INTERNET

Spukhafter Schlüssel

Geheimdienste wollen in Zukunft mit Quantencomputern jeden Code knacken. Physiker halten jetzt schon dagegen: Sie schützen Daten – ebenfalls mit Quanten.

Der menschliche Erfindergeist, schrieb Krimi-Autor Edgar Allan Poe im Jahr 1841, „kann keinen Code entwickeln, den menschlicher Erfindergeist nicht knacken kann“. Seit Jahrtausenden geht das so: Geheimnisträger verschlüsseln ihre Botschaften mit immer neuen Methoden; Schnüffler entschlüsseln sie mit immer neuen Tricks.

„Die Geschichte hat Poe recht gegeben – bislang zumindest“, sagt Artur Ekert, Professor für Quantenphysik und Kryptographie an der britischen University of Oxford. Seine These ist gewagt: Die Geheimnisträger, glaubt Ekert, werden am Ende über die Schnüffler siegen, mit Hilfe der Physik. „Vielleicht müssen wir uns bald keine Sorgen mehr über unzureichende Verschlüsselung machen.“

Allerdings forscht der amerikanische Geheimdienst NSA angeblich an einem Quantencomputer, wie Anfang Januar in der „Washington Post“ zu lesen war. Mit einem derartigen Superrechner, heißt es, könnten die Schnüffler in Zukunft fast jeden Code knacken. Dies wäre die endgültige Niederlage der Geheimnisträger.

Quantencomputer basieren auf surreal anmutenden Prinzipien. Sie operieren nicht wie herkömmliche Rechner mit Nullen und Einsen, sondern mit physikalischen Eigenschaften von Elementarteilchen. Die kleinste Recheneinheit, das Quantenbit, kann dabei nicht nur zwei, sondern viel mehr unterschiedliche Zustände annehmen. Dadurch ließen sich gängige Verschlüsselungsmethoden wie RSA in rasender Eile knacken.

Allerdings ist die Entwicklung dieser Technologie noch Grundlagenforschung; bis es funktionierende Quantenrechner gibt, schätzt Ekert, werden noch „5 bis 50 Jahre“ vergehen.

Die Gegenseite arbeitet ebenfalls mit den seltsamen Gesetzen der Physik kleinster Teilchen – und sie ist weiter: Verschlüsselungsexperten wie Grégoire Ribordy von der Firma ID Quantique aus der Nähe von Genf verkaufen bereits Geräte, die Geheimbotschaften vor Lauschangriffen schützen. Dabei macht Ribordy sich einen Effekt zunutze, der geradezu magisch erscheint: Zwei Lichtteilchen verschränkt sein Gerät so miteinander, dass sie sich selbst an unterschiedlichen Orten fast so verhalten, als wären sie telepathisch verbunden.

Worauf die Teleportation beruht, bleibt unklar, unstrittig ist aber, dass sie funktioniert. Albert Einstein beschrieb diesen Effekt als „spukhafte Fernwirkung“.

Über hundert Banken, Regierungsstellen und Hochschulen benutzen den Spuk bereits testweise. Für die Übertragung eines kompletten Briefs ist das System noch zu langsam, daher werden bislang nur die Schlüssel zum Knacken des Codes teleportiert. Das verschlüsselte Dokument selbst kommt meist ganz normal übers Internet.

Das Geniale bei der Schlüsselverteilung mit Hilfe von Quanten: Sobald ein Spion eines der verschränkten Lichtteilchen abfängt, verändert er dessen Zustand – die Schnüffelei fliegt auf. Quantenbotschaften sind wie durch eine Alarmanlage vor Spionage geschützt.

Auch David Deutsch ist begeistert. Der britische Physiker gilt als einer der wichtigsten Vordenker der Quantencomputerei, für die vielleicht eines Tages ein Nobelpreis verliehen wird. „Quantenverschlüsselung kann durch Quantencomputer nicht gebrochen werden“, sagt Deutsch.

Die größte Schwäche der geisterhaften Geheimbotschaften ist derzeit ihre begrenzte Reichweite. Anton Zeilinger, Physiker und berühmter Pionier der Quantenteleportation an der Universität Wien, beamte 2012 verschränkte Photonen von La Palma auf die Nachbarinsel Teneriffa: 143 Kilometer, Distanzrekord.

Um die Reichweite zu steigern, plant Zeilinger die Teleportation von einem Satelliten zu zwei Bodenstationen, eine in Griechenland, eine in Spanien. Allerdings könnten die Quantenschlüssel nur bei wolkenfreiem Himmel gesendet werden.

„Quantenkryptographie würde viele Sicherheitsprobleme lösen“, sagt Zeilinger: „Aber die Industrie ist zu konservativ, um existierende Systeme umzubauen.“ Ein erster Quantensatellit für das Experiment soll 2016 von China aus starten.

Fast nach Science-Fiction klingt ein Projekt an der Universität München: Der Physikprofessor Harald Weinfurter plant die Quantifizierung des Alltags: „Wenn Sie an einen Geldautomaten gehen, könnten Sie Ihre PIN mit einem Handy-artigen Quantengerät an die Bank übertragen“, sagt Weinfurter. Wann könnte es so weit sein? „Wenn die EU das fördert, bekommen wir einen Prototyp in vier Jahren hin.“

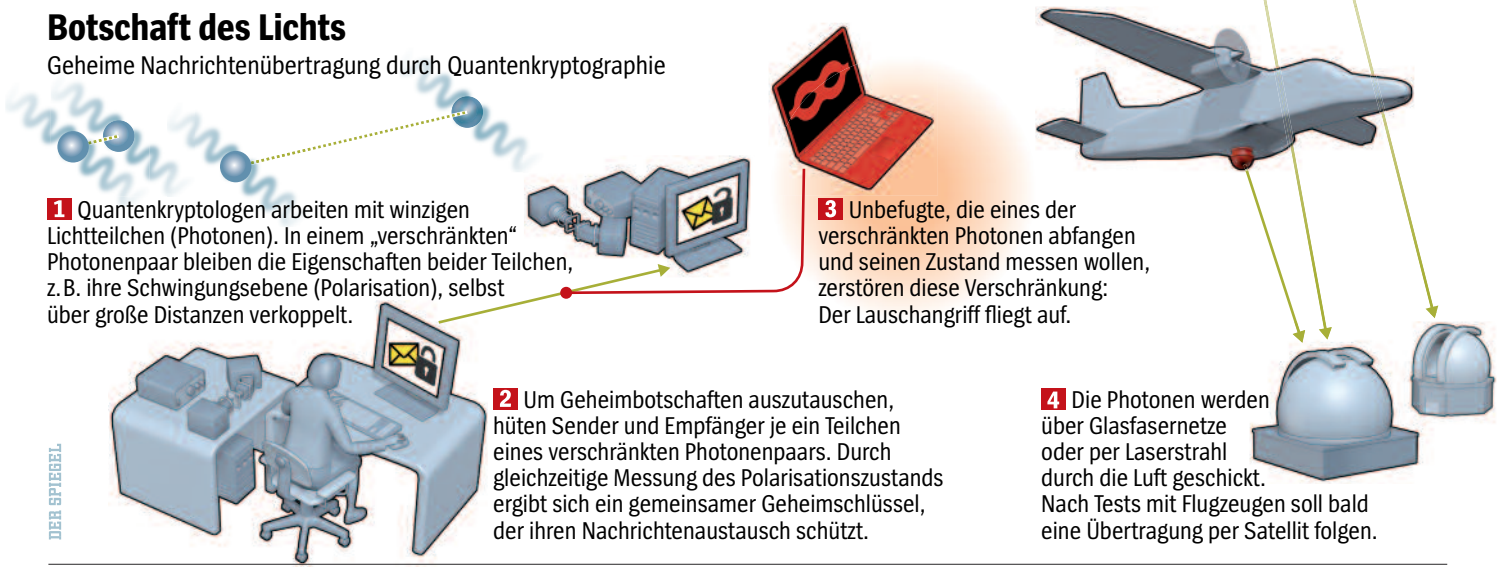
Wie Ekert in Oxford glaubt auch Weinfurter, dass sich mit Hilfe der Physik ein Quantum Vertraulichkeit zurückerobern lässt: „Die Codemacher könnten den jahrtausendelangen Wettkampf gegen die Codebrecher für sich entscheiden.“

„Bullshit“, sagt Bruce Schneier, einer der renommiertesten Sicherheitsberater der USA. Bislang, meint der Informatiker, hätten Schnüffler jeden noch so cleveren Code geknackt. „Der Quantenverschlüsselung wird es da nicht anders ergehen.“

Hilmar Schmundt

Botschaft des Lichts

Geheime Nachrichtenübertragung durch Quantenkryptographie



1 Quantenkryptologen arbeiten mit winzigen Lichtteilchen (Photonen). In einem „verschränkten“ Photonenpaar bleiben die Eigenschaften beider Teilchen, z. B. ihre Schwingungsebene (Polarisation), selbst über große Distanzen verkoppelt.

2 Um Geheimbotschaften auszutauschen, hüten Sender und Empfänger je ein Teilchen eines verschränkten Photonenpaars. Durch gleichzeitige Messung des Polarisationszustands ergibt sich ein gemeinsamer Geheimschlüssel, der ihren Nachrichtenaustausch schützt.

3 Unbefugte, die eines der verschränkten Photonen abfangen und seinen Zustand messen wollen, zerstören diese Verschränkung: Der Lauschangriff fliegt auf.

4 Die Photonen werden über Glasfasernetze oder per Laserstrahl durch die Luft geschickt. Nach Tests mit Flugzeugen soll bald eine Übertragung per Satellit folgen.

DER SPIEGEL