

Linz, 15. April 2021

Quantenkryptographie: Neue Methode für abhörsichere Kommunikation

Bankgeschäfte, E-Mails, Handel – die moderne Gesellschaft ist auf virtuellen Informationsaustausch aufgebaut. Genau das macht sie angreifbar und Cyber-Security zu einem wesentlichen Faktor. Quantentechnologie basierend auf Quantenlicht verspricht eine absolut sichere Kommunikation.

Forscher*innen der Johannes Kepler Universität Linz ist es gemeinsam mit der Uni Wien gelungen, erstmalig eine neuartige Quantenlichtquelle für die Erzeugung von verschränkten Lichtteilchen aus Halbleiternanostrukturen für eine sichere Quantenkommunikation zu demonstrieren. Ein wesentlicher Vorteil dieser Lichtquellen ist die Rauscharmut und im Prinzip höherer Datenrate gegenüber bisher genutzten Lichtquellen.

Mit 85 Bit pro Sekunde ist die Übertragung zwar noch nicht praxistauglich, aber: „Die Quantenübertragung war nicht nur fehlerfrei – sie kann auch nicht mehr unbemerkt abgehört werden“, erklären die JKU Physiker DI Christian Schimpf und Prof. Armando Rastelli (Abteilung für Halbleiterphysik). Jeder Versuch würde die Verschränkung zwischen den Photonen stören – und somit auffallen, noch ehe die Übertragung stattfindet.

Gelungene Übertragung zwischen Gebäuden

Tatsächlich gelungen ist die Informationsübertragung zwischen dem Physikgebäude der JKU und dem Open Innovation Center des Linz Institute of Technology. „Damit ist die technische Machbarkeit nachgewiesen“.

Anders als bei vorherigen Demonstrationen stammen die Photonen erstmalig aus Halbleiternanostrukturen, sogenannten Quantenpunkten, die aus Materialien ähnlich wie herkömmliche Lichtquellen für die faserbasierte Kommunikation aufgebaut sind. Der Vorteil dieser Methode: „Zwar ist noch weitere Forschung notwendig, aber mit unserer Methode sind Übertragungsraten im Bereich von hunderten Megabit pro Sekunde durchaus möglich“, ist Rastelli sicher.

Ein weiterer Vorteil besteht in der Qualität der erzeugten Photonen. „Quantenpunkte erzeugen wirklich Photonen in einer Qualität, die bisher genutzte Photonenquellen nicht erreichen“, so Philip Walther. Daher sind diese Art von Quellen nicht nur für die Quantenkommunikation von Interesse, sondern auch für optische Quantencomputer und Quantensimulatoren. Das Paper wurde gestern im renommierten Journal "Science Advances" unter dem Titel „Quantum Cryptography with highly entangled photons from semiconductor quantum dots“ publiziert.

EU-Interesse an Forschung

Die Teams aus Linz und Wien sind durch die Partnerschaft in der Lage, ihr Wissen und ihre Erfahrung synergetisch zu kombinieren, um die Quanten-Verschlüsselung weiterzuentwickeln und an weiteren Anwendungen für die Quantenpunkte in den Bereichen Kommunikation, Sicherheit und Informationsverarbeitung zu forschen. Forschung in diesen Bereich wird vom Linz Institute of Technology (LIT) im Rahmen des Projektes „EQKD-QD - Entanglement-Based Quantum Key Distribution with On-Demand Photons Generated by Semiconductor Quantum Dots“, dem LIT Secure and Correct Systems Lab, die FWF Forschungsgruppe FG5 „Multiphoton Experiments with Semiconductor Quantum Dots“ (geleitet von der JKU und mit Partner*innen an der Universität Wien und der Universität Innsbruck) sowie der EU unterstützt.