SUCCESS STORY

Know-Center | Know-Center GmbH – Research Center for Data-Driven Business & Big Data Analytics

Programm: COMET – Competence Centers for Excellent Technologies

Förderlinie: COMET-Zentrum (K1)

Projekttyp: DDAI COMET Modul

©Adobe Stock

SICHERHEITSLÜCKE BEI IBM QUANTENCOMPUTERN

AUSWERTUNGEN AUF QUANTEN-HARDWARE SOLLTEN SICHER SEIN. AM KNOW CENTER WURDE AUF EINE SCHWACHSTELLE DURCH BESTEHENDES „RAUSCHEN“ GEPRÜFT UND GEFUNDEN.

Quantencomputer werden zurzeit weltweit intensiv beforscht und einige Firmen stellen bereits „Quantencomputer in der Cloud“ zur Verfügung. Das heißt, man kann bereits heute die Vorteile von Quantencomputern nutzen, indem man seine Daten und Auswertungen auf entsprechend online verfügbarer Quanten-Hardware laufen lässt.

Sicheres Quantencomputing

Am Know Center wird intensiv daran geforscht, solche Auswertungen auf Quantencomputern sicher zu machen und auch hier Daten und Algorithmen zu schützen. In einer ersten Arbeit haben Forscher am Know Center das „Rauschen“ der Qubits, der Grundbausteine eines Quantencomputers, ausgenützt, um zu bestimmen, was vorher am Quantencomputer gerechnet wurde.

Störfaktoren wie kosmische Strahlung, die physikalische Umgebung des Quantencomputers und sogar andere Qubits, können innerhalb der Quantenschaltkreise ein „Rauschen“ erzeugen. Dieses kann Ergebnisse einer Berechnung beeinflussen und somit zu Fehlern führen. Die

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

Version 01/2020

derzeitige Forschung fokussiert daher stark auf die Minimierung dieses Rauschens.

Seitenkanalangriff
Inspiriert durch die klassische Hacking-Methode der Seitenkanalangriffe - dabei wird auf indirekte Informationen im Computersystem zugegriffen, anstatt das System direkt anzugreifen, entstand die Idee einen "Prime-and-Probe"-Angriff durchzuführen. Bei dieser Art von Angriff wird versucht, das System in einen bestimmten Zustand zu versetzen, der dann eine indirekte Analyse ermöglicht. Alle Rechnungen auf der öffentlichen Cloud-Quantencomputing-Plattform von IBM landen in einer Warteliste und werden der Reihe nach am jeweiligen Quantencomputer abgearbeitet.

Rauschen hat Aussage
Die Forscher am Know Center haben ausgenutzt, dass sich das Rauschen der Qubits nicht zufällig verändert und konnten durch geschickte Bestimmung und Beeinflussung des Zustandes des Quantencomputers unmittelbar vor und nach einer fremden Rechnung rekonstruieren, welche Berechnung ausgeführt wurde.

Die Ergebnisse deuten auf eine potenzielle Sicherheitslücke im Cloud-basierten Quantencomputing hin, die dementsprechend weiter erkundet werden sollte.

Das Experiment der Wissenschaftler hat inzwischen auch die Aufmerksamkeit von Forschungsgruppen in Europa und den USA auf sich gezogen, die Rauschminderung zur Sicherung von Cloud-basierten Quantencomputersystemen und die Optimierung von Quantenalgorithmen erforschen. Auch eine lose Zusammenarbeit mit Forschern der Universität Yale soll verwandte Themen gemeinsam weiter erkunden.

Projektkoordination
Dr. Andreas Trügler, Know-Center
T +43 (0) 316 – 87330895
atruegler@know-center.at

Know-Center GmbH
Sandgasse 36
8010 Graz
T +43 (0) 316 87330801
office@know-center.at
www.know-center.at

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

Österreichische
Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at