SUCCESS STORY

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

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Center (K1)

Type of project: DDAI COMET Module

IBM QUANTUM COMPUTERS SECURITY BREACH

EVALUATIONS ON EXISTING QUANTUM HARDWARE SHOULD BE SECURE. KNOW CENTER RESEARCHERS CHECKED FOR VULNERABILITIES BY ANALYZING EXISTING "NOISE" – FINDING A POTENTIAL WEAKNESS.

Quantum computers are currently being researched intensively worldwide, and some companies are already providing “quantum computers in the cloud”. This means that quantum computers can already be taken advantage of, by running data and analysis on appropriate online quantum hardware.

Secure quantum computing

Intensive research is underway at the Know Center, to make such evaluations on quantum computers secure and to protect data and algorithms. In initial work, researchers at the Know Center exploited the “noise” of qubits, the basic building blocks of a quantum computer, to determine what was previously calculated on the quantum computer. Interfering factors such as cosmic rays, the physical environment of the quantum computer, and even other qubits, can create “noise” within the quantum circuits. This can affect the results of a calculation and thus lead to errors. Current research, therefore, focuses heavily on minimizing this noise.

Side-channel attack

Inspired by the classic hacking method of side-channel attacks – accessing indirect information in the computer system instead of attacking the system directly – the idea of performing a “prime-and-probe” attack emerged. This type of attack attempts to put

the system in a certain state, which then allows indirect analysis. All computations on IBM's public cloud quantum computing platform end up on a waiting list and are processed in order on the respective quantum computer.

Noise with meaning

The researchers at the Know Center exploited the fact that the noise of the qubits does not change randomly. They were able to reconstruct which computation was performed, by cleverly determining and manipulating the state of the quantum computer immediately before and after an extraneous computation. The results point to a potential security vulnerability in cloud-based quantum computing that should accordingly be explored further.

The scientists' experiment has since attracted the attention of research groups in Europe and the U.S. that are exploring noise mitigation to secure cloud-based quantum computing systems and the optimization of quantum algorithms. A loose collaboration with researchers at Yale University is also expected to further explore related topics together.

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

Know-Center GmbH
Sandgasse 26
8010 Graz
T +43 (0) 316 – 87330895
office@know-center.at
www.know-center.at