# Contents

## Part I Quantum Computation

**Quantum Identification of Boolean Oracles**  
Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, Shigeru Yamashita  
3

1. Introduction  
2. Formalization  
3. General Upper Bounds  
4. Relation With Learning Theory  
5. Tight Upper Bounds for Small $M$  
6. Classical Lower and Upper Bounds  
7. Concluding Remarks  
References  
Index

**Query Complexity of Quantum Biased Oracles**  
Kazuo Iwama, Rudy Raymond, Shigeru Yamashita  
19

1. Introduction  
2. Goldreich–Levin Problem and Biased Oracles  
   2.1 The Model of Quantum Biased Oracles  
3. Upper Bounds of the Query Complexity of Biased Oracles With Special Conditions  
   3.1 Basic Tools for Quantum Computation  
   3.2 Quantum Biased Oracles With the Same Bias Factor  
   3.3 Quantum Biased Oracles With Resettable Condition  
4. Lower Bounds of the Query Complexity of Biased Oracles  
5. Concluding Remarks  
References  
Index

## Part II Quantum Information

**Quantum Statistical Inference**  
Masahito Hayashi  
45
Quantum Key Distribution: Security, Feasibility and Robustness
Xiang-Bin Wang ............................................. 185
1 Introduction ................................................ 185
2 Security Proof of BB84 QKD With Perfect Single-Photon Source . 187
  2.1 Hashing and Error-Correction in Classical Communication ... 188
  2.2 The Main Idea of Entanglement Purification ............... 190
  2.3 Error Test ............................................. 192
  2.4 Entanglement Purification by Hashing ..................... 192
    2.4.1 Bit-Flip Error Correction .......................... 193
    2.4.2 Phase-Flip Error Correction ........................ 194
  2.5 Classicalization ....................................... 195
3 Secure Key Distillation With a Known Fraction of Tagged Bits ... 196
  3.1 Final Key Distillation With a Fraction of Tagged Bits . 196
  3.2 PNS Attack ............................................ 198
4 The Decoy-State Method .................................... 200
  4.1 The Main Ideas and Results ................................ 201
  4.2 The Issue of Unconditional Security ....................... 206
  4.3 Robustness Analysis ................................... 206
  4.4 Final Key Rate and Further Studies ....................... 209
  4.5 Summary .............................................. 210
5 QKD With Asymmetric Channel Noise .......................... 210
  5.1 Channel Error, Tested Error and Key-Bits Error ........... 211
  5.2 QKD With One-Way Classical Communication ............... 212
  5.3 Six-State Protocol With Two-Way Classical Communications. 214
6 Quantum Key Distribution With Encoded BB84 States ............ 217
  6.1 A Protocol For Collective Channel Noise .. 219
    6.1.1 Protocol 1 and Security Proof ....................... 220
    6.1.2 Protocol 2 ......................................... 221
    6.1.3 Physical Realization .............................. 223
    6.1.4 Another Protocol For Robust QKD With Swinging
         Objects ............................................. 223
    6.1.5 Summary and Discussion ........................... 224
  6.2 A Protocol With Independent Noise ....................... 225
    6.2.1 The Method and the Main Idea ....................... 225
Why Quantum Steganography Can Be Stronger Than Classical Steganography
Shin Natori .................................................... 235
1 Introduction ................................................ 235
2 Definitions .................................................. 235
  2.1 General Model of Steganography System ............... 235
  2.2 Classical Model of Steganography System ............. 237
3 Related Works ............................................. 237
4 Quantum Steganography .................................. 237
  4.1 Model of Quantum Steganography System ............... 237
  4.2 Comparison Between Classical and Quantum Steganography 238
5 Conclusions and Future Work ............................. 240
References .................................................... 240
Index .................................................................... 240

Part IV Realization of Quantum Information System
Photonic Realization of Quantum Information Systems
Akihisa Tomita, Bao-Sen Shi .................................... 243
1 Introduction .................................................. 243
2 Cryptography .................................................. 244
  2.1 High-Sensitivity Photon Detector ....................... 245
  2.1.1 Requirement for Single-Photon Detectors .......... 245
  2.1.2 Improved Single-Photon Detector for Fiber Transmission 246
  2.2 Single-Photon Transmission Over 150 km in a Unidirectional System With Integrated Interferometers .............. 248
  2.3 Refinements Toward a Practical QKD System .......... 251
  2.3.1 Temperature-Insensitive Interferometer .......... 251
  2.3.2 High-Speed Operation ............................. 253
3 Quantum Computation ..................................... 256
  3.1 Measured Quantum Fourier Transform ............... 256
  3.1.1 Implementation and Experimental Results ........ 256
  3.1.2 Effects of Imperfection .......................... 258
  3.1.3 Validity of Majority Voting ....................... 260
  3.1.4 Toward Quantum Computers ...................... 262
  3.2 Control-Unitary Gates .................................. 263
3.2.1 Solid-State Bell State Measurement Devices by Two-Photon Absorption ........................................ 264
4 Generation of Entangled Photon Pairs by SPDC ................ 265
  4.1 SPDC With Two-Crystal Geometry ............................ 266
  4.2 Interferometric Generation of Entangled Photon Pairs ...... 269
  4.3 A New Material for SPDC: Periodically Poled KTP .......... 270
5 Conclusion .................................................................. 272
References .................................................................... 273
Index ............................................................................ 275

Index ............................................................................ 277