Damit Geheimes auch geheim bleibt

QUANTENMECHANIK ERMÖGLICHT ABHÖRSICHERE KOMMUNIKATION

Geheime Informationen auch wirklich nur demjenigen zukommen zu lassen, für den sie bestimmt sind, daran liegt Banken, Firmen, Geheimdiensten und Militärs viel. Doch mindestens genauso viel liegt anderen daran, diese verschlüsselten Informationen zu dechiffrieren. Am Institut für Theoretische Physik wird daran gearbeitet, mit Hilfe der Quantenmechanik eine wirklich sichere Verschlüsselungsmethode weiterzuentwickeln.

Auch wenn der Glanz der »New Economy« und der Glaube an die Internet-Start-Ups in den letzten Monaten etwas verblasst ist, leben wir in einer Zeit, in der weltweite Kommunikation und Informationsübertragung immer wichtiger werden. Während man sich als »normaler« Internetnutzer meist wenig Sorgen über Datensicherheit macht, treten jedoch auch bei Otto-Normalsurfer schnell Fragen nach der Vertraulichkeit auf: So möchte man Gewissheit haben, dass beim Bezahlen mit der Kreditkarte niemand die Geheimnummer mitlesen kann; eben so wenig möchte man seinen Kontostand preisgeben und vielleicht verschickt man hin und wieder E-Mails, die man auch mit der klassischen Post nicht als Postkarte, sondern als versiegelten Brief verschickt hätte. Verständlicherweise haben gerade Organisationen, die von Natur aus als verschwiegen gelten, wie Banken, große Konzerne und Militärs, ein noch größeres Interesse an der Vertraulichkeit ihrer Geheimnisse.

Die Wissenschaft, die sich mit der Geheimhaltung und der sicheren Übermittelung von Daten beschäftigt, nennt sich Kryptografie.

Kryptografie ist eine sehr alte Wissenschaft.

Die Verschlüsselungsmaschine »Enigma« wurde von den Deutschen im Zweiten Weltkrieg benutzt. Aber auch schon von Cäsar ist übermittelt, dass er eine einfache

Krypto-Technik benutzte, um geheime Befehle an seine Getreuen zu schicken: Um den Text zu verschlüsseln, wurde jeder Buchstabe, durch den ihm im Alphabet folgenden ersetzt, also aus »A« wurde »B«, aus »E« wurde »F« und so weiter. Leider lässt sich die Nachricht leicht entschlüsseln, hat man erst einmal den Trick herausgefunden.

Die so genannte »Vernam-Verschlüsselung«, 1918 entwickelt von Gilbert Vernam für das amerikanische Militär, geht einen Schritt weiter.

Die zwei Personen, man nenne sie »Alice« und »Bob«, die sich geheim unterhalten wollen, einigen sich bei einem gemeinsamen Treffen auf eine Zufallsfolge von Zahlen. Dieser Schlüssel muss den beiden

bekannt sein, aber niemand sonst darf Information darüber haben, sprich, es ist eine geheime Zufallsfolge.

Dann benutzen sie eine Erweiterung der Cäsar-Verschlüsselung: Jeder Buchstabe des Textes wird nicht nur um einen Buchstaben verschoben, sondern um so viele, wie es die entsprechende Zahl des Schlüssels angibt.

Da das Alphabet aus 26 Buchstaben besteht, kann das schon ziemlich unübersichtlich werden.

Einfacher wird es, wenn man die Nachricht in Binärzahlen, also in »0« und »1« übermittelt; es ist immer möglich, einen Text zu Binärzahlen hin- und zurück zu verwandeln. In dieser Binärsprache bedeutet eine Null im Schlüssel, dass die gesendete Zahl einfach bestehen bleibt (um Null »verschoben« wird) und eine Eins, dass die zusendende Zahl umgedreht (Eins nach Null, Null nach Eins) wird.

Ein Beispiel:

Text:
1 0 0 1 1 0 1 1 0 1 0 1
Schlüssel:
1 0 1 0 0 0 1 0 1 1 0 1
Geheimnachricht:
0 0 1 1 1 0 0 1 1 0 0 0

Tatsächlich ist dieses Verfahren absolut sicher, solange nur Alice und Bob den Schlüssel kennen, dieser mindestens so lang ist wie die Nachricht und nur einmal benutzt wird.

Aber genau hierin liegt auch das Problem dieses ansonsten so einfachen Verfahrens: Bevor man gesichert kommunizieren kann, muss man einen Schlüssel gesichert austauschen; das Problem wird im Grunde nur auf den Schlüsselaustausch verlagert.

Eine Möglichkeit, über diesen Nachteil hinweg zu kommen, bilden »Public-Key-Verfahren«, bei denen die Nachricht mit einem öffentlich bekannten Schlüssel verschlüsselt wird und nur mit dem privaten, dem Empfänger bekannten Schlüssel entschlüsselt werden kann.

Diese Verfahren sind in den letzten dreißig Jahren von der Mathematik entwickelt worden; die bekanntesten Verfahren sind RSA [Referenz 3], benannt nach seinen drei Entwicklern und DES (Data Encryption Standard). Beide nutzten eine so genannte »Falltür«-Eigenschaft von bestimmten mathematischen Problemen, die besagt: Es gibt Probleme, die lassen sich nur unter größtem Zeitaufwand lösen, hat man jedoch eine vermeintliche Lösung, so lässt sich schnell überprüfen, ob sie richtig ist. Die Zerlegung großer Zahlen in Primfaktoren ist solch ein Problem, auf dem auch das RSA Verfahren aufbaut.

Public-Key-Verfahren sind inzwischen weit verbreitet, so nutzen alle gängigen Internetbrowser diese Technik, um beispielsweise beim Homebanking die Daten geheim zu halten.

Dennoch hat auch dieser Verschlüsselungsansatz einen Nachteil: Es ist nicht bewiesen, dass das zugrunde liegende mathematische Problem wirklich so schwer zu lösen ist, dass es die Sicherheit der Nachricht garantiert. Darüber hinaus stellt die Quantenmechanik – speziell durch in möglicherweise mittlerer Zukunft verfügbare Quantencomputer – einen Angriff auf solche Verfahren dar, weil gerade ein Quantencomputer das zugrunde liegende Faktorisierungsproblem und damit die Nachricht selbst besonders schnell knackt.

Glücklicherweise stellt die Quantenmechanik mit ihren ungewöhnlichen Eigenschaften nicht nur eine Bedrohung für die Public-Key-Kryptografie dar, sondern weist auf der anderen Seite auch gleich einen Weg zu sicheren Verschlüsslungsverfahren.

Die Idee besteht darin, das »Vernam«-Verfahren zu erweitern. Das Grundproblem dort war, auf sichere Art und Weise einen Schlüssel auszutauschen; ist dieser Austausch geheim gelungen, ist absolute Sicherheit garantiert.

Nun hat die Quantenmechanik eine Eigenschaft, die hierfür besonders gelegen kommt. Sie besagt, etwas vereinfacht, dass jede Messung an einem System, die man ausführen muss, um Information zu gewinnen, auf das System zurückwirkt und dieses stört.[1] Diese Störung ist von fundamentaler physikalischer Natur und lässt sich nicht vermeiden oder rückgängig machen.

Alice und Bob, die vor dem eigentlichen Nachrichtenaustausch einen Schlüssel tauschen wollen, gehen so vor:

- Alice erzeugt als Schlüssel für das Vernam-Verfahren eine zufällige Binärzahlenfolge. Dann präpariert sie, abhängig davon, ob sie Bob eine 1 oder 0 schicken will, ein quantenmechanisches Teilchen in einem bestimmten Quantenzustand, der zu 1 oder 0 korrespondiert. Beispielsweise könnte sie Lichtteilen, also Photonen, in verschiedenen Polarisationen erzeugen.
- Dieses Teilchen schickt sie dann zu Bob, der mit einer Messung herauszufinden versucht, ob Alice eine 0 oder eine 1 kodiert hat.

Es liegt an den Gesetzen der Quantenphysik, welche letztendlich die Sicherheit dieses Verfahrens begründen, dass Bob nicht bei jedem übertragenen Teilchen entscheiden kann, welche Zahl Alice schicken wollte.

Das ist jedoch kein Problem, da die beiden in diesen Fällen die übertragene Zahl verwerfen und nicht in ihrem Schlüssel verwenden.

Dieser Vorgang nennt sich »Aussieben« und da es sich um einen Zufallsschlüssel handelt, ist es egal, wenn einige Bits verworfen werden.

1 Die Autoren sind sich bewusst, dass es so genannte »non-demolition-measurements« gibt, bei denen Information ohne Störung gewonnen wird. Dies ist aber nur bei speziell im voraus präparierten Quantensystemen möglich; die Quantenkryptografie nutzt gerade Systeme, die nicht so präpariert sind.

Abbildung 1
Die Verschlüsselungsmaschine »Enigma«
Foto: Jan Braun, Heinz Nixdorf MuseumsForum

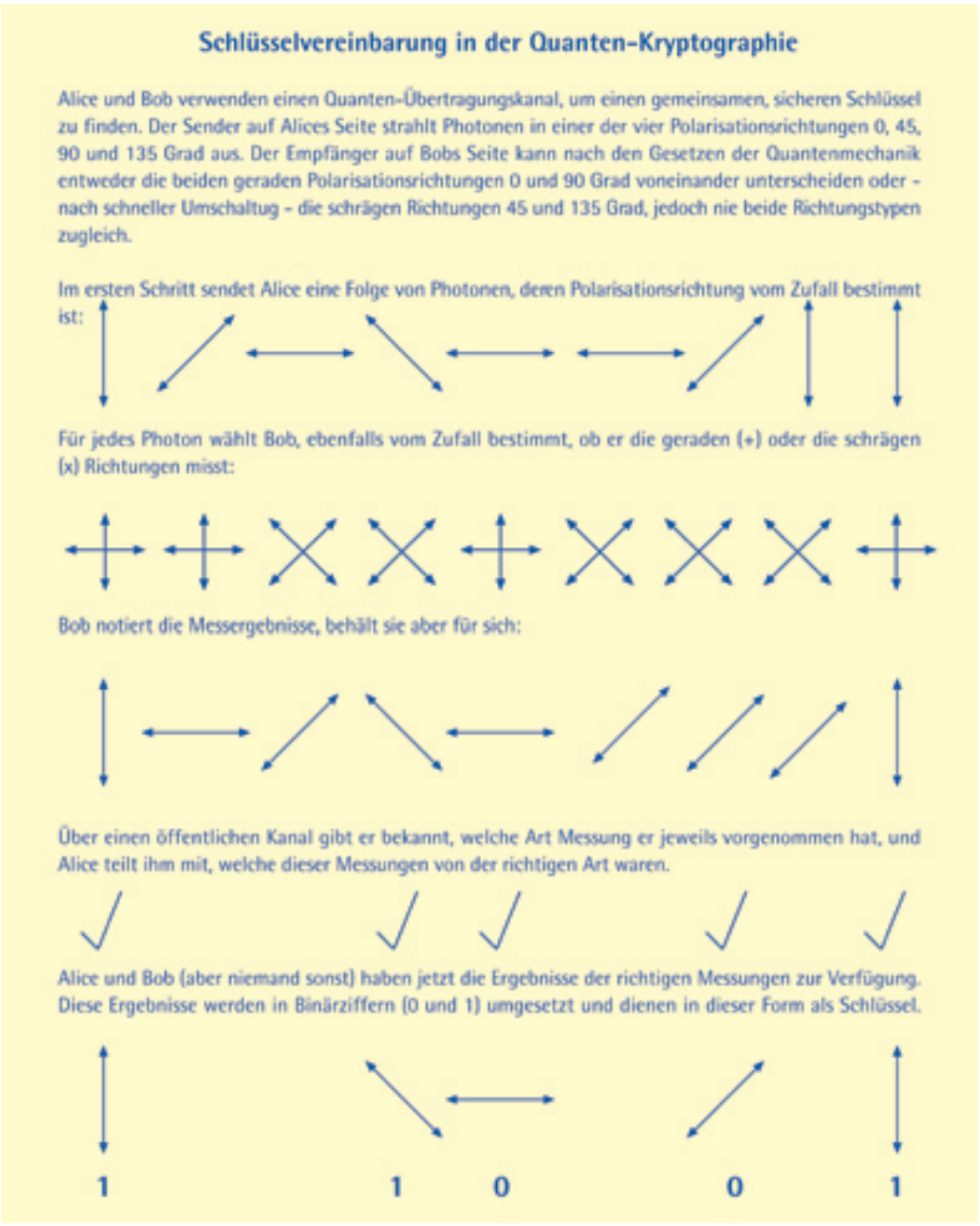


Abbildung 2
Grafik »Schlüsselvereinbarung in der Quanten-Kryptographie«

Abbildung 3 (rechts)
Eine Photonenpaar-Quelle übermittelt Quantenschlüssel per Glasfaserkabel über große Distanzen. An der Universität Genf werden solche Verfahren erforscht.
Foto: Hugo Zbinen, Université Genève

Abbildung 4 (ganz rechts)
Ein quantenmechanisches Verschlüsselungsset auf dem Weg zur Serienreife.
Foto: id Quantique SA

Nachdem Alice alle ihre Ziffern übertragen und unerkannte Bits ausgesiebt wurden, teilen sich Alice und Bob idealerweise identische Schlüssel - »idealerweise« deshalb, weil an der Leitung ein Lauscher mitgehört haben könnte, und dieser hätte notgedrungen die Übertragung stören müssen.

Aus Tradition hat auch die Lauscherin in der Informationswissenschaft einen Namen bekommen: Sie heißt Eve, nach dem englischen »eavesdropping« (dt: Lauschen).

Alice und Bob werden nun Teile ihres Schlüssels vergleichen. Stellen sie dabei fest, dass keine Fehler auftreten, können sie sicher sein, dass die Übertragung unbelauscht und geheim vonstatten ging.

Das garantiert gerade das Prinzip, dass jede zur Informationsgewinnung nötige Messung Störungen erzeugt und somit auch Fehler in Bobs Schlüssel. Ist der Schlüssel aber fehlerfrei und damit schlussendlich auch geheim übertragen worden, kann man ihn für das Vernam-Verfahren nutzen und geheim kommunizieren. Der Rückschluss »Keine Störung —> Geheime Übertragung des Schlüssels« ist das entscheidende Merkmal, das die Quantenmechanik zur Kryptografie beiträgt.

Es sind in den letzten Jahren verschiedene quantenmechanische Protokolle vorgeschlagen worden, die zum sicheren Austausch von Schlüsseln verwendet werden können.

Sie unterscheiden sich im wesentlichen dadurch, auf welche Weise Alice eine 0 oder 1 in einem bestimmten physikalischen System kodiert.

Der älteste Vorschlag ist das BB84-Protokoll [Verweis Referenz 4], bei dem Alice jeweils zwei zufällig zu wählende Möglichkeiten hat, eine 0 oder 1 zu kodieren, sie nutzt also insgesamt vier verschiedene Zustände, die üblicherweise als Polarisationen eines Photons realisiert werden.

In der Grafik erkennt man das Grundprinzip, wie man mit verschieden ausgerichteten Polarisationen Zahlen übertragen kann.

Weitere Protokolle sind eine Verallgemeinerung von BB84 auf sechs Zustände oder das so genannte B92-Protokoll, das nur zwei, dafür aber nicht-orthogonale Zustände benutzt.

Die Güte oder auch Sicherheit verschiedener Implementierungen unterscheidet sich vor allem in der Charakteristik, wie viel Information Eve gewinnen kann, wenn sie eine festgelegte Störung nicht überschreitet.

Je mehr Störung ein Lauscher erzeugen muss, um Information über die ausgetauschten Schlüssel zu erlangen, desto sicherer ist das Verfahren.

Die Charakteristik zwischen erzeugter Störung und Informationsgewinn trägt in der englischen Literatur den bezeichnenden Ausdruck »Trade-off«.

Die genaue, quantitative Untersuchung dieses Trade-offs ist der wichtigste Schritt, um die Sicherheit eines Protokolls zu beweisen.

Dabei steht man vor der Schwierigkeit, dass man, um absolute Sicherheit nachzuweisen, Eve als technisch bestmöglichst ausgerüstet annehmen muss – sprich, sie kann versuchen, jeden Lauschangriff zu starten, der nicht aufgrund physikalischer Gesetze unmöglich ist. Diese starke Forderung führt zu mathematisch komplexen Szenarien. Man behilft sich typischerweise damit, Eves Möglichkeiten einzuschränken auf die Technologie, die in absehbarerer Zeit verfügbar sein wird.

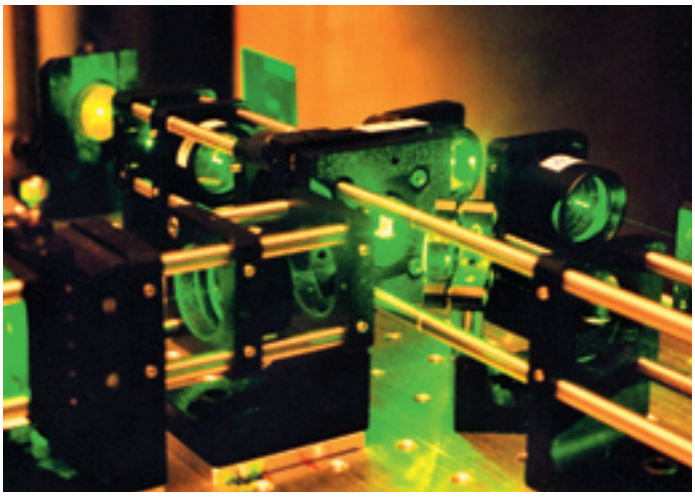
Dennoch stellen diese leicht vereinfachten Untersuchungen einen wichtigen Schritt hin zu dem Beweis ultimativer Sicherheit dar.

Prof. Dr. Maciej Lewenstein
Jahrgang 1955, ist Leiter der Abteilung Theoretische Quantenoptik des Instituts für Theoretische Physik.

Dr. habil. Dagmar Bruß
Jahrgang 1963, ist Oberassistentin in der Abteilung Theoretische Quantenoptik des Instituts für Theoretische Physik.

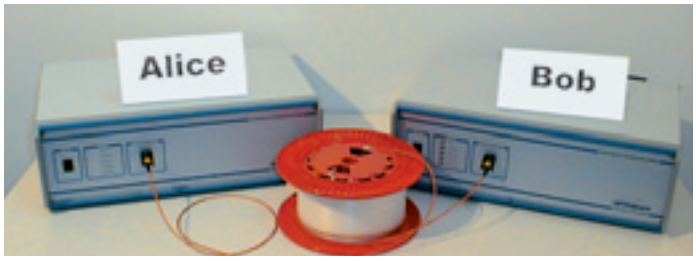
Normann Plaß
Jahrgang 1975 ist Diplomand in der Abteilung Theoretische Quantenoptik des Instituts für Theoretische Physik.

Mit einer ähnlichen Technik wurden unter Laborbedingungen bereits Entfernungen von bis zu 67 Kilometern überwunden. Im Los Almanos National Laboratory wurden einzelne Lichtteilchen auf einer Distanz von zehn Kilometern durch die freie Atmosphäre verschickt. Man hofft, damit letztendlich Quantenkanäle von und zu Satelliten aufbauen zu können.



Grundlegende Arbeiten über Messungen an korrelierten Systemen oder über die Sicherheit der Sechs-Zustands-Variante von BB84 sind Schritte auf dem Weg zum Beweis absoluter Sicherheit.

Diese Fortschritte entstanden in einem Umfeld vielfältiger quantenmechanischer Grundlagenforschung, die das Fundament für die aktuelle quantenkryptografische Entwicklung bildet.



Tatsächlich sind quantenkryptografische Konzepte, die aus der theoretischen Physik entstammen, inzwischen experimentell realisiert worden; teilweise steht man sogar kurz vor kommerziell einsetzbaren Systemen.

Die Universität von Genf hat eine Firma [Referenz 5] gegründet, die handliche Geräte vertreibt, die den Schlüssel über Glasfaserkabel austauschen – dazu können auch bestehende Glasfaserleitungen der Telekommunikation genutzt werden.

Die Arbeitsgruppe um Professor Maciej Lewenstein an der Universität Hannover beschäftigt sich auch mit der Analyse quantenkryptografischer Protokolle.

Unter anderem wurden verallgemeinerte Protokolle in höheren Dimensionen vorgeschlagen und untersucht.

Referenzen

1. Singh, S.: The Code Book; Anchor Books, August 2000; ISBN: 0385495323
2. Spektrum der Wissenschaft: »Dossier Kryptografie«; 4/2001
3. Rivest, R. L., Shamir, A., Adleman, L. A.: A method for obtaining digital signatures and public-key cryptosystems; Communications of the ACM, Vol. 21, Nr. 2, 1978, S.120–126. Oder: http://theory.lcs.mit.edu/~cis/pubs/rivest/rsapaper.ps
4. C. H. Bennett, G. Brassard: »Quantum cryptography: Public Key Distribution and Coin Tossing«; Proc. IEEE »International Conference on Computers, Systems and Signal Processing«, 1984, S. 175–179
5. http://www.idquantique.ch
6. Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., Review of Modern Physics 74, 145 (2002)