



© FREEPIK / stwul

Geheimcode im Laserfunk – wie Quantenkryptographie Spione abwehrt

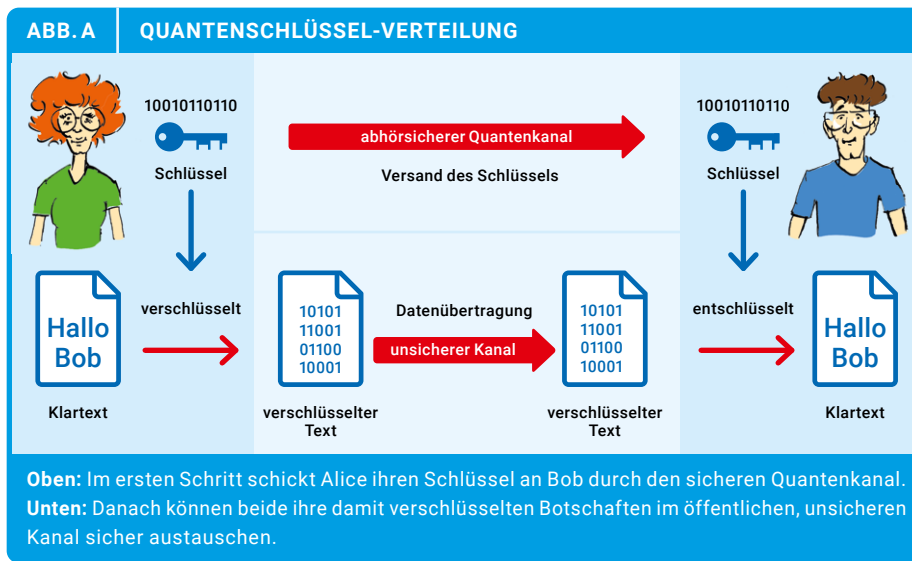
Geheime Nachrichten so zu verschlüsseln, dass nur der Empfänger sie lesen kann: Das ist heute wichtiger denn je. Die Quantenphysik bietet einzigartige Möglichkeiten für einen Austausch von Geheimschlüsseln über größere Distanzen. Auf dem Gebiet dieses Quantenschlüssel-Austauschs, auch Quantenkryptographie genannt, forschen mehrere Max-Planck-Teams. Dabei geht es um das Senden von Geheimschlüsseln durch Glasfasern und via Satellit.

Das wissenschaftliche Wort „Kryptographie“ basiert auf dem Altgriechischen und heißt so viel wie „geheimes Schreiben“. Heute werden selbst im privaten Chat über soziale Netzwerke starke Verschlüsselungen verwendet. Sie sind nur mit so hohem Rechenaufwand zu brechen, dass das auf heutigen Computern nicht möglich ist. Allerdings: Dass eine Verschlüsselung absolut knacksicher ist, lässt sich selbst für die besten Verfahren mathematisch nicht beweisen. Man setzt darauf, dass selbst die leistungsfähigsten Supercomputer zu lange rechnen müssen, um den Code zeitnah brechen zu können. Dieser Strategie droht jedoch eine neue Gefahr, die aus der Quantenwelt kommt: Sobald **Quantencomputer** praktisch einsetzbar sein werden, ist kein heute etablierter Code mehr sicher gegen schnelles Entschlüsseln.

Selbst stärkere Codes, die derzeit entwickelt werden, sind nicht beweisbar sicher gegen künftige Quantencomputer-Angriffe.

Doch die Quantenwelt bietet ein wirksames Gegenmittel: den abhörsicheren Austausch von sogenannten **Quantenschlüsseln**. Tatsächlich gibt es schon seit einigen Jahren kommerzielle Anbieter. Allerdings sind diese abhörsicheren Verbindungen bislang nur über relativ kurze Glasfaserverbindungen praktikabel – trotz Rekordmeldungen von hunderten von Kilometern. Diese Technologie erfordert also noch viel Grundlagenforschung.

Giulio Malavolta arbeitet am Max-Planck-Institut für Sicherheit und Privatsphäre unter anderem an Protokollen für eine sichere Nachrichtenübermittlung in Quantennetzwerken. „Quanteninformation ist nicht kopierbar“, sagt er. Das unterscheidet sie grundlegend von klassischer Information: Im Alltag kopieren wir andauernd klassische Bits von einem Gerät auf ein anderes, zum Beispiel wenn wir Videos streamen. In der Wissenschaft heißt diese spezielle Eigenschaft der Quanteninformation **„No-Cloning-Theorem“** – Klonen bedeutet Kopieren. Wenn also eine Alice (für „A“) einem Bob (für „B“) einen quantenverschlüsselten „Brief“ schickt, kann Bob beim Empfang erkennen, ob jemand



Da Photonen als Quantenteilchen auch Welleneigenschaften haben, entspricht die Polarisierung der Schwingungsrichtung der Welle. „Ihr könnt sie euch als fliegende Zeiger vorstellen“, erklärt die Mutter den Geschwistern: „Sie zeigen senkrecht zur Flugbahn und dürfen nach den Quantenregeln nur in zwei verschiedene Richtungen einrasten“. Definiert man eine der beiden Richtungen willkürlich als 1, dann ist die andere die 0.

Die Mutter drückt nun Alice und Bob jeweils ein Tablet in die Hand. Alices Tablet ist mit dem sendenden Laser verbunden, Bobs mit dem Empfänger mit einem sehr empfindlichen Lichtsensor. Das Laserlicht wird im Sender so abgeschwächt, dass nur noch

einzelne Photonen die Strahlstrecke entlangflitzen können – wie ein Wasserstrahl zu einzelnen Tropfen wird, wenn der Hahn fast zuge dreht ist. Nach dem Laser müssen sie einen sogenannten Polarisator passieren. Er ist über das Tablet in zwei zueinander senkrechten Richtungen drehbar und prägt so dem Qubit einen Zustand 0 oder 1 auf. Außerdem kann Alice den Polarisator um 45° drehen. Auch in dieser verdrehten „Messbasis“ kann sie 0 oder 1 anwählen.

ABHÖRSICHERE PHOTONENPOST

Natürlich werden in der Quantenkryptographie keine Papierbriefe verschickt, sondern Lichtquanten – Photonen – mittels Laserlicht. Die abhörsichere Quantenverbindung dient auch allein dem Austausch eines Quantenschlüssels zwischen Alice und Bob. Damit verschlüsseln sie dann ihre eigentliche Botschaft. Diese können sie nun unbesorgt durch das ganz normale öffentliche Netz schicken, denn das geht viel schneller als im Quantenkanal (Abb. A). Alle können mitlauschen, aber niemand kann die Botschaft knacken. Wirklich niemand? Tatsächlich lässt sich für einen Quantenschlüssel genau ausrechnen, wie knacksicher er ist. Das unterscheidet die Quantenkryptografie grundlegend von der klassischen Kryptografie. Einfach gesagt: Je länger der Quantenschlüssel ist, desto kleiner ist das Risiko einer Entschlüsselung. Die Schrumpfung dieses Restrisikos auf fast Null ist technisch kein Problem.

Das einfachste quantenkryptographische Verfahren setzt auf die Nichtkopierbarkeit von Quanteninformation. Die Idee hatten der US-amerikanische Physiker Charles Bennet und sein frankokanadischer Kollege Gilles Brassard bereits 1984, weshalb dieses Protokoll kurz „BB84“ genannt wird. Es funktioniert im Prinzip wie das Briefbeispiel. Die Quanteninformation des Schlüssels wird dabei in einen langen Zug aus Photonen hineingeschrieben. Jedes Photon entspricht einem Quantenbit, das sich unterwegs in einer Eve unbekannten Überlagerung der beiden Bit-Zustände 0 und 1 befindet. Hineingeschrieben wird die Quanteninformation über eine geeignete Messung – und so auch gelesen.

STILLE POST BEI ALICE UND BOB ZUHAUSE

Stellen wir uns wieder Alice und Bob vor (s. Techmax 36). Ihre Mutter, Physikerin, hat im langen Flur eine kleine Laseranlage mit Sender und Empfänger aufgebaut. Die Quanteninformation schreibt der Sender hier in die sogenannte Polarisierung der Photonen hinein.

Den Polarisator kann man sich einfach als quadratische Scheibe mit einem Schlitz vorstellen (Abb. B links). Die Drehposition kann Alice über eine kleine App wechseln. „Den Schlüssel erzeugst du, indem du zwischen den beiden Polarisatorpositionen wechselst und dir die gewählte Messbasis notierst“, erklärt ihr die Mutter: „Dann drückst du auf den Senden-Button, und ein Photon mit der aufgeprägten Information fliegt zu Bob.“

In Bobs Empfänger ist ein um 45° drehbares Teil eingebaut, das wie zwei um 90° gekreuzte Polarisatoren wirkt. Diesen „Analyзатор“ muss das empfangene Photon passieren, bevor es auf einem hochempfindlichen Fotodetektor auftrifft. Wir können ihn uns als Quadrat mit einem Kreuzschlitz vorstellen (Abb. B rechts). Er kann in der gewählten Messbasis die Bits 0 und 1 unterscheiden.

Bob kennt die von Alice gewählten Einstellungen nicht. Also muss er über seine App eine der beiden Messbasen willkürlich voreinstellen und das Empfangsergebnis notieren. „Nun kommt der Clou“, erklärt die Mutter: „Immer wenn ihr zufällig die gleiche Messbasis gewählt habt, hat Bob eine korrekte Quanteninformation empfangen.“ Ist Bobs Messbasis gegenüber der von Alice um 45° verdreht, dann ist die Quanteninformation zerstört. Der Detektor meldet zwar dann eine zufällig gemessene 0 oder 1, aber das ist keine von Alice gesendete Information. „Genau das bringt die Quantensicherheit in diese Übertragungsstrecke“, erklärt die Mutter. Aber wie erhält Bob nun den richtigen Schlüssel?

Dazu müssen Alice und Bob nur die Listen mit ihren Messbasiseinstellungen austauschen, etwa über ihre Smartphones. Sie vergleichen die beiden Listen und behalten nur die Bits 0 oder 1 bei gleicher Einstellung. Ist kein Photon verlorengegangen, dann erhalten Alice und Bob exakt gleiche Listen mit Nullen und

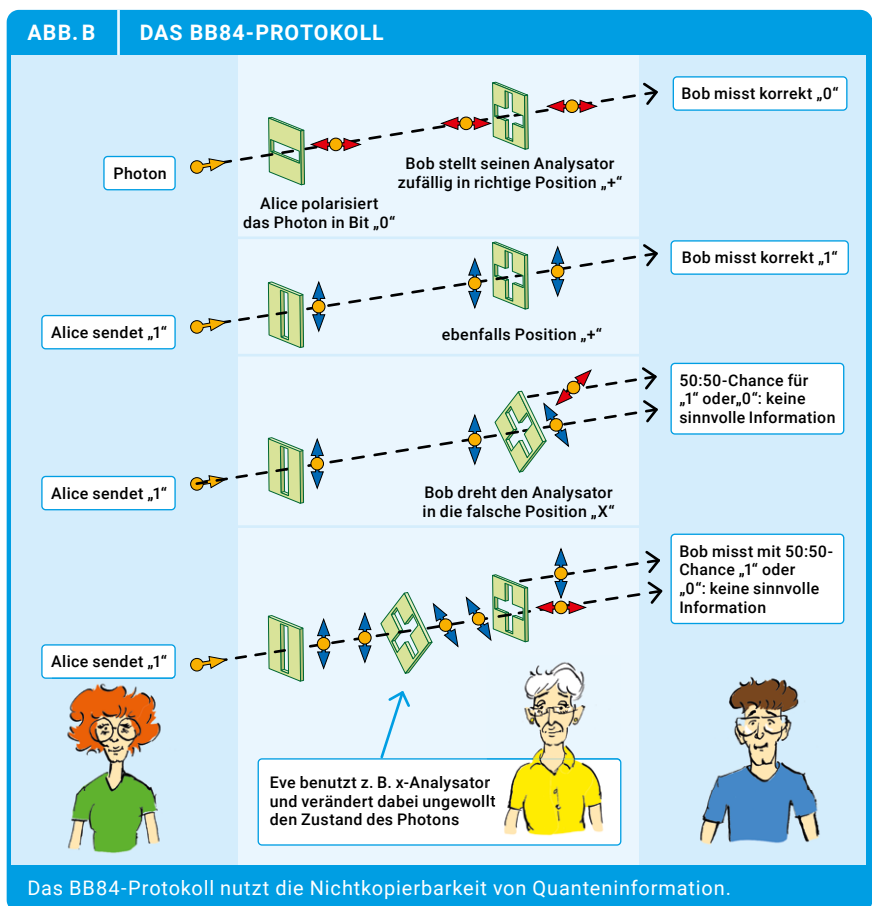
Einsen. Das ist der von Alice gesendete Schlüssel, mit dem sie nun ihre Botschaften für den öffentlichen, klassischen Kanal verschlüsseln können. Natürlich kann eine Lauscherin Eve die beiden im öffentlichen Kanal belauschen und die Liste der Messeinstellungen korrekt kopieren. Doch ihr fehlt die entscheidende Information, ob Alice bei einer bestimmten Messeinstellung nun eine 0 oder 1 verschickt hat. Sie kommt also so nicht an den Schlüssel heran. Was passiert, wenn sie sich in den Quantenkanal einschaltet?

Die Mutter macht das nun in der Rolle der Eve. Sie schiebt in die Mitte der Übertragungsstrecke ein Gerät, das einen Empfänger mit Analysator und einen Sender mit Polarisator vereint. Damit kann sie Alices Photon abfangen, analysieren und dann ein Photon mit der von Eve gemessenen Information an Bob weiterschicken. Auch bei diesem Experiment notiert Alice, welche Information sie empfangen hat. Nun vergleichen die Geschwister wieder ihre Listen und verwenden die gleich gewählten Messbasen für den Schlüssel. Bei diesem Vergleich erkennen sie viele Fehler. Das liegt daran, dass Eve die von Alice versendete Information ohne Listenaustausch nicht kennen konnte. Also hat sie Falschinformation an Bob weitergesendet.

DOPPELT SICHER MIT VERSCHRÄNKUNG

Diese Art des Quantenschlüssel-Austausch nach dem **BB84-Protokoll** heißt auf Englisch auch „Prepare and Measure“, also „Präpariere und Messe“. Eine noch viel merkwürdigere Eigenschaft der Quantenphysik kann die Sicherheit noch steigern: die Verschränkung (s. [Techmax 36](#)). Hier verschickt der Sender gleich zwei Photonen, eines an Alice und eines an Bob. Die beiden Photonen werden aber nun miteinander verschränkt ([Abb. C](#)). Sie bilden damit eine Art gemeinsames Quantenobjekt, enthalten aber noch keine Information über den Schlüssel. Alice kann nun durch eine Messung an ihrem Photon zum Beispiel eine 0 erzeugen. Diese Messung legt dann beim verschränkten Photon, das Bob erreicht, sofort eine 1 fest. Hat er seinen Analysator zufällig auf die korrekte Messbasis eingestellt, misst er diese 1 korrekt. Der Vorteil: Sobald sich Eve in die Übertragungsstrecke einschaltet, zerstört sie mit ihrer Messung die Verschränkung und damit die Schlüsselübertragung zu Bob.

Diese Idee hatte der polnisch-britische Physiker Artur Ekert 1991. Viele Experimente zeigten inzwischen, dass das **E91-Protokoll** funktioniert. Will man allerdings das vorhandene Glasfasernetz nutzen, dann gehen mit wachsender Übertragungsstrecke immer mehr Photonen verloren. Das begrenzt eine praktikable Übertragungsstrecke auf eine Größenordnung von 100 Kilometern. „Grob kann man sagen, dass alle zehn Kilometer nur noch die Hälfte der Photonen da ist“, erklärt Gerhard Rempe, Direktor am Max-Planck-Institut für Quantenoptik. Er forscht an Lösungen

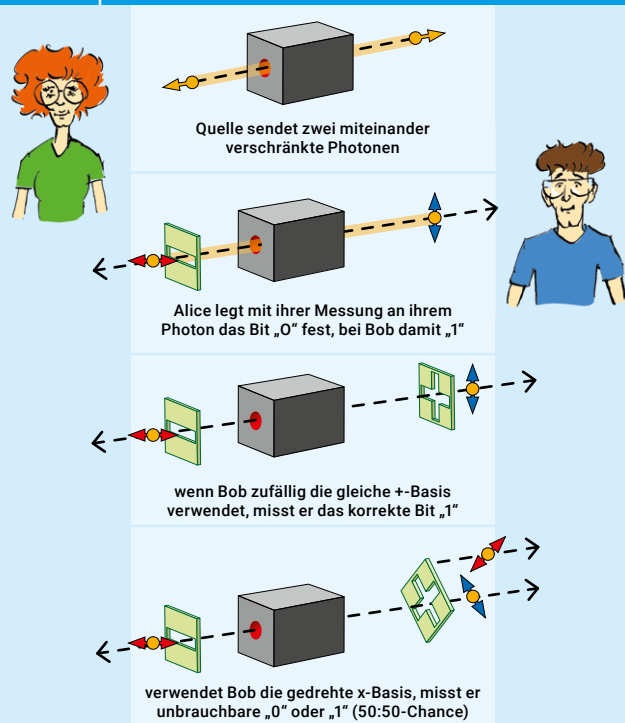


für dieses Grundproblem eines glasfaserbasierten Quanteninternets. Nach jeder Streckenverdopplung ist also nur noch die Hälfte der Photonen in der Quantenpost vorhanden: Der Verlust ist exponentiell!

ROBUSTERE GLASFASERÜBERTRAGUNG

Also suchte das Team von Rempe nach einem Gegenmittel. Die Lösung: Es verteilte die Verschränkung und damit das zu übertragende Qubit auf einen Schwarm von Photonen, die hintereinander aus dem Sender in die Glasfaser fliegen. „Wenn maximal die Hälfte der Photonen weg ist, lässt sich nach dem Empfang noch die Verschränkung und damit das Quantenbit rekonstruieren“, erklärt der Physiker. Die Verpackung der verschränkten Quanteninformation erfordert allerdings abstrakte Mathematik.

Rempes Team nutzt dafür sogenannte **Graph-Zustände**. Man kann sie sich wie einen Weihnachtsdeko-Bausatz aus LED-Lichtern vorstellen, die sich mit kurzen Kabeln zu verschiedenen Figuren zusammenstecken lassen: Ketten, Leitern, Ringe oder baumartige Verzweigungen. Die LED-Lichter symbolisieren die Photonen, die Kabel die Verschränkung zwischen ihnen. Das spielt sich allerdings in einem abstrakten mathematischen Raum ab. In der Realität bleibt die Reihenanordnung der hintereinander fliegenden Photonen unverändert. Wenn man diese Graph-Zustände geschickt einsetzt, dann verteilen sie die Verschränkung über diesen Photonschwarm so, dass sogar nur noch die Hälfte von ihnen die Quantenpost lesbar ins Ziel bringen kann. Damit sollte sich die Übertragungsstrecke trotz Verlusten deutlich verlängern lassen. Rempes Team erforscht, wie das gelingen kann.



Die Verschränkung macht das E91-Übertragungsprotokoll noch sicherer. Nachteil: Ihre besondere Empfindlichkeit gegen Störungen erhöht den technischen Aufwand.

QUANTENFUNK ÜBERS WELTALL

Wie wäre es, wenn man vom exponentiellen Verlust an Photonen wegkäme? Genau das ist bei der **Satellitenübertragung** im Prinzip möglich, an der Christoph Marquardt am Max-Planck-Institut für die Physik des Lichts forscht. Ein Beispiel ist die europäische Demonstrationssonde **EAGLE-1**, die schon eine Vorstufe zu einem kommerziellen Quantensatelliten darstellt. Sie soll 2026 in die Umlaufbahn geschossen werden. Marquardts Team hat in vielen Jahren das Übertragungsprotokoll und zusammen mit Partnern den „Transmitter“ und Empfänger entwickelt. Der Transmitter „Alice“ befindet sich an Bord: Er erzeugt den Quantenschlüssel und sendet ihn nach dem Prepare-and-Measure-Prinzip, also im Prinzip BB84, zu zwei Bobs zur Erde. Diese können damit dann sicher über einen öffentlichen Kanal kommunizieren.

Ein Laserstrahl ohne Welleneigenschaften würde sich nun vom Satelliten gleichbleibend dünn bis zur Atmosphäre ausbreiten und sich erst dort durch Turbulenzen aufweiten. Allerdings verhindert das die Wellennatur des Lichts. Wellen laufen auch um Kanten herum, sie werden „gebeugt“ (s. **Techmax 15**). Daher weitet die Austrittsoptik im Transmitter den Laserstrahl etwas auf. Wie auf der Oberfläche eines kugelförmigen Ballons, der aufgeblasen wird, wächst die Querschnittsfläche des Strahls mit der Entfernung. Sie tut das quadratisch. Unter realistischen Bedingungen müsste das Empfangsteleskop am Boden einen Durchmesser von mehr als 10 Metern besitzen. So große Teleskope wären

aber zu teuer, eine typische Empfangsschüssel ist so klein wie eine große TV-Satellitenschüssel. Diese ist auf die sogenannte Telekom-Wellenlänge von 1500 Nanometern ausgelegt, also Infrarotlicht. Dieselbe Wellenlänge wird auch bei EAGLE-1 verwendet, weil es dafür bewährte Technik gibt. „Quadratisch ist aber viel besser als exponentiell“, sagt Marquardt zu dem Verlust. Bei der Satellitenkommunikation ist diese geometrische Strahlaufweitung entscheidend. Verloren gehen Photonen nur auf den letzten Kilometern in der dünnen Atmosphäre. Das macht einen vergleichsweise kleinen Verlustanteil aus. Hinzu kommt der Verlust dadurch, dass die Satellitenschüssel nur einen Ausschnitt des Strahls erfasst. Dafür war Marquardts Team mit anderen Herausforderungen konfrontiert. Zum einen ist die Überflugzeit des Satelliten auf einige Minuten beschränkt. EAGLE-1 soll in einer niedrigen Höhe von rund 500 Kilometern die Erde umkreisen.

TEST FÜR DEN QUANTENSATELLITEN

Die andere Herausforderung ist der Doppler-Effekt. Seine akustische Variante kennen wir: Wenn ein Polizeiwagen auf uns zufährt, ist der Sirenton höher als wenn er sich entfernt. Das liegt daran, dass die Schwingungen der Schallwellen erst gestaucht, dann auseinandergezogen werden. Das passiert auch beim Licht durch die Bewegung des Satelliten. Je nach Bewegung zwischen Alice und Bob wird damit der Zug der eintreffenden Photonen ebenfalls gestaucht oder verlängert, zudem ändert sich ihre Frequenz. Für die korrekte Schlüsselübertragung müssen ihre Messungen an den Photonen aber genau synchronisiert sein. Verstolpert sich einer der Empfänger, dann erhält er einen falschen Schlüssel.

Zu EAGLE-1 sagt Marquardt: „Wichtig ist, dass wir diese Technologie jetzt ausprobieren.“ So können Testempfänger in Europa, sei es im verregneten Irland oder dem hitzeblimmernden Griechenland, die Empfangsqualität in der Praxis testen. Die dabei auftretenden Fehler liefern nützliche Informationen für Verbesserungen. Wenn das Demonstrationsprojekt funktioniert, will Europa kommerzielle Satelliten für eine sichere Quantenschlüssel-Verteilung ins All bringen.

Schlüsselbegriffe

BB84-Protokoll, E91-Protokoll, EAGLE-1, Graph-Zustände, No-Cloning-Theorem, Quantencomputer, Quantenkryptographie, Quantenschlüssel, Satellitenübertragung

Link-Tipps

- Die Architektur des Quanteninternets
www.mpg.de/t371
- EAGLE-1
www.mpg.de/t372

Video-Tipp

- Abhörsicher durch Zufall
www.mpg.de/t373 ► QR



Der Comic zum Techmax-Heft

www.mpg.de/t374

www.max-wissen.de

der Link zur Forschung für Schulen ►



Hier finden Lehrkräfte Hintergrundinformationen und Materialien für den Unterricht zu den Ausgaben von **BIOMAX**, **GEOMAX** und **TECHMAX**. Weitere Exemplare können Lehrkräfte auf der Webseite kostenfrei bestellen.

CC-Lizenztexte sind unter <https://creativecommons.org/licenses> und im Detail bei den einzelnen Heften auf www.max-wissen.de zu finden.