Aktueller Begriff

Deutscher Bundestag ■ Wissenschaftliche Dienste

# Quantenkryptographie

Die Sicherheit vertraulicher Informationen vor unbefugtem Zugriff hat große Bedeutung in vielen Bereichen, sei es für Unternehmen, Finanzinstitutionen, Strafverfolgungsbehörden oder Politik und Verwaltung. Die Quantenkryptographie (QKG) könnte eine Möglichkeit bieten, die Übertragung von Daten absolut sicher zu machen. Die Entwicklung befindet sich hier in einem Stadium intensiver Grundlagenforschung. Die Basis für erste praktische Anwendungen ist bereits gelegt. Das BMBF unterstützt in diversen Förderprogrammen die Arbeit auf diesem Gebiet. Ebenso ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit diesem Themenkomplex beschäftigt.

## Sicherheit durch Verschlüsselung (Kryptographie)

Kryptographische Methoden konventioneller Art sind bereits heute weit verbreitet. Erste Anwendungen der Kryptographie reichen bis in vorchristliche Zeit zurück. Schon damals wurden Botschaften vor feindlichen Augen verborgen. Neben Nachrichten sind heute viele weitere wichtige Daten vor unbefugtem Zugriff Dritter zu schützen. Dazu gehören Finanztransaktionen, Wirtschafts- und Unternehmensdaten, aber auch personenbezogene und medizinische Daten. Um die Sicherheit der Kommunikation zu gewährleisten, müssen vier Aspekte erfüllt sein: Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit. Die **Vertraulichkeit** garantiert, dass nur Zugriffsberechtigte die Nachricht lesen können. **Authentisch** ist eine Botschaft, wenn der Absender eindeutig zu identifizieren ist. **Integrität** ist gewährleistet, wenn nachzuprüfen ist, ob die Nachricht unterwegs durch Dritte verändert wurde. Schließlich ist die Nachricht **verbindlich**, wenn der Absender seine Urheberschaft nicht abstreiten kann, sondern sich diese auch gegenüber Dritten nachweisen lässt.
Um eine Nachricht zu chiffrieren, bedarf es eines Schlüssels, der aus dem Klartext den verschlüsselten Text macht. Zur Dechiffrierung ist dann wieder ein Schlüssel erforderlich. Generell unterscheidet man zwei Verschlüsselungsverfahren: das symmetrische und das asymmetrische. Beim symmetrischen Verfahren besitzen Sender und Empfänger den gleichen Schlüssel, müssen diesen also vorher ausgetauscht haben. Beim asymmetrischen Verfahren hingegen gibt es einen öffentlichen (Public Key) und einen geheimen Schlüssel (Private Key). Der Sender verwendet den Public Key, um die Botschaft zu kodieren, und der Empfänger kann mit seinem Private Key später den Klartext wieder herstellen. Die Nachricht ohne Kenntnis des Schlüssels zu entziffern ist zwar nicht prinzipiell unmöglich, erfordert jedoch einen sehr großen Rechenaufwand, mit dem aktuell verfügbare Computer jahrelang beschäftigt wären. Heute gängige Verschlüsselungsmethoden verwenden zumeist dieses asymmetrische Public-Key-Verfahren. Seine (relative) Sicherheit beruht in erster Linie auf der Annahme begrenzter Rechenleistung eines Angreifers. Die verfügbare Leistung moderner Rechner steigt jedoch unaufhörlich – nicht nur durch kontinuierlichen technischen Fortschritt, sondern in Zukunft möglicherweise auch sprunghaft durch die Realisierung eines neuen Konstruktionsprinzips (Quantencomputer). Damit könnten die heute gängigen Public-Key-Verfahren ihre relative Sicherheit verlieren.

## Quantenkryptographie

Eine Übertragung mit quantenkryptographischen Methoden wäre davon jedoch nicht betroffen. Hier beruht die Sicherheit nicht auf dem zu hohen Aufwand für mathematische Operationen, sondern auf physikalischen Naturgesetzen. Die Quantenkryptographie (QKG) dient dabei als Teil eines zweistufigen Verfahrens ausschließlich dazu, einen sicheren Schlüsselaustausch zu ermöglichen, nicht jedoch zum Kodieren der Nachricht selbst. Für die Übertragung der zu schützenden

Information wird im zweiten Schritt die konventionelle symmetrische Verschlüsselung angewandt. Auch dieser Schritt kann absolut sicher gestaltet werden, wie Gilbert Vernam 1918 nachwies. Dazu muss der Schlüssel die gleiche Zeichenlänge wie die Botschaft besitzen und aus völlig zufälligen Zeichen bestehen. Zudem darf jeder Schlüssel nur einmal verwendet werden. Die einzig verbleibende Sicherheitslücke dieses Verfahrens bestand bisher im Schlüsselaustausch; diese Lücke könnte zukünftig durch die QKG behoben werden.
Es existieren zwei physikalische Möglichkeiten für den Austausch des Schlüssels nach quantenkryptographischen Methoden. Die erste Variante verwendet Lichtteilchen (Photonen), die vom Sender zum Empfänger beispielsweise über Glasfaserkabel gesandt werden. Die Information über die Bestandteile (Bits) des Schlüssels wird in Form der Schwingungsebene (Polarisation) des Lichts kodiert und übermittelt. Sie kann horizontal, vertikal oder diagonal ausgerichtet sein. Diese Übertragungsvariante ist bereits weiter erforscht und entwickelt. Es gibt erste Firmen, die quantenkryptographische Geräte auf dieser Grundlage anbieten.
Die zweite Möglichkeit nutzt ein anderes physikalisches Phänomen, so genannte verschränkte Teilchen. Quanten-Verschränkung liegt dann vor, wenn zwei Teilchen sich in demselben, gemeinsamen Zustand befinden und deshalb bei jeder Messung gleichartige Eigenschaften zeigen. Führen Sender und Empfänger also Messungen an zwei Teilchen durch, die auf diese Weise miteinander verschränkt sind, so erhalten daraus beide notwendigerweise dieselbe Information und können diese für die Zeichen (Bits) eines Schlüssels verwenden.
Bei beiden Verfahren sind Lauschangriffe nicht auszuschließen. Die Besonderheit quantenkryptographischer Verfahren liegt jedoch darin, dass ein Abhörversuch aufgrund der speziellen Eigenschaften quantenmechanischer Systeme vom Empfänger mit hoher Wahrscheinlichkeit bemerkt werden könnte. Dieser könnte dann den abgehörten Schlüssel verwerfen und entweder einen neuen Versuch der Schlüsselübermittlung starten oder aber auf den zweiten Schritt, die Übertragung der eigentlichen Botschaft mit Hilfe des Schlüssels, ganz verzichten. Die zu schützende Information wäre damit nicht verraten.

**Absolute Sicherheit?**

Das Verfahren der QKG wird – im Gegensatz zu konventionellen Verfahren – als absolut sicher beschrieben. Diese Aussage hat ihre Grundlage in den Naturgesetzen. In der Quantenphysik gilt, dass jede Messung, jede Beobachtung eines Systems Rückwirkungen auf das System selbst hat. Im Fall der Übertragung mit Photonen würde daher jeder Lauschangriff das übertragene Signal stören und einen vom Empfänger messbaren Fehler hinterlassen. Durch eine zu geringe Qualität des übertragenen Signals – ähnlich einem verrauschten Fernsehbild – wären beide Kommunikationspartner über die Anwesenheit eines Dritten informiert.
Dies gilt zumindest dann, wenn die Signalqualität ansonsten hinreichend hoch ist und nur geringes eigenes Rauschen aufweist, so dass ein Unterschied eindeutig festgestellt werden kann. Prinzipiell ist es dem Zuhörer zwar immer möglich, ein gewisses Mindestmaß an Information aus der Kommunikationsverbindung zu extrahieren, jedoch steigt mit der gewonnenen Information auch die dadurch eingeführte Störung. Daher müssen Sender und Empfänger genaue Angaben machen, bis zu welcher Fehlerrate eine Übertragung des Schlüssels noch als sicher betrachtet werden kann. Diese Fehlerrate kann durch ausgefeilte Technik sehr niedrig gehalten werden.

**Fazit**

Die Quantenkryptographie könnte eine Möglichkeit bieten, den zukünftigen Gefährdungen im Informations- und Datenaustausch entgegenzutreten. Damit könnte selbst dann, wenn Lauscher sich die Entwicklung immer leistungsfähigerer Rechner zunutze machen, die Vertraulichkeit und Integrität der Datenübertragung gewährleistet werden.

**Quellen und weiterführende Literatur:**


- Bennett, Charles H.; Brassard, Gilles (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore.
- BMBF (2007). Förderbekanntmachung Quantenoptik / „Neue optische Wirkprinzipien“. Im Internet: http://www.bmbf.de/foerderungen/7534.php.
- Bruß, Dagmar, Weinfurter, Harald (2005). Geheime Botschaften aus Licht – Die Quantenmechanik ermöglicht prinzipiell abhörsichere Kommunikation. Physik Journal 11/2005, S. 57ff.
- Ekert, Artur K. (1991). Quantum Cryptography Based on Bell’s Theorem. Physical Review Letters, Bd. 67, S. 661.
- Ludl, Andreas (2001). Verschlüsselungstechnik und Kryptographie. telekom praxis, Januar 2001, Band 78, S. 16-26
- Stix, Gary (2005). Datenschutz mit Quantenschlüsseln. Spektrum der Wissenschaft, Mai 2005, S. 68-73
- Technology Review (2007). Angriff auf Quantenkryptographie. www.heise.de/newsticker/meldung/89151/from/rss09


Verfasser: Prakt. Dennis Glüsenkamp, Dr. Daniel Lübbert - Fachbereich WD8 – Umwelt, Naturschutz, Reaktorsicherheit, Bildung und Forschung