# Quantentechnologie – Quantencomputer

## Worum geht es?

Bei einem Quanten-Computer werden die Prinzipien Überlagerung und Verschränkung [1] verwendet, um eine sehr große Anzahl an Rechnungen parallel durchführen zu können.

Allerdings muss hierbei beachtet werden, dass damit nur ganz bestimmte mathematische Berechnungen durchgeführt werden können wie z.B. eine Primfaktorenzerlegung einer großen Zahl. Dadurch kann ein Quantencomputer einen privaten Schlüssel aus einem bekannten öffentlichen Schlüssel eines asymmetrischen Verschlüsselungssystems sehr viel schneller berechnen als klassische Computer. Bei der Verwendung von herkömmlichen Computern geht man davon aus, dass solche Berechnungen viele Jahre dauern. Dadurch wird angenommen, dass die verwendeten Verschlüsselungsmethoden sicher genug sind. Wenn allerdings solche Berechnungen in wenigen Stunden anstatt in Jahren erfolgen können, wird ein Quanten-Computer zu einer Bedrohung unserer heutigen asymmetrischen Verschlüsselungssysteme. Weiters können bestimmte mathematischen Optimierungsprobleme von Quanten-Computern viel rascher gelöst werden als dies klassische Computer können.
Die besondere technologische Herausforderung bei einem Quanten-Computer besteht darin, die verschiedenen Umwelteinflüsse auf die empfindlichen Quantenzustände der Teilchen zu beherrschen. Verschiedenste Einflüsse aus der Umwelt wie Temperaturschwankungen, elektromagnetische Strahlung etc. verändern Quantenzustände und müssen somit bei Messvorgängen berücksichtigt werden oder mit sehr viel Aufwand abgeschirmt werden.
IBM, Google, Microsoft, Intel, etc. als auch ganze Nationalstaaten wie China, USA und Israel forschen derzeit sehr aktiv an dieser Technologie [2, 3, 4, 5, 6]. Es gibt verschiedene technische Ansätze um Quanten-Computer zu realisieren; ein aktuell weit entwickelter Ansatz arbeitet mit Teilchen beim absoluten Nullpunkt; d.h. -237 C. Weitere Ansätze bei Zimmertemperatur sind in der Forschung ebenfalls in der Entwicklung wie z.B. an der Uni Innsbruck in Österreich [7]. Aber es gilt noch einige technische Hürden zu überwinden und es ist somit nicht ganz klar abzuschätzen, bis wann ein erster Quanten-Computer wirklich funktioniert, aber die Experten gehen davon aus, dass in den nächsten 5-15 Jahren wesentlich Fortschritte gemacht werden. Weitere Informationen: [1] [8].

## Warum ist dieser Trend wichtig?

- Der Quantencomputer stellt aktuell eine potentielle Bedrohung unserer asymmetrischen Verschlüsselungssysteme dar.
- Neue mathematische Berechnungen und Simulationen können erst mit einem Q-Computer effektiv berechnet werden

## Das österreichische Ökosystem zu diesem Trend

- Quanten-Computer Aktivitäten erfolgen an Universitäten wie Innsbruck, Wien und ISTA
- Derzeit keine Produkt- und Industrie-Aktivitäten in Österreich. Österreich hat eine international führende Rolle im Bereich der QKD Quantenverschlüsselung eingenommen um der Bedrohung durch den Quantencomputer entgegenwirken zu können (siehe [1, 3]).

## Wo finde ich weiterführende Information?

- Leopold H., Hübel H., Pacher Ch., Stierle M., Monyk Ch., Quantentechnologien – eine Einführung, AIT Austrian Institute of Technology Report, 3.8.2019.
- AIT/BMVIT Studie, Mai 2018: Quantentechnologie – Möglichkeiten zur stärkeren Industrialisierung

## Weiterführende Informationen

Siehe dazu auch die Zusammenfassungen der I4.0 Technologietrends *„Quantentechnologien“, und „Quantenkommunikation - Quantum Key Distribution QKD“*

## Videos

- Wie funktionieren Quantencomputer?

- Quantencomputer – Einfach erklärt.

**Referenzen:**


[1] Leopold H., Hübel H., Pacher Ch., Stierle M., Monyk Ch., *Quantentechnologien – eine Einführung*, AIT Austrian Institute of Technology Report, 29.7.2019

[2] Google stellt neuen Quantencomputer namens Bristlecone vor, FAZ Frankfurter Allgemeine, 6. März 2018, https://www.faz.net/aktuell/wirtschaft/diginomics/google-stellt-neuen-quantencomputer-namens-bristlecone-vor-15480332.html

[3] China leads in Publications on Quantum Computing, but US is more integrated internationally, Web of Science, BCG Center for Innovation Analytics,

[4] Tom Simonite, NSA Says It “Must Act Now” Against the Quantum Computing Threat, MIT Technology Review, February 3rd, 2016, https://www.technologyreview.com/s/600715/nsa-says-it-must-act-now-against-the-quantum-computing-threat/

[5] IBM-Quantencomputer kann nicht mehr als normale Computer, future zone, 11.1.2019, https://futurezone.at/science/ibm-quantencomputer-kann-nicht-mehr-als-normale-computer/400374263

[6] Israel will Quantencomputer entwickeln, 23.8.2018, https://www.gtai.de/GTAI/Navigation/DE/Trade/Maerkte/suche,t=israel-will-quantencomputer-entwickeln,did=1970208.html

[7] Quantencomputer „Made in Austria“ kommt, 12.2.2018, https://www.uibk.ac.at/newsroom/quantencomputer-made-in-austria-kommt.html.de

[8] Strategische Analyse der Möglichkeiten zur stärkeren Industrialisierung der Ergebnisse der österreichischen Quantenforschung, Studie vom AIT Austrian Institute of Technology im Auftrag vom Bundesministerium für Verkehr, Innovation und Technologie (bmvit), Mai 2018, Quantentechnologie – Möglichkeiten zur stärkeren Industrialisierung