

Broadview  
www.broadview.com.cn

Broadview®  
www.broadview.com.cn

突破传统密码学界限，迎接量子安全新时代

Quantum Security

# 量子安全 信息保护新纪元

Chahot◎著

量子安全信息保护新纪元

电子工业出版社



中国工信出版集团



电子工业出版社  
http://www.phei.com.cn

## <Book> Quantum Security: A New Era in Information Protection

This is a Chinese book (**published in July 2024**), signed with the 4th-ranked publisher in the field of Chinese technology books, the "Publishing House of Electronics Industry, PHEI". The purpose of providing this contract is to demonstrate my understanding of quantum computing and information security and my eagerness for in-depth learning. As you may know, foundational knowledge is often easy to grasp and explain to others, but when it comes to delving into more profound technical principles, one needs an exceptional advisor/supervisor. At the end of this document, I have attached the signed publishing contract, which can be found on the last page of the PDF file.

Here's the translated table of contents in English:

---

1. Information Security and Cryptography .....	1
1.1 Information Security .....	1
1.1.1 Information Protection .....	1
1.1.2 Encryption and Decryption: Basic Security Mechanisms .....	4
1.1.3 Information Security Education and Non-Design Mechanism Security .....	9
1.2 Modern Cryptography .....	10
1.2.1 Basics of Cryptography: XOR Operation .....	10
1.2.2 Symmetric Encryption .....	11
1.2.3 Asymmetric Encryption .....	23
1.2.4 Keys and Random Numbers .....	34
1.3 Types of Modern Cryptography .....	41
1.3.1 Block Ciphers .....	41
1.3.2 Stream Ciphers .....	53
1.4 Modern Network Security Communication Systems .....	58
1.4.1 Hybrid Cryptosystems .....	58
1.4.2 One-Way Hash Functions .....	60
1.4.3 Message Authentication Codes .....	65
1.4.4 Digital Signatures .....	68
1.4.5 Trusted Certification Authorities .....	70
1.4.6 Network Security Communication Systems Based on Modern Cryptography .....	72
2. Network Security: Applications of Information Security .....	75
2.1 Information Security Evaluation Standards .....	75
2.1.1 Security Concepts Based on Information Theory .....	75
2.1.2 Security Deployment Rules in Commercial Environments .....	79
2.1.3 Black Box, Gray Box, and White Box Attack Models .....	81
2.2 Network Security Threats .....	82
2.2.1 Various Network Attacks .....	82
2.2.2 Malware .....	86

2.2.3 Modern Network Attack Outlook .....	90
2.3 Changing Network Environment .....	92
2.3.1 Internet of Things (IoT) .....	93
2.3.2 Smart Cities .....	95
2.3.3 Metaverse .....	97
 3. Fundamentals of Quantum Computing .....	 100
3.1 Linear Algebra and Quantum Mechanics .....	100
3.1.1 Waves and Particles .....	100
3.1.2 Quantum States and Wave Functions .....	103
3.1.3 Inner Product, Outer Product, and Tensor Product .....	109
3.1.4 Quantum Operators: Pauli Matrices .....	114
3.1.5 Quantum Gates and Quantum Circuits .....	116
3.1.6 Quantum Phenomena: Quantum Superposition, Quantum Interference, and Quantum Entanglement .....	121
3.1.7 Quantum Phase .....	124
3.1.8 Quantum Phase Flip and Phase Kickback .....	127
3.2 Quantum Computers .....	133
3.2.1 Physical Quantities in Quantum Computing .....	134
3.2.2 Hardware Framework of Quantum Computers .....	137
3.2.3 Implementation of Quantum Computing .....	139
3.2.4 Error Correction in Quantum Computers .....	141
3.2.5 DiVincenzo Criteria .....	142
 4. Quantum Technology Development Trends .....	 148
4.1 Current Status of Quantum Technology in China .....	148
4.1.1 isQ-Core and Qingguo .....	149
4.1.2 Origin Quantum .....	150
4.1.3 Huayi Quantum .....	151
4.1.4 Turing Quantum .....	153
4.1.5 Quantum Spin Technology .....	153
4.1.6 Magnet Technology .....	154
4.1.7 Developments of Other Institutions .....	155
4.1.8 Dynamics of Quantum Security Related Industries .....	157
4.2 Current Status of Quantum Technology Internationally .....	158
4.2.1 Cirq .....	160
4.2.2 Qiskit .....	161

4.2.3 Q# .....	162
4.3 Impact of Quantum Computing on Information Security Systems and Prospects for Global Security .....	163
4.3.1 Frontier Research on Post-Quantum Security .....	163
4.3.2 Challenges in Information Security in the Quantum Era .....	164
4.3.3 Quantum Innovation and Information Security: From Nobel Prizes to Global Technological Competition ..	166
4.3.4 Recent Investments and Financing in Quantum Communication and Security .....	167
4.3.5 Quantum Security Deployment Scenarios and Key Industry Applications .....	168
 5. Quantum Programming Practice .....	 171
5.1 Simple Methods for Quantum Programming Based on Graphical Interfaces .....	171
5.1.1 IBM Quantum .....	171
5.1.2 IBM Quantum Composer .....	178
5.1.3 Quantum Programming Case Studies Based on Graphical Interfaces .....	181
5.2 Advanced Quantum Programming Methods Based on Qiskit .....	185
5.2.1 Introduction to Quantum Programming Based on Qiskit .....	185
5.2.2 Installation and Configuration of Qiskit .....	186
5.2.3 Quantum Programming Case Studies Based on Qiskit .....	195
5.3 Practical Application: Calculating $\pi$ Through Quantum Programming .....	202
5.3.1 Quantum Fourier Transform .....	203
5.3.2 Quantum Phase Estimation .....	208
5.3.3 $\pi$ Calculation Program Based on QPE .....	217
 6. Quantum Algorithms .....	 224
6.1 Grover's Algorithm .....	224
6.1.1 Data Retrieval and Grover's Algorithm .....	224
6.1.2 Programming Practice: Quantum Secret Guessing Based on Grover's Algorithm .....	232
6.1.3 Programming Practice: Quantum Optimization Based on Grover's Algorithm .....	237
6.2 Error Correction and Quantum Error Correction Algorithms .....	244
6.2.1 Quantum Error Correction: Qubit Flip Correction .....	245
6.2.2 Quantum Error Correction: Phase Flip Correction .....	248
6.3 Shor's Algorithm .....	251
6.3.1 Threat of Shor's Algorithm to RSA .....	252
6.3.2 Practical Application of Shor's Algorithm: Simple Factorization .....	256
6.4 Quantum Random Walk Algorithms .....	261
6.4.1 Random Walk Algorithms and Quantum Random Walk Algorithms .....	261
6.4.2 Examples of Quantum Random Walk Algorithms .....	264

7. Quantum Security and Quantum Network Communication .....	273
7.1 Fundamentals of Quantum Security .....	273
7.1.1 Quantum Random Number Generators .....	274
7.1.2 Security Analysis of Quantum State Determination and Quantum Integrity Verification .....	276
7.2 Quantum Security and Communication .....	277
7.2.1 Quantum Teleportation .....	277
7.2.2 Quantum Dense Coding .....	289
7.2.3 Quantum Unconditionally Secure Communication .....	294
7.2.4 Quantum Key Distribution .....	295
7.2.5 Quantum Security Authentication .....	307
7.2.6 Quantum Steganography .....	313
7.3 Quantum Repeaters and Quantum Networks .....	322
7.4 Future Prospects and Challenges of Quantum Internet .....	329
8. Next-Generation Cryptographic Technology .....	335
8.1 Lightweight Cryptography .....	335
8.1.1 TinyJAMBU .....	336
8.1.2 Ascon .....	342
8.1.3 ACORN .....	345
8.1.4 AEGIS-128 .....	346
8.1.5 Deoxys-II .....	348
8.2 Homomorphic Encryption .....	351
8.2.1 Concept of Homomorphic Encryption .....	351
8.2.2 Classification of Adversary Models .....	354
8.2.3 Implementation of Homomorphic Cryptography .....	356
8.2.4 Efficiency Bottlenecks of Homomorphic Cryptography .....	365
8.2.5 Quantum Homomorphic Encryption .....	366
8.3 Zero-Knowledge Proof .....	368
8.4 Secure Multi-Party Computation .....	371
8.5 Next-Generation Cryptographic Technology and Quantum Security .....	375
9. Post-Quantum Security and Post-Quantum Cryptography .....	381
9.1 Post-Quantum Security .....	381
9.1.1 Hash-Based Post-Quantum Cryptography .....	382
9.1.2 Lattice-Based Post-Quantum Cryptography .....	384

9.1.3 Code-Based Post-Quantum Cryptography .....	385
9.1.4 Multivariate Polynomial Equation-Based Post-Quantum Cryptography .....	386
9.2 Recommendations and Candidates for Post-Quantum Cryptography .....	388
9.2.1 Classic McEliece .....	390
9.2.2 CRYSTALS-KYBER .....	392
9.2.3 NTRU .....	393
9.2.4 SABER .....	394
9.2.5 CRYSTALS-DILITHIUM .....	394
9.2.6 FALCON .....	396
9.2.7 Rainbow .....	397
9.2.8 BIKE .....	399
9.2.9 FrodoKEM .....	399
9.2.10 HQC .....	400
9.2.11 NTRUPrime .....	401
9.2.12 SIKE .....	402
9.2.13 GeMSS .....	403
9.2.14 Picnic .....	405
9.2.15 SPHINCS+ .....	407
 10. Overview of Cutting-Edge Quantum Security Technologies .....	 410
10.1 Quantum One-Time Pad .....	410
10.2 Quantum Secure Ghost Imaging .....	415
10.3 Quantum Secure Blockchain .....	418
10.3.1 Quantum Hash Functions .....	419
10.3.2 Quantum Digital Signatures .....	420
10.3.3 Quantum Communication and Consensus Mechanisms .....	422
10.4 Quantum Machine Learning .....	424
 <a href="#">Appendix A: Quantum Computing Terminology and Compilation Environment Language Issues</a> ....	 <a href="#">428</a>
1. Quantum Computing Terminology .....	428
2. Compilation Environment Language Issues .....	432
 <a href="#">Appendix B: IBM Update Notes</a> .....	 <a href="#">434</a>
1. Retirement of Cloud Simulators .....	434
2. Retirement of IBM Quantum Lab .....	435



选题编号：202300496

审批日期：2024-05-23

合同编号：2024(2109)

# 电子工业出版社有限公司

## 出版合同

选题名称：量子安全与网络通信

作品名称：量子安全：信息保护新纪元

☒ 包括配书电子出版物

☒ 包括配书音像制品

☒ 包括教学资料包

☒ 包括其他附件（见补充条款规定）

（注：所选项目前□内划“√”，表示甲方同意完成该项附件，所选项目□内划“×”，表示甲方提交乙方的稿件不包括该项附件，以下简称“作品”）

甲方：陈昊天

封面署名及著作方式：Chahot 著

扉页署名及著作方式：Chahot 著

乙方：电子工业出版社有限公司