Check for updates

DOI: 10.1002/piuz.202401725

Weltweite Vernetzung der Quantentechnologien

Quantenkommunikation via Satellit

Kai Bongs | Christian Fuchs | Kaisa Laiho | Florian Moll | Sabine Wölk | Matthias Zimmermann

Quantentechnologien sind auf dem Weg, die Welt zu verändern. Die weltweite Vernetzung kann ihr Potenzial vervielfachen und neue Anwendungsmöglichkeiten eröffnen.

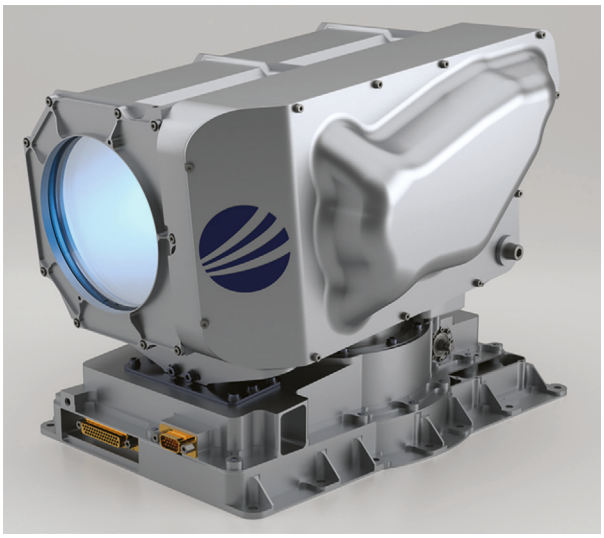


Abb. 1 ***Tesat Spacecom Laser Communication Terminal*** *(Foto: Tesat).*

Wenn Sie diesen Text online lesen, dann nutzen Sie mit den Halbleitern in ihrem Computer und den Lasern in der optischen Faserverbindung Technologien, die zu den Quantentechnologien der ersten Generation gehören. Diese basieren auf dem quantenmechanischen Verständnis der Energieniveaus in Festkörpern und treiben die digitale Revolution seit Jahrzehnten an.

Jetzt stehen wir an der Schwelle zu einer „Quantenrevolution 2.0“, die mit Quanteneffekten wie der quantenmechanischen Überlagerung und der Verschränkung von weit entfernten Objekten ganz neue Möglichkeiten bei der Datenerfassung, der Datenkommunikation und der Datenverarbeitung eröffnet. Die quantenmechanische Überlagerung basiert auf dem Phänomen, dass einzelne Quantenteilchen in mehreren Zuständen gleichzeitig exisitieren können. Dieses Konzept wird durch die Verschränkung auf mehrere Teilchen erweitert, so dass deren Überlagerungszustände nicht mehr getrennt voneinander betrachtet werden können, sondern Korrelationen aufweisen.

In einer stark vereinfachten Betrachtungsweise können Quantencomputer durch den Einsatz von Bits in verschränkten Überlagerungszuständen, sogenannten Qubits, gleichzeitig verschiedene Rechenpfade erforschen und damit bestimmte Probleme – wie Datenbanksuchen, die Entschlüsselung bestimmter Kryptographieverfahren oder quantenmechanische Molekülrechnungen – sehr stark beschleunigen. Eine wesentliche technische Herausforderung bei der Realisierung eines Quantencomputers liegt darin, dass die Überlagerungszustände der Qubits extrem empfindlich gegenüber Umgebungseinflüssen sind und sehr gut abgeschirmt werden müssen, um die Rechnung nicht zu stören. Die Quantensensorik und die Quantenkommunikation machen sich diese Empfindlichkeit dagegen zunutze, um hochpräzise Messungen zu realisieren und um Lauschangriffe zu detektieren. Daher sind bereits jetzt erste kommerzielle Quantensensoren und Quantenkommunikationsysteme erhältlich. In Quantennetzwerken (siehe Physik in unserer Zeit **2023**, *54*(1), 18 und „Internet“ auf S. 8) sollen diese unterschiedlichen Quantentechnologien in Zukunft gemeinsam genutzt werden und per Satellit sogar über weit entfernte Distanzen miteinander kommunizieren.

In einem ersten Schritt werden derzeit zahlreiche urbane optische Quantennetzwerke entwickelt, um diese neue Technologie zu erforschen. Inzwischen gab es bereits einige eindrucksvolle Demonstrationen der Quantenschlüsselverteilung (siehe „Quantenverschlüsselung“ auf S. 3) in solchen auf Glasfasern basierenden Netzwerken, die beispielsweise in Cambridge, Delft, Wien oder Peking-Shanghai aufgebaut werden [1]. Allerdings ist die derzeitig mögliche Kommunikationsdistanz über Glasfasern ohne vertrauenswürdige Zwischenstationen auf wenige 100 km beschränkt. Da die Quantenkommunikation einzelne Photonen als Qubits nutzt, die ungestört, das heißt auch ohne Verstärkung, den Empfänger erreichen müssen, hängt die mögliche Kommunikationsdistanz kritisch von den Verlusten der Kommunikationsstrecke ab. Um mit Glasfasern längere Kommmunikationsdistanzen zu ermöglichen, sind entweder vertrauenswürdige Zwischenstationen oder sogenannte Quantenrepeater [2] notwendig, wobei letztere noch im Experimentierstadium sind. Für eine interkontinentale Verbindung

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Online-Ausgabe unter: wileyonlinelibrary.com

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

durch Ozeane scheinen beide Lösungen aber technologisch zu aufwendig, um eine wirtschaftliche Lösung darzustellen. Hier bieten Freistrahlsysteme über Satelliten eine globale Alternative [3].

Quantenschlüsselverteilung via Satellit

Die satellitenbasierte Quantenschlüsselverteilung funktioniert grundsätzlich wie die auf Glasfasern basierende Version. Der Satellit agiert hier meist als vertrauenswürdige Zwischenstation, er kann zu verschiedenen Punkten auf der Erde Verbindungen aufbauen und dabei Quantenschlüssel erzeugen. Das macht ihn zu einer Art Schlüsseldienstanbieter. Der technische Unterschied zum Fasersystem ist bedingt durch den freistrahloptischen Kommunikationkanal. Um eine optische Kommunikationsverbindung zwischen dem Satelliten und der Gegenstelle am Boden aufbauen zu können, muss der Satellit seinen Sendestrahl äußerst präzise ausrichten können. Außerdem müssen verschiedene störende Effekte dieses Kommunikationskanals berücksichtigt werden, etwa Signalverzerrungen durch die atmosphärische Wellenausbreitung oder Hintergrundlicht. Dass dies machbar ist

QUANTENSCHLÜSSELVERTEILUNG

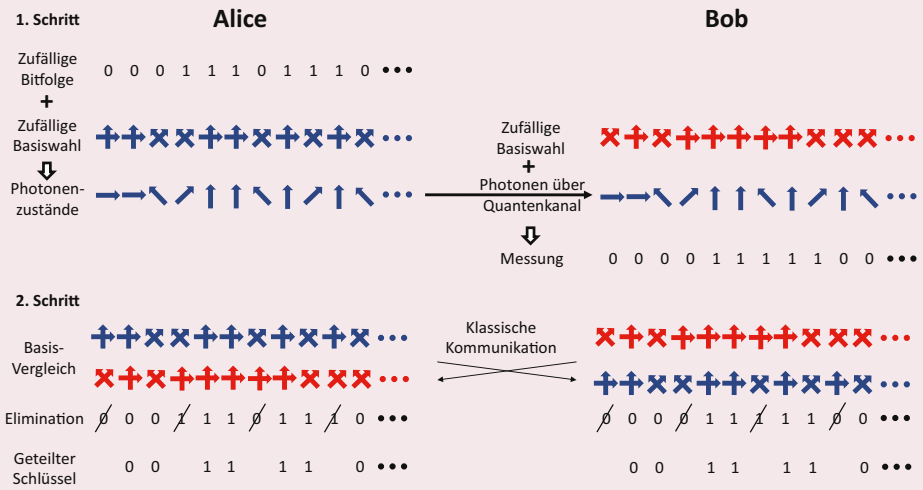
Die Quantenschlüsselverteilung, oder Quantum Key Distribution (QKD), ist bereits kommerziell verfügbar. Ihre Sicherheit ist im Prinzip durch physikalische Gesetze gewährleistet. Dabei macht man sich zu Nutze, dass quantenmechanische Zustände nicht kopiert werden können (No-Cloning-Theorem) und dass eine Messung an einem einzelnen Quantenobjekt im Allgemeinen keine vollständige Information über dessen Quantenzustand liefert. Ein Beispiel für letzteres ist die Messung der Polarisationszustände von Photonen.

Im Prinzip kann man jeden Polarisationszustand eines Photons durch eine Überlagerung von zwei Basis-Polarisationszuständen ausdrücken. Diese können zum Beispiel vertikale und horizontale Schwingungen des Lichtfelds sein. Ein Messinstrument wäre dann ein Polarisationsstrahlteiler mit Fotodetektoren an beiden Ausgängen. Richtet man den Filter so aus, dass er vertikale Lichtschwingungen durchlässt und horizontale reflektiert, so erzeugt jedes vertikal polarisierte Photon einen „Klick“ des Detektors geradlinig hinter dem Strahlteiler, während Photonen in einem horizontalen Polarisationszustand einen „Klick“ auf dem seitlichen Detektor verursachen.

Wenn bekannt ist, dass die ankommenden Photonen entweder in einem horizontalen oder vertikalen Polarisationszustand sind, dann kann man auf diese Art den Polarisationszustand bestimmen. Ist der Polarisationszustand des einfallenden Photons allerdings um 45° gedreht, dann würde jeder der Detektoren mit fünfzigprozentiger Wahrscheinlichkeit zufällig reagieren, folglich wäre eine Zustandsbestimmung mit einer einzigen Messung nicht möglich. Wegen des No-Cloning-Theorems kann man dies auch nicht dadurch beheben, dass man Kopien des Polarisationszustands herstellt, um die statistische Verteilung mehrerer Messungen zu analysieren.

Verschiedene Protokolle

Mit solchen Polarisationszuständen von Photonen kann ein Protokoll zur Quantenverschlüsselung umgesetzt werden, das Charles Bennet und Gilles Brassard bereits 1984 vorgeschlagen haben. Dieses BB84-Protokoll ist ein sogenanntes Prepare-and-Measure-Protokoll, bei dem der Sender definierte Zustände herstellt und versendet (Abbildung). Das in der Abbildung dargestellte typische Szenario illustriert dies mit einer Absenderin Alice, die einen Schlüssel mit einem Empfänger Bob teilen möchte. Wenn beide einen Teil des Schlüssels „opfern“ und Messeinstellungen vergleichen, können sie herausfinden, ob eine Spionin Eve sich eingeschaltet und mitgelauscht hat.



Schlüsselaustausch im BB84-Protokoll. Im ersten Schritt kodiert Alice eine zufällige Bitfolge mit einer zufälligen Basisauswahl in Photonenzuständen, die über einen Quantenkanal an Bob übertragen werden. Dieser detektiert sie mit einer eigenen lokalen, zufälligen Abfolge von Detektorausrichtungen und übersetzt sie in eine Bitfolge. Im zweiten Schritt kommunizieren Alice und Bob über einen klassischen Kanal und tauschen die jeweils gewählten Basiszustände, also Detektorausrichtungen, aus. Für die übereinstimmenden Fälle behalten beide die Bits und erhalten so einen gemeinsamen geheimen Schlüssel.

Ist dieser Schlüsselanteil bei beiden gleich, dann können sie davon ausgehen, dass die entsprechenden Photonen ungestört übertragen und nicht abgehört wurden. Wenn nämlich Eve ein Photon mit der von ihr gewählten Polarisationsausrichtung detektiert, kann sie bestenfalls ein neues Photon mit dem von ihr gemessenen Polarisationszustand zu Bob weitersenden. Falls sie allerdings die Detektorausrichtung anders als Alice gewählt hat, so wird Bob bei Wahl derselben Ausrichtung wie Alice mit gewisser Wahrscheinlichkeit einen anderen Zustand messen, als Alice gesendet hat. Dies wird dann als Fehler beim Schlüsselvergleich registriert.

Es gibt noch zahlreiche weitere Protokolle zur Quantenschlüsselverteilung. Das von Artur Ekert 1991 erdachte E91-Protokoll ist der Prototyp der wichtigen Klasse der verschränkungsbasierten Schlüsselverteilung (siehe „verschränkungsbasierte Quanteninformationsübertragung“ auf S. 5). Dabei erzeugt eine Quelle verschränkte Photonenpaare, die in der Polarisation korreliert sind. Davon können Alice und Bob je ein Photon mit einem polarisationsempfindlichen Detektor detektieren und so nach Kommunikation ihrer Detektorausrichtungen untereinander ihren Schlüssel generieren. Auch in diesem Fall ist es für Alice und Bob möglich, eine Spionin Eve zu enttarnen.

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

15213943, 2025, 3, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/piuz.202401725 by Disch Zentrum F. Luft-U. Raum Fahrt In D. Helmholtz Gemein., Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

und die technischen Herausforderungen gemeistert werden können, ließ sich schon vielfach im Bereich der freistrahloptischen Telekommunikation via Satellit unter Beweis stellen. Verschiedene Firmen bieten diese Systeme mittlerweile als Produkte an, die in vergangenen und aktuellen Satellitenmissionen schon operationell oder testweise eingesetzt werden. Ein Beispiel ist das Satellitenterminal in Abbildung 1, das aktuell für die schnelle Datenübertragung in größeren Satellitennetzen genutzt werden soll.

Die Machbarkeit eines satellitenbasierten Quantenschlüsselaustauschs hat erstmals der chinesische Satelliten Micius aufgezeigt. Dieser Satellit wurde für verschiedene Experimente genutzt, etwa für die Quantenschlüsselverteilung mittels vertrauenswürdiger Zwischenstation [4] und für die Verschränkungsverteilung aus dem All [5]. In Europa sind derzeit verschiedene Missionen in der Vorbereitung und Umsetzung, so etwa die deutschen Satelliten QUBE und QUBE-II [6] (Abbildung 2) sowie der europäische Satellit EAGLE-1. Letzterer nutzt auch das in Abbildung 1 gezeigte Satellitenterminal als Sendesystem für das Quantensignal. Der Erfahrungsgewinn aus diesen Satellitenmissionen ist ein wichtiger Schritt bei der Entwicklung zukünftiger operationeller Satellitensysteme zur Quantenschlüsselverteilung.

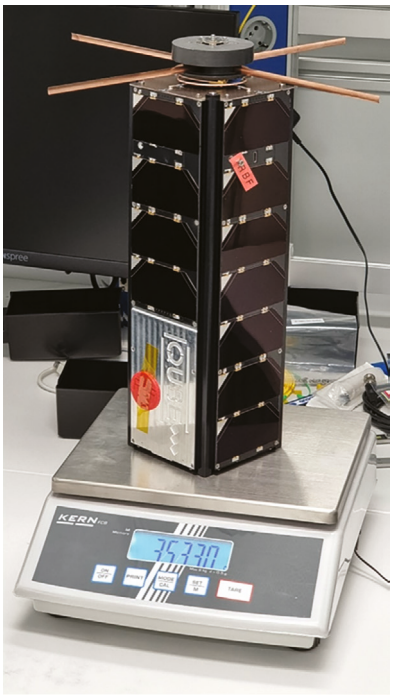


Abb. 2 ***QUBE-Satellit zur sicheren Quantenschlüsselverteilung*** *(Foto: Zentrum für Telematik, Würzburg).*

Um als Nutzer am Boden einen Schlüssel zu erhalten, ist eine passende Empfangsstation, eine optische Bodenstation, notwendig. Diese besteht im Wesentlichen aus einem optischen Teleskop und einem Quantenempfänger. Das vom Satelliten abgestrahlte Quantensignal wird vom Teleskop eingefangen und zur Detektion an den Quantenempfänger weiterleitet. Diese Empfangsstation kann auf dem Dach des Nutzers stehen oder als eine gesonderte Antenne betrieben werden. Im ersten Fall würde das Quantensignal vom Teleskop in eine Glasfaser gekoppelt und an den Quantenempfänger im Gebäude weitergeleitet werden. Im zweiten Fall würde das Teleskop an einem vom Nutzer entfernten Standort stehen. Das Teleskop würde ebenso das Quantensignal empfangen und in eine Glasfaser koppeln. Anschließend ginge es aber über ein terrestrisches Fasernetzwerk weiter bis zum Nutzer, in dessen Gebäude wieder der Quantenempfänger steht. So ist jeweils sichergestellt, dass der Schlüssel in einer sicheren Umgebung erzeugt wird und nicht einfach kompromittiert werden kann. Als alternative Methode lässt sich auch das Quantensignal freistrahloptisch direkt hinter dem Teleskop vermessen, ohne Nutzung einer Glasfaser. Bei dieser Variante muss jedoch sichergestellt werden, dass das Teleskop gut vor dem Zugriff Dritter geschützt ist. Eine entsprechende experimentelle Empfangsstation, mit der diese verschiedenen Arten der Nutzeranbindung getestet werden, steht auf dem Dach des DLR-Instituts für Kommunikation und Navigation in Oberpfaffenhofen und ist in Abbildung 3 gezeigt. Sie wurde von unserer Arbeitsgruppe aufgebaut und wird in Demonstrationsexperimenten betrieben.

Die Bemühungen hinsichtlich eines zukünftigen operationellen Satellitensystems zur Quantenschlüsselverteilung sind weltweit in vollem Gange. Die nahe Zukunft wird Systeme bringen, die nach dem Prepare-and-Measure-Prinzip arbeiten, das heißt noch ohne die Nutzung von verschränkten Zuständen. Bei dieser Variante der Quantenschlüsselverteilung kennt der Satellit den erzeugten Schlüssel und muss somit eine vertrauenswürdige Zwischenstationen sein. Die Forschungs- und Entwicklungsbemühungen zur Nutzung von verschränkten Zuständen sind aber bereits seit einiger Zeit im Gange. Hier kennt der Satellit den erzeugten Schlüssel am Ende nicht, was ein Vorteil hinsichtlich der Systemsicherheit ist. Die beiden unterschiedlichen Systemarten sind in Abbildung 4 dargestellt. Desweiteren stellt die Verschränkungsverteilung die Basisressource für ein zukünftiges globales Quantennetzwerk dar.

Die Verschränkungsverteilung via Satellit ist auch für die Grundlagenphysik interessant. Es stellt sich nämlich die Frage, ob die durch das Erdschwerefeld bewirkte relativistische Zeitverschiebung eine Dekohärenz bewirkt, wenn zum Beispiel ein Photon eines verschränkten Paars zum Satellit hinauf fliegt und das andere an der Erdoberfläche verbleibt. Mit Micius wurde ein solches Experiment 2019 durchgeführt, das keinen solchen Dekohärenzeffekt finden konnte [7].

Verschränkung als Werkzeug

Um auf vertrauenswürdige Zwischenstationen bei der Quantenschlüsselverteilung verzichten zu können, sind einige Herausforderungen zu meistern. Hierbei ist die Implementierung aufwendigerer, verschränkungsbasierter Kommunikationsprotokolle (siehe „Quantenverschlüsselung“ sowie „Verschränkungsbasierte Quanteninformationsübertragung“ auf S. 5) essenziell. Wie für Prepare-and-Measure-Protokolle treten auch hier bei

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

15213943, 2025, 3, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/piuz.202401725 by Dtsch Zentrum F. Luft-U. Raum Fahrt In D. Helmholtz Gemein., Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

der Kommunikation über Glasfaser oder Freistrahl Photonenverluste auf. Allerdings könnte die Verschränkung mit Hilfe von Quantenspeichern, die als Quantenrepeater in den Zwischenstationen fungieren [2], auf beliebige Distanzen ausgedehnt werden. Für interkontinentale Kommunikation wären solche Quantenspeicher auf Satelliten eine Lösung, um Zwischenstationen im Ozean zu vermeiden. So lässt sich prinzipiell eine sichere globale Kommunikation erzielen.

Noch sind auf Verschränkung basierende Quantennetzwerke aber ein aktueller Forschungsgegenstand, da es einen riesigen Parameterraum an unterschiedlichen Photonenquellen und Quantenspeichern gibt, die aufeinander abgestimmt und für eine Systemlösung ausgewählt werden müssen. Bei satellitenbasierten Quantennetzwerken ist zudem die Robustheit und Praktikabilität der Komponenten zu bedenken.

Verschränkung kann man inzwischen in vielen Quantensystemen – Photonen, Ionen, Neutralatomen oder Störstellen in Festkörpern – generieren. Für Kommunikationszwecke bieten sich komplett photonische Systeme an. Mit integrierter Optik hat man eine hervorragende Plattform, um praktische und robuste photonische Quantenquellen herzustellen. Dabei hat sich gezeigt, dass die Telekom-Wellenlängen, die zwischen etwa 1,3 und 1,5 µm liegen, bestimmte Vorteile haben, die sich in geringen Verlusten bei Faserlinks und bei Freistrahlanwendungen in einer größeren Reichweite unter dunstigen Atmosphärenverhältnissen erkennbar machen [8]. Die Verfügbarkeit robuster kommerzieller integrierter Bauteile, um die gewünschten Lichtfreiheitsgrade wie Polarisation und Phase zu modifizieren,

Abb. 3 ***Experimentelle optische Empfangsstation des DLR in Oberpfaffenhofen*** *(Foto: DLR).*

ist ein weiterer Vorteil bei diesen Wellenlängen. Allerdings wird hier für die Einzelphotonendetektion häufig auf kryogene Detektoren zurückgegriffen, was praktische Nachteile mit sich bringt.

Bei der Auswahl der photonischen Quellen für die Verschränkungserzeugung in Quantennetzwerken ist die Kompatibilität mit existierenden Quantenspeichern ausschlaggebend, um ein funktionierendes Netzwerk zu realisieren. Momentan sind Quantenspeicher typischerweise sehr schmalbandig, im MHz-Bereich, und

VERSCHRÄNKUNGSBASIERTE QUANTENINFORMATIONSÜBERTRAGUNG

Die Quantenteleportation und das Superdense Coding sind zwei Verfahren, um verschränkungsbasiert Information übertragen zu können [22]. Bei der Quantenteleportation liegt der Fokus auf dem Austausch von Quanteninformation, das heißt der Übertragung eines unbekannten Quantenzustands. Das Superdense Coding hingegen ermöglicht die verschränkungsbasierte Übertragung einer klassischen Information.

Quantenteleportation

Bei der Quantenteleportation befinden sich zwei Teilchen A und B an unterschiedlichen Knoten eines Quantennetzwerks und werden initial in einem gemeinsamen Bell-Zustand präpariert. Anschließend ist es möglich, den Quantenzustand eines dritten Teilchens C, das sich am gleichen Netzwerknoten wie Teilchen A befindet, durch Kopplung an das Teilchen A auf den Zustand des Teilchens B zu übertragen. Hierzu wird eine projektive Messung der Teilchen A und C durchgeführt, und die klassischen Messergebnisse werden als zwei Bits über einen klassischen Kanal übermittelt. Anschließend werden von diesen Messergebnissen abhängige Operationen am Teilchen B durchgeführt, um dieses in den ursprünglichen Quantenzustand von Teilchen C zu überführen.

Ein Spion, der diesen klassischen Kanal abhört, könnte allein mit der Kenntnis der klassischen Messerergebnisse den Quantenzustand von C nicht rekonstruieren. Die initial bestehende Verschränkung von A und B ist dabei essenziell für die Quantenteleportation des Quantenzustands von C.

Superdense Coding

Auch beim Superdense Coding ist initial ein Paar maximal verschränkter Qubits A und B an zwei Netzwerkknoten vorhanden. An Teilchen A werden nun lokale Quantengatter-Operationen ausgeführt und damit einer der vier möglichen Bell-Zustände für das verschränkte Qubit-Paar präpariert. Die Wahl der vier lokalen Quantengatter ist abhängig von den vier möglichen klassischen Zwei-Bit-Zuständen 00, 01, 10, 11, die vom ersten an den zweiten Netzwerkknoten übertragen werden sollen.

Nach der Ausführung des Quantengatters wird das Qubit A dann an den zweiten Netzwerkknoten versendet. Dort ist es nun möglich, mit Hilfe einer Messung an den beiden Teilchen A und B die klassische Zwei-Bit-Information auszulesen, obwohl nach der Codierung der klassischen Information nur ein einzelnes Qubit A an den zweiten Netzwerkknoten übertragen wurde. Durch das Abfangen der Übertragung des gesendeten Qubits A ist es zudem nicht möglich, die Information der zwei klassischen Bits vollständig zu rekonstruieren, da hierfür auch das anfänglich verteilte verschränkte Qubit B notwendig ist.

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

15213943, 2025, 3, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/piuz.202401725 by Dtsch Zentrum F. Luft-U. Raum Fahrt In D. Helmholtz Gemein., Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Abb. 4 *Szenariodarstellung von Satelliten-basierter Quantenschlüsselverteilung nach dem Prepare-and-Measure-Prinzip (linke Bildhälfte) und auf Basis von Verschränkungsverteilung (rechte Bildhälfte).*

besonders wellenlängenselektiv. Zur Erzeugung schmalbandiger Photonen können Kaskaden aus Quantenpunkten eingesetzt werden [9]. Quantenpunkte sind nulldimensionale Festkörper, die aus Halbleitermischungen hergestellt werden. Allerdings werden für schmalbandige Anwendungen häufig kryogene Temperaturen benötigt, um Störungen durch Phononen im Festkörper zu verringern. Als Alternative können schmalbandige Photonenpaare aus nichtlinearen optischen Prozessen hergestellt werden, Beispiele finden sich in [10] und [11].

Eine wesentliche Anforderung an Quantenspeicher für die globale Quantenkommunikation via Satellit ist eine Speicherzeit im Bereich von zirka 100 ms, sodass Variationen von Photonenlaufzeiten über einige 1000 km ausgeglichen werden können.

Die Realisierung von Quantenrepeatern, die auf Quantenspeichern auf Satelliten basieren, ermöglicht nicht nur globale Quantenschlüsselverteilung, sondern verspricht zusätzliche Funktionalität. In Zukunft könnten solche Repeaterstationen auch weitere Verschränkungsdienstleistungen anbieten. Dazu zählt die Erhöhung der Verschränkung durch sogenannte Destillation, das ist die Erzeugung einer kleineren Anzahl hochverschränkter Photonenpaare aus einer größeren Anzahl an Photonenpaaren, deren Verschränkung durch Verluste oder Rauschen reduziert wurde. Außerdem ist auch die Umwandlung eines Verschränkungsfreiheitsgrads des Lichts in einen anderen möglich. Ein Beispiel hierfür ist die Umwandlung einer Verschränkung in der Polarisation in eine Verschränkung im Bahndrehimpuls der Photonen (Orbital Angular Momentum, OAM) mit einer spiralförmigen Phasenstruktur („Twisted Light“) als bekanntestem Spezialfall [12]: Die Verschränkung in solchen OAM-Modenzahlen ist attraktiv, da diese quantisierten Zahlen im Prinzip beliebig hoch sein können. Eine weitere Möglichkeit ist die Benutzung von Hyperverschränkung, also eine Verschränkung in mehreren Freiheitsgraden, was eine höhere Robustheit und vielfältigere praktische Umsetzbarkeit ermöglicht.

Quantennetzwerke

Während bei der Quantenschlüsselverteilung der quantenbasierte Austausch von Schlüsseln für die sichere Kommunikation im Vordergrund steht, bieten Quantennetzwerke perspektivisch viele weitere Einsatzmöglichkeiten und erlauben insbesondere die Verknüpfung unterschiedlicher Quantentechnologien. Hierzu wird ein Quantennetzwerk generell als ein Netzwerk von Quantensystemen betrachtet, welche Quanteninformation generieren, senden, speichern, empfangen und verarbeiten können. Ein Quantennetzwerk, wie in Abbildung 4 gezeigt, besteht aus drei essenziellen Hardware-Komponenten [13]:

1. Quantenkanäle, welche die Übertragung von Quantenzuständen wie Qubits beispielsweise über Glasfaser oder Satellit ermöglichen. Häufig kommen zudem auch klassische Kommunikationskanäle zum Einsatz.
2. Quantenrepeater, die Quantenspeicher enthalten und benötigt werden, um eine verlustfreie Übertragung von Quantenzuständen zu garantieren. Mit diesen Geräten können optische Verluste in den Quantenkanälen ausgeglichen und die Quantenkommunikation über große Distanzen etabliert werden.
3. Endknoten, die bestimmte Quantentechnologien an das Quantennetzwerk anbinden. Hierbei kann es sich beispielsweise um Quantensensoren, Quantenspeicher oder sogar Quantencomputer handeln. Da diese Geräte auf ganz unterschiedlicher Hardware – Photonen, Supraleiter, Ionen, Atome, Stickstofffehlstellen-Zentren etc. – basieren, ist es essenziell, entsprechende Hardware-Schnittstellen für Quantennetzwerke zu entwickeln. Beispielsweise ist es erst kürzlich gelungen, sowohl nanophotonische [14] als auch atomare [15] Quantenspeicher über ein Telekommunikationsnetzwerk zu verschränken.

Wie bei einem klassischen Netzwerk ist darüber hinaus auch bei einem Quantennetzwerk die Netzwerktopologie von großer Relevanz. Bei einem Netzwerk mit vielen Parteien lassen sich keine direkten Kommunikationskanäle zwischen allen beteiligten Knoten etablieren. Daher muss man je nach Anwendungszweck beispielsweise eine Ring-, Stern- oder Bus-Topologie der Quanten- und klassischen Kanäle in Erwägung ziehen.

Zusätzlich ist für Quantennetzwerke die Entwicklung eines Netzwerk-Schichtenmodells nötig, analog dem TCP/IP-Referenzmodell oder dem OSI-Schichtenmodell für das klassische Internet. Hier übernehmen unterschiedliche Netzwerkschichten bestimmte Protokolle und Aufgaben im Netzwerk, wie die Gewährleistung

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

15213943, 2025, 3, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/piuz.202401725 by Dtsch Zentrum F. Luft-U. Raum Fahrt In D. Helmholtz Gemein., Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

einer fehlerfreien Übertragung oder die Vermittlung und Fragmentierung von Datenpaketen. Aufgrund der unterschiedlichen Optionen für die Übertragung von Quanteninformation, die im Folgenden näher erläutert werden, müssen hier einige grundlegend neue Konzepte entwickelt werden.

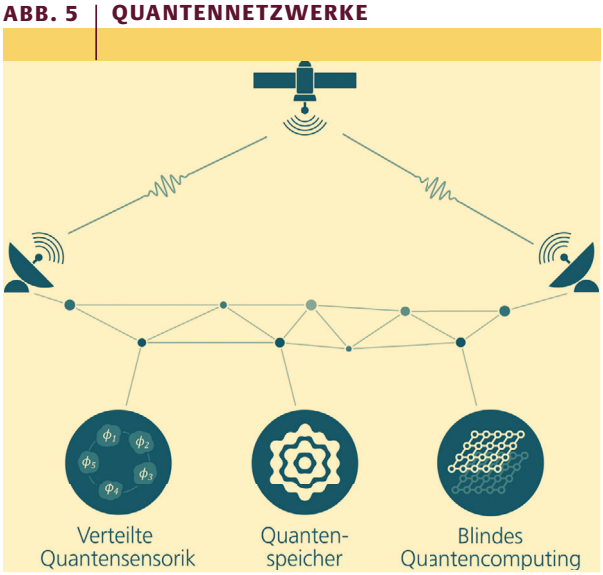
In einem klassischen Netzwerk wird die Information mittels Nullen und Einsen zwischen den Netzwerkknoten übertragen. Bei einem Quantennetzwerk stehen hingegen verschiedene Optionen für die Übermittlung von Quanteninformation zwischen den Netzwerkknoten zur Verfügung. Einerseits können, analog zur klassischen Informationsübertragung, die Quantenzustände von Qubits als Informationsträger im Rahmen der direkten Zustandsübertragung über Quantenkanäle versendet werden. Andererseits erlauben verschränkungsbasierte Protokolle die teilweise Trennung von Kommunikation und Informationsübertragung, wie beispielsweise in der Quantenteleportation, bei der zunächst ein verschränktes Photonenpaar an Sender und Empfänger verteilt wird. Anschließend wird dann der unbekannte Zustand eines Quantenteilchens beim Sender ohne dessen eigentliche Vermessung übertragen. Hierzu führt der Sender lokale Bell-Messungen (siehe Physik in unserer Zeit **2015**, *46*(6), 28) durch und überträgt die klassischen Messergebnisse über einen klassischen Kanal an den Empfänger. Dieser ist mit Hilfe lokaler Operation an seinem verschränkten Qubit, welche auf den empfangenen klassischen Informationen basieren, in der Lage, den entsprechenden Quantenzustand herzustellen (siehe „Verschränkungsbasierte Quanteninformationsübertragung“). Diese Protokolle sind insbesondere im Hinblick auf Sicherheitsaspekte von besonderer Relevanz.

Anwendungsperspektiven für Quantennetzwerke

Im Folgenden geben wir einen Ausblick auf perspektivische Anwendungsmöglichkeiten von Quantennetzwerken, wie sie in Abbildung 5 dargestellt sind. Diese lassen sich grob in die drei Kategorien Skalierung von Quantenressourcen, Gewährleistung von Sicherheit und neue Funktionalitäten einteilen.

Klassische Netzwerke dienten zunächst der Ermöglichung von Echtzeitkommunikation über größere Distanzen, beispielsweise via Telefon. Einen weiteren Durchbruch haben sie erlebt, als hierüber klassische Rechner vernetzt werden konnten, um deren Rechenleistung zu steigern. Letzendlich hat hierauf basierend das Internet zum weltweiten Zugang zu Information und einem ganzen Blumenstrauß an Anwendungsmöglichkeiten geführt. Daher ist ein großer Motivationstreiber hinter der Schaffung von Quantennetzwerken die Vernetzung von Quantencomputern und deren Verbundbetrieb. Wie im klassischen Bereich des High Performance Computings (HPC), bei dem komplexe Rechnungen auf mehrere Rechenknoten verteilt werden, soll es mit Hilfe von

ABB. 5 | QUANTENNETZWERKE



Illustrative Darstellung eines Quantennetzwerks, in dem als Anwendungen beispielsweise verteilte Quantensensorik oder Blindes Quantencomputing ausgeführt werden können *(Foto: DLR).*

Quantennetzwerken möglich sein, „verteiltes Quantencomputing“ durchzuführen. Das erhöht die verfügbaren Quantenrechenressourcen. Momentan werden an unterschiedlichen Stellen bereits erste Schritte in Richtung der Vernetzung von QPUs (Quantum Processing Units) unternommen. Beispielsweise sieht die Quantum Computing Roadmap von IBM (siehe „Internet) bereits für 2025 die Einbindung von QPUs in ein Netzwerk mit klassischer und Quantenkommunikation vor. Hierdurch soll eine Skalierung der zur Verfügung stehenden Quantenressourcen ermöglicht werden.

Zu den möglichen Anwendungen im Bereich Sicherheit zählen insbesondere klassische Netzwerkanwendungen, deren Sicherheit durch die Existenz von Quantencomputern bedroht sind. Insbesondere der Shor-Algorithmus als Faktorisierungsverfahren wird herkömmliche Verschlüsselungen „knackbar“ machen, die bislang als sicher gelten. Daher wird in diesem Bereich nach sicheren quantenbasierten Alternativen gesucht. Als prominentes Anwendungsszenario im Bereich der Kommunikation ist, wie erwähnt, natürlich die Quantenschlüsselverteilung zu nennen, auch als Quantenkryptographie bekannt. Darüber hinaus gibt es weitere sicherheitsrelevante Anwendungen in der Kommunikation, wie das Quantum Secret Sharing, bei dem ein Geheimnis von einem Sender über eine bestimmte Anzahl von Empfängern verteilt wird. Auf Basis des quantenmechanischen No-Cloning-Theorems wird sichergestellt, dass dieses Geheimnis nur enthüllt werden kann, wenn mehrere Empfänger zusammen arbeiten [16]. Auch die Sicherheit bestehender elektronischer Wahlverfahren ist durch die Existenz von Quantencomputern gefährdet, weshalb Quantenwahlverfahren untersucht werden [17].

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

15213943, 2025, 3, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/piuz.202401725 by Disch Zentrum F. Luft-U. Raum Fahrt In D. Helmholtz Gemein., Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Beim quantenbasierten Wählen geht es im Wesentlichen um zwei Verfahren. Entweder wird ein „reisender Stimmzettel“ betrachtet, welcher durch ein Quantensystem realisiert ist, das mit einem anderen Quantensystem bei einer Autorität, etwa der Wahlleitung, verschränkt ist. An jedem Netzwerkknoten führt ein Wähler eine lokale Operation am „reisenden Stimmzettel“ durch, welche abhängig von dessen Stimmabgabe ist. Bei der Autorität kann dann das gesamte Wahlergebnis nur unter Vermessung beider Quantensysteme ermittelt werden. Alternativ erhält jeder Wähler ein separates Quantensystem über das Quantennetzwerk, und diese Systeme sind alle mit einem Quantensystem der Autorität verschränkt. Auch hier führen die Wähler stimmabhängige Operationen an den lokalen Netzwerkknoten durch. In diesem Fall kann das gesamte Wahlergebnis ebenfalls nur unter Vermessung aller Quantensysteme bei der Autorität ermittelt werden. In beiden Fällen handelt es sich aber um theoretische Konzepte, die noch nicht alle für eine Wahl erforderlichen Sicherheitsmerkmale erfüllen, jedoch gegenüber quantenbasierten Angriffen einen fundamentalen Schutz bieten.

Darüber hinaus wird auch an Quantenwährungen [18] als Alternativen zu klassisch-kryptographisch gesicherten Bitcoins geforscht. Zudem bieten verschränkungsbasierte Quantentechnologien große Sicherheitsvorteile für die sichere Identifizierung von Kommunikationspartnern [19].

Von besonderem Interesse sind die neuen Funktionalitäten, die Quantennetzwerke bieten können. Beispielsweise ermöglichen sie die Verschränkung verteilter Quantensensoren und bieten damit die Perspektive, eine höhere Messgenauigkeit zu erzielen. Auch eine verbesserte Synchronisation von Atomuhren über Quantennetzwerke bildet eine zukünftige Anwendung [20]. Darüber hinaus ist hier das „Blinde Quantencomputing“ [21, 22] zu nennen, bei dem ein Client nur eingeschränkte Quantenfunktionalitäten besitzt – etwa einen Quantencomputer mit nur wenigen Quantenbits oder mit einem eingeschränkten Gatterset – und daher seine Rechnungen auf einem entfernten Quantenserver durchführen muss. Mit Hilfe des „Blinden Quantencomputings“ (Abbildung 5 rechts unten) ist es in bestimmten Szenarien möglich, den Quantenserver zu nutzen, ohne dass dessen Betreiber prinzipiell Zugriff auf bestimmte Quantendaten bekommt oder sogar den dort ausgeführten Algorithmus eindeutig erkennen kann.

INTERNET

EAGLE 1
https://t1p.de/EAGLE_1

Quantum Roadmap von IBM
https://www.ibm.com/roadmaps/quantum

Artikel über Quanteninternet in Physik in unserer Zeit
https://t1p.de/Quanteninternet

Sicherlich werden uns die Quantennetzwerke, wenn sie erst einmal zur Verfügung stehen, mit vielen weiteren neuen Funktionalitäten ins Staunen versetzen. Für all diese Zukunftsszenarien sind jedoch noch viele Weiterentwicklungen nötig, die eine enge Zusammenarbeit von Theorie, Experiment und Implementierung verlangen. Dafür ist die fachübergreifende Expertise und Kooperation erforderlich, insbesondere zwischen der Physik, Informatik und den Ingenieurswissenschaften. Erst dann kann es uns gelingen, das volle Potenzial der Quantennetzwerke zu entfalten und ein Quanteninternet zu etablieren.

Zusammenfassung

Die Quantenschlüsselverteilung ist eine der fortschrittlichsten Quantentechnologien. Entsprechende Komponenten sind kommerziell erhältlich. Ihr Einsatz auf Satelliten und in vielen Demonstrationsnetzen wird weltweit erprobt. Allerdings benötigen die bisher meist verwendeten Verfahren „vertrauenswürdige“ Zwischenstationen, etwa Satelliten. Weltweit arbeiten viele Forschungsgruppen daran, Verfahren mit globaler Reichweite zu entwickeln, die ohne diese speziellen und möglicherweise kompromittierbaren Zwischenstationen auskommen. Eine vielversprechende Lösung sind verschränkungsbasierte Quantennetzwerke via Satellit. Diese ermöglichen zudem die perspektivische Vernetzung von Quantentechnologien wie Quantencomputer, Quantenuhren und Quantensensoren. Das bietet ganz neue Funktionalitäten. Allerdings erfordern viele dieser Konzepte Quantenspeicher an Bord der Satelliten, die als Quantenrepeater fungieren.

Stichwörter

Quantentechnologien, Satellitenkommunikation, optische Links, Quantenschlüsselverteilung, Quantenverschränkung, Quanteninformationsübertragung, Quantennetzwerke, Quantenrepeater, verteiltes Quantencomputing.

Danksagung

Wir danken B. Kubala und A. Sauer sowie den Quanten-Teams des Instituts für Quantenphysik der Universität Ulm und der Bundesdruckerei GmbH für zahlreiche Diskussionen zu zukünftigen Anwendungen von Quantennetzwerken. Wir sind S. Luhn dankbar für die graphische Darstellung der Quantennetzwerke.

Open-Access-Veröffentlichung ermöglicht und organisiert durch Projekt DEAL.

Literatur

[1] D. Castelvecchi, Nature **2018**, *554*, 289.
[2] C. Becher et al., Physik in unserer Zeit **2016**, *47*(1), 20.
[3] J.S. Sidhu et al., IET Quant. Comm. **2021**, *2*(4), 182.
[4] S.-K. Liao et al., Nature **2017**, *549*(7670), 43.
[5] J. Yin et al., Science **2017**, *356*, 1140.
[6] M. Hutterer et al., in: Proc. of IAC, Paris 2022, https://t1p.de/QKD_CubeSat.
[7] P. Xu et al., Science **2019**, *366*, 132.
[8] S-K. Liao, H-L. Yong, C. Liu et al., Nat. Photon. **2017**, *11*, 509.
[9] T. Huber et al., Nano Lett. **2014**, *14*, 7107.

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

15213943, 2025, 3, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/piuz.202401725 by Dtsch Zentrum F. Luft-U. Raum Fahrt In D. Helmholtz Gemein., Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

[10] X.-H. Bao et al., Phys. Rev. Lett. **2008**, *101*, 190501.
[11] Y. C. Yu et al., Phys. Rev. A **2018**, *97*, 043809.
[12] R. Fickler et al., Science **2012**, *338*, 640.
[13] S. Wehner, D. Elkouss, R. Hanson, Science **2018**, *362*, eaam9288.
[14] C. M. Knaut et al., Nature **2024**, *629*, 573.
[15] J.-L. Liu et al., Nature **2024**, *629*, 579.
[16] M. Hillery et al., Phys. Rev. A **1998**, *59*(3), 1829.
[17] M. Hillery et al., Phys. Lett. A **2006**, 349, 75.
[18] St. Wiesner, SIGACT News **1983**, *15*, 78.
[19] Sh. Ben-David, O. Sattath, Quantum **2023**, *7*, 901.
[20] P. Kómár et al., Nature Phys. **2014**, *10*, 582.
[21] J. F. Fitzsimons, Quantum Inf. **2017**, *3*, 23.
[22] S. Barz. et al., Science **2012**, *335*, 303.
[23] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, 10th Anniversary Edition. Cambridge University Press, Cambridge 2010.

Die Autoren

V.r.n.l.: Kai Bongs promovierte an der Leibniz Universität Hannover und leitet das Institut für Quantentechnologien des Deutschen Zentrums für Luft- und Raumfahrt (DLR) in Ulm mit assoziierter Professur an der Universität Ulm. Sabine Wölk promovierte an der Universität Ulm im Bereich Quanteninformationsverarbeitung und leitet kommissarisch die Abteilung Quanteninformation und -kommunikation am selben Institut des DLR in Ulm. Matthias Zimmermann promovierte an der Universität Ulm im Bereich der atomaren Quantensensorik und leitet die Gruppe Quantensimulationen und -anwendungen am selben Institut in Ulm. Kaisa Laiho (kein Foto) ist promovierte Physikerin im Bereich der experimentellen Quantenoptik und arbeitet am selben Institut in Ulm.

Florian Moll (links) studierte Elektrotechnik an der Technischen Universität München und leitet die Gruppe Systeme der Quantenkommunikation am Institut für Kommunikation und Navigation DLR in Oberpfaffenhofen. Christian Fuchs (rechts) promovierte an der Christian-Albrechts-Universität zu Kiel und leitet die Abteilung optische Satellitenlinks am selben Institut des DLR in Oberpfaffenhofen.

Anschrift
Prof. Dr. Kai Bongs, DLR Institut für Quantentechnologien, Wilhelm-Runge Straße 10, 89081 Ulm. kai.bongs@dlr.de

© 2025 The Author(s). Physik in unserer Zeit published by Wiley-VCH GmbH

15213943, 2025, 3, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/piuz.202401725 by Dtsch Zentrum F. Luft-U. Raum Fahrt In D. Helmholtz Gemein., Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License