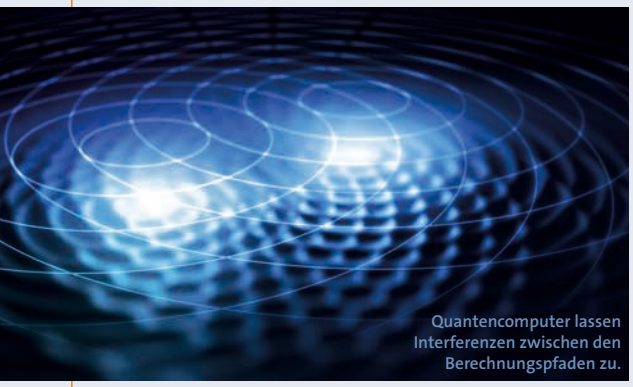
Potenzial für völlig neue technische Lösungen

QUANTEN TECHNOLOGIEN



Quantencomputer lassen Interferenzen zwischen den Berechnungspfaden zu.

Quantentechnologien bilden die Basis für Mikrochips, Laser, Breitbandinternet und Satellitennavigation. Effekte wie Quanteninterferenz und Quantenverschränkung sind erst heute technologisch nutzbar und bieten das Potenzial für völlig neue technische Lösungen wie Quantencomputer, Quantensensoren und -metrologie, Quantenkryptographie und -kommunikation sowie Quantensimulation. Die Forschung am FI CODE konzentriert sich auf die Themen Quantencomputing, Post-Quanten-Kryptografie und Quantenkommunikation.

So erreichen Sie uns

Forschungsinstitut CODE
Universität der Bundeswehr München
Carl-Wery-Str. 22
81739 München

code@unibw.de
+ 49 89 6004 -7302/-7303
www.unibw.de/code

Twitter: @FI_CODE
LinkedIn: Forschungsinstitut Cyber Defence (CODE)
YouTube: Forschungsinstitut Cyber Defence

Im Netz

Weitere Informationen über das Q-Lab des Forschungsinstituts CODE sowie über das Projekt MuQuaNet unter www.unibw.de/code/forschung/zentrallabore/q-lab und dtecbw.de/home/forschung/unibw-m/projekt-muquanet

Q-Lab des FI CODE

Projekt MuQuaNet

Redaktion: Lisa Scherbaum, Volker Eiseler / FI CODE; **Abbildungsnachweis:** IBM (2), iStock, Shutterstock (2); **Gestaltung:** M. Berwanger / Tausendblauwerk, www.tausendblauwerk.de

FI CODE

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

QUANTEN FORSCHUNG

der Bundeswehr
Universität München

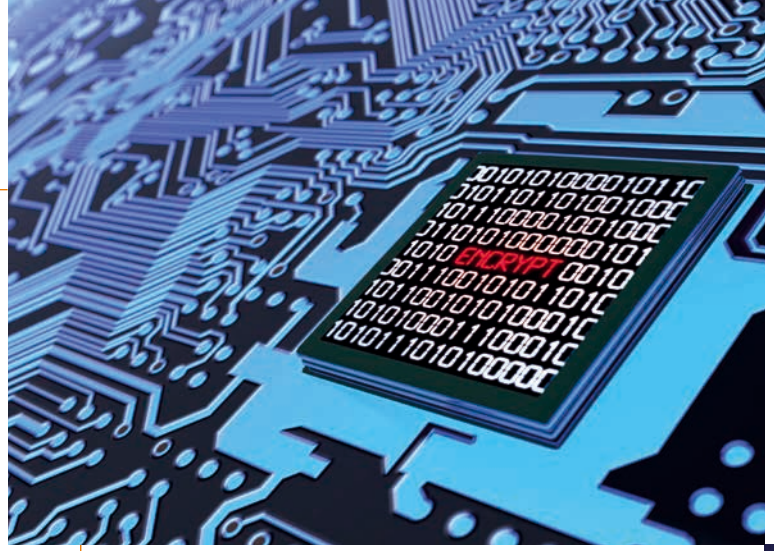
Quantencomputing

Ein völlig neues Berechnungsparadigma, das verspricht, einige der schwierigsten Probleme in Wissenschaft und Wirtschaft zu lösen – das ist Quantencomputing (QC).

Mögliche Anwendungsgebiete liegen in den Bereichen Energie, Finanzen, Gesundheitswesen sowie Luft- und Raumfahrt. Das Forschungsinstitut CODE beschäftigt sich seit 2018 wissenschaftlich mit Anwendungen, die mit universellen Quantencomputern umsetzbar sind: Forschungsthemen wie Quantenoptimierung (z. B. Lieferkettenoptimierung), Materialsimulation und Quantum Machine Learning werden auch auf Quantencomputern getestet.

Als Mitglied des IBM Quantum Network betreibt das FI CODE einen von weltweit nur 16 Zugängen zur IBM-Quantencomputer-Infrastruktur als sogenanntes IBM Q-Hub. Die aktuellen, noch mit Rauschen behafteten IBM Q-Hub-Quantencomputer verfügen über bis zu 65 Qubits mit einem aktuellen Quantenvolumen von 128. Zusätzlich zu der Entwicklung von Quantensoftware für mögliche Anwendungen sind Quantenschaltkreisoptimierung sowie Fehlerminderungs- und Fehlerkorrekturtechniken zentrale Forschungsthemen. ■

Der IBM-Quantencomputer im Inneren.



Quantencomputer werden die meisten bisherigen Verschlüsselungsverfahren unsicher machen.

Gefahren für die Kommunikation

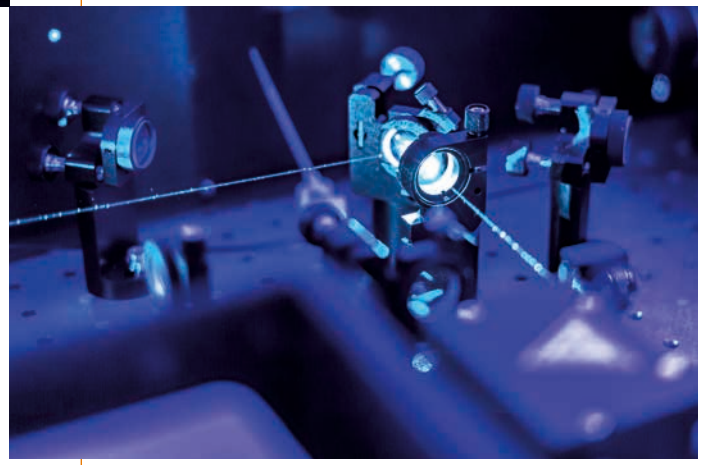
Sichere Kommunikation über das Internet ist eine wesentliche Voraussetzung für eine vertrauensvolle Zusammenarbeit in allen Bereichen unserer Gesellschaft.

Leistungsfähige, universelle Quantencomputer, die bereits in ersten Testversionen verfügbar sind, würden praktisch alle heute eingesetzten Public-Key-Verschlüsselungs- und Schlüsselaustauschverfahren unsicher machen. Bereits heute muss daher mit den Vorbereitungen für die „Post-Quanten-Zeit" begonnen werden. Betroffen sind dabei zum Beispiel der Austausch persönlicher Nachrichten, Videokonferenzen und Onlinebanking.

Zur Gewährleistung der staatlichen Souveränität ist die sensible militärische Kommunikation besonders abzusichern. Hierzu verfolgt das FI CODE zwei verschiedene Ansätze: den der Quantum Key Distribution aus der Quantenkommunikation sowie die **Post-Quanten-Kryptografie** (PQC) als Teilgebiet der klassischen Kryptografie. PQC ist eine neue Art der Verschlüsselung, die ohne Quantentechnologien auf klassischen Computern ausgeführt werden kann. Sie soll Sicherheit gegen Angriffe durch Quantencomputer bieten. ■

Quantum Key Distribution

Quantum Key Distribution (QKD) ist ein Verfahren, das die physikalischen Eigenschaften der Quantenmechanik nutzt, um zwei Parteien einen gemeinsamen, sicheren Schlüssel für die Kommunikation zur Verfügung zu stellen.



Laserreflektion auf optischem Tisch in einem Quantenlabor.

Die Sicherheit von QKD beruht auf physikalischen Gesetzmäßigkeiten: Ein potenzieller Angreifer, der die Schlüsselverteilung abhört, kann nur durch eine Messung an den verschickten Quantenzuständen Informationen abgreifen. Eine solche Messung ist jedoch invasiv, das heißt, sie verändert den Quantenzustand des Systems deutlich. Daher kann ein solcher Angriff schnell bemerkt und die Menge der abgegriffenen Informationen berechnet werden. Zur Erforschung und zum experimentellen Nachweis nutzbarer Quantum Key Distribution wurde 2020 das dtec.bw-Projekt MuQuaNet (Das **Qua**nten-**Net**zwerk im Großraum **Mü**nchen) aufgesetzt. Mehr dazu erfahren Sie online. ■