PRESSEINFORMATION

Erste quantengesicherte Videokonferenz zwischen zwei Bundesbehörden

Initiative QuNET demonstriert hochsichere und praxisnahe Quantenkommunikation

Bonn

In Bonn haben heute erstmals zwei deutsche Bundesbehörden quantengesichert per Video kommuniziert. Das Projekt QuNET, eine vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Initiative zur Entwicklung hochsicherer Kommunikationssysteme, zeigt damit, wie Datensouveränität in Zukunft gewährleistet werden kann. Diese Technologie wird nicht nur für Regierungen und Behörden wichtig sein, sondern auch um Daten des täglichen Lebens zu schützen.

Es war ein Vorgeschmack auf die Kommunikation der Zukunft – oder besser: die »Datensicherheit« der Zukunft. Denn als Bundesforschungsministerin Anja Karliczek heute zu einer Videokonferenz mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einlud, war zumindest augenscheinlich für den Außenstehenden alles beim Alten. Gemeinsam mit Andreas Könen, Abteilungsleiter CI »Cyber- und IT-Sicherheit« im Bundesministerium des Innern, für Bau und Heimat (BMI) und BSI-Vizepräsident Dr. Gerhard Schabhüser unterhielt sich die Ministerin via Videostream.

Und doch schlägt diese Videokonferenz ein neues Kapitel in der hochsicheren Kommunikation der Zukunft auf. Denn was das Auge nicht sieht: Verschlüsselt wurde das Gespräch nicht mit herkömmlichen Methoden, sondern mittels Lichtquanten. Der Clou dabei: Versucht ein Angreifer auf die zur Datenübertragung verwendeten Schlüssel zuzugreifen, so werden die Lichtteilchen manipuliert. Diese Manipulation kann von Sender und Empfänger nachgewiesen und ein Abhörversuch damit verhindert werden. Der Nachweis beruht dabei auf physikalischen Prinzipien. Wurde ein Lauschangriff entdeckt, wird der Schlüssel verworfen und ein neuer erzeugt. Mittels dieser Strategie wird eine langfristige Sicherheit der vereinbarten Schlüssel erreicht. Damit ist ein neuer Meilenstein für die Vertraulichkeit von Daten in einer digitalen Welt gesetzt.

Ein neues Kapitel für die hochsichere Kommunikation der Zukunft

Notwendig wird diese sogenannte »Quantenkommunikation« insbesondere vor dem Hintergrund künftiger technologischer Entwicklungen: Quantencomputer und neue

Desiree Haak | Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF | Telefon +49 3641 807-803 |
Albert-Einstein-Straße 7 | 07745 Jena | www.iof.fraunhofer.de | desiree.haak@iof.fraunhofer.de

Algorithmen werden voraussichtlich in Zukunft in der Lage sein, bisher übliche Methoden zur Datenverschlüsselung zu knacken. Nach dem Motto »Store now, decrypt later« (dt.: »Jetzt speichern, später entschlüsseln«) können bereits heute Daten abgespeichert und später, z. B. mithilfe leistungsfähigerer Rechner, ausgelesen werden.

Bedroht sind davon insbesondere Daten mit langfristigem Schutzbedarf, also jene Daten, die für Hackerinnen und Hacker auch in entfernter Zukunft noch von großem Wert sein werden. Dies beinhaltet nicht nur Informationen von Regierungen und Behörden, sondern auch Unternehmensgeheimnisse oder personenbezogene Gesundheitsdaten von Bürgerinnen und Bürgern.

Hierzu erklärte Bundesforschungsministerin Anja Karliczek: »Quantenkommunikation ist eine der entscheidenden Schlüsseltechnologien in der IT-Sicherheit und kann uns für zukünftige Bedrohungsszenarien rüsten. Das ist wichtig, denn Sicherheit und Souveränität im Netz sind Voraussetzungen für eine stabile Demokratie. Ich habe daher vor zwei Jahren die QuNET-Initiative ins Leben gerufen. Sie ist ein wichtiger Motor zur Umsetzung von Forschungsergebnissen aus der Grundlagenforschung zur Quantenkommunikation in alltagstaugliche Systeme. Ziel ist es, mit den Arbeiten von QuNET und den weiteren durch das Bundesforschungsministerium geförderten Vorhaben im Bereich der Quantenkommunikation die Basis für ein Ökosystem von Herstellern und Anbietern von Quantenkommunikationslösungen in Deutschland zu schaffen. So bringen wir die innovativen Technologien und Komponenten zeitnah in die breite Anwendung.«

Um die Privatsphäre von Bürgerinnen und Bürgern sowie Staaten und Unternehmen auch in Zukunft schützen zu können, gibt es schon heute einen großen Handlungsbedarf. Dabei geht es nicht allein darum, neue und hochsichere Kommunikationssysteme basierend auf Quanten-Knowhow zu entwickeln, sondern auch Wege zu finden, diese neue Technik in bereits bestehende IT-Infrastrukturen (z. B. Glasfaserkabel) einzubinden sowie etablierte kryptografische Verfahren zu berücksichtigen. Eine besondere Herausforderung besteht zudem bei großen Distanzen. Hier können Satelliten eine zentrale Rolle spielen.

Langfristige Datensicherheit durch Verschlüsselung mit Quanten

Die QuNET-Initiative verfolgt das Ziel langfristige Datensicherheit zu ermöglichen. Auf dem Weg dorthin haben die Forscherinnen und Forscher aller beteiligten Institute nun die erste quantenbasierte Videokonferenz zwischen dem BMBF und dem BSI in Bonn realisiert. Im Fokus der QuNET-Arbeit steht dabei der sogenannte »Quantenschlüsselaustausch«, auch QKD genannt (kurz für engl.: »Quantum Key Distribution«). Die QKD ermöglicht den Austausch symmetrischer Schlüssel, deren

Sicherheit quantifizierbar ist. Das BSI begleitet dabei die Initiative QuNET und bereitet flankierende und unabhängige Prüfkriterien in internationaler Zusammenarbeit vor.

Bereits Ende des vergangenen Jahres präsentierten die an der Initiative beteiligten Forschungsgesellschaften – die Fraunhofer-Gesellschaft, die Max-Planck-Gesellschaft sowie das Deutsche Zentrum für Luft- und Raumfahrt (DLR) – wichtige Grundlagen für moderne und sichere Kommunikationsstandards. Die Wissenschaftlerinnen und Wissenschaftler haben demnach ebenso die Gesamtarchitektur für Systeme zur quantensicheren Kommunikation weiterentwickelt, wie auch Möglichkeiten zum Austausch von Quantenschlüsseln über lange, mittlere sowie kurze Distanzen mittels Freistrahl- und Fasersystemen.

Im Aufbau der ersten quantenbasierten Videokonferenz zwischen dem BMBF und dem BSI wurden nun mehrere Freistrahl- und Fasersysteme eingesetzt. Dies entspricht einem komplexeren Szenario als einer Verbindung über einen einzigen Kanal. Neben der erstmaligen Videokonferenzübertragung versteht sich der Versuchsaufbau dementsprechend auch als ein Experiment, in welchem wertvolle Erkenntnisse für die Kommunikation in komplexen Netzen der Zukunft gewonnen werden.

Zahlen und Fakten zur Initiative QuNET

Start:	Herbst 2019
Laufzeit:	7 Jahre
Fördermittelgeber:	Bundesministerium für Bildung und Forschung
Volumen:	125 Millionen Euro Förderung geplant
Beteiligte:	Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF, Fraunhofer Heinrich-Hertz-Instituts (HHI), Max-Planck-Institut für die Physik des Lichts (MPL), DLR-Institut für Kommunikation und Navigation
Webseite	https://www.qunet-initiative.de/

Fragen und Antworten zur Initiative QuNET

Warum diese Initiative?

Immer leistungsfähigere digitale Technologien wirken auf die Datennetzwerke von heute ein und sind zunehmend eine Gefahr für die Sicherheit der kritischen Infrastruktur der modernen

Informationsgesellschaft. Hinzu kommt die voranschreitende Entwicklung der Quantencomputer. Mit der Fähigkeit, eine Vielzahl von möglichen Optionen gleichzeitig zu berechnen und zu analysieren, werden nicht nur neue Chancen, sondern auch Risiken geschaffen. Viele der zurzeit weit verbreiteten Kernbestandteile der Verschlüsselung, auf denen die Sicherheit fußt, lassen sich damit brechen. Daher müssen vor allem Regierungsorganisationen, das Gesundheitssystem und sicherheitskritische Unternehmen ihre Sicherheitsinfrastrukturen überdenken und erneuern.

Was ist das Ziel der Initiative?

Primäres Ziel von QuNET ist die anwendungsorientierte Entwicklung der physikalisch-technischen Grundlagen sowie der notwendigen Technologien für hochsichere Kommunikationsnetze unter realen Bedingungen unter Nutzung der Quantenphysik. Dabei steht zunächst die praktische Anwendung für eine quantensichere Vernetzung, beispielsweise von Behörden im Vordergrund. Doch QuNET ermöglicht mehr als nur sichere Kommunikation: Die perspektivischen Anwendungen der Übertragungen von Quantenzuständen reichen bis hin zu vernetzten Quantencomputern, dem sogenannten Quanteninternet.

Wie ist der Stand der Technik bei der Quantenkommunikation?

Quantenkommunikation bietet viele Einsatzmöglichkeiten zum Wohl der Wirtschaft und der Gesellschaft. Davon ist der Quantenschlüsselaustausch (QKD) eines der wohl am besten untersuchten und international am weitesten fortgeschrittenen Beispiele.

Wie funktioniert Quantenverschlüsselung?

Die Quantenverschlüsselung macht sich die Eigenschaft von Quantenteilchen zunutze, dass sie nicht unbemerkt vermessen oder kopiert werden können. So erzeugt z. B. eine Quantenquelle Lichtpulse, die zwischen zwei Orten ausgetauscht werden. Aus den Ergebnissen einer quantenmechanischen Messung würde eine Manipulation oder ein Abhören der Lichtpulse erkannt werden. Darauf aufbauend lässt sich ein Schlüssel erzeugen, der nur dem Sender und Empfänger bekannt ist und der für eine Verschlüsselung genutzt werden kann. Dieses Verfahren ist auch gegen alle zukünftigen Angriffe durch einen Quantencomputer sicher. Um größere Distanzen zu überwinden, können Satelliten mit Quantenquellen die Quantenschlüssel über interkontinentale Distanzen erzeugen, oder aber künftige Entwicklungen sogenannter Quantenrepeater (vgl. Q.Link.X) genutzt werden.

Welche Forschungsinstitute sind an der Initiative beteiligt?

Das **Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF** mit Sitz in Jena forscht an der Weiterentwicklung von Licht als Mittel zur Lösung unterschiedlichster Fragestellungen und Anwendungsszenarien. Die Arbeit des 1992 gegründeten Forschungsinstituts konzentriert sich daher auf die anwendungsorientierte Forschung an der Lichtentstehung, Lichtführung und Lichtmessung. Gemeinsam mit Forschenden aus der Grundlagenforschung und Industrie entstehen innovativen Lösungen, die in der Wissenschaft und Wirtschaft einen technologischen Vorteil bedeuten und für die Photonik neue Anwendungsfelder erschließen.

Innovationen für die digitale Gesellschaft von morgen stehen im Mittelpunkt der Forschungsarbeit des **Fraunhofer Heinrich-Hertz-Instituts (HHI)** in Berlin. Dabei ist das 1928 gegründete Institut weltweit führend in der Erforschung von mobilen und optischen Kommunikationsnetzen und -systemen sowie der Kodierung von Videosignalen und Datenverarbeitung. Gemeinsam mit internationalen Partnern aus Forschung und Industrie arbeitet das Fraunhofer HHI im gesamten Spektrum der digitalen Infrastruktur – von der grundlegenden Forschung bis zur Entwicklung von Prototypen und Lösungen. Das Institut trägt signifikant zu den Standards für Informations- und Kommunikationstechnologien bei und schafft neue Anwendungen als Partner der Industrie.

Das **Max-Planck-Institut für die Physik des Lichts (MPL)** in Erlangen deckt ein breites Forschungsspektrum ab, darunter nichtlineare Optik, Quantenoptik, Nanophotonik, photonische Kristallfasern, Optomechanik, Quantentechnologien, Biophysik und – in Zusammenarbeit mit dem Max-Planck-Zentrum für Physik und Medizin – Verbindungen zwischen Physik und Medizin. Das MPL wurde im Januar 2009 gegründet und ist eines der über 80 Institute der Max-Planck-Gesellschaft, die Grundlagenforschung in den Natur-, Bio-, Geistes- und Sozialwissenschaften im Dienste der Allgemeinheit betreiben. Heute arbeiten knapp 400 Menschen aus rund 40 Nationen am Institut. Die Forscherinnen und Forscher verfügen zum Teil über jahrzehntelange Erfahrung im Bereich der Quantenkommunikation. Dabei verwenden sie auch Telekom-Technologie für den Austausch von Quantenschlüsseln, was erlaubt, die Verfahren schnell kommerziell zu nutzen. Darüber hinaus untersucht das Institut seit mehr als zehn Jahren, wie sich die Schlüssel am Boden mit Laserlicht über mehrere Kilometer übertragen lassen (Freistrahlverbindung genannt) oder per Satellit über größere Distanzen. Dabei ist das MPL – auch in Zusammenarbeit mit der nationalen Industrie – an vielen großen nationalen und internationalen Projekten maßgeblich beteiligt.

Das **DLR-Institut für Kommunikation und Navigation** widmet sich der missionsorientierten Forschung in ausgewählten Bereichen der Kommunikation und Navigation. Seine Arbeiten reichen dabei von den theoretischen Grundlagen bis hin zur Demonstration neuer Verfahren und Systeme im realen Umfeld und sind in die DLR-Programme Raumfahrt, Luftfahrt, Verkehr, Digitalisierung und Sicherheit eingebettet. Das Institut beschäftigt derzeit rund 200 Mitarbeitende, darunter 150 Wissenschaftlerinnen und Wissenschaftler, an den Standorten Oberpfaffenhofen und Neustrelitz. Das Institut erarbeitet Lösungen zur globalen Vernetzung von Mensch und Maschine, zur hochpräzisen und zuverlässigen Positionierung für zukünftige Navigationsanwendungen sowie Verfahren für autonome und kooperative Systeme im Verkehr und in der Exploration. Darüber hinaus befasst sich das Institut mit der Cybersicherheit. Zu den Schwerpunkten in diesem Bereich zählen u. a. die Post-Quantum-Kryptografie und die Übertragung von Quantenschlüsseln per Satellit.