Frankfurter Allgemeine Zeitung, 2010-09-08

Listige Attacke auf den Quantenschlüssel

Verwundbare Kryptographie: Clevere Hacker knacken einen vermeintlich sicheren Quantencode und zeigen damit zwei kommerziellen Systemen ihre Grenzen auf.

Von Manfred Lindinger

Ob beim Online-Banking, beim Einkauf im Internet oder beim Austausch internen Firmenwissens und von Bankgeheimnissen – vertrauliche Informationen sollte man stets verschlüsselt weitergeben, damit sie nicht in falsche Hände geraten. Trotz aller Bemühungen lassen sich Nachrichten mit klassischen Verschlüsselungsverfahren aber noch immer nicht sicher übertragen. Einen Ausweg verspricht die Quantenkryptographie, die zum Austausch vertraulicher Informationen die Prinzipien der Quantenphysik nutzt. Dadurch sollte das heimliche Abhören so gut wie unmöglich werden. Doch auch diese Technik scheint offenkundig ihre Schwachpunkte zu haben, wie eine deutsch-norwegische Forschergruppe nun zeigen konnte.

Herkömmliche Verschlüsselungstechniken beruhen darauf, dass bestimmte Rechenoperationen wie die Primfaktorzerlegung nur mit großem Rechenaufwand ausgeführt werden können. Doch mit fortschreitender Computertechnik wird es wahrscheinlicher, dass jeder als sicher geltende Code in kürzester Zeit geknackt werden kann. Anders bei der Quantenkryptographie. Bei dieser Technik wird nicht die Botschaft selbst übermittelt, sondern eine zufällige Folge von binären Nullen und Einsen, die als Schlüssel dient. Erst mit diesem Schlüssel kann der Empfänger („Bob") die eigentliche Nachricht des Senders („Alice") lesen. Der Clou des Verfahrens ist, dass ein Spion – „Eve" –, der die verschlüsselten Informationen „abhört", diese selbst merklich verändert, wodurch jeglicher Angriff enttarnt wird.

Ein häufig verwendetes kryptographisches Verfahren beruht auf einer Idee von Charles Bennett und Gilles Brassard aus dem Jahre 1984. Bei dieser Technik – BB84-Protokoll genannt – übermittelt Alice an Bob eine zufällige Folge von Nullen und Einsen in Form einzelner Lichtteilchen mit insgesamt vier verschiedenen Polarisationen. Als „Null" und „Eins" werden dabei die jeweils senkrecht zueinander polarisierten Schwingungszustände interpretiert. Der Empfänger misst die Polarisationszustände der Photonen und vergleicht anschließend sein Ergebnis mit der Bitfolge des Senders. Ein Lauscher, der den Versuch unternimmt, einzelne Photonen abzufangen und deren Polarisationen zu messen, würde dabei sofort bemerkt, da er diese unweigerlich veränderte und eine Fehlerrate bei der Übertragung erzeugte – eine grundlegende Eigenschaft der Quantenphysik.

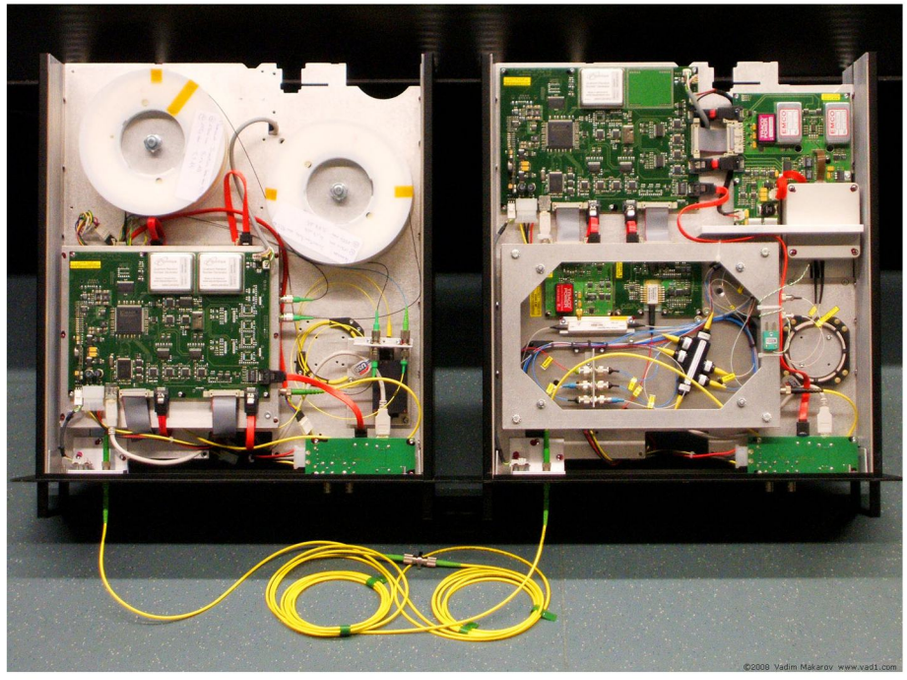
Doch während die einen Forscher ihre Verschlüsselungsverfahren ständig verbessern, loten andere die Sicherheitslücken aus. So haben Physiker vom Massachusetts Institute of Technology in Cambridge unlängst demonstriert, dass man die Quantenkryptographie mit ihren eigenen Mitteln attackieren kann. Zum Anzapfen der Polarisationszustände von Photonen machten sie sich die quantenmechanische Verschränkung zunutze. Diese verknüpft die Eigenschaften von zwei verschiedenen Photonen auf eine Weise, dass sich beide Teilchen stets wie ein einheitliches Quantensystem verhalten. Die Forscher verschränkten die Photonen des Senders mit Lichtpulsen, die sie als potentielle Abhörer erzeugten. Auf diese Weise hofften sie, unbemerkt an Informationen über Schwingungszustände der Lichtteilchen zu gelangen und den Quantenschlüssel abzufangen. Diese Art von Lauschangriff erzeugt allerdings eine auffällige hohe Rate an fehlerhaften Bits. Das scheint aber mittlerweile keine unüberwindliche Hürde mehr zu sein. Forscher von der University of Toronto haben weitere Schwachstellen einer kommerziellen Hardware ausgenutzt, um beim Abhören eine Fehlerrate von nur 19,7 Prozent zu erzeugen. Dies liegt knapp unter der obersten Schwelle, unterhalb der ein Quantenschlüssel als sicher gilt.

Völlig unbemerkt blieb auch der Lauschangriff der Forscher um Gerd Leuchs vom Max-Planck-Institut für die Physik des Lichts in Erlangen und Vadim Makarov von der Norwegischen Universität für Wissenschaft und Technologie in Trondheim. Seit langem versuchen die Forscher, Sicherheitslücken bei kommerziellen Geräten aufzudecken. Bei zwei Systemen ist es ihnen nun offenkundig geglückt. Wie Makarov und seine Kollegen in der Online-Ausgabe der Zeitschrift „Nature Photonics" (doi: 10.1038/NPHOTON.2010.214) berichten, haben sie dazu gezielt einen technischen Schwachpunkt von Bob ausgenutzt: seine Detektoren.

Zum Nachweis schwacher Lichtpulse oder einzelner Photonen werden üblicherweise sogenannte Lawinenphotodioden verwendet. Diese sind extrem empfindliche Sensoren, die schnell auf ein ankommendes einzelnes Signal reagieren können. Trifft ein Lichtteilchen auf eine solche Diode, entstehen Paare von Elektronen und positiv geladenen Löchern. Ihre Zahl ist allerdings zu gering, um von dem Instrument wahrgenommen zu werden. Man legt deshalb eine elektrische Hochspannung an, die eine Lawine von weiteren Ladungen auslöst. So erzeugt bereits ein einzelnes Lichtteilchen einen messbaren elektrischen Strom im Detektor. Die Situation ändert sich, wenn die Photodiode unter Dauerbeschuss vieler Photonen steht. Dann wird sie unempfindlich für einzelne Photonen und deren Quanteneigenschaften. Der Detektor verhält sich wie ein klassischer Lichtsensor.

Dieses Verhalten haben die Forscher für ihren Lauschangriff ausgenutzt. Während Eve die Photonen von Alice abfing und deren Polarisation bestimmte, schickte sie entsprechende Lichtpulse in Bobs Richtung. Damit Bob nichts davon merkte, richtete Eve während des Lauschangriffs einen kontinuierlichen infraroten Laserstrahl auf ihn. Davon war sein Einzelphotonendetektor derart geblendet, dass dieser fortan wie ein klassischer Lichtsensor arbeitete. Bob, der von alldem nichts mitbekam, hielt Eves Lichtpulse nach wie vor für einzelne Photonen, die Alice ihm schickte. Eine erhöhte Fehlerrate wurde durch den Angriff nicht erzeugt. Auf diese Weise konnte der Lauscher unbemerkt die Photonen von Alice abfangen und daraus den Quantenschlüssel rekonstruieren.

Mit ihren Versuchen wollen die Forscher keine kriminellen Energien bei anderen Hackern wecken. Sie dienten alleine dazu, die Sicherheit von kommerziellen Quantenkryptographie-Systemen auszuloten, damit die Hardware entsprechend verbessert werden kann, sagte Christoffer Wittmann, einer der Physiker vom MPI in Erlangen, im Gespräch mit dieser Zeitung. Deshalb hatte man vor der Veröffentlichung der Ergebnisse die betroffenen Hersteller über den bestehenden Sicherheitsmangel informiert. Beide hätten den Hinweis dankend aufgenommen und bereits Gegenmaßnahmen entwickelt. Die technischen Details seien jedoch Firmengeheimnis.



Blick ins Innere von „Alice" (links) und „Bob" (rechts), die mit einer Glasfaser (gelb) verbunden sind. Die Geräte stammen von der Genfer Firma ID Quantique. Foto MPI, Erlangen