

# Introduction to QUANTUM CRYPTOGRAPHY

Thomas Vidick | Stephanie Wehner



# Introduction to Quantum Cryptography

Thomas Vidick

*California Institute of Technology, USA*

*Weizmann Institute of Science, Israel*

Stephanie Wehner

*Delft University of Technology, The Netherlands*



# Contents

<i>Preface</i>	<i>page ix</i>
<b>1 Background Material</b>	<b>1</b>
1.1 Mathematical Notation	1
1.2 What Are Quantum Bits?	4
1.3 Multiple Qubits	6
1.4 Combining Qubits Using the Tensor Product	9
1.5 Simple Measurements	13
1.6 Unitary Transformations and Gates	21
1.7 The Bloch Sphere	26
1.8 Implementing Quantum Cryptography	28
Chapter Notes	36
Problems	36
Quiz Solutions	37
Cheat Sheet	38
<b>2 Quantum Tools and a First Protocol</b>	<b>40</b>
2.1 Probability Notation	40
2.2 Density Matrices	41
2.3 General Measurements	53
2.4 The Partial Trace	58
2.5 Secure Message Transmission	63
Chapter Notes	72
Problems	72
Quiz Solutions	75
Cheat Sheet	76
<b>3 Quantum Money</b>	<b>78</b>
3.1 A (Too) Simple Quantum Money Scheme	78
3.2 Wiesner's Quantum Money	79
3.3 Quantum Channels	83
3.4 Attacks on Wiesner's Scheme	86
3.5 The Elitzur–Vaidman Bomb Tester	91
Chapter Notes	96
Problems	96
Quiz Solutions	98
<b>4 The Power of Entanglement</b>	<b>99</b>
4.1 Entanglement	99
4.2 Purifications	102

4.3	Two Applications	107
4.4	Bell Nonlocality	110
4.5	The Monogamy of Entanglement	115
	Chapter Notes	119
	Problems	119
	Quiz Solutions	123
	Cheat Sheet	124
<b>5</b>	<b>Quantifying Information</b>	<b>125</b>
5.1	When Are Two Quantum States Almost the Same?	125
5.2	What It Means to Be Ignorant	130
5.3	Measuring Uncertainty: The Min-Entropy	133
5.4	Uncertainty Principles: A Bipartite Guessing Game	140
5.5	Extended Uncertainty Relation Principles: A Tripartite Guessing Game	144
	Chapter Notes	149
	Problems	149
	Quiz Solutions	151
	Cheat Sheet	152
<b>6</b>	<b>From Imperfect Information to (Near) Perfect Security</b>	<b>153</b>
6.1	Privacy Amplification	153
6.2	Randomness Extractors	155
6.3	Solving Privacy Amplification Using Extractors	161
6.4	An Extractor Based on Hashing	161
	Chapter Notes	172
	Problems	172
	Quiz Solutions	175
<b>7</b>	<b>Distributing Keys</b>	<b>176</b>
7.1	Honest and Dishonest	176
7.2	Secure Key Distribution	177
7.3	Distributing Keys Given a Special Classical Channel	180
7.4	Information Reconciliation	183
7.5	Everlasting Security	188
	Chapter Notes	190
	Problems	190
	Quiz Solutions	193
<b>8</b>	<b>Quantum Key Distribution Protocols</b>	<b>194</b>
8.1	BB'84 Quantum Key Distribution	194
8.2	A Modified Protocol	201
8.3	Security of BB'84 Key Distribution	204
8.4	Correctness of BB'84 Key Distribution	211
	Chapter Notes	214
	Problems	214
	Quiz Solutions	217

<b>9 Quantum Cryptography Using Untrusted Devices</b>	<b>218</b>
9.1 The DIQKD Protocol	218
9.2 Security of Device-Independent Quantum Key Distribution	222
9.3 Testing EPR Pairs	228
Chapter Notes	235
Problems	235
Quiz Solutions	240
<b>10 Quantum Cryptography beyond Key Distribution</b>	<b>241</b>
10.1 Coin Flipping	241
10.2 Two-Party Cryptography	246
10.3 Oblivious Transfer	250
10.4 Bit Commitment	252
10.5 Kitaev's Lower Bound on Strong Coin Flipping	258
Chapter Notes	263
Problems	264
Quiz Solutions	269
<b>11 Security from Physical Assumptions</b>	<b>270</b>
11.1 The Noisy Storage Model	271
11.2 1-2 Oblivious Transfer in the Noisy Storage Model	272
11.3 Security from Quantum Uncertainty	274
Chapter Notes	280
Problems	280
Quiz Solutions	283
<b>12 Further Topics around Encryption</b>	<b>284</b>
12.1 The Key Length Requirements for Secure Quantum Encryption	284
12.2 Encryption with Certified Deletion	292
Chapter Notes	300
Problems	300
Quiz Solutions	301
<b>13 Delegated Computation</b>	<b>302</b>
13.1 Definition of the Task	302
13.2 Verifiable Delegation of Quantum Circuits	305
13.3 Delegation in the Measurement-Based Model	311
13.4 Classically Delegating to Two Quantum Servers	316
Chapter Notes	325
Problems	325
Quiz Solutions	326
<i>Index</i>	327