Pressemitteilung:

Mehr Sicherheit im Quantenzeitalter: Innsbrucker Forschungsteam erhält Zuschlag für erstes rechtswissenschaftliches Projekt zur Zukunft der Quantentechnologie

Wien/Innsbruck, 13. Dezember 2024 – Unsere Welt wird immer digitaler und vernetzter. Dabei werden täglich riesige Datenmengen über das Internet verschickt – von Online-Shopping bis zu hochsensiblen Banktransaktionen. Klassische Verschlüsselungssysteme, die unsere Daten bisher schützen, stoßen jedoch an ihre Grenzen: Quantencomputer, die gerade entwickelt werden, könnten diese Sicherheit in naher Zukunft aushebeln. Das BSI in Deutschland geht davon aus, dass Quantencomputer 2030 existieren werden. Es braucht also dringend neue Lösungen, um uns vor Cyberangriffen zu schützen.

Hier kommt die sogenannte Quantum Key Distribution (QKD) ins Spiel, die auf den physikalischen Prinzipien der Quantenmechanik basiert. Damit können Nachrichten so verschlüsselt werden, dass sie selbst mit den mächtigsten Quantencomputern nicht geknackt werden können. Doch so vielversprechend diese Technologie klingt, so gibt es ein Problem: Theoretisch ist QKD absolut sicher, aber in der Praxis gibt es noch einige Herausforderungen. Die heutigen Geräte, mit denen QKD umgesetzt wird, sind nicht perfekt, was zu Sicherheitslücken führen kann.

Um genau das zu ändern, haben sich die Quantum Technology Laboratories GmbH (qtlabs) aus Wien, die TU Wien und die Universität Innsbruck zusammengetan und das Projekt „Numerical Security Proof Toolkit for Quantum Key Distribution“ ins Leben gerufen. Gefördert durch die FFG über 2,5 Jahre, entwickelt das Team ein Software-Toolkit, das die Sicherheit von QKD-Systemen unter realistischen Bedingungen analysieren kann. Ziel ist es, die momentane Lücke zwischen Theorie mit der Praxis zu schliessen und QKD damit alltagstauglich zu machen.

„Heutige Sicherheitsbeweise für QKD-Systeme nehmen perfekte Geräte an – das entspricht aber nicht der Realität,“ erklärt Dr. Max Riegler, Projektleiter bei qtlabs. „Das hat auch zu Kritik von Cyber-Sicherheitsbehörden wie dem BSI geführt. Unser Projekt schließt diese Lücke, indem wir Sicherheitsbeweise entwickeln, die die Unvollkommenheiten heutiger Quantengeräte berücksichtigen und trotzdem garantieren, dass die Kommunikation quantensicher bleibt.“

Neben der technischen Umsetzung leistet das Projektteam auch wichtige Grundlagenarbeit. Die TU Wien, bekannt für ihre Expertise in Quantenkryptographie, arbeitet an den theoretischen Grundlagen. Prof. Glaucia Murta von der TU Wien erklärt: „Quantencomputer sind ein unglaubliches Werkzeug – sie könnten die Entwicklung neuer Materialien, Medikamente oder Logistiklösungen revolutionieren. Gleichzeitig stellen sie eine große Gefahr für unsere Cybersicherheit dar. Mit unserem Beitrag im Projekt legen wir die Basis für die Sicherheitsarchitektur der Zukunft.“

Auch die rechtlichen und ethischen Aspekte werden genau unter die Lupe genommen. Das Team der Universität Innsbruck, geleitet von Prof. Dr. Matthias C. Kettemann, untersucht, wie Standards und Richtlinien entwickelt werden können, die Fairness gewährleisten und digitale Ungleichheiten abbauen. „Es ist wichtig, dass der Fortschritt in der Quantenverschlüsselung allen zugutekommt,“ betont Prof. Kettemann. Gleichzeitig analysiert das Innsbrucker Team, wie internationale und europäische Normen für kritische Infrastrukturen mit den neuen Zertifizierungsstandards zusammenpassen, die das Toolkit schaffen wird. „Bei sozialen Medien und bei der KI haben wir zu spät reguliert“, meint Digitalisierungsforscher Prof. Kettemann, der das Institut für Theorie und Zukunft des Rechts an der Universität Innsbruck leitet: „Bei der Quantentechnologie haben wir alle Chancen, gute Regeln zu setzen, die Innovation fördern, aber negative individuelle und gesellschaftliche Folgen – etwa für die Sicherheit – reduzieren.“

Am Ende des Projekts soll ein Software Toolkit stehen, das Unternehmen und Institutionen dabei hilft, ihre QKD-Systeme zu bewerten und zu zertifiezieren. Gleichzeitig gibt das Projekt Handlungsempfehlungen, wie sich QKD sicher und effizient in der Praxis einsetzen lässt. Mit diesem interdisziplinären Ansatz macht das Projekt einen entscheidenden Schritt, um QKD zu einem festen Bestandteil moderner Cybersicherheitslösungen zu machen und Europa im Quantenzeitalter wettbewerbsfähig zu halten.

Kontakt:

Universität Innsbruck
Institut für Theorie und Zukunft des Rechts
Innrain 15, 6020 Innsbruck
Univ.-Prof. Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard)
Professur für Innovation, Theorie und Philosophie des Rechts
E-Mail: matthias.kettemann@uibk.ac.at