acatech

HORIZONTE

Quantentechnologien

Warum sind Quanten wichtig?

Grundlagen für das Verständnis der Quantentechnologien

Quantentechnologien der ersten und zweiten Generation

Gestaltungsspielräume und Erwartungsmanagement

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Mit der vorliegenden Publikationsreihe untersucht acatech bedeutende Technikfelder, die sich klar am Horizont abzeichnen, deren Auswirkungen aber noch geklärt werden müssen. Diese Technikfelder werden in acatech HORIZONTE fundiert und anschaulich aufbereitet. In diesen Prozess fließen der aktuelle Stand der internationalen Forschung, Entwicklung und Anwendung sowie die Wertschöpfungspotenziale der Technologien ein. Darüber hinaus nehmen die acatech HORIZONTE ethische, politische und gesellschaftliche Fragen sowie denkbare Entwicklungen und Gestaltungsoptionen in den Blick. Mit den acatech HORIZONTEN möchte die Akademie die Diskussion über neue Technologien anregen, politische Gestaltungsräume aufzeigen und Handlungsoptionen formulieren – und so einen Beitrag für eine vorausschauende Innovationspolitik leisten.

3.2.2 Quantenkommunikation und Quantenkryptografie

Wird der Quantencomputer realisiert, kann sich das auch auf die Sicherheit unserer Kommunikation auswirken: Denn ein Quantencomputer könnte viele Verschlüsselungsmethoden, die wir gegenwärtig verwenden, „knacken". Deshalb müssen unsere Sicherheitssysteme grundlegend überdacht und überarbeitet werden, um die Sicherheit unserer Kommunikation auch für die nächsten Jahrzehnte gewährleisten zu können. Hier setzen die Quantenkommunikation und die sogenannte Quantum-Safe-Kryptografie (diese wird häufig auch als „Post-Quantum-Kryptografie" bezeichnet) an, deren Verschlüsselung selbst ein Quantencomputer nicht knacken kann.

Quantenkommunikation

„Quantenkommunikation" ist ein Überbegriff für die Vermittlung einer Nachricht mittels Quantenkryptografie, das heißt die Übertragung von Verschlüsselungscodes mithilfe von kodierten Photonen (zur genauen Funktionsweise siehe Seite 42). Bei der (Quanten-) Kryptografie geht es darum, einen Schlüssel, den nur Sender und Empfänger kennen sollten, auf sichere Weise auszutauschen. Das heißt, es wird nicht die ganze Nachricht mittels Quantenkryptografie übertragen, sondern nur der Schlüssel zum Ver- und Entschlüsseln der Nachricht. Die eigentliche Kommunikation findet dann ganz ohne die Mitwirkung von Quanten über klassische Wege statt, beispielsweise durch das Versenden einer (verschlüsselten) Nachricht per E-Mail.

Während für Quantencomputer hochsensible und instabile Quantensysteme verwendet werden, benutzt man in der Quantenkommunikation und -kryptografie sehr stabile Quanten, die Photonen. Bisher haben wir das Photon nur als Quant kennengelernt, das in der Lage ist, den Zustand eines Quantensystems, etwa eines Atoms, zu modifizieren (siehe Kapitel 2). Das Photon ist allerdings auch selbst in der Lage, zwei unterschiedliche Zustände einzunehmen.[d] Man spricht hier auch von „Polarisation". Bezeichnet man wie beim Computer einen Zustand als 1 und den anderen Zustand als 0, kann man durch Messen, in welchem dieser Zustände sich das Photon befindet, Informationen übertragen und erhalten. Das Photon ist also nicht nur ein Quant, sondern auch ein Qubit.

Photonen-Qubits werden auch als „fliegende Qubits" bezeichnet, da sie mit Lichtgeschwindigkeit durch den Raum fliegen. Fliegende Qubits sind sehr robust: Solange sie existieren, behalten sie ihren Zustand stabil bei. Diejenigen, die es bis zum Empfänger schaffen, sind also vollkommen unverändert. Ein Problem ist jedoch, dass Photonen auf dem Weg vom Sender zum Empfänger durch Interaktion mit ihrer Umgebung verloren gehen können, indem sie zum Beispiel absorbiert werden.

Herausforderungen bestehen in der Quantenkryptografie momentan darin, dass die Datenraten noch nicht ausreichend sind und die Reichweite der auf einzelnen Photonen beruhenden Quantenschlüsselverteilungstechnologie (Quantum Key Distribution, kurz: QKD) über Glasfaser nur etwa hundert Kilometer beträgt. Möchte man Informationen über eine längere Strecke übertragen, benötigt man einen Vermittler dazwischen, der den Schlüssel weitergeben kann. Dieser Vermittler erzeugt Schlüssel mit dem Sender und dem Empfänger, gleicht diese ab und autorisiert schließlich einen gemeinsamen Schlüssel. Das setzt voraus, dass der Vermittler vertrauenswürdig ist. Eine Schwachstelle des Ansatzes mit dem Vermittler ist, dass sich an den Knotenpunkten, an denen dieser sitzt (also tatsächlich ein physisches Gebäude), auch Lauscher unberechtigten Zugang verschaffen könnten. Diese Orte müssen also gesichert werden. Allerdings ist es auch heute schon üblich, große Rechenzentren mit hohen Sicherheitsvorkehrungen zu umgeben.[19]

Ein üblicher Verstärker oder Repeater, wie man ihn in kleiner Form beispielsweise vom WLAN-System in Privathaushalten kennt, ist hingegen nicht zur Erhöhung der Reichweite einsetzbar, da unbekannte Quantenzustände nicht geklont und so verstärkt oder weitergereicht werden können (siehe Non-Cloning-Theorem auf Seite 42). Eine vielversprechende Möglichkeit, dies zu umgehen, ist aber der sogenannte Quanten-Repeater, der Quellen für verschränkte Photonenpaare und Verschränkungsaustausch über größere Distanzen hinweg nutzt, um deutlich höhere Reichweiten und Schlüsselraten zu erzielen. Die dafür nötigen Technologien werden derzeit im Labor entwickelt und getestet.[20]

Die kommerzielle Nutzung der glasfaserbasierten Quan-

d Das Photon bringt alle Voraussetzungen mit, die wir von einem idealen Übermittler von Information erwarten würden: Es ist Träger eines Drehimpulses, des Spin, der zwei Einstellrichtungen hat und das Photon zu einem Zwei-Zustands-System macht. Auch hier stehen alle Superpositionszustände zur Verfügung.

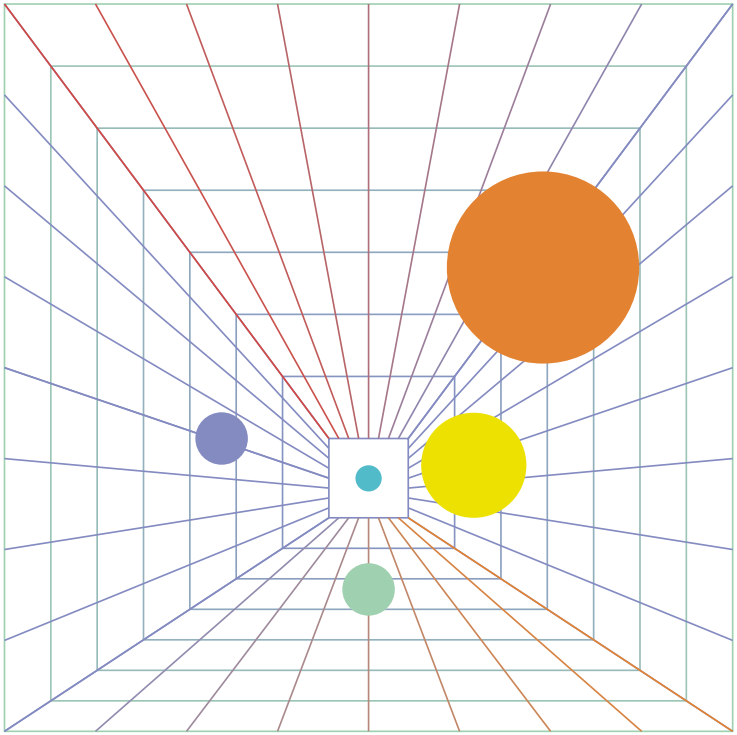
tenkommunikation erfordert auch den Aufbau eines neuen Quantennetzwerks, das aus qualitativ hochwertigen, dämpfungsarmen und „dunklen", das heißt exklusiv für QKD genutzten, Glasfasern besteht. Da der Aufbau einer derartigen Infrastruktur sehr teuer ist, wird erwartet, dass die QKD-Technologie in der Anfangsphase primär von Nutzern mit höchsten Sicherheitsbedürfnissen eingesetzt werden wird.

Es gibt jedoch alternative Technologien zur Glasfaser, die die genannten Probleme umgehen. Einige Wissenschaftler nutzen statt Glasfasernetzwerken Satelliten für QKD.[21] Dabei machen sie sich die Tatsache zunutze, dass sie ihre Photonen ungestört über einen großen Teil der Strecke durch das Beinahe-Vakuum des Weltraums senden können. Doch auch hier gibt es noch einige Herausforderungen, die überwunden werden müssen. Der Photonenstrahl, der vom Satelliten ausgesendet wird, muss auf den Empfänger ausgerichtet bleiben, während der Satellit in 300 Kilometern Höhe mit einer Geschwindigkeit von 8 Kilometern pro Sekunde über die Erde fliegt.[22] Auch die Durchquerung der Luft, sobald sich die Photonen der Erde nähern, stellt eine Herausforderung dar, da sie in der Erdatmosphäre absorbiert, gestreut oder von Wolken gänzlich abgehalten werden können. Da die optische Übertragung per Satellit sehr von atmosphärischen Bedingungen am Boden abhängt, ist diese jedoch nur bei guten Wetterbedingungen möglich. Die Schlüssel, die von einer Station auf der Erde empfangen werden, müssen in einer sicheren Hardware gesammelt und bis zur Verwendung gespeichert werden. Erschwerend kommt hinzu, dass die QKD aktuell nur bei Dunkelheit, also in der Nacht, erfolgen kann, da selbst kleine Mengen von gestreutem Sonnenlicht die hochsensiblen Einzel-Photonen-Detektoren blenden würden. Werden diese Herausforderungen gemeistert, wäre ein sicherer Austausch von Schlüsseln mittels QKD über enorme Reichweiten möglich.

Das ultimative Ziel der Quantenkommunikation ist es, nicht nur Schlüssel sicher zu verschicken, sondern zwei Quantencomputer, die sich zudem in unterschiedlichen Ländern befinden können, komplett miteinander zu koppeln. Dazu könnte der Zustand eines Qubits zwischen zwei Quantencomputern teleportiert werden, was letztlich zum visionären Quanteninternet führen würde. Dies ist allerdings noch Zukunftsmusik, und es gibt viele Probleme, die noch gelöst werden müssen, bevor diese Art der Quantenkommunikation Realität werden kann.

Insgesamt betrachtet bleiben in der Praxis bei der Quantenkommunikation noch weitere Gefahren bestehen, zum Beispiel Schwachstellen im Computer des Senders oder Empfängers, die Zugriff auf bereits entschlüsselte Informationen erlauben. Ein weiterer Schwachpunkt ist der Missbrauch von Identitäten, den auch die Quantenkryptografie nicht lösen kann. Es braucht Authentifizierungsmechanismen, die garantieren, dass Alice wirklich Alice und Bob wirklich Bob ist. Doch diese Risiken gelten natürlich auch für die klassische Kryptografie.

„Auch Quantenkryptografie ist kein Allheilmittel. Wenn man das Passwort aufschreibt und ein Hacker den Zettel findet, bringt auch die sicherste kryptografische Technologie recht wenig."



Quantum Key Distribution

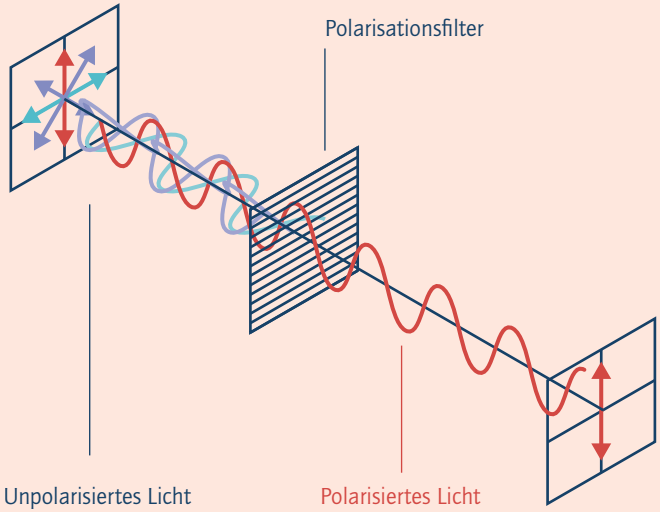
Wie kann man Quanteneigenschaften nutzen, um den Schlüssel zu übertragen, der zum Dekodieren einer verschlüsselten Nachricht benötigt wird? Das Verfahren dafür wird als Quantenschlüsselverteilungs-Technologie oder häufiger als „Quantum Key Distribution" (QKD) bezeichnet. Dabei wird der Schlüssel mittels einer Sequenz aus kodierten Photonen übertragen. Die Sicherheit dieses Verfahrens basiert auf dem Beobachtereffekt und dem sogenannten Non-Cloning-Theorem. Zweiteres besagt, dass ein unbekannter Quantenzustand nicht kopiert werden kann. Dazu müsste das ursprüngliche Photon (= das Quant) gemessen werden. Wie in Kapitel 2.4 beschrieben führt dieser Messprozess aber zu einer Änderung des Zustands. Die Kopie unterscheidet sich dann vom Original. Beispielhaft kann man an ein Bild denken, das kopiert werden muss, ohne dass man es kennt. Doch wie funktioniert QKD genau?

1. Übertragung von Photonen von Alice an Bob

Alice möchte eine Nachricht an Bob senden und dafür QKD nutzen. Zu diesem Zweck sendet sie, vereinfacht gesagt, Photonen oder genauer fliegende Qubits zum Beispiel über eine Glasfaserleitung an Bob, wobei sie die Photonen zuerst „polarisiert". Das heißt nichts anderes, als dass die Photonen[e] in eine bestimmte Richtung schwingen.

In unserem Beispiel werden vier verschiedene Polarisationszustände verwendet: rechts- und linksdiagonal sowie vertikal und horizontal. Alice weist den einzelnen Zuständen dabei Werte zu: Rechtsdiagonale und vertikale Photonen stellen eine 1 dar, linksdiagonale und horizontale Photonen eine 0. Alice verwendet vier verschiedene Filter zur Erzeugung dieser Polarisationszustände, die in zufälliger Reihenfolge eingesetzt werden.

Auf der anderen Seite versucht Bob, die Polarisation der Photonen, die ihm zugeschickt wurden, zu messen. Dafür benutzt er zwei unterschiedliche Detektoreinheiten in zufälliger Reihenfolge. Die eine erlaubt es in der horizontal/vertikal orientierten Basis, Nullen von Einsen eindeutig zu unterscheiden, die andere in der rechts-/linksdiagonal orientierten Basis. Nur wenn er zufällig die passende Detektoreinheit ausgewählt hat, kann er die korrekte Information auslesen. Die Chance dafür ist aufgrund der zufälligen Auswahl der Polarisationsbasen 50/50. Das gehört zum Konzept und stellt die Abhörsicherheit der Kommunikation sicher, wie später noch gezeigt wird.

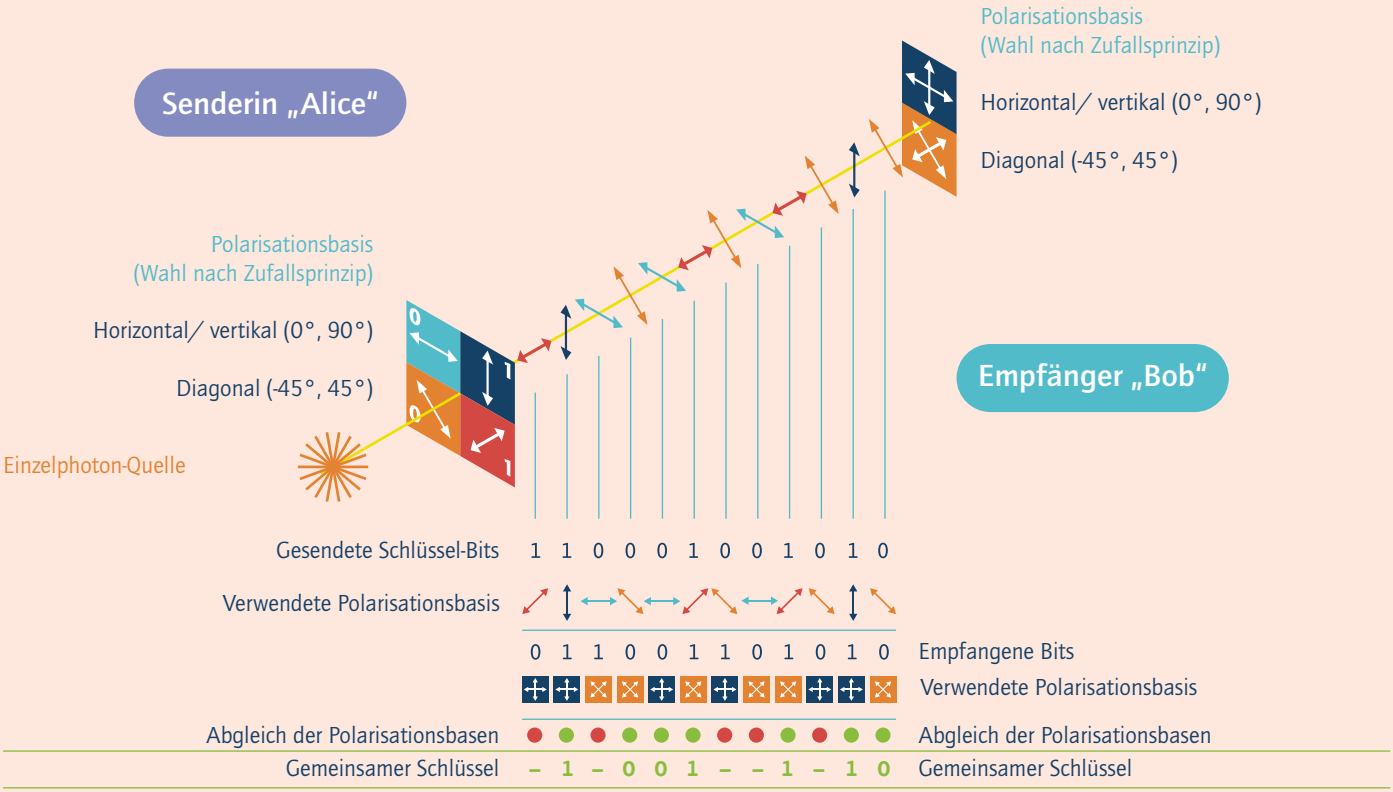


Quelle: Eigene Darstellung nach Zivkovic et al. 2019[23]

2. Identifikation des Schlüssels

Alice und Bob vergleichen nach der Übertragung nur die Einstellungen der jeweils gewählten Polarisationsbasen, um den richtigen Schlüssel zu bestimmen. Dieser Abgleich kann sogar öffentlich, auf klassischem Weg passieren, also zum Beispiel per Telefon. Würde jemand den Vergleich mithören, so würde man beispielsweise nur „horizontal/vertikal" oder „diagonal", aber nicht das dazugehörige Messergebnis, also 1 oder 0, hören. Nach dem Vergleich entfernen Alice und Bob diejenigen Messergebnisse aus der Sequenz, für die Bob eine andere Polarisationsbasis als Alice verwendet hat. Der Quantenschlüssel ergibt sich dann aus den Messergebnissen, bei denen die verwendeten Polarisationsbasen übereingestimmt haben.

e Genauer gesagt die elektrischen Felder dieser Photonen



Quelle: Eigene Darstellung nach Mavroeidis et al. 2018[24]

3. Lauschangriff durch Eve

Die Spionin Eve plant einen Lauschangriff auf Alice und Bob. Dafür versucht sie, erstens den Schlüssel während der Übertragung der Photonen von Alice an Bob abzufangen, und zweitens, den Filtervergleich zwischen Alice und Bob abzuhören. Denn Eve kann mit der Information aus dem Abhören des Filtervergleichs alleine eben nichts anfangen. Auch im ersten Schritt, beim Abfangen des Schlüssels, treten Probleme auf. Wenn Eve, die ebenfalls ihre Filter zufällig wählen muss, die übertragenen Photonen abfängt, kommen sie beim Empfänger gar nicht mehr an: Sie wurden ja von Eve durch ihre „Beobachtung“ entfernt (siehe „Beobachtereffekt“ in Kapitel 2.4) und tragen so nicht mehr zum gemeinsamen Schlüssel von Alice und Bob bei – die Information ist für die Spionin also wertlos.

Alleine durch das Abfangen der Photonen bemerken Bob und Alice noch nicht, dass Eve sie belauschen wollte. Auch wenn Eve einen Teil der Photonen herausfiltert, ist das noch kein Problem für Alice und Bob, die ihren Schlüssel einfach aus dem restlichen Anteil bilden. Da der Übertragungsweg entweder über Glasfaser oder Satellit ohnehin stark verlustbehaftet ist, würden Alice und Bob nicht zwangsweise darauf schließen, dass sie belauscht worden sind.

Wenn Eve nach ihrer Messung vermeintlich passende Ersatzphotonen einschleusen und an Bob weiterleiten würde, hilft ihr das auch nicht weiter, da sie bei falsch eingestellter Polarisationsbasis nur zufällige und damit falsche Messergebnisse erhält und weiterleitet. Dafür sorgt das Non-Cloning-Theorem: Eve kann die Photonen, die sie von Alice abgefangen hat, nicht exakt nachbilden. Alice und Bob würden dann durch Auswertung und Vergleich von Prüfsummen den Angriff erkennen und den gemeinsamen Schlüssel als falsch verwerfen.

Aufgrund dieser Hindernisse, die es Eve unmöglich machen, den Schlüssel zu stehlen, gilt die Übertragung mittels QKD (und genauer per BB84-Protokoll[25]) als abhörsicher.

Quantum-Safe-Kryptografie

Auch wenn es zum Verwechseln ähnlich klingt, bezeichnet die „Quantum-Safe-Kryptografie" ein ganz anderes Verfahren als die Quantenkryptografie, das zudem nichts direkt mit Quanten zu tun hat. Es geht vielmehr darum, gegenwärtige Verschlüsselungsmethoden „quantensicher" zu machen. Der Grund, warum unsere gebräuchlichsten Kryptografieverfahren so leicht von einem Quantencomputer geknackt werden können, ist, dass dieser potenziell über eine extrem hohe Rechenleistung verfügt. Unsere Verschlüsselungsmethoden beruhen unter anderem auf dem mathematischen Problem der Primfaktorzerlegung, für dessen Lösung normale Computer extrem viel Zeit benötigen. Ein universeller Quantencomputer mit ausreichender Anzahl an Qubits könnte dieses Problem allerdings durch Anwendung des sogenannten Shor-Algorithmus sehr effektiv lösen. Der amerikanische Mathematiker Peter Shor entwickelte diesen Algorithmus bereits in den 1990er Jahren.[26] Für kleine Primzahlen wurde experimentell gezeigt, dass der Shor-Algorithmus erfolgreich auf einem Quantencomputer durchgeführt werden kann.[27]

„Wir müssen uns jetzt schon Gedanken machen über die Verschlüsselung von morgen und dürfen nicht warten, bis es zu spät ist. Beim Internet haben wir es verpasst, Sicherheit von Anfang an mitzudenken."

Quantum-Safe-Kryptografie, also quantensichere Kryptografie, befasst sich mit der Suche nach Verschlüsselungsalgorithmen, die gegen Entschlüsselungsversuche sowohl von klassischen als auch von Quantencomputern resistent sind. Die Idee ist, andere mathematische Probleme als die Primfaktorzerlegung zur Verschlüsselung zu verwenden, die von einem Quantencomputer nicht so schnell berechnet werden können. Dabei tappen wir allerdings etwas im Dunkeln, da wir noch nicht sicher wissen, wie viel Zeit ein Quantencomputer für welche Berechnungen benötigen wird. Deshalb wird an unterschiedlichen Ansätzen getüftelt – in der Hoffnung, dass sich einer davon gegen einen möglichen Quantencomputer in der Zukunft behaupten kann. Bei der Quantum-Safe-Kryptografie geht es vor allem darum, die Sicherheit von morgen schon heute mitzudenken und sich auf zukünftige Herausforderungen vorzubereiten – was nicht heißt, dass die Verfahren nicht bereits heute angewandt werden könnten, um unsere Kommunikation schon jetzt sicherer zu gestalten. Deswegen ist die Bezeichnung „Post-Quantum-Kryptografie", die für diesen Bereich häufig auch verwendet wird, eher irreführend.

Implikationen für Wirtschaft und Gesellschaft

Ob wir jemals mit Quantenkommunikation oder quantensicherer Kryptografie eine komplett abhörsichere Kommunikation für alle realisieren können, bleibt ungewiss. Am Ende müssen sich die Verfahren für die Anwender rechnen, das heißt einen Mehrwert bringen. Das mag in manchen Fällen durchaus der Fall sein, denn der Bedarf an Quantenkryptografie ist teilweise tatsächlich schon in sicherheitsrelevanten Bereichen vorhanden. Mit entsprechendem Aufwand können bestimmte wichtige Kanäle, zum Beispiel zwischen wichtigen Behörden, sicherer gestaltet werden. Ähnlich wie beim Quantencomputer könnte es letztlich eine strategische Entscheidung sein, die Technologien dafür hierzulande weiterzuentwickeln oder sie von außen einzukaufen. Gegenwärtig gibt es in Deutschland große Entwicklungsbemühungen in Richtung Quantenkryptografie und auch Quantum-Safe-Kryptografie.[28]

3.2.3 Quantenmetrologie, Quantensensorik und quantenbasierte Bildgebung

Was sind Metrologie, Sensorik und Bildgebung, und wie hängen sie zusammen? Während die Metrologie die Wissenschaft des Messens ist, sind die Sensoren die Geräte, mit denen relevante Messgrößen wie beispielsweise Temperatur oder Beschleunigung im Alltag tatsächlich erfasst werden. Auch für die Bildgebung braucht es einen Sensor, meistens einen optischen Sensor in Form eines Kamerachips. Setzt man ein „Quanten-" vor die Begriffe, also „Quantenmetrologie", „Quantensensorik" und „Quantenbildgebung", bedeutet das, dass die Prozesse des Messens und Erfassens jeweils mithilfe von Quanten geschehen und deshalb sehr genau sind.

Quantenmetrologie

Abstände, Temperatur, Zeit, Druck, Gewicht oder Geschwindigkeit – über all diese physikalischen Größen möchten wir in unserem Alltag oft sehr genau Bescheid wissen. Niemand würde sich gerne in ein Auto ohne Tachometer setzen oder ein Medikament einnehmen, ohne die korrekte Dosierung zu kennen.

Die Quantenmetrologie, auch „quantenbasierte Metrologie" genannt, erforscht, wie Quanteneffekte genutzt werden

Literaturverzeichnis

1 Buhrman, H., Cleve, R., van Dam, W. (2001): zitieren: **„Letter from Einstein to Max Born, 3 March 1947; The Born-Einstein Letters, Correspondence between Albert Einstein and Max and Hedwig Born from 1916 to 1955, Walker, New York, 1971."** In: Quantum Entanglement and Communication Complexity. SIAM Journal on Computing, 30(6):1829–1841.

2 Tegmark, M., Wheeler, J. A. (2001): **100 Years of Quantum Mysteries.** Scientific American.

3 Jaeger, L. (2018): **Die zweite Quantenrevolution.** Vom Spuk im Mikrokosmos zu neuen Supertechnologien. Springer, Berlin.

4 Physikalisch-Technische Bundesanstalt (PTB) (2012): **PTR/PTB: 125 Jahre metrologische Forschung**. Online verfügbar unter https://www.ptb.de/cms/fileadmin/internet/publikationen/ptb_mitteilungen/mitt2012/Heft2/PTB-Mitteilungen_2012_Heft_2.pdf, zuletzt geprüft am 03.11.2020.

5 Britannica: **Learn about Thomas Young's double-slit experiment which contradicted Newton's theory of light**. Online verfügbar unter https://www.britannica.com/video/179685/experiment-Thomas-Young, zuletzt geprüft am 21.10.2020.

6 Jönsson, C. (1961): **Elektroneninterferenzen an mehreren künstlich hergestellten Feinspalten.** Zeitschrift für Physik, 161(4):454–474.

7 Filk, T. (2019): **Zitate zur Quantentheorie.** Albert Einstein über die Quantenmechanik in einem Brief an Cornelius Lanczos, 21. März 1942, Einstein-Archiv 15-294, zitiert nach Einstein, Briefe, Seite 65, zitiert nach Alice Calaprice (Hrsg.): Einstein sagt, Piper-Verlag, München, Zürich 1996, S. 146. In: Filk, T. (Hrsg..), Quantenmechanik (nicht nur) für Lehramtsstudierende. Springer Spektrum, Berlin.

8 Konitzer, F. (2014): **Atomuhren**. Welt der Physik. Online verfügbar unter https://www.weltderphysik.de/gebiet/technik/atomuhren/atomuhren/, zuletzt geprüft am 21.10.2020.

9 Seabaugh, A. (2013): **The Tunneling Transistor**. IEEE Spectrum. Online verfügbar unter https://spectrum.ieee.org/semiconductors/devices/the-tunneling-transistor, zuletzt geprüft am 21.10.2020.

10 Brooks, M. (2019): **Beyond quantum supremacy: the hunt for useful quantum computers**. Nature, 574(7776):19–21.

11 Krieger, S. (2019): **Künstliche Intelligenz und Quantencomputing: Das Beste aus beiden Welten.** Online verfügbar unter https://www.f05.uni-stuttgart.de/fakultaet/aktuelles/news/Kuenstliche-Intelligenz-und-Quantencomputing-Das-Beste-aus-beiden-Welten-00003/, zuletzt geprüft am 21.10.2020.

12 Feynman, R., Mößbauer, R., Summerer, S. (1990): **Vom Wesen physikalischer Gesetze.** Piper, München.

13 Olson, E. (2019): **How quantum computers work**. Electronics 360. Online verfügbar unter https://electronics360.globalspec.com/article/13553/how-quantum-computers-work, zuletzt geprüft am 14.09.2020.

14 Hui, J. (2019): **QC - How to build a Quantum Computer with Superconducting Circuit?** Medium. Online verfügbar unter https://jonathan-hui.medium.com/qc-how-to-build-a-quantum-computer-with-superconducting-circuit-4c30b1b296cd, zuletzt geprüft am 21.10.2020.

15 Tavernelli, I. (2018): **Quantum Computing at IBM.** Quantum Computing for High Energy Physics. IBM Research – Zürich. Online verfügbar unter https://indico.cern.ch/event/719844/contributions/3019718/attachments/1749768/2835637/CERN_Tavernelli4_I.pdf, zuletzt geprüft am 05.11.2020.

16 Castelvecchi, D. (2017): **The strange topology that is reshaping physics**. Nature News, 547(7663):272.

17 Bechtold, A., Rauch, D., Li, F., Simmet, T., Ardelt, P.-L., Regler, A., Müller, K., Sinitsyn, N. A., Finley, J. J. (2015): **Three-stage decoherence dynamics of an electron spin qubit in an optically active quantum dot**. Nature Physics, 11(12):1005–1008.

18 Popkin, G. (2016): **Scientists are close to building a quantum computer that can beat a conventional one.** Online verfügbar unter https://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one, zuletzt geprüft am 02.11.2020.

19 Giles, M. (2019): **Explainer: What is quantum communication?** MIT Technology Review. Online verfügbar unterhttps://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/, zuletzt geprüft am 21.10.2020.

20 Bundesministerium für Bildung und Forschung (2018): **Q.Link.X. Quantenrepeater für eine abhörsichere Kommunikation über große Distanzen. Q.Link.X, Verbundprojekt Quanten-Link-Erweiterung.** Online verfügbar unter https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/q-link.x, zuletzt geprüft am 05.11.2020.

21 Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., Zhou, Y.-L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.-A., Liu, N.-L., Wang, X.-B., Zhu, Z.-C., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., Pan, J.-W. (2017): **Satellite-to-ground quantum key distribution.** Nature, 549(7670):43–47.

22 Popkin, G. (2017): **China's quantum satellite achieves 'spooky action' at record distance.** Science, American Association for the Advancement of Science (AAAS), Online verfügbar unter https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance, zuletzt geprüft am 27.11.2020.

23 Zivkovic, A. B., Hristov, N. P., Jerković, D. D., Bogdanović, B. S., Milutinović, J. M. (2019): **Automatic measurement of precision and accuracy from the hit pattern of small arms using electronic target system.** IOP Conference Series: Materials Science and Engineering, 659:12015.

24 Mavroeidis, V., Vishi, K., Zych, M., Jøsang, A. (2018): **The Impact of Quantum Computing on Present Cryptography.** International Journal of Advanced Computer Science and Applications, 9(3).

25 Bennett, C. H., Brassard, G. (1984): **Quantum Cryptography: Public Key Distribution and Coin Tossing.** Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing.

26 Shor, P. W. (1997): **Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.** SIAM Journal on Computing, 26(5):1484–1509.

27 Martín-López, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.-Q., O'Brien, J. L. (2012): **Experimental realization of Shor's quantum factoring algorithm using qubit recycling.** Nature Photonics, 6(11):773–776.

28 Bundesministerium für Bildung und Forschung (2019): **BMBF-Initiative QuNET baut hochsicheres Quantennetzwerk.** Online verfügbar unter https://www.bmbf.de/de/bmbf-initiative-qunet-baut-hochsicheres-quantennetzwerk-10126.html, zuletzt geprüft am 27.11.2020

29 Bureau International des Poids et Mesures (2019): **The International System of Units (SI).** 9. Auflage.

30 Johnson, A. (2014): **How the Ford Motor Co. Invented the SQUID.** IEEE Spectrum. Online verfügbar unter https://spectrum.ieee.org/tech-history/silicon-revolution/how-the-ford-motor-co-invented-the-squid, zuletzt geprüft am 06.11.2020.

31 Thiel, L., Rohner, D., Ganzhorn, M., Appel, P., Neu, E., Müller, B., Kleiner, R., Koelle, D., Maletinsky, P. (2016): **Quantitative nanoscale vortex imaging using a cryogenic quantum magnetometer.** Nature nanotechnology, 11(8):677–681.

32 The Royal Swedish Academy of Sciences: **The Nobel Prize in Chemistry 2014.** The Royal Swedish Academy of Sciences has decided to award the Nobel Prize in Chemistry for 2014 to Eric Betzig, Stefan W. Hell and William E. Moerner "for the development of super-resolved fluorescence microscopy". Online verfügbar unter https://www.nobelprize.org/uploads/2018/06/press-26.pdf, zuletzt geprüft am 27.11.2020

33 Fischer, L. (2014): **Bilder von der Grenze zwischen Biologie und Chemie.** Nobelpreise 2014. Spektrum.de. Online verfügbar unter https://www.spektrum.de/news/nobelpreis-fuer-chemie-2014-geht-an-deutschen-und-zwei-amerikanische-mikroskopieforscher/1311875, zuletzt geprüft am 19.10.2020.

34 Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF (2019): **Quantenrevolution in der Medizintechnik kündigt sich an.** Quantenimagingsystem vom Fraunhofer IOF liefert erste vielversprechende Bilder. Online verfügbar unter https://www.iof.fraunhofer.de/de/presse-medien/pressemitteilungen/2019/Quantenrevolution.html, zuletzt geprüft am 27.11.2020

35 Bundesministerium für Bildung und Forschung (2018): **Quantentechnologien von den Grundlagen zum Markt.** Rahmenprogramm der Bundesregierung. Online verfügbar unter https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf, zuletzt geprüft am 20.10.2020.

36 Deutscher Bundestag (2020): **Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/17500. Hochsicheres Quantennetzwerk QuNET.** Online verfügbar unter https://dip21.bundestag.de/dip21/btd/19/183/1918355.pdf, zuletzt geprüft am 20.10.2020.

37 Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF (2020): **Wie verschränkte Quanten unsere Kommunikation revolutionieren.** Online verfügbar unter https://www.fraunhofer.de/de/forschung/aktuelles-aus-der-forschung/quantentechnologie/quantenkommunikation.html, zuletzt geprüft am 04.11.2020.

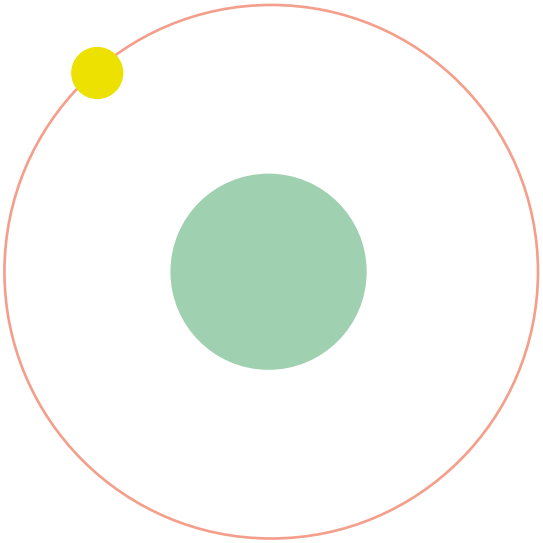
38 Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., Li, Y., Shen, Q., Cao, Y., Li, F.-Z., Wang, J.-F., Huang, Y.-M., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N.-L., Koidl, F., Wang, P., Chen, Y.-A., Wang, X.-B., Steindorfer, M., Kirchner, G., Lu, C.-Y., Shu, R., Ursin, R., Scheidl, T., Peng, C.-Z., Wang, J.-Y., Zeilinger, A., Pan, J.-W. (2018): **Satellite-Relayed Intercontinental Quantum Network.** Physical review letters, 120(3):30501.

39 Kagermann, H., Süssenguth, F., Körner, J., Liepold, A. (2020): **Innovationspotenziale der Quantentechnologien der zweiten Generation** (acatech IMPULS), München.

40 Bundesministerium der Finanzen (2020): **Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken.** Ergebnis Koalitionsausschuss 3. Juni 2020. Online verfügbar unter https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Konjunkturpaket/2020-06-03-eckpunktepapier.pdf, zuletzt geprüft am 20.10.2020.

Interviewpartnerinnen und Interviewpartner

Die Festlegung der Inhalte und die Arbeit am Text erfolgten durch die auf Seite 62 vorgestellte Projektgruppe. acatech hat für diese Publikation telefonisch oder persönlich insgesamt 28 Experteninterviews mit Vertreterinnen und Vertretern aus Wissenschaft, Wirtschaft, Politik und Gesellschaft geführt. Die Gespräche fanden zwischen Januar und April 2020 statt. Einige ausgewählte Kerngedanken der Befragten sind im Text als anonymisierte Zitate aufgeführt.



Das acatech Präsidium dankt allen Beteiligten sehr herzlich für ihre Teilnahme an den Interviews:

Prof. Dr. Monika Aidelsburger, Gruppenleiterin, Max-Planck-Institut für Quantenoptik/Ludwig-Maximilians-Universität München

Prof. Dr. Stefanie Barz, Institut für Funktionelle Materie und Quantentechnologien, Leitung Quantum Information & Technology, Universität Stuttgart

Prof. Dr. Immanuel Bloch, Direktor, Max-Planck-Institut für Quantenoptik/Leiter Abteilung Quanten-Vielteilchensysteme, Quantum Optics Group, Ludwig-Maximilians-Universität München

Dr. Astrid Elbe, Managing Director, Intel Labs Europe, Intel Deutschland GmbH

Christin Eisenschmid, Managing Director, Vice-President und General Manager, Intel Deutschland GmbH

Prof. Dr. Claudia Felser, Direktorin, Max-Planck-Institut für Chemische Physik fester Stoffe/acatech

Jens Fuhrberg, Government Affairs/Public Affairs, Intel Deutschland GmbH

Verena Fulde, Pressesprecherin/Corporate Blogger, Deutsche Telekom AG

Dr. Marc Geitz, Innovation Architect, Telekom Innovation Laboratories

Dr. Markus Gräfe, Head of Quantum-Enhanced Imaging Group, Fraunhofer-Institut für Angewandte Optik und Feinmechanik/Co-Founder, Quantum Optics Jena GmbH

Prof. Dr. Michael J. Hartmann, Lehrstuhl für Theoretische Physik, Friedrich-Alexander-Universität Erlangen-Nürnberg

Prof. Dr. Stefan Kück, EURAMET TC-PR Chair, Leiter der Abteilung Optik, Physikalisch-Technische Bundesanstalt

Dr. Manfred Lochter, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Prof. Dr. Hilbert von Löhneysen, Emeritus, Physikalisches Institut, Karlsruher Institut für Technologie/acatech

Dr. Sebastian Luber, Leitung Quantum iCommunity, Infineon

Prof. Dr. Dieter Meschede, Gruppenleiter Quantentechnologie, Institut für Angewandte Physik, Universität Bonn

Prof. Dr. Stuart Parkin, Director, Max Planck Institute of Microstructure Physics

Dr. Thomas Pöppelmann, Senior Staff Engineer, Infineon Technologies AG

Dr. Heike Riel, IBM Fellow, Department Head Science & Technology, IBM Research

Prof. Dr. Martin Schell, Institutsleiter, Fraunhofer Heinrich-Hertz-Institut

Prof. Dr. Oliver Schmidt, Institutsdirektor, Institute for Integrative Nanosciences, Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V./acatech

Dr. Torsten Siebert, Quantum Technologies Programme, Fraunhofer-Gesellschaft | Think Tank

Dr. Thomas Strohm, Koordinator und Senior Research Scientist für Quantentechnologien, Robert Bosch GmbH

Dr. Michael Totzeck, Fellow, Corporate Research and Technology, Carl Zeiss AG

Prof. Dr. Andreas Tünnermann, Institutsleiter, Fraunhofer-Institut für Angewandte Optik und Feinmechanik/acatech

Prof. Dr. Dr. h. c. Joachim Ullrich, Präsident, Physikalisch-Technische Bundesanstalt/acatech

Dr. Walter Weigel, Vice-President & CSO, European Research Institute, Huawei Technologies

Prof. Dr. Artur Zrenner, Department Physik, Universität Paderborn/acatech

Mitwirkende

Gesamtleitung acatech HORIZONTE:
Prof. Dr.-Ing. Jürgen Gausemeier, Vizepräsident acatech, Seniorprofessor Heinz Nixdorf Institut der Universität Paderborn

Leitung Innovationsforum:
Prof. Dr. Martina Schraudner, Vorstandsmitglied acatech, Leiterin Fraunhofer Center for Responsible Research and Innovation

Projektgruppe Quantentechnologien:
Prof. Dr. Stefanie Barz, Institut für Funktionelle Materie und Quantentechnologien, Leitung Quantum Information & Technology, Universität Stuttgart

Dr. Astrid Elbe, Managing Director, Intel Labs Europe, Intel Deutschland GmbH

Dr. Markus Gräfe, Head of Quantum-Enhanced Imaging Group, Fraunhofer-Institut für Angewandte Optik und Feinmechanik/Co-Founder, Quantum Optics Jena GmbH

Prof. Dr. Stefan Kück, EURAMET TC-PR Chair, Leiter der Abteilung Optik, Physikalisch-Technische Bundesanstalt

Dr. Thomas Pöppelmann, Senior Staff Engineer, Infineon Technologies AG

Dr. Heike Riel, IBM Fellow, Department Head Science & Technology, IBM Research

Dr. Thomas Strohm, Koordinator und Senior Research Scientist für Quantentechnologien, Robert Bosch GmbH

Dr. Michael Totzeck, Fellow, Corporate Research and Technology, Carl Zeiss AG

Prof. Dr. Andreas Tünnermann, Institutsleiter, Fraunhofer-Institut für Angewandte Optik und Feinmechanik/acatech

Prof. Dr. Dr. h. c. Joachim Ullrich, Präsident, Physikalisch-Technische Bundesanstalt/acatech

Prof. Dr. Artur Zrenner, Department Physik, Universität Paderborn/acatech (Leiter Projektgruppe)

Konzeption, Text und Experteninterviews:
Dr. Alexandra Heimisch-Röcker, acatech Geschäftsstelle, HORIZONTE (Autorin)

Christina Müller-Markus, acatech Geschäftsstelle, HORIZONTE (Autorin)

Vivian Würf, acatech Geschäftsstelle, HORIZONTE

Sebastian Grünwald, acatech Geschäftsstelle, HORIZONTE

Mit Unterstützung durch:
Iris Michalik, acatech Geschäftsstelle, HORIZONTE

Annette Wiedemann, acatech Geschäftsstelle, Kommunikation HORIZONTE

acatech -

Deutsche Akademie der Technikwissenschaften

acatech berät Politik und Gesellschaft, unterstützt die innovationspolitische Willensbildung und vertritt die Technikwissenschaften international. Ihren von Bund und Ländern erteilten Beratungsauftrag erfüllt die Akademie unabhängig, wissenschaftsbasiert und gemeinwohlorientiert. acatech verdeutlicht Chancen und Risiken technologischer Entwicklungen und setzt sich dafür ein, dass aus Ideen Innovationen und aus Innovationen Wohlstand, Wohlfahrt und Lebensqualität erwachsen. acatech bringt Wissenschaft und Wirtschaft zusammen. Die Mitglieder der Akademie sind herausragende Wissenschaftlerinnen und Wissenschaftler aus den Ingenieur- und den Naturwissenschaften, der Medizin sowie aus den Geistes- und Sozialwissenschaften. Die Senatorinnen und Senatoren sind Persönlichkeiten aus technologieorientierten Unternehmen und Vereinigungen sowie den großen Wissenschaftsorganisationen. Neben dem acatech FORUM in München als Hauptsitz unterhält acatech Büros in Berlin und Brüssel.

Weitere Informationen unter www.acatech.de.

HERAUSGEBER:
acatech – Deutsche Akademie der Technikwissenschaften

ADRESSEN STANDORTE
Geschäftsstelle
Karolinenplatz 4
80333 München
T +49(0)89 / 520309-0
F +49(0)89 / 520309-900

Hauptstadtbüro
Pariser Platz 4a
10117 Berlin
T +49(0)30 / 2063096-0
F +49(0)30 / 2063096-11

Brüssel-Büro
Rue d'Egmont / Egmontstraat 13
B-1000 Brüssel
T +32(0)2 / 2 13 81-80
F +32(0)2 / 2 1381-89
horizonte@acatech.de
https://www.acatech.de/horizonte

Empfohlene Zitierweise:
acatech (Hrsg.): Quantentechnologien (acatech HORIZONTE), München 2020

Redaktionelle Bearbeitung:
Karola Klatt

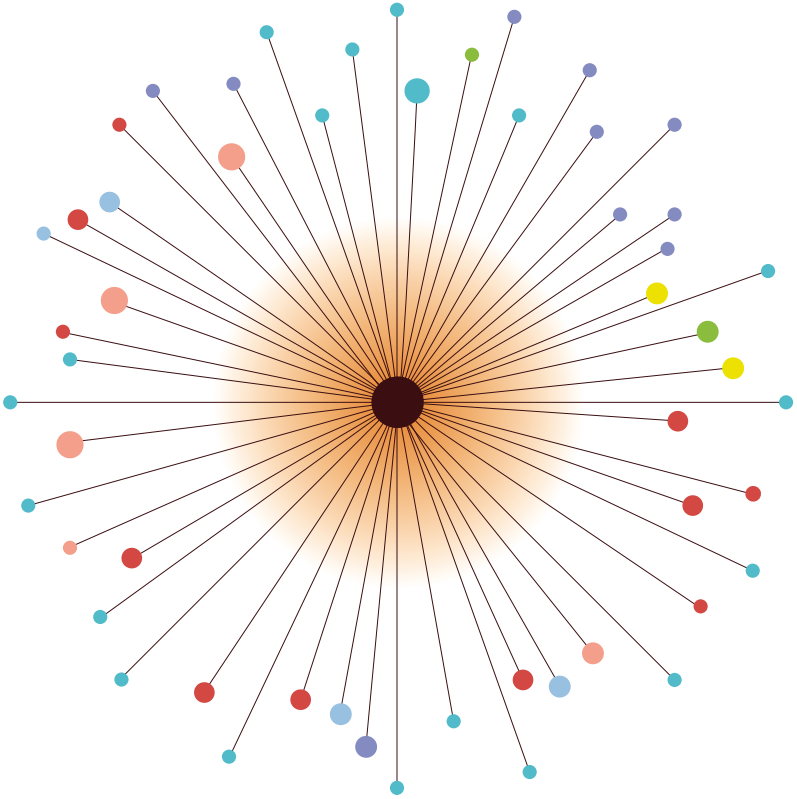
Lektorat:
Lektorat Berlin

Layout, Satz und Illustrationen:
Joseph & Sebastian – Grafikdesign, München

Druck:
Kern GmbH, Bexbach

Mehr zu acatech HORIZONTE Quantentechnologien, inklusive der Grafiken, finden Sie auch unter:
https://www.acatech.de/projekt/acatech-horizonte-quantentechnologien

München 2020
acatech HORIZONTE ISSN 2625-9605



Über die zweite Generation der Quantentechnologien, zu denen auch der Quantencomputer gehört, kursieren viele Mythen. Auch deshalb, weil die Grundlagen dieser Technologie – die Quanten und deren Manipulation – ferner von unserer Alltagswelt kaum liegen könnten.

Was sind Quanten überhaupt? Was ist momentan technisch möglich? Was ist Hype, und wo liegen die Potenziale der Technologien? Auf diese und weitere Fragen möchte die vorliegende HORIZONTE-Ausgabe Antworten geben.