FRAUNHOFER-INSTITUT FÜR ANGEWANDTE OPTIK UND FEINMECHANIK IOF

PRESSEINFORMATION

Cyberangriffe auf Gasleitsysteme & Co. verhindern

Neues Forschungsprojekt MANTIS will mithilfe von Quanten kritische Infrastruktur schützen

Jena

Sichere Gasleitsysteme, ebenso wie Stromtrassen oder Kommunikationsnetzwerke, sind essenziell und zählen daher zur kritischen Infrastruktur. Angesichts der Bedrohung durch Cyberangriffe zielt ein neues Forschungsprojekt unter der Leitung des Fraunhofer-Instituts für Angewandte Optik und Feinmechanik IOF in Jena darauf ab, diese Netzwerke mithilfe moderner Quantentechnologie vor Hackerangriffen zu schützen. Im Projekt MANTIS werden speziell die Vorteile der sogenannten MDI-QKD gegenüber klassischen QKD-Verfahren erforscht. Das Projekt im Umfang von fünf Millionen Euro ist nun offiziell mit einem Kickoff gestartet.

»Die jüngsten Überschwemmungen in Süddeutschland haben gezeigt, was es bedeuten kann, wenn Strom, Gas oder Wärmeversorgung zusammenbrechen«, sagt Dr. Christopher Spiess. Der Fraunhofer-Forscher koordiniert das Projekt MANTIS, das heute mit einem Kickoff in Jena in seine dreijährige Laufzeit gestartet ist.

Ziel des Projektes ist es, die Sicherheit von kritischen Infrastrukturen wie Gasleitnetzen, Stromtrassen oder Kommunikationssystemen zu revolutionieren. Denn im digitalen Zeitalter sind es nicht allein Naturkräfte, sondern allem voran Cyberangriffe von Menschenhand, die eine akute Bedrohung für die Sicherheit derartiger Netzwerke darstellen.

MANTIS will diese Netzwerke daher robuster gegen solche Angriffe machen. Die Technologie, die im Mittelpunkt der Forschungs- und Entwicklungsarbeit steht, ist die Quantenkommunikation, insbesondere die sogenannte Quantenschlüsselverteilung (QKD). Diese nutzt Prinzipien der Quantenphysik, um hochsichere Kommunikationswege zu schaffen.

Neues Maß an Sicherheit dank QKD unabhängig von Messgeräten

Gegenüber standardmäßiger QKD will das Projekt MANTIS einen wichtigen Schritt weitergehen: Das Projekt zielt auf die Entwicklung einer messgeräteunabhängigen und chipbasierten QKD (MDI-QKD) ab. Als spezifischer Anwendungsfall wird der Einsatz für Gasleitsysteme untersucht werden. Die Abkürzung MANTIS steht daher für: »**M**essgerätunabhängige QKD und sichere Systemsynchronisation für **AN**wendungen in Gasle**i****T**systemen und kritischer **I**nfra**S**truktur«.

Redaktion
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

MANTIS adressiert damit eine der größten Herausforderungen bei der Umsetzung von klassischen QKD-Systemen: die sogenannten Seitenkanalangriffe. Diese können bei standardmäßiger QKD auftreten, wenn Angreifer Zugang zu den Messgeräten haben, die zur Entschlüsselung der Quantenschlüssel beim Empfänger genutzt werden.

»Bei standardmäßiger QKD befinden sich die Messgeräte des Empfängers in einer sicheren Umgebung. Auf diese Weise wird ein Zugriff durch Unbefugte von außen verhindert«, erklärt Projektleiter Christopher Spiess. »Wenn allerdings ein Angreifer physischen Zugang zu den Messgeräten bekäme, dann ist das standardmäßige QKD nicht mehr sicher.«

Vorteile der MDI-QKD gegenüber traditionellen QKD-Ansätzen

Demgegenüber ist die MDI-QKD, um die sich beim Projekt MANTIS alles dreht, eine spezielle Form der QKD. Hier übermitteln mehrere Nutzer Quantensignale an einen zentralen Knoten. Durch die Überprüfung der Korrelation von Messergebnissen wird die Vertraulichkeit des Schlüsselaustauschs gewährleistet und eine Reihe bekannter Angriffsvektoren auf das Detektionssystem ausgeschlossen.

Anders als die standardmäßige QKD ermöglicht die MDI-QKD selbst dann einen sicheren Austausch von Quantenschlüsseln, wenn ein Angreifer physischen Zugang zu den Messgeräten hat. »Alle Messgeräte können hier praktisch direkt in den Händen eines Hackers liegen. Allerdings nützt der Zugang zu den Messgeräten dem Angreifer nichts, denn das MDI-QKD-Protokoll stellt sicher, dass die Messinformationen für den Abhörer unbrauchbar sind«, führt Spiess weiter aus. »Mit MANTIS setzen wir neue Maßstäbe in der Quantenkommunikation. Die MDI-QKD geht über die traditionellen Ansätze hinaus und bietet daher auch unter extremen Bedingungen maximale Sicherheit.«

Twin-Field QKD: »Ein wichtiger Meilenstein hin zu extremen Entfernungen«

Zusätzlich soll das Projekt MANTIS ein wichtiger Zwischenschritt hin zur sogenannten Twin-Field QKD (TF-QKD) sein. Im Gegensatz zu klassischen Methoden, bei denen Sender und Empfänger direkt miteinander kommunizieren, wird bei MANTIS ein dritter Punkt, eine Zwischenstation, eingeführt. Dieser Aufbau ist sehr ähnlich zu TF-QKD, wo zusätzlich noch eine hochgenaue Stabilisierung der Wegstrecken eine Rolle spielt. Diese Stabilisierung ermöglicht es mit TF-QKD besonders weite Übertragungsstrecken zu erreichen.

»Aktuelle Forschungen zeigen, dass mit TF-QKD Distanzen von bis zu 1.000 km in optischer Glasfaser überbrückt werden können«, erläutert Spiess. »Aufbauend auf dem Vorhaben in MANTIS soll es perspektivisch ein solches Twin-Field-Protokoll geben. Die Arbeit im Projekt MANTIS ist daher auch ein wichtiger Meilenstein hin zu extremen Entfernungen für die Quantenkommunikation.«

Projektpartner im Projekt MANTIS

Das Projekt MANTIS wird mit einem Budget von 5,11 Millionen Euro umgesetzt werden. Davon fließen ca. 1,45 Millionen Euro an das Fraunhofer IOF in Jena. Das Forschungs- und Entwicklungsvorhaben ist bis 2027 angelegt und wird vom Bundesministerium für Bildung und Forschung (BMBF) mit einem Förderanteil von 86% unterstützt.

Zu den Partnern gehören neben dem Fraunhofer IOF auch das Fraunhofer-Institut für Integrierte Schaltungen IIS/EAS aus Dresden sowie das Fraunhofer-Institut für Angewandte Informationstechnik FIT mit seinem Standort Aachen. Weiterhin gehören die Universität Münster sowie das Unternehmen PSI Software SE aus Berlin dem Konsortium an.

Über das Fraunhofer IOF

Das Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF in Jena betreibt anwendungsorientierte Forschung auf dem Gebiet der Photonik und entwickelt innovative optische Systeme zur Kontrolle von Licht – von der Erzeugung und Manipulation bis hin zu dessen Anwendung. Das Leistungsangebot des Instituts umfasst die gesamte photonische Prozesskette vom opto-mechanischen und opto-elektronischen Systemdesign bis zur Herstellung von kundenspezifischen Lösungen und Prototypen. Am Fraunhofer IOF erarbeiten rund 500 Mitarbeitende das jährliche Forschungsvolumen von 40 Millionen Euro.

Weitere Informationen über das Fraunhofer IOF finden Sie unter:
www.iof.fraunhofer.de

FAQ: Fragen und Antworten rundum Quanten(-kommunikation)

Was sind Quanten überhaupt?

Die Welt ist eine Quantenwelt. Soll heißen: Alles besteht aus Quanten, sofern wir uns nur hinreichend kleine Systeme anschauen. Denn Quanten sind die kleinsten und unteilbaren Einheiten, die physikalische Wechselwirkungen hervorrufen. Auch Photonen, also Lichtteilchen, sind demnach winzige Quantenobjekte.

Diese Quantenobjekte besitzen faszinierende Eigenschaften, die sich Forschende bei der Entwicklung von modernsten Quantentechnologien zu Nutze machen. Eine besondere Eigenschaft ist dabei die Verschränkung von Quantenobjekten. Verschränkung bedeutet hier, dass Paare miteinander verschränkter Teilchen (z. B. Photonen) erzeugt werden. Ein jedes Teilchen weiß dabei stets um den exakten Zustand seines »Zwillings« – selbst dann, wenn dieser weit entfernt ist.

Wie können wir mithilfe von Quanten unsere Daten bzw. Kommunikation schützen?

Unsere moderne Welt ist hochvernetzt und deswegen in besonderem Maße anfällig für Cyberangriffe. Attacken z. B. auf kritische Infrastrukturen wie etwa Energieversorgungssysteme können dabei nicht nur sensible Daten, sondern potenziell Leben gefährden. Derzeit werden unsere Kommunikationssysteme mit kryptografischen Algorithmen verschlüsselt, die auf der Lösung bestimmter numerischer Probleme basieren. Das zu erwartende Aufkommen des Quantencomputers – d. h. Hochleistungsrechner der nächsten Generation, die Rechenaufgaben, für die konventionelle Rechner mehrere Jahre brauchen würden, binnen Sekunden lösen können – sowie mögliche Durchbrüche in der Mathematik gefährden die Sicherheit dieser Methode jedoch nachhaltig. Aus diesem Grund bedarf es neuer Ansätze, um schon heute die langfristige Sicherheit unserer Daten sicherzustellen.

Und was sind in diesem Zusammenhang Quantenschlüssel bzw. ein Quantenschlüsselaustausch (QKD)?

Die Kommunikation mithilfe von Quanten verspricht ein völlig neues Maß an Sicherheit. Im Gegenzug zu konventionellen Kryptografie-Verfahren basiert die Quantenkryptografie auf physikalischen Prinzipien. Eine mögliche Methode ist dabei die Messung miteinander verschränkter Lichtteilchen, die zuvor zwischen Sender und Empfänger ausgetauscht wurden. Die technologische Grundlage dafür ist der sogenannte Quantenschlüsselaustausch, auf Englisch »Quantum Key Distribution«, kurz: QKD.

Die QKD ermöglicht die gemeinsame Nutzung von Zufallsschlüsseln zwischen legitimen Nutzern, indem sie besondere Sicherheit auf der Grundlage der Gesetze der Quantenmechanik und nicht auf der Rechenleistung eines Gegners garantiert.

Wissenschaftlicher Kontakt

Dr. Christopher Spiess
Fraunhofer IOF
Abteilung Zukunftstechnologien / Projektleiter MANTIS

Telefon: +49 (0) 3641 807 - 571
Mail: christopher.spiess@iof.fraunhofer.de

Pressebilder

Folgendes Bildmaterial finden Sie im Pressebereich des Fraunhofer IOF unter https://www.iof.fraunhofer.de/de/presse-medien/pressemitteilungen.html zum Download.

Logo des Forschungsprojektes MANTIS © Fraunhofer IOF