Thomas Jennewein, Gregor Weihs, Anton Zeilinger

Schrödingers Geheimnisse

Absolut sichere Kommunikation durch Quantenkrytopgraphie

Ausgerechnet die seltsame Welt der Quantenmechanik – ansonsten eigentlich eher das Spielfeld für Philosophen und theoretische Physiker – bietet Mittel und Wege zur absolut sicheren Kommunikation. An der Quantenkryptographie beißt sich jeder noch so versierte Spion die Zähne aus.

Das Jahr 2020: Alice, eine Mitarbeiterin einer Bank in Deutschland, muss Bob, einem Kollegen in der Schwesterbank in New York, eine Datei mit neuesten Wirtschaftsprognosen übermitteln. Da die Bankbetreiber größten Wert auf die Sicherheit bei der Übertragung so sensitiver Daten legen, wird diese Übertragung mit Quantenkryptographie durchgeführt, dem teuersten, aber absolut sicheren Verschlüsselungsverfahren. Dazu bestellen Alice und Bob bei QTP, einem global agierenden Quantenkommunikations-Anbieter, je einen Speicher mit verschränkten Atomen. Nachdem sie die Speicher an ihre Schlüsselextraktoren angeschlossen haben, erhalten sie jeweils einen identischen, zu 100 % sicheren Kryptoschlüssel. Alice kodiert mit ihrem Schlüssel die sensitiven Daten zu einer vollkommen unleserlichen Datei. Über eine beliebige herkömmliche Datenleitung erhält Bob das Kryptogramm und dekodiert es mit seinem Schlüssel, dessen Sicherheit durch die speziellen Eigenschaften der Quantenphysik garantiert ist.

Zukunftsmusik? Die Basis zu dieser Vision liefert ein neuer und sehr rasch wachsender Forschungszweig der Physik: die Quanteninformatik. Die Quanteninformatik ist ein wunderbares Beispiel dafür, wie aus reinen Grundlagenwissenschaften neuartige Technologien entstehen können. Die Entwicklungen der Quanteninformatik umfassen so klingende Anwendungen wie Quantenteleportation, Quantenkryptographie und Quantencomputer [1, 2, 3] – die Konzepte versprechen gänzlich neue und aufregende Verfahren, möglicherweise einen 'Quantensprung' in der Informationsverarbeitung.

Klassische Kryptosysteme

Bei den 'klassischen Kryptosystemen' unterscheidet man im Wesentlichen zwei Methoden: symmetrische und unsymmetrische Verschlüsselungsverfah-

ren. Bei symmetrischen Verfahren kommunizieren die Teilnehmer mit einem geheimen Schlüssel, der beiden Teilnehmern zur Verfügung steht, zum Beispiel im 'Data Encryption Standard' (DES), bei Blowfish oder beim One-Time-Pad Protokoll. Unsymmetrische Verfahren hingegen arbeiten mit Hilfe eines zweigeteilten Schlüssels: Die Information wird mit dem öffentlichen Schlüssel eines Teilnehmers kodiert und kann dann nur von der Person in Besitz des zugehörigen privaten Schlüssels im Klartext gelesen werden. Beispiele sind RSA und Pretty Good Privacy (PGP). Den klassischen Verfahren ist jedoch gemein, dass deren Sicherheit auf dem vertraulichen Austausch eines Schlüssels zwischen den Teilnehmern und/oder auf dem rechnerischen Aufwand beim Hacken der Schlüsselkombination durch Probieren oder Ausrechnen eines Algorithmus beruht.

Die Sicherheit eines Kryptosystems kann zwar sehr hoch sein, letztlich jedoch ist sie aber immer von der Integrität eines Kuriers oder von Rechenleistung abhängig, die potenziellen Angreifern zur Verfügung steht. Das mindeste Ziel ist also, dass die Verschlüsselung so lange der Entschlüsselung trotzt, wie die betreffende Information noch wertvoll ist. In diesem Zusammenhang fürchten Sicherheitsexperten den Einzug der Quantencomputer, die gerade für Entschlüsselungsalgorithmen (Faktorisieren großer Zahlen) im Prinzip eine massiv gesteigerte Rechenleistung erzielen könnten. Jedoch sind diese Quantencomputer kaum noch über das Stadium theoretischer Konzeption hinausgekommen [1, 2, 3]. Sinnigerweise bietet gerade die Quanteninformatik aber auch die Möglichkeit zu einer absolut sicheren Kryptographie, welche mit keinem System geknackt werden kann, nicht einmal mit einem Quantencomputer.

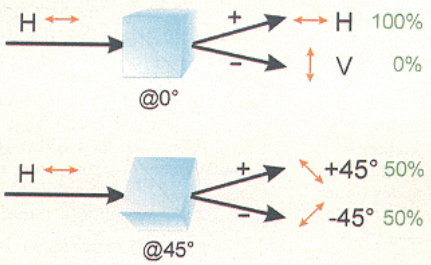
Quantum Magic

Dabei ist die Quantenkryptographie selbst noch kein System zur sicheren Übertragung von Information, sondern eine Erweiterung bestehender Kryptosysteme, die deren potenzielle Sicherheitslücke in der Schlüsselverteilung schließt. Das Grundkonzept der Quantenkryptographie ist einfach: Der Schlüssel wird durch einzelne Qubits übertragen oder durch Messungen an Qubits erzeugt. Ist die Schlüsselverteilung abgeschlossen, so kann dann im Nachhinein, durch eine statistische Analyse des Quantenschlüssels jeder erdenkliche Lauschangriff ausgeschlossen werden. Dies klingt wie Magie und dennoch bedarf es 'nur' der Gesetze der Quantenphysik. Das Besondere an dem Quantenschlüssel ist dabei, dass dessen Sicherheit durch Grundprinzipien der Natur gewahrt wird und nicht 'nur' durch die Kompliziertheit eines Algorithmus, geschickte Camouflage oder durch die Verlässlichkeit eines Kuriers.

Quantengeld

Ausgehend von den ersten Ideen in den 70er Jahren von Stephen Wiesner [4] zu fälschungssicherem Quantengeld, wurden mehrere Protokolle für die Quantenkryptographie entwickelt, die sehr ähnlich arbeiten. 1979 griffen Charles Bennett und Gilles Brassard das Thema auf und veröffentlichten ihre Ergebnisse auf der Konferenz Crypto'82; die versammelte Fachwelt zeigte sich allerdings skeptisch – es herrschte der Eindruck vor, dass Quantenkryptographie aufgrund der auf absehbare Zeit nicht beherrschbaren Technologie zum Scheitern verurteilt sei. Den ersten erfolgreichen experimentellen Quantenschlüsselaustausch führten Bennett und Brassard dann im Oktober 1989 durch; die Länge des Freiluft-Quantenkanals betrug dabei 32 cm.

1984 stellten Bennett und Brassard ein System vor, das heute als BB84-Schema bezeichnet wird [5]. Dabei kommunizieren zwei Teilnehmer Alice und Bob über einen so genannten Quantenkanal sowie einen öffentlichen klassischen Kanal. Alice kann über den Quantenkanal einzelne Qubits an Bob schicken. Eine sehr gute Realisierung eines Quantenkanals ist eine optische Glasfaser, in der einzelne Photonen als Qubits verschickt werden – der Einfachheit halber halten wir uns bei den weiteren Ausführungen an das Beispiel der Photonen.



Polarisationsmessung eines horizontal polarisierten Photons: Angegeben sind die verschiedenen Messwahrscheinlichkeiten für das Photon.

Ein Qubit ist die elementare Informationseinheit der Quanteninformatik: Das Qubit hat zwei ausgezeichnete Zustände, 0 und 1, kann aber auch in einer Superposition von 0 und 1 sein, wodurch sich das Qubit grundlegend von der klassischen Informationseinheit unterscheidet. Eine mögliche Realisierung eines Qubits ist die Polarisation eines einzelnen Photons.

Die Polarisation von Photonen ist die Schwingungsebene des zugehörigen elektrischen Feldes. Schwingt das Feld in einer Ebene, nennt man dies lineare Polarisation, und dreht sich das Feld, so ist dies die zirkulare Polarisation. Jede Polarisation lässt sich aus zwei unabhängigen Komponenten zusammensetzen. Überlagert man beispielsweise zwei lineare Polarisationskomponenten in horizontaler und vertikaler Ebene, so ergibt eine gleichphasige Überlagerung der zwei Komponenten die lineare Polarisation in der 45°-Ebene – eine um 90° phasenverschobene Überlagerung ergibt eine zirkulare Polarisation.

Die Analyse der Polarisation eines Photons kann nur die Amplituden von den zwei Komponenten feststellen, zum Beispiel die horizontale oder vertikale Komponente. Wegen der heisenbergschen Unschärferelation ist es jedoch nicht möglich, gleichzeitig die Phase zwischen den zwei Komponenten zu messen, wodurch sich die ursprüngliche Polarisation nicht bestimmen lässt. Misst man nun ein einzelnes Photon, welches zum Beispiel in der horizontalen Polarisationsebene definiert wurde, mit einem Polarisator, welches auf 45° ausgerichtet ist, wird das Photon völlig zufällig im +45°- oder –45°-Ausgang zu finden sein.

In dem BB84-Schema verfügt nun Alice über eine spezielle (hypothetische) Quelle, die einzelne Photonen mit einer von vier möglichen Polarisationen erzeugt: 0°, 90° und 45°, 135°. Es ist dabei wesentlich, dass Alice die Wahl der Polarisation zufällig trifft und dies auch streng geheim hält. Bob empfängt das Photon und versucht durch eine Analyse mit seinem Polarisator, der zwei Ausgänge besitzt ('+' und '–'), die orthogonalen Polarisationsrichtungen entsprechen, die Polarisation des Photons zu bestimmen.

Polarisierte Geheimnisse

Die Polarisationen der Photonen sind aber sehr geschickt gewählt: Photonen mit 0° oder 90° Polarisation können nur mit dem Polarisator von 0° analysiert werden, und Photonen mit 45° oder 135° mit dem Polarisator auf 45°. Analysiert man 0°- oder 90°-Photonen mit dem Polarisator auf 45°, so erhält man rein zufällige Ergebnisse, das heißt, es kann nichts über die Polarisation des Photons ausgesagt werden. Dasselbe gilt für die Messung der 45°- oder 135°-

Verschränkung: Die Quelle emittiert die verschränkten Photonen in zwei Richtungen. Wenn die Polarisatoren parallel orientiert sind und das linke Photon im +-Ausgang gemessen wird, so muss das rechte Photon im –-Ausgang sein und umgekehrt. Die roten Pfeile symbolisieren die entsprechenden Polarisationen der Photonen.

Polarisation mit dem Polarisator auf 0°. Da Bob aber von vornherein nichts über die Polarisation des Photons weiß, bleibt ihm nichts anderes übrig, als seinen Polarisator zufällig in die 0°- oder 45°-Ausrichtung zu schalten und das Photon in einem der Ausgänge des Polarisators zu detektieren. Er hat damit jedenfalls eine 50-Prozent-Chance, die zum Photon passende Polarisatorausrichtung zu erwischen. Bob registriert jedenfalls das Ergebnis der Polarisationsmessung und die Einstellung des Polarisators. Diese Unsicherheit in der Messung der Photonen ist der Knackpunkt in der Sicherheit der Übertragung. Es ist dabei für Bob beziehungsweise auch für einen potenziellen Lauscher, der die Photonen abfängt, ohne Zusatzinformation von Alice unmöglich festzustellen, welche Messungen richtig sind und welche nicht.

Sind alle Qubits übertragen und bei Bob registriert, kommt die Kommunikation über den öffentlichen klassischen Kanal zum Einsatz. Über diesen teilt Bob an Alice mit, welche Polarisatorausrichtung er bei dem jeweiligen Photon eingesetzt hat, nicht aber das konkrete Resultat. Die Zuordnung von Alices Abschicken des Photons und Bobs Detektion kann über eine Zeitmessung geschehen, die die Laufzeit der Photonen berücksichtigt. Alice vergleicht nun Bobs Einstellung mit der tatsächlichen Polarisation des Photons und teilt Bob über den klassischen Kanal mit, welche Photonen er mit der richtigen Einstellung gemessen hat. Aus diesen richtigen Messungen bilden Alice (sie kennt die ursprüngliche Polarisation des Photons) und Bob (er hat die Polarisation richtig gemessen) nun jeweils für sich ihren Quantenschlüssel, indem sie der 0°-Polarisation eine logische '0' zuordnen, der 90°-Polarisation eine logische '1', beziehungsweise der 45° eine '0' und der 135° eine '1'. Danach sollten Alice und Bob im Besitz einer identischen, zufälligen Folge von '0' und '1' sein – dem Quantenschlüssel.

Internationaler Stand der Forschung

In vielen Ländern der Welt wird fieberhaft an quantenkryptographischen Verfahren geforscht und entwickelt. Zwei übernationale Projekte, die von der Europäischen Kommission gefördert werden, sind EQCSPOT (Entwicklung eines quantenkryptographischen Aufbaus zur Prototypenreife) und QuComm ('Long Distance Photonic Quantum Communication', http://www.ele.kth.se/QEO/qucomm/).

Die (bekannten) Experimente in den USA werden hauptsächlich im Los Alamos National Laboratory durchgeführt, wo man sich mehr auf Quantenkryptographie im freien (Luft-)Raum im Hinblick auf Satellitenkommunikation konzentriert (http://p23.lanl.gov:80/Quantum/). Den Weltrekord in Bezug auf die Distanz von Alice und Bob hält mit 11 km die Gruppe GAP (Group of Applied Physics, http://www.gapoptique.unige.ch/, sowohl an EQCSPOT als auch QuComm beteiligt) an der Universität Genf.

In Deutschland und Österreich befassen sich im Wesentlichen zwei Gruppen experimentell mit Quantenkryptographie: die Gruppe von H. Weinfurter in München (http://scotty.quantum.physik.uni-muenchen.de/) und die Gruppe um A. Zeilinger in Wien (http://www.quantum.at).

Schlüsselprüfung

Wie finden nun Alice und Bob heraus, ob sie tatsächlich im Besitz eines sicheren Schlüssels sind? Dazu müssen sie beide ein zufälliges Sample aus dem Schlüssel herausnehmen und durch deren Vergleich auf die Fehlerrate des Schlüssels schließen. Dieser Sicherheitstest beruht darauf, dass nach den Gesetzen der Quantenmechanik ein elementares System wie ein Photon (Qubit) nicht teilbar ist und nicht kopiert werden kann, ohne das System auf eine offensichtliche Weise zu stören. Versucht ein Lauscher etwa durch das Einbringen eines Strahlteilers einige der Photonen abzuzweigen um diese zu analysieren, so kommen diese Photonen einfach bei Bob nicht an und tragen nicht mehr zum Schlüssel bei – der Lauschangriff war wertlos. In manchen praktischen Systemen kann jedoch diese Methode mit einem Strahlteiler doch funktionieren, nämlich wenn die Quelle nicht perfekt ist und manchmal mehr als ein Photon auf einmal erzeugt. Dies kann etwa beim Einsatz von abgeschwächten Laserpulsen als Photonenquelle der Fall sein.

Viel gefährlicher ist ein Angriff, bei dem der Lauscher alle Photonen abfängt, selbst analysiert und dann neue Photonen in der gemessenen Polarisation an Bob weiterschickt. Bob würde, wenn es geschickt angestellt wird, nichts von alledem merken und getrost den Quantenschlüssel erzeugen, den der Lauscher kennt. Jedoch muss auch der Lauscher – wie Bob – erraten, welche Polarisatorausrichtung für die jeweiligen Photonen die richtige ist, und das kann er auch nur mit einer 50-Prozent-Wahrscheinlichkeit. Dies bedeutet, dass bei den falsch gemessenen Photonen völlig zufällige Ergebnisse auftreten werden, die Hälfte davon sind zufällig richtig, die andere Hälfte zufällig falsch. Alles in allem hat der Lauscher also für ein Viertel der Photonen die falsche Polarisation gemessen beziehungsweise an Bob weitergeschickt. Alice und Bob werden nach der Schlüsselerzeugung eine Fehlerrate von 25 Prozent feststellen und wissen sofort, dass die Qubits gestört wurden. Genaue Analysen, welche alle theoretisch möglichen Abhörmethoden einbeziehen, ergeben schließlich eine Mindestfehlerrate von circa 14 Prozent, die eine sicherheitsbedenkliche Angriffsmethode verursachen muss.

Kopieren ausgeschlossen

In diesem Zusammenhang sollte erwähnt werden, dass insbesondere das Kopieren von Qubits ausgeschlossen ist. Man kann nach den Gesetzen der Quantenmechanik ein Qubit nicht kopieren, ohne Fehler im Original und der Kopie zu erzeugen, weil die Information in einem Qubit (anolog zu einem Bit) bei diesem Prozess insgesamt erhalten bleiben muss. Nach dem 'Kopiervorgang' muss sich diese aber auf zwei Qubits aufteilen, das Original und die Kopie, sodass die Gesamtinformation erhalten bleibt und die zwei Qubits jeweils weniger als ein Bit Information enthalten, also nicht mehr den richtigen Zustand haben. Deshalb ist der Versuch, eine Kopie des Photons für das Abhören herzustellen und das Original dann an Bob weiterzuschicken nicht möglich, da wieder die Fehlerrate diesen Angriff verrät. Dies bedeutet zugleich aber auch, dass Qubits unterwegs nicht nachverstärkt werden können, was eine starke Einschränkung in der möglichen Distanz der Übertragung darstellt.

Panorama mit der ungefähren Position der Quelle und den Stationen Alice und Bob, die in allgemeinen Räumen des Technik-Areals der Universität Innsbruck untergebracht waren.

Praktische Systeme

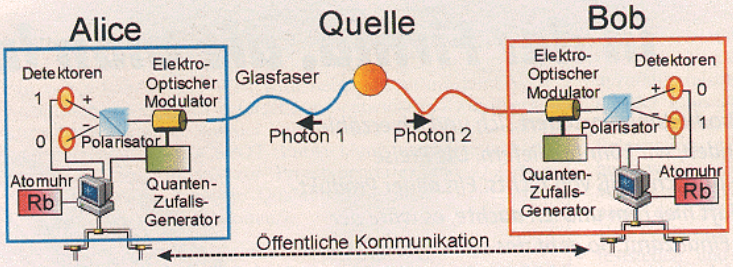
Bei der praktischen Implementation der Quantenkryptographie sind unter anderem zwei wesentliche Bedingungen zu erfüllen: Die Wahl der Polarisation von Alice und die Wahl der Analyserichtung von Bob müssen perfekt zufällig und unvorhersagbar ein und die Photonenquelle darf stets ein, und nur ein, Photon erzeugen. Der perfekte Zufall kann nur mit guten physikalischen Zufallsgeneratoren realisiert werden, da etwa vorgespeicherte oder pseudozufällige Sequenzen immer vorhersagbar sind. Schwieriger zu realisieren ist die Photonenquelle, da eine ideale Einzelphotonenquelle derzeit nicht existiert, wenn auch kürzlich vielversprechende Versuche in dieser Richtung gemacht worden sind [6]. Eine Möglichkeit ist beispielsweise, einen Laserpuls derart abzuschwächen, dass im Mittel weniger als ein Photon pro Puls übrig bleibt (maximal ein Zehntel!), um die Wahrscheinlichkeit für zwei Photonen pro Puls vernachlässigen zu können. Dies dezimiert natürlich die erzielbare Rate an Photonen.

Verschränkte Photonen

Es gibt aber eine sehr gute Möglichkeit, die zwei Kriterien, den Zufall und die Einzelphotonenbedingung, auf einmal zu erfüllen: nämlich durch Einsatz von so genannten verschränkten Photonenpaaren. Diese liefern von Natur aus rein zufällige Messresultate, und die Wahrscheinlichkeit dafür, zwei Paare zugleich zu erzeugen, ist sehr gering. Wir haben auf der Basis von verschränkten Photonen ein komplettes BB84-Quantenkryptographiesystem realisiert, das wir nun im Detail erklären [7, 8]. Verschränkung bedeutet, dass die Polarisationen der beiden Photonen quantenmechanisch korreliert sind, unabhängig von der Distanz zwischen ihnen.

Weshalb gestattet nun die Korrelation von verschränkten Photonenpaaren deren Einsatz in der Quantenkryptographie? Betrachten Sie dazu folgende Situation: Ein Photon wird zu Alice geschickt und das andere Photon zu Bob. Alice und Bob messen beide die Polarisation der bei ihnen eintreffenden Photonen mittels eines Polarisators, der individuell verdreht werden kann. Die Verschränkung der Photonenpaare bewirkt nun, dass bei parallel ausgerichteten Polarisatoren immer entgegengesetzte Ergebnisse gemessen werden, unabhängig von der absoluten Richtung. Wenn also Alice und Bob beispielsweise beide ihre Polarisatoren entlang der 0°-Achse (oder beide auf 45°!) orientieren, so wird, falls Alice das erste Photon im +-Ausgang misst, Bob sein Photon im —Ausgang finden. Eine weitere, wichtige Eigenschaft der Verschränkung ist, dass die +/— beziehungsweise –/+-Kombinationen von Natur aus rein zufällig auftreten (Quanten-Zufall), immer gleich häufig sind und auf keine Weise gesteuert oder vorherbestimmt werden können.

Der perfekte Gegensatz nimmt nun ab, wenn Alice und Bob unterschiedliche Orientierungen für ihre Polarisatoren einsetzen. Bei einer Winkeldifferenz von 45° erhalten Alice und Bob völlig unabhängige Messergebnisse, das heißt auch die +/+ und –/– treten dann gleich häufig und zufällig auf. Oder anders gesagt: Alice und Bob erhalten für sich absolut zufällige Folgen, die je nach Polarisatorstellungen korreliert sind. Die perfekte Antikorrelation der verschränkten Photonenpaare für 0° Winkeldifferenz erzeugt bei Alice und Bob eine identische Zufallsfolge, und das Verschwinden der Korrelation bei 45° Winkeldifferenz bewirkt die Sicherheit in der Übertragung.



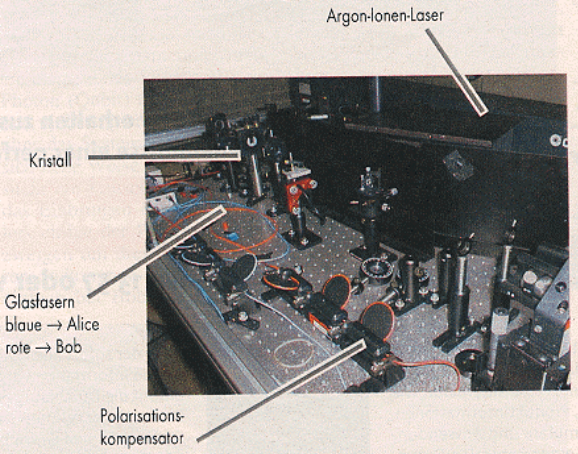
Schematische Darstellung des gesamten Systems: Die öffentliche Kommunikation läuft komplett über das TCP/IP-Netz der Universität.

Generierung des Quantenschlüssels

Um den Quantenschlüssel zu erzeugen, messen Alice und Bob nun für einige Zeit alle eintreffenden Photonen, wobei sie die Orientierung ihres Polarisators zufällig zwischen 0° und 45° hin- und herschalten. Die Messergebnisse (+ oder –) halten sie geheim. Nach Abschluss der Messreihe extrahieren Alice und Bob die Quantenschlüssel aus den Messdaten. Dazu müssen sie über ein nicht manipulierbares, öffentlich zugängliches Medium kommunizieren. Alice und Bob suchen zunächst jene Photonenpaare heraus, die sie zufällig mit gleicher Orientierung der Polarisatoren (0°, 0° oder 45°, 45°) gemessen haben – das ist die Hälfte. Die Messergebnisse halten sie weiterhin streng geheim. Die Verschränkung der Photonen garantiert nun, dass die zugehörigen Ergebnisse eine perfekt entgegengesetzte Abfolge von + und – bilden. Wenn Alice nun die Ersetzung + (r) 1, – (r) 0 vornimmt und Bob + (r) 0, – (r) 1 abbildet, so sind anschließend beide Teilnehmer im Besitz der identischen, zufälligen Bitfolge, dem Quantenschlüssel.

Um den erzeugten Quantenschlüssel zu überprüfen, müssen Alice und Bob ein zufälliges Sample des Quantenschlüssels vergleichen und daraus die statistische Fehlerrate bestimmen. Liegt diese unterhalb des Grenzwertes von 14 %, so ist der Quantenschlüssel absolut sicher, man kann in diesem Fall aus Prinzip ein erfolgreiches Abhören oder Manipulieren der Quanten ausschließen. Wurde diese Hürde erfolgreich geschafft, kann mit dem Schlüssel nach Belieben weitergearbeitet werden. Um vorhandene Bit-Fehler zu dezimieren, kann eine klassische Bit-Korrektur implementiert werden, im einfachsten Fall durch Paritätsprüfung von kleineren Bit-Blöcken. Auf diese Weise erhalten Alice und Bob letztlich einen verkürzten, aber fehlerkorrigierten Schlüssel.

In unserem Quantenkryptographiesystem waren die zwei identischen Detektorstationen Alice und Bob mit Hilfe von Glasfasern an die Photonenquelle gekoppelt. Die Entfernung zwischen Alice und Bob betrug etwa 360 Meter, limitiert



Die Photonenquelle: Damit die Polarisatorausrichtungen rein zufällig ausgewählt werden, stellen zwei Zufallsgeneratoren, die auf dem Quanten-Zufall basieren, mit einer Periode von 100 Nanosekunden eine zufällige Polarisatorrichtung ein.

Glossar

One-Time-Pad Verschlüsselung: Bereits im Jahre 1926 entwickelte G. S. Vernam das 'One-Time-Pad', ein symmetrisches Kryptosystem, welches mit keinerlei statistischen Methoden entschlüsselbar ist. Erzielt wird diese Sicherheit durch den Einsatz von zufälligen Schlüsselsequenzen, die mindestens so groß sein müssen wie die zu übermittelnde Nachricht und nur einmal verwendet werden dürfen. Um eine Nachricht zu verschlüsseln, addiert man bitweise den Schlüssel zur Nachrichten-Zeichenkette (XOR), was zu einer neuen, scheinbar zufälligen Sequenz führt. Für die Dekodierung addiert man neuerlich den Schlüssel bitweise dazu, wodurch die ursprüngliche Nachricht wieder herausfällt. Das 'One-Time-Pad' ist einerseits eine sehr aufwendige Verschlüsselungsmethode, denn es erfordert schließlich eine gleich große Menge an Schlüsseln wie zu übertragende Daten, andererseits aber auch sehr sicher, da statistische Analysen nicht möglich sind, sofern die Schlüssel absolut zufällig sind, sicher übermittelt und nur einmal benutzt wurden. Versucht man die Nachricht durch Ausprobieren von Schlüsselsequenzen zu entdecken, so erhält man alle möglichen sinnvollen und sinnlosen Nachrichten mit der entsprechenden Länge, ohne irgendeinen Anhaltspunkt darüber zu haben, welche die richtige Nachricht ist.

Superposition und Verschränkung: Diese Begriffe bezeichnen den deutlichsten Unterschied zwischen Quantenphysik und klassischer Physik. In der Quantenphysik kann sich ein System zugleich in mehreren verschiedenen Zuständen befinden, was als Superposition bezeichnet wird. Erst bei einer Beobachtung trifft man das System in einem bestimmten Zustand an. Die 'Essenz der Quantenphysik', wie es Erwin Schrödinger genannt hat, offenbart sich aber in der Verschränkung. Dabei sind sogar verschiedene Systeme in einer gemeinsamen Superposition. Es entscheidet dann bereits die Messung an einem System auch den Zustand des anderen Systems (siehe Kasten auf Seite 269).

Quanten-Zufall: In welchem Ausgang des Strahlteilers ein bestimmtes Photon zu finden ist, ist nach der Quantentheorie absolut zufällig und nicht vorherbestimmt (das Photon 'weiß' es nicht einmal selbst), es ist ein echter Quanten-Zufall. Auch die Messergebnisse der einzelnen verschränkten Photonen sind in diesem Sinne ein Quanten-Zufall.

Quanten-Zufallsgenerator: Den Quanten-Zufall am Strahlteiler kann man ausnutzen, um Zufallsgeneratoren zu realisieren. Diese 'Quanten-Zufallsgeneratoren' erzeugen ein sehr schnell und zufällig variierendes digitales Signal abhängig von der Detektion von Photonen im einen oder anderen Ausgang eines Strahlteilers, welches praktisch alle Tests der Zufälligkeit besteht [8]. Das erzeugte Zufallssignal hat eine Autokorrelationszeit von 12 ns und Bitfolgen können mit über 1 MBit/s erzeugt werden. Der Einsatz von 'echtem' Zufall ist entscheidend für die Sicherheit der Quantenkryptographie (analog zur klassischen Kryptographie), da ein Angreifer eine voraufgezeichnete oder algorithmische Zufallssequenz erraten oder gar manipulieren kann und somit die Sicherheit des Systems nicht mehr gegeben ist.

durch die Ausdehnung des Technik-Areals der Universität Innsbruck. Das Herzstück der Photonen-Quelle ist ein Argon-Ionen Laser, der durch einen Beta-Bariumborat-Kristall (BBO) leuchtet und dabei korrelierte Photonenpaare erzeugt, die mittels Glasfasern jeweils zu Alice und zu Bob geführt werden. Da unsere Photonen die unübliche Wellenlänge von 702 Nanometer haben – in diesem Bereich gibt es sehr effiziente Einzelphotonendetektoren, was für die in der Telekommunikationstechnik üblichen Wellenlängen nicht der Fall ist –, mussten eigene Glasfasern installiert werden, die leider auf einer Strecke von 500 Metern bereits die Hälfte der gesendeten Photonen schlucken. Bei Alice und Bob treten die Photonen wieder aus den Fasern heraus, durchlaufen einen schnellen optischen Schalter, der die Analyserichtung bestimmt, und werden anschließend hinter einem Polarisator in dessen beiden Ausgängen mit den Einzelphotonendetektoren registriert.

Elektronik und Software

Trotz Quanteninformatik benötigten wir noch jede Menge klassische Informationsverarbeitung im Experiment. Alice und Bob hatten jeweils einen PC, der die lokalen Parameter steuerte und die Messdaten speicherte. Über TCP/IP konnten die PCs von jedem beliebigen Rechner aus kontrolliert werden. Die Datenerfassung, Steuerung und Kommunikation realisierten wir vollständig in dem grafischen Programmiersystem LabView von National Instruments.

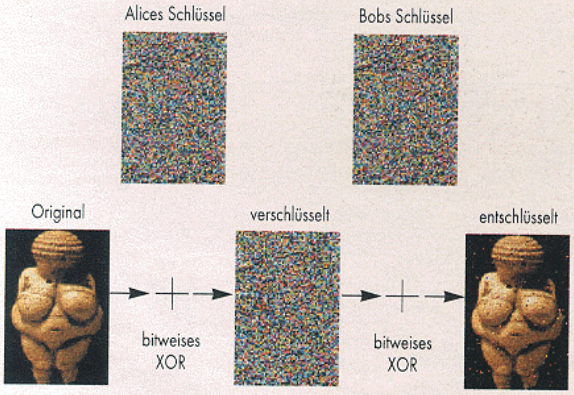
Alice und Bob speichern ihre Photonendetektionen auf ihren jeweiligen lokalen Festplatten, damit erst nach Ablauf einer Messreihe das Protokoll zur Ermittlung des Quantenschlüssels durchgeführt werden kann. Damit Alice und Bob nun ihre detektieren Photonen eindeutig miteinander vergleichen können, müssen sie die Ankunftszeiten der Photonen mit einer Genauigkeit von einer Nanosekunde – dies ist die Detektorauflösung – festhalten. Um eine ausreichende Menge an Photonenpaaren zu erfassen, müssen Alice und Bob außerdem mehrere Minuten lang messen. Diese Genauigkeits- und Stabilitätsanforderungen an die Zeitbasen von Alice und Bob (eine Nanosekunde für einige Minuten) bedingen den Einsatz von synchronisierten Rubidium-Atomuhren bei Alice und Bob. Ein Laserpuls auf einer zweiten Glasfaser synchronisierte beide Zeitbasen zu Beginn jeder Messreihe.

Das Aufzeichnen der Zeitpunkte der Photonendetektion auf eine Nanosekunde genau war für sich eine messtechnische Herausforderung. PC-Einsteckkarten, die eigentlich für den Vergleich von Präzisionsuhren entwickelt worden waren, konnten wir durch Abänderung der Treibersoftware für unsere außergewöhnliche Anwendung einsetzen. Durch die aufwendige Zeitmessung und Protokollierung entstand ein riesiger Datenoverhead: Für jedes registrierte Photon existiert ein 10 Byte großer Zeitstempel, der die Zeitinformation mit 0,1 ns Auflösung beinhaltet, sowie das Messresultat und die jeweilige Ausrichtung des Polarisators. Der effektive Datenoverhead pro erzieltem Bit des Quantenschlüssels war noch viel größer, da wegen systematischer Verluste nur fünf Prozent der von Alice und Bob registrierten Photonen von einem gemeinsamen Paar stammten. Deshalb fielen pro Bit des Quantenschlüssel jeweils rund 200 Byte an Messdaten an. Die Daten belegten nach einigen Messtagen bereits mehrere hundert MByte, und wie zu erwarten, waren sie auch nicht komprimierbar, weil eben zufällig.

Eine sehr schlanke, optimierte C-Routine, die direkt aus der LabView-Umgebung aufgerufen wurde, erledigte das Herausfiltern der gleichzeitigen Ereignisse aus den Rohdaten durch Korrelation von Alices und Bobs Datensätzen. Die gesamte öffentliche Kommunikation, die dafür zwischen Alice und Bob notwendig ist, lief über das vorhandene Netzwerk der Universität in TCP/IP. Es sollte betont werden, dass diese Kommunikation zwischen Alice und Bob, die zur Erzeugung der Quantenschlüssel durchgeführt wird, beliebig offen sein kann, da aus dieser keine Rückschlüsse auf den eigentlichen Quantenschlüssel möglich ist. Genau genommen steigt die Sicherheit sogar, je öffentlicher diese Kommunikation stattfindet.

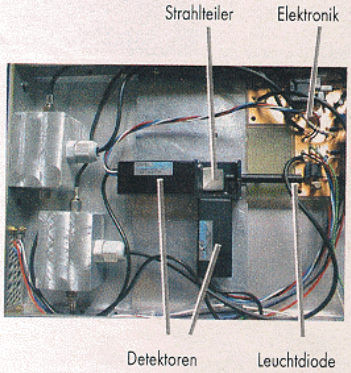
Alles läuft

Erst mit all diesem Rüstzeug war es möglich, das Schlüsselerzeugungsprotokoll vollständig durchführen. So gelang es Alice



Quantenkryptographie in Aktion: Alice kodiert die Farben der Pixel mit ihrem Quantenschlüssel, überträgt das unleserliche Bild an Bob, der das Original durch eine Dekodierung mit seinem Quantenschlüssel wieder erhält.

und Bob, den Quantenschlüssel mit einer Bit-Rate von 850 Bit/s und einer Bit-Fehlerrate von 2,5 Prozent zu erzeugen. Durch eine einfache Fehlerkorrektur mit einer Paritätsüberprüfung wurde die Fehlerrate auf 0,4 Prozent abgesenkt. Das Resultat: ein 50 000 Bit großer Quantenschlüssel. Wie bereits erwähnt, ist der Quantenschlüssel erst die Basis für eine Informationsübertragung mit klassischer Kryptographie. Die sicherste Variante ist die Verwendung des 'One Time Pad'-Protokolls (siehe Kasten). Alice konnte nun ein Bild der 'Venus von Willendorf' an Bob übertragen. Dazu legte sie vorerst ein 60 × 90 Pixel großes Bild mit 8 Bit Farbinformation pro Pixel (60 × 90 × 8 = 43 200 Bit Bildinformation) im Windows-BMP-Format an. Ein Visual-Basic-Programm realisierte nun die Verschlüsselung der Bilddaten nach dem One-Time-Pad-Protokoll, indem je ein Byte des Bildes und des Quantenschlüssels eingelesen, bitweise addiert (XOR-Funktion) und wieder ausgegeben wurde. Dadurch entstand eine neue Bilddatei, die statistisch gesehen eine perfekt zufällige Anordnung von Farbpunkten darstellte und somit keine verwertbare Information mehr enthielt. Dieses wurde über das Netzwerk an Bob verschickt, der mit exakt derselben Routine die empfangene Nachricht mit Hilfe seines Quantenschlüssels dekodiert. Durch das zweimalige bitweise Addieren des Schlüssels zur Nachricht fällt der Schlüssel heraus und gibt die Nachricht wieder frei. Da der Quantenschlüssel von Alice und Bob immer noch circa 0,4 Prozent Bit-Fehlerrate hatte, zeigt Bobs dekodierte Bild einige falsch gefärbte Pixel.



Innenleben eines Quanten-Zufallsgenerators

Um tatsächlich ein absolut sicheres Quantenkryptographiesystem zu realisieren, muss man in der Praxis allerdings noch mehrere Punkte beachten: Um Angriffe durch eine statistische Analyse zu verhindern, spielt der Zufall eine bedeutende Rolle. Hier kommen Alice und Bob die verschränkten Photonen sehr entgegen, da die Messresultate von Natur aus schon zufällig sind. Große Vorsicht müssen die Teilnehmer jedoch beim Umschalten ihrer Analysatoren walten lassen, weil eine vorhersagbare Schaltfolge – zum Beispiel durch einen Pseudozufallsgenerator oder einen schlechten physikalischen Zufallsgenerator – eine Sicherheitslücke darstellt.

Ein wichtiges Problem der klassischen Kryptographie bleibt trotz aller Quantentechnologie bestehen, nämlich die Authentifizierung des Kommunikationspartners. Alice kann zwar gemeinsam mit Bob einen Quantenschlüssel erzeugen, weiß aber dennoch nicht, ob Bob der ist, der er vorgibt zu sein. Nach derzeitigem Wissensstand gibt es keine Möglichkeit, mittels Quantentechnologie die Benutzerauthentifizierung zu verbesseren.

Eine andere Möglichkeit, die Quantenkryptographie zu beeinträchtigen, entstünde, wenn der Angreifer die gesamte Kommunikation zwischen Alice und Bob, also den Quantenkanal und die klassischen Verbindungen, auftrennen und sich unbemerkt zwischenschalten könnte. Unsere beiden Protagonisten können dies verhindern, indem sie sehr weit reichende öffentliche Medien wie etwa Radiosender oder Zeitungsinserate einsetzen. Wir sehen also, dass der klassische Kommunikationsanteil nicht nur offen sein darf, sondern sogar öffentlich sein muss. Natürlich bleiben auch bei Einsatz der Quantenkryptographie allgemeine, potenzielle Sicherheitslöcher erhalten, wie etwa schlecht abgeschirmte Hardware, unberechtigter Zugriff auf gespeicherte Quantenschlüssel durch Hacker oder über Trojaner sowie auch Bedienungsfehler und Nachlässigkeit der Anwender.

Zukunftsmusik?

Was hält eine Bank nun heute noch davon ab, sich so ein kleines Quanten-Kryptographiesystem einbauen zu lassen, um Kundendaten vor fremden Augen und Ohren geschützt zu übertragen? Nun, da ist ein etwas komplexes System von Optik, Argon-Ionen-Laser, Kristall zur Erzeugung von verschränkten Photonenpaaren und Glasfasern zu bedienen, wozu derzeit ein ausgebildeter Quantenoptiker notwendig ist. In mehreren Forschungsprogrammen, wie EQCSPOT (siehe Kasten auf S. 262), wird jedoch daran gearbeitet, die einzelnen Technologien zur Marktreife zu bringen. Unser System erlaubt bereits die Übertragung einer Nachricht über 1000 m und wäre auf eine Glasfaserstrecke von einigen Kilometern erweiterbar. Die Verkabelung des gesamten Finanzzentrums einer Großstadt wäre sicherlich mit dieser Technik zu bewerkstelligen. Eine sehr interessante Variante benutzt die Übertragung der Photonen im freien Raum, wobei Sender und Empfänger mit Teleskopen ausgestattet sind. Nach heutigem Stand wäre bereits auch eine Übermittlung von Photonen zu einem Satelliten beziehungsweise zwischen Satelliten möglich.

Teilchenspeicher

Den wirklichen Durchbruch der Quantenkryptographie und anderer Quantennetzwerke könnte jedoch die Entwicklung von lange speicherbaren verschränkten Teilchen mit sich bringen. Dies erlaubt etwa zwei Teilnehmern je einen Speicher mit verschränkten Teilchen mit sich zu tragen und zu einem beliebigen späteren Zeitpunkt an einem beliebigen Ort daraus einen Quantenschlüssel zu generieren. Man kann dann sogar die gespeicherten verschränkten Teilchen mit einem herkömmlichen, ungesicherten Kurierdienst an die zwei Teilnehmer versenden, weil ja nach dem Prinzip der Quantenkryptographie die Teilnehmer jegliche Manipulation, oder einen Versuch, die verschränkten Teilchen irgendwie anzuzapfen, feststellen werden.

Man könnte sich auch vorstellen, mehrere Teilnehmer kaufen bei einem Provider einen Satz Teilchen, die jeweils verschränkt sind mit Teilchen,

welche noch beim Provider gespeichert sind. Möchte nun Teilnehmer A mit Teilnehmer B eine Quantenkryptopraphieverbindung aufbauen, so melden sich beide beim Provider an und dieser verschränkt die zu A und B gehörigen gelagerten Teilchen miteinander. Darauf sind automatisch die Teilchen von A mit denen von B verschränkt und ein Quantenschlüssel kann erzeugt werden. Dieser Vorgang wird als 'Entanglement Swapping' bezeichnet, eine Verallgemeinerung der Quanten-Teleportation. Die Möglichkeiten der Informationsverarbeitung mittels gespeicherter Qubits sind vom jetzigen Standpunkt in ihrer Tragweite heute nur schwer zu erahnen. Es sind bereits mehrere Forschungsinstitute rund um den Globus auf der Suche nach solchen Qubitspeichern. Mögliche Kandidaten sind etwa eingefangene Atome oder Bose-Einstein-Kondensate.

Die Quanteninformatik ist ein sehr neuer und stark wachsender Forschungszweig, der sicherlich noch viele Überraschungen bereithält. Daher setzt die Forschung alles daran, möglichst viel über deren ungewöhnlichen Fähigkeiten zu erfahren, und neue Einsatzmöglichkeiten zu entdecken. Jedenfalls ist bereits heute vorstellbar, dass die Methoden der Quanteninformatik, wie etwa die verschränkten Photonen, ein Bestandteil der Kommunikationstechnologie von morgen sein könnten. (wst)

Anton Zeilinger ist seit 1999 Professor am Institut für Experimentalphysik der Universität Wien. Gregor Weihs und Thomas Jennewein arbeiten als wissenschaftliche Mitarbeiter in der Arbeitsgruppe 'Quantum Experiments and the Foundations of Physics' von Professor Zeilinger.

Literatur

[1] Jürgen Rink, Alice im Wunderland, c't 3/97, S. 110

[2] Jürgen Rink, Quäntchen für Quäntchen, c't 16/98, S. 150

[3] Jürgen Kirchner, Vom Bit zum Qubit – Neues vom Quantencomputer, c't 11/99, S. 44

[4] S. Wiesner, SIGACT News 15, 78 (1983)

[5] C. Bennett, G. Brassard, A. Ekert, Quantum Cryptography, Scientific American, 50, Oct. 1992

[6] Wolfgang Stieler, Häppchenweise Licht, c't 2/2001, S. 44

[7] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, Quantum Cryptography with Polarization Entangled Photons, Physical Review Letters, 84, (2000) bzw. als Preprint auf http://xxx.lanl.gov/abs/quant-ph/9912117

[8] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, A. Zeilinger, A Fast and Compact Quantum Random Number Generator, Rev. Sci. Inst. 71, 1675-1680 (2000) beziehungsweise als Preprint auf http://xxx.lanl.gov/abs/quant-ph/9912118

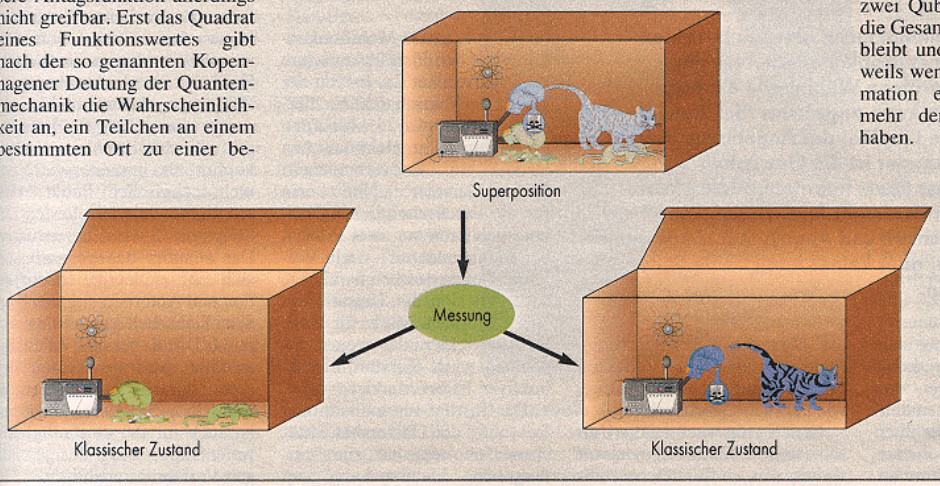
Schrödingers Katze und das Qubit

Quanteninformatiker rechnen mit Qubits – einer für die Alltagserfahrung gespenstisch wirkenden Überlagerung von 0 und 1. Die Quantentheorie kann solche Zustände zwar beschreiben; über die Interpretation dieser Beschreibung diskutieren Physiker aber seit den zwanziger Jahren.

An Stelle einer Bewegungsgleichung, die beschreibt, an welchem Ort zu welcher Zeit sich ein Teilchen befindet, tritt die Schrödingergleichung mit der so genannten Wellenfunktion. Die Wellenfunktion ergibt eine komplexe Zahl – eine komplexe Funktion ist für unsere Alltagsfunktion allerdings nicht greifbar. Erst das Quadrat eines Funktionswertes gibt nach der so genannten Kopenhagener Deutung der Quantenmechanik die Wahrscheinlichkeit an, ein Teilchen an einem bestimmten Ort zu einer bestimmten Zeit zu finden. Eine genaue Vorhersage, wo sich das Teilchen exakt aufhält, ist praktisch nie möglich.

Zu welchen verblüffenden Folgerungen das führen kann, versuchte Erwin Schrödinger um 1935 mit einem 'Schrödingers Katze' genannten Gedankenexperiment zu zeigen: In einer geschlossenen Kiste befindet sich eine Katze und ein radioaktives Atom, von dem wir nicht genau wissen, wann es zerfällt. Wenn das aber passiert, setzt ein Detektor über ein Relais eine tödliche Substanz frei. Die Quantentheorie lehrt, dass die Katze gleichzeitig 'tot' und 'lebendig' ist, solange die Kiste ungeöffnet bleibt. Erst die Messung, also das Öffnen der Kiste, gibt preis, ob die Katze noch lebt. Offensichtlich steht das Gedankenexperiment mit der Wirklichkeit im Widerspruch, denn wir beobachten entweder nur tote oder lebendige Katzen. Der Widerspruch löst sich, wenn man berücksichtigt, dass Systeme nie isoliert von ihrer Umgebung sind. Sie folgen damit nicht streng der Schrödingergleichung, die nur geschlossene Systeme beschreibt. Die Wechselwirkung mit der Umgebung zerstört die Superposition.

Übrig bleibt ein einziger Zustand, wie wir ihn aus unserer Alltagswelt kennen. Den zahlreichen Interpretationen der Quantenmechanik hat Anton Zeilinger eine weitere hinzugefügt: Er schlägt vor, die Quanten-Realität mit Hilfe elementarer Systeme zu beschreiben, die genau ein Bit Information enthalten. Diese Information muss bei Operationen, die auf das System wirken, erhalten bleiben. Ein polarisiertes Photon, das ein Qubit Information 'transportiert', kann man somit nicht 'abhören', ohne Fehler im Original und der Kopie zu erzeugen. Nach dem 'Kopiervorgang' muss sich diese aber auf zwei Qubits aufteilen, so dass die Gesamtinformation erhalten bleibt und die zwei Qubits jeweils weniger als ein Bit Information enthalten, also nicht mehr den richtigen Zustand haben. (wst)



Schrödingers Katzen leben länger: Erst nach einer Messung ('Deckel auf') zerfällt die Superposition von 'tot' und 'lebendig' in einen definierten klassischen Zustand.