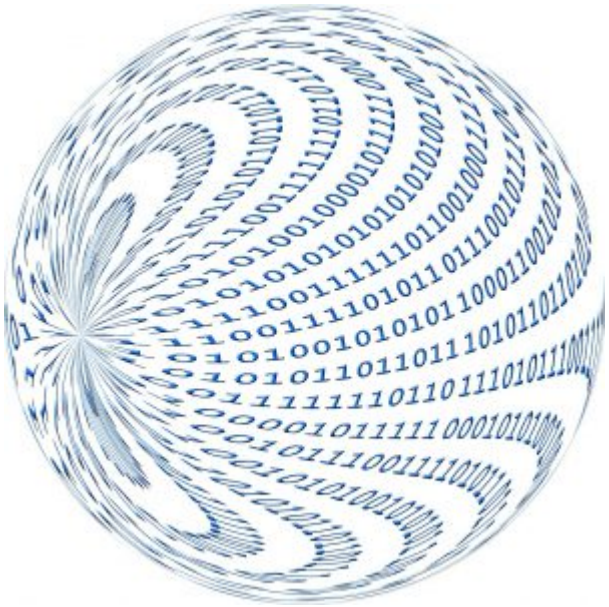
Quantencomputer als Risiko



Die Skepsis war groß. Aber die Wissenschaft hat es tatsächlich fertiggebracht, einen funktionierenden Quantencomputer zu bauen, und über die Cloud wird er sogar für kommerzielle User nutzbar gemacht (1.).

Damit ließe sich viel Unheil anrichten, ist die gebremst begeisterte Aussage dazu (2.). Nach der Skepsis also die Furcht – ist der Quantencomputer tatsächlich so ein Monstrum, dass man Angst vor ihm haben müsste? (Bild: geralt, pixabay)

Von der Theorie her unbedingt. Da geht es voll in die Quantenmechanik und ihre mathematischen Verstrickungen hinein (links alle von wiki). Der Quantencomputer nutzt Qubits, also Systeme, die nur durch die Quantenmechanik korrekt beschrieben werden. Sie sind durch die Superposition ihrer 0/1-Zustände gekennzeichnet, haben aber nur zwei durch Messung klar unterscheidbare Zustände. Alle Informationen des Qubits enthält nach der Kopenhagener Deutung der Quantenmechanik nur

(Psi), die Wellenfunktion, die den quantenmechanischen Zustand beschreibt. Das Ganze im Hilbertraum, einem Vektorraum über dem Körper der komplexen Zahlen, versehen mit einem

Skalarprodukt wie . Dort ist auch definiert, wobei

der quantenmechanische (Ortseigen-)Zustand mit dem *ket*-Symbol dargestellt wird.

Es gibt aber auch einfachere Methoden, die Wirkungsweise der Quantencomputer zu beschreiben. Zwei schöne Ansätze liefern Welt der Physik (3.) und Zeit Online (4.). Demnach ist der Quantencomputer nicht länger ein "Abenteuerspielplatz für kauzig-geniale Physiker". Neuerdings werde mächtig in diese "mysteriöse Technologie" investiert. Google, IBM und Microsoft sind dabei, die EU und China, Geheimdienste und sogar Volkswagen – warum?

Diese Frage beantwortete Zeit Online sich selbst schon vor ein paar Jahren: Datenkonzerne und Geheimdienste wollen noch mächtiger werden (5.). Es geht sogar um ein neues Rattenrennen für neue Cyberwaffen: Die existiserenden digitalen Verschlüsselungsmethoden lassen sich mit Quantencomputern angreifen (6. und 7.).

Bezeichnend ist die Skepsis vieler Leserkommentare. In der *Zeit* (4.) wird der Hype um den Quantencomputer mit dem um das Fusionskraftwerk verglichen. Bei Zero Hedge (7.) mit dem um das Anti-Raketen-Raketensystem, und ein ZH-Spezi liefert sogar einen Algorithmus:

1. dream big
2. bill bigger [cost++]
3. profit!
4. fail to deliver
5. iterate a new version before they figure out the original will never work
6. GOTO 2.

Tja, bei vielen – und nicht nur militärischen – Projekten funktioniert dieser Algorithmus einwandfrei. Aber die Skepsis beim Quantencomputer ist eigentlich schon von gestern, weil

das Konzept tatsächlich funktioniert. Das gibt den Lesern Raum für Verschwörungstheorien: US-Navy and -Airforce sind demnach schwer dabei, nur deshalb tun sie so, als ob es sie nicht interessiert.

Aber was ist das beschworene Risiko? Ursprünglich war die Idee, dass der Quantencomputer am besten Quantenprozesse abbildet, z.B. die in der Chemie (alle chemischen Reaktionen betreffen die Elektronenhüllen der Atome, und die Reaktionen der Elektronen gehorchen der Quantenphysik). Aber solche Quanten-Simulationen sind nur *ein* potentieller Bereich für Quantencomputer.

Es gibt auch (Quanten-Such-)Algorithmen wie den Grover-Algorithmus. Der basiert darauf, dass die Einträge in einem -dimensionalen Zustandsraum nur durch Wurzel Qubits dargestellt werden (ein Qubit enthält qua Superposition wesentlich mehr Informationen als ein Bit). Dort wird ein Operator (Orakel genannt) definiert, der den Eigenzustand des gesuchten Eigenwerts identifiziert, so dass man mit Versuchen gegenüber den herkömmlichen Rechenschritten auskommt (siehe O-Notation).

Entsprechendes gilt für den Shor-Algorithmus zur Faktorisierung großer Zahlen – und da wird es gefährlich. Denn auf der Primzahlzerlegung von großen Zahlen basiert die Sicherheit vieler Systeme zur verschlüsselten Datenübertragung, Beispiel Kryptosysteme.

Bei Verschlüsselung und Signatur von Daten werden Zahlenpaare und verwendet, wobei ein Produkt aus zwei großen Primzahlen ist. Der Verschlüsseler berechnet aus seiner Nachricht den Geheimtext , er verschickt diesen Geheimtext , und der Entschlüssler kriegt

aus die Nachricht zurück. Das Problem für Datendiebe liegt in der Schwierigkeit, einen Hilfswert (p-1) (q-1) zu finden, der für die Schlüsselerstellung nötig ist, ohne die Faktoren p und q zu kennen.

Dazu muss er sehr lange herumprobieren, und die Quantencomputer schaffen das mit viel weniger Versuchen. Panik ist aber noch nicht angebracht, denn auch die Quantencomputer haben so ihre Problemchen. Sie müssen sehr tief gekühlt werden, damit sie kohärent bleiben, damit also die Quantenzustände erhalten bleiben. Die Dekohärenz tritt nach ca. 1/10 sec ein; bis dahin müssen die Rechnungen abgeschlossen sein. Zusätzlich gibt es jede Menge Probleme, die auf all die Unwägbarkeiten im Quantenmilieu zurückgehen.

Aber das Risiko ist real, zumal sich auf dem Krypto-Gebiet eine Menge schlauer Tunichtgute tummeln.

Medien-Links:

1. Erster Quantencomputer wird kommerziell – An die Cloud angeschlossener Quantencomputer bald auch für Unternehmen nutzbar (Scinexx 7.3.17): *Der Computerkonzern IBM will in wenigen Monaten den ersten Quantencomputer für kommerzielle Zwecke nutzbar machen. Schon jetzt ist das fünf-Qubit-System "IBM Q" für Forschungsexperimente über die Cloud verfügbar.* (Die Rede ist von einem Rechner mit 5 Qubits, der auf 20 Qubits erweitert werden soll. Der Einsatz soll vor allem in der Chemie stattfinden).
2. „Damit ließe sich viel Unheil anrichten“ (brand eins 3/18): *Quantencomputer sollen die IT revolutionieren. Doch sie könnten auch gängige Verschlüsselungsverfahren knacken.* Demnach hat IBM kürzlich einen Quantenchip mit 50 Quantenbits vorgestellt, D-Wave Systems sogar ein komplexes System mit mehr als 2000. Damit es gefährlich

wird, müsste man angeblich Millionen Qubits haben.

3. Wie funktioniert ein Quantencomputer? (Welt der Physik 26.2.16): *Auch wenn Wissenschaftler weltweit auf dieses Ziel hinarbeiten, Quantencomputer außerhalb der Laborsituation wird es erst einige Jahrzehnte in der Zukunft geben. Allerdings sah noch vor siebzig bis achtzig Jahren die Situation bei herkömmlichen Computern ähnlich aus. Als Universalrechner wird sich ein Quantencomputer jedoch auch künftig nicht durchsetzen.*
4. Technologie: Wie funktioniert ein Quantencomputer? (Zeit Online 30.1., 160 Kommentare): *Zwanzig Jahre lang waren Quantencomputer eine fixe Idee von Grundlagenforschern. Nun investieren Google, IBM und Microsoft, die EU und China, Geheimdienste und sogar Volkswagen in die mysteriöse Technologie. Warum?*
5. Surren, blinken, leben / Quantencomputer: Null oder eins? Beides! (Zeit Online 2.5.14): *Quantencomputer rechnen anders als nur binär. Mit ihnen wollen Datenkonzerne und Geheimdienste noch mächtiger werden.*
6. Everybody was Quantum fighting, those computers were fast as lightning …. (The Hutch Report 19.3.): *Quantum computing is a critical new arms race and the reasons are quite clear. It will render existing cyber security methods useless.*
7. "Everybody Was Quantum Fighting… Those Computers Were Fast As Lightning…" (Zero Hedge 25.3., 106 Kommentare).
8. The Third Wave of Artificial Intelligence is game changing (AI Summit June 18th, 2018): *This AI Summit will connect you with the present and the future of AI. Get your ticket. ai-summit.de*
9. Quanten machen große Sprünge (Physik-Journal 3/18, mit Zahlsperre): *Im April 2016 gab die Europäische Kommission – versteckt in einer umfangreichen Pressemitteilung – bekannt, im Rahmen einer European Cloud Initiative ein europaweites Flaggschiff zu Quantentechnologien fördern zu wollen. Grundlage der Entscheidung, im Laufe von zehn Jahren etwa 500*

Millionen Euro zu investieren, sofern die Mitgliedsstaaten einen ähnlichen Beitrag durch nationale Fördermittel aufbringen, war das „Quantum Manifesto“.

10. Quantum Manifesto – A New Era of Technology May 2016 (QUROPE 2.2.16): *This manifesto is a call to launch an ambitious European initiative in quantum technologies, needed to ensure Europe’s leading role in a technological revolution now under way.*

Links von wissenbloggt dazu:

- Quanten-Artikel
- Qubits: auf und nieder, immer wieder
- Einsteins Spuk
- Daten besteuern?
- KI mit neuem Optimismus
- Superintelligenz in Arbeit
- Nachdenken über Denkmaschinen
- In der KI-Falle
- Digitale Machtergreifung