Cluster Natur- und Technikwissenschaftliche Rüstungskontrollforschung

Fact Sheet Februar 2024

Quantentechnologie

Quantentechnologie und ihre Sicherheitsrelevanz

Lena Bühring (CNTR/PRIF), Prof. Dr. Markus Gräfe (TU Darmstadt)

Der rapide Fortschritt in der Quantentechnologie ist eine der spannendsten technologischen Entwicklungen der letzten Jahre. Im sicherheitspolitischen Kontext wird sie oft zusammen mit anderen Dual-Use-Technologien wie Künstlicher Intelligenz (KI) oder additiven Fertigungsverfahren genannt. Ein wesentliches Unterscheidungsmerkmal der Quantentechnologie liegt darin, dass sie nicht als eine einzelne spezifische Technologie betrachtet werden kann. Stattdessen umfasst sie ein breites Spektrum verschiedener Technologien, die alle auf einem modernen Verständnis quantenmechanischer Prinzipien basieren. Diese innovativen Technologien bieten potenzielle militärische Vorteile, wie gesicherte Kommunikation und verbesserte Aufklärungsfähigkeiten durch präzisere Sensoren. Sie rufen jedoch auch Bedenken hinsichtlich der Sicherheit konventioneller Systeme hervor. Die relevanten Technologiebereiche der Quantentechnologie lassen sich in vier Hauptkategorien gliedern.

Computing

Quantencomputing ist eine Technologie, die auf den Gesetzen der Quantenmechanik basiert und Quantenzustände, sog. Qubits, nutzt, um komplexe Berechnungen schneller als traditionelle Computer durchzuführen. Quantencomputer werden als existenzielle Gefahr für traditionelle Verschlüsselungssysteme eingeschätzt. Allerdings sind Systeme, die aktuelle Verschlüsselungsverfahren wie RSA brechen können, noch einige Jahre entfernt. Die neu erschlossene Rechenkapazität von potenziell Tausenden von Qubits könnte aber auch zur Optimierung von KI zur Zielerfassung verwendet werden. Außerdem wäre perspektivisch eine verbesserte Auswertung von lückenhaften Sensordaten denkbar.

Kommunikation

Quantenschlüsselverteilung (QKD) verwendet Eigenschaften der Quantenmechanik wie Verschränkung, um abhörsichere Kommunikationskanäle zu schaffen, indem sie Schlüssel für die Codierung von Nachrichten auf sichere Weise überträgt. Neue, auf quantenmechanischen Zusammenhängen beruhende Verschlüsselungssysteme sind langfristiger resistent gegen Entschlüsselung und ihre Sicherheit ist nicht von vertrauenswürdiger Infrastruktur abhängig. Zwar wird QKD-Verschlüsselung bereits in einigen Kontexten zivil angewendet, die militärische Anwendung ist Anfang 2024 wegen hoher technischer Anforderungen bei der Implementierung aber noch in der Erprobung.

Sensorik

Quantensensorik nutzt quantenmechanische Eigenschaften wie Superposition und Verschränkung zur Messung physikalischer Größen wie Gravitation oder Zeit mit extrem hoher Präzision, weit über die Möglichkeiten konventioneller Sensoren hinaus. Quantentechnologie kann so zu Verbesserungen im Bereich Aufklärung beitragen. Neue Sensoren könnten präzise Veränderungen in magnetischen und elektrischen Feldern feststellen. Dies ist besonders nützlich, um dichte Massen wie zum Beispiel U-Boote oder Minen aufzuspüren. Durch optische Uhren auf Quantenbasis könnte präzise Navigation zudem unabhängig von GPS-Signalen werden. Letztere sind anfällig für elektronische Störmaßnahmen.

Bildgebung

Quantenbildgebung verwendet Phänomene wie Verschränkung, Korrelation und Kohärenz, um Bilder mit geringer Strahlung zu erzeugen, und ermöglicht das Erfassen bisher unsichtbarer Details in Medizin und Forschung durch die effiziente Erschließung extremer Spektralbereiche. Dies ermöglicht neue Werkzeuge für die biomedizinische Diagnostik und Pathogendetektion. Die Technologie könnte auch zur Fernaufklärung beitragen, etwa durch superempfindliche optische Abstandsmessung (Quantum-LIDAR) und Erkundungsmissionen, die vom Beobachtungsziel nur schwer bemerkt werden können.

Generationen der Quantentechnologie

Erste Generation: folgte auf die Entwicklung der Quantentheorie in den 1930er Jahren; heute weitläufig in Gebrauch.

Laser · integrierte Schaltkreise · Satelliten und GPS

Atomuhr · Magnetresonanztomografie (MRT)

Zweite Generation: befindet sich in der Entwicklungsphase oder ist seit kurzem in ersten Anwendungen auf dem Markt. Der Kern ist die präzise Kontrolle von einzelnen Quantensystemen.

Quantenrepeater · Quantensimulatoren · Quantenbildgebung

Quantengravimeter · universelle Quantencomputer

Quantum Key Distribution (QKD) · Quantenmagnetometer

Rasanter Anstieg der Rechenleistung

2
Qubits

Der erste Quantencomputer – entwickelt am MIT **1998**. Er kann nur bis vier zählen, simuliert aber bereits erfolgreich ein Quantensystem.

133
Qubits

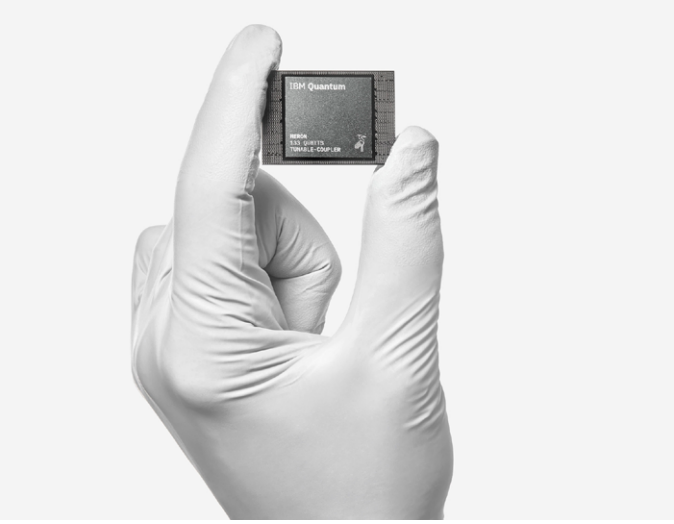
Der IBM Quantum Heron, vorgestellt im Dezember **2023**, ist robust und flexibel genug, um als Rechenwerkzeug in der Wissenschaft verwendet zu werden.

1.225
Qubits

Die Firma Atom Computing stellt Oktober **2023** den ersten Quantencomputer mit mehr als 1000 Qubits vor – eine besondere Herausforderung, da mit der Zahl an Qubits auch die Fehleranfälligkeit steigt.

10.000
Qubits

Dieser noch theoretische Quantencomputer könnte laut japanischen Forschern von Fujitsu möglicherweise in 104 Tagen einen heute üblichen 2048-bit RSA Encryption Key knacken.



IBM Quantum Heron (Photo: Ryan Lavine for IBM, CC BY-ND 2.0)

Die Leistungsfähigkeit von Quantencomputern hängt neben der Anzahl von Qubits auch von anderen Faktoren ab, etwa von den verwendeten Algorithmen und der Qualität der Fehlerkorrektur.

Anhang

Impressum

CNTR ist ein Forschungsverbund zwischen dem Peace Research Institute Frankfurt (PRIF), der Justus-Liebig-Universität Gießen und der Technischen Universität Darmstadt. www.cntrarmscontrol.org · V.i.S.d.P.: Elisabeth Waczek (PRIF), Baseler Straße 27–31, Frankfurt a.M., Deutschland, Telefon (069) 959104-0, cntr@prif.org, www.prif.org · Design: media | machine GmbH · Layout: CNTR

Gefördert durch: Auswärtiges Amt aufgrund eines Beschlusses des Deutschen Bundestages