



Verbundprojekt HSM-QCC

Ausführungsmodul für sicheres Cloud-Quantencomputing

Motivation

Zahlreiche Unternehmen, darunter Google, IBM, Honeywell, Amazon und Xanadu, bauen derzeit kleinformige Quantencomputer. In der fernen Zukunft werden diese über Quantennetzwerke gesichert und Kunden remote zur Verfügung gestellt. Auf Grund vielfältiger technischer Herausforderungen wird, um geschützten Zugang zu Quanten-Cloud-Diensten zu ermöglichen, für lange Zeit eine Übergangslösung auf Basis kurzzeitig verfügbarer Technologien benötigt, die die Sicherheit und den Schutz der Privatsphäre gewährleistet, das Potenzial der Quantentechnologie erschließt, und einen strategischen Vorteil für Unternehmen und Forschung in der EU schafft. Dies ist das Kernziel dieses Projekts.

Ziele und Vorgehen

Ziel dieses Projekts ist die Entwicklung eines eigenständigen vertrauenswürdigen Ausführungsmoduls, das sicheres Cloud-Quantencomputing ermöglicht. Dieses Modul wird im Rahmen des Projekts validiert, indem eine vollständige Software-Hardware-Integration des weltweit ersten sicheren optischen Zugangs zu einer photonischen Quantencomputer-Implementierung für Multi-User-Quantencloud-Anwendungen demonstriert wird.

Innovation und Perspektiven

Unsere Arbeit konzentriert sich auf die Entwicklung von Protokollen für Quanten-Cloud-Plattformen, die die Korrektheit, Resilienz und Vertrauenswürdigkeit von Quantencomputern gewährleisten. Konkret zielen wir darauf ab:

- Gewährleistung der Korrektheit durch den Entwurf und die Implementierung von Datenverarbeitungsprotokollen, die wie von ihren Entwicklern vorgesehen funktionieren.
- Verbesserung der Resilienz durch die Entwicklung von Protokollen, die Fehler und Störungen (Rauschen) in der Hardware tolerieren können.
- Gewährleistung der Vertrauenswürdigkeit, indem den Nutzern eine sichere und private Umgebung für den Umgang mit ihren Daten geboten wird.



Quantenklave und Hardware-Sicherheitsmodul

Projekttitlel:

Hardware-Sicherheitsmodul für sicheres delegiertes Quantum-Cloud-Computing (HSM-QCC)

Programm:

Forschungsprogramm Quantensysteme

Fördermaßnahme:

Quantera Call 2023

Projektvolumen:

168.000 Euro (zu 70 % durch das BMBF gefördert)

Projektlaufzeit:

01.08.2024 – 31.07.2027

Projektpartner:

- QuiX Quantum GmbH, Stuttgart
- University of Twente, Twente, Niederlande
- University of Edinburgh, Edinburgh, Vereinigtes Königreich
- VeriQloud, Montrouge, Frankreich
- Thales-Gruppe, Paris La Defense, Frankreich
- Sorbonne Université, Paris, Frankreich
- Eötvös Loránd University, Budapest, Ungarn

Projektkoordination:

University of Twente
Prof. Dr. P.W.H. Pinkse
E-Mail: p.w.h.pinkse@utwente.nl