NAIST-IS-DD0461039

Doctoral Dissertation

The Ability of Quantum Information Processing Under the Resource-restricted Circumstances

Yumiko Murakami

August 21, 2008

Department of Information Systems
Graduate School of Information Science
Nara Institute of Science and Technology

A Doctoral Dissertation
submitted to Graduate School of Information Science,
Nara Institute of Science and Technology
in partial fulfillment of the requirements for the degree of
Doctor of ENGINEERING

Yumiko Murakami

Thesis Committee:

Professor Yasuhiko Nakashima	(Supervisor)
Professor Hiroyuki Seki	(Co-supervisor)
Associate Professor Shigeru Yamashita	(Co-supervisor)
Assistant Professor Masaki Nakanishi	(Co-supervisor)

The Ability of Quantum Information Processing Under the Resource-restricted Circumstances*

Yumiko Murakami

Abstract

This dissertation provides the studies on quantum information processing, especially under the circumstances that the computational resources are restricted. Quantum computing is a new computational paradigm based on the quantum mechanics. It has excellent potential abilities of information processing compared to traditional computing called classical computing. However, ideal quantum computers would not be implemented under the current technology and the various computational restrictions are considered to be imposed on the actual quantum computers. Thus, it is quite important to clarify the ability of quantum computing under such restricted circumstances. The main results of this dissertation are as follows.

First, the recognition ability of the quantum computational model with the memory restricted to a stack, quantum pushdown automata, is compared with that of the classical pushdown automata in a deterministic scene. In the computational model theory, the relationship between the recognition abilities of the quantum and classical automata is still an open problem and some negative results which show that the ability of the quantum computational model is weaker than tha classical counterpart are provided. Thus, it is not obvious that the recognition ability of quantum automata is superior. The dissertation shows that quantum pushdown automata can solve a certain problem with no error which cannot be solved by classical deterministic pushdown automata. The modified generalized Ogden ' s lemma is utilized to show that classical deterministic automata cannot solve the problem. This implies that quantum pushdown automata can be more powerful than classical counterparts.

* Doctoral Dissertation, Department of Information Systems, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-DD0461039, August 21, 2008.

Second, a new quantum secure direct communication protocol is proposed. Most of the current quantum secure direct communication schemes use the brilliant resource unique to the quantum information processing, quantum entanglement, which requires the extremely delicate handling. In contrast, the proposed protocol employs no entanglement resource at all. Thus it can be said that the feasibility of implementation of this protocol is higher than the other proposals under the current technology. The proposed protocol can send quantum information as well as classical information. Thus, in order to discuss the security of the proposed protocol, a new criterion is needed which can measure the amount of quantum information. This dissertation introduces a new criterion that is based on the fidelity of quantum states, and it is shown that the proposed protocol satisfies the criterion against the man-in-the-middle attack.

Keywords:

quantum computing, quantum pushdown automata, quantum secret communication, quantum key distribution, unconditional security

資源を限定した状況下における量子計算の能力に関する研究*

村上　ユミコ

内容梗概

本論文は，量子情報処理分野のうち，特に計算資源が限定された状況下での量子計算に関する研究により得られた成果をまとめたものである．量子計算は，量子力学に基づく新しい計算パラダイムであり，従来の計算（古典計算と呼ばれる）に比べ潜在的に強力な情報処理が可能である．しかし現代の技術では理想的な量子計算機を構築することはできず，実際に実現される量子計算機にはその操作について様々な制約が課されることが予想される．よって，様々な制約状況下での計算能力を考える必要がある．本研究の主要な成果は以下の通りである．

第一に，メモリがスタックに限定された量子計算モデルである量子プッシュダウンオートマトンについて，従来の決定性プッシュダウンオートマトンと認識能力を比較する．計算理論においては，量子オートマトンと古典オートマトンの認識能力の関係はまだ未解決の問題である．量子オートマトンの方が古典のものよりも能力的に劣っているとの否定的な結果もすでにいくつか報告されており，量子計算の優位性は自明のものではないことがわかっている．本論文では，古典の決定性プッシュダウンオートマトンが解くことのできないある種の問題を，量子プッシュダウンオートマトンが決定的に解けることを示す．古典プッシュダウンオートマトンがその問題を解けないことについては，一般化されたOgdenの補題を修正したものを用いて証明を行った．この結果は，量子プッシュダウンオートマトンが古典のものよりも強い能力を持っていることを示唆するものである．

第二に，新しい量子直接秘密通信プロトコルを提案する．従来の量子直接秘密通信プロトコルは，量子エンタングルメントと呼ばれる状態維持の非常に難しい量子計算特有の資源を利用するものが多い．しかし提案手法は，この資源を一

* 奈良先端科学技術大学院大学 情報科学研究科 情報システム学専攻 博士論文, NAIST-IS-DD0461039, 2008年8月21日.

切使用しないため，他の提案手法に比べ，現在の技術でも実装がしやすいと考えられる．また提案手法は，古典情報に加え量子情報を送信することができるため，安全性の評価として，量子情報に関する何らかの定量的な基準が必要になる．本論文では，量子状態の忠実度に基づく新たな安全基準を提案し，提案手法がなりすまし攻撃に対してその安全基準を満たしていることを証明する．

キーワード

量子計算, 量子プッシュダウンオートマトン, 量子直接秘匿通信, 量子鍵配布, 無条件安全

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Today the innovations of computers see the end coming. Scaling of transistors has physical limitations. It is very obvious that the size of elemental devices can never exceed the limit of atom. Moreover, at such level it can no longer be expected to make architecture designs within classical mechanics – so it is a world dominated by quantum mechanics. To get around this issue, many down-to-earth solutions have been attempted. "Quantum computing" is a bit different solution, which is essentially based on quantum mechanics, not like traditional computing (called *classical* computing) based on Newtonian mechanics.

The history of quantum computing started with an allusion by Bennett in 1973 that there exists a reversible computational process [3]. Feynman indicated in 1982 that it might take only a linear time to simulate quantum physics by quantum computers although it would take an exponentially time by classical computers [13]. Deutsch formulated the model of quantum computing, quantum Turing machines, in 1985 [11]. This triggered speculation that computing could be done more efficiently, if they made use of quantum effects. But constructing quantum computers proved to be tricky and the field developed slowly since no one knows the specific method to use the quantum effects to speed up computation. It was not until 1994, when a polynomial-time quantum algorithm for prime factorization was announced by Shor [21], that quantum computing captured the widespread attention in the world. It was a significant milestone since this discovery destroyed the popular belief that we will probably never acquire a polynomial-time algorithm for enormous number's factorization on which the safety of today's cipher communications is based. This discovery attracted both of

theoreticians and experimentalists and encouraged the research and development activities of other drastic quantum algorithms and construction of quantum computers. In addition, some other quantum algorithms were proposed, such as Grover's search algorithm [16] and quantum key distribution [4], which had a very strong processing power compared to the classical solutions. They solved the problems which had been believed to be impossible to solve in the practical time in classical computing. These remarkable quantum algorithms built up the expectations that the ability of quantum computers extremely exceeds that of classical computers, however, quantum computing has some practical problems such as it can handle only a limited number of quantum bits at a time. Most of the proposed sophisticated quantum algorithms suppose the ideal quantum computers and processing. But, in practice, we have only the subset in the current technology. Thus, it is important to clarify the quantum processing ability with the limited processing power such that the poor computational resources are available. The aim of this dissertation is to show that quantum computing would exploit its ability even under such realistic circumstances, that is, a limited number of quantum bits, the limited access to quantum bits, the low-precision devices, the short coherent time, no entanglement available, and so on.

The first result of this dissertation shows that the quantum computation with the stack memory, the quantum pushdown automata (QPAs), which is a quantum computational model, is stronger than the classical counterpart in a *deterministic* scene. The result that the 1-way quantum finite automata is weaker than the 1-way classical finite automata is already known. So, it is nontrivial to show that the quantum is stronger than the classical in the computational theory.

QPAs is the quantum computational model defined by Golovkins in 2000 [15] and it is shown that the class of languages recognized by QPAs contains the class of languages recognized by classical finite automata. However, no one knows the relationships between the recognitive ability of QPAs and the classical counterparts. This dissertation gives a proposition that the QPAs can deterministically solve a certain problem, which cannot be solved by any deterministic pushdown automata. Golovkins showed in [15] that QPAs can recognize

- every regular language with probability 1;
- a non-regular language $L_{a=b} = \{\omega \in (a,b)^* |\ |\omega|_a = |\omega|_b\}$ with probability 1;

- a non-context-free language $L_{a=b=c} = \{\omega \in (a,b,c)^* | \ |\omega|_a = |\omega|_b = |\omega|_c\}$ with probability $2/3$; and
- a non-context-free language $L_{xor} = \{\omega \in (a,b,c)^* | \ |\omega|_a = |\omega|_b \text{ xor } |\omega|_a = |\omega|_c\}$ with probability $4/7$,

where $|\omega|_a$ denotes the number of occurrences of a in ω. Golovkins showed that the class of languages recognized by finite automata is properly contained in the class of languages recognized by QPAs, and that QPAs might be more powerful than the classical counterpart in a *bounded error scenario*. This dissertation shows that QPAs can be more powerful even in a *deterministic* case. That is, there exists a problem which can be solved by QPAs deterministically, but cannot be solved by deterministic pushdown automata. This result suggests that quantum computing could be superior to classical computing even if the use of the quantum memory is restricted.

The second result refers to the case that the computational resources are restricted. The elegant quantum information processing often exploits the computational resource called the "quantum entanglement." This is greatly useful, but, it is very difficult to keep such a useful state during the computation in the current technology. This dissertation presents a new quantum secret direct communication protocol (QSDC), that does not need such expensive resources, and shows that it achieves the good security against the man-in-the-middle attack.

The protocol has the following advantages over the current QSDC protocols. First, it can carry an unknown quantum state. This implies that the protocol can be used as a quantum communication scheme between two hubs of a quantum network. Second, no entanglement resource is employed in the protocol. This is an advantage in feasibility. In addition, an eavesdropper on a channel can be detected efficiently. In general, many decoy qubits are required to increase the detection rate, however, in our protocol, the *message shuttle* increases the detection rate and decreases the information an eavesdropper has at her hand as well. Besides, our protocol tolerates against Photon-Number-Splitting attacks, because the encoding operations applied to the secret quantum state never be announced at any step of the protocol. So, even if an eavesdropper could obtain a perfect "copy" of the coded secret qubit, it is insufficient for unveiling the secret perfectly. Thus, an ideal photon generator is not required in the protocol.

Since the proposed protocol can send quantum information as well as classical information, in order to discuss the security of the proposed protocol, a new criterion is needed which can measure the amount of *quantum* information. This dissertation introduces a new criterion based on *fidelity* of quantum states, which is a mathematical measure of the similarity between the two arbitrary quantum states, and shows that the proposed protocol satisfies it against the man-in-the-middle attack. The fidelity between the original secret state and the copy created by the eavesdropper gets really worse if the eavesdropper wants to decrease the detection probability. Conversely, if she wants to get the secret information with good fidelity, she will be detected with extremely high probability.

This dissertation is organized as follows. The next chapter, Chapter 2, gives basics of quantum computing necessary to understand various quantum algorithms. Chapter 3 first introduces the definition of quantum pushdown automata and its configuration and then gives a proposition that the QPAs can deterministically solve a certain problem, which cannot be solved by any deterministic pushdown automata. Chapter 4 first considers how well the depolarized channel keeps the fidelity of quantum states. Then a new QSDC protocol is presented. A new security criterion based on the fidelity of quantum states discussed above is introduced and it is shown that the presented protocol satisfies the criterion against the man-in-the-middle attack. Chapter 5 concludes this dissertation.

Chapter 2

Basics of Quantum Computing

This chapter gives the basics of quantum computation, quantum systems, evolution, measurement, entanglement, density matrix, and fidelity.

2.1. Quantum state

A quantum bit, *qubit*, is like a probabilistic bit which is '0' with probability a and '1' with probability b, where $a + b = 1$. The significant difference between a qubit and a traditional bit (classical bit) is that, while a classical bit denotes either '0' or '1' at a certain moment, a qubit can be in the both state at the same time. The two possible states for a qubit are described by $|0\rangle$ and $|1\rangle$ using the Dirac notation, corresponding to traditional '0' and '1' respectively. A quantum state of a qubit can be in the state:

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

where α and β are complex numbers which are called *probability amplitudes* and $|\alpha|^2 + |\beta|^2 = 1$. Thus, a quantum state can be regarded as a unit-length vector in a two dimensional complex vector space with inner product, that is, a Hilbert space, and an arbitrary quantum state is described by the linear combination of the orthonormal basis states of the state space, called *superposition*. The basis $\{|0\rangle, |1\rangle\}$ is called the computational basis and described as vectors $|0\rangle = (1\ 0)^t, |1\rangle = (0\ 1)^t$. Note that the computational basis is just one of many possible bases, and an arbitrary quantum state can be re expressed in terms of another basis, for example, consider the following

basis: $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$: then,

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle && (2.1)\\ &= \frac{\alpha}{\sqrt{2}}\{|+\rangle + |-\rangle\} + \frac{\beta}{\sqrt{2}}\{|+\rangle - |-\rangle\} && (2.2)\\ &= \frac{\alpha+\beta}{\sqrt{2}}\,|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}\,|-\rangle\,. && (2.3) \end{aligned}$$

The superposition yields the remarkable quantum computation power, especially when it is a composite system of plenty of qubits. The notation of a composite system is represented by a tensor product of each qubit, like $|1\rangle \otimes |0\rangle$. It would be described like simply $|10\rangle$ or $|2\rangle$ decimally.

Consider the n qubit system, that is, the 2^n dimensional Hilbert space. Let the basis states be

$$|0\rangle = (1\ 0\ 0 \cdots 0)^t, |1\rangle = (0\ 1\ 0 \cdots 0)^t, \cdots, |2^n - 1\rangle = (0\ 0 \cdots 0\ 1)^t$$

and then the quantum state $|\psi\rangle = (\alpha_0\ \alpha_1 \cdots \alpha_{2^n-1})^t$ can be described as a linear combination of the basis states with complex coefficients:

$$|\psi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle + \cdots + \alpha_{2^n-1}\,|2^n - 1\rangle = \sum_{i=0}^{2^n-1} \alpha_i\,|i\rangle,$$

where $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$. In quantum systems, the state space increases exponentially with the size of the system. This enormous potential computational power would provide us various advantages of quantum computation.

2.2. Evolution

The classical systems are governed by the Newtonian equation, whereas the quantum systems by the Schrödinger equation. The evolution of a closed quantum system is described by a *unitary transformation* U, that is $UU^\dagger = U^\dagger U = I$, where $U^\dagger$ is conjugate of U, and it can be regarded as a rotation of a complex vector space. I is an identity matrix. A 2×2 unitary matrix describes an operation to a qubit. An operation to n-qubit system is specified as a 2^n-dimensional unitary matrix. It would be described as a tensor product of some sub-dimensional unitary matrices, e.g.,

$$U_0 \otimes U_1\{\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_0 \otimes |1\rangle_1\},$$

where U_0 and U_1 are the unitary operators for the first qubit and the second qubit of the two-qubit system, respectively. Because of the linearity, applying the unitary operator U to a superposition state is represented as follows.

$$\begin{aligned} U|\psi\rangle &= U\sum_{i=0}^{2^n-1}\alpha_i|i\rangle \\ &= \sum_{i=0}^{2^n-1}U\alpha_i|i\rangle . \end{aligned}$$

This means that the unitary operator can be applied to each computational state $|i\rangle$ individually. This parallelism could be advantages of quantum computation.

The often-used unitary operators, Hadamard transform and Pauli operators are defined as follows.

2.2.1 Hadamard transform

The Hadamard transform, H is defined as follows.

$$\begin{aligned} H: \quad |0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

Applied to basis vector $|0\rangle$, H creates the superposed state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Furthermore, applied to n qubits individually, H creates the superposition of all 2^n possible states. The n-bit Hadamard transform, H_n, is defined as follows.

$$\begin{aligned} & H_n|x_0x_1\cdots x_{n-1}\rangle \\ &= (H\otimes H\otimes\cdots\otimes H)|x_0x_1\cdots x_{n-1}\rangle \\ &= \frac{1}{\sqrt{N}}\{(|0\rangle + (-1)^{x_0}|1\rangle)\otimes(|0\rangle + (-1)^{x_1}|1\rangle)\otimes\cdots\otimes(|0\rangle + (-1)^{x_{n-1}}|1\rangle)\} \\ &= \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}(-1)^{x_0y_0+x_1y_1+\cdots+x_{n-1}y_{n-1}}|y_0y_1\cdots y_{n-1}\rangle , \end{aligned}$$

where $y = 2^{n-1}y_0 + 2^{n-2}y_1 + \cdots + 2^0y_{n-1}$ and $N = 2^n$. For example,

$$\begin{aligned} H_3|000\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \end{aligned}$$

On the other hand,

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

It is called a quantum *interference* that a unitary operation increase or decrease each amplitude.

2.2.2 Pauli group

The *Pauli group* G consists of the following four operators extremely useful 2×2 matrices.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_y = i\sigma_x\sigma_z = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

2.2.3 No-cloning

One of the peculiar features of quantum state is "no-cloning." The reason why anyone can make a perfect copy of an electronic information is that the information lives in classical dynamics. In contrast, in quantum dynamics, anyone cannot make a perfect copy of an unknown quantum state. The proof is a simple application of the linearity of unitary transformations. Assume that U is a unitary transformation that clones a qubit, such that $U|a0\rangle = |aa\rangle$ and $U|b0\rangle = |bb\rangle$. Consider $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$. By the linearity,

$$\begin{aligned} U|c0\rangle &= \frac{1}{\sqrt{2}}\{U|a0\rangle + U|b0\rangle\} \\ &= \frac{1}{\sqrt{2}}\{|aa\rangle + |bb\rangle\}. \end{aligned} \tag{2.4}$$

But, if U is a genuine cloning transformation, then

$$U|c0\rangle = |cc\rangle = 1/2(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle),$$

which is not equal to (2.4). Thus, there is no unitary operation that can correctly clone an unknown quantum state.

2.3. Measurement

We cannot examine a qubit to determine its quantum state definitely, that is, to specify the value of α and β. When the qubit state, $\alpha|0\rangle+\beta|1\rangle$, is measured, the $|0\rangle$ is obtained with probability $|\alpha|^2$ or the $|1\rangle$ with probability $|\beta|^2$, and the information of α and β is lost. That is, measurement of a quantum state transforms the state into one of the measuring device's associated basis states, the computational basis in this case. We define the measurement formally as follows.

Let $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{n-1}|n-1\rangle$. Given the *observable* that corresponds to the orthogonal decomposition of the state space $E = E_0 \oplus E_1 \oplus \cdots \oplus E_{m-1}$ which devides the state space into orthogonal subspaces E_i's. Consider a *projection* of $|\psi\rangle$ to each of E_i. The squared magnitude of the projection is the probability with which the associated outcome is obtained. The outcome is $i \in \{0, \cdots m-1\}$ and the state after measurement is in the subspace. For example, consider a four-dimensional complex vector space whose basis states are $|0\rangle$, $|1\rangle$, $|2\rangle$ and $|3\rangle$. Let the state $|\psi\rangle$ be a vector that lives in the space and $|\psi\rangle = \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle - \frac{1}{2}|3\rangle$. Let the observable correspond to the orthogonal decomposition $E = E_a \oplus E_b \oplus E_c$, where E_a is a space spanned by $|0\rangle$ and $|1\rangle$, E_b is a space spanned by $|2\rangle$, and E_c is a space spanned by $|3\rangle$. That is, the outcome of measurement is 'a' with probability $1/2$ or 'b' with probability $1/4$ or 'c' with probability $1/4$. It should be noted that the original quantum state is destructed unless the appropriate observable is used.

2.4. Entanglement

Entanglement is an essential resource for the sophisticated quantum computation, which is a strong correlation among qubits even if separated physically, and can never be implemented in the classical dynamics. Consider a composite quantum system in the state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.5}$$

When the first qubit is measured, the outcome is either 0 with probability $1/2$ or 1 with probability $1/2$ and the state of the whole system collapses to $|00\rangle$ or $|11\rangle$ respectively. Thus, the other qubit is determined as $|0\rangle$ or $|1\rangle$ with certainty. This unique

correlation such that the measurement of one has an impact to the other is called *entanglement*. Also from the mathematical view, the entangled state $|\psi\rangle_{AB}$ cannot be considered as the tensor product of the two separate individual systems. When the degree of entanglement is maximum like (2.5), it is said to be in a *maximally entangled* state, especially, in the case of two-qubit system it is called an EPR pair, and in the case of three-qubit system a GHZ state. Entanglement is a fairly useful resource, but, with the current technology it is not easy to keep up the entangled state.

2.5. Density matrix

The *density matrix* is another way to describe a quantum state. It provides a convenient means particularly for describing a quantum system whose state is a classical mixture of several states. When a quantum system is in one of $|\psi_i\rangle$'s with probability p_i, the density matrix for the system is defined as

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|.$$

For example, when a quantum system is in the state $|0\rangle$ with probability $1/2$ and in the state $\frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\}$ with probability $1/2$, the density matrix of the system is $\rho = 1/2\,|0\rangle\langle 0| + 1/2\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\}\{\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\}$. In general, it is not clear for us how the exact state of a quantum system is because of the influence of environment or something else. The following case provides a good example. Suppose each of the two parties, Alice and Bob, has one qubit of an EPR pair, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If Alice measures her qubit and she does not inform Bob of the outcome, Bob cannot specify his qubit state exactly. The state of Bob's qubit is half-and-half mixture of $|0\rangle$ and $|1\rangle$, that is, $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. Like this, the ambiguous state of a quantum system can be described by a density matrix. A quantum state is simply classified into two groups, a *pure state* and a *mixed state*. A pure state satisfies $tr(\rho^2) = 1$, while a mixed state satisfies $tr(\rho^2) < 1$. In particular, when $\rho = I/2$, ρ is said to be in a maximally mixed state and the state has a maximum entropy. The evolution of the density matrix is described by the equation

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger.$$

Let the composite system of A and B whose density matrix be ρ_{AB}. The reduced density operator for system A is defined by

$$\rho_A = Tr_B(\rho_{AB}),$$

which is used when subsystem A is focused on in the whole system, where Tr_B is a map of operators known as the partial trace over system B. The partial trace is defined by

$$Tr_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|) = |a_1\rangle \langle a_2| \langle b_1|b_2\rangle ,$$

where $|a_1\rangle$ and $|a_2\rangle$ are any two vectors in the state space of A, $|b_1\rangle$ and $|b_2\rangle$ are any two vectors in the state space of B.

2.6. Fidelity

The fidelity is a measure that quantities the similarity between quantum states. It provides a quantitative criterion of the reliability of a quantum channel, i.e., how well a quantum channel preserves information.

The fidelity of the two states ρ and σ is defined as

$$F(\rho, \sigma) \triangleq tr(\rho^{1/2}\sigma\rho^{1/2}).$$

When ρ and σ are commutative:

$$\rho = \sum_i r_i |i\rangle \langle i| ; \;\; \sigma = \sum_i s_i |i\rangle \langle i|,$$

where $\{|i\rangle\}$ is a set of the orthonormal basis states, we see

$$\begin{aligned} F(\rho, \sigma) &= tr(\Sigma r_i s_i |i\rangle \langle i|) \\ &= \Sigma r_i s_i. \end{aligned}$$

In particular, when ρ is a pure state,

$$\begin{aligned} F(|\psi\rangle , \sigma) &= tr(\langle\psi| \sigma |\psi\rangle |\psi\rangle \langle\psi|) \\ &= \langle\psi| \sigma |\psi\rangle \end{aligned} \tag{2.6}$$

The fidelity is invariant under unitary transformation.

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma).$$

Chapter 3

Recognition Ability of Quantum Pushdown Automata

3.1. Introduction

In quantum computational theory, some quantum counterparts of classical computational models were introduced. In particular, the results of quantum finite automata (QFAs) [1, 17] and quantum counter automata (QCAs) [5, 18, 24, 25] are remarkable. Fig. 3.1 illustrates the relationships between the recognition abilities of classical automata and their counterparts. The number at the head, 1 or 2, denotes one-way or two-way, respectively, which mean the direction that the input tape head can move. The number before "CA" denotes the numbers of counters. Thus, "1Q2CA" means a one-way quantum automaton with two counters. In this figure, the lower model is resource-restricted more strongly than the upper models. This figure, for example, shows that the recognition ability of the one-way quantum finite automata is properly contained in that of the one-way classical finite automata, while the recognition ailities of the two-way quantum finite automata and the two-way quantum one-counter automata properly contains their classical counterparts. In other words, quantum computation is not always stronger than classical computation under the resource-restricted circumstances.

This chapter focuses on a quantum pushdown automaton (QPA), which is a generalization of a counter automaton. QPAs is the quantum computational model defined by Golovkins in 2000 [15] and it is shown that the class of languages recognized by

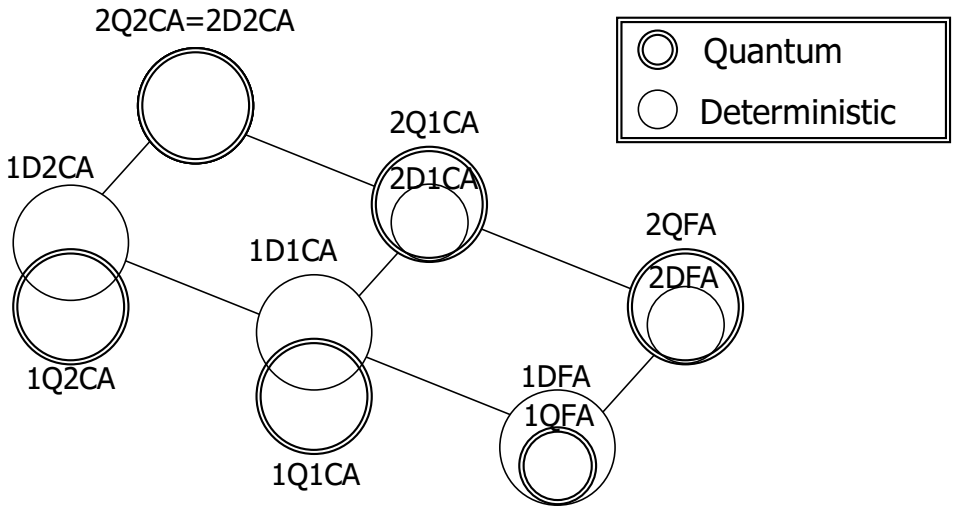

Figure 3.1. The relationships between the recognition abilities of classical automata and their counterparts

QPAs contains the class of languages recognized by classical finite automata. However, no one has known the relationships between the recognitive ability of QPAs and the classical counterparts. This dissertation shows that QPAs can solve a certain problem with no error, which cannot be solved by any classical deterministic pushdown automata[1] .

QPAs was first introduced by Moore and Crutchfield [20], but there the authors actually deal with the so-called generalized quantum pushdown automata, whose evolution does not have to be unitary. Thus, Golovkins reintroduced the model QPAs by giving a definition that would confirm unitarity requirement [15] on which I advance a discussion based.

Golovkins showed in [15] that QPAs can recognize

- every regular language with probability 1;
- a non-regular language $L_{a=b} = \{\omega \in (a,b)^* |\ |\omega|_a = |\omega|_b\}$ with probability 1;

[1] In the classical deterministic automaton model, transitions are occured deterministically, that is, an exact computation

- a non-context-free language $L_{a=b=c} = \{\omega \in (a,b,c)^* |\ |\omega|_a = |\omega|_b = |\omega|_c\}$ with probability $2/3$; and
- a non-context-free language $L_{xor} = \{\omega \in (a,b,c)^* |\ |\omega|_a = |\omega|_b$ xor $|\omega|_a = |\omega|_c\}$ with probability $4/7$,

where $|\omega|_a$ denotes the number of occurrences of a in ω. Golovkins showed that the class of languages recognized by finite automata is properly contained in the class of languages recognized by QPAs, and that QPAs might be more powerful than the classical counterpart in a *bounded error scenario*. This dissertation shows that QPAs can be more powerful even in a deterministic case. That is, there exists a problem which can be solved by QPAs deterministically, but cannot be solved by DPAs.

This chapter is organized as follows. Section 3.2, following this introduction, first defines the model of QPAs, its configuration, and so on, and then introduces the lemma called generalized Ogden's lemma and the quantum algorithm called Deutsch-Jozsa algorithm, which are useful in the following section. Section 3.3 defines the problem and shows that QPAs can solve it with no error. Section 3.4 shows that no deterministic pushdown automata (DPAs) solve the problem. Section 3.5 concludes this chapter.

3.2. Preliminaries

3.2.1 Definitions

This section cites the definition of QPAs, their configuration and evolution from [15].

Definition 3.1. ***(Quantum Pushdown Automaton)*** *A Quantum Pushdown Automaton, QPA, is defined as the following 8-tuple.* $A = (Q, \Sigma, T, q_0, Q_{acc}, Q_{rej}, D, \delta)$ *is specified by a finite set of states* Q*, a finite input alphabet* Σ*, a finite stack alphabet T, an initial state* $q_0 \in Q$*, sets* $Q_{acc} \subset Q$*,* $Q_{rej} \subset Q$ *of accepting and rejecting states, respectively, with* $Q_{acc} \cap Q_{rej} = \phi$*, a function* $D : Q \longrightarrow \{\downarrow, \rightarrow\}$*, where* $\{\downarrow, \rightarrow\}$ *is the set of directions of input tape head, remaining at the current position or moving one cell forward, and a transition function* $\delta : Q \times \Gamma \times \Delta \times Q \times \Delta^* \longrightarrow \mathbf{C}$*, where* $\Gamma = \Sigma \cup \{\#, \$\}$ *is the input tape alphabet of* A *and* $\#, \$$ *are end markers not in* Σ*,* $\Delta = T \cup \{z\}$ *is the working stack alphabet of* A*, and* $z \notin T$ *is the stack bottom symbol.* □

The transition function is restricted to the following requirement:
If $\delta(q, \alpha, \beta, q', \tau) \neq 0$, then

1. $|\tau| \leq 2$, and
2. $\tau \in \beta T^*$ if $|\tau| \neq 0$.

Definition 3.2. ***(Configuration)*** *A configuration of a QPA is denoted as* $|c\rangle = |\nu_i q_j \nu_k, \tau_l\rangle$*, where the automaton is in a state* $q_j \in Q$*,* $\nu_i\nu_k \in \#\Sigma^*$ *is a finite word on the input tape,* $\tau_l \in zT^*$ *is a finite word on the stack tape, the input tape head is above the first alphabet of the word* ν_k*, and the stack head is above the last alphabet of the word* τ_l*. Note that the rightmost symbol of* τ_l *is the stack top symbol.* □

Let C be the set of all configurations of a QPA. Set C is countably infinite. Since every configuration $|c\rangle$ denotes a basis vector in Hilbert space $H_A = l_2(C)$, a global state of A in space H_A has a form $|\psi\rangle = \sum_{c \in C} \alpha_c |c\rangle$, where $\alpha_c \in \mathbf{C}$ denotes the probability amplitude of a configuration $|c\rangle$, and $\sum_{c \in C} |\alpha_c|^2 = 1$.

Definition 3.3. ***(linear operator)*** *Let* $|c\rangle = |\nu_i q_j \sigma \nu_k, \tau_l \tau\rangle$*. A linear operator* U_A *is defined as follows:*
$U_A |c\rangle = \sum_{(q,\tau') \in Q \times \{\varepsilon, \Delta, \Delta^2\}} \delta(q_j, \sigma, \tau, q, \tau') |f(|c\rangle, q), \tau_l \tau'\rangle$*, where* $f(|\nu_i q_j \sigma \nu_k, \tau_l \tau\rangle, q)$

$$= \begin{cases} \nu_i q \sigma \nu_k, & if\ D(q) = \text{`}\downarrow\text{'} \\ \nu_i \sigma q \nu_k, & if\ D(q) = \text{`}\rightarrow\text{'}. \end{cases}$$

□

For QPA $A = (Q, \Sigma, T, q_0, Q_{acc}, Q_{rej}, D, \delta)$, $C_{acc} = \{|\nu_i q_j \nu_k, \tau_l\rangle \in C | q_j \in Q_{acc}\}$, $C_{rej} = \{|\nu_i q_j \nu_k, \tau_l\rangle \in C \mid q_j \in Q_{rej}\}$, and $C_{non} = C \setminus (C_{acc} \cup C_{rej})$. E_{acc}, E_{rej}, and E_{non} are subspaces of H_A spanned by C_{acc}, C_{rej}, and C_{non}, respectively. The observable $\mathcal{O}$ that corresponds to the orthogonal decomposition $H_A = E_{acc} \oplus E_{rej} \oplus E_{non}$ is used. The outcome of each measurement is either "accept" or "reject" or "non-halting."

The computation of QPA A proceeds as follows. For an input $\omega \in \Sigma^*$, assume that computation starts with configuration $|q_0 \# \omega \$, z\rangle$. Each computation step consists

of two parts. First, linear operator U_A is applied to the current state, and then the resulting superposition is measured with respect to the observable $\mathcal{O}$ defined above. Let the state before the measurement be $\sum_{c \in C} \alpha_c |c\rangle$, and then the probability that the resulting superposition is projected into subspace E_i, $i \in \{acc, rej, non\}$, is $\sum_{c \in C_i} |\alpha_c|^2$. Computation continues until the result of a measurement is "accept" or "reject."

A QPA is considered valid in terms of quantum theory if its evolution operator is unitary.

Well-formedness conditions.

In the following expressions, δ^* represents a complex conjugate of δ.

1. $\forall (q_1, \sigma_1, \tau_1) \in Q \times \Gamma \times \Delta$,
$$\sum_{(q,\omega) \in Q \times \Delta^*} |\delta(q_1, \sigma_1, \tau_1, q, \omega)|^2 = 1.$$

2. For all triples $(q_1, \sigma_1, \tau_1) \neq (q_2, \sigma_1, \tau_2)$ in $Q \times \Gamma \times \Delta$,
$$\sum_{(q,\omega) \in Q \times \Delta^*} \delta^*(q_1, \sigma_1, \tau_1, q, \omega) \delta(q_2, \sigma_1, \tau_2, q, \omega) = 0.$$

3. $\forall (q_1, \sigma_1, \tau_1, \tau_2) \in Q \times \Gamma \times \Delta^2$,
$$\sum_{(q,\tau,\omega) \in Q \times \Delta \times \{\varepsilon, \tau_2, \tau_1\tau_2\}} |\delta(q, \sigma_1, \tau, q_1, \omega)|^2 = 1.$$

4. $\forall (q_1, \sigma_1, \tau_1), (q_2, \sigma_1, \tau_2) \in Q \times \Gamma \times \Delta, \forall \tau_3 \in \Delta$,

   (a) $$\sum_{(q,\tau) \in Q \times \Delta} \delta^*(q_1, \sigma_1, \tau_1, q, \tau) \delta(q_2, \sigma_1, \tau_2, q, \tau_3\tau) + \sum_{q \in Q} \delta^*(q_1, \sigma_1, \tau_1, q, \varepsilon) \delta(q_2, \sigma_1, \tau_2, q, \tau_3) = 0,$$

   (b) $$\sum_{q \in Q} \delta^*(q_1, \sigma_1, \tau_1, q, \varepsilon) \delta(q_2, \sigma_1, \tau_2, q, \tau_2\tau_3) = 0.$$

Theorem 3.1. *The evolution of a QPA is unitary if and only if Well-formedness conditions are satisfied.*

Proof. See the proof of Theorem 2 in [15]. □

Throughout this dissertation, only unitary QPAs that satisfy Well-formedness conditions is considered.

3.2.2 Extension of generalized Ogden's lemma

Let $\mathbf{N}$ be the set of natural numbers.

Lemma 3.1. (generalized Ogden's lemma) *For any context-free language L, $\exists n \in \mathbf{N}$ such that $\forall z \in L$, if p positions in z are "distinguished" and q positions are "excluded," with $p > n^{q+1}$, then $\exists u, v, w, x, y$ such that $z = uvwxy$ and*

1. *vx contains at least one distinguished positions and no excluded positions,*
2. *if p' is the number of distinguished positions and q' is the number of excluded positions in vwx, then $p' \leq n^{q'+1}$,*
3. *$\forall i \in \mathbf{N}$, $uv^iwx^iy \in L$.*

Proof. See [2]. □

It is straightforward to see that the proof of lemma 3.1 can be applied to not only for strings of terminal symbols, but also for strings including non-terminal symbols or string w such that $uXy \stackrel{+}{\Rightarrow} uvXxy \stackrel{+}{\Rightarrow} uvwxy$. Thus, it is obvious that the following corollary holds.

Corollary 3.1. *For any context-free grammar G, $\exists n \in \mathbf{N}$ such that $\forall z \in (T \cup V)^*$ derived by G, where T and V are sets of terminal and non-terminal symbols, respectively, if p positions in z are "distinguished" and q positions are "excluded", with $p > n^{q+1}$, then $\exists u, v, w, x, y$ such that $z = uvwxy$ and*

1. *vx contains at least one distinguished positions and no excluded positions,*
2. *if p' is the number of distinguished positions and q' is the number of excluded positions in vwx, then $p' \leq n^{q'+1}$,*
3. *$\forall i \in \mathbf{N}$, uv^iwx^iy is derived by G.*

3.2.3 Deutsch-Jozsa algorithm

Deutsch-Jozsa algorithm is the algorithm that solves the following problem deterministically.

Deutsch's XOR problem

Given a function $f : \{0,1\} \longrightarrow \{0,1\}$, as a black box, the question is whether $f(0) \oplus f(1) = 0$ or 1 (i.e. whether f is constant of balanced).

This is a very simple problem of guessing whether a given coin is genuine (with head on one side and tail on the other) or fake (with both sides the same). In the classical world, we need to look at the coin twice (both sides) to find out which case it is. In other words, in classical computing, we need obviously two applications of f, to 0 and to 1, to solve the problem. Surprisingly, there is a quantum solution to the problem, which uses only one application of f and provides in all cases the exact answer.

Deutsch-Jozsa algorithm

Let U_f be the unitary mapping of $|x\rangle |y\rangle \longrightarrow |x\rangle |y \oplus f(x)\rangle$. Apply first the two-dimensional Hadamard transform to two registers in the initial state $|0\rangle |1\rangle$ and then U_f to get

$$
\begin{aligned}
|0\rangle |1\rangle &\xrightarrow{H_2} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)), \\
&= \frac{1}{2}\{|0\rangle (|0\rangle - |1\rangle) + |1\rangle (|0\rangle - |1\rangle)\}, \\
&\xrightarrow{U_f} \frac{1}{2}\{|0\rangle (|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle (|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)\}, \\
&= \frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)} |1\rangle)(|0\rangle - |1\rangle). \\
&\xrightarrow{H_2} (-1)^{f(0)} |(f(0) \oplus f(1))\rangle |1\rangle , \\
&= \begin{cases} (-1)^{f(0)} |0\rangle |1\rangle & \text{if } f \text{ is constant}, \\ (-1)^{f(0)} |1\rangle |1\rangle & \text{if } f \text{ is balanced}. \end{cases}
\end{aligned} \tag{3.1}
$$

By measuring the first qubit in (3.1), we can immediately see whether f is constant of balanced.

3.3. QPAs that solve a certain problem deterministically

This section shows that QPAs can solve the following problem deterministically.

Problem I

[Input] A string $\omega = x\%y\%z\%y'\%z'$, where % is a separator symbol, $x = x_n x_{n-1} \cdots x_1$, $y = y_1 y_2 \cdots y_m$, and $z = z_1 z_2 \cdots z_l$ are sequences of n, m, and l letters in $\{a, b, c\}$, respectively, and $y', z' \in \{a, b, c\}^*$. Let i be an index such that $x_1 x_2 \cdots x_{i-1} = y_1 y_2 \cdots y_{i-1}$ and $x_i \neq y_i$. Let j be an index such that $x_1 x_2 \cdots x_{j-1} = z_1 z_2 \cdots z_{j-1}$ and $x_j \neq z_j$. It is promised that y_i,$z_j \neq a$ and ω is either of the following two:

(c1) $|y'| = |y_{i+1} y_{i+2} \cdots y_m| = m - i$,
$|z'| = |z_{j+1} z_{j+2} \cdots z_l| = l - j$, and $i = j$;

(c2) $|y'| \neq m - i$ and $|z'| \neq l - j$.

[Output] Decide whether the input satisfies (c1) and $y_i = z_j$. In that case the automaton *accepts* the input. If (c1) and $y_i \neq z_j$, or (c2) is satisfied, the automaton *rejects* it.

Problem I is a promise problem such that the set of input strings is decomposed into "acceptable," "rejectable," and "don't care" inputs, and only the "acceptable" and "rejectable" inputs are identified correctly.

Theorem 3.2. *There exists a QPA that solves Problem I deterministically.*

Proof. A QPA $M = (Q, \Sigma, T, q_0, Q_{acc}, Q_{rej}, D, \delta)$ that solves Problem I deterministically is constructed as follows. $Q = Q_\downarrow \cup Q_\rightarrow$, where $Q_\downarrow = \{q_0, q_i, q^i_{rej}\}$ and $Q_\rightarrow = \{q^i_j\}$ ($1 \leq i \leq 4$, $1 \leq j \leq 6$), $\Sigma = \{a, b, c, \%\}$,$T = \{a, b, c, u\}$, $Q_{acc} = \{q_2\}$, $Q_{rej} = \{q_4, q^i_{rej}\}$, $D(q) =$'$\rightarrow$' if $q \in Q_\rightarrow$, otherwise '$\downarrow$'. Transition function δ is defined as Figure 3.3. The main idea utilizes the Deutsch-Jozsa algorithm [12] whose transition goes along as follows:

$$|0\rangle|1\rangle \xrightarrow{H^{\otimes 2}} \frac{1}{2}\{|M_0\rangle(|0\rangle - |1\rangle) + |M_1\rangle(|0\rangle - |1\rangle)\} \tag{3.2}$$

$$\xrightarrow{U_f} \frac{1}{2}\{|M_0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |M_1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)\}, \tag{3.3}$$

$$= \frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle). \tag{3.4}$$

$$\xrightarrow{H^{\otimes 2}} (-1)^{f(0)}|(f(0) \oplus f(1))\rangle|1\rangle, \tag{3.5}$$

$$= \begin{cases} (-1)^{f(0)}|0\rangle|1\rangle & \text{if } f \text{ is constant,} \\ (-1)^{f(0)}|1\rangle|1\rangle & \text{if } f \text{ is balanced.} \end{cases} \tag{3.6}$$

Let M_0 and M_1 represent 0 and 1, respectively, and $U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle$, where $f(0) = g(y_i), f(1) = g(z_j), g(b) = 0$, and $g(c) = 1$.

QPA M consists of two independent sub-QPAs, M_0 and M_1 (cf. Figure 3.2), which have analogous behaviors. After reading the left end marker, M goes to the superposed state of q_1^1, q_1^2, q_1^3, and q_1^4 with amplitudes $+\frac{1}{2}, -\frac{1}{2}, +\frac{1}{2}$, and $-\frac{1}{2}$, respectively. Expression (3.2) is considered to be this transition, e.g., $|M_0, 0\rangle$ represents state q_1^1 (to be exact, the configuration at q_1^1 containing the stack information and the position of the input tape head). M_0 is a sub automaton that starts in the superposition of q_1^1 and q_1^2, searches for i such that y_i first discords from x_i, and examines whether $|y_{i+1} \cdots y_m| = |y'|$. M_1 is also a sub automaton that starts in the superposition of q_1^3 and q_1^4, searches for j such that z_j first discords from x_j, and examines whether $|z_{j+1} \cdots z_l| = |z'|$. M_0 and M_1 run simultaneously. As will hereinafter be described in detail, M_0 and M_1 go to states $q_6^1, \ldots, q_6^4$ at the same time iff $i = j$, $|y_{i+1} \cdots y_m| = |y'|$, and $|z_{i+1} \cdots z_l| = |z'|$. Note that if $y_i(z_j)$ is b, the amplitudes of q_6^1 and q_6^2 (q_6^3 and q_6^4) are $+\frac{1}{2}$ and $-\frac{1}{2}$, while if $y_i(z_j)$ is c, then $-\frac{1}{2}$ and $+\frac{1}{2}$. These transitions correspond to Exp. (3.3), that is, the application of U_f denotes the simultaneous running of M_0 and M_1. For example, suppose that $i = j$, $y_i = b$, and $z_j = c$, the configuration of M

$$\frac{1}{2}\{(|q_6^1\rangle - |q_6^2\rangle) + (-|q_6^3\rangle + |q_6^4\rangle)\},$$

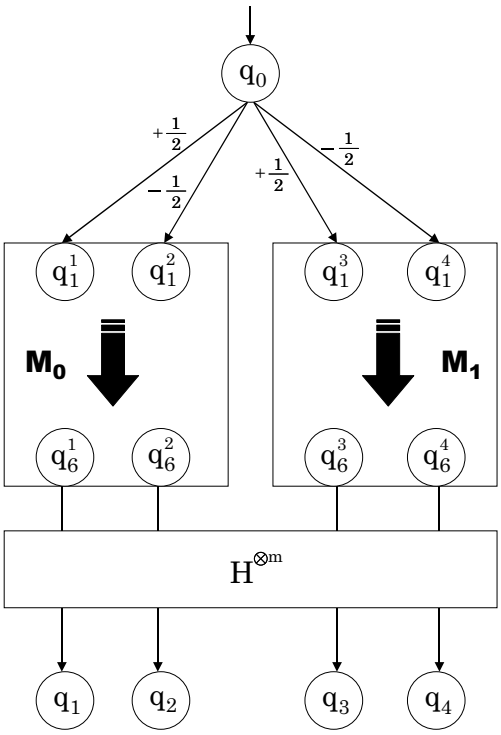

Figure 3.2. QPA that solves Problem I deterministically.

corresponds to Exp. (3.3)

$$\frac{1}{2}\{|M_0\rangle\,(|0\rangle - |1\rangle) + |M_1\rangle\,(|1\rangle - |0\rangle)\}. \tag{3.7}$$

By applying the Hadamard transform to Exp. (3.7), $|1\rangle\,|1\rangle$ is obtained, corresponding to q_4, namely, a rejecting state.

Note that this algorithm successfully functions iff condition (c1) is satisfied, since the two sub-QPAs must be in the superposed state of four q_6^i's at the same time and with the same stack configuration so that the interference of the second Hadamard transform is performed well. Thus, M can properly handle inputs that satisfy (c1). Before considering case (c2), I illustrate the sub-QPAs (cf. Figure 3.3).

Since they have analogous behaviors as previously described, only one of them, M_0 is explained here. Sub-QPA M_0

1. reads x and puts it into the stack, remaining at q_1^1 and q_1^2;

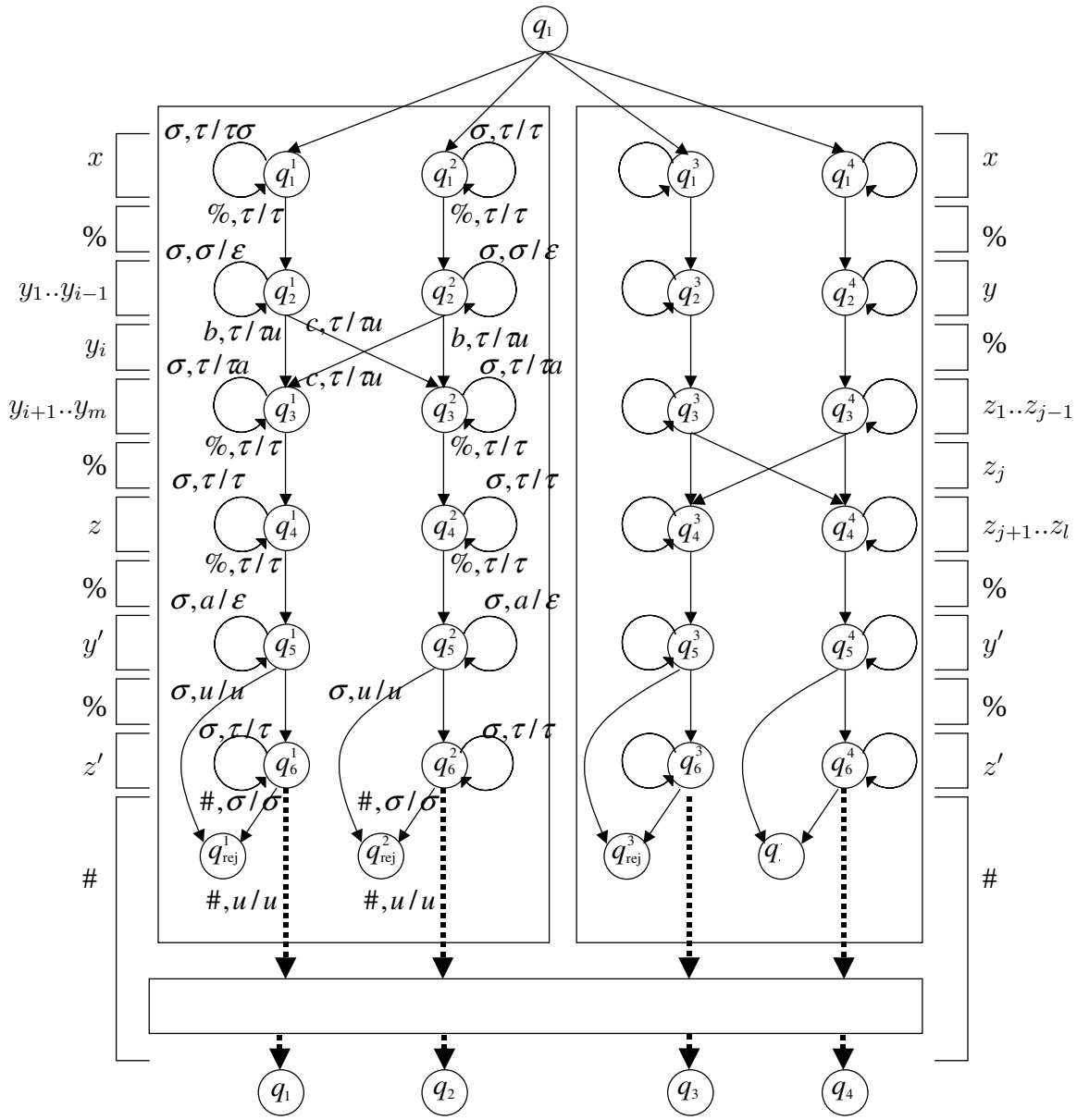

Figure 3.3. The behaviors of the sub-QPAs. $(\sigma, \tau/\tau')$ represents the transition that when the input symbol is σ with the stack top τ, τ is retrieved and τ' is pushed into the stack, where $\sigma \in \Sigma$ and $\tau \in T$.

2. reads % and goes to the superposed state of q_2^1 and q_2^2;

3. keeps retrieving a stack top symbol one by one at the superposed state until discordance between the stack top symbol and the input letter occurs, namely, y_i is read;

4. reads y_i and pushes u into the stack, and goes to

   (a) q_3^1 from q_2^1 and q_3^2 from q_2^2 if $y_i = b$,

   (b) q_3^1 from q_2^2 and q_3^2 from q_2^1 if $y_i = c$;

5. continues pushing a into the stack at the states while reading $y_{i+1} \cdots y_m$,

6. reads %, goes to the superposed state of q_4^1 and q_4^2, and skips z at the state;

7. reads %, goes to the superposed state of q_5^1 and q_5^2, and keeps retrieving a stack top one by one while reading y';

8. reads %, goes to q_6^1 and q_6^2, and skips the remainder of the input.

Note that if the input satisfies (c1), M_0 and M_1 go to q_6^i's at the same time. Consider (c2). If $y_{i+1} \cdots y_m$ is shorter than y', at step (7) symbol u must show up at the stack top before reading through y' and M_0 goes to $q_{rej}^{1,2}$, namely, rejecting states. If $y_{i+1} \cdots y_m$ is longer, the stack top symbol will never be u when reading the right end marker, and then the automaton goes to $q_{rej}^{1,2}$. Remember that M_1 has a similar behavior, it is easy to show that the input that satisfies (c2), leads both M_0 and M_1 to the rejecting states; disagreement of arrival timings have no need to be discussed. Therefore, M accepts input (c1) and rejects input (c2) with certainty.

Finally, the unitarity of the evolution of M is discussed. Obviously, the transition of M is reversible deterministic except for two Hadamard transforms. Thus, it is straightforward that the undefined transitions of δ can be defined properly to satisfy Well-formedness conditions. □

Further, it should be emphasize that this theorem also holds for 1-way QPAs. This QPA can be seen as a 1-way QPA since the tape head always goes right except when it reads \$, or the finite state control comes to the accepting or rejecting state.

3.4. No DPAs can solve Problem I

This section shows that no DPAs can solve the problem defined in Section 3.3. Since DPAs are special cases of non-deterministic pushdown automata, NPAs, the following theorem indicates that there are no DPAs that solve Problem I.

Theorem 3.3. *There exist no NPAs that solve Problem I.*

Proof. (Outline) If there were NPAs that solved Problem I, there would exist a context-free grammar G that derives every acceptable input string of the problem and some "don't care" strings, and does not derive any rejectable inputs. Thus, by Ogden's lemma, for any string z derived by G, there exists a decomposition $z = uvwxy$ such that for all $i \geq 0$, uv^iwx^iy is also derived by G. (cf. Figure 3.4) Such a decomposition is called *a good decomposition*. The author shows that there exist no good decompositions, that is, G is not context-free.

However, Lemma 3.1 is insufficient for our purpose. Since Problem I is a promise problem, an awkward problem emerges that there can be a decomposition such that for some i, uv^iwx^iy is a "don't care" input derived by G. The modified Ogden's lemma, Corollary 3.1, can be applied to the string to which the lemma or the corollary is already applied, so that such an awkward problem can be resolved as follows. If such an awkward decomposition is a good decomposition, there exists a non-terminal symbol X such that $uXy \stackrel{+}{\Rightarrow} uvXxy \stackrel{+}{\Rightarrow} uvwxy = z$, where '$A \stackrel{+}{\Rightarrow} B$' represents that A is derived from B by one or more applications of the production rule of G. For such a z, consider $z' = uXy$ or $z' = w$. By Corollary 3.1, similarly, there exists a decomposition $z' = u'v'w'x'y'$ such that for all $j \geq 0$, $u'v'^jw'x'^jy'$ is also derived

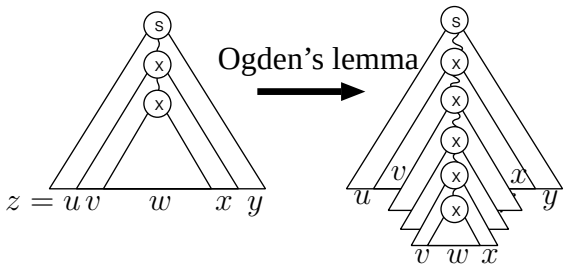

Figure 3.4. Syntax trees of $z = uvwxy$ and uv^iwx^iy generated by G.

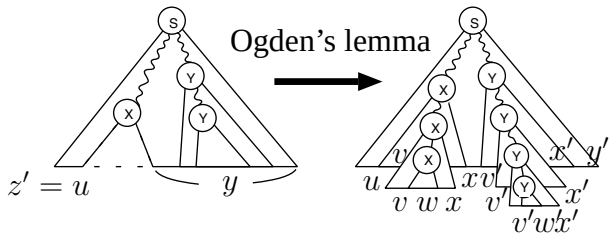

Figure 3.5. Syntax trees of $z' = uXy$ and $(uv^iwx^i..)v'^jw'x'^jy'$ generated by G.

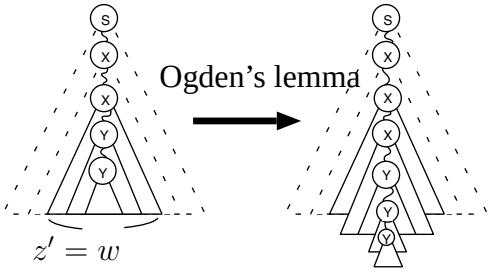

Figure 3.6. Syntax trees of $z' = w$ and $u'v'^j(..v^iwx^i..)x'^jy'$ generated by G.

by G. (cf. Figs. 3.5 and 3.6) In this way, by implementing the independent multi parameter of iterations, say i and j such that $(uv^iwx^i..)v'^jw'x'^jy'$ in Figure 3.5, The author shows the contradiction that for a certain string derived by G, there are no good decompositions.

(Details) Let L_1 be the set of YES instances of Problem I and L_2 be the set of NO instances, with $L_1 \cap L_2 = \phi$. The author shows that no NPAs can recognize any language that contains all $s \in L_1$ but does not contain any $s \in L_2$. Assume that there exists a context-free grammar G by which all $s \in L_1$ and no $s \in L_2$ are derived. By Lemma 3.1, $s \in L_1$ can be decomposed, where $|s| > n$ and n is the constant of the lemma, as $s = uvwxy$ such that for all i, uv^iwx^iy is derived by G.

Consider a string $s_1 = ac_1^N b_1^N \% b_2^N c_2^N \hat{b} b_3^N \%\ b_4^N c_3^N \hat{b} c_4^N \% b_5^N \% c_5^N \in L_1$, where b_i and $\hat{b}$ represent the letters 'b' and c_i does 'c'. Hereafter, throughout this proof, Let $a, \hat{b}$, %, and the leftmost and rightmost letters of the substrings b_i^N $(1 \geq i \geq 5)$ and c_i^N

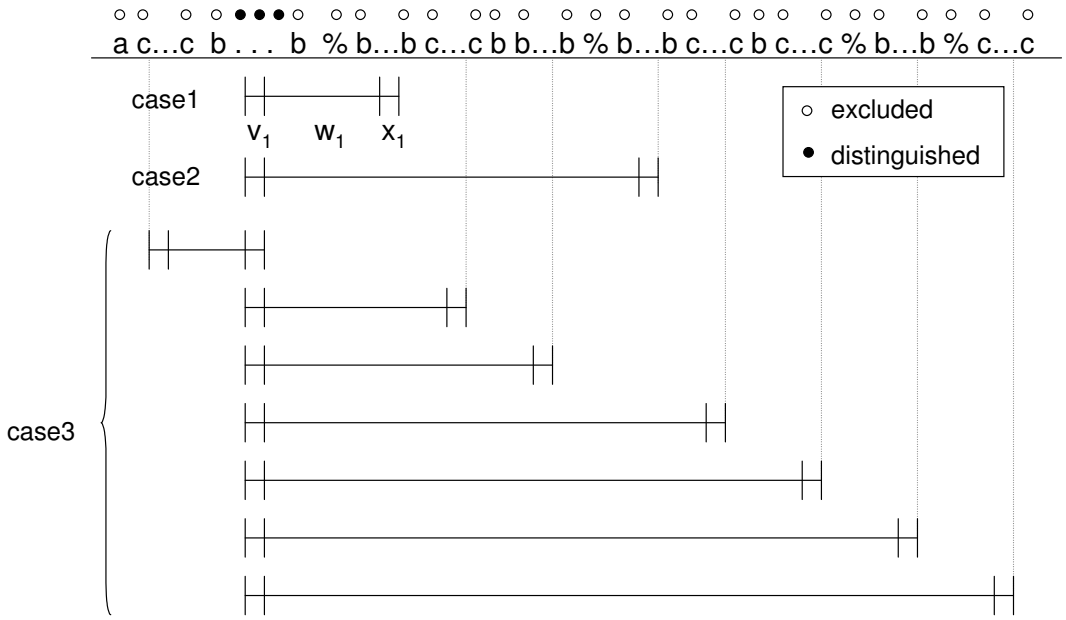

Figure 3.7. Decompositions of Cases 1, 2, and 3.

$(1 \geq i \geq 5)$ be excluded. Let the number of the excluded be $p(= 27)$ and $N = n^p + 2$. Let each letter of b_1's be distinguished except the leftmost and rightmost letters (which are excluded). By Lemma 3.1, $\exists u_1, v_1, w_1, x_1, y_1$ such that $s_1 = u_1 v_1 w_1 x_1 y_1$ and $\forall i \geq 0$, $u_1 v_1^i w_1 x_1^i y_1$ is derived by G. Consider the following three cases as candidates of good decompositions and show that none of them are good decompositions, leading to a contradiction.

Case 1: $v_1 = b_1^+$, $x_1 = b_2^+$, and $|v_1| = |x_1|$;

Case 2: $v_1 = b_1^+$, $x_1 = b_4^+$, and $|v_1| = |x_1|$;

Case 3: others.

Figure 3.7 illustrates intuitively how each case decomposes s_1. Consider Case 1:

$$s_1 = \underbrace{ac_1^N b_1..}_{u_1} \underbrace{...}_{v_1} \underbrace{..b_1 \% b_2..}_{w_1} \underbrace{...}_{x_1} \underbrace{..b_2 c_2^N..c_5^N}_{y_1}.$$

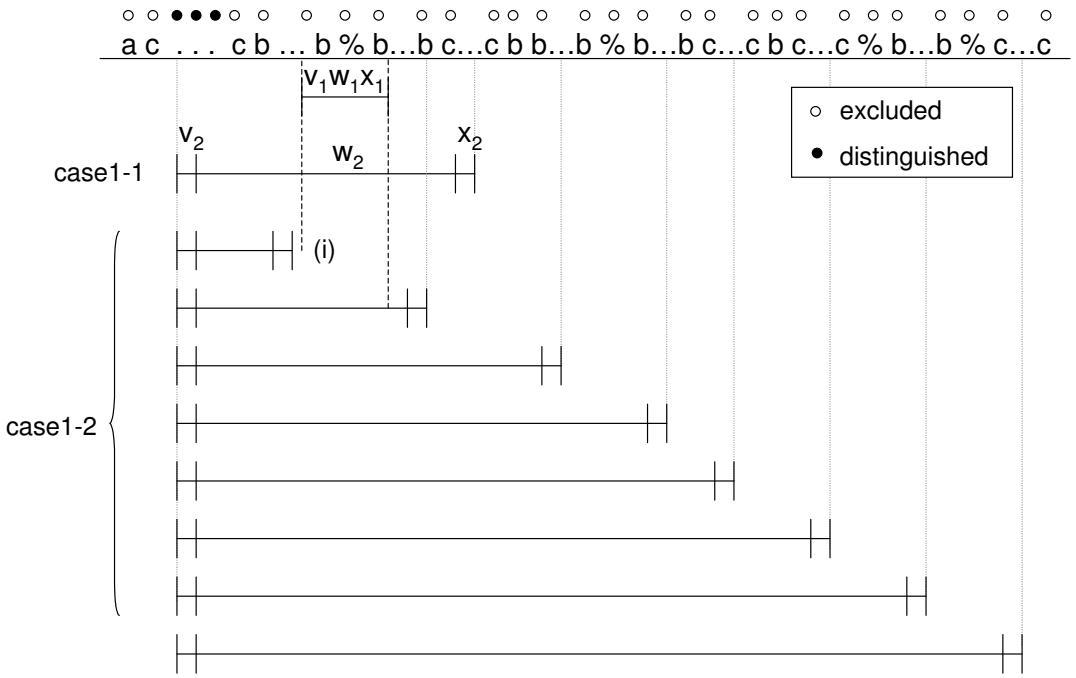

Figure 3.8. Decompositions of Cases 1-1 and 1-2.

Note that for all i, $u_1 v_1^i w_1 x_1^i y_1 \notin L_2$. Consider the string $u_1 X_1 y_1$, where X_1 is a non-terminal symbol such that $u_1 X_1 y_1 \stackrel{+}{\Rightarrow} u_1 v_1 X_1 x_1 y_1 \stackrel{+}{\Rightarrow} u_1 v_1 w_1 x_1 y_1$. Let $s_2 = u_1 X_1 y_1$ and let each letter of c_1's except both end letters be distinguished. By Corollary 3.1, $\exists u_2, v_2, w_2, x_2, y_2$ such that $s_2 = u_2 v_2 w_2 x_2 y_2$ and $\forall j \geq 0$, $u_2 v_2^j w_2 x_2^j y_2$ is derived by G. Consider the following two cases as candidates of good decompositions. (Figure 3.8)

Case 1-1: $v_2 = c_1^+$, $x_2 = c_2^+$, and $|v_2| = |x_2|$;

Case 1-2: other.

Afterward, in this way, the layered decomposition as shown in Figure 3.9 is employed. If none of the lower layers are good decompositions, it is assured that the upper layer is not a good decomposition. Consider Case 1-2 ((i) in Figure 3.8).

$$s_2 = \underbrace{ac_1..}_{u_2}\ \underbrace{...}_{v_2}\ \underbrace{..c_1 b_1..}_{w_2}\ \underbrace{...}_{x_2}\ ..b_2 c_2..\ \underbrace{X_1}_{v_1 w_1 x_1}\ ...c_5.$$

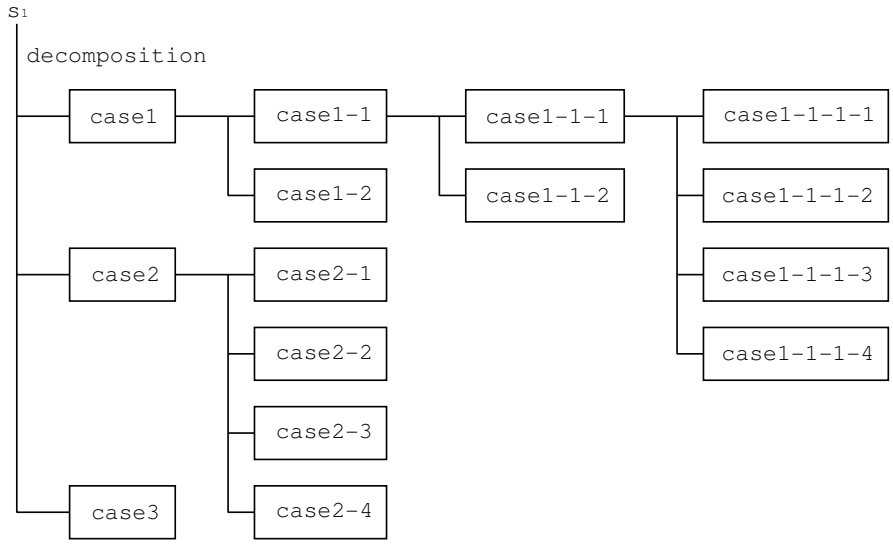

Figure 3.9. Layered decomposition.

For $i = 1$ and $j = 0$, $(u_1v_1^iw_1x_1^iy_1')v_2^jw_2x_2^jy_2 = ac^{N-|v_2|}\ b^{N+|v_1|}\ \%b^{N+|v_1|}\ c^Nbb^N\ \%$ $b^Nc^Nbc^N\ \%b^N\%c^N \in L_2$. Thus, this is not a good decomposition. Similarly, all of the others in Case 1-2 are not good decompositions. Next, consider Case 1-1. Note that for all i and j, $u_2v_2^j(..v_1^iw_1x_1^i..)x_2^jy_2 \notin L_2$. Let X_2 be a non-terminal symbol such that $u_2X_2y_2 \stackrel{+}{\Rightarrow} u_2v_2X_2x_2y_2 \stackrel{+}{\Rightarrow} u_2v_2w_2x_2y_2$. Let $s_3 = u_2X_2y_2$ and let each letter of b_5's except both end letters be distinguished. By Corollary 3.1, $\exists u_3, v_3, w_3, x_3, y_3$ such that $s_3 = u_3v_3w_3x_3y_4$ and $\forall k \geq 0$, $u_3v_3^kw_3x_3^ky_3$ is derived by G. Consider the following two cases as candidates of good decompositions. (Figure 3.10)

Case 1-1-1: $v_3 = b_3^+$, $x_3 = b_5^+$, and $|v_3| = |x_3|$;

Case 1-1-2: others.

In Case 1-1-2, it can be shown that there exist some i, j, and k such that respective decompositions are not good decompositions, for example, the case $i \neq k$. Next, consider Case 1-1-1. Note that for all i, j and k, $(u_2v_2^j(..u_1^iw_1x_1^i..)x_2^j..)v_3^kw_3x_3^ky_3 \notin L_2$. Let X_3 be a non-terminal symbol such that $u_3X_3y_3 \stackrel{+}{\Rightarrow} u_3v_3X_3x_3y_3 \stackrel{+}{\Rightarrow} u_3v_3w_3x_3y_3$. Let $s_4 = w_3$ and let each letter of c_3's except both end letters be distinguished. By Corollary 3.1, $\exists u_4, v_4, w_4, x_4, y_4$ such that $s_4 = u_4v_4w_4x_4y_4$ and $\forall l \geq 0$, $u_4v_4^lw_4x_4^ly_4$

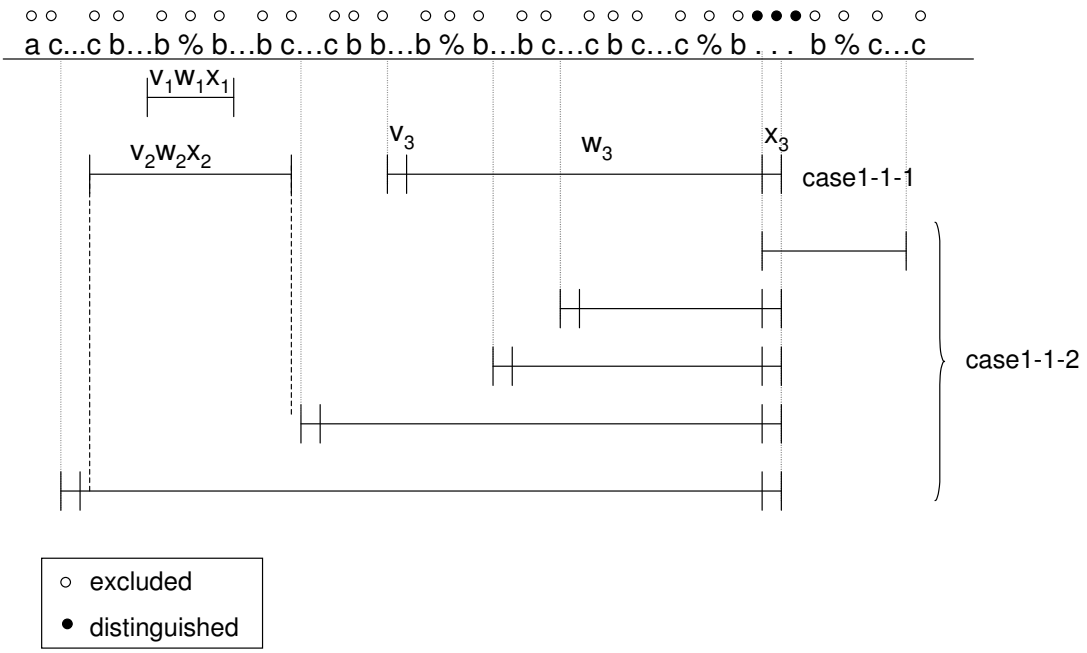

Figure 3.10. Decompositions of Cases 1-1-1 and 1-1-2.

is derived from X_3 by G. Consider the following four cases as candidates of good decompositions. (Figure 3.11)

Case 1-1-1-1: $v_4 x_4 = c_3^+$;

Case 1-1-1-2: $v_4 = b_4^+$, $x_4 = c_3^+$;

Case 1-1-1-3: $v_4 = c_3^+$, $x_4 = c_4^+$;

Case 1-1-1-4: others.

Consider Case 1-1-1-1. Note that for all i, j, k and l, $(u_2 v_2^j (..u_1^i w_1 x_1^i ..) x_2^j ..) v_3^k (..u_4^l w_4 x_4^l ..) x_3^k y_3 \notin L_2$. Let X_5 be a non-terminal symbol such that $u_5 X_5 y_5 \stackrel{+}{\Rightarrow} u_5 v_5 X_5 x_5 y_5 \stackrel{+}{\Rightarrow} u_5 v_5 w_5 x_5 y_5$. Let $s_5 = u_3 X_3 y_3$ and let each letter of c_5's except both end letters be distinguished. By Corollary 3.1, $\exists u_5, v_5, w_5, x_5, y_5$ such that $s_5 = u_5 v_5 w_5 x_5 y_5$ and $\forall m \geq 0$, $u_5 v_5^m w_5 x_5^m y_5$ is derived by G. Consider the following five cases. (Figure 3.12)

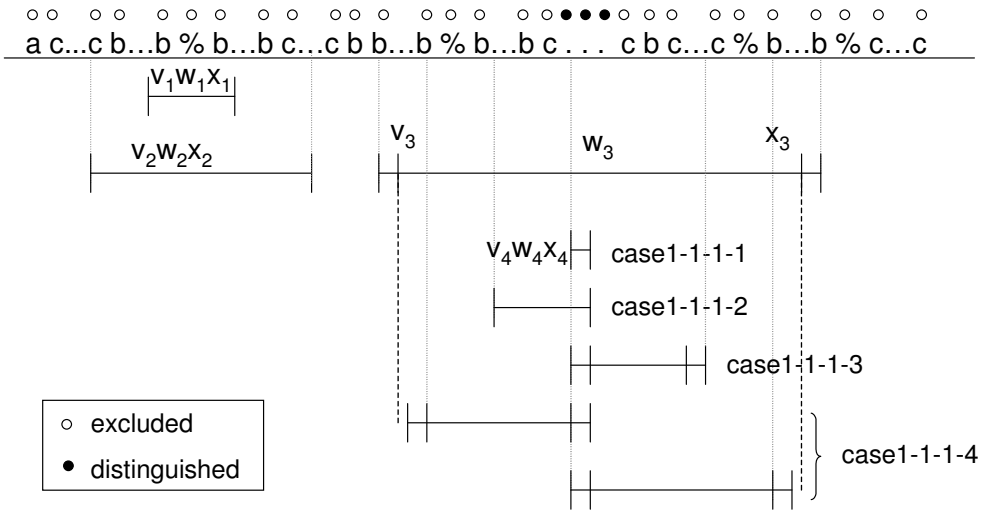

Figure 3.11. Decompositions of Cases 1-1-1-1, 1-1-1-2, 1-1-1-3, and 1-1-1-4.

$$v_5x_5 = c_5^+, \tag{3.8}$$

$$v_5 = b_5^+ \; and \; x_5 = c_5^+, \tag{3.9}$$

$$v_5 = b_3^+ \; and \; x_5 = c_5^+, \tag{3.10}$$

$$v_5 = c_2^+ \; and \; x_5 = c_5^+, and \tag{3.11}$$

$$v_5 = c_1^+ \; and \; x_5 = c_5^+. \tag{3.12}$$

As shown below, for each of the above there exist i, j, k, l, and m such that the iterated string is in L_2.

In case (3.8), for $i = j = k = 1$, $(l-1)|v_4x_4| = (m-1)|v_5x_5|$, $ac^Nb^N\%b^Nc^Nbb^N\%b^Nc^{N_1}bc^N\%b^N\%c^{N_2} \in L_2$, where $N_1 = N + (l-1)|v_4x_4|$ and $N_2 = N + (m-1)|v_5x_5|$.

In case (3.9), for $i = j = k = 1, l = m = 0$, $ac^Nb^N\%b^Nc^Nbb^N\%b^Nc^{N_1}bc^N\%b^{N_2}\%c^{N_3} \in L_2$, where $N_1 = N - |v_4x_4|$, $N_2 = N - |v_5|$ and $N_3 = N - |x_5|$.

In case (3.10), for $i = j = k = 1, l = m = 0$, $ac^Nb^N\%b^Nc^Nbb^{N_1}\%b^Nc^{N_2}bc^N\%b^N\%c^{N_3} \in L_2$, where $N_1 = N - |v_5|$, $N_2 = N - |v_4x_4|$ and $N_3 = N - |x_5|$.

In case (3.11), for $i = j = k = l = 1$, and $m = 2$, $ac^Nb^N\%b^Nc^{N_1}bb^N\%b^Nc^Nbc^N\%b^N\%c^{N_2} \in L_2$, where $N_1 = N + |v_5|$ and $N_2 = N + |v_4x_4|$.

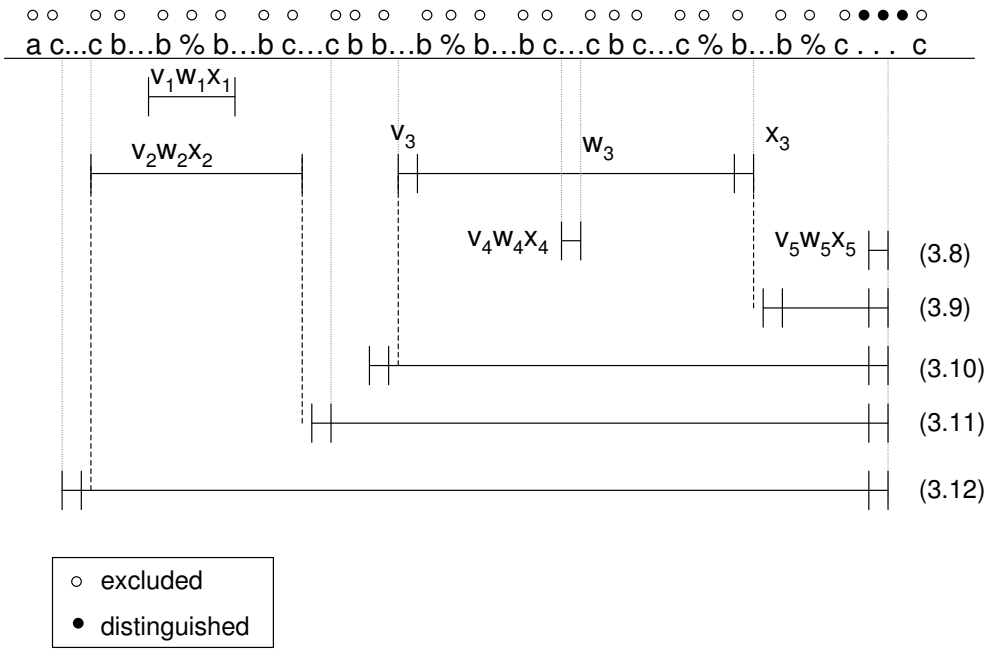

Figure 3.12. Decompositions of Cases (3.8),...,(3.12).

In case (3.12), for $i = j = k = l = 1$, and $m = 0$, $ac^N b^N \% b^N c^{N_1} b b^N \% b^N c^N b c^N \% b^N \% c^{N_2} \in L_2$, where $N_1 = N - |v_5|$ and $N_2 = N - |v_4 x_4|$.

These cases similarly go for the other cases, Cases 1-1-1-2, 1-1-1-3, and 1-1-1-4. Thus, Case 1 is not a good decomposition.
Cases 2 and 3 are also similar to Case 1. Therefore, there exist no good decompositions on $s_1 \in L_1$.

□

3.5. Conclusion

This chapter showed that QPAs can solve a certain problem deterministically. The inputs of the problem are strings in form of $x\%y\%z\%y'\%z'$. To construct such QPAs, two sub-QPAs are utilized, where one examines some relationships among x and y and y', and the other examines some relationships among x and z and z'. The two sub-QPAs ran in parallel and utilized Deutsch-Jozsa algorithm, which is a deterministic

quantum algorithm for Deutsch's XOR problem. Furthermore, it is shown that no DPAs can solve the problem by using extended generalized Ogden's lemma in the fourth section. These results lead to the conclusion that the quantum computational model would have the stronger power than the classical counterpart, even under the restricted circumstance such as the stack memory.

Chapter 4

Quantum Secure Direct Communication Protocol

4.1. Introduction

Although finding a perfectly secure secret communication protocol has been one of the most considerable issues in human history, we do not have any absolute solution yet. The dilemma that a secure key distribution is needed for a secure data transmission seems to be resolved by the appearance of public key cryptosystems (PKCs). However, they have several non negligible problems, e.g., the heavy workload and the security based on the computational assumption. Furthermore, most of the current PKCs are considered to be defeated by quantum computers. The quantum key distribution (QKD) protocol [4] realized a key distribution with unconditional security, which is not based on any computational assumption. This is a protocol by which distant two parties can have the same random private classical key by using quantum devices. This so-called BB84 triggered the growth of constructions of secure quantum cryptosystems. These days, there are so many QKD algorithms and the unconditional security of each protocol is discussed from various angles. QKD stands on the position that, for safe data transmission, it is enough to agree on the same key by communicators securely.

These days, different approaches of quantum secret communication protocols have been taken, and especially I focus on one of them, which is called quantum secure direct communication (QSDC) protocol [6, 7, 10, 14, 19, 22, 23, 26]. A QSDC protocol

basically enables a direct secret transmission without key agreement in the process. Compared to QKD, QSDC has a big difference that a sender can transfer the *desired* data, not random. This dissertation proposes a new QSDC protocol, which has some advantages over the other QSDCs and some QKDs. Every current QSDC has any of the following undesirable features: the secret information is restricted to be classical and many EPR pairs or GHZ states are required. In particular, the latter is not a good feature because of the technical difficulty. As for the security, they have not disscussed it information theoretically.

It is the first time to propose a QSDC protocol which solves these problems at the same time and provide a sophisticated security criterion.

ADVANTAGES: First, it can carry an unknown quantum state. This implies that the protocol can be used as a quantum communication scheme between two hubs of a quantum network. Second, no entanglement resource is employed in the protocol. This is an advantage in feasibility. In addition, an eavesdropper on a channel can be detected efficiently. In general, many decoy qubits are required to increase the detection rate, however, in our protocol, the *message shuttle* increases the detection rate and decreases the information an eavesdropper has at her hand as well. Besides, our protocol tolerates against Photon-Number-Splitting (PNS) attacks, because the encoding operations applied to the secret quantum state never be announced at any step of the protocol. So, even if an eavesdropper could obtain a perfect copy of the coded secret qubit, it is insufficient for unveiling the secret perfectly. Thus, an ideal photon generator is not required in our protocol.

SECURITY: Obviously the PNS attack is not the only eavesdropping. This dissertation shows that our protocol is secure against the *man-in-the-middle attack* that an eavesdropper pretends to be a legitimate receiver. The probability that the attack goes well is extremely small, or the quality of the copy of the secret gets really worse if the eavesdropper wants to decrease the detection probability. It should be noted that the quality of the copy, that is the information quantity the eavesdropper obtains, is discussed in terms of the *fidelity*, which is introduced as a new security criterion.

This chapter is organized as follows. In the next section, Section 2, several basics required to understand the security proof are explained. Section 3 presents a new QSDC protocol. Section 4 introduces a new security criterion and shows that the protocol is secure against the man-in-the-middle attack. Section 5 concludes this chapter.

4.2. Asymmetric Universal Cloning Machine and the Depolarizing Probability

Consider an asymmetric universal cloning machine whose two copies emerge from depolarizing channels. Through the channel, a quantum state ρ is depolarized as it is replaced by the maximally mixed state, $I/2$, with probability p and it is left untouched with probability $1-p$. The consequent quantum state, $\mathcal{E}_p(\rho)$, is described as

$$\mathcal{E}_p(\rho) = (1-p)\rho + pI/2. \tag{4.1}$$

The fidelity of $\mathcal{E}_p(\rho)$ is described as

$$\begin{aligned} & F(\rho, \mathcal{E}_p(\rho)) \\ = \; & Tr\sqrt{\rho}\{(1-p)\rho + pI/2\}\sqrt{\rho} \\ = \; & 1 - \frac{p}{2}. \end{aligned} \tag{4.2}$$

Because, for arbitrary ρ, $I/2 = (\rho + \sigma_x\rho\sigma_x^\dagger + \sigma_y\rho\sigma_y^\dagger + \sigma_z\rho\sigma_z^\dagger)/4$, where σ_x, σ_y and σ_z are the Pauli operators, (4.1) can be rewritten as follows.

$$\begin{aligned} \mathcal{E}_p(\rho) &= (1 - \frac{3p}{4})\rho + \frac{p}{4}(\sigma_x\rho\sigma_x^\dagger + \sigma_y\rho\sigma_y^\dagger + \sigma_z\rho\sigma_z^\dagger) \\ &= (1-p')\rho + \frac{p'}{3}(\sigma_x\rho\sigma_x^\dagger + \sigma_y\rho\sigma_y^\dagger + \sigma_z\rho\sigma_z^\dagger), \end{aligned}$$

where $p' = 3p/4$. The depolarizing channel can regarded as the noise such that the operators σ_x, σ_y and σ_z are applied to the quantum state ρ with the isotropic error probability $p'/3$.

Now, consider that the two copies of ρ emerge from the depolarizing channels of probabilities p and q. Let their isotropic error probabilities be $p'/3(= p/4)$ and $q'/3(= q/4)$, respectively, and then the relationship between p' and q' must satisfy the *no-cloning inequality* [8],

$$p' + \sqrt{p'q'} + q' \geq 3/4.$$

Therefore,

$$p + \sqrt{pq} + q \;\; \geq \;\; 1. \tag{4.3}$$

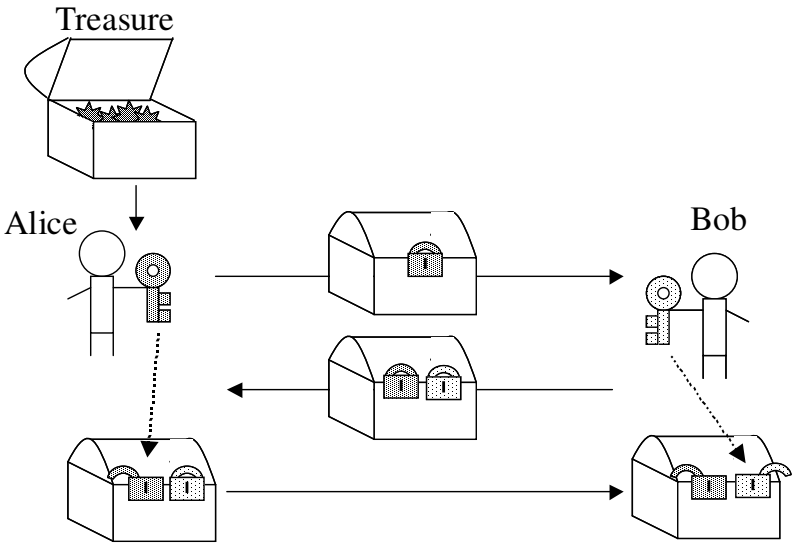

Figure 4.1. Physical implementation.

4.3. The Model and Protocol

First, the key idea of our direct communication protocol is illustrated in Figure 4.1. Consider the situation that a sender, Alice, wants to send a secret message to a receiver, Bob, securely, but they have no encoding-key agreement in advance.

Physically, they achieve the purpose as in Figure 4.1. Alice has a treasure box and wants to send it to Bob. First, Alice locks the box. She holds the key in her hands and sends the box to Bob by post or something. Bob can never open it unless he has Alice's key. He puts a new lock on the box, and holds his key and sends the box back to Alice. Alice opens her lock and sends the box to Bob. Finally, Bob gets the treasure just by his key. At every transmission, the box is locked by either key. An outsider who does not have the keys cannot open the box.

This method has both of advantage and disadvantage. The advantage is that this method needs no key agreement. A sender and a receiver simply have their private keys in their keeping. This means the tolerance of some attacks like PNS attack. The disadvantage is that the classical (digital) implementation of this method cannot achieve good security against the man-in-the-middle attack.

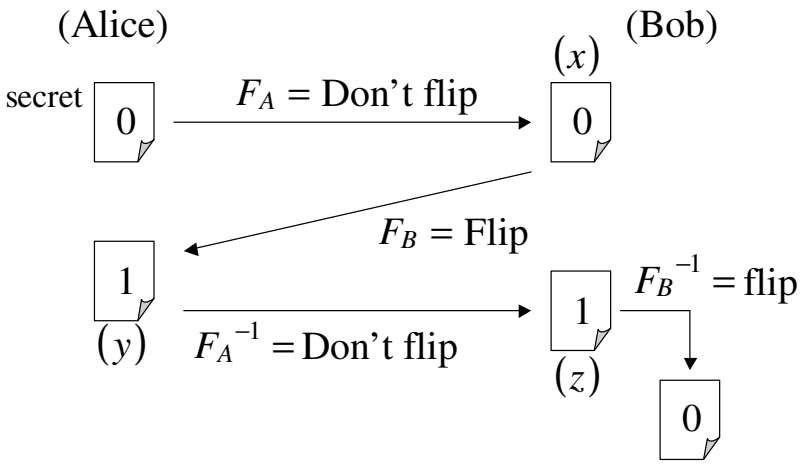

Figure 4.2. Digital implementation.

4.3.1 Classical implementation and the problem

Figure 4.2 illustrates a digital implementation. Alice has a secret bit, s, say 0 in the figure for simplicity. She encodes it by operation F_A="Don't flip" for example and sends $x = F_A(s) = 0$ to Bob. Bob similarly encodes the data by operation F_B="Flip" (independent from F_A) and sends $y = F_B(x) = 1$ back to Alice. Alice decodes the bit by F_A^{-1} ="Don't flip" and sends $z = F_A^{-1}(y) = 1$ to Bob. Bob decodes z the bit by F_B^{-1} ="Flip" and gets the secret data, 0.

An eavesdropper, Eve, keeps watching the transmission channel. She makes a copy of every transmitted data, x, y and z and gets the secret since $x \oplus y \oplus z = s$. The reasons why she needs no special efforts to get the secret data are as follows:

- the data encoding is whether flip or not;
- anybody can see the transmitted data without destruction; and
- anybody can make a perfect copy of the transmitted data.

Consider the following naive quantum implementation.

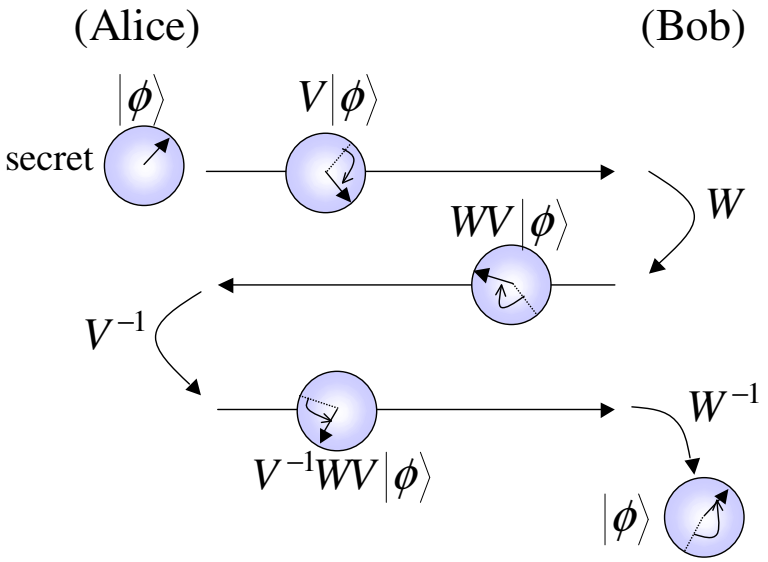

Figure 4.3. The naive quantum implementation.

4.3.2 Quantum implementation

Figure 4.3 illustrates the framework of our quantum implementation. Alice has a secret of a single-qubit state to be sent which is described as a unit-length vector of Bloch sphere, $|\phi\rangle$. Let S be Pauli group, i.e., $S = \{I, \sigma_x, \sigma_y, \sigma_z\}$. Alice chooses an operator $V \in S$ randomly, applies it to $|\phi\rangle$, and sends it to Bob through a quantum channel. (Needless to say, the transmitted quantum state appears as a maximally mixed state for others.) Bob also independently chooses an operator, $W \in S$, applies it to $V|\phi\rangle$, and sends it back to Alice. Alice applies $V^\dagger$ to $WV|\phi\rangle$ and sends it to Bob. Last of all, Bob applies $W^\dagger$ to $V^\dagger WV|\phi\rangle$ and gets the secret, $|\phi\rangle$.

In this implementation, the eavesdropping as in the classical implementation does not work well, because

- nobody can "see" the state of the qubit and calculate the difference between arbitrary two quantum states without destruction; and
- nobody can make a perfect copy of an unknown quantum state.

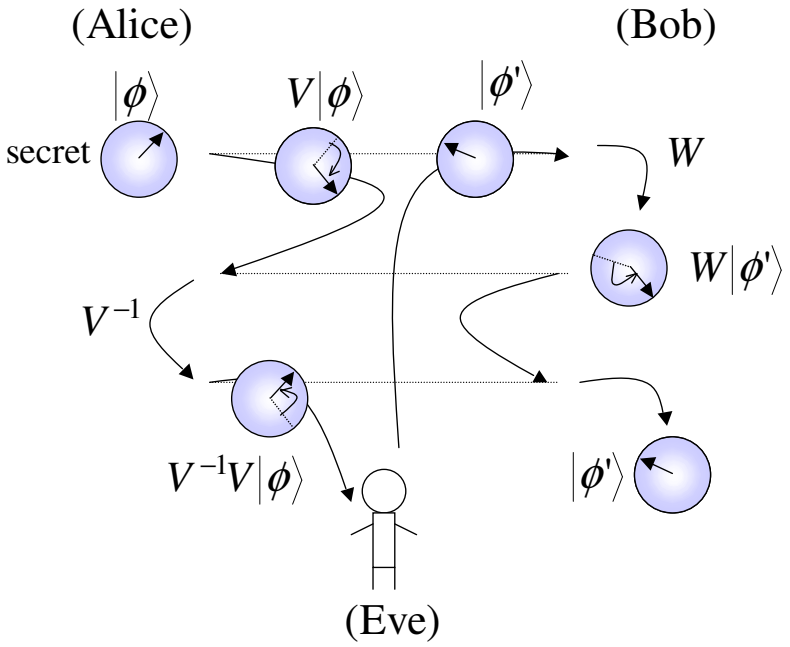

Figure 4.4. Eve's man-in-the-middle attack.

However, Eve can make an active attack as in Figure 4.4, the man-in-the-middle attack. Eve intercepts the transmitted qubit from Alice to Bob and gets it back to Alice directly, pretending she is Bob. Alice opens her lock and sends state $V^{\dagger}V\,|\phi\rangle$ to Bob. Eve has only to steel the qubit.

This weak and naive implementation is improved as the following QSDC protocol.

4.3.3 The model of our protocol

The model of the proposed protocol is defined as follows. There are two noiseless channels between Alice and Bob, an unauthenticated quantum channel and an authenticated classical public channel. This dissertation does not consider the loss of qubits and assumes that the quantum communication devices, e.g., a photon generator and a detector, are ideal instruments which don't make any mistakes. Alice and Bob, in advance, agree on a set of unitary operators, S, such that for any two distinct elements

V and W in S, $W^\dagger V^\dagger W V \left|\phi\right\rangle = e^{i\theta} I \left|\phi\right\rangle$ and $\sum_{V \in S} \frac{1}{|S|} V \left|\phi\right\rangle \left\langle\phi\right| V^\dagger$ is a maximally mixed state, Pauli group for example.

4.3.4 The procedure

The numbers k and r are determined in advance based on the security parameter, where k is the number of decoy qubits and r is the total number of rounds.

(P1) **(Setup)** Alice has a secret of a single-qubit state. Set $i = 1$.

(P2) **(Alice's encoding phase)** If $i = r$, jump to phase (P5). Alice chooses an operation, V_i, from S randomly and applies it to the secret qubit. Alice newly prepares k qubits (decoys), where each is in a random initial state in the 2-dimensional Hilbert space. Alice randomly picks out one position from $k + 1$ positions and puts the encoded secret there and the decoys in the other positions at random. Alice sends the sequence of the qubits (the secret and the decoys) to Bob.

(P3) **(Bob's encoding phase)** Bob randomly chooses $k + 1$ operators from S and applies them to the received sequence. He permutes the order of the sequence and sends it back to Alice. At this moment, he does not know which operation is applied to the secret, but, let the operation be W_i for convenience.

(P4) **(Detection phase)** Alice informs Bob of the reception and the positions of decoys in phase (P2). Bob announces his permutation and the operators applied to decoys through the classical channel. By using these information, Alice cancels Bob's operations for decoys and runs a detection test, which is the measurement of every decoy with respect to the initial state and its orthonormal state. When the answer is not "being in the initial state," Alice and Bob abort this protocol. Otherwise, set $i = i + 1$. Return to phase (P2).

(P5) **(Alice's decoding phase)** Alice applies $V_i = (V_{i-1} V_{i-2} \cdots V_1)^\dagger$ to the secret qubit. Alice prepares k decoys in random states and randomly picks out one position from $k + 1$ positions and puts the secret qubit there and the decoys in the other positions at random. Alice sends the sequence to Bob.

(P6) **(Detection phase)** Bob informs Alice of the reception. Alice announces the position of decoys and their states. Bob runs the detection test similarly to phase (P4). If any of the decoys has changed, they abort this protocol.

(P7) **(Bob's decoding phase)** Bob applies $W_i = (W_{i-1}W_{i-2}\cdots W_1)^\dagger$ to the secret qubit and gets the original secret.

In the protocol, resending the secret is restricted, because it is impossible to make a perfect copy of an unknown quantum state. The issue is left out of consideration in this dissertation.

4.4. The security analysis of the proposed protocol

Eve cannot directly know the secret even if she keeps watch on the channel because every quantum state on the channel is maximally mixed. In our protocol, a sender and a receiver do not have an encoding-key agreement in advance nor in the process nor afterward, but instead they individually encode the secret by their private keys, and *shuttle* it any number of times. Their encodings are the sequences of all the quantum operations that they choose randomly at all rounds but the last, and so the subsequence is of no help in decoding. Thus, if once Bob applies an operation to the secret, there is no chance intuitively for Eve to remove the operation, because the quantum state to which his operation is applied goes into a maximally mixed state and she cannot recover the information.

4.4.1 The model of Eve's man-in-the-middle attack

An eavesdropper, Eve, wants to steal the secret information without being detected. As in Figure 4.4, she attempts to intercept the transmission and keep the secret qubit from Bob. Figure 4.5 illustrates her attack generally at a round-trip. Eve intercepts both the transmitted ways, the way from Alice to Bob and the way to return to Alice. Eve's attack can be generalized as follows. Eve can intercept the transmitted quantum system, S, which is a composite system of both the secret qubit and decoys. Then, she prepares an ancillary system A and applies a unitary operation $\hat{E}$ on $\varphi \otimes \omega$, where φ

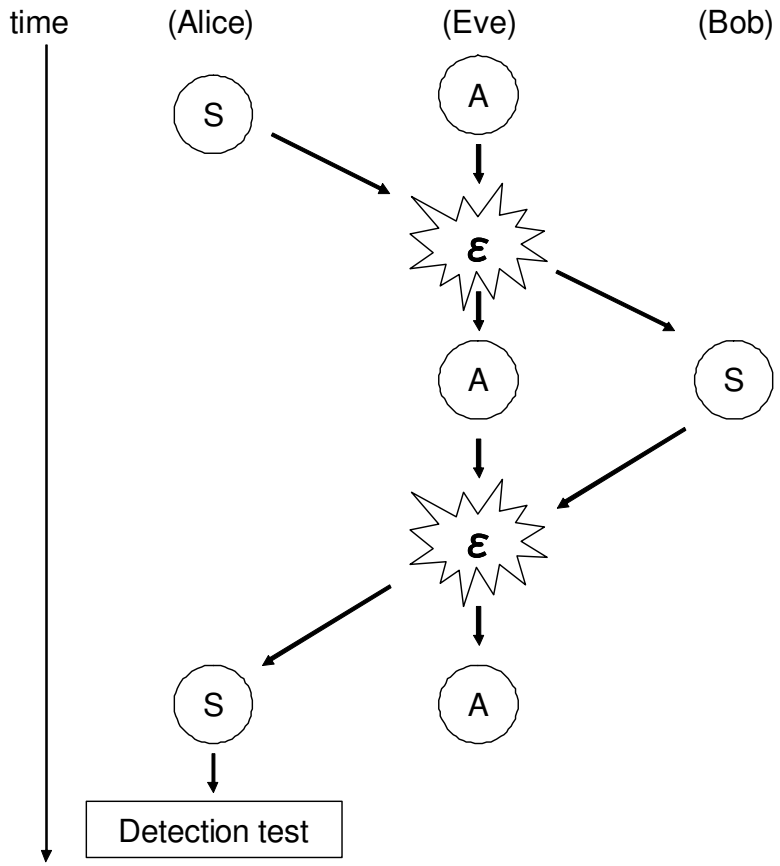

Figure 4.5. Eve's attack. S and A are the quantum systems. $\mathcal{E}$ is some sort of operation.

and ω are the quantum states of S and A, respectively. Let $\mathcal{E}$ be this Eve's attack, and the outcoming state φ' is

$$\varphi' = \mathcal{E}(\varphi) = Tr_A\{\hat{E}(\varphi \otimes \omega)\hat{E}^\dagger\}.$$

Eve sends φ' to Bob/Alice.

This dissertation considers the specific attack model suited for her purpose as follows. Figure 4.6 illustrates the flow of a single-qubit state in our protocol with Eve, especially the secret qubit for simplicity, but, the following Eve's attack is for every qubit. $|\psi_0\rangle$ is the secret state. Alice and Bob have r round-trips. ρ_i and ρ_i' are the mixed states Alice sends and Bob receives in the first-half of the i-th round, respectively. η_i and η_i' are the mixed states Bob sends and Alice receives in the last-half of the

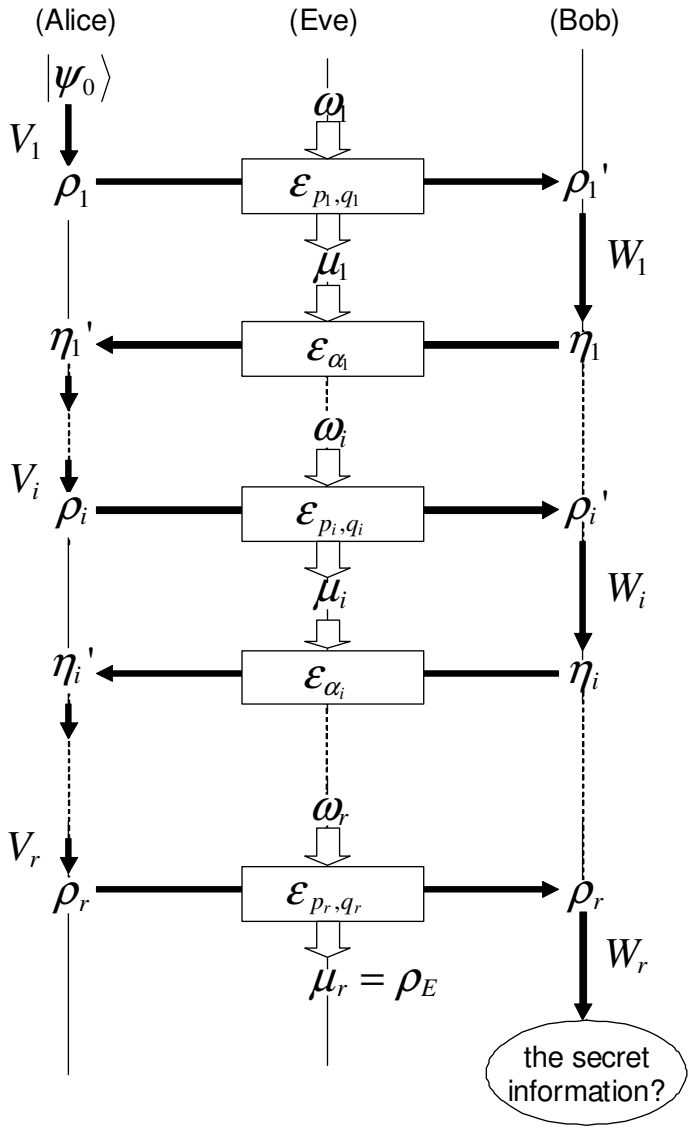

Figure 4.6. The flow under the influence of Eve's attack. The classical auxiliary information is omitted.

i-th round, respectively. V_i and W_i are Alice's and Bob's operations in S, respectively. Note that $V_r \cdots V_1 = I$ and $W_r \cdots W_1 = I$. Eve clones the whole quantum system on the way from Alice to Bob. $\mathcal{E}_{p_i,q_i}$ means such a cloning channel, a *depolarizing channel*, where p_i and q_i relates the accuracy of the clones μ_i and ρ_i', respectively. She keeps one of the clones in her hands and sends the other one to Bob. Then, in order to gain the secret information, Eve would replace η_i with μ_i on the way back to Alice. The accuracy of the eavesdropping rests on the fidelity between the state ρ_i and the actual returning state η_i'. But, the lower the fidelity between the appropriate state $W_i \rho_i W_i^\dagger$ and η_i' is, the higher the detection probability at the subsequent test is. Thus, Eve should make an attack such that both the fidelities are high concurrently, that is, she returns a mixture of μ_i and η_i as η_i':

$$\eta_i' = \alpha_i \mu_i + (1 - \alpha_i)\eta_i,$$

where α_i is a classical probability. Eve has to repeats this attack at every round, for the reason mentioned above. At the last r-th round, a clone of ρ_r Eve makes is the clone of the secret $|\psi_0\rangle$ in this attack. Let the clone be ρ_E.

4.4.2 The security analysis

Let us start with the preparations for the security analysis. μ_i and ρ_i' are the two copies of ρ_i which emerge from depolarizing channel $\mathcal{E}_{p_i,q_i}$ as seen in Section 4.2. Then, by (4.1), they can be rewritten as

$$\begin{aligned} \mu_i &= (1 - p_i)\rho_i + p_i I/2 \\ \rho_i' &= (1 - q_i)\rho_i + q_i I/2. \end{aligned}$$

Thus,

$$\begin{aligned} \rho_i &= V_i \eta_{i-1}' V_i^\dagger \\ &= V_i \{\alpha_{i-1}\mu_{i-1} + (1 - \alpha_{i-1})I/2\} V_i^\dagger \\ &= V_i \{\alpha_{i-1}\{(1 - p_{i-1})\rho_{i-1} + p_{i-1} I/2\} + (1 - \alpha_{i-1})I/2\} V_i^\dagger \\ &= \alpha_{i-1}(1 - p_{i-1}) V_i \rho_{i-1} V_i^\dagger + (1 - \alpha_{i-1}(1 - p_{i-1}))I/2 \\ &\cdots \\ &= \prod_{m=1}^{i-1} \alpha_m (1 - p_m) V_i \cdots V_1 |\psi_0\rangle \langle\psi_0| V_1^\dagger \cdots V_i^\dagger + \{1 - \prod_{m=1}^{i-1} \alpha_m (1 - p_m)\} I/2. \end{aligned}$$

Here, let $|\psi_i\rangle = V_i \cdots V_1 |\psi_0\rangle$ and rewrite ρ_i simply as follows:

$$\rho_i = \prod_{m=1}^{i-1} \alpha_m (1-p_m) |\psi_i\rangle \langle\psi_i| + \{1 - \prod_{m=1}^{i-1} \alpha_m (1-p_m)\} I/2. \quad (4.4)$$

By (4.4), μ_i can be rewritten with $|\psi_i\rangle$ as follows.

$$\begin{aligned} \mu_i &= (1-p_i)\rho_i + p_i I/2 \\ &= \prod_{m=1}^{i-1} \alpha_m \prod_{m=1}^{i} (1-p_m) |\psi_i\rangle \langle\psi_i| + \{1 - \prod_{m=1}^{i-1} \alpha_m \prod_{m=1}^{i} (1-p_m)\} I/2. \end{aligned} \quad (4.5)$$

Now we are ready to go to the security analysis. First, a new security criterion is defined.

Definition 4.1. *A protocol is secure if and only if an eavesdropper can obtain the information about the secret message with the fidelity* $|F(|\psi_0\rangle \langle\psi_0|, \rho_E) - 1/2| \leq O(2^{-s})$*, where* $|\psi_0\rangle$ *is the state of the original secret;* ρ_E *is the clone state of* $|\psi_0\rangle$ *Eve reconstructs; and* s *is the security parameter the sender decides.*

Theorem 4.1. *When Alice and Bob use a constant number of decoys (say* c *decoys) and repeat the rally* $4s$ *times, our protocol is secure against the man-in-the-middle attack defined above.*

Before the proof of this theorem, several lemmas are introduced.

Lemma 4.1. *If* $F(\rho_i, \rho_i') \geq 1 - O(\delta)$*, then* $F(\rho_i, \mu_i) \leq 1/2 + O(\sqrt{\delta})$.

Proof. Let $F(\rho_i, \rho_i') = F_B$ and $F(\rho_i, \mu_i) = F_E$. By (4.2), $F_B = 1 - q_i/2 \geq 1 - O(\delta)$ and $F_E = 1 - p_i/2$. By no-cloning inequality (4.3), $\sqrt{(1-F_B)(1-F_E)} \geq 1/2 - (1-F_B) - (1-F_E)$. Therefore,

$$\begin{aligned} O(\delta) &\geq 1 - F_B \\ \therefore O(\sqrt{\delta}) &\geq \sqrt{1-F_B} \\ &\geq \sqrt{(1-F_B)(1-F_E)} \\ &\geq 1/2 - (1-F_B) - (1-F_E) \\ &\geq 1/2 - (1-F_E) - O(\delta) \\ \therefore F_E &\leq 1/2 + O(\sqrt{\delta}) \end{aligned}$$

□

Lemma 4.2. *Let ε and δ be positive real numbers less than* 1. *Suppose that for some i, $|F(\rho_i, |\psi_i\rangle\langle\psi_i|) - 1/2| \leq \varepsilon$, where $|\psi_i\rangle = V_i \cdots V_1 |\psi_0\rangle$. If $F(\rho_i, \rho_i') \geq 1 - O(\delta)$, $|F(|\psi_i\rangle\langle\psi_i|, \mu_i) - 1/2| \leq O(\sqrt{\delta}\varepsilon)$.*

Proof. By three equations (4.1), (4.2) and (4.4), the fidelity between ρ_i and $|\psi_i\rangle$ is given as

$$\begin{aligned} F(\rho_i, |\psi_i\rangle\langle\psi_i|) &= 1/2\{1 + \prod_{m=1}^{i-1} \alpha_m(1 - p_m)\}. \\ \therefore \prod_{m=1}^{i-1} \alpha_m(1 - p_m)/2 &\leq \varepsilon. \end{aligned} \tag{4.6}$$

By Lemma 4.1, $F(\rho_i, \mu_i) - 1/2 = 1/2(1 - p_i) \leq O(\sqrt{\delta})$. Therefore,

$$\begin{aligned} F(|\psi_i\rangle\langle\psi_i|, \mu_i) - 1/2 &= 1/2 \prod_{m=1}^{i-1} \alpha_m \prod_{m=1}^{i} (1 - p_m) \\ &= 1/2 \prod_{m=1}^{i-1} \alpha_m (1 - p_m) \cdot (1 - p_i) \\ &\leq O(\sqrt{\delta}\varepsilon). \end{aligned}$$

□

Lemma 4.3. *Suppose that $F(\rho_{i_1}, \rho_{i_1}'), \cdots, F(\rho_{i_{2n}}, \rho_{i_{2n}}') \geq 1 - O(\delta)$, where $i_1, \cdots, i_{2n}$ are mutually distinct, then $|F(|\psi_0\rangle\langle\psi_0|, \rho_E) - 1/2| \leq O(\delta^n)$.*

Proof. Without loss of generality, $i_1 < i_2 < \cdots < i_n$. Suppose $|F(\rho_{i_1}, |\psi_{i_1}\rangle\langle\psi_{i_1}|) - 1/2| = \varepsilon$, then $|F(|\psi_{i_1}\rangle\langle\psi_{i_1}|, \mu_{i_1}) - 1/2| \leq O(\sqrt{\delta}\varepsilon)$ by Lemma 4.2, and thus $1/2 \prod_{m=1}^{i_1-1} \alpha_m \prod_{m=1}^{i_1} (1 - p_m) \leq O(\sqrt{\delta}\varepsilon)$.

$$\begin{aligned} \therefore |F(\rho_{i_2}, |\psi_{i_2}\rangle\langle\psi_{i_2}|) - 1/2| &= 1/2\{\prod_{m=1}^{i_2-1} \alpha_m(1 - p_m)\} \\ &\leq 1/2\{\prod_{m=1}^{i_2-2} \alpha_m(1 - p_m)\} \\ &\leq \cdots \\ &\leq 1/2\{\prod_{m=1}^{i_1-1} \alpha_m(1 - p_m)\} \\ &\leq O(\sqrt{\delta}\varepsilon). \end{aligned}$$

By substitution $O(\sqrt{\delta}\varepsilon)$ with ε in Lemma 4.2, $|F(|\psi_{i_2}\rangle\langle\psi_{i_2}|, \mu_{i_2}) - 1/2| \leq O(\delta\varepsilon)$. By repeated this, $|F(|\psi_{i_{2n}}\rangle\langle\psi_{i_{2n}}|, \mu_{i_{2n}}) - 1/2| \leq O(\delta^n)$. Therefore,

$$\begin{aligned} F(|\psi_0\rangle\langle\psi_0|, \rho_E) - 1/2 &= 1/2 \prod_{m=1}^{r-1} \alpha_m (1 - p_m) \\ &\leq 1/2 \prod_{m=1}^{i_{2n}-1} \alpha_m \prod_{m=1}^{i_{2n}} (1 - p_m) \\ &\leq O(\delta^n). \end{aligned}$$

□

Lemma 4.4. *If $F(\rho_i, \rho_i') < 1 - \Omega(\delta)$, the probability that Eve passes the detection test by Alice in the i-th transmission is $(1 - \Omega(\delta))^k$ at most, where k is the number of decoy qubits.*

Proof. It should be noted that, in our protocol, the qubit carrying the secret message is not an object of the detection test, but every decoy qubit is. First, let us consider the average probability that Eve passes the detection test in the i-th transmission per decoy qubit. Eve returns $\eta_i' = \alpha_i \mu_i + (1 - \alpha_i)\eta_i$ to Alice and Alice performs the detection test on $W_i^\dagger \eta_i' W_i$. The fidelity between $W_i^\dagger \eta_i' W_i$ and ρ_i corresponds to the likelihood that Eve passes the detection test.

$$\begin{aligned} W_i^\dagger \eta_i' W_i &= \alpha_i W_i^\dagger \mu_i W_i + (1 - \alpha_i) W_i^\dagger \eta_i W_i \\ &= \alpha_i W_i^\dagger \mu_i W_i + (1 - \alpha_i)\rho_i' \\ &= \alpha_i W_i^\dagger \{(1 - p_i)\rho_i + p_i I/2\} W_i \\ &\quad + (1 - \alpha_i)\{(1 - q_i)\rho_i + q_i I/2\} \end{aligned} \tag{4.7}$$

Since $W_i^\dagger (I/2) W_i = I/2$,

$$\begin{aligned} (4.7) &= \alpha_i (1 - p_i) W_i^\dagger \rho_i W_i + (1 - \alpha_i)(1 - q_i)\rho_i + \{\alpha_i + (1 - \alpha_i) q_i\} I/2 \\ &= \{\alpha_i (1 - p_i) W_i^\dagger \rho_i W_i + (1 - \alpha_i (1 - p_i)) I/2\} + \\ &\qquad \{(1 - \alpha_i)(1 - q_i)\rho_i + (1 - (1 - \alpha_i)(1 - q_i)) I/2\} - I/2. \end{aligned}$$

Let $\lambda = \alpha_i (1 - p_i) W_i^\dagger \rho_i W_i + (1 - \alpha_i (1 - p_i)) I/2$ and $\xi = (1 - \alpha_i)(1 - q_i)\rho_i + (1 - (1 - \alpha_i)(1 - q_i)) I/2$. By the linearity,

$$F(W_i^\dagger \mu_i W_i, \rho_i) = F(\rho_i, \lambda) + F(\rho_i, \xi) - F(\rho_i, I/2). \tag{4.8}$$

Considering $W_i \in S$,

$$\begin{aligned} \lambda &= \frac{1}{4}\sum_{\sigma_j \in G}\{\alpha_i(1-p_i)\sigma_j^\dagger \rho_i \sigma_j + (1-\alpha_i(1-p_i))I/2\} \\ &= I/2. \\ \therefore F(\rho_i, \lambda) &= 1/2. \\ F(\rho_i, \xi) &= 1/2 + 1/2(1-\alpha_i)(1-q_i). \end{aligned}$$

Therefore,

$$\begin{aligned} (4.8) &= 1/2 + 1/2(1-\alpha_i)(1-q_i) - 1/2 \\ &= (1-\alpha_i)(1-q_i/2) - (1-\alpha_i)/2 \\ &\leq (1-\alpha_i)(1-q_i/2) \\ &\leq 1 - q_i/2 \\ &= F(\rho_i, \rho_i') \end{aligned}$$

By the assumption of this lemma,

$$F(W_i^\dagger \mu_i W_i, \rho_i) \leq 1 - \Omega(\delta).$$

Therefore, the probability that all the k decoys pass the detection test is $(1-\Omega(\delta))^k$. □

The next corollary follows this lemma.

Corollary 4.1. *If for $i = i_1, \cdots, i_n$, $F(\rho_i, \rho_i') < 1 - \Omega(\delta)$, the probability that Alice detects Eve through this protocol is at least $1 - (1-\Omega(\delta))^{kn}$.*

Now, we are ready to prove Theorem 4.1.

(Proof of Theorem 4.1) First, consider the case that an eavesdropper, Eve, makes a 'strong' attack at more than half the rounds such that Bob gets the poor information. In other words, for $i = i_1, \cdots, i_{2s}, \cdots$ (all mutually distinct), $F(\rho_i, \rho_i') \leq 1 - \delta$, where δ is a constant ($0 < \delta < 1/2$). Alice detects Eve by the end with probability

$1-(1-\delta)^{2s\cdot c}$ at least, by Corollary 4.1, and the protocol aborts in the middle. In this case, it is obvious that $F(|\psi_0\rangle\langle\psi_0|, \rho_E) = 1/2$ and she cannot get any information about the secret. With the extremely low probability, $(1-\delta)^{2nc}$, Eve can obtain the full information about the secret, and thus the average fidelity is at most

$$\begin{aligned} F_{avg}(|\psi_0\rangle\langle\psi_0|, \rho_E) &= (1-\delta)^{2nc}\cdot 1 + \{1-(1-\delta)^{2nc}\}\cdot 1/2 \\ &= 1/2 + 1/2(1-\delta)^{2sc}. \end{aligned}$$

Next, consider the case that Eve makes a 'weak' attack at more than half the rounds such that Bob gets the good information. In other words, for $i = i_1, \cdots, i_{2s}, \cdots$ (all mutually distinct), $F(\rho_i, \rho_i') \geq 1-\delta$. By Lemma 4.3,

$$\begin{aligned} |F(|\psi_0\rangle\langle\psi_0|, \rho_E) - 1/2| &\leq O(\delta^s) \\ &\leq O(2^{-s}). \end{aligned}$$

□

4.5. Conclusion

This chapter presented a new QSDC protocol in which the legitimate communicators can have a direct message of quantum states securely; no entanglement resource is employed; and an eavesdropper is detected efficiently. The protocol exploits the features unique to the quantum information processing, such as uncertainty, the no-cloning property, and indistinguishability. The two legitimate communicators have the message shuttle between them and transmit the secret without key-agreement in advance nor in the process nor afterward. Moreover, the protocol does not require a perfect photon emitter which emits just one particle each time. An imperfect photon generator which emits some particles at a time would cause the factual vulnerability in QKD. So, it could be said that the feasibility of the proposed protocol is higher than some other QSDCs or QKDs which rely on the entanglement or ideal devices.

And a new security criterion for the method of sending quantum information using the mathematical metrics, "fidelity', is introduced. The fidelity uniquely determines the distance between the two quantum states and gives a means to determine how alike the states are. It is shown that the proposed protocol satisfies the criterion against

the attack. The fidelity between the original secret state and the copy the eavesdropper creates gets extremely worse if she wants to decrease the detection probability. Conversely, if she wants to get the secret information with good fidelity, she will be detected with extremely high probability.

In conclusion, I have proposed the new quantum secure direct communication protocol under the restricted circumstance such that no entanglement resource and no perfect photon generator are available.

Chapter 5

Conclusion

This thesis found some evidences such that the quantum algorithms would be stronger than the classical counterparts even under the restricted circumstances. Many sophisticated quantum algorithms were proposed and it is generally thought the quantum computation must be more excellent than the classical computation in every scene. However, in fact, the quantum computation requires the particular undesirable restrictions such as the reversibility, the expensive computational resources (e.g., qubits), the severe operational environment, and so on. Thus, in order to take advantage of the quantum information processing technology to do a fine job within the current or the near future technology, it is extremely important to clarify the ability of the quantum computation under the various restricted circumstances. In this thesis, some restricted circumstances are considered and it was shown the quantum algorithms would be excellent even under the circumstances.

The first result is about the quantum computational model with the stack memory, QPAs. It has been already known that QPAs might be more powerful than the classical counterpart in *bounded error scenario*. In other words, the class of the languages recognized by classical finite automata is properly contained in the class of languages recognized by QPAs, and some languages *not* recognized by classical pushdown automata can be probabilistically recognized by QPAs. But no one knews the relationship between QPAs and the classical counterpart in a *deterministic* case. Chapter 3 showed that a QPA can solve a certain problem with certainty which cannot be solved by DPAs.

The second result is about a quantum secret direct communication (QSDC) protocol with a limited number of computational resources. Chapter 4 proposed a new QSDC protocol. The quantum information processing often uses the useful quantum features (e.g., quantum entanglement, no-cloning theorem) to accomplish some *miracle*s such as quantum teleportation, the unconditionally secure key distribution schemes and so on. However, quantum entanglement is very expensive to keep the useful state during the computation. The proposed protocol employs no entanglement. Furthermore, a new security criterion for sending quantum states using the mathematical metrics, fidelity, is introduced. So, it is the first time to introduce the strict criterion in terms of the fidelity of quantum states and give the proof of the security against the man-in-the-middle attack.

It seems that the computational ability of the realistic quantum computer is different from the ideal one. We need to keep pursuing the studies in the future.

Acknowledgements

I would like to express my sincere appreciation to Professor Yasuhiko Nakashima, Professor Hiroyuki Seki, Associate Professor Shigeru Yamashita, and Assistant Professor Masaki Nakanishi of Nara Institute of Science and Technology for thier continuous guidance, helpful suggestions, accurate criticisms and encouragements for this research.

I would also like to express my thanks to Professor Emeritus Katsumasa Watanabe of Nara Institute of Science and Technology for his continuous guidance, helpful suggestions, accurate criticisms and encouragements for this research.

I would also like to express my thanks to Ph.D Manabu Hagiwara of National Institute of Advanced Industrial Science and Technology for discussion and invaluable suggestions, accurate criticisms and helpful support throughout this research.

Thanks are due to all the members of the Professor Nakashima's laboratory for their discussions and helpful supports.

References

[1] A. Ambainis and R. Freivalds, “1-way quantum finite automata: strengths, weaknesses and generalizations,” Proc. of FOCS’98, pp. 332–341, 1998.

[2] C. Bader and A. Moura, “A generalization of Ogden’s lemma,” Journal of the Association for Computing Machinery, vol. 29, no. 2, pp. 404–407, 1982.

[3] C. H. Bennett, “Logical reversibility of computation,” IBM J. Res. Dev., vol. 6, pp. 525–532, 1973.

[4] C. H. Bennet and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” Proc. IEEE International Conf. Computers, Systems, and Signal Processing Math. Nachr., 1984.

[5] R. F. Bonner, R. Freivalds, and M. Kravtsev, “Quantum versus probabilistic one-way finite automata with counter,” Proc. of SOFSEM 2001, LNCS 2234, pp. 181–191, 2001.

[6] K. Boström and T. Felbinger, “Deterministic secure direct communication using entanglement,” Phys. Rev. Lett., 89, 187902, 2002.

[7] Q. Cai and B. Li, “Improving the capacity of the Bostroem-Felbinger protocol,” Phys. Rev. A, 69, 054301, 2004.

[8] N. J. Cerf, “Pauli cloning of a quantum bit, ” Phys. Rev. Lett., 84, 4497, 2000.

[9] R. Cleve, Artur K. Ekert, Chiarra Macchiavello, and M. Mosca, “Quantum algorithms revisited,” Proc. R. Soc. Lond., A 454, pp. 339–354, 1998.

[10] F. G. Deng and G. L. Long, “Secure direct communication with a quantum one-time pad,” Phys. Rev. A, 69, 052319, 2004.

[11] D. Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” Proc. R. Soc. Lond., A 400, pp. 97–117, 1985.

[12] D. Deutsch and R. Jozsa, “Rapid solution of problem by quantum computation,” Proc. R. Soc. Lond., A 439, pp. 553–558, 1992.

[13] R. P. Feynman, “Simulating physics with computers,” Int. J. Theor. Phys., vol. 21, pp. 467–488, 1982.

[14] T. Gao, F. L. Yan and Z. X. Wang, “Quantum secure direct communication by Einstein-Podolsky-Rosen pairs and entanglement swapping,” quant-ph/0406083, 2004.

[15] M. Golovkins, “Quantum pushdown automata,” SOFSEM 2000, LNCS 1963, pp. 336–346, 2000.

[16] L. Grover, “A fast quantum mechanical algorithm for database search,” Proc. of STOC ’96, pp. 212–219, 1996.

[17] A. Kondacs and J. Watrous, “On the power of quantum finite state automata,” Proc. of FOCS ’97, pp. 66–75, 1997.

[18] M. Kravtsev, “Quantum finite one-counter automata,” Proc. of SOFSEM 1999, LNCS 1725, pp. 431–441, 1999.

[19] Y. Li and Y. Liu, “Quantum secure direct communication based on supervised teleportation,” quant-ph/0711282, 2007.

[20] C. Moore and J. P. Crutchfield, “Quantum automata and quantum grammars,” Theoretical Computer Science, 237(1-2), pp. 275–306, 2000.

[21] P.Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comput., 26, pp. 1484–1509, 1997.

[22] J. Wang, Q. Zhang and C. J. Tang, “Quantum secure direct communication without using perfect quantum channel,” quant-ph/0511092, 2005.

[23] J. Wang, Q. Zhang and C. J. Tang, “Quantum secret direct communication based on order rearrangement of single photons,” quant-ph/0603100, 2006.

[24] T. Yamasaki, H. Kobayashi, Y. Tokunaga, and H. Imai, “One-way probabilistic reversible and quantum one-counter automata,” Theoretical Computer Science, 289(2), pp. 963–976, 2002.

[25] T. Yamasaki, H. Kobayashi, and H. Imai, “Quantum versus deterministic counter automata,” Theoretical Computer Science, 334(1-3), pp. 275–297, 2005.

[26] Z. H. Zhang and Z. X. Man, “Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations,” quant-ph/0403218, 2004.

Publication List

Journal papers

• Y. Murakami, M. Nakanishi, S. Yamashita, and K. Watanabe, ”Quantum versus classical pushdown automata in exact computation,” IPSJ Journal, vol. 46, no. 10, pp. 2471–2480, October 2005.

International Conferences

• Y. Murakami, M. Nakanishi, S. Yamashita, Y. Nakashima, and M. Hagiwara, “A quantum secure direct communication protocol for sending a quantum state and its security analysis,” Proc. of the 6th WSEAS International Conference on Information Security and Privacy, pp. 91–97, December 2007.

• Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita, and Y. Nakashima, “A quantum secure direct communication protocol for sending a quantum state and its security analysis,” The Tenth Workshop on Quantum Information Processing (poster presentation), January 2007.

• Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita and Y. Nakashima,“Quantum secure direct communication protocols for sending a quantum state,” Proc. of the 2006 International Symposium on Infromation Theory and its Applications, October 2006.

• Y. Murakami, M. Nakanishi, S. Yamashita, and K. Watanabe, “Quantum pushdown automata that can deterministically solve a certain problem,” Proc. of International Symposium on Mesoscopic Superconductivity and Spintronics, pp. 310–315, March 2004.

Workshops

• Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita and Y. Nakashima,“Quantum secure direct communication protocol for sending a quantum state and its security analysis,” Proc. of Symposium on Cryptography and Information Security, 2D1-2, January 2008.

• Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita and Y. Nakashima,“Quantum secure direct communication protocols for transmitting quantum states,” Proc. of IEICE Technical Report, QIT2006-28, pp. 233–234, May 2006.

• Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita and Y. Nakashima,“No preshared-key quantum secret communication protocol,” Proc. of the 2006 IEICE General Conference, DS-1-12, March 2006.