Ludwig-Maximilians-Universität München

27.07.2022 – 17:00 Uhr

Quantenkryptografie: Hackerangriff sinnlos

München, Bayern (ots) -

- Forscher der LMU und der University of Singapore haben eine erweiterte Form der Quantenkryptographie zum ersten Mal experimentell realisiert.
- Ihr Kodierungsprotokoll ist geräteunabhängig und damit noch sicherer als bisherige quantenkryptografische Methoden.
- Die Arbeiten legt das Fundament für zukünftige Quantennetzwerke, in denen zwischen weit entfernten Orten eine absolut sichere Kommunikation möglich ist.

Im Internet wimmelt es nur so von hochsensiblen Informationen. Ausgeklügelte Verschlüsselungstechniken sorgen in der Regel dafür, dass solche Inhalte nicht abgefangen und gelesen werden können. Doch vor allem leistungsstarke Quantencomputer könnten in Zukunft die Schlüssel teils in Sekundenschnelle knacken.

Der quantenmechanische Schlüsselaustausch - im Fachjargon "Quantum Key Distribution (QKD) genannt - ist abhörsicher gegen Angriffe auf die Verbindungsleitungen. QKD ist also immun auch gegen Quantencomputer, nicht aber gegen Attacken oder Manipulationen der Geräte selbst. Die Geräte könnten einen Schlüssel ausgeben, den der Hersteller schon zuvor abgespeichert und womöglich an einen Hacker weitergeben hatte. Die so genannte "Device independent QKD", kurz DIQKD, überprüft nun auch die Sicherheit der Geräte. Theoretisch ist diese Methode seit den 1990er Jahren bekannt, nun hat sie eine internationale Forschergruppe um LMU-Physiker Harald Weinfurter und Charles Lim von der National University of Singapore (NUS) zum ersten Mal experimentell realisiert.

Im vorliegenden Experiment nutzten die Physiker zum Schlüsselaustausch zwei miteinander verschränkte Rubidiumatome, die sich in zwei 400 Meter voneinander entfernten Laboren auf dem LMU-Campus befinden. Die beiden Standorte sind über ein 700 Meter langes Glasfaserkabel verbunden, das unter dem Geschwister-Scholl Platz vor dem Hauptgebäude der Universität verläuft.

Zum Austausch eines Schlüssels, messen die beiden Parteien die Quantenzustände ihrer Atome. Das geschieht jeweils zufällig in zwei, beziehungsweise vier Richtungen. Stimmen die Richtungen überein, sind die Messergebnisse aufgrund der Verschränkung identisch und können zur Erzeugung eines geheimen Schlüssels verwendet werden.

Mit den anderen Messergebnissen lässt sich eine sogenannte Bellsche Ungleichung auswerten. John Bell entwickelte diese Ungleichung um zu testen, ob die Natur mit verborgenen Variablen beschrieben werden kann. Bei der DIQKD wird dieser Test nun verwendet, um sicherzustellen, dass es "keine Manipulationen an den Geräte gibt, also nicht schon vorab verborgene Messresultate in den Geräten gespeichert wurden", so Weinfurter.

Das NUS Protokoll verwendet nun zwei Messeinstellungen. "Dadurch wird es viel schwieriger, Informationen abzuhören. So kann mehr Rauschen toleriert und geheimer Schlüssel auch bei höherem Rauschen erzeugt werden", sagt Charles Lim.

"Mit unserer Methode können wir nun auch mit nicht charakterisierten und potenziell nicht vertrauenswürdigen Geräten geheime Schlüssel sicher erzeugen", erklärt Weinfurter. "Unsere Arbeit legt das Fundament für zukünftige Quantennetzwerken, in denen zwischen weit entfernten Orten eine absolut sichere Kommunikation möglich ist", sagt Charles Lim.

Publikation:

Zhang W., van Leent, T. Redeker, K. et al.: A device-independent quantum key distribution system for distant users, Nature, 2022.

Kontakt:

Prof. Harald Weinfurter

Experimental Quantum Physics

Faculty of Physics / LMU

Tel: +49 89 2180-2044

Email: h.w@lmu.de

Pressekontakt:

Claudia Russo
Leitung Kommunikation & Presse
Ludwig-Maximilians-Universität München
Leopoldstr. 3
80802 München

Phone: +49 (0) 89 2180-3423
E-Mail: presse@lmu.de