Deutsche Physikalische Gesellschaft DPG

QUANTUM FLAGSHIP

Sonderausgabe Nr. 3 zu den Quantentechnologie-Initiativen der EU und des BMBF

PHYSIKonkret

Nr. 40

Mit Quanten abhörsicher kommunizieren

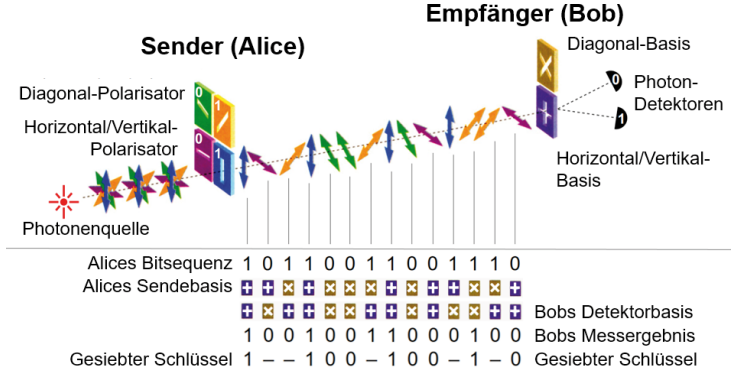
- Mit Quantenteilchen lässt sich abhörsicher kommunizieren.
- Für weite Strecken benötigt man noch geeignete Schnittstellen und sogenannte Quantenrepeater.
- Ein abhörsicheres Quanten-Internet nimmt langsam Gestalt an.

Unsere elektronische Kommunikation soll nicht an falsche Ohren gelangen, dafür verlassen wir uns auf deren abhörsichere Übertragung. Diese beruht derzeit auf mathematischen Verschlüsselungsalgorithmen, welche zwar schwierig, aber nicht unmöglich zu knacken sind, insbesondere wenn dem Lauscher ein Quantencomputer zur Verfügung stünde [1]. Diese Bedenken gibt es nicht, wenn die sensible Information mittels Quantenteilchen übertragen wird. Dann können die physikalischen Gesetze der Quantenmechanik Abhörsicherheit garantieren. Das liegt am sogenannten no-cloning-Gesetz. Das verbietet das verlustfreie Kopieren eines Quantenteilchens. Die übertragene Information kann zwar abgefangen werden, jedoch nicht unbemerkt, weil sie nicht vollständig wiederhergestellt werden kann. Darauf basierend haben Charles Bennett und Gilles Brassard 1984 ihr Protokoll BB84 zur Vereinbarung eines sicheren Schlüssels mithilfe von einzelnen Quantenteilchen beschrieben (Abb. 1). Ein anderes Protokoll, Ekert91, verwendet sogenannte quantenmechanisch verschränkte Teilchen.

Die geeignetsten Quantenteilchen zur Informationsübertragung sind Lichtteilchen (Photonen) in deren Polarisation (der Schwingungsrichtung der Lichtwelle) die Information in sogenannten Quantenbits codiert werden kann. Quantenbits sind die quantenphysikalische Erweiterung zu den klassischen Bits. Sie können nicht nur Werte von Null oder Eins annehmen, sondern auch alle Zustände (Überlagerungen) dazwischen. Wenn sie jedoch nachgewiesen – z. B. abgehört – werden, ergibt sich nur eins von zwei möglichen Ergebnissen, und damit geht ihr Überlagerungszustand verloren. Ein solcher kann deshalb nicht zweimal gemessen und daher auch nicht abgehört werden.

Diese Empfindlichkeit der Quantenbits garantiert die Informationssicherheit. Jedoch ist keine Übertragungsstrecke verlustfrei, so dass einzelne Photonen nur eine begrenzte Reichweite von unter 100 km haben. Um größere Strecken zu überwinden, würde man gerne das Photon wie in der klassischen Kommunikation mit sog. Repeatern weiterleiten. Dem steht aber das no-cloning-Gesetz im Wege. Deshalb ist ein sogenannter Quantenrepeater nötig. Dieser nutzt eine besondere Korrelation zwischen Quantenteilchen: Die Verschränkung. Mithilfe von Quantenspeichern in kurzen Abständen wird die Verschränkung über längere Strecken bis zu den Kommunikationspartnern weitergereicht, welche sie dann nach dem Ekert91-Protokoll zur verschlüsselten Kommunikation nutzen.

Abb. 1



Schlüsselerstellung nach dem BB84-Protokoll. Die Bitsequenz des Senders ist in Photonen in zwei Basen (Diagonal/Antidiagonal oder Horizontal/Vertikal) mit je zwei Polarisationen (0/1) kodiert. Der Empfänger wechselt willkürlich die Messbasis. Die Basen werden dann verglichen. Wenn sie übereinstimmen, ist das Messergebnis zuverlässig, sonst wird es verworfen. Es verbleibt der gesiebte Schlüssel, der nur Sender und Empfänger bekannt ist.
(Quelle: Wolfgang Tittel et al., Physikalische Blätter, 55-6, 1999, S. 25)

„Quanten-Kommunikation öffnet das Tor zu physikalisch, d. h. messbar sicherer Kommunikation."

Dieter Meschede, Präsident der Deutschen Physikalischen Gesellschaft

Abb. 2

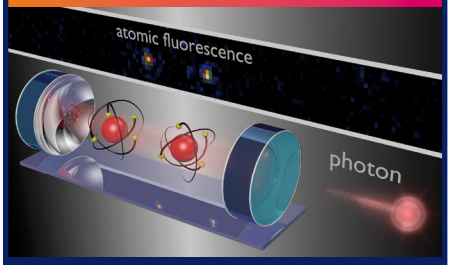


Illustration einer Atom-Photon-Schnittstelle. Einzelne Atome werden durch das Lichtfeld zwischen zwei Spiegeln zum Aussenden einzelner Photonen angeregt. Zur Realisierung eines Quantenrepeaters werden zwei Atome als Quantenspeicher verwendet (im Hintergrund ein reales Kamerabild). (Bild: Stephan Welte, Max-Planck–Institut für Quantenoptik)

Der Quantenrepeater ist ein Schlüsselelement. Ihm wird aktuell große Forschungsaktivität gewidmet, in Deutschland besonders im BMBF-geförderten Verbundprojekt Q.Link.X. Ein wesentliches Element ist die Schnittstelle, an der übertragene Quantenbits empfangen, gespeichert und gesendet werden; dies geschieht in Atomen oder atom-artigen Systemen wie Halbleiter-Quantenpunkten oder Farbzentren in Diamant (Abb. 2). Um die Quantenbits in existierende optische Fasernetzwerke einzuspeisen, ist zusätzlich ein Konverter erforderlich, welcher die Photonen in die für die Faserübertragung optimalen Wellenlängen umwandelt. Für alle diese Elemente gibt es bereits Labor-Prototypen. Ein abhörsicheres Quanten-Internet, das vor Kurzem noch nach Science-Fiction klang, nimmt also langsam Gestalt an.

Quelle:
[1] Quantencomputer – Rechner der Zukunft? Physikkonkret Nr. 29 https://www.dpg-physik.de/veroeffentlichungen/publikationen/physikkonkret/quantencomputer-rechner-der-zukunft

Deutsche Physikalische Gesellschaft

Die Deutsche Physikalische Gesellschaft e. V. (DPG), deren Tradition bis in das Jahr 1845 zurückreicht, ist die älteste nationale und mit mehr als 60.000 Mitgliedern auch die größte physikalische Fachgesellschaft weltweit. Sie versteht sich als Forum und Sprachrohr der Physik und verfolgt als gemeinnütziger Verein keine wirtschaftlichen Interessen. Die DPG unterstützt den Gedankenaustausch innerhalb der wissenschaftlichen Gemeinschaft mit Tagungen und Publikationen. Sie engagiert sich in der gesellschaftspolitischen Diskussion zu Themen wie Nachwuchsförderung, Chancengleichheit, Klimaschutz, Energieversorgung und Rüstungskontrolle. Sie fördert den Physikunterricht und möchte darüber hinaus allen Neugierigen ein Fenster zur Physik öffnen.

In der DPG sind Wissenschaftlerinnen und Wissenschaftler, Studierende, Lehrerinnen und Lehrer, in der Industrie tätige oder einfach nur an Physik interessierte Personen ebenso vertreten wie Patentanwälte oder Wissenschaftsjournalisten. Gegenwärtig hat die DPG neun Nobelpreisträger in ihren Reihen. Weltberühmte Mitglieder hatte die DPG immer schon. So waren Albert Einstein, Hermann von Helmholtz und Max Planck einst Präsidenten der DPG.

Die DPG finanziert sich im Wesentlichen aus Mitgliedsbeiträgen. Ihre Aktivitäten werden außerdem von Bundes- und Landesseite sowie von gemeinnützigen Organisationen gefördert. Besonders eng kooperiert die DPG mit der Wilhelm und Else Heraeus-Stiftung.

Die Quantentechnologie-Initiativen der EU und des BMBF

Im Rahmen des Programms Future and Emerging Technologies startete die Europäische Union im Jahr 2018 das Quantum-Flagship als eine der größten und ambitioniertesten Forschungsinitiativen. Das Quantum-Flagship ist mit einem Budget von einer Milliarde Euro ausgestattet und hat eine Laufzeit von zehn Jahren. Hauptziel der Initiative ist es, die wissenschaftliche Führung und Exzellenz Europas auf diesem Forschungsgebiet zu festigen und auszubauen sowie die quantenphysikalische Forschung vom Labor auf den Markt zu bringen.

Bereits im September 2018 beschloss die Bundesregierung darüber hinaus das Förder-Rahmenprogramm „Quantentechnologien – von den Grundlagen zum Markt“ mit einem Umfang von 650 Millionen Euro für Forschung und Entwicklung. Ziel ist, die Entwicklung der Quantentechnologien in Deutschland strategisch voranzutreiben. Deutsche Institute und Unternehmen sollen die sogenannte zweite Quantenrevolution maßgeblich mitgestalten und eine führende Rolle beim Transfer in die Anwendung und Vermarktung übernehmen. Das Rahmenprogramm definiert die Ausgangslage und skizziert Ziele und Maßnahmen bis 2022.

Deutsche Physikalische Gesellschaft e. V.

Geschäftsstelle
Hauptstraße 5
53604 Bad Honnef

Tel.: 02224 / 92 32 - 0
Fax: 02224 / 92 32 - 50
E-Mail: dpg@dpg-physik.de

Die Deutsche Physikalische Gesellschaft dankt Jürgen Eschner und Christoph Becher, Universität des Saarlandes, für die wissenschaftliche Beratung.