Quantencomputing

Sichere Kryptographie auf dem Prüfstand

Kai-Oliver Detken

Seit ein paar Jahrzehnten geistert der Begriff des Quantencomputers durch die Medienlandschaft. Dieser soll um ein Vielfaches leistungsfähiger sein, als unsere heutigen Rechnersysteme. Schließlich basieren deren Architekturen auf den Gesetzen der klassischen Physik und kommen durch fortschreitende Miniaturisierung immer mehr an ihre technischen Grenzen. Spätestens in der Größenordnung weniger Atome treten Effekte wie Tunnelströme auf, die zu Fehlfunktionen führen würden. Zwar setzen neuere Verfahren diese Grenze immer weiter herab, aber irgendwann kommt man bei der Suche nach noch kleineren Strukturen an der Quantenmechanik einfach nicht mehr vorbei. Wie weit diese Technik ist, die von IBM und Google bereits heftig beworben wird, und welche Anwendungen es dafür gibt, soll dieser Artikel aufzeigen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

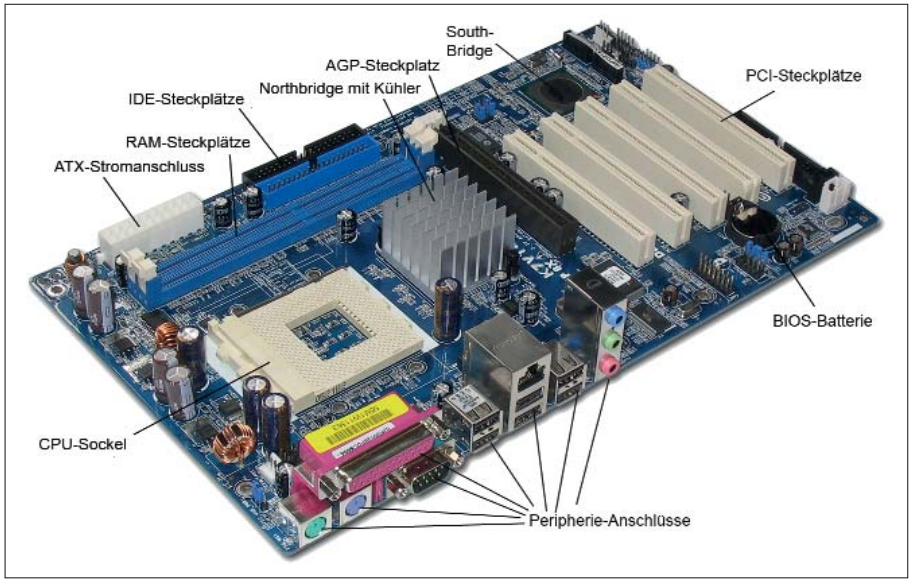


Bild 1: Mainboard eines klassischen Rechnersystems (gemeinfrei) (Quelle: https://commons.wikimedia.org/wiki/File:ASRock_K7VT4A_Pro_Mainboard_Labeled_German.PNG)

Heutige Rechnerarchitekturen basieren in den meisten Fällen letztendlich immer noch auf der Von-Neumann-Architektur (VNA) der 1940-er Jahre. Sie besitzen einen gemeinsamen Speicher, ein Bussystem, eine Kontrolleinheit und einen zentralen Prozessor (*Bild 1*), der Rechenoperationen und logische Verknüpfungen durchführt. Diese Operationen werden sequenziell abgearbeitet (Von-Neumann-Zyklus) und garantieren einen deterministischen Programmablauf. Dateninkohärenzen oder „Race Conditions" sind durch das Bussystem, über den die CPU auf Daten und Programme zugreift, ausgeschlossen. Eine Parallelverarbeitung wird demnach nicht ermöglicht und ist in diesem Konzept auch nicht erwünscht. Eine Leistungssteigerung lässt sich daher nur herbeiführen, indem man den zentralen Prozessor immer schneller werden lässt.

Dies ist aber an technische Grenzen gekoppelt, was man bereits bei heutigen Prozessoren erkennen kann, da dort seit einiger Zeit nicht mehr die Taktfrequenz erhöht wird, sondern ausschließlich die Zahl der Kerne. Dadurch ist die CPU theoretisch in der Lage, Operationen parallel zu berechnen. Allerdings muss auch die genutzte Software den Vorgang unterstützen, da sonst die Anzahl der CPU-Kerne nicht relevant wäre.

Hinzu kommt, dass der Minimierung der Elektronik physikalische Grenzen gesetzt sind, so dass man seit ein paar Jahrzehnten bereits über sogenannte Quantencomputer nachdenkt.

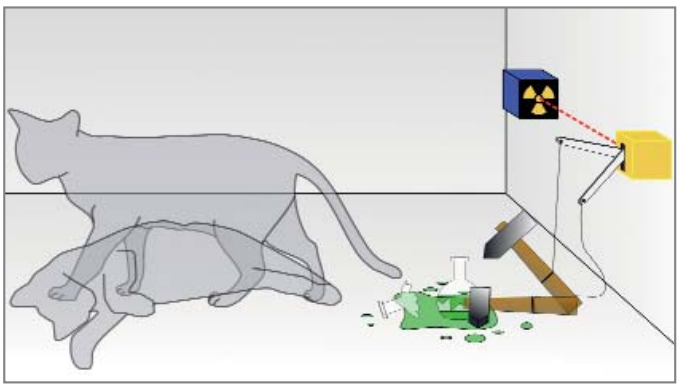
Prinzip der Quantenmechanik

Die sogenannten Quantencomputer sind nicht mehr an die klassische Physik (u.a. Atome, Elektronen) gebunden, sondern ermöglichen durch den Einsatz der Quantenmechanik die Ausnutzung einer Art Parallelexistenz. So muss sich hierbei ein Elektron nicht entscheiden, ob es durch eines von zwei Löchern in einer Wand fliegt, sondern nutzt einfach beide Wege gleichzeitig. In der Physik wird diese Eigenschaft als Superposition bezeichnet. Der klassische Computer müsste beide Möglichkeiten indes nacheinan-

der abarbeiten. So lassen sich heute selbst durch die schnellsten Supercomputer Moleküle mit über 50 Atomen nicht simulieren – zu hoch wäre der Rechenaufwand. Der Quantencomputer hingegen könnte dies, da sich in einem Verbund von mehreren Teilchen die Zahl der Superpositionen nicht nur addiert, sondern multipliziert. Der kleinste Baustein eines solchen Rechners wäre dann nicht mehr das Bit, das einen Wert von 0 oder 1 annehmen kann, sondern das Quantenbit (Qubit), das die Werte 0 und 1 gleichzeitig speichert.

Um die Quantenmechanik zu verstehen, muss man etwas in der Geschichte zurück gehen. Die Grundlagen dieser Theorie wurden bereits zwischen 1925 und 1932 von u.a. Heisenberg, Schrödinger und von Neumann erarbeitet. Nachdem die klassische Physik bei der systematischen Beschreibung der Vorgänge in den Atomen versagt hatte, wurde eine Theorie entwickelt, die sich auf materielle Objekte bezieht und diese als Teilchen oder Systeme

Bild 2: Experiment mit Schrödingers Katze (gemeinfrei)



(Quelle: https://de.wikipedia.org/wiki/Schr%C3%B6dingers_Katze#/media/Datei:Schrodingers_cat.svg)

modelliert, die wiederum aus einer bestimmten Anzahl von einzelnen Teilchen bestehen. Dadurch konnten nun Elementarteilchen, Atome, Moleküle und makroskopische Materie detailliert beschrieben werden. Viele Physiker verstanden damals diese Theorie nicht oder hatten Vorbehalte, u.a. auch Albert Einstein. Dieser äußerte einmal in einem Brief: „Die Theorie liefert viel, aber dem Geheimnis des Alten (A.d.R.: Gott) bringt sie uns kaum näher. Jedenfalls bin ich überzeugt, dass der Alte nicht würfelt."

Erwin Schrödinger versuchte daher 1935 durch ein Gedankenexperiment das Paradoxon in der Quantenmechanik, dass ein Teilchen zwei Zustände gleichzeitig annehmen kann, zu vereinfachen. Er erfand Schrödingers Katze, die sich unsichtbar für den Betrachter in einer Kiste befindet, in der sich auch ein instabiler Atomkern aufhält, der innerhalb einer bestimmten Zeitspanne mit einer gewissen Wahrscheinlichkeit eine Strahlung ausstößt. Diese Strahlung löst mittels eines Geigerzählers die Freisetzung von Giftgas

aus, das das Tier tötet. Die Frage ist nun, welchen Zustand die Katze hat: Ist sie tot oder lebendig? Laut Schrödinger befindet sich nicht nur der instabile Atomkern, sondern auch die Katze in einem Zustand der Überlagerung. Dieser Zustand würde erst dann beendet werden, wenn man die Kiste öffnet und den Zustand der Katze überprüft. Dies stellt damit eine Messung dar, die entweder das Ergebnis „tot" oder „lebendig" ergibt. Bis dahin wäre die Katze also lebendig und gleichzeitig tot (*Bild 2*).

Ähnlich verhält es sich mit einem Qubit: Dieses besitzt so lange den Wert 0 und 1, bis man den Wert ausliest. Durch Quantengatter werden Qubits nun miteinander verknüpft, um die Informationen verarbeiten zu können. Diese Verknüpfung wird in der Quantenmechanik als Verschränkung bezeichnet, was von Albert Einstein einmal passenderweise als „spukhafte Fernwirkung" bezeichnet wurde. Denn zwei Teilchen, die einmal miteinander interagiert haben, sind von diesem Zeitpunkt an miteinander verbunden, auch wenn sie kilometerweit voneinander entfernt sind. Verändert sich das eine Teilchen, wird sich auch das andere verändern. Diese Verschränkung ermöglicht es Quantencomputern, sämtliche Schaltvarianten gleichzeitig auszuführen!

Anwendungsfall Kryptographie

Durch diese Eigenschaft können Quantencomputer mühelos Aufgaben lösen, für die herkömmliche Computer aktuell noch astronomische Zeiträume bräuchten. Einen Anwendungsfall kann man sich bereits sehr gut vorstellen: das Knacken asymmetrischer Verschlüsselungsverfahren. Denn die heute eingesetzten Algorithmen wie z.B. Diffie-Hellmann und RSA setzen darauf, dass das Ausprobieren sämtlicher Varianten für heutige Rechner zu lange dauern würde. Bei Einsatz von Quantencomputern wären diese Verfahren in jedem Fall nicht mehr sicher und müssten ersetzt werden. Aus diesem Grund gibt es derzeit auch ein Wettrennen zwischen den USA, China und Europa, da dadurch auch die nationale Sicherheit auf dem Spiel stehen würde.

Aktuell beschäftigen sich daher Kryptologen mit Verfahren, denen die Quantencomputer nichts anhaben können und auf den Namen Post-Quanten-Kryptographie (PQ-Kryptographie) hören. Der Begriff wurde geprägt, da asymmetrische Verschlüsselungsverfahren auf Primfaktorenzerlegung und der Berechnung diskreter Logarithmen beruhen, die durch den Shor-Algorithmus gelöst werden könnten. Symmetrische Verschlüsselungsverfahren sind hingegen nicht betroffen, da die gestiegene Rechenleistung einfach durch entsprechend längere Schlüssel kompensiert werden kann. Dies wird heute bereits auch so angewendet. Sichere Verschlüsselungsalgorithmen auf PQ-Basis werden derzeit erforscht. Dabei konnten folgende Verfahren bereits als quantensicher ausgemacht werden:

- Einsatz von Gitterverfahren (z.B. NTRUEncrypt-Patent);
- Einsatz multivarianter Polynome (z.B. Unbalanced-Oil-and-Vinegar-Verfahren);
- Einsatz verschlüsselter Hash-Funktionen (z.B. Lamport-Diffie-Einmalsignaturverfahren);
- Einsatz fehlerkorrigierter Codes (z.B. McEliece-Kryptosystem).

Welche Post-Quanten-Verfahren sich letztendlich durchsetzen werden, ist allerdings noch unklar. Code- und Hash-Verfahren sind zwar sicher, beinhalten aber einen langen Schlüssel oder lange Signaturen. Gitterbasierte und multivariante Verschlüsselungen sehen hingegen vielversprechender aus. Die US-Standardisierungsbehörde NIST (**www.nist.gov**) hat daher einen mehrjährigen Wettbewerb ausgerufen, um quantensichere Algorithmen in zukünftigen Standards auszuwählen und die Entwicklung von PQ-Verschlüsselungsalgorithmen zu fördern. Von den ursprünglich 69 Vorschlägen sind Anfang des Jahres inzwischen nur noch 26 übriggeblieben.

Auch in Deutschland wurde ein PQ-Verfahren entwickelt. Die TU Darmstadt hat das hashbasierte Verfahren XMSS (Extended Merkle Signature Scheme) entwickelt und bis zur Praxistauglichkeit gebracht. Vorteilhaft ist dabei, dass XMSS im Vergleich mit anderen PQ-Verfahren mit deutlich kürzeren Schlüsseln und Signaturen auskommt. Hinzu kommt, dass XMSS auch anwendbar bleibt, wenn die eingesetzte Hash-Funktion von Hackern bereits geknackt werden konnte. Denn es gibt nicht nur eine Hash-Funktion, sondern eine Vielzahl. XMSS ist daher eine Art Container, in den eine neue Hash-Funktion eingesetzt werden kann, falls eine alte nicht mehr ausreichend sicher ist. Inzwischen wurde das Verfahren auch in der IETF-Spezifikation RFC-8391 beschrieben, so dass einem Internetstandard quasi nichts mehr im Wege stehen sollte. An Implementierungen wird ebenfalls bereits gearbeitet.

Fazit

Bis reine Quantencomputer verfügbar sind, werden noch mindestens zehn bis 15 Jahre vergehen. Vielleicht werden sie auch nie realisierbar sein, weshalb einige Experten an eine hybride Zukunft aus klassischen Prozessoren und Quantenchips glauben. Während der Quantenchip bei der Berechnung von Big Data (z.B. Klimamodellen) und maschinellem Lernen helfen könnte, würde der klassische Prozessor schneller Lösungen bei Standardberechnungen finden. Beide Techniken könnten sich entsprechend ergänzen.

Inzwischen investieren jedenfalls nicht nur große Konzerne wie Google, Microsoft, IBM und Intel in diese Technik, sondern auch Startups und Regierungen. So hat die US-Regierung zusätzlich 1,2 Mrd. $ zur Verfügung gestellt, um neben Quantencomputern auch die Entwicklung neuartiger Sensoren oder abhörsichere Kommunikationssysteme zu unterstützen. China hat diese Investition mit 10 Mrd. $ sogar weit übertroffen. Dagegen kommen einem die 10 Mio. € der EU zum Bau des Quantenrechners OpenSuperQ (**www.opensuperq.eu**) fast schon wie ein Taschengeld vor. Eines scheint bei diesen Ausgaben aber gewiss: Der Quantencomputer wird kommen und nur beim Zeitpunkt darf noch gerätselt werden. *(bk)*