Christian Kurtsiefer und Harald Weinfurter

Mit Photonen zum Schlüssel

Quantenphysik garantiert erstmals abhörsichere Kommunikation

Wie versende ich Nachrichten, ohne dass ein Abhörer deren Inhalt erfahren kann ? Nach zahlreichen Versuchen mittels komplizierter Maschinen oder Mathematik die Nachricht zu schützen ermöglichen die Grundgesetze der Quantenphysik erstmals Abhörversuche zu entdecken. Aber können diese Ideen auch in der Praxis eingesetzt werden ?

Seitdem Menschen Nachrichten austauschen, versuchen Sie auch, diese Botschaften vertraulich zu übermitteln. Und wohl ebenso lange versuchen wiederum Dritte, diese geheime Mitteilung zu entschlüsseln. Doch nun scheint es, dass die Codemacher den Jahrtausende langen Wettkampf gegen die Codebrecher für sich entscheiden können. Zusammen mit dem one-time pad ermöglicht die Quantenkryptographie erstmals abhörsichere Kommunikation. Ohne „wenn und aber“, nur auf den Gesetzen der modernen Physik aufbauend, kann erstmals jeder denkbare Abhörversuch entdeckt werden, bevor kritische Information übermittelt wird.

Die klassische Kryptographie stellt dem Benutzer eine Fülle von Methoden zur Verschlüsselung und Entschlüsselung geheimer Nachrichten zur Verfügung (siehe Einsichten 2/2002). Zumeist beruht die Sicherheit auf der Komplexität des Verschlüsselungsmechanismusses (Enigma) oder auf der mathematischen Schwierigkeit, aus einem bekannten Schlüsselteil den vollständigen Schlüssel zu ermitteln (RSA). Dabei verläßt man sich notwendigerweise immer auf Annahmen über die Fähigkeit oder besser Unfähigkeit des Abhörers. „Bekannte Technologie und Algorithmen“ werden meist als Maßstab für die Sicherheit einer Nachrichtenübertragung verwendet. Aber kenne ich immer den Stand der Technik? Und wie lange wird es dauern, bis neue, bessere Verfahren entwickelt werden?

Das neue Gebiet der Quanteninformatik zeigt, wie grundlegende Quanteneffekte in neuartigen Methoden der Informationsverarbeitung und -übermittlung genutzt werden können. Neben der Quantenkryptographie ist hier besonders der Quantencomputer zu erwähnen, für den leistungsfähigere und schnellere Rechenalgorithmen vorgeschlagen wurden, als sie für herkömmliche Computer möglich sind (siehe Einsichten 2/2000). Sollte es in einigen Jahren gelingen, große Quantencomputer zu bauen, werden sie im Moment schier unlösbare Aufgaben, wie die für die Entschlüsselung des RSA-Codes notwendige Primzahlzerlegung großer Zahlen, durchführen. Es ist eine gewisse Ironie: Auf der einen Seite sind durch den Einsatz der Quantenphysik heute gebräuchliche Verschlüsselungsverfahren mit einem Schlag angreifbar und damit nutzlos. Auf der anderen Seite stellt die Quantenkryptographie neue Möglichkeiten zur Nachrichtenübermittlung bereit, deren Sicherheit aber nun nicht mehr durch mathematische Annahmen, sondern durch physikalische Gesetze gewährleistet wird.

Die Leistungsfähigkeit der neuen Quanteninformationsverfahren beruht auf einer Erweiterung der herkömmlichen digitalen Kodierung von Information. Üblicherweise wird die Grundeinheit der Information, das Bit, durch die Werte „0“ und „1“ dargestellt. Der physikalische Träger der Information ist der jeweiligen technischen Realisierung angepaßt, meist kommt Strom, Spannung oder Licht zum Einsatz. Zum Beispiel wird in Mikrochips ein Spannungspegel von 0 Volt für logisch „0“ und ein Pegel von 5 Volt für „1“ verwendet, oder bei der Informationsübertragung mittels Glasfaserleitungen wird kein Licht für „0“ und ein kurzer Lichtpuls für „1“ gesendet.

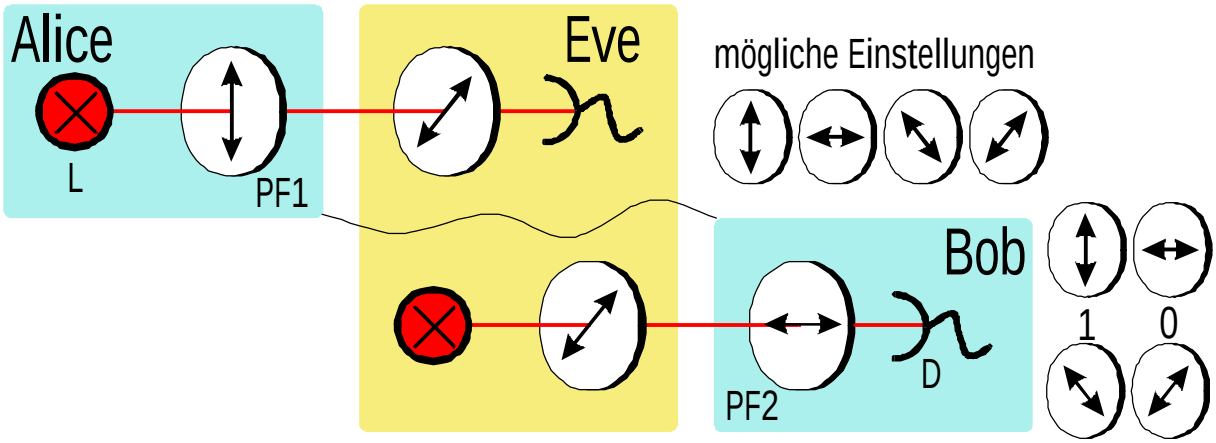

Abb 1. Schema einer Verbindung zur Quantenkryptographie. Alice erzeugt mittels der Lichtquelle (L) einzelne Photonen und definiert deren Polarisation durch ein Filter (PF1). Wenn Sie diese an Bob schickt, wird dessen Detektor (D) kein Photone registrieren, wenn sein Polaraisationsfilter (PF2) senkrecht auf das erste steht. Unterbricht aber ein Abhörer die Leitung und versucht durch Messung die eingestellte Polarisationsrichtung zu bestimmen, verursacht er den Gesetzen der Physik entsprechend Fehler. Während in der klassischen Physik jede Messung mit beliebiger Präzision durchgeführt werden kann, ohne das gemessene Objekt zu stören, wird ein Quantenzustand durch eine Messung neu definiert. Bob wird bei einem derartigen Angriff im Mittel ein Viertel der Photonen mit der falschen Orientierung detektieren. Dies erlaubt es Alice und Bob die Attacke zu erkennen, bevor geheime Nachrichten übermittelt werden.

Die Quanteninformatik verwendet als Träger der Information Quantenobjekte. Gibt es für eine bestimmte Eigenschaft zwei unterscheidbare Einstellungen, können diese zur Darstellung von „0“ und „1“ verwendet werden. Mögliche Systeme sind zum Beispiel lineare Polarisation eines Lichtquants, des sogenannten Photons, mit den Einstellungen H (horizontal) und V (vertikal) für „0“ und „1“, oder Grund- und angeregter Zustand eines Atoms.

Während aber für ein klassisches Bit lediglich die zwei Möglichkeiten „0“ und „1“ erlaubt sind, kann das Quantensystem jeden Zustand annehmen, der sich aus einer Überlagerung (Superposition) der Komponenten des ersten Richtungspaares (H/V) ergibt. So können wir die Polarisation des Photons auch unter +45° oder -45° einstellen. Um auf die erweiterten Eigenschaften dieser neuen Informationsträger hinzuweisen wird die darauf codierte Information als Qubit bezeichnet. Entsprechend der Heisenbergschen Unschärferelation ist es aber unmöglich ein Qubit, also zum Beispiel die Polarisation eines einzelnen Photons, gleichzeitig unter H/V und unter +45°/-45° zu bestimmen. Diese quantenmechanische Ungewißheit macht erfolgreiche Abhörversuche unmöglich.

Ein Abhörer, der die Quanteneigenschaften der einzelnen Photonen zu bestimmen versucht, wird unweigerlich Fehler und Rauschen verursachen und damit von Sender (Alice) und Empfänger (Bob) entdeckt. Alice und Bob werden daher die Methode der Quantenkryptographie zur Erzeugung einer geheimen, zufälligen Folge von bits, dem Schlüssel, verwenden. Erst wenn die Sicherheit der Übertragung zweifelsfrei feststeht, wird mit diesem Schlüssel die Nachricht bit für bit codiert und übertragen. Wenn der Schlüssel gleich lang wie die zu übertragende Nachricht ist und aus einer zufälligen Folge von Schlüsselbuchstaben besteht, so gibt es keine Möglichkeit mehr, von der Chiffre auf die geheime Nachricht zu schließen (one-time-pad-Code). Nur die (legitimen) Besitzer des Schlüssels können die Botschaft lesen.

Zur sicheren Schlüsselerzeugung und -übertragung sind Alice und Bob durch einen sogenannten Quantenkanal zur Übermittlung der Photonen und durch eine herkömmliche Kommunikationsverbindung, z. B. Telefon oder Funk, verbunden. Über den Quantenkanal sendet Alice Qubits, zum Beispiel die zuvor erwähnten polarisierten Photonen, zu Bob.

Zufällig wählt sie für jedes Photon eine von vier Möglichkeiten, entweder H, V, +45° oder -45° für die Polarisationsrichtung. Bob schaltet seinen Polarisationsanalysator ebenfalls zufällig zwischen dem H/V-Richtungspaar und dem +45°/-45°-Paar und teilt Alice mit, wann und unter welcher Einstellung er ein Photon gemessen hat (nicht aber, welches Resultat er erhalten hat). Alice überprüft in ihrer Liste die Detektionszeitpunkte und teilt ihrerseits Bob mit, wann sie beide das gleiche Richtungspaar verwendeten.

Da ein von Alice z. B. als horizontal polarisiert gesendetes Photon im H/V-Analysator nur im H-Ausgang detektiert werden kann, besteht für den Fall, dass beide die gleiche Einstellung verwendeten, eine eindeutige Beziehung zwischen dem von Alice eingestellten Wert und dem von Bob detektierten. Sie können daher diese Bitfolge als Schlüssel verwenden.

Wie können Alice und Bob nun auch sicher sein, dass dieser Vorgang nicht abgehört wurde? Ein Abhörvorgang bei der Quantenübertragung entspricht einer Messung, bei der der Abhörer versucht, die Polarisation des von Alice gesendeten Photons zu detektieren und ein entsprechend polarisiertes an Bob weiterzuschicken. Ist der Meßapparat des Abhörers gleich orientiert wie die Sendeeinrichtung von Alice, so wird er das richtige Bit beobachten und es entsprechend an Bob weiterschicken. Ist dieser Apparat aber in der anderen Basis orientiert, so wird mit 50 % Wahrscheinlichkeit ein falscher Bitwert beobachtet und an Bob gesendet, der seinerseits dann wieder mit 50% Wahrscheinlichkeit ein falsches Bit detektieren wird (Abb. 1). Während ein Angriff auf die Übertragung klassischer Signale immer so durchgeführt werden kann, dass er von Sender und Empfänger nicht bemerkt wird, verursacht ein Abhören der Qubits unweigerlich Fehler im Schlüssel! Durch Vergleich einiger weniger Bits des Schlüssels können Alice und Bob daher sofort feststellen, ob die Schlüsselübertragung sicher und ungestört durchgeführt wurde. Der so erhaltene Schlüssel kann ideal zur one-time-pad-Chiffrierung verwendet werden und garantiert damit erstmals wirklich sichere Kommunikation.

Für die praktische Umsetzung eignen sich die Lichtquanten bestens. Mittels Glasfasern oder über die direkte Verbindung durch Teleskope können die einzelnen Photonen auch über größere Entfernungen übermittelt werden. Der erste, sichere Quantenschlüssel zwischen Alice und Bob wurde 1991 im Labor des IBM-Forschungszentrum in Yorktown Heights in USA erzeugt. Schwache Laserpulse überquerten die 32 Zentimeter zwischen Sende- und Empfangseinheit. Die Erfinder der Quantenkryptographie, Charles Bennett und Giles Brassard, zeigten, dass Alice und Bob gemeinsam herausfinden können, ob ein Abhörer die Übertragung der Photonen störte oder ob sie einen Schlüssel extrahieren können, den sonst niemand kennt oder auch je nachträglich ermitteln kann.

Verluste entlang der Leitung reduzieren die Zahl der übertragenen Photonen, haben aber auf die Sicherheit der Übertragung keinen Einfluß. Allerdings ist die Länge der Übertragungsstrecke derzeit noch durch die Verluste begrenzt. Entsprechend den Gesetzen der Quantenphysik kann es nämlich keine fehlerfreien Verstärker für Quantensysteme und Qubits geben. Ein dazwischen geschalteter Verstärker oder Repeater würde das gleiche Rauschen wie ein Abhörer verursachen und daher dessen Erkennung verhindern. Rauschen der Detektoren führt außerdem zu einer kleinen Zahl von Fehlern im Schlüssel von Alice und Bob. Zwar können sichere Verfahren zur Korrektur verwendet werden, allerdings muß dabei auch ein Teil des Schlüsselmaterials geopfert werden. Der Anteil des Rauschens darf daher nicht vergleichbar mit dem durch einen möglichen Abhörangriff verursachten Fehler werden, da sonst bei der Korrektur alles Material aufgebraucht wird. Eine Möglichkeit, über sehr große Entfernungen Qubits zu übermitteln ist der sogenannte Quantenrepeater. 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. Wie wir sehen werden, kann aber auch existierende Technologie für einen globalen Schlüsselaustausch genutzt werden.

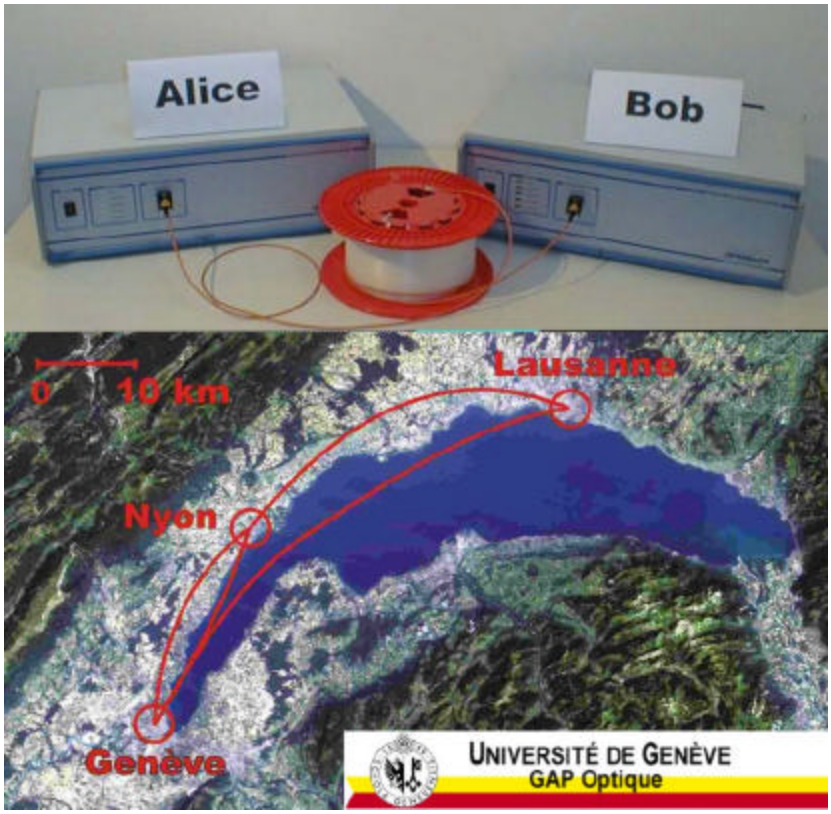

Abb. 2. Quantenkryptographie über eine Glasfaserverbindung zwischen Genf und Lausanne. Die Glasfaser wird an die beiden Kästchen angeschlossen in denen die Optikkomponenten für Sender und Empfänger montiert sind.

Nach dem ersten Vorbild von Bennett und Brassard werden derzeit weltweit Systeme für den praktischen Einsatz entwickelt. Je nachdem, ob Glasfaser oder Teleskope zur Verbindung von Sender und Empfänger benutzt werden können, wurden zwei Arten von Systemen konstruiert. Verfügen Alice und Bob bereits über eine direkte Glasfaserverbindung, so können sie am besten die Geräte der Universität Genf verwenden. Dabei wurde das Prinzip der Quantenkryptographie in der Gruppe von Nicolas Gisin und Hugo Zbinden trickreich erweitert, um eine sehr hohe Präzision und Güte der Schlüsselerzeugung zu erreichen. Störungen entlang der Glasfaserleitung werden kompensiert, wodurch die Übertragungslänge bis auf derzeit 67 Kilometer gesteigert werden konnte (Abb. 2). Damit konnte Alice von Genf nach Lausanne, wo Bob seinen Apparat an die Glasfaserleitung angeschlossen hatte, einen sicheren Schlüssel übermitteln. Diese Geräte arbeiten zuverlässig und können einfach an Computer angeschlossen werden. Diese kontrollieren den Ablauf der Schlüsselübertragung und können natürlich auch für die Übermittlung der geheimen Nachricht eingesetzt werden.

Steht keine direkte Glasfaserverbindung zur Verfügung, so kann die direkte Kopplung durch Teleskope eingesetzt werden. Die erforderlichen Komponenten für eine derartige optische Richtfunkstrecke konnten wir in unserer Gruppe an der Universität München entwickeln und zusammen mit Mitarbeitern der englischen Firma QinetiQ erfolgreich testen.

Für die tägliche Arbeit stehen in Quantenopiklabors verwendet man üblicherweise separate Halterungen für alle Komponenten wie Spiegel, Linsen und Laserdioden. Dies erlaubt ein sehr flexibles Arbeiten und die Aufbauten können den unterschiedlichen Anforderungen angepasst werden. Allerdings sind diese Aufbauten dadurch relativ groß. Typische Aufbauten zur Quantenkryptographie benötigen ein Fläche von mehr als 50 cm x 50 cm. Durch die Unzahl 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.

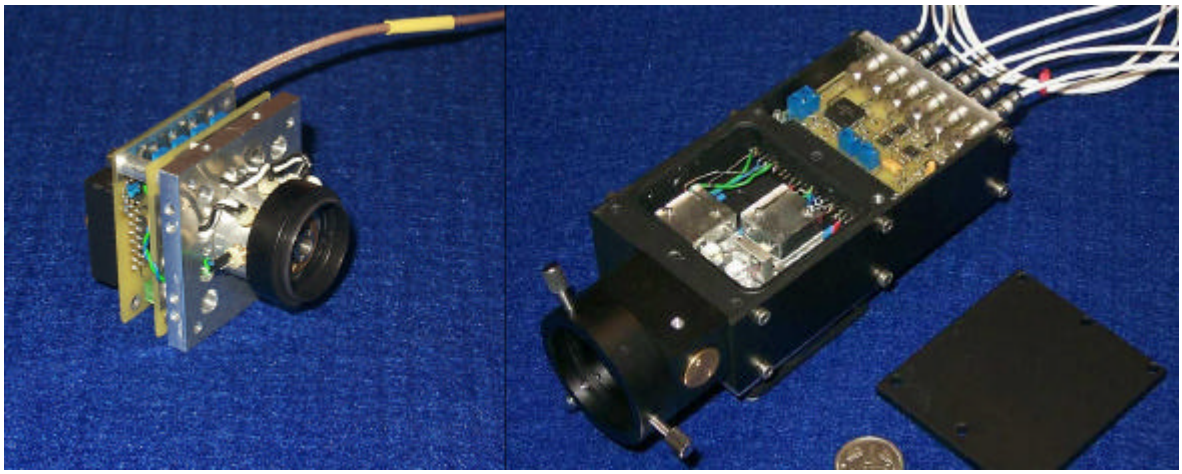

Abb. 3. Sender- und Empfängermodule zur Quantenkryptographie über Teleskopverbindungen.

Eine große Herausforderung unserer Entwicklungen war es daher, die benötigte Optik auf ein Minimum zu reduzieren und für eine hohe Stabilität zu sorgen. Abb. 3 zeigt die Sende- und Empfängermodule. 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. Abhängig welche der vier Dioden durch einen kurzen Strompuls eingeschaltet wird, wird eine der erforderlichen Codierungen durchgeführt. Die gesamte Optik des Empfängermoduls konnte ebenfalls sehr kompakt auf einer Fläche von 5 cm x 5 cm montiert werden. 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. 4). Trotz der recht unwirtlichen äußeren Bedingungen, wie Temperaturen von -20 Grad und Wind konnten über die Distanz von 23 km abhörsicher Schlüssel ausgetauscht werden. Damit sind nun zwei Einsatzgebiete denkbar: Einerseits können Verbindungen zwischen Gebäuden innerhalb einer Stadt aufgebaut werden. Zum Beispiel zwischen den Gebäuden einer Firma oder einer Bank oder vom Anwender zum nächstgelegenen Glasfaserverteiler kann dann die Kommunikation abhörsicher übermittelt werden. Da in den von uns entwickelten Modulen nur Laserdioden ähnlich denen in CD-Spielern zum Einsatz kommen und wir auch die notwendige Optik auf ein Minimum reduzieren konnten, sollten diese Verbindungen auch eines Tages sehr kostengünstig herzustellen sein.

Andererseits ermöglicht die direkte Kopplung zwischen Teleskopen aber auch den Schlüsselaustausch zu Satelliten. Dabei würde man die Sendeeinheit im Satelliten einbauen. Aus ca. 500--1000 km Höhe visiert das Senderteleskop im Überflug eine Bodenstation an und sendet entsprechend polarisierte Lichtpulse. 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 kann ein geheimer Schlüssel zwischen den beiden Bodenstationen ermittelt werden, wodurch praktisch alle Entfernungsschranken fallen.

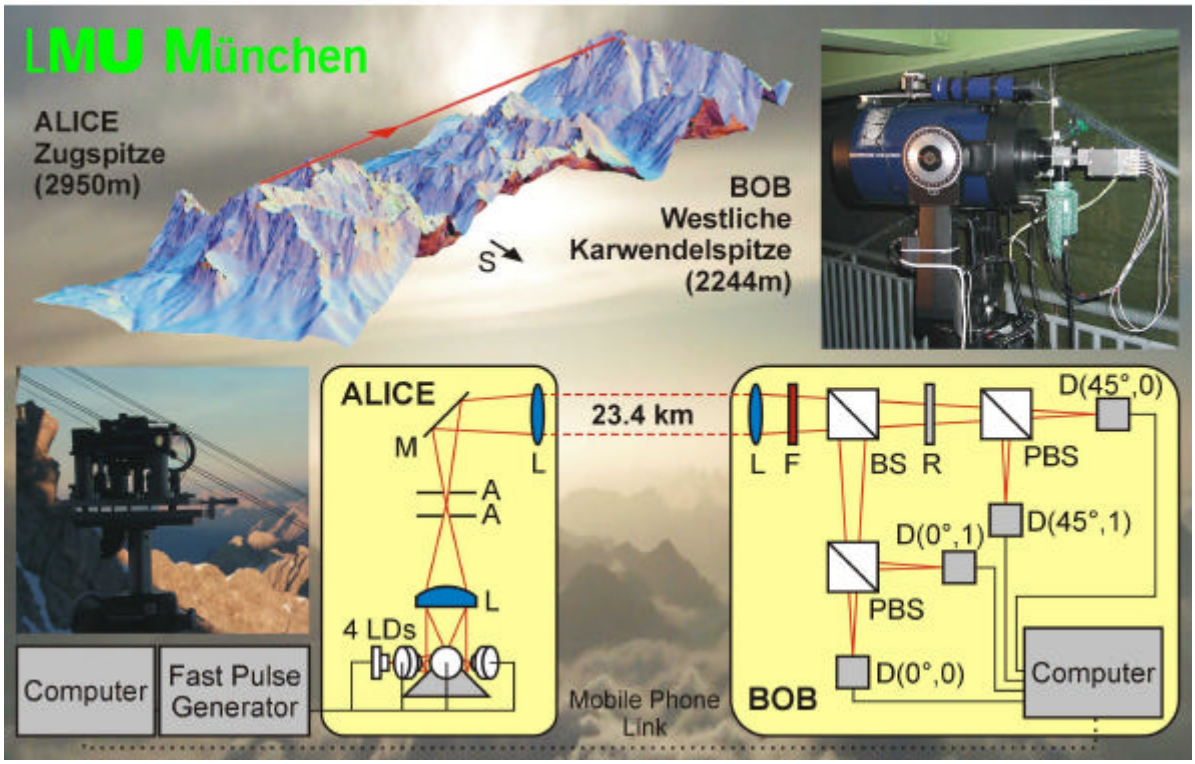

Abb. 4. Test über 23.4 km zwischen Zugspitze und westl. Karwendelspitze. Das rechte Fotoinsert zeigt Bobs Spiegelteleskop mit dem Empfangsmodul, während Alices Sendemodul direkt in einem Galilei-Teleskop integriert ist.

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. Ein erstes System wird bereits kommerziell angeboten, andere Firmen haben für 2003 weitere Produkte angekündigt. 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.

Literatur:

A step towards global key distribution, Ch. Kurtsiefer, P. Zarda, M. Halder; H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity: Nature 419, 450 (2002).

Quantum Cryptography, Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden, Reviews of Modern Physics, Vol 74, 145 (2002).

Quantenkryptographie, C.H. Bennett, G. Brassard, A.K. Ekert, Sektrum der Wissenschaften, Dezember 1992.