Lass Quanten fließen

Momentan funktioniert er noch nicht. Oder doch. Aber nicht richtig. Also so ein bisschen. Mit angezogener Hand- und beiden Beinen auf der Fußbremse.

Gemeint ist der Quantencomputer, bei dem man zwei Flavors unterscheidet: Quantum Annealing und Quantum Gates. Beim Quantum Annealing sucht die Maschine das absolute Minimum einer Messgröße einer Konstellation voneinander abhängiger Werte. Ein prominenter Hersteller dieser Gattung von Computern ist D-Wave. Bei gerade mal 2000 Qubits ist die Menge an möglichen Daten aber noch sehr begrenzt.

Die andere Technologie läuft in Schritten ab – einzelnen Zuständen. Das ist einem normalen Computer ähnlich. Die Gatter, die zwischen den Zuständen schalten, sind aber eben Quanten-Gates. IBM ist hier einer der namhaften Hersteller.

Der Aufwand für diese derzeit noch mickrigen Erfolge ist gigantisch. Da die Quantenbausteine extrem empfindlich sind, müssen sie im Tieftemperaturbereich betrieben werden – genauer im Millikelvin-Bereich, also Milligrad über dem absoluten Nullpunkt. Das bedarf eines erheblichen Aufwands an Isolierung und Kühlung, weshalb der walnussgroße Quantenbaustein in einer zimmergroßen Apparatur steckt.

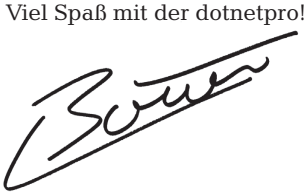
Nicht nur von der Größe her legt der Stand der aktuellen Entwicklungen den Vergleich mit den 40er Jahren des vergangenen Jahrhunderts nahe. Stichwort Konrad Zuse und seine Z3:

Ein fast drei Meter hoher und breiter Raum für einen einzigen Computer – vor 75 Jahren und heute.

Trotzdem gehen alle davon aus, dass der Quantencomputer kommt. Wer dann dabei sein will, wenn er vielleicht erst in zehn Jahren nennenswerte Berechnungen ausführt, muss heute schon einsteigen in die Fortbildung und das Sammeln von Erfahrungen. Google, IBM, D-Wave: Alle sind dabei. Sogar Microsoft mischt mit der eigenen Quanten-Programmiersprache Q mit.

Eines ist auf jeden Fall klar: Wenn der Quantencomputer verfügbar ist, sind alle bislang verwendeten Verschlüsselungsalgorithmen obsolet. Angesichts dessen erscheint die Jahr-2000-Problematik (Y2K) wie Kindergarten, meinte Matthias Ziegler von Accenture auf der OpenMunich in seinem Vortrag zum aktuellen Stand des Quantencomputing. Deshalb wird auch schon kräftig an neuen, quantensicheren Verschlüsselungen gearbeitet.

Viel Spaß mit der dotnetpro!



Tilman Börner
Chefredakteur dotnetpro

Hendrik Lösch

gibt im Schwerpunkt einen tiefen Einblick in das Refaktorisieren von Anwendungen (S. 8)

Christian Wißmann

führt Sie Schritt für Schritt zum API-Management in der Cloud (S. 50)

Nico Franze

ist einem Speicherleck der UWP auf den Grund gegangen (S. 56)