1\rangle + \rho_2|2\rangle + \cdots + \rho_{N^2-1}|N^2 - 1\rangle \tag{25}$$

ISSN: 1941-6679-On-line Copy

.

where the initial values of ρ_m are $1/\sqrt{2^{2k}}$. The initial state of the qubits for $f_{a,N}(m)$ is

$$|\psi_2\rangle = |000\ldots0\rangle = |0\rangle \tag{26}$$

$|\psi_1\rangle$ and $|\psi_2\rangle$ are placed into a quantum circuit which computes $f_{a,N}(m)$ as shown in Figure 9.

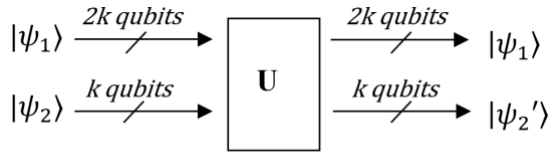

Figure 9: Quantum Computation in Shor's algorithm

The output states from the quantum circuit can be written as

$$U|\psi_1\rangle|\psi_2\rangle = U|m\rangle|0\rangle = |m\rangle\left|f_{a,N}(m)\right\rangle = |\psi_1\rangle|\psi_2'\rangle \tag{27}$$

$|\psi_1\rangle$ and $|\psi_2'\rangle$ are entangled. For example, in the case with $a = 7$ and $N = 15$ ($k = 4$), by using the result of (22), $|\psi_1\rangle|\psi_2'\rangle$ is written as

$$|\psi_1\rangle|\psi_2'\rangle = \frac{1}{\sqrt{256}}\left(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + \cdots + |254\rangle|1\rangle + |255\rangle|7\rangle\right) \tag{28}$$

Obviously, $|\psi_1\rangle$ and $|\psi_2'\rangle$ cannot be expressed as a separable state like their initial states.

When the second set of qubits $|\psi_2'\rangle$ is measured, the superposition state of $|\psi_2'\rangle$ is corrupted and one of four states (i.e., $\psi_2 = 1,7,4,13$) is observed on $|\psi_2'\rangle$. But, the first set of qubits $|\psi_1\rangle$ is still in a superposition state. When 4 is yielded by the measurement on $|\psi_2\rangle$, the state (28) will be

$$\begin{aligned}|\psi_1\rangle|\psi_2'\rangle &= \frac{1}{\sqrt{64}}\left(|2\rangle|4\rangle + |6\rangle|4\rangle + |10\rangle|4\rangle + \cdots + |254\rangle|4\rangle\right) \\ &= \frac{1}{\sqrt{64}}\left(|2\rangle + |6\rangle + |10\rangle + \cdots + |254\rangle\right)|4\rangle \end{aligned} \tag{29}$$

Thus, the period r of $f_{a,N}(m)$ can be observed as the distance Δt between successive possible states of $|\psi_1\rangle$ in Figure 10.

.

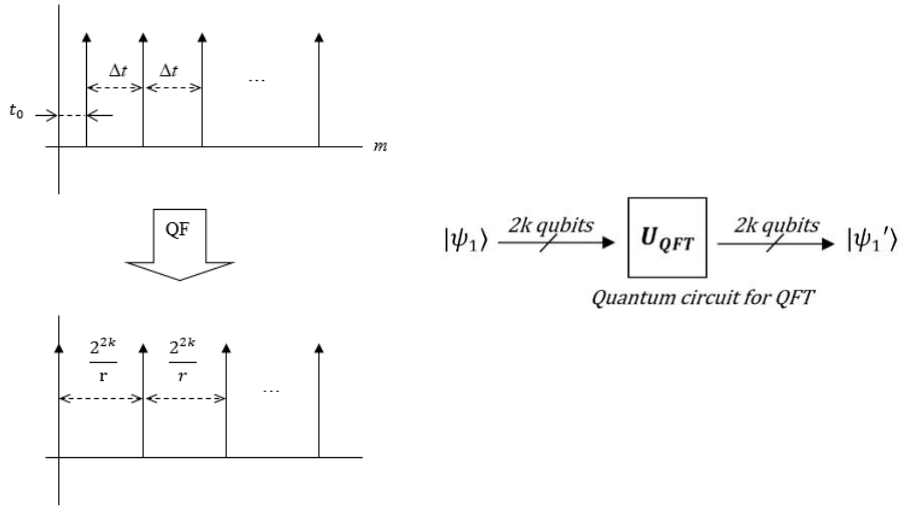

Figure 10: Discrete Fourier Transform

A simple measurement on $|\psi_1\rangle$ is not useful to find r since the measurement result is $m = l\Delta t + t_0$ (where t_0 is unknown and $l = 0,1,2,3, \ldots$). The offset t_0 needs to be eliminated before the measurement. A quantum circuit for Discrete Fourier Transform for qubits, called quantum Fourier Transform (QFT), is designed to eliminate the offset in $|\psi_1\rangle$ and to convert Δt to $2^{2k}/r$. After the QFT operation, the measurement on the state $|\psi_1{}'\rangle$ yields a number $c = j[2^{2k}/r]$ $(j = 1,2,3, \ldots)$. Since 2^{2k} is known, the result value c can be divided by 2^{2k}.

$$\frac{c}{2^{2k}} = \frac{j}{r} \tag{30}$$

By using the continued fraction expansion, the closest rational to j/r can be found (Rieffel & Polak, 2000; Williams & Clearwater, 1998). By repeating this quantum operation several times, the period r can be found.

Summary of Shor's algorithm

To factor a large integer N,

1. Randomly choose integer a that satisfies both $0 < a < N$ and $\gcd\{a, N\} = 1$.
2. Find the period r for $a^m mod\ N$ ($0 < m < N^2$) by using the quantum computation with the classical continued fraction expansion.
3. When r is an even number, compute $gcd\ \{a^{r/2} - 1, N\}$ and $gcd\ \{a^{r/2} + 1, N\}$.
    a. If r is an odd number, repeat steps 1 and 2.
4. Check if one of the results from step 3 is the factor of *N*. If not, repeat all steps.

ISSN: 1941-6679-On-line Copy

.

Quantum Key Distribution

Quantum cryptography (Gisin, Ribordy, Tittel, & Zbinden, 2002) is currently one of the most practical applications of quantum information science. The most well-known quantum cryptography is the quantum key distribution (QKD) protocol (Bennett & Brassard, 1984), which has been implemented and commercially available for more than a decade. The OKD with the *one-time pad* can provide theoretically unbreakable end-to-end security by utilizing quantum mechanical properties in a classical cryptographic protocol. Here "unbreakable" means that the security of the cryptography does not rely on the complexity of the algorithm but a physical property that prevents decryptions without the key. The one-time pad is classical cryptography known to be a perfect encryption scheme (Schneier, 1996). The protocol is simple as follows. A sender, called Alice, generates *n*-bit random number *K* as a one-time shared key and delivers it to a receiver, called Bob, before the communication.

$$K = \{k_i = 0,1 \mid i = 1,2,3, \dots n\}$$

When Alice wants to deliver an *n*-bit secret message *M* to Bob, Alice performs exclusive OR operations for each bit in *M* and *K*, respectively. Then, she sends the resulting bit sequence *C* to Bob and discards the *K*.

$$M = \{m_i = 0,1 \mid i = 1,2,3, \dots, n\}$$

$$C = \{c_i = m_i \oplus k_i \mid i = 1,2,3, \dots, n\}$$

Bob decrypts the ciphertext *C* by performing exclusive OR operations with the shared key *K* and discards the *K*.

This is an entirely secure protocol. The random bit sequence added to the message produces an utterly random bit sequence. Since the key is used only once, there is no possible attack except making a guess of *n*-bit random bit sequence for an *n*-bit message. The problem with this method is that there is no perfectly secure way to deliver the key (i.e., *K*) to Bob prior to the communication. If classical cryptography such as RSA or AES was used, the strength of the one-time pad protocol relies on the strength of the classical cryptography, which is not a perfect encryption scheme. QKD plays a significant role in delivering the keys for the one-time pad. The first QKD was proposed by C.H. Bennett and G. Brassard in 1984, called BB84 protocol. BB84 uses photons to deliver a random sequence of bits, which will be used as a shared key between Alice and Bob after the completion of the protocol. We introduce the implementation of BB84 with the photon polarization in the following discussion to be consistent with the experiments introduced in section 2.

Figure 11 shows a simple BB84 example, which is very similar to Figure 1.

ISSN: 1941-6679-On-line Copy

.

The difference is that the polarization angles of Filters are variable.

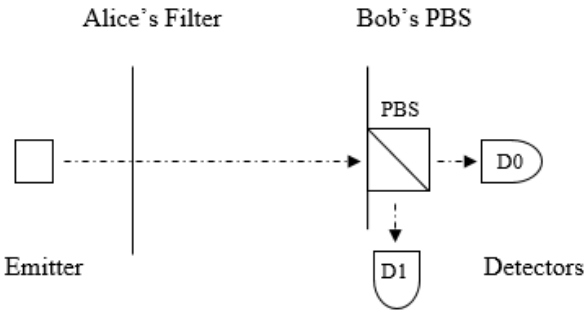

Figure 11: A simple BB84 example

Alice's filter can be set to four different angles: 0°, 45°, 90°, and 135° while Bob can change the orientation of the base angle (PBS) to 0° or 45° degrees (Figure 12).

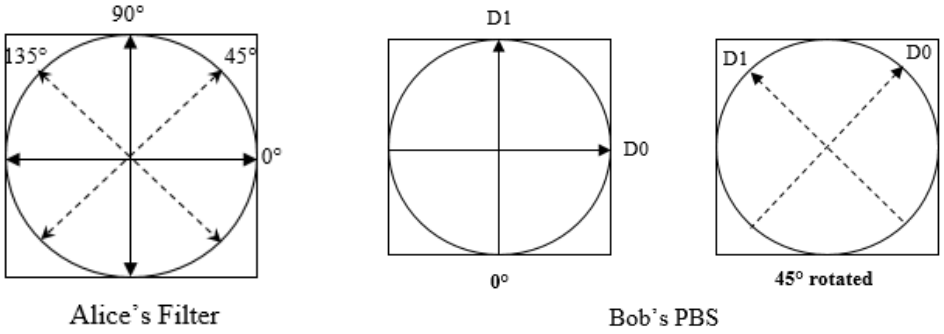

Figure 12: Alice's filter and Bob's filter angles

In the BB84 protocol,

1. Alice generates a *t*-bit random bit sequence, *R*.
$$R = \{r_i = 0,1 \mid i = 1,2,3, \dots t\}$$
2. Alice randomly chooses a horizontal-vertical base (H-V) or diagonal base (D) before she sends each photon. When Alice chooses a horizontal-vertical base and $r_i = 0$, Alice adjusts her filter to be 0° position so that a horizontally polarized photon is sent to Bob. When Alice chooses a horizontal-vertical base and $r_i = 1$, Alice adjusts her filter to be 90° position so that a vertically polarized photon is sent to Bob. Similarly, when Alice chooses the diagonal base and $r_i = 0$, Alice adjusts her filter to be 45° position so that a photon polarized by 45° is sent to Bob. When Alice chooses the diagonal base and $r_i = 1$, Alice adjusts her filter to be 135°

ISSN: 1941-6679-On-line Copy

position so that a photon polarized by 135° is sent to Bob.

3. Bob also independently chooses a horizontal-vertical base or diagonal base before he receives each photon at his PBS.
4. Once Alice has sent all *t* photons for *R* to Bob, Alice and Bob exchange the information about which base they chose for each transmission and reception over a public channel (e.g., telephone). Only those bits for their bases matched are kept as a shared bit sequence *K*. The result for each transition is shown in Table 5.

Table 5: Bob's measurement result for each of Alice's transmission

	Alice			Bob		
Chosen Base	Random Bit r_i	Rotation Angle	Photon State	Chosen Base	Photon State after PBS	Measured Result
Horizontal -Vertical (H-V)	0	0°	↔	H-V	↔	0
				D	⤢ or ⤡	?
	1	90°	↕	H-V	↕	1
				D	⤢ or ⤡	?
Diagonal (D)	0	45°	⤢	H-V	↔ or ↕	?
				D	⤢	0
	1	135°	⤡	H-V	↔ or ↕	?
				D	⤡	1

In the cases that Alice and Bob chose the same base by chance, Alice and Bob can share the same classical bit information. However, when Alice and Bob used different bases, the bit information is discarded because Bob's measurement result is not reliable.

For example, when Alice chooses D base and $r_i = 0$, the polarization is rotated by 45 degrees. Thus, by using a rotation operator, Jones matrix for a rotator (Saleh & Teich, 1991),

$$U_{R(\theta)} = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix} \tag{31}$$

the state of the photon can be written as

$$|\psi_i\rangle = U_{R(45°)}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \tag{32}$$

Similar to the example in Figure 2, if Bob chooses the H-V base, Bob obtains $|0\rangle$ or $|1\rangle$ with the probability $\frac{1}{2}$. When there is a 45-degree difference between the

.

rotation angle of Alice's photon and the orientation of Bob's base, Bob's measurement result is 0 or 1 with the probability of $\frac{1}{2}$.

The same rule is applied to the measurements by an eavesdropper, Eve. If Eve has the same equipment as Alice and Bob, she can intercept the photons from Alice and retransmit the same state of a photon to Bob. However, since Eve does not know which base she should use for the measurement, 25% of the measurement results are wrong. If Eve encodes new photons based on her measurement results and transmits them to Bob, the 25 % of Bob's measurement results are also incorrect. Thus, the existence of an eavesdropper significantly increases the error rate. Alice and Bob can detect Eve's attack by checking some bits in *K* to calculate the error rate. Although Eve may try to make copies of Alice's photon to avoid increasing errors, the *no-cloning theorem* forbids the replication of an arbitrary unknown quantum state.

CHALLENGES

Quantum Computer

As listed in "The European Quantum Technologies Roadmap" (Acín et al., 2018), many approaches to realize quantum commuters have been explored for decades, and some approaches have successfully demonstrated quantum operations. In 2001, the first implementation of Shor's algorithm (factorization of $15 = 3 \times 5$) was realized using nuclear magnetic resonance (NMR) (Vandersypen et al., 2001). The controlled-Not gate operations have been realized with trapped ions (Schmidt-Kaler et al., 2003), superconductors (Plantenberg, de Groot, Harmans, & Mooij, 2007), and optical systems (O'Brien, Pryde, White, Ralph, & Branning, 2003). As of 2019, the largest number of qubits tested in laboratories is 53-qubit on a superconducting based quantum computer. IBM has 20-qubit superconducting based commercial quantum computers. Google, IonQ, and Rigetti also have quantum computers in their laboratories.

Theoretically, if universal quantum gates are developed as hardware, any arbitrary quantum circuit can be designed. However, there are many technical challenges in building the hardware for gate-based quantum computation with a large number of qubits (DiVincenzo, 2000; Nielsen & Chuang, 2010). For example, whatever material chosen as a qubit must be robustly represented as a stable two-level system and must have a longer decoherence time than the gate operations. (Decoherence is the coupling between the qubit and its environment.) If the decoherence time is not enough for a gate operation, the output state from the gate is likely to have errors. Thus, each qubit (e.g., ion, electron) needs to be well isolated from its environment, including neighbor qubits. Quantum error correction (Calderbank & Shor, 1996)

ISSN: 1941-6679-On-line Copy

.

can correct some errors, but the error correction mechanism requires a lot of extra qubits to be managed. Also, the operations with the qubits need to be performed at cryogenic temperatures. This requires refrigeration technologies, which are scalable to quantum circuits with a few hundred qubits.

D-Wave's quantum computer uses superconducting flux qubit generated inside the circulating current in a loop acting as a quantum mechanical spin (Lupaşcu et al., 2007) and currently has about 2000 qubits (Gibney, 2017), but is not a general-purpose computer like the gate-based quantum computer. It uses quantum annealing (Kadowaki & Nishimori, 1998) to solve only specific types of problems, such as optimization problems. It has not been reported that D-wave's quantum computer can perform Shor's algorithm or Grover's algorithm with large numbers.

Quantum Key Distribution

QKD schemes have been implemented in free space (Hughes, Nordholt, Derkacs, & Peterson, 2002) and optical fiber (Gordon, Fernandez, Townsend, & Buller, 2004).

A QKD system with a phase encoding in a standard telecommunication optical fiber network was implemented (Gobby, Yuan, & Shields, 2004). In 2004, the first real bank transfer utilizing a QKD system took place (Poppe et al., 2004). In 2012, the QKD system over 260 km in standard telecom fiber was experimentally realized (Wang et al., 2012). In 2017, the free-space QKD system over 53 km in daylight was demonstrated (Liao et al., 2017). Also, several companies have been offering QKD commercial products for more than a decade ("ID Quantique," n.d.; "MagiQ Technologies.," n.d.). However, they have not been disseminated widely through the community of information security practitioners.

One of the significant issues with a QKD for the practitioners is that there is no commercially available quantum repeater to extend the distance and to fan out across a network. A photon is, by its nature, prone to interfere with its environment. It is not a critical problem for a short distance QKD scheme because the data transmitted over a quantum channel are random bits that can be discarded when they have errors. For long-distance, the amplification of the signal (i.e., a photon) is necessary due to the high SNR (signal to noise ratio). However, it is very challenging (if possible) to develop a quantum repeater (Meter & Touch, 2013) since replication of a transmitted unknown photon is not possible due to the *no-cloning theorem*. Although quantum repeaters have been proposed (Briegel, Dür, Cirac, & Zoller, 1998; Jiang et al., 2009; Meter & Touch, 2013; Zwerger, Dür, & Briegel, 2012; Zwerger, Pirker, Dunjko, Briegel, & Dür, 2017), current commercially available QKD systems are generally designed to be used with point-to-point dedicated connections between networks (Aleksic et al., 2015). Thus, the

.

application of the QKD is still limited to metropolitan area networks (W. Chen et al., 2009; Elliott et al., 2005; Sasaki et al., 2011; Stucki et al., 2011).
In 2018, the distribution of entangled photon pairs via a satellite was demonstrated. It enabled sharing the entangled photon pairs between two locations separated by more than 1200 km (Yin et al., 2017). The satellite system may be used for entanglement-based QKD (Ekert, 1991) and as a repeater station for QKD networks.
Another issue about QKD schemes is their security. The QKD schemes do not generally guarantee that the origin of the message is genuine. If an eavesdropper is capable of compromising both quantum and classical channels, the man-in-the-middle attack against QKD schemes is possible (Pacher et al., 2016; Svozil, 2005). Therefore, authentication functionalities need to be incorporated into QKD schemes, especially for multipoint connections.

CONCLUSION

In this paper, the fundamental principles used in the quantum computations and three well-known quantum applications were introduced. Quantum computing is a promising technology, which changes our lives in many ways. Quantum computer improves database search significantly and solves many optimization problems used in business such as data analytics (e.g., big data (Philip Chen & Zhang, 2014)), logistics (e.g., optimizing routes of 10,000 taxies (Cusumano, 2018)), and medical research (Parsons, 2011) while quantum computing can be a cybersecurity threat until we have post-quantum cryptography (cryptographic algorithms that are secure against the attacks by quantum computers (L. Chen et al., 2016; Mailloux, Lewis, Riggs, & Grimaila, 2016).)
After Shor's and Grover's algorithms were found, researchers have not found many useful quantum algorithms that substantially outperform classical algorithms. Shor states in his paper, "Any quantum algorithm offering a speed-up over classical computation must use interference; this phenomenon is unknown in classical computer science, and most theoretical computer scientists are not used to reasoning about it" (Shor & W., 2003). As researches in quantum computing get more attention from government, industry, and academia, more useful quantum algorithms are expected to be found.
Although it may take ten years to build a quantum computer that significantly outperforms classical computers, every business needs to think of new quantum applications to prepare for the day. As fortune 500 companies have kept investing in quantum computing, there must be chances to find a high grade of gold ore in this research and business fields.

ISSN: 1941-6679-On-line Copy

.

REFERENCE

(Bo) Ewald, R. H. (2019). An Introduction to Quantum Computing and Its Application. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 11413 LNCS, pp. 3–8). Springer Verlag. https://doi.org/10.1007/978-3-030-14082-3_1

Acín, A., Bloch, I., Buhrman, H., Calarco, T., Eichler, C., Eisert, J., … Wilhelm, F. K. (2018). The quantum technologies roadmap: a European community view. *New Journal of Physics*, *20*(8), 080201. https://doi.org/10.1088/1367-2630/aad1ea

Aleksic, S., Hipp, F., Winkler, D., Poppe, A., Schrenk, B., & Franzl, G. (2015). Perspectives and limitations of QKD integration in metropolitan area networks. *Optics Express*, *23*(8), 10359–10373. https://doi.org/10.1364/OE.23.010359

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Benioff, P. (1980). *The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines*. *Journal of Statistical Physics* (Vol. 22).

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *the IEEE International Conference on Computers, Systems and Signal Processing* (pp. 175–179). Bangalore, India: IEEE.

Bernstein, D. J. (2010). Grover vs. McEliece. In *Third International Workshop, PQCrypto 2010* (pp. 73–80). Darmstadt, Germany: Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-12929-2_6

Briegel, H.-J., Dür, W., Cirac, J. I., & Zoller, P. (1998). Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Physical Review Letters*, *81*(26), 5932–5935. https://doi.org/10.1103/PhysRevLett.81.5932

Calderbank, A. R., & Shor, P. W. (1996). Good quantum error-correcting codes exist. *Physical Review A*, *54*(2), 1098–1105. https://doi.org/10.1103/PhysRevA.54.1098

Chalmers Brown. (2018). Adding A Little Quantum Computing To Your Business. Retrieved June 27, 2019, from https://www.forbes.com/sites/forbestechcouncil/2018/04/13/adding-a-little-quantum-computing-to-your-business/#2256706e41cc

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-

.

Tone, D. (2016). *Report on Post-Quantum Cryptography*. Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8105

Chen, W., Han, Z. F., Zhang, T., Wen, H., Yin, Z. Q., Xu, F. X., … Guo, G. C. (2009). Field experiment on a "star type" metropolitan quantum key distribution network. *IEEE Photonics Technology Letters*. https://doi.org/10.1109/LPT.2009.2015058

Coles, P. J., Eidenbenz, S., Pakin, S., Adedoyin, A., Ambrosiano, J., Anisimov, P., … Zhu, W. (2018). Quantum Algorithm Implementations for Beginners.

Cusumano, M. A. (2018). The business of quantum computing. *Communications of the ACM*, *61*(10), 20–22. https://doi.org/10.1145/3267352

D-Wave: Quantum Computing Applications. (2019). Retrieved June 27, 2019, from https://www.dwavesys.com/quantum-computing/applications

DiVincenzo, D. P. (2000). The Physical Implementation of Quantum Computation. *Fortschritte Der Physik*, *48*(9–11), 771–783. https://doi.org/10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67*(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., & Yeh, H. (2005). Current status of the DARPA quantum network. In E. J. Donkor, A. R. Pirich, & H. E. Brandt (Eds.), *SPIE, Quantum Information and Computation III* (Vol. 5815, pp. 138–149). International Society for Optics and Photonics. https://doi.org/10.1117/12.606489

Feynman, R. P. (1982). *Simulating Physics with Computers*. *International Journal of Theoretical Physics* (Vol. 21).

Gibney, E. (2017). D-Wave upgrade: How scientists are using the world's most controversial quantum computer. *Nature*, *541*(7638), 447–448. https://doi.org/10.1038/541447b

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145

Gobby, C., Yuan, Z. L., & Shields, A. J. (2004). Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, *84*(19), 3762–3764. https://doi.org/10.1063/1.1738173

Gomes, L. (2018). Quantum computing: Both here and not here. *IEEE Spectrum*, *55*(4), 42–47. https://doi.org/10.1109/MSPEC.2018.8322045

Gordon, K. J., Fernandez, V., Townsend, P. D., & Buller, G. S. (2004). A short wavelength GigaHertz clocked fiber-optic quantum key distribution system. *IEEE Journal of Quantum Electronics*, *40*(7), 900–908. https://doi.org/10.1109/JQE.2004.830182

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search.

.

In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96* (pp. 212–219). Philadelphia, Pennsylvania: ACM. https://doi.org/10.1145/237814.237866

Hughes, R. J., Nordholt, J. E., Derkacs, D., & Peterson, C. G. (2002). Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, *4*(1), 43–43. https://doi.org/10.1088/1367-2630/4/1/343

IBM. (n.d.). IBM Q Experience. Retrieved June 27, 2019, from https://www.research.ibm.com/ibm-q/

IBM Unveils World's First Integrated Quantum Computing System for Commercial Use - Jan. 8, 2019. (2019). Retrieved June 27, 2019, from https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use

ID Quantique. (n.d.). Retrieved June 27, 2019, from https://www.idquantique.com/quantum-safe-security/products/

Jiang, L., Taylor, J. M., Nemoto, K., Munro, W. J., Van Meter, R., & Lukin, M. D. (2009). Quantum repeater with encoding. *Physical Review A*, *79*(3), 032325. https://doi.org/10.1103/PhysRevA.79.032325

Kadowaki, T., & Nishimori, H. (1998). Quantum annealing in the transverse Ising model. *Physical Review E - Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics*, *58*(5), 5355–5363. https://doi.org/10.1103/PhysRevE.58.5355

Liao, S.-K., Yong, H.-L., Liu, C., Shentu, G.-L., Li, D.-D., Lin, J., … Pan, J.-W. (2017). Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, *11*(8), 509–513. https://doi.org/10.1038/nphoton.2017.116

Lupaşcu, A., Saito, S., Picot, T., de Groot, P. C., Harmans, C. J. P. M., & Mooij, J. E. (2007). Quantum non-demolition measurement of a superconducting two-level system. *Nature Physics*, *3*(2), 119–123. https://doi.org/10.1038/nphys509

MagiQ Technologies. (n.d.). Retrieved June 27, 2019, from https://www.magiqtech.com/solutions/network-security/

Mailloux, L. O., Lewis, C. D., Riggs, C., & Grimaila, M. R. (2016). Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. *IT Professional*, *18*(5), 42–47. https://doi.org/10.1109/MITP.2016.77

Mano, M. M. (1995). *Digital Design, Second Edition*. Prentice Hall.

Meter, R., & Touch, J. (2013). Designing quantum repeater networks. *IEEE Communications Magazine*, *51*(8), 64–71. https://doi.org/10.1109/MCOM.2013.6576340

Montanaro, A. (2016). Quantum algorithms: an overview. *Npj Quantum Information*, *2*(1), 15023. https://doi.org/10.1038/npjqi.2015.23

.

Morsch, O. (2008). *Quantum bits and quantum secrets : how quantum physics is revolutionizing codes and computers*. Wiley-VCH.

National Aeronautics and Space Administration. (2015). Quantum Computer Project Accelerating Advanced Computing for NASA Missions. Retrieved January 27, 2020, from https://nas.nasa.gov/assets/pdf/Quantum_Computer_Fact_Sheet_Fall2015.pdf

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information* (10th Anniv). Cambridge University Press.

O'Brien, J. L., Pryde, G. J., White, A. G., Ralph, T. C., & Branning, D. (2003). Demonstration of an all-optical quantum controlled-NOT gate. *Nature*, *426*(6964), 264–267. https://doi.org/10.1038/nature02054

Pacher, C., Abidin, A., Lorünser, T., Peev, M., Ursin, R., Zeilinger, A., & Larsson, J.-Å. (2016). Attacks on quantum key distribution protocols that employ non-ITS authentication. *Quantum Information Processing*, *15*(1), 327–362. https://doi.org/10.1007/s11128-015-1160-4

Parsons, D. F. (2011). Possible medical and biomedical uses of quantum computing. *NeuroQuantology*, *9*(3), 596–600. https://doi.org/10.14704/nq.2011.9.3.412

Pednault, E., Gunnels, J., Maslov, D., & Gambetta, J. (2019). On "Quantum Supremacy." Retrieved January 25, 2020, from https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

Philip Chen, C. L., & Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences*, *275*, 314–347. https://doi.org/10.1016/J.INS.2014.01.015

Plantenberg, J. H., de Groot, P. C., Harmans, C. J. P. M., & Mooij, J. E. (2007). Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits. *Nature*, *447*(7146), 836–839. https://doi.org/10.1038/nature05896

Poppe, A., Fedrizzi, A., Ursin, R., Böhm, H. R., Lorünser, T., Maurhardt, O., … Zeilinger, A. (2004). Practical quantum key distribution with polarization entangled photons. *Optics Express*, *12*(16), 3865. https://doi.org/10.1364/OPEX.12.003865

Preskill, J. (2012). Quantum computing and the entanglement frontier. Retrieved from http://arxiv.org/abs/1203.5813

Quantum Development Kit | Microsoft. (2019). Retrieved June 27, 2019, from https://www.microsoft.com/en-us/quantum/development-kit

Rieffel, E., & Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, *32*(3), 300–335. Retrieved from http://doi.acm.org/10.1145/367701.367709

Robert Hackett. (2019). Big Businesses Racing to Use Quantum Computing to

.

Solve Big Problems | Fortune. Retrieved June 27, 2019, from http://fortune.com/longform/business-quantum-computing/

Saleh, B. E. A., & Teich, M. C. (1991). *Fundamentals of Photonics*. John Wiley & Sons, Inc. Retrieved from http://gautier.moreau.free.fr/cours_optique/introduction.pdf

Sara Castellanos. (2019). Quantum Computing Holds Promise for Banks, Executives Say 'You could argue that finance has got the shortest path to impact,' says Goldman's head of research-and-development engineering. Retrieved January 24, 2020, from https://www.wsj.com/articles/quantum-computing-holds-promise-for-banks-executives-say-11573230983

Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., … Zeilinger, A. (2011). Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express*, *19*(11), 10387. https://doi.org/10.1364/OE.19.010387

Schmidt-Kaler, F., Häffner, H., Riebe, M., Gulde, S., Lancaster, G. P. T., Deuschle, T., … Blatt, R. (2003). Realization of the Cirac–Zoller controlled-NOT quantum gate. *Nature*, *422*(6930), 408–411. https://doi.org/10.1038/nature01494

Schneier, B. (1996). *Applied cryptography : protocols, algorithms, and source code in C*. Wiley.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). Santa Fe, NM: IEEE. https://doi.org/10.1109/SFCS.1994.365700

Shor, P. W., & W., P. (2003). Why haven't more quantum algorithms been found? *Journal of the ACM*, *50*(1), 87–90. https://doi.org/10.1145/602382.602408

Stallings, W. (1999). *Cryptography and network security : principles and practice* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Stucki, D., Legré, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., … Zbinden, H. (2011). Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics*, *13*(12), 123001. https://doi.org/10.1088/1367-2630/13/12/123001

Svozil, K. (2005). Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography. *International Journal of Quantum Information*, *03*(04), 649–654. https://doi.org/10.1142/S0219749905001511

Van Meter, R., & Horsman, C. (2013). A blueprint for building a quantum computer. *Communications of the ACM*, *56*(10), 84–93. https://doi.org/10.1145/2494568

Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., & Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, *414*(6866),

.

883–887. https://doi.org/10.1038/414883a

Wang, S., Chen, W., Guo, J.-F., Yin, Z.-Q., Li, H.-W., Zhou, Z., … Han, Z.-F. (2012). 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Optics Letters*, *37*(6), 1008. https://doi.org/10.1364/OL.37.001008

Wheatley, M. (n.d.). SiliconANGLE: D-Wave debuts new 5,000-qubit quantum computer | D-Wave Systems. Retrieved January 26, 2020, from https://www.dwavesys.com/media-coverage/siliconangle-d-wave-debuts-new-5000-qubit-quantum-computer

Williams, C. P., & Clearwater, S. H. (1998). *Explorations in quantum computing*. New York, NY: Springer-Verlag.

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299*(5886), 802–803. https://doi.org/10.1038/299802a0

Yanofsky, N. S., & Mannucci, M. A. (2008). *Quantum computing for computer scientists*. New York, NY: Cambridge University Press.

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., … Pan, J.-W. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science (New York, N.Y.)*, *356*(6343), 1140–1144. https://doi.org/10.1126/science.aan3211

Zwerger, M., Dür, W., & Briegel, H. J. (2012). Measurement-based quantum repeaters. *Physical Review A*, *85*(6), 062326. https://doi.org/10.1103/PhysRevA.85.062326

Zwerger, M., Pirker, A., Dunjko, V., Briegel, H. J., & Dür, W. (2017). Long-range big quantum-data transmission. *Physical Review Letters*, *120*(3), 030503. https://doi.org/10.1103/PhysRevLett.120.030503

  ISSN: 1941-6679-On-line Copy

.