Pressemitteilung

Quantensicherheit made in Germany – Startschuss für Industrieverbund

Deutscher Industrieverbund für Quantensicherheit (DIVQSec) gegründet mit dem Ziel, industriell nutzbare Lösungen für quantensichere Kommunikation und Kryptographie durch nationale Wertschöpfungskette zu fördern und dadurch technologische Souveränität zu gewährleisten

Die kryptographische Absicherung der kritischen Infrastruktur Deutschlands, sensibler Daten in Unternehmen oder des weltweiten Zahlungsverkehrs gegen Angriffe von außen bekommt in unserer zunehmend vernetzten und digitalisierten Welt einen immer höheren Stellenwert. Ebenso wichtig ist der zuverlässige Schutz staatlicher Informationen, um auch künftig nationale Souveränität gewährleisten zu können.

Aktuelle Entwicklungen in der Quantentechnologie und hier insbesondere die Fortschritte im Bereich Quantum Computing stellen eine neue Herausforderung dar, denn etablierte und weitverbreitete kryptographische Verfahren können gebrochen werden. Mit entsprechenden Quantenalgorithmen ist es möglich, aus dem notwendigerweise öffentlichen Schlüssel asymmetrischer Verfahren auch den eigentlich geheimen privaten Schlüsselanteil zu rekonstruieren. Dadurch ist ein wesentlicher Teil der kryptographischen Infrastruktur gefährdet, und es müssen neue Lösungen entwickelt werden.

Eine dieser Lösungen ist die „Quantenschlüsselverteilung“ (QKD für das englische „Quantum Key Distribution“). Bei korrekter Implementierung ist QKD informationstheoretisch beweisbar sicher – auch gegen noch unbekannte Quantenalgorithmen oder gegen Attacken durch Supercomputer in Kombination mit neuen mathematischen Überlegungen. Alternative Ansätze verfolgen eine algorithmische Lösung und untersuchen komplexere mathematische Probleme, um Angriffe auf den Schlüsselaustausch abzuwehren („Post Quantum Cryptography“ (PQC) oder „Quantum Resistant Algorithms“ (QRA)).

Beide Wege bilden die tragenden Säulen für eine „quantensichere“ Kryptographie.

Die wissenschaftlichen Grundlagen dafür wurden in den letzten Jahrzehnten in Deutschland und international erarbeitet. Insbesondere wurden neue Komponenten, Protokolle und Systeme in den Quantentechnologien entwickelt. Europaweite Förderprogramme[1] zielen aktuell darauf ab, den technologischen Reifegrad zu erhöhen und eine Integration der Technologien in bestehende Infrastrukturen zu ermöglichen. In Deutschland[2] geschieht dies durch die Zusammenarbeit namhafter Institute, Universitäten und industrieller Partner in Verbundprojekten und Vorhaben. Exemplarisch hierfür sind großangelegte Projekte wie Q.Link.X[3] und QuNET[4] oder Projekte im PQC-Bereich, die verschiedene Anwendungsfälle adressieren[5].

[1] Quanten Flagship Programm der EU: https://qt.eu/
[2] „Quantentechnologien - von den Grundlagen zum Markt“, https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf und „Innovationspotenziale der Quantentechnologien der zweiten Generation“ https://www.acatech.de/publikation/innovationspotenziale-der-quantentechnologien/
[3] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/q-link.x
[4] https://www.bmbf.de/de/bmbf-initiative-qunet-baut-hochsicheres-quantennetzwerk-10126.html
[5] https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/pqk

Die Grundlagenforschung allein reicht jedoch nicht aus, um Anwendungen zu erschließen, die technisch und ökonomisch auf dem Markt vertretbar wären. Es ist deshalb notwendig, eine wertsteigernde Überführung der Forschungsergebnisse zu QKD und PQC in hochsichere Systeme für reale Einsatzfälle umzusetzen. Dies erfordert allerdings die langjährige Industrieerfahrung verschiedener Akteure aus den Bereichen der klassischen Kryptographie, Systemsicherheit, Komponentenherstellung und Systemintegration sowie der Netzarchitektur und des Netzbetriebs.

Um diese interdisziplinäre Aufgabe lösen zu können, wird ein Interessensverbund der deutschen Industrie mit nachfolgendem Manifest gegründet.

Manifest

Der Deutsche Industrieverbund für Quantensicherheit (DIVQSec) macht es sich zur Aufgabe, industriell nutzbare Lösungen für quantensichere Kommunikation und Kryptographie durch eine nationale Wertschöpfungskette zu fördern und somit technologische Souveränität zu gewährleisten.

Die Lösungen sollen im europäischen Wirtschaftsraum entwickelt und angeboten werden und als Grundlage zur Sicherung nationaler und europäischer kritischer Infrastruktur dienen. Insbesondere sollen sie auch staatliche Institutionen sowie hochsensible Daten in privatwirtschaftlichen Unternehmen schützen.

DIVQSec dient als Kommunikationsplattform und Gestalter eines Ökosystems zur quantensicheren Kryptographie und eines zukünftigen Quanten-Internets, um insbesondere der interdisziplinären Natur dieser Technologie gerecht zu werden.

Die Interessen der beteiligten Unternehmen werden durch DIVQSec konsolidiert und gemeinsam repräsentiert. Dadurch wird der Austausch zur Bundes- und Europapolitik, zu entsprechenden Interessensgruppen in anderen EU-Mitgliedsstaaten oder auf europaweiter Ebene, sowie zur Öffentlichkeit und der Grundlagenforschung gestärkt.

Beteiligte Partner:

ADVA Optical Networking SE

Deutsche Telekom AG

Industrieanlagen-Betriebsgesellschaft mbH

KEEQuant GmbH

OHB System AG

qutools GmbH

Rohde & Schwarz Cybersecurity GmbH
Rohde & Schwarz SIT GmbH

Tesat-Spacecom GmbH & Co. KG

TOPTICA Photonics AG