INFORMATION
SECURITY

Guihua Zeng

Quantum Private Communication

量子保密通信

高等教育出版社
HIGHER EDUCATION PRESS

INFORMATION SECURITY

Guihua Zeng

Quantum Private Communication

量子保密通信

LIANGZI BAOMI TONGXIN

With 96 Figures

高等教育出版社 · 北京
HIGHER EDUCATION PRESS BEIJING

Author

Prof. Guihua Zeng
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, 200240, China
E-mail: ghzeng@sjtu.edu.cn

图书在版编目（CIP）数据

量子保密通信=Quantum Private Communication：英文/曾贵华著.—北京：高等教育出版社，2010.1
（信息安全系列丛书）
ISBN 978-7-04-025479-2

Ⅰ.量… Ⅱ.曾… Ⅲ.量子力学-保密通信-研究-英文 Ⅳ.0413.1 TN918

中国版本图书馆CIP数据核字（2009）第153729号

策划编辑 陈红英　**责任编辑** 陈红英　**封面设计** 张　楠
责任印制 陈伟光

出版发行	高等教育出版社	**购书热线**	010-58581118
社　　址	北京市西城区德外大街4号	**免费咨询**	800-810-0598
邮政编码	100120	**网　　址**	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	涿州市星河印刷有限公司	**畅想教育**	http://www.widedu.com
开　　本	787×1092　1/16	**版　　次**	2010年1月第1版
印　　张	24.25	**印　　次**	2010年1月第1次印刷
字　　数	450 000	**定　　价**	59.00元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 25479-00

Sales only inside the mainland of China
仅限中国大陆地区销售

Preface

Since Wiesner first found that quantum laws may be applied for protecting legitimate information in 1969, the quantum cryptology — a combination of the quantum physics and classic cryptology — has attracted much attention since then. With further investigations, the infrastructure of the quantum cryptology has become more and more clear. To conclude these research results, some excellent books have been devoted to describe various aspects of the quantum cryptology, such as the *Quantum computation and quantum information* by Nielsen and Chuang, *Quantum cryptography and secret-key distillation using quantum cryptography* by Assche, and *Quantum cryptology* by Zeng. As a main application direction of the quantum cryptology, the quantum private communication which combines the quantum cryptology and communication techniques has recently made great progress. By far, various investigations on this aspect have been presented, even some techniques have been applied in practices. This means that the quantum private communication has entered gradually the commerce field. This book devotes to describe fundamental principles, typical schemes, and technical implementations for the quantum private communication.

Because the quantum private communication has currently become a practical reality with products available commercially, it is important to focus not only on the theoretical topics but also on the practical issues. Accordingly, this book arranges the contents from pure theoretical descriptions to practical applications. To reach this aim, a broad range of materials are covered in this book, including how to protect confidentiality and authentication of the private communication using quantum tools and typical techniques for practical applications of quantum private communication in fiber telecommunication systems, wireless optical communication (including satellite communication), IP networks, and mobile communication systems, etc. Consider that cryptology, quantum physics, and information theory are necessary ingredients to build framework of the quantum private communication, brief introduction on these issues is employed to make the book self-consistent.

This book originated out of a graduate course of lectures in Quantum Secure Communication given at the Shanghai Jiaotong University. The content of this book is based on my investigations on the quantum cryptography as well as the quantum private communication since 1997. It aims at giving an introduction on fundamental principles, typical schemes, technical implementations, and practical applications of the private communication in quantum ways. Since the quantum cryptography, and subsequently the quantum private communication is a multi-disciplinary subject, in this respect it may benefit readers with various backgrounds. Thus, this book is suitable for researchers and graduate students in the field of quantum cryptography, classic cryptography, communication engineering, computer science, electronic engineering, quantum physics, and mathematics, etc.

This book addresses systemically some hot topics in the private communication implemented using quantum techniques from fundamental theories to practical application techniques. It contains 9 chapters. Chapter 1 tries to build a quantum private communication model by analogy with the Shannon private communication theory. Then an overview of the quantum private communication is presented. Chapter 2 constructs a quantum security theory which is an important fundament for the quantum private communication. Chapter 3 introduces some preliminaries from the viewpoint of quantum bits, which are associated with basic principles of quantum mechanics. Chapter 4 introduces the well-known quantum key distribution which has been investigated widely. Chapter 5 investigates how to protect the confidentiality using quantum cryptographic algorithms. Chapter 6 demonstrates fundamental principles of implementing quantum authentication, including identity verification, message authentication, quantum signature, and channel authentication. Both Chapters 7 and 8 introduce how to implement physically the quantum private communication using single photon signal and continuous variable quantum signals, respectively. Finally, typical quantum private communication systems in practices are introduced in Chapter 9.

Logically, embodied contents in this book may be divided into three parts, i.e., fundamentals, quantum cryptographic schemes, and technical implementations in practical communication systems. Chapters 1 – 3 consist of the first part which is engaged in building a basic theory model for the quantum private communication from three aspects including information theory, complexity theory, and security theory. To make the book self-consistent, some quantum mechanics principles and mathematical backgrounds are introduced briefly. For those readers who have knowledge on these aspects, one may skip the corresponding sections. Chapters 4 – 6 are regarded as the second part which focuses on discussing how to protect basic security requirements, i.e., confidentiality and authentication, of the modern communication system using quantum techniques. To reach this aim, three aspects are addressed in this part. Since protecting the confidentiality and authentication of the private communication using quantum tools needs firstly to generate a key-pair, the quantum key management is introduced in Chapter 4. This topic is actually a main research issue in the quantum private communication. After that some typical quantum encryption algorithms and quantum authentication schemes are described in this part. Chapters 7 – 9 consist of the final part which focuses on the technical implementations of the quantum private communication in practices. According to the current development, the quantum private communication may be applied possibly in the fiber telecommunication, wireless optical communication, IP networks, and mobile communication systems. All these applications are briefly introduced. Each of the three parts in the book is self-consistent. Accordingly, they may be also regarded as independent parts, respectively. Readers may only read the parts interested although the author recommends to read throughout this book. This will not influence the understanding on the corresponding contents.

Guihua Zeng
Shanghai, November 2009

Acknowledgements

I would like to thank many researchers and collaborators who have worked on the research projects as described in this book. They have supplied research results, thoughts, advices, challenges, criticisms, suggestions, or help that have influenced my writing of the book. Especially, Dr. Guangqiang He and Dr. Jin Xiong, who are my staff and long-term cooperators, contribute their thoughts and research results for the book. In addition, Dr. Guangqiang He has checked carefully Chapter 8. While discussions with Prof. Zhiming Zhang, Prof. Weiping Zhang, Prof. Zhongyang Wang, and Prof. Chun Jiang motivate my further considerations on some key issues on the quantum private communication and quantum information processing. Prof. Hiroki Takesue, Prof. Markus Aspelmeyer, and Prof. Gerald S.Buller etc. provide kindly their original figures for me. Mr. Jun Zhu, Mr. Yuan Lu, and Mr. Hu Li who are my students help me to type or plot some figures. All these have improved the organization, readability, and overall quality of this book immeasurably. I apologize if I have forgotten to mention someone else; the oversight is accidental.

I would also like to take this opportunity to thank Mrs. Hongying Chen, Higher Education Press, for her great help in compiling this book. In addition, her help in correcting grammatical mistakes have improved the readability of this book.

If someone alleges to have written a book alone, distrust the person immediately. While an author is working more than 12 hours a day on the writing of the book, someone else needs to see to all the other aspects of life, from simple things like food, clothing and shelter, to complex things like social and family responsibilities. My wife, Yuanyuan Qi, took the time from her professional schedule so that I could devote my full energy to writing. Therefore, it is with great pleasure that I dedicate this book to Yuanyuan, the other half of the team that caused this book to be written.

This book is supported by the Natural Science Foundation of China (No: 60773085, 60801051, 60970109) and NSFC-KOSEF international collaborative research funds (No: 60811140346, F01-2008-000-10021-0).

Contents

1 Introduction

An introduction on the quantum private communication is presented. Issues including security requirements of the modern communication, overview of the quantum private communication, and relationships among the quantum private communication and other disciplines are addressed. In addition, a communication model for the quantum private communication is built by analogy with the Shannon private communication model. Finally, some key notations and notions for the private communication are introduced.

The quantum private communication is a combination of the quantum cryptography and modern communication techniques such as the optical communication, mobile communication, and Internet network techniques. It provides a novel way for protecting the confidentiality and authentication of modern communication systems. Different from the classic private communication, the quantum private communication is closely associated with the physical characteristics of employed quantum signals and involved communication systems, and its security depends on the corresponding quantum physics laws, such as the well-known Heisenberg uncertainty principle and no-cloning theorem. Accordingly, quantum features have naturally become important ingredients in this scenario. In applications, the quantum private communication is always merged with the classic private communication due to limitations on current quantum technologies. Some technologies such as the message encryption using classic algorithm with quantum key distribution and quantum random number generation have become practical in commercial applications. This chapter presents an overview on the quantum private communication and builds a quantum private communication model. The aim is to outline the infrastructure of the quantum private communication from both the theory and the implementation.

1.1 Security Requirements of Communication

Communication is a widely used word in our daily life and engineering. For example, when two persons talk about something, the communication between them for information exchange occurs. Actually, the communication exists everywhere and everytime in activities of the human being. Subsequently, the communication has become an interesting topic in many situations.

This book focuses on communication topics where the communication is as an academic subject like physics, chemistry, maths, etc. In this sense, the communication is regarded as an important component of the well-known information science. It is doubtless that the communication plays significant role in the information era. From the viewpoint of information science, the communication is defined as a whole procedure of information generation, processing, transmission, and receiving [1]. Generally, the information is represented with a message while the message is encoded into a set of suitable codewords. Then the encoded message (information) is carried by a proper signal for the transmission and processing. The employed signal may be variously physical forms, e.g., optical signals, electromagnetic signals, etc.

Any message exchange procedure is associated with a communication system. With the rapid development of communication technologies and computing technologies, communication systems and the associated communication information processing technologies have been used widely in engineering, commerce and our daily life. Currently, the optical fibre communication system and the wireless communication system are two mainstream ways in the modern communication field. The optical fiber communication uses telecommunication fiber as physical channel, and the transmitted signal is laser light with telecommunication wavelengths, e.g., 1310 nm and 1550 nm. The wireless communication is a topic which includes both radio communication and wireless optical communication. The wireless optical communication is also called the free space optical communication. This kind of optical communication is employed in some special cases which are difficult to pave fiber. For example, the communications in outer space and water, and the communication bestriding a canyon may use the wireless optical communication techniques. Different from the optical fiber communication system, there are no fixed physical channels in the wireless optical communication system. Surely, the wireless communication is commonly implied to the radio communication which uses radio signals to carry the message. This way of communication has been developed rapidly and widely used in our daily life. With the development of communication technologies, both the optical fiber communication and wireless communication have become more and more integrated. For example, the wireless communication system is often used as an access network in the optical fiber communication network system. Especially, the recently developed technique of "radio over fiber" is just a combination of optical fiber communication systems and wireless radio communication systems [2], and this technique has been adopted in some commercial communication systems.

As usual, if the transmitted signal in a communication system is the classic signal which obeys the classic physics laws, this kind of communication is called the classic communication. While if the transmitted signal obeys the quantum physics laws, this way is naturally called the quantum communication [20]. It is well-known that the classic communication has been investigated widely and played important roles in the modern communication field. The quantum communication has also attracted much attention since 1990s in the last century [4, 5]. By far, it has become an interesting issue in the communication field. Generally, both a classic communication system and a quantum communication system consist of the message source, channel, and message sink. Their availability and creditability are ensured by coding techniques and secure techniques, respectively.

Performance is an important parameter for a classic communication system or a quantum communication system in the modern communication. To reach an optimal performance one has to ensure at least the availability of the communication system. Usually, the availability is associated with the communication quality which is used to be called the quality of service (briefly called QoS). To guarantee the optimal availability of the communication system, one should depress noise's influences so that the efficient signal can be distilled from a received signal which has a strong noise background. For the sake of finical request and efficiency, the data from the source should be encoded which is called the source encoding. Subsequently, the encoded source should be decoded at the sink side which is called the source decoding. To guarantee the availability of the message transmitted in the channel, a so-called channel encoding and subsequently a channel decoding must be necessary at the transmitter and receivers, respectively. Except for the above operations, other techniques such as modulation and demodulation, are also needed in a communication system. In summarization, an available communication system is always described using the well-known Shannon communication model as shown in Fig.1.1 [6]. Note, this communication model is suitable for classic communication systems as well as quantum communication systems.

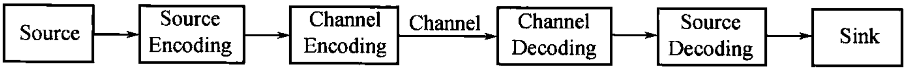

Fig. 1.1. Shannon communication model

Suppose arbitrated two legitimate communicators, i.e., Alice and Bob, want to exchange their information through a communication system. If transmitted messages may be public, which means each communicator may know the content of messages, they can communicate directly with the communication model in Fig.1.1. However, if exchanged messages are secret between Alice and Bob, then such communication is not available since anyone may read easily messages. In this case Alice and Bob would like to let their messages be transmitted privately since transmitted messages contain their secrecy or privacy. Any discovery of the secrecy of transmitted messages may harm communicators' benefits. In addition, illegitimate communicator, called Oscar, will try to forge Alice and Bob's legitimate messages which