

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Quanteninformatik – warum?	1
1.2	Philosophischer Hintergrund	3
1.3	Voraussetzungen für das Lesen dieses Buches	7
<b>2</b>	<b>Quantenmechanische Phänomene</b>	<b>9</b>
<b>3</b>	<b>Grundlagen der Quantenmechanik</b>	<b>17</b>
3.1	Unschärfeprinzip und Statistik	17
3.2	Wellenfunktion, Superposition und Verschränkung	19
3.2.1	Die Axiome	20
3.2.2	Messung, Wirkung, Verschränkung	23
3.2.3	Von den Axiomen zur Theorie: zwei Beispiele	27
3.2.4	Eigenwerte und Eigenfunktionen	33
3.3	Formalisierung der Theorie	37
3.3.1	Der Hilbert-Raum – unitäre Räume	37
3.3.2	Quantenmechanische Objekte	40
3.3.2.1	Eigenfunktion und Superposition	40
3.3.2.2	Überlagerung und Verschränkung	42
3.3.2.3	Messung	47
3.3.2.4	Zusammenfassung	49
3.3.3	Dichte-Operator	49
3.3.3.1	Die Dichtematrix	49
3.3.3.2	Invarianten: die Spur der Dichtematrix	51
3.3.3.3	Messungen und Wirkungen im Dichtebild	53
3.3.3.4	Partielle Spur	54
3.3.4	Anwendung der Theorie auf polarisierte Photonen	55
3.4	Schrödinger-Gleichung und Unschärferelation	58
3.4.1	Die Schrödinger-Gleichung(en)	58
3.4.2	Klassifikation von Operatoren	60
3.4.3	Operatorformen und Unschärferelation	62

3.4.4	Die Übertragung auf die Praxis .....	64
3.5	Drehimpuls und Spin .....	65
3.5.1	Der Drehimpuls .....	65
3.5.2	Der Spin .....	67
3.5.3	Unitäre Spintransformationen in der Praxis .....	70
3.5.4	Zeitliche Stabilität von Zuständen .....	72
3.6	Lokalität und Klonen .....	75
3.6.1	Das EPR-Problem und die Bell-Gleichung .....	75
3.6.1.1	Ist die Theorie unvollständig? .....	75
3.6.1.2	2-Photonen-Experiment .....	76
3.6.1.3	3-Spin-Experiment .....	79
3.6.1.4	Praktische Auswirkungen .....	81
3.6.2	Verschränkung und lokale Wirkung .....	81
3.6.3	Das „No Cloning“-Theorem .....	83
3.7	Entropie und Information .....	84
3.7.1	Klassische Entropie und Information .....	85
3.7.2	Entropie und Information in der Quantentheorie .....	87
<b>4</b>	<b>Lichtquanten und Verschlüsselung .....</b>	<b>91</b>
4.1	Klassische Verschlüsselungsverfahren und Motivation .....	91
4.2	Arbeitsweise der Quantenkryptographie .....	93
4.2.1	Photonen und Polarisation .....	93
4.2.2	Quantenkryptografie .....	96
4.3	Protokolle für die Schlüsselerzeugung .....	98
4.3.1	1-Photonen-4-Zustände-Protokoll .....	98
4.3.1.1	Das Basisprotokoll im ungestörten Fall .....	98
4.3.1.2	Angriff auf den Quantenkanal .....	99
4.3.2	1-Photonen-6-Zustände-Protokoll .....	101
4.3.3	Die Ermittlung der fehlenden Schlüsselbits .....	102
4.3.4	2-Photonen-2-Zustände-Protokoll .....	104
4.4	Fortgeschrittene Angriffsmethoden .....	108
4.4.1	Angriff mit Quantencomputern .....	108
4.4.2	Angriff mit einem Quantenkopierer (Kloner) .....	111
4.4.2.1	Untergrenze der Sicherheit .....	111
4.4.2.2	Universeller optimaler Kloner .....	114
4.4.3	Zusammenfassung der Szenarien .....	116
4.5	Fehlerkorrektur .....	117
4.5.1	Allgemeine Vorgehensweise .....	117
4.5.2	Der klassische Ansatz: Verwerfen der Messinformationen ..	120
4.5.2.1	Advantage Distillation .....	121
4.5.2.2	Eves „Advantage“ .....	122
4.5.2.3	Information Reconciliation .....	125
4.5.2.4	Privacy Amplification .....	126
4.5.2.5	Fazit .....	126

4.5.3	Nutzung von Informationen aus Quantenverfahren .....	127
4.5.3.1	Kaskadierende 2/1-Bitextraktion .....	127
4.5.3.2	$n/m$ -Blockextraktion .....	130
4.5.3.3	$n/m/1$ -Alphabet .....	134
4.5.3.4	$k * m/m/m'$ -Alphabete .....	135
4.5.4	Authentifizierung der Verbindung .....	136
4.5.5	Simulation von Szenarien .....	140
4.6	Erzeugungsstatistik polarisierter Photonen .....	149
4.6.1	Statistik des Erzeugungsprozesses .....	149
4.6.2	Angriff mit einfachem Strahlenteiler .....	152
4.6.3	Einfaches System mit Gedächtnis .....	153
4.6.4	Selektive Strahlenteiler .....	154
4.6.5	Hardware ./ Software .....	155
4.7	Primäre Photonenquellen: Laserdioden .....	156
4.7.1	Anforderungen .....	156
4.7.2	Grundlagen der Halbleitertechnik .....	157
4.7.3	Photo- und Laserdioden .....	162
4.7.4	Erzeugen kurzer Impulse .....	164
4.8	1-Photonen-Emitter .....	165
4.9	Erzeugen verschränkter Photonenpaare .....	168
4.9.1	Induzierte Konversion .....	168
4.9.2	Quantenpunkt-Laserdioden und Verschränkung .....	173
4.10	Komponenten des optischen Erzeugungssystems .....	174
4.10.1	Komplettsystem .....	174
4.10.2	Strahlenvereinigung .....	176
4.10.3	Interferenzfilter .....	176
4.10.4	Abschwächer .....	177
4.10.5	Polarisatoren/Analysatoren .....	177
4.10.6	Phasenschieber und Rotatoren .....	178
4.10.7	Systemeichung .....	181
4.11	Übertragung polarisierter Photonen .....	182
4.11.1	Luftübertragung .....	182
4.11.2	Lichtwellenleiter .....	183
4.11.3	Selbstkompensierende Systeme .....	185
4.12	Detektion polarisierter Photonen .....	188
4.12.1	Messanordnung .....	188
4.12.2	Photodetektor .....	190
4.12.3	Neutrale Strahlenteiler .....	190
4.12.4	Polarisierende Strahlenteiler .....	191
4.13	Realisierte Angriffe .....	192
4.13.1	Trojaner .....	192
4.13.2	Zeitverschiebungsangriffe .....	195
4.13.3	Phasenverschiebungsangriffe .....	197
4.14	Die Zukunft der Quantenkryptografie .....	199

<b>5</b>	<b>Teleportation</b>	203
5.1	Nur Science Fiction?	203
5.2	Funktionsprinzip der Teleportation	204
5.3	Ein einfaches Protokoll für die Teleportation	206
5.3.1	Die Theorie	206
5.3.2	Das Experiment	209
5.4	Komplexere Protokolle	213
5.4.1	Theorie zum Transport von Mehrteilchensystemen	213
5.4.2	Experimentelle Nachweise	216
5.5	Fehlerverminderung	216
5.6	Speicherung verschränkter Zustände	218
5.7	Transport ohne verschränktes Teleportersystem	219
5.8	Praktische Auswirkungen	222
<b>6</b>	<b>Quantencomputer</b>	225
6.1	Funktionsweise von Quantenrechnern	225
6.2	Konsequenzen von Quantencomputern	228
6.3	Elemente eines Quantencomputers	230
6.3.1	Das Qbit und das Qbit-Register	230
6.3.2	Basis-Operatoren im Quantencomputer	231
6.3.2.1	Grundsätzliches	231
6.3.2.2	NOT-Operation	235
6.3.2.3	Controlled-NOT-Operation	235
6.3.2.4	Toffoli-Operation oder CCNOT	237
6.3.2.5	Der SWAP- und der cSWAP-Operator	239
6.3.2.6	Der Hadamard-Operator	240
6.3.2.7	Wurzeln aus NOT- und SWAP-Operatoren	240
6.3.3	Elementaroperationen: Rotationen und Phasenverschiebungen	241
6.3.4	Zerlegung von Quantenoperatoren	242
6.3.4.1	Zerlegung unitärer Transformationen	243
6.3.4.2	Kontrollierte Phasendrehung	244
6.3.4.3	Beliebige durch 1 Qbit kontrollierte Operationen	244
6.3.4.4	Realisierung der CNOT-Operation	245
6.3.4.5	Operationen mit mehreren Kontrollbits	248
6.3.5	Aufwandsbilanz	251
6.4	Arithmetische Operationen	252
6.4.1	Operationsfolgen und Quantenregister	252
6.4.2	Fourier-Transformation	255
6.4.3	Additionsalgorithmen	257
6.4.3.1	Notationen	258
6.4.3.2	Klassische Addition mit Hilfsregister	260
6.4.3.3	Kontrollierte Addition	263
6.4.3.4	Qbit-sparende Addition	264

6.4.3.5	Quantenaddition .....	267
6.4.3.6	Modulare Addition .....	268
6.4.4	Multiplikation .....	270
6.4.4.1	Die klassische Multiplikation .....	270
6.4.4.2	Divisionsalgorithmus .....	272
6.4.4.3	Modulare Multiplikation .....	273
6.4.5	Modulare Exponentiation .....	275
6.4.6	Zusammenfassung .....	277
6.5	Problemlösungen mit Quantencomputern .....	278
6.5.1	Suchen in unsortierten Mengen .....	279
6.5.1.1	Ein Suchalgorithmus auf Quantencomputern .....	280
6.5.1.2	Effizienz der Algorithmus .....	285
6.5.1.3	Zählen der Zustände .....	287
6.5.1.4	Die Orakel-Funktion .....	288
6.5.2	Der Faktorisierungsalgorithmus von Shor .....	293
6.5.2.1	Der klassische Ansatz .....	293
6.5.2.2	Die Quantencomputerversion .....	294
6.5.2.3	Der Quanten-Algorithmus im Detail .....	296
6.5.2.4	Ermittlung der Periode .....	299
6.5.2.5	Erfolgswahrscheinlichkeit .....	300
6.5.3	Verschlüsselung auf Basis des diskreten Logarithmus .....	301
6.5.4	Fazit .....	302
6.6	Fehlerkorrekturverfahren .....	303
6.6.1	Allgemeines .....	303
6.6.2	Bitflips und ihre Korrektur .....	305
6.6.3	Phasenflips und ihre Korrektur .....	306
6.7	Simulation auf klassischen Systemen .....	307
6.7.1	Was können wir simulieren? .....	308
6.7.2	Datentypen .....	309
6.7.3	Rechenoperatoren und Tensorprodukte .....	312
6.7.4	Unitäre Transformationen .....	314
6.7.5	Kontrollierte Transformationen .....	317
6.7.6	Operationen auf großen Quantenregistern .....	324
6.7.7	Messung .....	329
6.7.8	Statistisches .....	332
6.7.9	Fehlersimulation .....	334
6.7.10	Ein Simulationsbeispiel: Suchalgorithmus nach Grover .....	335
6.7.11	Weitere Aufgaben .....	337
6.8	Nicht lokale Quantensysteme .....	337
6.8.1	Entfernte Rotation .....	338
6.8.2	Entfernte CNOT-Operation .....	340
6.9	Technische Realisierung von Quantenrechnern .....	341
6.9.1	Übersicht .....	342
6.9.2	Optische Quantencomputer .....	345

6.9.3	Kernspinresonanz in Molekülen .....	346
6.9.4	Kernspinresonanz in Festkörpern .....	348
6.9.5	Klassische Ionenfallen .....	356
6.9.6	Halbleiter-Ionenfallen und anderes .....	364
6.9.7	Cooper-Paare in supraleitenden Materialien .....	365
6.9.8	Dissipative Systeme .....	366
6.10	Fazit und Ausblick .....	367
<b>Sachverzeichnis .....</b>		<b>371</b>