bitkom

Steckbrief Quantencomputing

Perspektiven für den Verteidigungssektor | April 2022

AK Verteidigung: PG IT-Innovationen

Thema: Quantencomputing

Ausgangssituation

Beschreibung:

Quantencomputer verarbeiten Informationen, die in Form von Quantenbits (**Qubits**) dargestellt werden. Hieraus ergibt sich ein entscheidender Vorteil, denn Qubits können im Vergleich zu ihrem klassischen Analogon – den Bits – viel mehr Informationen gleichzeitig repräsentieren und verarbeiten somit in jeder einzelnen Rechenoperation mehr Daten.

Qubits sind die Grundeinheit des Quantencomputers. Durch das Prinzip der Superposition kann dieses nicht nur null oder eins sein, sondern auch eine Überlagerung beider Werte gleichzeitig repräsentieren. Während ein klassischer Computer nur für einzelne Eingaben nacheinander das Ergebnis errechnen kann, ermöglicht die Superposition dem Quantencomputer, mit mehreren Eingaben gleichzeitig zu rechnen. Das erhöht die Rechengeschwindigkeit drastisch.

- Unter Quantencomputing (QC) versteht man die Nutzung von Effekten auf Quantenebene zur Berechnung von Daten.
- Je nach Implementierung sind Rechenoperationen oftmals nur bei extrem niedrigen Temperaturen durchführbar. Einige technologische Ansätze können aber perspektivisch auch in normalen Temperaturumgebungen arbeiten.
- Die aktuell besten Quantencomputer haben meist nur circa 100 physikalische Quantenbits (Qubits). Vereinzelte Modelle haben bereits 500 Qubits. Für die meisten sinnvollen Anwendungen sind jedoch mehrere hundert stabile logische Qubits notwendig. Mehrere physikalische Qubits bilden dabei zwecks Fehlerkorrektur ein logisches Qubit. Es gilt zudem, dass nicht nur die Qubit-Anzahl, sondern vielmehr die Quantenstabilität und damit -qualität ausschlaggebend ist für erfolgreiche Operationen.
- In bestimmten Anwendungsfällen könnten Quantencomputer klassischen Computern deutlich überlegen sein.
- Quantencomputer können die mathematischen Probleme, auf denen asymmetrische Kryptografie beruht, deutlich schneller berechnen als klassische Computer. Auch symmetrische Verfahren sind durch Grover‘s search und ggf. durch die Quantum Algebraic Attack gefährdet. Quantencomputer können sowohl asymmetrische Kryptografieverfahren brechen, die auf dem diskreten Logarithmus basieren, als auch jene, deren Sicherheit auf der Laufzeit für Faktorisierungsverfahren beruht sowie die Sicherheit von symmetrischer Kryptografie halbieren.

- Bereits heute sind Brückentechnologien auf klassischer Siliziumchipbasis für bestimmte Anwendungen verfügbar, sei es Quantensimulation auf klassischen Hochleistungsrechnern oder durch Quanten-Annealing inspiriertes digitales Annealing.

Bewertung:

- Vorteilen von Quantencomputern stehen gegenwärtig noch viele Probleme bei der technischen Realisierung gegenüber. Das BSI hat in seiner Handlungsempfehlung »Migration zu Post-Quanten-Kryptografie« betont, dass die Bedrohung durch binäre Technologien (parallell computing e. g. hashcat, high performance computing) schon für eine Migration reicht.
- QC werden klassische Arbeitsplatzrechner oder Rechenzentren nicht ersetzen.
- Brückentechnologien auf Basis des »Quanten-inspired Computing« sind schon heute mit QC-Algorithmen nutzbar. Diese sind in der Lage, Lösungen für signifikante Problemgrößen zu liefern und fügen sich nahtlos in eine bestehende Datacenter-Infrastruktur ein.
- Hybride Ansätze, bei denen jede Technologie ihre speziellen Vorteile ausspielt, werden diskutiert und erforscht.
- Das Brechen heute gängiger Verschlüsselungen durch QC stellt ein Sicherheitsrisiko für Streitkräfte dar. Weitere Gefährdungen sind langfristig zu erwarten für bspw. Technologien wie Blockchain und damit für Logistiklösungen oder digitale Währungen [To instead break the encryption within one day, it would require only 13 million physical qubits. If the base physical error rate was instead the more optimistic value of 10−4, 33 million, physical qubits would be required to break the encryption in 1 hour. This large physical qubit requirement implies that the Bitcoin network will be secure from quantum computing attacks for many years (potentially over a decade)].
- Ebenso besteht die Gefahr für digitale Identitäten, insbesondere eMRTDs, da diese größtenteils chipbasiert auf asymmetrischer Kryptografie beruhen. Die Quantencomputerentwicklung geht derzeit schneller voran, als geglaubt.

Gemeinsames Ziel/Nutzungspotentiale

- Nutzung in der Geoinformatik
- Verbesserung der Aufklärung – Fähigkeit, aus komplexen Datenmengen Lagebilder zu erstellen
- Revolution von Kryptierverfahren, Kryptoanalyse, Resilienzverbesserung, Post-Quanten-Kryptografie
- Optimierungen in der Logistik (Routen- und Lageroptimierung) sowie finanzmathematische Berechnungen
- Optimierung der Führungsfähigkeit
- Einsatz als Mittel für die Abwehr ballistischer Raketen
- Neuerungen in der KI und Algorithmensystematik
- Kryptografie, QC-resistente Schlüsseleinigung
- Energieeinsparung, Einsatz in der Materialforschung und zum Erkennen des Abstrahlverhaltens / der Reflexionsoptimierung

- Cyber Warfare
- Simulation
- Operations Research
- Schließen von Fähigkeitslücken, z. B. im Bereich quantenresistenter Verschlüsselung
- Cyberdefense, z. B. durch Erkennung von Anomalien
- Big Data Analysis und Deep Learning
- sichere Quanten-Schlüsselverteilung für existierende VPN-Netzwerke

Stellgröße

- Schnelligkeit hinsichtlich F&E zur Nutzung in realen Umgebungen – Echtzeitanforderungen
- Effizienz (Verringerung des Ressourceneinsatzes zur Erlangung einer bestimmten Wirkung)
- Effektivität (Verbesserung des Wirkungsgrades bestimmter Funktionalitäten) – Qualitätsanforderungen, neue Anwendungsfelder erschließen, z. B. Optimierungen, die mit klassischen Ansätzen schwierig sind, disruptive Anforderungen
- Optimierungen in Bereichen klassischer Verfahren (Digital Annealing / Quantum Annealing = Abweichung von Optimum vs. Rechenzeit)
- Erkennen und Bewerten von Bedrohungsszenarien inkl. der Fähigkeit zur Reaktion
- Erreichen von Benchmark-Werten im internationalen Bereich (Outcome-orientiert)
- Verfügbarkeit und Zugang zu QC als Stellgröße
- Quantencomputerresistente Verfahren (Post-Quanten-Kryptografie, Schlüsseleinigung, Protokolle) entwickeln
- Fehlerkorrekturverfahren von QC verbessern, um Rauschen der Qubits zu kompensieren
- Qualität / Wirkungsgrad von Algorithmen

Maßnahmen/Vorgehensweise

- Entwicklung einer grundlegenden Idee für den Verteidigungssektor, wozu QC eingesetzt und genutzt werden kann und wie dies bereits in anderen Sektoren erfolgt ist.
- Es ist eine Abschätzung, mit welcher Geschwindigkeit sich die Fähigkeiten von Quantencomputern in den nächsten Jahren entwickeln werden und wo diese ihre Anwendung finden, nötig.
- Die Vorbereitung auf einen eventuellen Technologiesprung, sowohl bei der Hardware als auch bei den Algorithmen, inklusive der Nutzung vorhandener Brückentechnologien (Nutzung und ggf. Abwehr), ist zwingend.
- Der Übergang vom klassischen Computing sollte frühzeitig sichergestellt werden, inkl. der Validität klassischer Sicherheitstechnologie (Krypto & Blockchain)

- Hybride Anwendungsszenarien (klassische IT im Zusammenspiel mit Quantencomputern) sind einzuschätzen und zu bewerten
- Der mögliche Wettbewerbsnachteil in der Hardwareentwicklung sollte durch gezielte Förderung auf der Anwendungsseite ausgeglichen werden
- Quantencomputing kann für viele Anwendungsbereiche »Quantensprünge« generieren, noch aber ist der Schwerpunkt (Ressourceneinsatz) eindeutig auf den Bereich der Forschung zu legen.
- Brückentechnologien nutzen die gleichen Algorithmen wie QC und bieten schon jetzt die Möglichkeit des Know-how-Aufbaus und Berechnungen für erste Bereiche, z. B. Optimierungen (identisches Ökosystem)
- Die Krypto-Agilität muss bereits jetzt zum Design-Kriterium erhoben werden.
- Die Politik sollte die Verfügbarkeit und den Zugang zu Quantencomputern sicherstellen. Den wahren Mehrwert stellen, wie auch bei klassischer IT, die darauf laufenden Anwendungen dar. Diese sind für Quantencomputer zu entwickeln
- Evaluierung von Ideen zu den Begleittechnologien
- Intensivierung von Forschungsaktivitäten: Welche Anwendungen lassen sich sinnvollerweise mit Qcs rechnen – ggf. auch schon mit wenigen Qubits als Optimierungen – die mit klassischen Ansätzen schwierig wären und welche Anwendungen können in klassischen Bereichen verbleiben?