# <<量子保密通信>>

## 图书基本信息

书名：<<量子保密通信>>

13位ISBN编号：9787040254792

10位ISBN编号：7040254794

出版时间：2010-1

出版时间：曾贵华 高等教育出版社 (2010-01出版)

作者：曾贵华

## 前言

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 tobuild 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 con- tent of this book is based on my investigations on the quantum cryptography as well as the quantum private communication since 1997.

## 内容概要

《量子保密通信》内容简介：Quantum Private Communication covers the fundamentals of the areas of secure communication, quantum cryptography, quantum communication, and their physical implementation with applications. The book appears in a timely manner for an emerging field at the crossroad of classic private communication and quantum physics. Graduate students and scientists alike in communication engineering,computer science, electronic engineering, physics and mathematics will benefit from the book.

## 作者简介

Professor Guihua Zeng teaches and conducts research at the Department of Electronic Engineering of Shanghai Jiao Tong University and spent an Alexander von Humboldt Fellowship at the University of Freiburg，Germany.

## 书籍目录

## 章节摘录

插图：This chapter devotes to building a security infrastructure for the quantum private communication. To reach this aim, some fundamental subjects including quantum mechanics, quantum information theory and quantum complexity theory are introduced. Of these fundamental subjects, the quantum mechanics is the cornerstone. With these fundamental subjects, a security theory for the quantum private communication is built.In previous chapter, an overview of the quantum private communication has been presented and a quantum private communication model has been constructed. This chapter investigates the security theory for the quantum private communication. For convenience, this kind of security theory is called a quantum security theory in this book. As usual, both the information theoretic security and computational security which is very useful in practical applications are contained in the quantum security theory. Different from the scenarios in the classic private communication, however, the information- theoretic security and computational security are here based on the quantum information theory and quantum complexity theory, respectively. To construct the quantum security theory, three aspects are involved including the information theory, complexity theory, and security model. The information theory contains both the Shannon information theory and quantum information theory. The complexity theory is associated with the classic complexity and quantum complexity theory which is based on the quantum Turing machine (TM). And the security model is a general description for the quantum security theory based on the information theory and complexity theory. Before describing in detail the quantum security theory, some fundamentals including the mathematical backgrounds and quantum mechanics are described. They are actually the cornerstones of the quantum security theory.

## 编辑推荐

《量子保密通信》是信息安全系列丛书。