idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Karlsruher Institut für Technologie
Christian Könemann

02.04.2025
http://idw-online.de/de/news850059

Forschungsergebnisse
Informationstechnik
überregional

Neue Verschlüsselung schützt vor Quantenangriffen von morgen

Quantencomputer sind ein Schreckgespenst für die Datensicherheit. Denn solche könnten zukünftig viele der heute verwendeten Verschlüsselungsverfahren knacken. Dies betrifft unter anderem verschlüsselte E-Mails, Messenger-Dienste oder Online-Banking. Forschende des Karlsruher Instituts für Technologie (KIT) haben gemeinsam mit Partnern ein Verfahren entwickelt, das Internetverbindungen schon heute vor der Quantentechnologie von morgen verlässlich schützen kann.

Das Problem: „Die rasanten Fortschritte bei der Entwicklung von Quantencomputern sind eine Bedrohung für die Datensicherheit und verschlüsselte Kommunikation“, sagt Laurent Schmalen, Professor am Institut für Nachrichtentechnik des KIT. „Denn die gebräuchlichen Verschlüsselungsverfahren basieren auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen – also in Zahlen, die nur durch eins und sich selbst teilbar sind.“ Dieser Prozess sei für herkömmliche Computer extrem umständlich und zeitaufwendig, für Quantencomputer aber nicht, erklärt der Experte. „Und wer die Primfaktoren einer großen Zahl kennt, kann die Verschlüsselung brechen.“

Klassische Verfahren schützen vor Angriffen der Zukunft

Die Lösung: Quantenangriffe lassen sich dennoch mit klassischen Kryptografie-Verfahren abwehren, nämlich mit symmetrischer Verschlüsselung. Hierbei müssen beide Parteien vor dem Aufbau der verschlüsselten Verbindung einen virtuellen Schlüssel austauschen, um die übertragenen Daten später wieder decodieren zu können. Das ist zwar abhörsicher, bislang sind dafür aber komplizierte und teure Geräte notwendig. Jetzt haben die Forschenden hingegen lediglich herkömmliche Hardware eingesetzt: „Wir konnten den Quantenschlüsselaustausch mit Standardhardware aus der Glasfaserkommunikation durchführen, wie sie beispielsweise bei Glasfaseranschlüssen in Häusern und Wohnungen verwendet wird, und nicht mit kostspieligen Spezialgeräten“, sagt Schmalen. Dadurch sei binnen fünf Jahren ein flächendeckender Einsatz möglich. „So können wir das globale Telekommunikationsnetz abhörsicher machen.“

Erfolgreiche Demonstration

Am vergangenen Donnerstag, 27. März 2025, hat das Projektteam das Verfahren in Echtzeit an der Ludwig-Maximilians-Universität München demonstriert. Dabei wurde eine Videoübertragung über eine Glasfaser am Campus realisiert, die mit dem Quantenschlüsselaustausch geschützt war. Die Forschenden des KIT haben dafür neuartige Algorithmen zum Schlüsselabgleich entwickelt. Diese stellen sicher, dass beide Parteien, die eine verschlüsselte Verbindung aufbauen wollen, einen absolut identischen Schlüssel besitzen und dabei trotzdem die Verbindung abhörsicher ist. „Unsere neuen Algorithmen zum Schlüsselabgleich sind ein entscheidender Schritt, um abhörsichere Verbindungen zu gewährleisten. Sie passen sich dynamisch an wechselnde Bedingungen an und

verhindern, dass Angreiferinnen und Angreifer Informationen aus dem Schlüsselaustausch gewinnen können“, erläutert Schmalen.

Tobias Fehenberger, Director R&D; bei ADVA Network Security, ergänzt: „Das Projekt markiert einen bedeutenden Meilenstein in der Entwicklung quantensicherer Verschlüsselung. Durch die erfolgreiche Validierung eines modularen, leistungsstarken Systems beweist es, dass Quantensicherheit mit kommerziellen Komponenten und einer offenen Architektur praxistauglich eingesetzt werden kann.“

Das Bundesministerium für Bildung und Forschung (BMBF) förderte das Projekt „Entwicklung hochperformanter Übertragungskomponenten für quantensichere Kommunikation über Glasfaserleitungen in Metro- und Weitverkehrsnetzen“ (DE-QOR) mit 3,4 Millionen Euro. Davon erhielt das KIT rund 350 000 Euro. Projektpartner neben dem KIT und der ADVA Network Security GmbH sind die Ludwig-Maximilians-Universität München, die Leibniz Universität Hannover sowie Microwave Photonics GmbH und Creonic GmbH.

Weitere Informationen: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/de-qor

Als „Die Forschungsuniversität in der Helmholtz-Gemeinschaft“ schafft und vermittelt das KIT Wissen für Gesellschaft und Umwelt. Ziel ist es, zu den globalen Herausforderungen maßgebliche Beiträge in den Feldern Energie, Mobilität und Information zu leisten. Dazu arbeiten rund 10 000 Mitarbeiterinnen und Mitarbeiter auf einer breiten disziplinären Basis in Natur-, Ingenieur-, Wirtschafts- sowie Geistes- und Sozialwissenschaften zusammen. Seine 22 800 Studierenden bereitet das KIT durch ein forschungsorientiertes universitäres Studium auf verantwortungsvolle Aufgaben in Gesellschaft, Wirtschaft und Wissenschaft vor. Die Innovationstätigkeit am KIT schlägt die Brücke zwischen Erkenntnis und Anwendung zum gesellschaftlichen Nutzen, wirtschaftlichen Wohlstand und Erhalt unserer natürlichen Lebensgrundlagen. Das KIT ist eine der deutschen Exzellenzuniversitäten.

wissenschaftliche Ansprechpartner:

Dr. Felix Mescoli
Pressereferent
Tel.: +49 721 608 41171
felix.mescoli@kit.edu

URL zur Pressemitteilung: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/de-qor