Bricht die Quanten Überlegenheit bald alle Passwörter?

Student Group

First Name	Surname	Matrikel Nr.

Table of Contents

Bricht die Quanten Überlegenheit bald alle Passwörter? 2

Bricht die Quanten Überlegenheit bald alle Passwörter?

Beim Rennen um den größten Quantecomputer überbieten sich in letzter Zeit IBM, Intel und Google. Letzteres Unternehmen hat gerade einen Computer basierend auf 72 Qubits vorgestellt, nachdem die Messlatte zum Jahreswechsel bei etwa 50 Qubits lag. Auch im Bereich der Quantencomputer scheint es eine Art Moores Law zu geben, mit einer Verdopplung der Qubits etwa alle 3-5Jahre. Nur, dass sich mit einem einzigen Qubit mehr die Anzahl der durchrechenbaren Zustände verdoppelt - im klassischen Rechner müsste dazu auch die Anzahl der Transistoren verdoppelt werden. Mit Googles 72 Qubits lassen sich so 4'722'366'482'869'645'213'696 Zustände gleichzeitig abbilden.

Interessant hierbei: Systeme über 50.. 100 Qubits können aktuell nicht mehr mit Supercomputern nachgebildet werden. Es scheint also, als ob in diesem Jahr die Quantum Supremacy erreicht wird. Einerseits bedeutet das, dass die Quantenrechner sich schnell einer Leistung zum Brechen immer längerer Schlüssel nähern. Asymmetrische Verschlüsselung scheint dabei anfälliger zu sein - es werden etwa doppelt so viele Qubits, wie Anzahl der Bits im Schlüssel benötigt.

Andererseits bedeutet es auch, dass die größeren Quantencomputer nicht mehr klassisch überprüft werden können. Ein großes Problem der Quantenrechner ist die Qualität des Qubits zu gewährleisten, bzw. eine ausreichende Qualität durch Korrekturalgorithmen (und weiteren Qubits) herzustellen.

Es wird erwartet, dass RSA2048 in 10..20 Jahren nicht mehr sicher ist.

From:
https://wiki.mexle.org/ - **MEXLE Wiki**

Permanent link:
https://wiki.mexle.org/blog/bricht_die_quanten_ueberlegenheit_bald_alle_passwoerter

Last update: **2021/05/09 11:14**