Research Institute
Cyber Defence
Bundeswehr University Munich

Annual Conference CODE 2020 - Summary of Workshop 3

Quantum Technologies

This year the focus was on advances in Quantum Computing and Post Quantum Cryptography. On the one hand quantum computing and the related hardware are a direct result of applying quantum mechanical effects. On the other hand PQC is an improvement of classical cryptographic methods which has to resist possible aGacks with the help of a quantum device.

Understanding the theory of quantum circuits provides an insight into currently available hardware. While transmon qubits make use of controlled-X or controlled-Z 2-qubit gates currently connecting at most to the four neighbors in 2 dimensions, ion-trap qubits employ the Ising-XX 2-qubit gate and are all-to-all connected. We are still in the NISQ era working with non-error-corrected qubits and in search for suitable problems which can be tackled by those devices.

The Grover and Shor algorithms from the 90s of the last century are still the best examples for the usefulness of a quantum approach. These methods endanger symmetric and asymmetric cryptography where the laGer in form of ECC and RSA is more effected. Therefore, a NIST process is underway for standardizing new methods to improve current digital signatures, key exchange protocols and public key cryptography.

IBM recently announced an ambitious roadmap towards more than 1000 Qubits for the year 2023. This might finally open the door for better treatment of errors and their correction. Consequently PQC will be required rather sooner than later.