Unknackbare Codes

Unknackbare Codes

Zur Übermittlung geheimer Botschaften setzt ein neuartiges Verfahren Fotonen ein statt numerische Codes. So lassen sich die verschlüsselten Botschaften nicht mehr unbemerkt abhören.

VON OLIVIER DESSIBOURG

James Bond wird es bestätigen: Ein guter Spion fängt eine geheime Nachricht ab, ohne dass dies Empfänger oder Absender ahnen. Zumindest in der Informatik dürften seit einiger Zeit selbst würdige Nachfolger des Agenten 007 damit Mühe haben. Denn seit einem Jahrzehnt zeichnet sich eine völlig neuartige Verschlüsselungstechnik ab: die Quantenkryptografie. Der an der Universität Genf tätige Physiker Grégoire Ribordy war an der Gründung des Unternehmens ID Quantique in Carouge beteiligt, das diese revolutionäre Technologie vermarkten will.

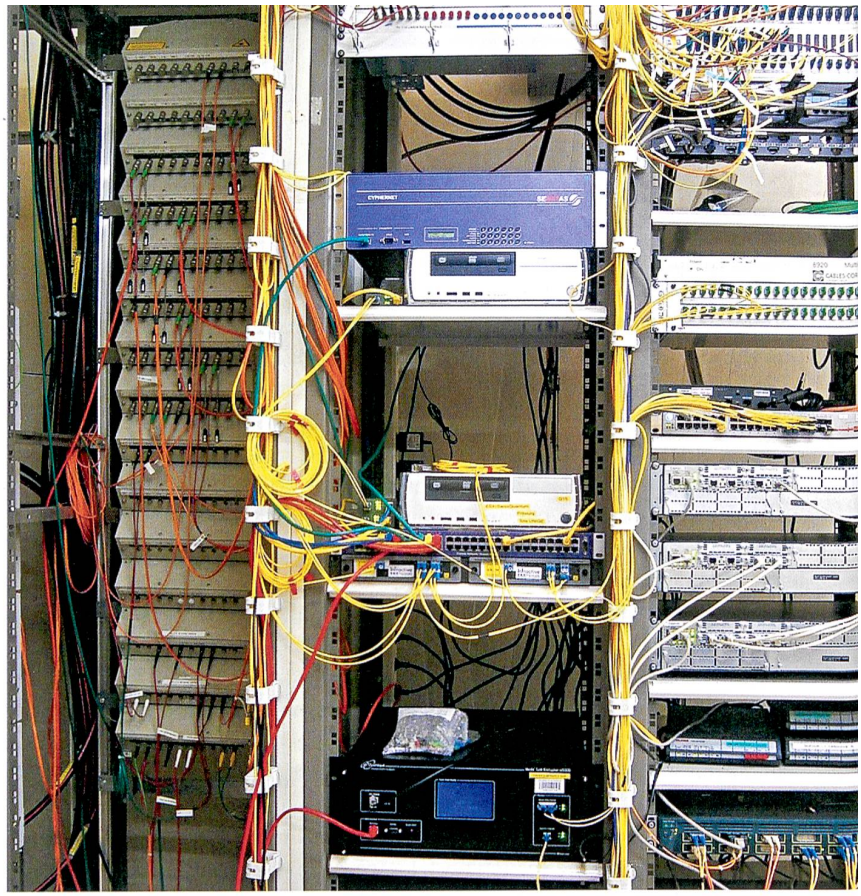
Bis heute verwenden Verschlüsselungssysteme «Schlüssel», um Nachrichten in Binärcodes mit den Werten 0 und 1 umzuwandeln. Damit die miteinander kommunizierenden Stellen diese richtig entziffern können, müssen sie die ebenfalls numerischen Schlüssel austauschen – mit dem Risiko, dass die Schlüssel dabei abgehört werden.

Fotonenkette als Schlüssel

Auf Initiative von Nicolas Gisin setzten die Physiker der Universität Genf genau an diesem Punkt an: Zur Übermittlung verwenden sie Fotonen. Werden diese Lichtteilchen durch Filter geleitet, sind sie so «ausgerichtet», dass ihnen ein Bitwert von 0 oder 1 zugeordnet werden kann. Wiederholt man diesen Vorgang, entsteht ein Schlüssel in Form einer Fotonenkette. Dieser Lichterzug wird über ein Glasfaserkabel zum Gesprächspartner geschickt – mit nahezu perfekter Abhörsicherheit: «Nach der sogenannten heisenbergschen Unschärferelation können die Teilchen nicht gemessen werden, ohne dass dies ihre Ausrichtung stört», so Grégoire Ribordy. Wenn also ein Spion die Nachricht abfängt, bemerken es die Gesprächspartner und können reagieren.

Eines ist für Ribordy klar: Verschlüsselungssysteme sind nie hundertprozentig sicher. «Es geht nicht um die Sicherheit der Technologie, sondern um die Sicherheit der Umsetzung. Die Umsetzung des idealen Modells hängt nämlich immer auch von elektronischen und optischen Komponenten ab. Wenn diese aber optimal eingesetzt werden, sind diese Systeme den klassischen kryptografischen Verfahren überlegen.»

In diesem wachsenden Markt hat ID Quantique mit dem amerikanischen Unternehmen MagiQ und der französischen Firma Smart Quantum zwei Konkurrenten. Der wirkliche Rivale ist nach Grégoire Ribordy aber noch immer die klassische Kryptografie. Wo befindet sich das Schweizer Start-up? «Ganz vorne! Wir haben unsere Systeme bei den Genfer Wahlen 2007 bereits in einer realen Situation getestet. Auch wurden wir als bisher einziges Unternehmen Ende 2009 für den Markt zertifiziert. Und vor allem entwickeln wir unsere Technologie nun im Rahmen eines funktionellen Netzwerks weiter.» Unter dem Namen SwissQuantum wird dieses Netzwerk von der Universität Genf unterhalten und vom Schweizerischen Nationalfonds unterstützt. «Ein wichtiges Ziel ist die Ausdehnung der Distanz, über die verschlüsselte Daten ausgetauscht werden können», erklärt der Forscher. «Diese Distanz beträgt 100 Kilometer im Feld und 250 im Labor. Dann verlieren sich die Fotonen… Um 500 Kilometer zu erreichen, brauchen wir Quantensignalverstärker, die das verschlüsselte Licht weiterbefördern. Mit dieser Technologie befassen sich die Physiker der Uni Genf, und im Rahmen des Nationalen Forschungsschwerpunkts Quantenfotonik inspirieren wir uns gegenseitig. So profitieren wir alle.» ■



Blackbox der anderen Art: Der unscheinbare Kasten unten in der Mitte des Netzwerkverteilschranks enthält ein Quantenverschlüsselungssystem. Von hier aus werden die Fotonen über ein Glasfaserkabel zum Empfänger geschickt.
Bild: idquantique.com