Quanteninformation

Geheime Botschaften aus Licht

Die Quantenmechanik ermöglicht prinzipiell abhörsichere Kommunikation

Dagmar Bruß und Harald Weinfurter

Durch die kommerzielle Bedeutung des Internet haben zuverlässige Methoden der Datenverschlüsselung Einzug in den Alltag gehalten. Ein gängiges Verschlüsselungsverfahren beruht darauf, dass es in endlicher Zeit kaum möglich ist, riesige Zahlen in ihre Primfaktoren zu zerlegen. Während es die Gesetze der Quantenmechanik im Prinzip erlauben, mit einem Quantencomputer dieses Verfahren zu knacken, liefern sie zugleich die Voraussetzungen für ein anderes, absolut sicheres Verschlüsselungsverfahren.

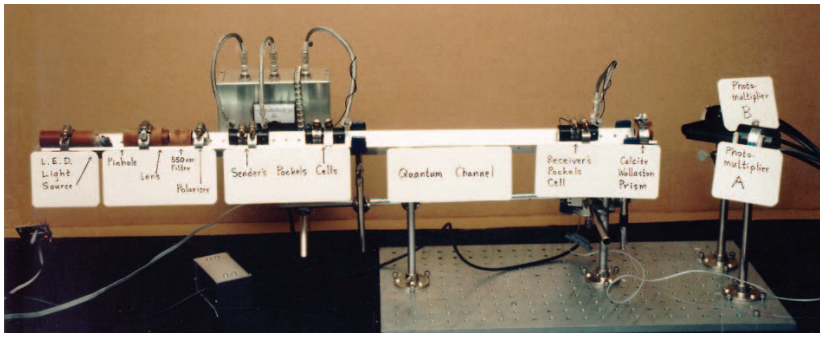

Abb. 1:
Mit diesem ersten Aufbau wurde 1991 bei IBM erstmals das Prinzip der Quantenkryptographie demonstriert [11].

Kryptographie ist die Lehre von der geheimen Nachrichtenübermittlung.[1)] Die Nachricht (der Klartext) wird vom Sender mit einem so genannten Schlüssel codiert und vom Empfänger decodiert oder entschlüsselt. Dazu müssen sich der Sender (traditionell Alice genannt) und der Empfänger (Bob) zuvor über die Verschlüsselungsmethode einigen. In der klassischen Kryptographie sind über die Jahrhunderte hinweg eine Vielzahl von Methoden entwickelt worden, die jeweils zum Ziel hatten, einem Spion (üblicherweise „Eve“ genannt, nach engl. *eavesdropping* = lauschen) die Entschlüsselung der abgefangenen Botschaft so schwer wie möglich zu machen. Wann immer es gelang, ein Verfahren zu „knacken“, wurden neue, komplexere Verschlüsselungsprotokolle entwickelt. Dieser historische Wettlauf zwischen Code-Erstellern und Code-Entschlüsselern ist in [1] auf fesselnde Weise dargestellt.

Altertümliche Methoden der Verschlüsselung sind die Transposition, bei der die Reihenfolge der Buchstaben der Nachricht geändert wird, und die Substitution, bei der jeder Buchstabe des Alphabets systematisch durch einen anderen ersetzt wird. Beide Verfahren bieten keinerlei Sicherheit, denn bereits eine einfache Analyse der Häufigkeitsverteilung erlaubt die Entschlüsselung. Im Jahr 1918 wurde die nach G. Vernam benannte Chiffre entwickelt, die nachweisbar sicher ist: Das wesentliche Element der *Vernam-Chiffre* ist ein *Zufallsschlüssel*, der aus einer zufälligen Folge von Nullen und Einsen besteht, die genauso lang wie die (zuvor ins Binäralphabet übersetzte) Nachricht ist. Alice addiert (modulo 2) den Zufallsschlüssel zur Botschaft und sendet diese verschlüsselte Nachricht an Bob. Wenn die Spionin Eve diese abfängt, erhält sie keinerlei Information über den Klartext. Bob hingegen, der ebenfalls im Besitz des geheimen Zufallsschlüssels ist, addiert diesen (wieder modulo 2) zur verschlüsselten Nachricht und erhält so die decodierte Botschaft. Der Schlüssel darf allerdings nur einmal verwendet werden, da Eve aus dem mehrmaligen Gebrauch Information gewinnen könnte, denn die Summe zweier mit dem gleichen Schlüssel codierten Nachrichten ist gleich der Summe der beiden Klartexte. Obwohl diese Methode im Prinzip absolut sicher ist, ist damit das Problem nur verschoben, nicht gelöst: wie erzeugt man einen binären Zufallsschlüssel, den nur Alice und Bob kennen?

Daher beruhen die heutzutage gängigen und weit verbreiteten Verfahren auf der Codierung mit einem sog. öffentlichen Schlüssel (*Public-Key-Kryptographie*). Hier verwendet der Sender einen allgemein zugänglichen Schlüssel; der Empfänger jedoch benötigt einen geheimen Schlüssel zur Decodierung. Die Verschlüsselung beruht hier auf einer mathematischen Funktion, deren Umkehrung sehr viel schwieriger zu berechnen ist als die Funktion selbst. Ein bedeutendes und viel verwendetes Beispiel für eine solche asymmetrische Methode ist das *RSA-Verfahren*, benannt nach R. Rivest, A. Shamir und L. Adleman. Es nutzt aus, dass die Zerlegung einer großen Zahl in Primzahlen sehr viel komplexer ist als die Multiplikation der gegebenen Primfaktoren. Was wäre aber, wenn ein allmächtiger Spion einen

Kompakt

- Verfahren der Quantenkryptographie ermöglichen es, geheime Zufallsschlüssel durch den Austausch von einzelnen Quantenzuständen zu generieren und auf ihre Abhörsicherheit zu überprüfen.
- Essenziell für die absolute Sicherheit ist dabei die Eigenschaft, dass man einen quantenmechanischen Zustand nicht messen („abhören“) kann, ohne ihn zu verändern.
- Inzwischen ist es gelungen, Quantenschlüssel sowohl über Telekom-Glasfasern als auch durch die Luft zu übertragen; erste kommerzielle Systeme sind erhältlich.

1) Das Wort Kryptographie leitet sich von den griechischen Wörtern κρυπτος („verborgen“) und γραφειν („schreiben“) ab.

Prof. Dr. Dagmar Bruß, Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf

Prof. Dr. Harald Weinfurter, Sektion Physik, LMU München, Schellingstraße 4/III, 80799 München

 1617-9439/05/1111-57

Quantencomputer besäße? Dann könnte er mit Hilfe des Quantenalgorithmus von Peter Shor große Zahlen effizient in Primfaktoren zerlegen, und RSA würde unsicher. Erkenntnisse aus der Quanteninformation bieten jedoch einen Ausweg – ein absolut sicheres Verschlüsselungsverfahren, dessen Sicherheit auf den Gesetzen der Quantenmechanik beruht: zur Erstellung des Schlüssels werden Quantenzustände verwendet. Jede Messung eines unbekannten Quantenzustands stört diesen jedoch, und so kann ein Spion keine Information erhalten, ohne Spuren zu hinterlassen.

Quantenkryptographische Protokolle

Alle heute gängigen Quantenkryptographie-Protokolle verwenden die Vernam-Chiffre, d. h. eigentlich müsste man genauer von Quanten-Schlüsselverteilung sprechen. Um einen gemeinsamen geheimen Zufallsschlüssels zu erstellen, sendet Alice einzelne Quantenzustände an Bob. Ein Quantenzustand liefert nach einer Messung bei Bob einen Eintrag in den Schlüssel. Die Sicherheit dieser Methode beruht auf dem *No-Cloning-Theorem* der Quantenmechanik. Dieses besagt, dass ein unbekannter Quantenzustand nicht perfekt kopiert werden kann (siehe Infokasten) [2]. Daher ist es unmöglich für Eve, eine Kopie des gesendeten Zustands zu erstellen und zu behalten, den ursprünglichen Zustand an Bob weiterzusenden und dann durch eine eigene Messung zweifelsfreie Information über den Schlüssel zu erhalten.

Es gibt mehrere etablierte quantenkryptographische Protokolle, die im Wesentlichen Variationen der beiden „Klassiker“, des BB84-Protokolls [3] und des Ekert-Protokolls [4], sind. Am Anfang eines jeden Protokolls steht immer die Authentifizierung (d. h. Alice und Bob müssen sich vergewissern, dass sie tatsächlich miteinander kommunizieren, und nicht mit einem Dritten).

Das Protokoll von Bennett und Brassard (BB84)

Im Jahr 1984 entwickelten Charles Bennett und Gilles Brassard das BB84-Protokoll [3] (Abb. 2). Hier wählt Alice einen von vier möglichen Zuständen zufällig aus und sendet ihn zu Bob. Diese vier möglichen Zustände sind $|0\rangle$, $|1\rangle$, $|\bar{0}\rangle = 1/\sqrt{2}\,(|0\rangle + |1\rangle)$ und $|\bar{1}\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle)$. Bei einer experimentellen Realisierung mit einzelnen polarisierten Photonen entsprechen die ersten beiden Zustände vertikaler und horizontaler Polarisation und die letzten beiden einer Polarisation in $\pm 45^0$. Alice und Bob haben vorher vereinbart, dass den Quantenzuständen $|0\rangle$ und $|\bar{0}\rangle$ der klassische Bitwert „0“, und den Zuständen $|1\rangle$ und $|\bar{1}\rangle$ der klassische Bitwert „1“ zugeordnet wird. Bob macht – wiederum zufällig ausgewählt – eine von zwei möglichen Messungen: Entweder orientiert er seinen Analysator so, dass er horizontal und vertikal polarisierte Photonen unterscheiden kann – dies entspricht einer Messung in der Basis $B_1 = \{|0\rangle, |1\rangle\}$ –, oder so, dass er Photonen, die in $\pm 45^0$ polarisiert sind, unterscheiden kann – dies entspricht einer Messung in der Basis $B_2 = \{|\bar{0}\rangle, |\bar{1}\rangle\}$. Danach informieren Alice und Bob einander mittels klassischer Kommunikation (Telefon), welche Basis sie jeweils benutzt haben. Diese Information ist nicht vor dem Spion geschützt. Daher darf Bob keine Angaben über sein Messergebnis machen, sondern nur über die verwendete Basis. Falls beide die Basis B_1 oder beide die Basis B_2 gewählt hatten, behalten sie das klassische Ergebnis, das ja perfekt korreliert ist. Falls sie verschiedene Basen verwendet hatten, ist das Messergebnis nicht für den Schlüssel verwendbar. Für eine Schlüssellänge von N Bits müssen Alice und Bob dieses Verfahren also etwa $2N$-mal durchführen und haben somit einen geheimen Zufallsschlüssel erstellt.

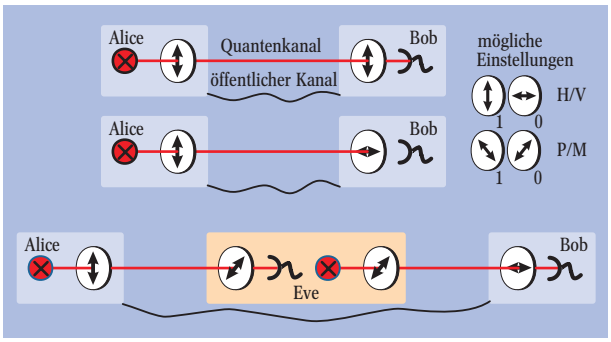

Abb. 2:
Beim Protokoll von Bennett und Brassard (BB84) zum quantenkryptographischen Austausch eines Schlüssels werden vier unterschiedliche Polarisationen der Photonen gewählt (vgl. Text).

Was passiert, wenn ein Spion Information über das Quantensignal erlangen möchte? Die einfachste Möglichkeit für Eve besteht darin, den Zustand auf dem Weg zu Bob abzufangen, ebenfalls entweder in der Basis B_1 oder B_2 zu messen und einen entsprechend dem Messresultat präparierten Zustand weiterzusenden. Falls Eve die gleiche Basis wie Alice gewählt hat, ist sowohl ihr Resultat als auch das von Bob perfekt mit Alices klassischem Bit korreliert. Falls Eve eine andere Basis als Alice benutzt (dies geschieht in der Hälfte der Fälle, also bei N Photonen), sendet sie ein Photon in der falschen Basis zu Bob. Misst dieser in der richtigen Basis (in $N/2$ Fällen), so erhält er mit Wahrscheinlichkeit 1/2 dennoch zufällig den richtigen klassischen Bitwert, andernfalls jedoch den falschen Bitwert. Bei diesem einfachen Lauschangriff werden also ein Viertel der klassischen Einträge in Bobs Schlüssel anders als die bei Alice sein. Dies können die beiden feststellen, indem sie einen Teil des Schlüssels vergleichen – sie können die Anwesenheit von Eve also feststellen. Danach können sie den Schlüssel mittels klassischer Verfahren verbessern: Fehlerkorrektur führt dazu, dass keine fehlerhaften Bits in Bobs String mehr auftauchen, und so genannte Vertraulichkeitsverstärkung (*privacy amplification*) reduziert Eves Information über den Schlüssel. Das Ziel für Alice und Bob in dieser Phase des Protokolls („Schlüsseldestillierung“) ist es, einen gemeinsamen Schlüssel zu erstellen, über den Eve nichts weiß.

Das Protokoll von Ekert

Im Jahr 1991 schlug Artur Ekert eine andere Methode zur Erstellung eines geheimen Zufallsschlüssels vor [4]. Seine wesentliche Idee beruht darauf, verschränkte Zustände für die Schlüsselverteilung zu verwenden. Alice und Bob besitzen jeweils ein Teilsystem des verschränkten Zustands und messen beide in einer von drei möglichen zufällig gewählten Basen. Per Telefon verständigen sie sich wieder, ob sie die gleiche Basis benutzt haben, und behalten in diesem Fall das perfekt korrelierte Ergebnis. Die restlichen Fälle werden für einen Test der Bell-Ungleichung herangezogen: Ist die Bell-Ungleichung nicht verletzt, so ist dies im schlimmsten Fall darauf zurückzuführen, dass ein Spion den Zustand verändert und somit die Verschränkung zwischen Alices und Bobs Zustand zerstört hat. Dann können Alice und Bob nicht davon ausgehen, dass sie tatsächlich einen geheimen Schlüssel besitzen. Die Details des Ekert-Protokolls wurden z. B. in [5]

beschrieben.

Diese beiden Protokolle sind gewissermaßen die Urbeispiele für zwei Klassen von Protokollen: „Präparieren und Messen“ versus „Verschränkungsbasiert“. Man kann jedoch zeigen, dass auch Protokolle der ersten Klasse als solche der zweiten umformuliert werden können.

Weitere Quantenkryptographie-Protokolle

Variationen des BB84-Protokolls bestehen darin, die Zahl der möglichen Zustände zu ändern: Im von C. Bennett vorgeschlagenen B92-Protokoll werden nur zwei nicht-orthogonale Quantenzustände verwendet; im so genannten Sechs-Zustands-Protokoll (*six state protocol*) [6] dagegen die sechs Eigenzustände der drei Pauli-Operatoren. Im letzteren Protokoll sinkt zwar die Effizienz gegenüber BB84, da Alice und Bob nur in einem Drittel der Fälle zufällig die gleiche Basis verwenden, gleichzeitig wird es aber auch schwieriger für Eve, Information zu erlangen, und daher bietet dieses Protokoll erhöhte Sicherheit. Werden anstelle von Zweizustandssystemen (Qubits) Systeme mit höherer Dimension verwendet, führt dies ebenfalls zu erhöhter Sicherheit [7]. Auch für Quantenkryptographie mit kontinuierlichen Variablen gibt es Protokolle, die z. B. auf der Verwendung von kohärenten Zuständen beruhen.

Die bisher beschriebenen Protokolle gehen davon aus, dass z. B. einzelne polarisierte Photonen als Signale verwendet werden. In der Praxis existieren jedoch noch keine perfekten Einzelphotonenquellen. Ein abgeschwächter Laserpuls liefert beispielsweise eine Poisson-Verteilung für Fock-Zustände (Photonzahlzustände), sodass mit gewisser Wahrscheinlichkeit mehr als ein Photon emittiert wird. Diese Situation gibt Eve die Möglichkeit eines gefährlichen Lauschangriffs, der so genannten *photon-number splitting*-Attacke. Hier behält Eve eines der Photonen in einem Mehr-Photonen-Ereignis, und erhält so nach Abwarten der Kommunikation zwischen Alice und Bob die volle Information über das jeweilige Signal.

Sicherheitsanalysen

Angesichts des No-Cloning-Theorems kann Eve keine vollständige Information über den Zufallsschlüssel erhalten. Im Prinzip ist es ihr jedoch durchaus möglich, Teilinformationen zu gewinnen, indem sie am von Alice gesandten Quantenzustand, zusammen mit einem eigenen Zustand, eine Transformation durchführt. Je mehr Information sie erhält, desto größer ist jedoch die Störung, die sie einführt. Dieser Trade-Off beruht auf den Gesetzen der Quantenmechanik und ist daher unumgänglich. Eve kann bestenfalls für eine gegebene Störung ihre Information maximieren. Die zugehörige Transformation ist dann ihr optimaler Lauschangriff. Entscheidend für die praktische Anwendbarkeit der Quantenkryptographie ist es nun, konkrete Angaben darüber zu machen, bis zu welcher Fehlergrenze Alice und Bob in der Lage sind, einen sicheren Schlüssel destillieren zu können. Ob die Fehler tatsächlich von Eve herrühren, wissen die beiden nicht, müssen jedoch im schlimmsten Fall davon ausgehen. Eve wird hier als omnipotent angenommen – insbesondere kann sie alle Quantenoperationen durchführen, darf jedoch nicht die Gesetze der Physik verletzen.

Ein Sicherheitsbeweis für ein bestimmtes Protokoll hängt im Prinzip davon ab, welche Ressourcen Alice und Bob zugestanden werden. P. Shor und J. Preskill [8] zeigten, dass BB84 auch dann „unbedingt“ sicher ist, wenn Alice und Bob nicht im Besitz eines Quantencomputers sind. (Von unbedingter Sicherheit spricht man, wenn Eve auch für einen unendlich langen Schlüssel kein Bit an Information gewinnen kann.) Dieser Beweis der absoluten Sicherheit wurde auch auf den realistischen Fall von imperfekten Quellen und Detektoren ausgeweitet [9]. Kürzlich wurde gezeigt [10], dass eine Vorverarbeitung (*pre-processing*) der Daten die Obergrenze der Fehlerrate für sichere Schlüsselerstellung erhöht: mit Vorverarbeitung liegt sie bei 12,4 % (ohne: 11 %) für BB84, und bei 14,6 % (ohne: 12,6 %) für das Sechs-Zustands-Protokoll.

Experimenteller Status

Für die praktische Umsetzung der Quantenkryptographie eignen sich Lichtquanten bestens. Mittels Glasfasern oder über die direkte Verbindung durch Teleskope lassen sich einzelne Photonen auch über größere Entfernungen übermitteln. Der erste, sichere Quantenschlüssel zwischen Alice und Bob wurde 1991 im Labor des IBM-Forschungszentrums in Yorktown Heights in USA erzeugt [11]. Schwache Laserpulse überquerten die 32 Zentimeter zwischen Sende- und Empfangseinheit (Abb. 1). Die Erfinder der Quantenkryptographie, Charles Bennett und Giles Brassard, zeigten zusammen mit Mitarbeitern, dass Alice und Bob tatsächlich gemeinsam herausfinden können, ob ein Abhörer die Übertragung der Photonen stört oder ob sie einen Schlüssel extrahieren können, den sonst niemand kennt oder auch je nachträglich ermitteln kann. Dieses erste Experiment verwendete eine Leuchtdiode als Lichtquelle und Pockels-Zellen zur schnellen Wahl der Polarisationsrichtungen. Verwendet der Empfänger einen Zwei-Wege-Polarisator (doppelbrechendes Prisma oder dielektrischer, polarisationsabhängiger Spiegel), so genügt hier eine Pockels-Zelle zur Wahl der Analysebasis. In diesem ersten Experiment wurde eine Schlüsselrate von einigen hundert Bit pro Sekunde erreicht (Rohschlüssel, also noch vor Fehlerkorrektur und privacy amplification). Vor allem aber wurde be-

Das No-Cloning-Theorem

Erst 1982 wurde das No-Cloning-Theorem [2] der Quantenmechanik formuliert: „Ein unbekannter Quantenzustand kann nicht perfekt kopiert werden.“ Der Grund dafür ist die Linearität der Quantenmechanik: Nehmen wir an, ein hypothetischer perfekter Quantenkopierer existiere, d. h. es gäbe eine unitäre Zeitentwicklung, unter der aus jedem beliebigen Zustand $|\psi\rangle$ zusammen mit einem gegebenen Anfangszustand $|a\rangle$ eines Hilfszustands (Ancilla) zwei Kopien ebendieses Zustands $|\psi\rangle$ entstehen, d. h. $\mathcal{U}\,|\psi\rangle|a\rangle = |\psi\rangle|\psi\rangle$. Insbesondere müsste dies für die Basiszustände $|0\rangle$ und $|1\rangle$ gelten, also

$$\begin{aligned}\mathcal{U}\,|0\rangle|a\rangle &= |0\rangle|0\rangle,\\ \mathcal{U}\,|1\rangle|a\rangle &= |1\rangle|1\rangle.\end{aligned} \qquad (1)$$

Diese Gleichungen legen aber schon die Entwicklung einer allgemeinen linearen Superposition der Basiszustände, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, mit $|\alpha|^2+|\beta|^2=1$, fest:

$$\begin{aligned}&\mathcal{U}\,(\alpha|0\rangle+\beta|1\rangle)|a\rangle\\ &= \alpha|0\rangle|0\rangle+\beta|1\rangle|1\rangle\\ &\neq |\psi\rangle|\psi\rangle.\end{aligned} \qquad (2)$$

Dies ist ein Widerspruch zu der Annahme, dass ein perfekter Quantenkopierer für jeden Zustand $|\psi\rangle$ existiert und beweist das No-Cloning-Theorem. Eine naheliegende und in der Literatur beantwortete Frage ist die nach der bestmöglichen Güte eines Quantenkopierers. Ein solcher „approximativer“ Quantenkopierer kann von Eve in der Quantenkryptographie eingesetzt werden, um Teilinformation über den Schlüssel zu erhalten. Jedoch führt sie dabei notwendigerweise Fehler in Bobs Signalzustand ein.

reits eine Reihe von unterschiedlichen Abhörattacken simuliert und auch gezeigt, wie sich Fehler und Rauschen korrigieren lassen, ohne die Sicherheit des Schlüssels zu verringern.

Nach diesem ersten Vorbild werden seither weltweit Systeme für den praktischen Einsatz entwickelt. Wichtigste Kriterien dabei sind möglichst hohe Schlüsselraten sowie große Entfernungen. Beides ist meist nicht gleichzeitig möglich – keine Kompromisse hingegen dürfen bei der Zuverlässigkeit und der Benutzerfreundlichkeit eingegangen werden. Diese Anforderungen entsprechen nicht unbedingt der täglichen Arbeit in Quantenoptiklabors. Dort verwendet man üblicherweise separate Halterungen für alle Komponenten wie Spiegel, Linsen und Laserdioden. Dies erlaubt ein sehr flexibles Arbeiten, und die Aufbauten lassen sich für unterschiedliche Experimente optimieren. Allerdings sind diese Aufbauten dadurch relativ groß, typischerweise benötigen Sender und Empfänger eine Fläche von mehr als 50 cm × 50 cm. Durch die große Zahl von Komponenten und Stellvorrichtungen wird der Aufbau auch relativ instabil und temperaturempfindlich. So werden die Experimente immer auf vibrationsisolierten Tischen in möglichst klimatisierten Räumen durchgeführt. Eine große Herausforderung aller Entwicklungen besteht daher darin, die benötigte Optik auf ein Minimum zu reduzieren und für eine hohe Stabilität zu sorgen. Um einfache Nutzung zu gewährleisten, sind auch Hilfsmittel für bzw. eine Automatisierung der Justage notwendig. Die Entwicklung von Quantenkryptographiesystemen wird mehr und mehr eine Aufgabe für Optik-, Elektronik- und Softwarespezialisten – die Quantenphysik bleibt oft außen vor.

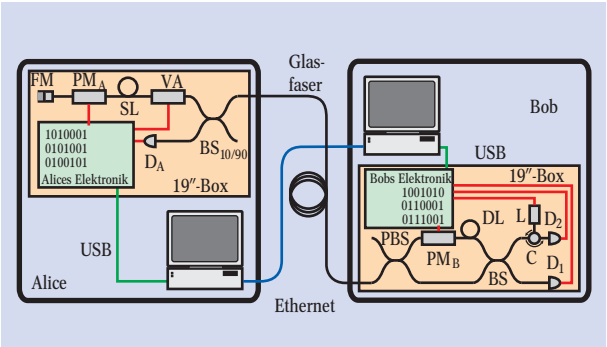

Abb. 3:
In jeweils eine 19-Zoll-Box passen bei diesem System der Universität Genf Sende- und Empfangsmodul. Diese Module haben es ermöglicht, einen Quantenschlüssel zwischen Genf und Lausanne über eine 67 km lange, normale Glasfaser der Swisscom auszutauschen.

Die Länge der Übertragungsstrecke ist derzeit durch die Verluste im Quantenkanal und durch die Effizienz und das Rauschen der Detektoren begrenzt. Verluste entlang der Leitung reduzieren die Zahl der übertragenen Photonen, haben aber auf die Sicherheit der Übertragung keinen Einfluss. Allerdings sinkt bei großen Verlusten der Anteil der Signalereignisse, bis dann durch das Rauschen der Detektoren der Fehleranteil größer als 11 % wird und trotz Fehlerkorrektur kein sicherer Schlüssel mehr erzeugt werden kann. Verstärker im Quantenkanal sind nicht möglich. Entsprechend den Gesetzen der Quantenphysik (No-Cloning-Theorem) kann es nämlich keine fehlerfreien Verstärker für Quantensysteme und Qubits geben. Ein dazwischen geschalteter Verstärker würde das gleiche Rauschen wie ein Abhörer verursachen und daher dessen Erkennung verhindern. Eine Möglichkeit, über sehr große Entfernungen Qubits zu übermitteln, ist der so genannte Quantenrepeater [12]. Durch abwechselnde Quantenfehlerkorrektur und Verbindung von Leitungssegmenten mittels *entanglement swapping* lässt sich so effizient Quanteninformation übermitteln. Dessen Entwicklung wird zwar auch noch einige Jahre dauern, die dafür notwendigen Quantenlogikbausteine sind aber die gleichen, wie sie auch für den Quantencomputer benötigt werden.

Quantenkryptographiesysteme unterscheiden sich im Wesentlichen durch den verwendeten Quantenkanal. Je nachdem, ob Sender und Empfänger über Glasfasern oder Teleskope verbunden sind, unterscheidet man zwei Arten von Systemen. Verfügen Alice und Bob bereits über eine direkte Glasfaserverbindung, so kann hier bei den Standard-Wellenlängen der Telekommunikation (1300 nm bzw. 1550 nm) die beste Transmission erreicht werden. Für Zustandsmanipulation und Analyse eignen sich herkömmliche Telekom-Komponenten. Der hohe Entwicklungsstand dieser Teile ermöglicht eine relativ rasche Entwicklung der Systeme. Zu beachten ist, dass eine spannungsinduzierte Doppelbrechung in der Faser zu fluktuierender Polarisation führt. Dies lässt sich in gewissem Ausmaß kompensieren, allerdings ist dadurch zur Minimierung der Fehlerrate eine geänderte Kodierung der Zustände notwendig. Das Zwei-Zustands-System ist hier durch zwei zueinander kohärente, zeitlich versetzter Feldamplituden gegeben, unterschiedliche, relative Phasen zwischen den Komponenten definieren die nichtorthogonalen Zustände des gesendeten Qubits.

Nachteile dieses Wellenlängenbereichs sind das hohe Rauschen und die relativ geringe Effizienz der für diese Wellenlängen besten Einzelphotondetektoren (Ga- bzw. InGaAs-Avalanchedioden). Die Optimierung dieser Detektoren hat in den letzten Jahren immer neue Entfernungsrekorde ermöglicht (leider bei sehr kleinen Schlüsselraten von ca. 10 bit/s). Derzeit liegt das Team von Andrew Shields (Toshiba, England) mit 122 km wieder vor den Konkurrenten von NEC und Mitsubishi. Neue Detektorentwicklungen lassen auf noch deutlich größere Entfernungen hoffen, 200 km sollten in den nächsten Jahren möglich sein.

Quantenkryptographie über Glasfasern...

Ein besonders stabiles, zuverlässiges System wurde an der Universität Genf entwickelt. Dazu hat die Gruppe von Nicolas Gisin und Hugo Zbinden das Prinzip der Quantenkryptographie trickreich erweitert, um eine sehr hohe Präzision und Güte der Schlüsselerzeugung zu erreichen. Störungen entlang der Glasfaserleitung werden dadurch kompensiert, dass der Empfänger, Bob, mittels eines halben Mach-Zehnder-Interferometers zuerst kohärente, helle Lichtpulse erzeugt und zu Alice schickt. Sie schwächt die Pulse ab, moduliert die Phase und reflektiert sie mittels eines Faraday-Spiegels zurück zu Bob. Da spannungsinduzierte Doppelbrechung nur auf einer Zeitskala von Sekunden

fluktuiert, wird dieser Effekt auf dem Rückweg kompensiert. Auch die Phase des Mach-Zehnder-Teiles ist auf dem Rückweg noch die gleiche und hebt sich somit, abgesehen von Bobs erst auf dem Rückweg aktivierter Modulation, wieder auf. Nur die kontrollierten Phasenmodulationen von Alice und Bob bleiben übrig und bestimmen das Resultat der Messung – nun praktisch unempfindlich gegen Drifts und Schwankungen.

Abb. 4:
Zwei Firmen bieten bereits erste kommerzielle Netzwerkkomponenten an, die neben den herkömmlichen Kommunikationsaufgaben auch den sicheren Schlüsselaustausch mittels Quantenkryptographie beherrschen (Fotos: www.idquantique.com, www.magiq-tech.com).

Damit gelang es Alice, einen sicheren Schlüssel von Genf nach Lausanne, wo Bob seinen Apparat an die Glasfaserleitung angeschlossen hatte, zu übermitteln (Übertragungsrate ca. 130 bit/s, Abb. 3) [13]. Die Entfernung betrug hier zwar „nur“ 67 km, allerdings über eine normale Glasfaser der Swisscom. Sender und Empfangsmodule waren in 19-Zoll-Boxen untergebracht und in den Swisscom-Gebäuden aufgestellt, nicht in klimatisierten Labors. Diese zuverlässigen Systeme waren auch die ersten kommerziell erhältlichen Quantenkryptographieprodukte. Die spin-off-Firma idQuantique stellt mittlerweile mit Vectis eine sichere Punkt-zu-Punkt-Verbindung zur Verfügung, die direkt in bestehende Netzwerke eingebunden werden kann. Diesen wichtigen Schritt von einem Produkt für Physiker hin zu einem Produkt für Netzwerkbetreiber ging auch die zur Zeit zweite Firma. MagiQ, USA, bietet mit QPN einen Router an, dessen Sicherheit durch die Quantenkryptographie gewährleistet wird (Abb. 4).

... und durch die Luft

Steht eine direkte Sichtverbindung zur Verfügung, so lässt sich die Verbindung zwischen Alice und Bob mithilfe von Teleskopen und optischem Richtfunk herstellen. Sehr gut transmittiert die Atmosphäre z. B. im Bereich von 800 nm bis 850 nm, in dem auch sehr effiziente, rauscharme Si-Avalanchedioden zur Einzelphotondetektion zur Verfügung stehen. Alle Komponenten, insbesondere auch die Laserdioden, sind bei diesen Wellenlängen sehr kostengünstig. Da die Polarisationsmodulatoren sehr aufwändig und teuer sind, bietet es sich hier sogar an, für jede Polarisationsrichtung eine geeignet orientierte Diode vorzusehen und zur Zustandspräparation immer nur eine der Dioden zu aktivieren. Probleme entstehen für den optischen Richtfunk vor allem durch Luftturbulenzen, die die effektive Apertur der Teleskope stark reduzieren. Zur effizienten Kopplung über große Entfernungen sind daher relativ große Empfängerteleskope notwendig.

Abb. 5 zeigt das Schema neuer Sende- und Empfängermodule, wie wir sie für eine Demonstration über 23,4 km an der Universität München entwickeln und zusammen mit Mitarbeitern der englischen Firma QinetiQ erfolgreich testen konnten [14]. Im Sender wurden vier Laserdioden derart auf einem Ring montiert, dass die Polarisation des über einen kegelförmigen Spiegel reflektierten Lichts bereits in den vier unterschiedlichen Richtungen orientiert war. Die gesamte Optik des Empfängermoduls passt ebenfalls sehr kompakt auf eine Fläche von 5 cm × 5 cm. Speziell angefertigte Halter sorgen für die gewünschte Stabilität. Diese beiden Module eignen sich auch bestens zur Montage an Teleskope, wie sie zur Übermittlung der Photonen benötigt werden.

Um die Leistungsfähigkeit der Module und ihre Eignung für zukünftige Anwendungen zu testen, wollten wir eine möglichst große Entfernung durch die Teleskopverbindung überbrücken. Für eine klare Sicht und ruhige Luft bauten wir die Teststrecke zwischen der Zugspitze und der westlichen Karwendelspitze an der Grenze zwischen Deutschland und Österreich auf (Abb. 5). Trotz der recht unwirtlichen äußeren Bedingungen, wie Temperaturen von –20 °C und Wind, gelang es, abhörsicher Schlüssel auszutauschen (Übertragungsrate ca. 1000 bit/s). Derzeit laufen erste Tests für eine Kopplung über 140 km. Unser Team mit Mitarbeitern der Universitäten Bristol, München, Padua, Wien, des Max-Planck-Instituts für Quantenoptik und den Firmen Carlo Gavazzi Space, Contraves Space AG, Schweiz, Italien, und TESAT, Deutschland, sowie der ESA versucht hierbei zu zeigen, dass Quantenkryptographie über eine Distanz möglich ist, die der Entfernung zu erdnahen Satelliten nahekommt.

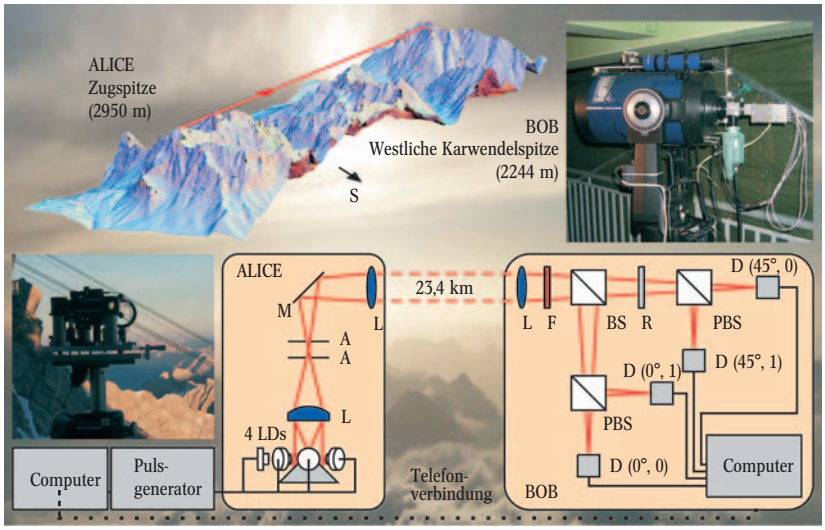

Abb. 5:
Dieses System erlaubte den Austausch eines Quantenschlüssels zwischen der Zugspitze und der 23,4 km entfernten westlichen Karwendelspitze. Das rechte Foto zeigt Bobs Spiegelteleskop mit dem Empfangsmodul, während Alices Sendemodul (links) direkt in ein Galilei-Teleskop integriert ist.

Damit sind nun zwei Einsatzgebiete denkbar: Einerseits können Verbindungen zwischen Gebäuden innerhalb einer Stadt aufgebaut werden. Zwischen den Gebäuden einer Firma oder einer Bank oder vom Anwender zum nächstgelegenen Glasfaserverteiler lässt sich dann beispielsweise die Kommunikation abhörsicher durchführen. Andererseits ermöglicht die direkte Kopplung zwischen Teleskopen aber auch den Schlüsselaustausch zu Satelliten. Dabei würde man die Sendeeinheit im Satelliten einbauen. Aus ca. 500 bis 1000 km Höhe

könnte das Senderteleskop im Überflug eine Bodenstation anvisieren und entsprechend polarisierte Lichtpulse senden. Die gesamte Luftschicht streut bei klarer Sicht nur etwa die Hälfte aller Photonen und verursacht so nur eine kleine Reduzierung der Übertragungsrate. Der einzige Pferdefuß dieses Verfahrens: Voraussetzung ist ein wolkenloser Himmel, sodass die Photonen auch wirklich zur Bodenstation gelangen. Überfliegt der Satellit später eine zweite Bodenstation, kann auch mit dieser ein Schlüssel ausgetauscht werden. Aus den beiden Einzelschlüsseln lässt sich ein geheimer Schlüssel zwischen den beiden Bodenstationen ermitteln, wodurch praktisch alle Entfernungsschranken fallen.

Während unsere Demonstrationen nur nachts durchgeführt werden, gelang es der Gruppe um Richard Hughes, Los Alamos, bereits, auch Freiraum-Quantenkryptographie bei Tageslicht zu demonstrieren. Wichtig dafür sind eine enge Filterung sowohl in der Zeit, der Wellenlänge als auch im Raumwinkel, der vom Empfänger „gesehen“ wird. Über eine Entfernung von ca. 10 m gelang es hiermit auch tagsüber, sichere Schlüssel auszutauschen. Ein extrem schnelles System wurde am NIST in Gaithersburg unter Leitung von Carl Williams und Allan Migdal aufgebaut. Hochintegrierte Elektronik ermöglichte über 400 m Pulsraten von 125 MHz, mit Schlüsselraten von mehr als 1 MHz.

Ausblick und neue Ansätze

Außer den oben beschriebenen Protokollen wurden in den letzten Jahren etliche Erweiterungen und neue Ansätze zu Quanten-Kryptographie-Protokollen entwickelt. Hier seien zwei Ideen erwähnt, die das Problem der *photon-number splitting*-Attacke von Eve lösen. Im so genannten *decoy state*-Protokoll [15] sendet Alice zusätzlich zu den Signalpulsen „Köder“-Pulse zu Bob. Die Köderpulse unterscheiden sich nur in der Photonzahl-Verteilung, nicht aber in der Wellenlänge oder anderen physikalischen Größen von den Signalpulsen. Durch Vergleich der Bitrate und Fehlerrate der Köderpulse können Alice und Bob eine bessere Performance des Protokolls und unbedingte Sicherheit erzielen. – Im kürzlich von Scarani und Mitarbeitern [16] vorgeschlagenen Protokoll führen Alice und Bob eine nachträgliche Selektion der Ereignisse durch, indem Alice nicht die Basis, sondern eine aus zwei nicht-orthogonalen Zuständen bestehende Menge ankündigt. Dies verschafft Alice und Bob einen Vorteil gegenüber Eve. Auch verbesserte Quellen für Einzelphotonen und (verschränkte) Photonenpaare könnten in Zukunft das Problem der *number-splitting*-Attacke lösen.

Welches der beschriebenen Protokolle sich schließlich in der Anwendung durchsetzen wird, kann sich erst nach experimentellen Tests und weiteren theoretischen Sicherheitsanalysen herausstellen. Derzeit werden dazu einerseits unterstützt durch die DARPA in Boston und andererseits innerhalb des EU-Projekts SECOQC in Wien Demonstratoren für langreichweitige und sichere Kommunikations-Netzwerke aufgebaut.[2)]

Der Wettkampf um sichere Kommunikation ist mit den Mitteln der Physik gewonnen. Ein geheimer Schlüssel kann über große Entfernungen übertragen werden und zur abhörsicheren Nachrichtenübermittlung verwendet werden. Erste Systeme sind bereits kommerziell erhältlich. Quanteneffekte sind nicht länger nur in den klimatisierten Labors weniger Universitäten und Forschungsinstitute beobachtbar, sondern können bald von jedermann genutzt werden, um vertrauliche Botschaften sicher zu senden.

2) Weitere Informationen unter *www.secoqc.net*

Literatur

[1] *S. Singh*, Geheime Botschaften, Deutscher Taschenbuch Verlag, München (2001)
[2] *W. Wootters* und *W. Zurek*, Nature **299**, 802 (1982)
[3] *C. Bennett* und *G. Brassard*, Proc. IEEE Int. Conf., 175 (1984)
[4] *A. Ekert*, Phys. Rev. Lett. **67**, 661 (1991)
[5] *W. Tittel* et al., Physikal. Blätter, Juni 1999, S. 25
[6] *D. Bruß*, Phys. Rev. Lett. **81**, 3018 (1998); *H. Bechmann-Pasquinucci* und *N. Gisin*, Phys. Rev. A **59**, 4238 (1999)
[7] *D. Bruß* und *C. Macchiavello*, Phys. Rev. Lett. **88**, 127901 (2002)
[8] *P. Shor* und *J. Preskill*, Phys. Rev. Lett. **85**, 441 (2000)
[9] *D. Gottesman, H.-K. Lo, N. Lütkenhaus* und *J. Preskill*, Quant. Inf. Comp. **4**, 325 (2004)
[10] *R. Renner, N. Gisin* und *B. Kraus*, quant-ph/0502064
[11] *C. H. Bennett, F. Bessette, G. Brassard, L. Salvail* und *J. Smolin*, J. Cryptology **5**, 3 (1992)
[12] *W. Dür, H.-J. Briegel, T. I. Cirac* und *P. Zoller*, Phys. Rev. A **59**, 169 (1999)
[13] *N. Gisin, G. Ribordy, W. Tittel* und *H. Zbinden*, Rev. Mod. Phys. **74**, 145 (2002)
[14] *Ch. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. Gorman, P. R. Tapster* und *J. G. Rarity*, Nature, **419**, 450 (2002)
[15] *H.-K. Lo, X. Ma* und *K. Chen*, Phys. Rev. Lett. **94**, 230504 (2005)
[16] *V. Scarani et al.*, Phys. Rev. Lett. **92**, 057901 (2004)

Die Autoren

Nach dem Physikstudium an der RWTH Aachen unternahm **Dagmar Bruß** einen Abstecher in die Astronomie (MSc an der U Edinburgh), bevor sie 1994 in theoretischer Teilchenphysik an der Uni Heidelberg promovierte. Als Postdoc in Oxford lernte sie Artur Ekert kennen, einen der Mitbegründer der Quanteninformationstheorie. Sie wechselte 1997 in dieses junge Forschungsgebiet und ging 1999 als Assistentin an die Uni Hannover, wo sie sich 2002 habilitierte. Seit 2004 leitet Bruß den Lehrstuhl für Theoretische Physik III an der Uni Düsseldorf. In ihrer Freizeit singt sie im Bachverein Düsseldorf und erkundet die Bräuche des Rheinlands.

Harald Weinfurter studierte an der TU Wien Technische Physik, wo er auch promovierte. An der Uni Innsbruck habilitierte er sich 1996 bei Anton Zeilinger. Seit 1999 ist er Professor für Quantenoptik an der LMU München. Für seine Arbeiten zur Quantenkrytographie erhielt er 2003 den Philip-Morris-Forschungspreis.