

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

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 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.

<<量子保密通信>>

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.

<<量子保密通信>>

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

1 Introduction 1.1 Security Requirements of Communication 1.2 Overview of Quantum Private Communication 1.3 Private Communication Models 1.3.1 Classic Secure Communication Model 1.3.2 Quantum Private Communication Model 1.4 History of Quantum Private Communication 1.5 Relationship with Other Subjects 1.6 Notations and Conventions 1.6.1 Random Variables 1.6.2 Cryptosystem and Cipher References 2 Quantum Security Theory 2.1 Introduction 2.2 Mathematical Background 2.2.1 Hilbert Space 2.2.2 Properties of Hilbert Space 2.2.3 Operators 2.2.4 Several Important Operators 2.2.5 Matrices Decomposition 2.3 Introduction to Quantum Mechanics 2.3.1 Quantum Systems 2.3.2 Dynamic Characteristics of Quantum Systems 2.3.3 Information Retrieval of Quantum Systems 2.3.4 Fundament of Quantum Optics 2.4 Introduction to Information Theory 2.4.1 Entropy 2.4.2 Mutual Information 2.4.3 Quantum Fano Inequality 2.5 Introduction to Complexity Theory 2.5.1 Turing Machine 2.5.2 Classic Complexity 2.5.3 Quantum Complexity 2.6 Security Model 2.6.1 Information-theoretic Security 2.6.2 Computational Security 2.6.3 Attack Strategy Analysis References 3 Quantum Bits 3.1 Classic Bits 3.2 Quantum Bit Definition 3.2.1 Binary Qubit 3.2.2 P-ary Qubit 3.2.3 Composite Qubit 3.3 Quantum Bit Transformation 3.3.1 Quantum Logic Gates 3.3.2 Quantum Circuits 3.4 Mathematical Property 3.4.1 Bloch Sphere 3.4.2 Orthogonality of Opposite Points 3.4.3 Rotations on Bloch Sphere 3.5 Physical Property 3.5.1 Superposition 3.5.2 Entanglement 3.5.3 Distinguishability 3.5.4 Quantum No-cloning 3.6 Information Property 3.6.1 Single Qubit Information 3.6.2 Nonorthogonal Qubits Information References 4 Quantum Key Distribution 4.1 Intuition on QKD 4.2 Standard QKD Schemes 4.2.1 BB84 Protocol 4.2.2 B92 Protocol 4.3 Quantum Communication Model for QKD 4.3.1 Quantum Source 4.3.2 Quantum Channel 4.3.3 Quantum Sink 4.4 Reconciliation 4.4.1 Reconciliation Model 4.4.2 Binary Reconciliation Protocol 4.4.3 Non-Binary Reconciliation Protocol 4.5 Privacy Amplification 4.5.1 Privacy Amplification Principle 4.5.2 Privacy Amplification Techniques 4.6 Security Model for QKD 4.6.1 Security Theory 4.6.2 Typical Attack Strategies References 5 Quantum Cryptosystem 5.1 Introduction 5.2 QKD-based Cryptosystem 5.3 Quantum Vernam Cipher 5.3.1 Classic Vernam Algorithm 5.3.2 Quantum Vernam Cipher 5.3.3 Private Quantum Channel 5.3.4 Security Model 5.4 Typical Quantum Vernam Ciphers 5.4.1 Classic-key-based Quantum Vernam Cipher 5.4.2 Bell-key-based Quantum Vernam Cipher 5.4.3 Teleportation as Quantum Vernam Cipher 5.5 Quantum Block Cipher 5.5.1 Theoretical Model 5.5.2 Quantum Block Algorithm for Binary Bits 5.6 Quantum Public Key Cryptosystem 5.7 Typical Quantum Public-key Algorithms 5.7.1 Algorithm based Subset-sum Problem 5.7.2 Algorithm based Quantum Coding References 6 Quantum Authentication 6.1 Introduction 6.2 Authentication Theory 6.2.1 Authentication Categories 6.2.2 Security Model 6.3 Message Authentication Code 6.3.1 Encoding Approach 6.3.2 Hash Function Approach 6.4 Quantum Identity Authentication 6.4.1 Scheme Description 6.4.2 Security Analysis 6.4.3 In Imperfect Channel 6.5 Quantum Signature Principle 6.6 Arbitrated Quantum Signature 6.6.1 Algorithm Description 6.6.2 Security Analysis 6.7 True Quantum Signature 6.7.1 Algorithm Description 6.7.2 Security Analysis..... Index

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.

<<量子保密通信>>

编辑推荐

《量子保密通信》是信息安全系列丛书。

<<量子保密通信>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>