

Quanten-Kryptographie

Die Bedeutung der Quantenmechanik in der Informationstechnik

von Manuel Sprock

Einleitung

Die Kryptographie spielt in der Informationstechnik eine immer wichtigere Rolle. Vertrauliche Informationen müssen in digitaler Form auf sichere Weise ausgetauscht werden können. Die Kryptographieverfahren, die heute Anwendung finden, basieren auf einem geheimen Schlüssel, der beiden Teilnehmern zur Verfügung steht (symmetrisches Verfahren) bzw. einem zweigeteilten Schlüssel (asymmetrisches Verfahren), bei dem ein Teil zum Ver- und der andere zum Entschlüsseln dient. Dieser Schlüssel wird aus Zufallswerten erzeugt, seine Länge bestimmt die Datensicherheit und die Dauer der Ver- und Entschlüsselungsvorgänge. Will man Daten, die auf diese Art verschlüsselt wurden, entschlüsseln, kann man versuchen, die Schlüsselkombination zu errechnen, also alle möglichen Schlüsselkombinationen ausprobieren. Alle gängigen Kryptographie-Protokolle können theoretisch auf diese Weise geknackt werden. Der Erfolg solcher Versuche ist abhängig von der zur Verfügung stehenden Rechenleistung. Heutige Computer würden für das Knacken eines gängigen Schlüssels viele Jahre brauchen. Dies könnte sich jedoch in Zukunft durch die Realisierung von Quantencomputern ändern, denn diese würden die Rechenleistung explosionsartig steigern.

Sichere Kryptographie

Das einzige absolut sichere Kryptographieverfahren ist das sogenannte One-Time-Pad. Hierbei handelt es sich um ein symmetrisches Verschlüsselungssystem, welches sich zufälliger Schlüsselsequenzen bedient, die mindestens so groß sein müssen wie die zu übermittelnde Nachricht. Verschlüsselt wird durch bitweise Addierung des Schlüssels zum Klartext (XOR). Zur Entschlüsselung addiert man bitweise den Schlüssel zum Geheimtext und man erhält wiederum den Klartext. Dieses Verfahren ist eigentlich nicht sinnvoll, weil der Schlüssel, der genauso lang ist wie die Nachricht, nur einmal benutzt werden kann auf sicherem Wege ausgetauscht werden muss. Also könnte man statt des Schlüssels auch gleich die zu übermittelnde Nachricht austauschen.

Quantenmechanik

An dieser Stelle setzt die Quanteninformatik an. Sie bietet die Möglichkeit einer absolut sicheren Verschlüsselung, die durch kein System geknackt werden kann. Grundlage hierfür sind die Naturgesetze der Quantenphysik. Diese bestimmen die Grenzen der Messung physikalischer Größen im Bereich der Elementarteilchen: die Heisenbergsche Unschärferelation besagt, dass es logisch unmöglich ist, jede Eigenschaft eines bestimmten Objektes mit vollkommener Genauigkeit zu messen. Präzise Messung der einen Eigenschaft schließt eine präzise Messung der anderen Eigenschaft aus; je genauer man eine Größe feststellt, desto ungenauer wird die Messung der anderen. Man kann also den Zustand eines Teilchens nicht bestimmen ohne ihn gleichzeitig zu verändern.

Quanten-Kryptographie

Die Implementierung des One-Time-Pads, die auf konventionelle Art nicht sinnvoll ist, führt in Verbindung mit den Gesetzen der Quantenmechanik in der Theorie zu einer absolut sicheren Kommunikationsmethode. Sie generiert einen Schlüssel aus einer Eigenschaft von Photonen, die über Glasfaserkabel übertragen werden. Die benutzte Eigenschaft eines Photons, die nicht ohne Veränderung des Grundzustandes gemessen werden kann, ist die Polarisation. Die Polarisation ist eigentlich ein Begriff aus der Wellenlehre und besagt, dass der Vektor der elektrischen Feldstärke seine Richtung im Raum bei der Betragsschwingung in bestimmter Weise ändert. Als „zirkuläre Polarisation“ bezeichnet man eine elliptische oder kreisförmige Bahnkurve der Vektorspitze, bei „linearer Polarisation“ schwingt der Vektor immer in eine Richtung. Diese Schwingung wurde auf das Photonenbild übertragen („Dualismus Teilchen-Welle“). Die Quantenkryptographie benutzt vier verschiedene lineare Polarisationen: 0° (horizontal), 90° (vertikal), 45° und 135° . Polarisationsfilter können Photonen derselben Polarisation filtern. Hierbei ist zu beachten, dass ein Polarisationsfilter für horizontal polarisierte Photonen jedoch neben den tatsächlich horizontal polarisierten Photonen auch diagonal polarisierte Photonen (45° oder 135°) mit einer Wahrscheinlichkeit von 50% durchlässt und diese dabei horizontal polarisiert werden.

Erzeugung eines Quantenschlüssels

Einer der beiden Kommunikationspartner, die zur Übermittlung einer Nachricht die Quantenkryptographie benutzen möchten, erzeugt nun Photonen mit einer dieser vier möglichen Polarisierungen (0° , 90° , 45° und 135°). Dies muss absolut zufällig geschehen und geheim bleiben. Der Empfänger analysiert die Photonen und muss sich zunächst für jedes einzelne Photon ebenfalls absolut zufällig zwischen 2 Detektoren (Polarisationsfiltern) entscheiden: der eine kann nur Photonen mit einer Polarisation von 0° oder 90° Grad (also horizontal oder vertikal polarisiert) unterscheiden, der andere nur solche mit 45° bzw. 135° (diagonal). Wird der falsche Detektor gewählt, kommen beide möglichen Ergebnisse mit einer Wahrscheinlichkeit von 50% vor. Neben dem Ergebnis der Messung wird auch die Wahl des Detektors notiert. Sind alle Photonen übertragen und gemessen, teilt der Empfänger dem Sender über einen anderen (öffentlichen) Kanal für jedes Photon die von ihm verwendete Einstellung des Detektors mit und erfährt ihm, ob diese richtig war. Das richtige Ergebnis wird natürlich nicht übermittelt, denn das kennen ja Empfänger und Sender für alle vom Empfänger mit der richtigen Einstellung gemessenen Photonen. Aus diesen richtigen Messungen bilden beide den sogenannten Quantenschlüssel, d.h. sie ordnen der 0° -Polarisation eine logische 0 und der 90° -Polarisation eine logische 1 zu und entsprechend für die zweite Detektor-Einstellung eine logische 0 für 45° und eine 1 für 135° . Zur Feststellung der Fehlerrate, die durch Paritätsprüfung gering gehalten werden kann, wird ein Segment des Schlüssels übertragen und verglichen. Liefert dieser Test einen zufriedenstellenden Wert, kann die Nachricht mit dem Schlüssel verschlüsselt und über den öffentlichen Kanal übertragen werden.

Sicherheit

Diese Methode ist als absolut sicher anzusehen, weil Photonen nicht „kopiert“ werden können, ohne Fehler im Original und in der Kopie zu erzeugen. Zweigt ein Angreifer bei der Übertragung einige Photonen ab, um diese zu analysieren, kommen diese einfach nicht beim eigentlichen Empfänger an und tragen somit nicht zum Quantenschlüssel bei. Fängt ein Angreifer alle Photonen ab, um sie zu analysieren, neue zu erzeugen und an den Empfänger zu schicken, ist die Messung nur mit einer Wahrscheinlichkeit von 50% richtig. Diese Fehlerrate gilt dann also auch für die neu erzeugten Photonen, die der richtige Empfänger dann wiederum mit der 50%-Wahrscheinlichkeit mit der richtigen Einstellung analysiert. Aus einem solchen Angriff resultiert nach dem Vergleich der Einstellungen und der Schlüsselerzeugung eine Fehlerrate von 25%, die den Angriff nicht unbemerkt lässt.

Praxis

Das Verfahren ist heute noch nicht im Einsatz, weil bei der Implementierung diverse Probleme auftreten. Es existiert keine Quelle, die einzelne Photonen erzeugen kann. Zur Synchronisation des Photonenstroms sind Zeitmessungen im Nanosekundenbereich nötig, die den Einsatz einer Atomuhr erfordern. Bei der Übertragung durch Glasfaserleitungen ist die Distanz begrenzt, weil das „Signal“, also der Photonenstrom, nicht verstärkt werden kann. Es kommt erschwerend hinzu, dass die benutzten Photonen eine andere Wellenlänge haben als die üblicherweise in der Glasfasertechnik benutzten, weil für die sonst üblichen Wellenlängen keine Einzelphotonendetektoren existieren. Dies verringert die Reichweite zusätzlich. Die fehlende Möglichkeit der Benutzerauthentifizierung und der perfekte und unvorhersagbare Zufallsgenerator für die Wahl der Polarisation und der Detektoreinstellung sind weitere Probleme.

Das beschriebene Verfahren ist auf dem Gelände der Universität Innsbruck in einem Versuchsaufbau umgesetzt. Die Übertragungsdistanz beträgt 360 Meter und es wird eine Quelle benutzt, die verschränkte Photonenpaare erzeugt, also 2 Photonen, die entgegengesetzt polarisiert sind. Dies gelingt jedoch nur bei ca. 5% der erzeugten Photonen, die dann von beiden Kommunikationspartnern analysiert werden müssen. Die übertragene Datenmenge ist im Vergleich zur Schlüssellänge daher sehr groß: auf jedes Bit des Quantenschlüssels kommen ca. 200 Byte.

In Zukunft kann jedoch mit einer praxistauglichen Umsetzung des Systems gerechnet werden, da internationale Forschergruppen intensiv daran arbeiten. Neben der Übertragung durch Glasfaserleitungen wäre auch eine Übertragung im freien Raum oder gar über Satelliten denkbar. Die Entwicklung einer perfekten Einzelphotonenquelle oder verschränkter Teilchen, die über einen längeren Zeitraum speicherbar sind, könnte einen weiteren Durchbruch bedeuten.

Quellen:

- c't 6/2001 S. 260
- www.informatik.hu-berlin.de/Institut/struktur/algorithmenII/Lehre/SS2001/Krypto/Quantenkryptographie.pdf