Quantenoptik

Quantenkryptographie

Die eigentümliche Natur der Quantenmechanik läßt sich für die Übertragung geheimer Nachrichten ausnutzen

Wolfgang Tittel, Jürgen Brendel, Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden

Obwohl die Quantenmechanik sämtliche Gebiete der modernen Physik durchzieht, stoßen wir immer wieder auf Probleme, wenn wir ihre Vorhersagen mit unserer klassischen Anschauung zu verstehen versuchen. Seit einigen Jahren geht der Trend dahin, die seltsam anmutenden Eigenheiten der Quantenwelt – Nichtlokalität, Superpositionsprinzip, Unschärferelation – auszunutzen, um Dinge zu realisieren, die innerhalb der klassischen Physik unmöglich sind. Die Quanten-Informationsverarbeitung, auch Quantenkommunikation genannt, ist aus diesem Ansatz hervorgegangen; erste Demonstrationsexperimente zum Quantencomputer sowie Quantenkryptographie-Prototypen haben gezeigt, welches Potential diese Entwicklung birgt [1, 2]. In diesem Artikel verdeutlichen wir, wie die Grundprinzipien der Quantentheorie in der Quantenkryptographie zur Anwendung kommen.

Die Quantenkryptographie ist seit einigen Jahren den Kinderschuhen entwachsen. Hier gezeigt ist das „Labor", in dem wir Verletzungen der Bell-Ungleichungen über 10 Kilometer nachweisen und so den Grundstein für Quantenkryptographie basierend auf nichtlokalen Korrelationen verschränkter Photonen legen konnten. Die Photonenpaarquelle befand sich in der Nähe des Genfer Bahnhofs Cornavin, die Analysatoren in Bellevue bzw. Bernex.

Kryptographie ist ganz allgemein die Kunst, eine Nachricht so zu verschlüsseln, daß sie für unbefugte Personen unlesbar und ohne jeglichen Informationsgehalt ist [3] (siehe Abb. 1). Erste Ansätze lassen sich bis zurück ins alte Ägypten verfolgen. Klassische Benutzer waren vor allem Militärs. Mit der Zunahme des elektronischen Datenverkehrs, bedingt durch die steigende Vernetzung durch das Internet, werden zuverlässige und schnelle Verschlüsselungsverfahren immer wichtiger für jeden von uns. Im folgenden werden wir zunächst die zwei Klassen der Kryptographie – mit öffentlichen oder geheimen Schlüsseln zur Chiffrierung einer Nachricht – kurz vorstellen und dann beschreiben, wie die Quantenmechanik das Problem der Übertragung eines geheimen Schlüssels lösen und die zuletzt genannte Klasse zu einem physikalisch sicheren Verfahren vervollständigen kann.

Kryptographie mit Hilfe „öffentlicher Schlüssel" wurde 1976 von Whitfield Diffie und Martin Hellman vorgeschlagen. Dabei gibt Bob als potentieller Empfänger einer Nachricht einen Schlüssel öffentlich bekannt. Jeder der möchte, kann diesen Schlüssel nun zum Chiffrieren seines Textes verwenden und diesen dann gefahrlos an Bob senden. Die Sicherheit dieses Verfahrens beruht darauf, daß der Schlüssel zum Dechiffrieren nicht aus der Kenntnis des öffentlichen Schlüssels abgeleitet werden kann. Die Grundlage dazu liefern „one way"-Funktionen, die in einer Richtung – der Verschlüsselung – leicht, in der umgekehrten Richtung – der Entschlüsselung – jedoch sehr schwer zu berechnen sind. Das bekannteste Beispiel dafür ist das von Ronald Rivest, Adi Shamir und Leonard Adleman 1977 entwickelte „RSA-Kryptographieverfahren", welches auf der Faktorisierung großer Zahlen beruht: Jeder von uns kann innerhalb kürzester Zeit ausrechnen, daß 107 mal 53 den Wert 5671 ergibt. Die Aufgabe jedoch, die Primfaktoren von 5671 zu finden, läßt sich nur durch viel Probieren lösen, ein effizienter Algorithmus ist bisher nicht bekannt. Nur Bob, der die beiden Primfaktoren im voraus kennt und aus diesen – seinem privaten Schlüssel – den öffentlichen Schlüssel berechnet, kann auf die Originalnachricht schließen. Die Rechenzeit für die Primfaktorenzerlegung wächst exponentiell mit der Anzahl der Eingabebits. Ein solches Rechenproblem wird in der Informationstheorie als schwierig bezeichnet. Im Falle der Kryptographie garantiert die Tatsache, daß das „Knacken" des öffentlichen Schlüssels lange dauert, die Sicherheit der Übertragung. Diese

Dipl.-Phys. Wolfgang Tittel, Dr. Jürgen Brendel, Prof. Dr. Nicolas Gisin, Dipl.-Phys. Grégoire Ribordy, Dr. Hugo Zbinden, GAP-Optique, Université de Genève, 20 rue de l'Ecole de Médecine, CH-1211 Genf, Schweiz

Physikalische Blätter 55 (1999) Nr. 6
0031-9279/99/0606-25
$17.50+50/0

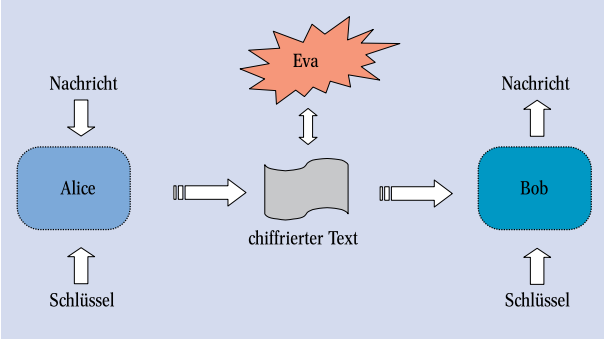


Abb. 1:
Allgemeines Schema für die Übertragung geheimer Nachrichten. Der Sender Alice kombiniert Nachricht und Schlüssel zu einem chiffrierten Text, den sie dann Bob sendet. Bob entschlüsselt den erhaltenen Text mit Hilfe seines Schlüssels und erhält so die ursprüngliche Nachricht. Eva ist die unerwünschte Lauscherin, die versucht, möglichst viel von der Nachricht mitzuhören.

Tabelle 1: Beim „one time pad" addiert Alice zu der aus Nullen und Einsen bestehenden Nachricht einen geheimen Schlüssel der gleichen Länge modulo 2 (d. h. 0 + 0 = 0; 0 + 1 = 1 + 0 = 1; 1 + 1 = 0). Den so chiffrierten Text schickt sie Bob. Dieser addiert den gleichen Schlüssel erneut modulo 2 und erhält die ursprüngliche Nachricht zurück.

Alice								
Nachricht	0	1	1	0	1	0	0	1
Schlüssel	1	0	0	1	1	0	1	0
Summe (modulo 2) = chiffrierter Text	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**1**
Übertragung								
Bob								
chiffrierter Text	1	1	1	1	0	0	1	1
Schlüssel	1	0	0	1	1	0	1	0
Summe (modulo 2) = Nachricht	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**

wäre aber in dem Moment hinfällig, in dem ein entsprechender Algorithmus entdeckt würde. Eine weitere Gefahr droht durch die Entwicklung des sogenannten Quantencomputers, einer „Maschine", die die Faktorisierung von großen Zahlen in Zeiten bewerkstelligen könnte, die lediglich in Form einer Polynomfunktion von der Zahl der Eingabebits abhängen.

Die zweite Klasse von Verschlüsselungsverfahren beruht auf geheimen Schlüsseln zur Chiffrierung der Nachricht. In Verbindung mit dem elektronischen Datenverkehr wird zumeist der „Data Encryption Standard" (DES, 1977) eingesetzt. Diese Methode benutzt den gleichen, bekannten Algorithmus zum Chiffrieren und zum Dechiffrieren sowie einen geheimen Schlüssel von 56 Bit Länge. Genau wie bei Methoden mit öffentlichen Schlüsseln basiert die Sicherheit auf mathematischer Komplexität, d.h. der Tatsache, daß der Spion viel Zeit zum Entschlüsseln der Nachricht benötigt. Eine andere, ebenfalls der Klasse geheimer Schlüssel zugehörende Möglichkeit wurde 1935 von Gilbert Vernam vorgeschlagen. Bei diesem, als „one time pad" bekannt gewordenen Verfahren addiert der Sender Alice zu dem aus Nullen und Einsen bestehenden Text Bit für Bit einen Schlüssel modulo 2 (siehe Tabelle 1). Besteht der Schlüssel aus einer zufälligen Abfolge von Nullen und Einsen, ist er genauso lang wie die zu übermittelnde Nachricht und wird er nur einmal benutzt, so ist der Informationsgehalt in der resultierenden Zahlenkette Null. Die so chiffrierte Nachricht kann nun über öffentliche Kanäle verschickt werden. Nur diejenigen Personen, die den Schlüssel kennen, können durch abermalige Addition (modulo 2) die ursprüngliche Nachricht finden. Im Gegensatz zu zuvor beschriebenen, auf mathematischer Komplexität beruhenden Methoden ist die Sicherheit dieses Verfahrens mathematisch bewiesen. Das Problem der Übermittlung einer geheimen Nachricht ist somit auf die sichere Verteilung eines Schlüssels reduziert. An diesem Punkt kommen nun die besonderen Eigenschaften der Quantenmechanik zum Tragen. Grob gesagt läßt sich ausnutzen, daß die Messung eines unbekannten Zustandes diesen im allgemeinen verändert. Sind Bits des Schlüssels während der Übertragung verändert worden, so kann man auf die Anwesenheit einer dritten Person schließen. Ist dies nicht der Fall, so ist der Schlüssel sicher und eignet sich zur Kodierung einer Nachricht.

Quantenkryptographie in der Theorie

Wir unterscheiden hier zwischen zwei Klassen der quantenmechanischen Schlüsselübertragung, basierend auf der Verwendung von Ein- oder Zweiteilchensystemen. Abbildung 2 skizziert Kryptographie mit Einteilchensystemen am Beispiel von Polarisationskodierung mit einzelnen Photonen. Dieses Protokoll wurde 1984 von Charles Bennett (IBM) und Gilles Brassard (Universität Montreal) vorgeschlagen und ist nun als BB84 Protokoll bekannt [4]. Alice, die die Übertragung initiiert, schickt Bob linear polarisierte Photonen. Wir identifizieren horizontal sowie unter – 45° polarisierte Photonen mit dem Bitwert „0" und vertikal sowie unter + 45° polarisierte mit dem Bitwert „1". Alice sendet einzelne Photonen in einem dieser vier Polarisationszustände und verzeichnet den gewählten Zustand jedes Photons in einer Liste. Bob, der legitime Empfänger, hat zwei Analysatoren zur Verfügung. Der erste ermöglicht die Unterscheidung zwischen horizontal und vertikal polarisierten Photonen, der zweite die zwischen diagonal polarisierten Photonen. Vor jeder Messung wählt Bob einen dieser beiden Analysatoren und dokumentiert die getroffene Wahl, sowie ob und wo er ein Photon registriert hat in seiner Liste. Nach Übertragung einer genügend großen Anzahl von Photonen vergleichen Alice und Bob öffentlich ihre Listen. Sie verständigen sich über diejenigen Ereignisse, bei denen Bobs Analysator an den Zustand des von Alice präparierten Photons angepaßt war. In diesen Fällen haben beide identische Bit-Werte: Die von Bob detektierten Photonen befinden sich in exakt dem Zustand, in dem sie von Alice präpariert worden sind. Alle Ereignisse, bei denen kein Photon detektiert wurde oder aber der Zustand des gesendeten Photons und der gewählte Analysator nicht im Einklang standen, werden nicht weiter berücksichtigt. Hierbei ist es wichtig, sich zu verdeutlichen, daß die öffentliche Kommunikation zwischen Alice und Bob zwar bekannt gibt, ob ein Photon horizontal-vertikal oder diagonal polarisiert war, jedoch keine detailliertere Information über den Zustand des gesendeten Teilchens verraten wird. Auf diese Art und Weise gelingt es Alice und Bob, Zahlenketten mit gleicher Abfolge von Nullen und Einsen aufzustellen.

Wie aber gewährleistet diese Art der Schlüsselverteilung die Sicherheit, daß keine dritte Person Information über den Kode erhält? Wir betrachten dazu beispielhaft die folgende Strategie der Spionage. Da die

Übertragung auf einzelnen Photonen basiert, ist es dem Spion unmöglich, einen kleinen, von Bob nicht bemerkbaren Anteil des optischen Signal abzuzweigen um seine Messung daran vorzunehmen. Er kann ein Photon entweder unbeobachtet zu Bob passieren lassen, in welchem Fall er keinerlei Information über dessen Zustand erhält, oder dieses als Ganzes messen und ein entsprechend dem Resultat der Messung präpariertes Ersatzphoton weiterschicken. Bedingt durch die Verwendung nichtorthogonaler Zustände ist es ihm jedoch unmöglich, den Zustand jedes Photons korrekt zu ermitteln: Wählt er z. B. ähnlich Bob für jede Messung einen von zwei Analysatoren, so wird er bei der Hälfte aller Messungen in einer falschen Basis messen und ein zufälliges Ergebnis erhalten. Demnach kommen in 50 % der Fälle, in denen der Zustand des von Alice gesendeten Photons und der von Bob gewählte Analysator übereinstimmen, veränderte Photonen bei Bob an. Bei wiederum 50 % dieser Photonen erhält Bob ein Ergebnis, das dem ursprünglich von Alice gewählten Zustand widerspricht. In Alice und Bobs Listen schleichen sich folglich 25 % Fehler ein. Um dies zu überprüfen, vergleichen beide nach der Übertragung eine zufällige Auswahl von Bits öffentlich. Stimmen diese exakt überein, können sie darauf schließen, daß auch die nicht veröffentlichten Bits identisch sind, daß also kein Spion die Datenleitung abhörte. Diese Bits formen dann den geheimen Schlüssel. Es gibt andere, subtilere Strategien der Spionage als die hier vorgestellte [5], allen gemein ist aber die Eigenschaft, daß sie in Alice und Bobs Protokoll Fehler hinterlassen, die von diesen entdeckt werden können.

1991 wies Artur Ekert darauf hin, daß auch nichtlokale Korrelationen verschränkter Zweiteilchensysteme zur Aufstellung korrelierter Bitsequenzen dienen können [6] (siehe auch Kasten „Das Superpositionsprinzip, Schrödinger-Katzen und die Nichtlokalität“). Wir beschreiben im folgenden kurz die ursprüngliche Idee der Schlüsselübertragung, die sich stark an Tests der Bell-Ungleichungen anlehnt. Genau wie im vorangehenden Abschnitt betrachten wir Polarisationszustände. Jede andere Art der Verschränkung (Ort-Impuls, Energie-Zeit, Spin....) ist aber ebenfalls einsetzbar. Eine spezielle Quelle produziert Paare verschränkter Photonen, die dann voneinander getrennt und zu Alice bzw. Bob geschickt werden (Abb. 3). Alice und Bob wählen vor jeder Messung zufällig eine von drei Stellungen ihrer polarisierenden Strahlteiler (bzw. wählen einen von drei unterschiedlich orientierten Strahlteilern). Analog dem zuvor beschriebenen Protokoll mit einzelnen Photonen notieren sie Orientierung und Resultat jeder Messung und vergleichen nach einer hinreichend großen Zahl von detektierten Photonenpaaren öffentlich die Wahl der Stellungen. Sämtliche Messungen werden einer von drei Kategorien zugeordnet: Entweder es ergeben sich perfekte korrelierte, aber nur Alice und Bob bekannte Ergebnisse. Oder die gewählten Orientierungen ermöglichen einen Test der Bell-Ungleichungen. Die dritte Klasse beinhaltet nichtkompatible Orientierungen sowie all die Fälle, bei denen nur ein oder kein Photon detektiert werden konnte; sie wird nicht weiter betrachtet. Die Möglichkeit, einen Lauschangriff zu entdecken, ist bei dieser Methode besonders elegant: Falls eine dritte Person Photonen abfängt, diese mißt und entsprechend dem Ergebnis der Messung präparierte Ersatzphotonen weiterschickt, so bricht sie notgedrungen die Verschränkung der beiden Photonen auf und die Bell-Ungleichung wird nicht mehr verletzt – daran erkennen Alice und Bob den Spion.

Quantenkryptographie in der Praxis

Alle bisherigen Experimente verwendeten Photonen als Informationsträger. Sie sind experimentell relativ einfach zu erzeugen und lassen sich mit Hilfe von Glasfasern transportieren, eine Technik, die innerhalb der letzten Jahrzehnte, bedingt durch die enorme Expansion der Telekommunikation, große Fortschritte zu verzeichnen hat. So sind etwa die Transmissionsverluste von mehreren dB pro Kilometer um etwa eine

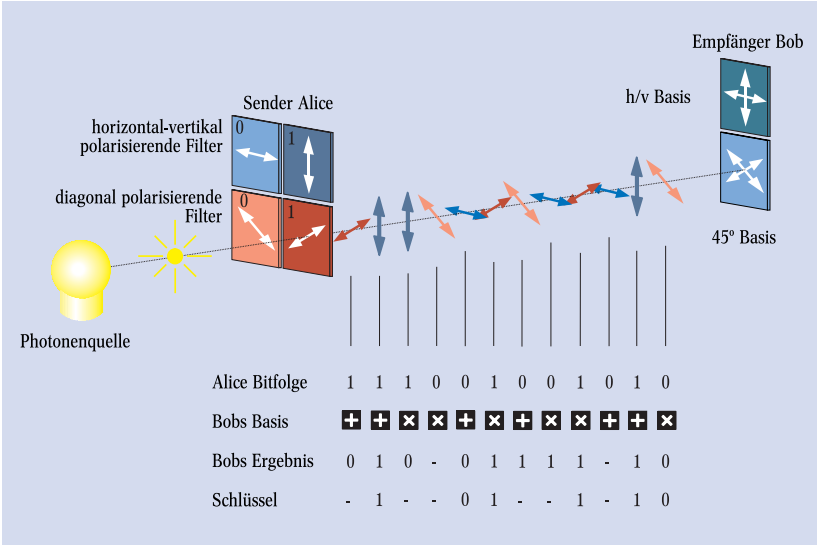
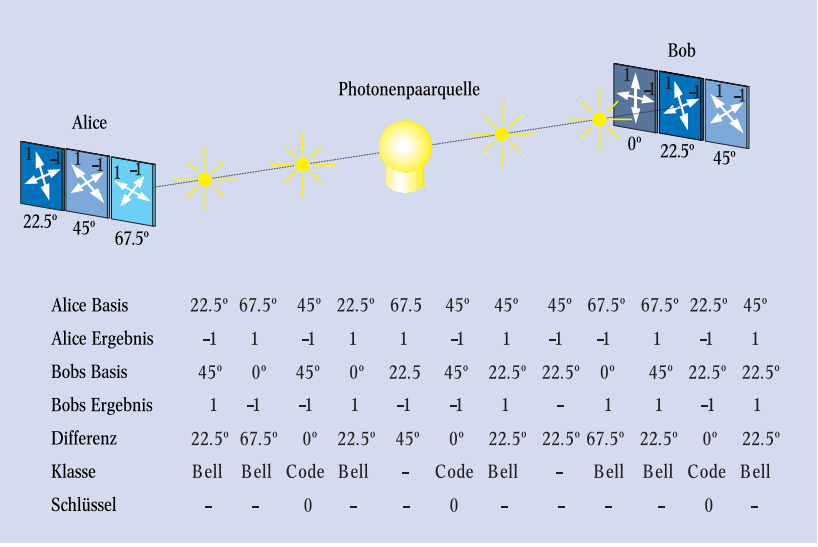


Abb. 2:
Quantenkryptographie (auch quantenmechanische Schlüsselübertragung, *quantum key distribution* genannt) löst das Problem der sicheren Schlüsselübertragung und vervollständigt den „one time pad“ so zu einem abhörsicheren System. Hier dargestellt ist das BB84-Protokoll. Die Bits sind als Polarisationszustände der einzelnen Photonen kodiert.



Alice Basis	22.5°	67.5°	45°	22.5°	67.5	45°	45°	45°	67.5°	67.5°	22.5°	45°
Alice Ergebnis	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
Bobs Basis	45°	0°	45°	0°	22.5	45°	22.5°	22.5°	0°	45°	22.5°	22.5°
Bobs Ergebnis	1	-1	-1	1	-1	-1	1	–	1	1	-1	1
Differenz	22.5°	67.5°	0°	22.5°	45°	0°	22.5°	22.5°	67.5°	22.5°	0°	22.5°
Klasse	Bell	Bell	Code	Bell	–	Code	Bell	–	Bell	Bell	Code	Bell
Schlüssel	–	–	0	–	–	0	–	–	–	–	0	–

Abb. 3:
Schlüsselübertragung mit verschränkten Photonen. Beim öffentlichen Vergleich der Analysatorstellungen teilen Bob und Alice alle Messungen entsprechend der relativen Orientierung der polarisierenden Strahlteiler in drei Klassen ein: Messungen mit Differenzen von 45° und solche, bei denen nur ein oder kein Photon detektiert wurde, werden nicht weiter berücksichtigt (Klasse „-“). Bei paralleler Orientierung ergeben sich korrelierte Ergebnisse, die im Weiteren als Schlüssel benutzt werden können (Klasse „Code“). Messungen mit Differenzen von 22,5° bzw. 67,5° ermöglichen Tests der Bell-Ungleichung. Wird sie verletzt, folgt, daß die von Bob und Alice registrierten Photonen quantenmechanisch verschränkt sind. Die Übertragung wurde nicht abgehört, denn ein Lauschangriff hätte die Korrelationen zerstört.

Größenordnung reduziert worden und betragen heute bei einer Wellenlänge von 1310 nm – im sogenannten zweiten Telekomfenster – nur noch 0,35 dB/km. Nach Transmission von zehn Kilometern Faser ist also erst die Hälfte der Photonen absorbiert worden, ein Wert, der Quantenkryptographie in lokalen Netzwerken ermöglicht.[1)] Es sei an dieser Stelle darauf hingewiesen, daß, obwohl fast alle Experimente auf Glasfasern zurückgreifen, ebenfalls Bestrebungen bestehen, Systeme zur Schlüsselübertragung zu Satelliten bzw. zwischen Satelliten zu entwickeln.

Wie immer in der Physik unterscheiden sich Theorie und Praxis in nicht vernachlässigbarer Art und Weise. Haben wir weiter oben behauptet, daß die Bitabfolgen von Alice und Bob bei Abwesenheit eines Spions perfekt korreliert sind, so entspricht dies mehr einem Wunschtraum als der Realität. Tatsächlich gibt es immer einige Fehler, sie liegen normalerweise im Bereich weniger Prozente. Das Verhältnis der Zahl der fehlerhaften zur Gesamtzahl der übertragenen Bits, die sogenannte Quantenbit-Fehlerrate, ist somit neben Distanz und Frequenz der Übertragung eine der charakteristischen Größen eines Quantenkryptographie-Systems.

Unkorrelierte Bits können durch verschiedene experimentelle Ungenauigkeiten hervorgerufen werden. Sendet Alice z. B. anstelle eines vertikal polarisierten Photons ein unter einem Winkel von 84° polarisiertes, so wird Bob in einem Prozent der Fälle das Photon im Kanal „horizontal“ entdecken. Entsprechendes gilt für Bobs Analysatoren. Eine weitere Fehlerquelle entspringt der Möglichkeit, daß die von Alice gewählten Quantenzustände während der Transmission zu Bob verändert werden können. Ein vertikal polarisiertes Photon muß auch vertikal polarisiert bei Bob ankommen. Bedingt durch die Doppelbrechung optischer Fasern ist dies im allgemeinen jedoch nicht der Fall. Da die Eigenschaften von Fasern zeitlich nicht konstant sind – mechanisch oder thermisch bedingte Spannungen etwa ändern sich auf einer Zeitskala von Minuten – ist also eine ständige Überwachung und Regelung vonnöten. Dies ist zwar möglich, aber nicht sehr praktisch. Eine dritte Ursache für nichtkorrelierte Bits ist das Rauschen der Detektoren. Es führt immer dann zum falschen Ergebnis, wenn ein Photon auf dem Weg zu Bob absorbiert worden ist und der Detektor des „falschen“ Kanals in dem Moment anspricht, in dem das Photon hätte ankommen sollen. Da für Wellenlängen mit geringen Faserverlusten nur Germanium- und InGaAs-Avalanche-Photodioden eingesetzt werden können, die sich durch relativ geringe Quantenausbeuten und viel Rauschen auszeichnen, sind die meisten Fehler einer Schlüsselübertragung in aller Regel nicht der Detektion von Photonen in einem falschen Kanal, sondern dem Detektorrauschen zuzuschreiben.

Nach einer Schlüsselübertragung muß der sogenannte Rohschlüssel folglich zunächst von Fehlern bereinigt werden. Dazu dienen klassische Fehlerkorrektur-Algorithmen. Da Alice und Bob jedoch nie sicher sein können, daß die gefundenen Fehler tatsächlich experimentellen Ungenauigkeiten und nicht der Präsenz einer dritten Person zuzuschreiben sind, wird in einem als „privacy amplification“ bekannten weiteren Schritt das hypothetische Wissen eines Lauschers bis auf beliebig kleine Werte reduziert. Dazu werden z. B. mehrere Bits zu einem einzigen zusammengefaßt, eine Prozedur, die bei zwei Schlüsseln nur dann zum gleichen Ergebnis führt, wenn alle ursprünglichen Bits gleich sind. Dies ist der Fall bei Alice und Bob. Kennt der Lauscher jedoch nur einen kleinen Teil des Rohschlüssels, so endet er mit einer völlig anderen Bitfolge. Leider verkürzt dieses Verfahrens vor allem bei großen Fehlerraten den Rohschlüssel sehr stark und ist nur bis hin zu einer Quantenbit-Fehlerrate von 15 % anwendbar. Alice und Bob haben daher ein großes Interesse daran, die Fehler bei der Übertragung so gering wie möglich zu halten.

Experimente

Zum ersten Mal wurde die Quantenkryptographie 1989 von Forschern bei IBM experimentell demonstriert. Der von ihnen gebaute Prototyp basierte auf Polarisationskodierung mit einzelnen Photonen[2)] und übertrug einen Schlüssel über 30 cm Luftweg. Seitdem sind enorme Fortschritte erzielt worden, und mehrere Gruppen konnten über Systeme berichten, die außerhalb des Labors funktionieren [7]. Wir geben im folgenden einen Überblick über die letzten Entwicklungen, werden diesen aber auf Systeme beschränken, die bei Wellenlängen arbeiten, welche für große Übertragungsstrecken geeignet sind.

1995 konnten wir zeigen, daß Quantenkryptographie, beruhend auf schwachen Pulsen, auch über große

[1)] Im Gegensatz zur „standard“ Telekommunikation lassen sich bei der Quanten-Kryptographie keine Verstärker einsetzen, da der Zustand einzelner Photonen nicht kopiert werden kann.

Das Superpositionsprinzip, Schrödingerkatzen und die Nichtlokalität

Hat die Schrödinger-Gleichung mehrere Lösungen – etwa $|\Psi_1\rangle$ und $|\Psi_2\rangle$ –, so entspricht die allgemeine Lösung der Linearkombination der beiden Wellenfunktionen: $|\Psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_2\rangle$. Diese als Superpositionsprinzip bekannte Tatsache folgt aus der Linearität der Wellengleichung. Sie ist eine der grundlegenden Regeln der Quantenmechanik und wird normalerweise ohne weiteres akzeptiert. Und doch führt genaueres Hinterfragen zu seltsam anmutenden Eigenschaften. Beschreiben die beiden Wellenfunktionen $|\Psi_1\rangle$ und $|\Psi_2\rangle$ etwa zwei verschiedene Orte, an denen sich ein Teilchen aufhalten kann, so entspricht die Linearkombination der beiden einem Teilchen, welches sich an beiden Orten gleichzeitig befindet. Oder aber wir gelangen zu einem Atom, welches zur gleichen Zeit existiert und bereits radioaktiv zerfallen ist. Diese Aussage wirkt besonders bizarr beim Übergang in die makroskopische Welt. Schrödinger brachte dies mit einem makabren Gedankenexperiment auf den Punkt: Koppelt man das quantenmechanische Einteilchensystem an einen Mechanismus, der eine Katze tötet, so ist die Katze gleichzeitig lebendig und tot.

Wenden wir das Superpositionsprinzip auf Zweiteilchensysteme an, so gelangen wir zu sogenannten verschränkten Zuständen. Ein solcher Zustand kann z. B. – um bei polarisierten Photonen zu bleiben – durch $|\Psi\rangle = 1/\sqrt{2}(|\mathrm{h}\rangle_1|\mathrm{v}\rangle_2 - |\mathrm{v}\rangle_1|\mathrm{h}\rangle_2)$ beschrieben werden: Photon 1 befindet sich im Polarisationszustand horizontal und Photon 2 im Zustand vertikal, überlagert mit der Möglichkeit, daß sich Photon 1 im Zustand vertikal und Photon 2 im Zustand horizontal befindet. Die Eigenschaft eines einzelnen Photons eines solchen Paares ist gemäß der Quantenmechanik also völlig undefiniert. Eine Messung in der Basis horizontal/vertikal kann sowohl horizontal als auch vertikal ergeben, die Natur entscheidet sich rein zufällig für eines der beiden Ergebnisse. Das Problem, woher das andere Photon, welches sich zur Zeit der Messung beliebig weit entfernt aufhalten kann, instantan „weiß“, welche Eigenschaft es annehmen muß – gemäß der Wellenfunktion immer orthogonal zum Ergebnis der Messung des anderen Photons –, hat schon immer für philosophische Debatten gesorgt. So führte es Albert Einstein, Boris Podolsky und Nathan Rosen im Jahre 1935 zur Formulierung eines als EPR-Paradoxon bekanntgewordenen Gedankenexperimentes und zu der Frage, ob die quantenmechanische Beschreibung durch eine Unterstruktur zu ergänzen sei [10]. Diese könnte das Verhalten der Teilchen im vornherein festlegen und somit den Aspekt „Zufall“ aus der Quantentheorie entfernen und die Nichtlokalität vermeiden. John Bell konnte 1964 mit den sogenannten Bell-Ungleichungen zeigen, daß die quantenmechanischen Voraussagen für Korrelationsmessungen von den Voraussagen lokaler Theorien, die auf den Vorschlag von Einstein, Podolsky und Rosen zurückgehen, abweichen [11, 12].

Der erste Test der Bell-Ungleichungen wurde 1972 von Freedman und Clauser durchgeführt, die bekanntesten Untersuchungen sind der Gruppe um Alain Aspect zu Beginn der achtziger Jahre zuzuschreiben [13]. Alle Experimente bestätigen die Voraussagen der Quantenmechanik, können damit aber das Unbehagen hinsichtlich der Nichtlokalität nicht ausräumen.

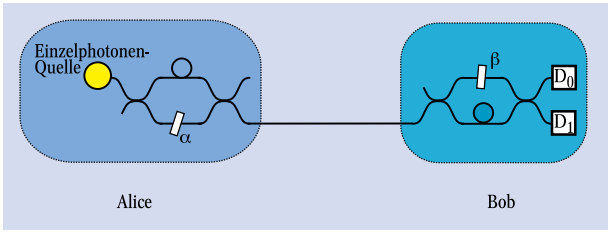


Abb. 4:
Quantenkryptographie, basierend auf Phasenkodierung mit einzelnen Photonen. Haben beide Interferometer – hier als Faserinterferometer angedeutet – gleiche Armlängenunterschiede, so sind die beiden Wege „langer Arm bei Alice, kurzer Arm bei Bob“ und „kurzer Arm bei Alice, langer Arm bei Bob“ ununterscheidbar und man beobachtet Interferenz, d. h. die Wahrscheinlichkeit für die Detektion eines Photons in Detektor D_0 bzw. D_1 hängt von den Phasen α und β ab. Zur Realisierung des BB84-Protokolls wählt Alice für jedes Photon zufällig eine der Phasen 0, $\pi/2$, π oder $3\pi/2$. Wählt Bob die Phase 0, so kann er zwischen Alices Wahl von 0 (Detektion in D_0) und π (Detektion in D_1) unterscheiden, wählt er eine Phase von $\pi/2$, kann er entsprechend $\pi/2$ von π trennen. Alles Weitere entspricht der Polarisationskodierung (Abb. 2).

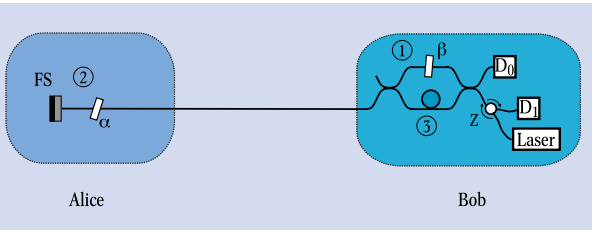


Abb. 5:
Das von uns entwickelte „Plug&Play“ System. Im Gegensatz zu dem in Abb. 4 gezeigten Aufbau sind die interferierenden Wege räumlich identisch, werden aber in unterschiedlicher Reihenfolge durchlaufen (1-2-3 interferiert mit 3-2-1). Dies führt zu einem automatischen Ausgleich aller Längenänderungen. Der Faraday-Spiegel (FS) – ein 45° Faraday-Rotator gefolgt von einem gewöhnlichen Spiegel – gewährleistet darüber hinaus die Kompensation sämtlicher Polarisationsänderungen während der Transmission von Bob zu Alice und wieder zurück zu Bob. Nach Reflexion an einem solchen Spiegel ist das Licht an jedem beliebigen Punkt immer orthogonal zum Zustand beim Hinweg polarisiert. α und β sind von Alice und Bob gewählte Phasen, D_0 und D_1 sind Detektoren und Z ist ein sogenannter Zirkulator, der dafür sorgt, daß alles vom Laser ausgesendete Licht in den optischen Aufbau und alles zurückkommende Licht in den Detektor D1 gelangt.

Entfernungen möglich ist. Wir verschickten dazu polarisierte Photonen über eine Strecke von 23 km unterhalb des Genfer Sees, wozu wir uns des Telekommunikations-Fasernetzes der Swisscom bedienten. Eine andere Art, die verschiedenen Quantenzustände für eine Schlüsselübertragung zu realisieren, beruht auf Phasenkodierung. Sie wurde 1993 von der Gruppe um Paul Townsend bei der British Telecom entwickelt und wird mittlerweile auch von Richard Hughes Gruppe am Los Alamos National Laboratory in New Mexiko benutzt. Abbildung 4 zeigt das Prinzip dieser Methode. Alice und Bob besitzen jeweils ein Mach-Zehnder-Interferometer mit gleichen Armlängendifferenzen. Die Interferometer dienen zur Präparation bzw. Detektion von Pulssequenzen mit bestimmten Phasenbeziehungen. Genau wie bei der Polarisationskodierung bedarf dieses System aktiver Kontrolle. Zum einen müssen die Armlängendifferenzen auf Bruchteile einer Wellenlänge gleich groß gehalten werden. Darüber hinaus ist nur dann ein gutes Ergebnis zu erwarten, wenn die Entwicklung des Polarisationszustands in den verschiedenen Armen jedes Interferometers identisch ist. Auch hier ist also eine Polarisationskontrolle notwendig. Innerhalb der letzten zwei Jahre konnten wir ein neues interferometrisches System entwickeln, welches im Gegensatz zu dem zuvor beschriebenen „wartungsfrei“ ist und weder Armlängen- noch Polarisationskontrolle bedarf (Abb. 5). Auch dieses System wurde erfolgreich für die Übertragung geheimer Schlüssel unterhalb des Genfer Sees verwendet.

Wie im theoretischen Teil gesagt, lassen sich auch Zweiteilchensysteme für die Quantenkryptographie einsetzen. Sämtliche Bell-Experimente zeigen die prinzipielle Machbarkeit auf. Es gibt allerdings bisher nur zwei Experimente, die im Zusammenhang mit Quantenkryptographie über große Distanzen zu nennen sind[3]. 1994 konnte die Gruppe um John Rarity vom DRA Malvern in Großbritannien Verletzungen der Bell-Ungleichungen mit in Energie und Zeit verschränkten Photonen im Labor demonstrieren, wobei einer der Analysatoren durch eine 4,3 km lange, auf einer Spule aufgerollte optische Faser von der Quelle getrennt war [8]. Basierend auf der gleichen Art der Verschränkung gelangen uns in den Jahren 1997 und 1998 eine Serie von Experimenten, mit denen wir nichtlokale Korrelationen auch außerhalb des Labors über eine Distanz von mehr als 10 Kilometern nachweisen konnten [9] (siehe Abb. auf der ersten Seite dieses Artikels). Die Photonenpaarquelle befand sich in einer Telekommunikationszentrale in der Nähe des Genfer Bahnhofs Cornavin, die Analysatoren in den 5 Kilometer südlich bzw. nördlich von Genf gelegenen Vororten Bellevue bzw. Bernex. Die das Zweiteilchensystem beschreibende Wellenfunktion erstreckte sich somit über einen Bereich von der Größe einer Kleinstadt. Dieses Experiment veranschaulicht die von Einstein angezweifelte „geisterhafte Fernwirkung“ zwischen den beiden Photonen besonders drastisch: Die Messung des einen Teilchens – der Kollaps der Wellenfunktion – führt instantan zu korreliertem Verhalten des anderen, 10 Kilometer entfernten Teilchens.

Wie bereits erwähnt, gibt es neben den hier präsentierten Experimenten weitere Prototypen, die bei Wellenlängen um 800 nm – im sogenannten ersten Telekom-Fenster – arbeiten. Aufgrund höherer Faserverluste ist die maximale Reichweite jedoch auf wenige Kilometer begrenzt. Mit einem solchen System hat die British Telecom 1997 ein auf Polarisationskodierung mit einzelnen Photonen beruhendes System entwickelt, das die bisher mit Abstand höchste Quantenbitrate von 1,2 MHz erzielen konnte. Forscher der Universität Innsbruck unter Leitung von Anton Zeilinger konnten im letzten Jahr ebenfalls über eine auf der Eigenschaft „Polarisation“ basierende Übertragung eines Schlüssels in Verbindung mit einem Test der Bell-Ungleichungen über 500 Meter berichten.

Die Zukunft

Quantenkryptographie, die am weitesten entwickelte Anwendung des neuen Gebietes der Quantenkommunikation, hat seit vier Jahren das Labor verlassen. Experimente unter realen Bedingungen sind, zumindest was Systeme angeht, die auf Kodierung mit „schwachen Pulsen“ beruhen, heutzutage schon fast eine Rou-

[2] Tatsächlich wurden in diesem wie in allen bisher durchgeführten Experimenten einzelne Photonen durch sogenannte „schwache Pulse“ simuliert, kohärente Zustände mit einer mittleren Photonenzahl von 0,1 Photonen pro Puls.

[3] Das liegt vor allem daran, daß fast alle Experimente mit Photonen einer Wellenlänge arbeiten, bei der es zwar gute Detektoren gibt, bei denen jedoch starke Absorptionsverluste in optischen Fasern bestehen.

tineübung. Reichweiten liegen in der Gegend von 20 – 30 Kilometern, und Quantenbit-Fehlerraten von wenigen Prozent sind niedrig genug, um einen Lauschangriff detektieren und die sichere Übertragung eines Schlüssels gewährleisten zu können. Somit können existierende System schon heute eine sichere Übertragung von Nachrichten garantieren, falls Verfahren, die auf mathematischer Komplexität beruhen, „geknackt" werden sollten. Verbesserungsbedarf besteht vor allem in der Distanz sowie der Übertragungsrate, die z. Zt. bei einigen hundert Hertz liegt. Zum Beispiel würde die Erstellung eines Schlüssels zur Kodierung dieses Textes – etwa 44 KByte ohne Bilder – mit Hilfe des „one time pads" unter Anwendung des in Abb. 5 gezeigten „Plug & Play" Systems etwa 20 Minuten dauern. Erste Systeme, die auf nichtlokalen Korrelationen verschränkter Photonen beruhen, wurden ebenfalls außerhalb des Labors demonstriert. Die tatsächliche Übertragung eines Schlüssels steht aber noch aus, zumindest über große Entfernungen. Ein dreijähriges ESPRIT-Projekt mit dem Namen „European Quantum Cryptography and Single Photon Optical Technologies" untersucht momentan, welche Methode der quantenmechanischen Schlüsselübertragung die beste ist.

Literatur

[1] Physics World, März 1998, Schwerpunktheft Quantenkommunikation.

[2] *H. K. Lo, S. Popescu* und *T. P. Spiller*, Introduction to Quantum Computation and Information, World Scientific, Singapore 1998

[3] *A. J. Menezes, P. C. Oorschot* und *S. A. Vanstone*, Handbook of Applied Cryptography, CRC, New York 1997

[4] *C. H. Bennett* und *G. Brassard*, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, S. 175 (1984)

[5] *C. A. Fuchs, N. Gisin, R. B. Griffiths*, *C.-S. Niu* und *A. Peres*, Phys. Rev. A **56**, 1163 (1997)

[6] *A. K. Ekert*, Phys. Rev. Lett. **67**, 667 (1991)

[7] *H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin* und *G. Ribordy*, Appl. Phys. B **67**, 743 (1998)

[8] *P. R. Tapster*, *J. G. Rarity* und *P. C. M. Owens*, Phys. Rev. Lett. **73**, 1923 (1994)

[9] *W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden* und *N. Gisin*, Phys. Rev. A **57**, 3229 (1998); *W. Tittel, J. Brendel, H. Zbinden* und *N. Gisin*, Phys. Rev. Lett. **81**, 3563 (1998)

[10] *A. Einstein, B. Podolsky* und *N. Rosen*, Phys. Rev. **47**, 777 (1935)

[11] *J. S. Bell*, Physics **1**, 195 (1964)

[12] *N. D. Mermin*, Am. J. Phys. **49**, 940 (1981)

[13] *J. Freedman* und *J. F. Clauser*, Phys. Rev. Lett. **28**, 938 (1972); *A. Aspect, P. Grangier* und *G. Roger*, Phys. Rev. Lett. **47**, 460 (1981); *A. Aspect, P. Grangier* und *G. Roger*, Phys. Rev. Lett. **49**, 91 (1982) *A. Aspect, J. Dalibard* und *G. Roger*, Phys. Rev. Lett. **49**, 1804 (1982)