

Contents

1. The Physics of Quantum Information:	
Basic Concepts	1
1.1 Quantum Superposition	1
1.2 Qubits	3
1.3 Single-Qubit Transformations	4
1.4 Entanglement	7
1.5 Entanglement and Quantum Indistinguishability	9
1.6 The Controlled NOT Gate	11
1.7 The EPR Argument and Bell's Inequality	12
1.8 Comments	14
2. Quantum Cryptography	15
2.1 What is Wrong with Classical Cryptography?	15
2.1.1 From SCYTALE to ENIGMA	15
2.1.2 Keys and Their Distribution	16
2.1.3 Public Keys and Quantum Cryptography	19
2.1.4 Authentication: How to Recognise Cinderella ?	21
2.2 Quantum Key Distribution	22
2.2.1 Preliminaria	22
2.2.2 Security in Non-orthogonal States: No-Cloning Theorem	22
2.2.3 Security in Entanglement	24
2.2.4 What About Noisy Quantum Channels?	25
2.2.5 Practicalities	26
2.3 Quantum Key Distribution with Single Particles	27
2.3.1 Polarised Photons	27
2.3.2 Phase Encoded Systems	31
2.4 Quantum Key Distribution with Entangled States	33
2.4.1 Transmission of the Raw Key	33
2.4.2 Security Criteria	34
2.5 Quantum Eavesdropping	36
2.5.1 Error Correction	36
2.5.2 Privacy Amplification	37
2.6 Experimental Realisations	43
2.6.1 Polarisation Encoding	43

2.6.2	Phase Encoding	44
2.6.3	Entanglement-Based Quantum Cryptography	46
2.7	Concluding Remarks	47
3.	Quantum Dense Coding	
	and Quantum Teleportation	49
3.1	Introduction	49
3.2	Quantum Dense Coding Protocol	50
3.3	Quantum Teleportation Protocol	51
3.4	Sources of Entangled Photons	53
3.4.1	Parametric Down-Conversion	53
3.4.2	Time Entanglement	54
3.4.3	Momentum Entanglement	57
3.4.4	Polarisation Entanglement	58
3.5	Bell-State Analyser	60
3.5.1	Photon Statistics at a Beamsplitter	60
3.6	Experimental Dense Coding with Qubits	62
3.7	Experimental Quantum Teleportation of Qubits	67
3.7.1	Experimental Results	69
3.7.2	Teleportation of Entanglement	72
3.7.3	Concluding Remarks and Prospects	72
3.8	A Two-Particle Scheme for Quantum Teleportation	74
3.9	Teleportation of Continuous Quantum Variables	77
3.9.1	Employing Position and Momentum Entanglement	77
3.9.2	Quantum Optical Implementation	79
3.10	Entanglement Swapping: Teleportation of Entanglement	84
3.11	Applications of Entanglement Swapping	88
3.11.1	Quantum Telephone Exchange	88
3.11.2	Speeding up the Distribution of Entanglement	89
3.11.3	Correction of Amplitude Errors Developed due to Propagation	90
3.11.4	Entangled States of Increasing Numbers of Particles	91
4.	Concepts of Quantum Computation	93
4.1	Introduction to Quantum Computation	93
4.1.1	A New Way of Harnessing Nature	93
4.1.2	From Bits to Qubits	94
4.1.3	Quantum Algorithms	98
4.1.4	Building Quantum Computers	100
4.1.5	Deeper Implications	101
4.1.6	Concluding Remarks	103
4.2	Quantum Algorithms	104
4.2.1	Introduction	104
4.2.2	Quantum Parallel Computation	105
4.2.3	The Principle of Local Operations	107

4.2.4	Oracles and Deutsch’s Algorithm	109
4.2.5	The Fourier Transform and Periodicities	114
4.2.6	Shor’s Quantum Algorithm for Factorisation	119
4.2.7	Quantum Searching and NP	121
4.3	Quantum Gates and Quantum Computation	
	with Trapped Ions	126
4.3.1	Introduction	126
4.3.2	Quantum Gates with Trapped Ions	126
4.3.3	N Cold Ions Interacting with Laser Light	128
4.3.4	Quantum Gates at Non-zero Temperature	130
5.	Experiments Leading Towards	
	Quantum Computation	133
5.1	Introduction	133
5.2	Cavity QED-Experiments:	
	Atoms in Cavities and Trapped Ions	134
5.2.1	A Two-Level System Coupled to a Quantum Oscillator	134
5.2.2	Cavity QED with Atoms and Cavities	135
5.2.3	Resonant Coupling: Rabi Oscillations	
	and Entangled Atoms	137
5.2.4	Dispersive Coupling: Schrödinger’s Cat	
	and Decoherence	143
5.2.5	Trapped-Ion Experiments	147
5.2.6	Choice of Ions and Doppler Cooling	148
5.2.7	Sideband Cooling	150
5.2.8	Electron Shelving and Detection of Vibrational Motion	153
5.2.9	Coherent States of Motion	154
5.2.10	Wigner Function of the One-Phonon State	157
5.2.11	Squeezed States and Schrödinger Cats with Ions	159
5.2.12	Quantum Logic with a Single Trapped $^9\text{Be}^+$ Ion	160
5.2.13	Comparison and Perspectives	161
5.3	Linear Ion Traps for Quantum Computation	163
5.3.1	Introduction	163
5.3.2	Ion Confinement in a Linear Paul Trap	164
5.3.3	Laser Cooling and Quantum Motion	167
5.3.4	Ion Strings and Normal Modes	169
5.3.5	Ions as Quantum Register	171
5.3.6	Single-Qubit Preparation and Manipulation	172
5.3.7	Vibrational Mode as a Quantum Data Bus	173
5.3.8	Two-Bit Gates in an Ion-Trap Quantum Computer	174
5.3.9	Readout of the Qubits	175
5.3.10	Conclusion	175
5.4	Nuclear Magnetic Resonance Experiments	177
5.4.1	Introduction	177
5.4.2	The NMR Hamiltonian	177

5.4.3	Building an NMR Quantum Computer	179
5.4.4	Deutsch's Problem	181
5.4.5	Quantum Searching and Other Algorithms	184
5.4.6	Prospects for the Future	185
5.4.7	Entanglement and Mixed States	188
5.4.8	The Next Few Years	188
6.	Quantum Networks	
	and Multi-Particle Entanglement	191
6.1	Introduction	191
6.2	Quantum Networks I:	
	Entangling Particles at Separate Locations	192
6.2.1	Interfacing Atoms and Photons	192
6.2.2	Model of Quantum State Transmission	193
6.2.3	Laser Pulses for Ideal Transmission	195
6.2.4	Imperfect Operations and Error Correction	197
6.3	Multi-Particle Entanglement	197
6.3.1	Greenberger–Horne–Zeilinger states	197
6.3.2	The Conflict with Local Realism	198
6.3.3	A Source for Three-Photon GHZ Entanglement	200
6.3.4	Experimental Proof of GHZ Entanglement	204
6.3.5	Experimental Test of Local Realism	
	Versus Quantum Mechanics	206
6.4	Entanglement Quantification	210
6.4.1	Schmidt Decomposition and von Neumann Entropy	210
6.4.2	Purification Procedures	212
6.4.3	Conditions for Entanglement Measures	214
6.4.4	Two Measures of Distance Between Density Matrices	216
6.4.5	Numerics for Two Spin 1/2 Particles	217
6.4.6	Statistical Basis of Entanglement Measure	219
7.	Decoherence and Quantum Error Correction	221
7.1	Introduction	221
7.2	Decoherence	222
7.2.1	Decoherence: Entanglement Between	
	Qubits and Environment	222
7.2.2	Collective Interaction and Scaling	224
7.2.3	Subspace Decoupled From Environment	225
7.2.4	Other Find of Couplings	225
7.3	Limits to Quantum Computation Due to Decoherence	227
7.4	Error Correction and Fault-Tolerant Computation	232
7.4.1	Symmetrisation Procedures	232
7.4.2	Classical Error Correction	234
7.4.3	General Aspects of Quantum Error Correcting Codes	236
7.4.4	The Three Qubit Code	237

7.4.5	The Quantum Hamming Bound	238
7.4.6	The Seven Qubit Code	239
7.4.7	Fault-Tolerant Computation	241
7.5	General Theory of Quantum Error Correction and Fault Tolerance	242
7.5.1	Digitisation of Noise	242
7.5.2	Error Operators, Stabiliser, and Syndrome Extraction ..	243
7.5.3	Code Construction	246
7.5.4	The Physics of Noise	248
7.5.5	Fault-Tolerant Quantum Computation	250
7.6	Frequency Standards	252
8.	Entanglement Purification	261
8.1	Introduction	261
8.2	Principles of Entanglement Purification	261
8.3	Local Filtering	269
8.4	Quantum Privacy Amplification	271
8.5	Generalisation of Purification to Multi-Particle Entanglement	275
8.6	Quantum Networks II: Communication over Noisy Channels	281
8.6.1	Introduction	281
8.6.2	Ideal Communication	282
8.6.3	Correction of Transfer Errors: The Photonic Channel	283
8.6.4	Purification with Finite Means	285
8.7	Quantum Repeaters	288
	References	294
	Index	311