brauchen, um die Theorien quantitativ verifizieren zu können.

HANS J. HERRMANN

**Prof. Dr. Hans Herrmann, Institut für Computeranwendungen der Universität Stuttgart, Pfaffenwaldring 27, 70569 Stuttgart**

[1] *A.L. Washburn*, Geol. Soc. Am. Bull. **67**, 823 (1956)
[2] *M.A. Kessler* und *B.T. Werner*, Science **299**, 380 (2003)
[3] *K. Kroy, G. Sauermann, H.J. Herrmann,* Phys. Rev. Lett. **88**, 054301 (2002)
[4] *H.A. Makse, S. Havlin, P.R. King* and *H.E. Stanley*, Nature **386**, 379 (1997)

## Mehr Sicherheit durch Quantenschlüssel

Das Bestreben der Menschen, Botschaften möglichst geheim verschicken zu können, ist so alt wie die Menschheit selbst [1]. Die kryptografischen Methoden wurden mit der Zeit immer ausgefeilter und haben nicht nur in sicherheitstechnischen Bereichen, sondern auch im Geschäftsleben eine besonders hohe, nicht zu unterschätzende Bedeutung. Bereits seit einigen Jahren sind kryptografische Verfahren in der Diskussion, die auf den speziellen Eigenschaften von Quantensystemen beruhen, etwa von nicht-orthogonalen Polarisationszuständen schwacher Lichtpulse oder von Paaren einzelner Photonen, die miteinander korreliert (verschränkt) sind.[1)] Nun ist es Frédérik Grosshans et al. gelungen zu zeigen, dass auch intensive Lichtfelder eine Quantenkryptografie ermöglichen, die zudem schneller und effizienter ist [2].

1) vgl. *H. Briegel,* Phys. Blätter, Juni 2000, S. 12 *W. Tittel, J. Brendel, N. Gisin, G. Ribordy* und *H. Zbinden*, Phys. Blätter, Juni 1999, S. 25

Bei der einzigen gemeinhin als absolut sicher geltenden Methode muss der Datensatz mit einem Zufallsdatensatz gleicher Länge verschlüsselt werden. Dieser Schlüssel darf aber nur einmal verwendet werden (*one time pad*). Das Problem bei diesem Verfahren ist der Austausch des geheimen Schlüssels zwischen Empfänger und Sender. Wenn die Sicherheitsstufe es erlaubt, wird heute oft das vergleichsweise einfache, aber um so wirksamere Verfahren des öffentlichen Schlüssels (*public key*) verwendet. Es beruht darauf, dass es Rechenaufgaben gibt, die in der einen Richtung vergleichsweise einfach und damit schnell durchzuführen sind, in der anderen aber unvergleichlich viel schwieriger. Diese Komplexität der Berechnung wird danach bewertet, ob die benötigte Rechenzeit polynomial oder exponentiell von der Größe der Zahl im Eingangsregister abhängt. Ein Beispiel ist die Multiplikation zweier ganzer Zahlen und deren Umkehrung, die Faktorisierung. Für die schwierige Richtung sind zwar keine Algorithmen bekannt, die auf herkömmlichen Rechnern effizient, d. h. in polynomialer Zeit ablaufen, aber es gibt bislang auch keinen mathematischen Beweis dafür, dass solche Algorithmen nicht existieren. Ein gewisses Unbehagen bleibt. Hinzu kommt, dass ein Quanten-Computer, der die besonderen Eigenschaften quantenmechanischer Systeme ausnutzt, die bekannten „schwierigen" Probleme effizient lösen kann. Ein solches Quanten-Rechenwerk für Spezialaufgaben gibt es zwar noch nicht und wird es wohl auch in absehbarer Zeit nicht geben, aber aus all den genannten Gründen steht hinter der heute kommerziell erwerbbaren Sicherheit ein kleines Fragezeichen.

Die Quantentheorie stellt der Kryptografie mit dem Quanten-Rechenwerk ein Bein; sie bietet aber auch einen Ausweg. Ein einzelnes unbekanntes Quantensystem, dessen mögliche Zustände nicht orthogonal sind, lässt sich durch eine Messung nicht vollständig charakterisieren. Damit Hand in Hand geht die Unmöglichkeit, ein unbekanntes Quantensystem exakt zu klonen bzw. davon eine Kopie anzufertigen. Das kanonische Beispiel hierfür ist ein einzelnes Photon, das in einer Überlagerung zweier unterschiedlicher Zustände vorliegt. Dies können z. B. zwei orthogonale lineare Polarisationszustände sein. S. Wiesner hatte die Idee, die besonderen Eigenschaften derartiger einfachster Quantenobjekte für die absolut geheime Verteilung kryptografischer Schüssel auszunutzen. Ein unerwünschter Mithörer kann zwar versuchen, die Botschaft abzufangen, aber er wird das Quantenobjekt, also z. B. das Photon, durch seine Messung so verändern, dass er nicht unentdeckt bleiben kann. Außerdem gibt es Verfahren in der (klassischen) Kryptografie, die einen geheimen Schlüssel aus den Korrelationen zwischen Sender und Empfänger „herausdestillieren" können. Dabei werden zunächst Fehler korrigiert, und dann mögliche Korrelationen mit einem Mithörer mittels sog. *privacy amplification* abgebaut [3]. Eine notwendige Voraussetzung dafür ist, dass die Korrelationen zwischen Empfänger und Sender noch quantenmechanische Züge tragen. Letztes Jahr erst ist es dem Team um Harald Weinfurter gelungen, von der Zugspitze aus einen geheimen Schlüssel zu einem 21 km entfernten Empfänger zu übertragen [4]. Und gerade erschien die Beschreibung eines neuen Experiments, das wesentlich für die Weiterentwicklung der Quanten-Schlüsselverteilung ist: die Teleportation eines Photons über 2 km [5]. Dabei handelt es sich um die Übertragung der Quantenstruktur von einem Photon der Wellenlänge 1,3 $\mu$m auf ein anderes der Wellenlänge 1,55 $\mu$m. Die Teleportation könnte es ermöglichen, künftig kryptografische Schlüssel über noch größere Distanzen zu verteilen.

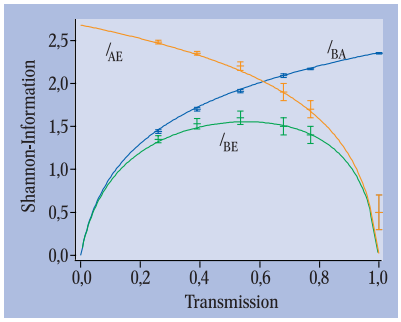
All diese Experimente benutzen (näherungsweise) einzelne Lichtquanten. Das stellt besondere Anforderungen an die Lichtquellen und begrenzt auch die Übertragungsrate. Vor kurzem wurde jedoch theoretisch gezeigt, dass Quanten-Schlüsselverteilung auch mit intensiven Lichtfeldern möglich ist, die viele Photonen pro Messzeitintervall enthalten. Solche Felder werden am besten durch kontinuierliche Quantenvariablen beschrieben, z. B. Amplitude und Phase. Es stellte sich heraus, dass sogar kohärente Laserfelder geeignet sind, die keine nichtklassischen Eigenschaften besitzen. Aber noch vor Jahresfrist wurde vermutet, dass die Schlüsselverteilung mit kohärenten Zustände nur möglich sei, wenn die Verluste auf der Übertragungsstrecke kleiner als 50 % sind. Seitdem sind zwei unterschiedliche Methoden zur Überwindung auch dieser Grenze gefunden worden, die beide das klassische Protokoll der *privacy amplification* benutzen, um einen geheimen Schlüssel aus geteilten Korrelationen herauszudestillieren. Dabei darf der Mithörer nach einer geeigneten Fehlerkorrektur keine vollständige Information über die korrigierten Korrelationen besitzen. Die Methoden unterscheiden sich darin, wie dieser Informationsvorsprung gegenüber dem Mithörer entsteht. Dieser Unterschied bezieht sich auf verschiedenen Fehlerkorrekturverfahren. In manchen Verfahren werden die Positionen von Fehlern durch interaktive Protokolle bekannt (bidirektional). Dies ist nicht der Fall bei der starren unidirektionalen Methode, die dafür den Nachteil hat, nicht effizient zu sein.

Die wesentliche Größe ist die gemeinsame Information, die zwei

**Prof. Dr. Gerd Leuchs, Priv.-Doz. Dr. Natalia Korolkova und Dr. Norbert Lütkenhaus, Zentrum für Moderne Optik, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen**

Partner teilen, die Shannon-Information. Bei drei Partnern Sender (A), Empfänger (B) und Mithörer (E) gibt es drei unterschiedliche Shannon-Informationen, $I_{AB}$, $I_{AE}$ und $I_{BE}$. Die Möglichkeit der sicheren Schlüsselverteilung hängt davon ab, wie sich diese drei Shannon-Informationen zueinander verhalten. Diese Größen lassen sich einfach berechnen, wenn man annimmt, dass der gesamte Signalverlust auf der Strecke dem Mithörer zuzuschreiben ist (Abb.). Bei der Transparenz 1, d. h. ohne Verluste auf der Strecke, hat der Mithörer keine Information, $I_{AB} = I_{max}$, $I_{AE} = 0$ und $I_{BE} = 0$. Bei 50 % Verlusten haben der Mithörer und der Empfänger im Idealfall gleich viel gemeinsame Information mit dem Sender, $I_{AB} = I_{AE}$. Im anderen Grenzfall ist die Strecke nicht transparent und der Empfänger erhält keine Information des Senders, $I_{AB} = 0$, $I_{AE} = I_{max}$ und $I_{BE} = 0$. Die Standard-Techniken zur Destillation eines gemeinsamen Schlüssels beinhalten bidirektionale Fehlerkorrektur und greifen, falls $I_{AB} > \max\{I_{AE}, I_{BE}\}$, d. h. bei genügend großer Transparenz. Bei größeren Verlusten wird $I_{AB}$ kleiner als $I_{AE}$, bleibt aber größer als $I_{BE}$. Vor dem Hintergrund dieser Shannon-Informationen lassen sich die beiden Methoden diskutieren, mit denen die 50 %-Grenze überwunden werden kann.

Die eine Methode verwirft solche Datensätze, bei denen der Mithörer nach Bekanntwerden der Fehlerpositionen einen Informationsvorsprung vor den rechtmäßigen Benutzern hat [6]. Der Empfänger behält nur die Daten, die er trotz vorhandener Quantenunsicherheit sicher interpretieren kann. Da es zwischen Empfänger und Mithörer keine Korrelationen im




**Die geteilte Information zwischen Sender (A), Empfänger (B) und Mithörer (E) als Funktion der Transparenz der Übertragungsstrecke. Durch die Berücksichtigung zusätzlichen Detektorrauschens im Empfänger verschiebt sich u. a. der Schnittpunkt der Kurven $I_{AB}$ und $I_{AE}$ (nach [2]).**

Quantenbereich gibt, ist dies ein entscheidender Nachteil für den Mithörer. Damit selektiert man Daten, für die $I'_{AB} > \max\{I'_{AE}, I'_{BE}\}$ gilt, und der Weg ist frei, um mit den Standardtechniken einen geheimen Schlüssel zu destillieren. Die andere Methode kommt ohne eine solche „Postselektion“ aus, denn es zeigt sich, dass die Information des Mithörers über die Daten von Sender und Empfänger asymmetrisch ist. Für das gewählte Mithörermodell gilt insbesondere, dass der Empfänger mehr Information mit dem Sender teilt als mit dem Mithörer, $I_{AB} > I_{BE}$. Diese Eigenschaft bleibt bei unidirektionalen Fehlerkorrekturmethoden erhalten. Diese letzte Methode wurde von Grosshans et al. demonstriert [2]. Dies ist gleichzeitig auch das erste Experiment zur Quantenschlüsselverteilung mit kontinuierlichen Variablen. Damit ist gezeigt, dass es keine prinzipielle Beschränkung der Reichweite für die Verteilung von Quanten-Schlüsseln mit kontinuierlichen Variablen gibt. Dank der benutzen Homodyn-Messungen besteht die Hoffnung, mittels einer hohen Repetitionsrate die erzeugte Schlüsselrate deutlich über die vergleichbarer Systeme mit Einzelphotonenzählern zu bringen.

GERD LEUCHS, NATALIA KOROLKOVA UND NORBERT LÜTKENHAUS

[1] *S. Singh*, „The code book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography“, Fourth Estate, London (1999)
[2] *F. Grosshans* et al., Nature **421**, 238 (2003)
[3] Für eine Übersicht über die klassischen Begleitprotokolle s. *N. Lütkenhaus*, Appl. Phys. **B 69**, 395 (1999)
[4] *Ch. Kurtsiefer* et al., Nature **419**, 450 (2002)
[5] *I. Marcikic* et al., Nature **421**, 509 (2003)
[6] *C. Silberhorn, T.C. Ralph, N. Lütkenhaus* und *G. Leuchs*, Phys. Rev. Lett. **89**, 167901 (2002)