

# Quantenkommunikationsnetze

Riccardo Bassoli • Holger Boche •  
Christian Deppe • Roberto Ferrara •  
Frank H. P. Fitzek • Gisbert Janssen •  
Sajad Saeedinaeeni

# Quantenkommunikationsnetze

Riccardo Bassoli  
Centre for Tactile Internet with  
Human-in-the-Loop (CeTI)  
Technische Universität Dresden  
Dresden, Deutschland

Holger Boche  
Technische Universität München, Münchner  
Zentrum für Quantenforschung Wissenschaft  
und Technologie  
München, Deutschland

Christian Deppe  
Technische Universität München  
München, Deutschland

Roberto Ferrara  
Technische Universität München  
München, Deutschland

Frank H. P. Fitzek  
Centre for Tactile Internet with  
Human-in-the-Loop (CeTI)  
TU Dresden  
Dresden, Deutschland

Gisbert Janssen  
Technische Universität München  
München, Deutschland

Sajad Saeedinaeni  
Technische Universität München  
München, Deutschland

Dieses Buch ist eine Übersetzung des Originals in Englisch „Quantum Communication Networks“ von Bassoli, Riccardo, publiziert durch Springer Nature Switzerland AG im Jahr 2021. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung durch den Dienst DeepL.com). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

ISBN 978-3-031-26325-5      ISBN 978-3-031-26326-2 (eBook)  
<https://doi.org/10.1007/978-3-031-26326-2>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Nature Switzerland AG 2023

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Axel Garbers

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Nature Switzerland AG und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Gewerbestrasse 11, 6330 Cham, Switzerland

# Vorwort

Wenn man einen kurzen Blick auf dieses Buch wirft, könnte man meinen: *Oh, hier kommt ein weiteres Buch über Quantencomputer, Quanteninformationstheorie und Quantenkommunikation!* Das mag teilweise stimmen. Die Quantenmechanik wurde zu Beginn des letzten Jahrhunderts geboren und hat im Laufe der Jahrzehnte große Popularität in der Mathematik und Physik erlangt. Darüber hinaus wurde die Quantenmechanik in den letzten 40–50 Jahren auf die Informatik und die Informationstheorie angewandt. In jüngster Zeit findet sie sich auch in der Kommunikation wieder.

Wenn man also die verfügbare wissenschaftliche Literatur durchforstet, findet man zahlreiche Bücher über Quantenmechanik, Quantencomputer und Quanteninformationstheorie sowie einige Werke über Quantenkommunikation. Die Frage ist also: *Ist dieses Buch im Panorama der wissenschaftlichen Literatur notwendig?* Die Antwort ist ja, und es gibt einige wichtige Gründe, die dafür sprechen.

Erstens sind viele der Bücher nicht sehr aktuell (vor allem aus der Sicht der Kommunikation), so dass sie einige wichtige Neuerungen gänzlich fehlen. Außerdem handelt es sich bei den meisten Büchern um Monographien, die sich auf bestimmte Forschungsbereiche der Quantentheorie und ihrer Anwendungen konzentrieren.

Zweitens hat nach dem bestem Wissen der Autoren noch kein Buch die neuen Perspektiven berücksichtigt, die Kommunikationsnetze allmählich erlangt haben. Tatsächlich vollzieht sich bei den Kommunikationsnetzen derzeit ein Paradigmenwechsel, bei dem die einfachen Transportkonzepte unserer ersten Kommunikationsnetze durch Rechen- und Speicherfunktionen ergänzt werden. Diese *softwarisierten* Lösungen bieten neue Möglichkeiten zur Verringerung der Latenzzeit und zur Erhöhung der Ausfallsicherheit, haben aber aufgrund der eingeführten Rechenlatenz und des Energieverbrauchs ein inhärentes Problem. Dieses Problem kann durch hybride klassisch-quantische Kommunikationsnetze gelöst werden.

Dieses Buch übernimmt das bestehende Paradigma des Rechnens in Netzwerken und nutzt es, um zukünftige Quantenkommunikationsnetzwerke zu beschreiben (die nicht nur das Quanteninternet sein werden). Das Buch konzentriert sich dabei auf

Quantencomputing, Quanteninformationstheorie, Quantenfehlerkorrektur und Architektur auf der Systemebene als verschiedene Bausteine, die künftige Compute-and-Forward-Quantenkommunikationsnetze aufbauen werden. Der Ansatz, der für die Darstellung der Theorie von Quantenkommunikationsnetzen verwendet wird, leiht sich einige Gesichtspunkte aus der laufenden Arbeit der IETF Quantum Internet Research Group (qirg) (an der die Autoren beteiligt sind). Dieses Buch erweitert und verallgemeinert diese Ansichten jedoch auch, um dem Leser die Freiheit zu geben, neue Entwürfe und Lösungen ohne architektonische Einschränkungen zu erforschen und zu entwickeln. Dies ist besonders in einem neuen Bereich wie den Quantenkommunikationsnetzen wichtig, in dem es noch keine standardisierten Lösungen gibt.

Nicht zuletzt greift dieses Buch ein Thema auf, das in diesem Bereich noch nie in Büchern behandelt wurde: das Forschungsproblem klassisch getesteter (mittels Software-Simulationen) quantenmechanischer Systeme. Aus diesem Grund werden am Ende des Buches bestehende Simulatoren von Quantenkommunikationsnetzen vorgestellt und ihre Vor- und Nachteile hervorgehoben. Auf diese Weise wird der Leser für diese wichtige offene Frage sensibilisiert, wenn es um die Erforschung von Quantenkommunikationsnetzen geht. Schließlich werden auch einige potenzielle Anwendungen von Quantenkommunikationsnetzen beschrieben. Dies stellt auch einen praktischen Gesichtspunkt für den Leser dar.

Als Autoren, die Experten auf den Gebieten der vorgestellten Forschung sind, hoffen wir, dass das Buch die Bedeutung quantenmechanischer Ressourcen für die effektive und effiziente Entwicklung zukünftiger Kommunikationsnetze vermittelt. Als wir dieses Manuskript schrieben, wollten wir sowohl Physikern als auch Ingenieuren ein wertvolles Nachschlagewerk für ihre Forschung auf dem Gebiet der Quantenkommunikationsnetze (und ihrer Teilgebiete) an die Hand geben. Darüber hinaus haben wir die Struktur und die Terminologie so geplant, dass sie sowohl genau als auch zugänglich sind, um ein hilfreiches Hilfsmittel für Vorlesungen in der Hochschulbildung und für Schulungen in der Industrie darzustellen.

Dresden, Deutschland  
September 2020

Riccardo Bassoli

# Danksagungen

Wir danken der Deutschen Telekom für die Unterstützung von R. Bassoli und F. Fitzek im letzten Jahr und für ihre Motivation, sich mit dem Thema der Quantenkommunikationsnetze zu beschäftigen.

Wir danken auch dem CeTI-Team für die Unterstützung von R. Bassoli und F. Fitzek. Das CeTI wird von der Deutschen Forschungsgemeinschaft (DFG) im Rahmen der Exzellenzstrategie EXC 2050/1 – Projekt ID 390696704 – Exzellenzcluster „Centre for Tactile Internet with Human-in-the-Loop“ (CeTI) der Technischen Universität Dresden gefördert.

Wir danken der Deutschen Forschungsgemeinschaft (DFG) im Rahmen des Gottfried Wilhelm Leibniz-Preises unter dem Förderkennzeichen BO 1734/20-1 für die Unterstützung von H. Boche und C. Deppe.

Darüber hinaus danken wir dem Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der nationalen Initiative für „Q.Link.X-Quantum Link Extended“ mit dem Projekt „System Design for Secure Quantum Repeater Systems: Basic Protocols and Secure Implementation“ unter dem Förderkennzeichen 16KIS0858 für die Unterstützung von H. Boche, G. Janssen und S. Saeedinaeeni und im Rahmen des Projekts „Quantum Information Theory and Communication Theory for Quantum Repeaters Beyond the Shannon Approach“ unter dem Förderkennzeichen 16KIS0856 für die Unterstützung von C. Deppe und R. Ferrara.

Wir danken auch dem Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der nationalen Initiative für „Q.COM-Quantum Communication“ mit dem Projekt „Information Theory of the Quantum Repeater: Abhörsichere Kommunikation, Angriffe und Systementwurf“ unter dem Förderkennzeichen 16KIS0118 für die Unterstützung von H. Boche und G. Janssen und mit dem Projekt „Abhörsichere Kommunikation über Quantenrepeater bei Nutzung unterschiedlicher Ressourcen“ unter dem Förderkennzeichen 16KIS0117 für die Unterstützung von C. Deppe.

Dank geht auch an das Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der nationalen Initiative „Post Shannon Communication (NewCom)“ mit dem Projekt „Grundlagen, Simulation und Demonstration für neue Kommunikationsmodelle“ unter dem Förderkennzeichen 16KIS1003K für die Unterstützung

von H. Boche und mit dem Projekt „Codierungstheorie und Codierungsverfahren für neue Kommunikationsmodelle“ unter dem Förderkennzeichen 16KIS1005 für die Unterstützung von C. Deppe und R. Ferrara.

Außerdem danken wir der Deutschen Forschungsgemeinschaft (DFG) im Rahmen der Exzellenzstrategie EXC-2111-390814868 für die Unterstützung von H. Boche und S. Saeedinaeni.

Darüber hinaus danken wir Werner Moorfeld für seine kontinuierlichen Bemühungen, verschiedene Gemeinschaften und Expertise zusammenzubringen. Die vielen wertvollen Diskussionen, die wir gemeinsam geführt haben, bildeten den Ausgangspunkt für dieses Buchprojekt.

Schließlich möchten wir E. Soeder für das Korrekturlesen des Buches und die sprachlichen Anregungen danken.

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	1
1.1	Die Entwicklung der klassischen Kommunikationsnetze	1
1.2	Auf dem Weg zu Quantenkommunikationsnetzen	6
1.3	Aufbau des Buches	11
<b>2</b>	<b>Grundlegender Hintergrund</b>	13
2.1	Vorbemerkungen zur Quantenmechanik	13
2.1.1	Postulate der Quantenmechanik	14
2.1.2	Formulierung der Quantenmechanik	16
2.1.3	Zusammengesetzte Systeme und Verschränkung	25
2.1.4	Zusammengesetzte Beobachtungswerte	28
2.2	Rauschen in Quantensystemen	30
2.2.1	Dichtematrix	31
2.2.2	Die Bloch-Sphäre eines Qubits	34
2.2.3	Komposit-Systeme	36
2.2.4	Quantenkanäle	38
2.3	Messungen	41
2.4	Quanteninformation	48
2.4.1	Statistische Theorien	48
2.4.2	Abstandsmaßnahmen	53
2.4.3	Quantenentropie	55
2.5	Bell-Nichtlokalität	58
2.5.1	Nichtlokale Spiele	68
2.6	Klassische Mechanik und Quantenmechanik	72
<b>3</b>	<b>Quantencomputing und Programmierung</b>	75
3.1	Universal-Gate-Sets	76
3.1.1	Quantenschaltkreis-Modell	77
3.1.2	Quantum Universal Gate Sets	83
3.2	Berechnungskomplexität	84
3.3	Die Quanten-Fourier-Transformation	87



3.4	„Orakel- und Versprechenprobleme“?	89
3.5	Interferenz: Ausgewogene Funktionen	93
3.5.1	Deutsch Algorithmus	94
3.5.2	Deutsch-Jozsa-Algorithmus	95
3.5.3	Bernstein-Vazirani-Algorithmus	96
3.6	Messungen: Versteckte Untergruppen	97
3.6.1	Mitgesetzte Zustände	99
3.6.2	Periodenfindungs-Algorithmus	100
3.6.3	Simons Algorithmus	102
3.7	Phasenabschätzung	102
3.8	Anwendung: Auftragsfindung und RSA	105
3.9	Grovers Suche	107
3.10	Quantensimulation	109
3.11	Andere Anwendungen	111
3.12	Unmittelbare Zukunft	112
<b>4</b>	<b>Quanteninformationstheorie</b>	<b>115</b>
4.1	Dichte Kodierung und Teleportation	118
4.2	Quanten-Hypothesentest: Quanten-Steinsches Lemma	122
4.3	Quellenkompression für speicherlose Quantenquellen	124
4.4	Nachrichtenübertragung über Quantenkanäle	127
4.4.1	Der diskrete speicherlose klassisch-quantische Kanal	127
4.4.2	Der diskrete speicherlose Quantenkanal	130
4.4.3	Einige Eigenschaften der Holevo-Menge	133
4.5	Verschrankungsunterstützte klassische Kommunikation	133
4.6	Informationstheoretische Sicherheit und CQQ-Abhörmodell	138
4.7	Öffentliche und sichere Identifizierung	140
4.7.1	Identifizierung über CQ-Kanäle	140
4.7.2	Sichere Identifizierung	143
4.8	Kanalunsicherheit: Zusammengesetzte und willkürlich schwankende Modelle	145
4.8.1	Notationen und Konventionen	148
4.8.2	Gleichzeitige Übertragung von klassischer und Quanteninformation	150
4.8.3	Zusammengesetzter Quanten-Rundfunkkanal mit vertraulichen Nachrichten	162
4.8.4	Robuste sichere Nachrichtenübertragung über den Abhörkanal mit einem Störsender	170
4.8.5	Robuste Identifikation über CQ-Kanal für öffentliche und sichere Kommunikation	174
<b>5</b>	<b>Quantenfehlerkorrektur</b>	<b>181</b>
5.1	Vorwärts-Fehlerkorrektur-Codes	182
5.2	Bit- und Phasenfehler: Quanten-Wiederholungskode	185
5.3	Einzelner Pauli-Fehler: Shor's Fehlerkorrektur-Code	188

5.4	Fehlerkorrekturbedingung und Codeabstand . . . . .	190
5.5	Lineare Codes und Stabilisator-Codes . . . . .	193
5.5.1	Lineare Block-Codes . . . . .	194
5.5.2	Stabilisator Codes . . . . .	194
5.5.3	Calderbank-Shor-Steane (CSS) Codes . . . . .	196
5.6	Universelle Logical-Gate-Sets . . . . .	197
5.7	Topologische Stabilisator-Codes . . . . .	199
5.7.1	Der torische Code . . . . .	203
5.7.2	Farbcodes . . . . .	204
<b>6</b>	<b>Quantenkommunikationsnetze: Entwurf und Simulation . . . . .</b>	<b>209</b>
6.1	Destillation in Quanten-Repeatern . . . . .	212
6.2	Taxonomie der Quanten-Repeater . . . . .	216
6.3	Speicherung in Quanten-Repeatern . . . . .	218
6.4	Verschrankungsverteilung . . . . .	222
6.5	Kanal mit Mehrfachzugriff in Quantenkommunikationsnetzen . . .	227
6.6	Klassische Simulation von Quantenkommunikationsnetzen . . . .	228
6.6.1	SimulaQron . . . . .	229
6.6.2	NetSquid . . . . .	230
6.6.3	QuNetSim . . . . .	231
6.6.4	QUADRAT . . . . .	232
6.6.5	SeQUeNZe . . . . .	232
6.6.6	QuISP . . . . .	233
6.6.7	LIQUiI) . . . . .	233
<b>7</b>	<b>Quantenkommunikationsnetze: Abschließende Überlegungen und Anwendungsfälle . . . . .</b>	<b>235</b>
<b>Literatur</b>	<b>. . . . .</b>	<b>239</b>

## Über die Autoren



**Riccardo Bassoli** ist wissenschaftlicher Mitarbeiter am Deutsche Telekom Lehrstuhl für Kommunikationsnetze, Fakultät Elektrotechnik und Informatik, Technische Universität Dresden (Deutschland). Er erhielt seinen B. Sc. und M.Sc. in Telekommunikationstechnik von der Universität Modena und Reggio Emilia (Italien) in den Jahren 2008 bzw. 2010. Anschließend promovierte er 2016 am 5G Innovation Centre der University of Surrey (Großbritannien). Außerdem war R. Bassoli Marie Curie ESR am Instituto de Telecomunicações (Portugal) und Gastforscher bei Airbus Defence and Space (Frankreich). Von 2016 bis 2019 war er Postdoktorand an der Universität von Trient (Italien). Er ist Mitglied von IEEE und ComSoc. Außerdem ist R. Bassoli Mitglied des technischen Gremiums „Glue Technologies for Space Systems“ des IEEE AESS.



**Holger Boche** erhielt an der Technischen Universität Dresden 1990 den Titel Dipl.-Ing. in der Elektrotechnik, 1992 den Dipl.-Ing. in der Mathematik und promovierte 1994 zum Dr.-Ing. in der Elektrotechnik. 1998 wurde er an der Technischen Universität Berlin zum Dr. rer. nat. in reiner Mathematik promoviert. Von 1994 bis 1997 absolvierte er ein Postgraduierenstudium an der Friedrich-Schiller-Universität Jena. 1997 wechselte H. Boche an das Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Berlin. Von 2002 bis 2010 war er ordentlicher Professor für mobile Kommunikationsnetze am Institut für Kommunikationssysteme der Techni-

schen Universität Berlin. Im Jahr 2003 wurde er Leiter des Fraunhofer German-Sino Laboratory for Mobile Communications, Berlin, und 2004 wurde er Leiter des Fraunhofer-Instituts für Nachrichtentechnik (HHI), Berlin, Deutschland. Derzeit ist H. Boche ordentlicher Professor am Institut für Theoretische Informationstechnik der Technischen Universität München, wo er seit Oktober 2010 tätig ist.



**Christian Deppe** erhielt 1996 das Diplom in Mathematik von der Universität Bielefeld, Bielefeld, Deutschland, und 1998 den Dr.-Math. von der Universität Bielefeld, Bielefeld, Deutschland. Von 1998 bis 2010 war er wissenschaftlicher Mitarbeiter und Lehrbeauftragter an der Fakultät für Mathematik der Universität Bielefeld. Von 2011 bis 2013 war C. Deppe Projektleiter des Projekts „Sicherheit und Robustheit des Quanten-Repeater“ des Bundesministeriums für Bildung und Forschung an der Fakultät für Mathematik der Universität Bielefeld. 2014 wurde er im Rahmen eines DFG-Projekts am Institut für Theoretische Informationstechnik der Technischen Universität München gefördert. Im Jahr 2015 hatte C. Deppe eine befristete Professur an der Fakultät für Mathematik und Informatik der Friedrich-Schiller Universität Jena. Derzeit ist er Projektleiter des Projekts „Abhörsichere Kommunikation über Quanten-Repeater“ des Bundesministeriums für Bildung und Forschung an der Fakultät für Mathematik, Universität Bielefeld. Seit 2018 ist zudem er am Lehrstuhl für Nachrichtentechnik an der Technischen Universität München tätig.



**Roberto Ferrara** erwarb seinen M.Sc. in Physik am Niels-Bohr-Institut der Universität Kopenhagen und seinen Dokortitel in Naturwissenschaften an der Abteilung für mathematische Wissenschaften der Universität Kopenhagen. In seiner Dissertation „An Information-Theoretic Framework for Quantum Repeaters“ untersuchte er die Grenzen der Destillation von zweiseitigen klassischen Schlüsseln aus Quantenzuständen, wenn die beiden Parteien die Verschränkung nur mit Hilfe einer dritten Partei, dem Quantenrepeater, teilen können, und behandelte dabei Themen wie Verschränkungsmaße, Quantenopera-

tionen und Quanteninformationstheorie. Seit 2019 ist R. Ferrara am Lehrstuhl für Nachrichtentechnik an der Technischen Universität München tätig.



**Frank H. P. Fitzek** ist Professor und Leiter des Deutsche Telekom Lehrstuhls für Kommunikationsnetze an der Technischen Universität Dresden und koordiniert das 5G Lab Germany. Er ist der Sprecher des DFG-Exzellenzclusters CeTI. F. Fitzek erhielt sein Diplom (Dipl.-Ing.) in Elektrotechnik von der Rheinisch-Westfälischen Technischen Hochschule (RWTH) Aachen, Deutschland, im Jahr 1997 und seinen Dokortitel (Dr.-Ing.) in Elektrotechnik von der Technischen Universität Berlin, Deutschland, im Jahr 2002 und wurde im selben Jahr außerordentlicher Professor an der Universität von Ferrara, Italien. Im Jahr 2003 wechselte er als außerordentlicher Professor an die Universität Aalborg und wurde später zum Professor ernannt. Im Jahr 2005 gewann F. Fitzek den YRP-Preis für seine Arbeit über MIMO MDC und erhielt den Young Elite Researcher Award of Denmark. Von 2007 bis 2011 wurde er mehrmals in Folge mit dem NOKIA Champion Award ausgezeichnet. Im Jahr 2008 wurde er mit dem Nokia Achievement Award für seine Arbeit über kooperative Netzwerke ausgezeichnet. Im Jahr 2011 erhielt F. Fitzek das SAPERE AUDE-Forschungsstipendium der dänischen Regierung und im Jahr 2012 den Vodafone-Innovationspreis. Im Jahr 2015 wurde ihm von der Budapester Universität für Technologie und Wirtschaft (BUTE) der Ehrentitel „Doctor Honoris Causa“ verliehen.



**Gisbert Janssen** war von 2010 bis 2019 als wissenschaftlicher Mitarbeiter am Institut für Theoretische Informationstechnik der Technischen Universität München tätig. Er erhielt 2010 ein Physik-Diplom von der Technischen Universität Berlin und 2016 den Dr. rer. nat. von der Technischen Universität München.



**Sajad Saeedinaeeni** erwarb 2010 den B.Sc. und 2015 den M.Sc. in Physik an der Royal Holloway University of London bzw. der Universität Leipzig. Er schrieb seine Masterarbeit über Quantenhypothesentests am Max-Planck-Institut für Mathematik in Leipzig. Derzeit promoviert er zum Dr. rer. nat in Physik am Institut für Theoretische Informationstechnik der Technischen Universität München (TUM) unter der Betreuung von Holger Boche.