QUICHE

Quantum Side Channel Analysis

Programm / Ausschreibung	Quantum Austria 3. Ausschreibung (2023/2024)	**Status**	laufend
Projektstart	31.03.2024	**Projektende**	30.01.2026
Zeitraum	2024 - 2026	**Projektlaufzeit**	23 Monate
Keywords	Quantum side-channel attacks, high-dimensional quantum systems, qudits, quantum securtiy, dynamic quantum circuits		

Projektbeschreibung

Dieser Forschungsantrag befasst sich mit den aufkommenden Sicherheits- und Datenschutzherausforderungen, die mit der rasanten Entwicklung von Quantencomputern, Fortschritten bei der Entwicklung von Qubit-Systemen und der Verbreitung benutzerfreundlicher Quanten-Cloud-Anwendungen verbunden sind. Da der Zugang zu Quantencomputing-Infrastruktur zunehmend einfacher wird, rücken Bedenken hinsichtlich des Datenschutzes, der Sicherheit von proprietären Quanten-Algorithmen und der generellen Möglichkeit von Informationslecks von Quantenhardware in den Vordergrund. Dieses Projekt widmet sich einer umfassenden Erforschung dieser Themen, mit besonderem Fokus auf Quanten-Seitenkanalangriffen. Spezielles Augenmerk wird auch auf die Datenschutzimplikationen dynamischer Quanten-Circuits gelegt, sowie auf den Übergang von Qubits zu Qudits, der eine verbesserte Rechenleistung verspricht, aber auch neue Sicherheit-Schwachstellen einführen könnte. Dieser Projektantrag zielt darauf ab, Quantencomputing-Anwendungen zugänglicher zu machen, indem unser Verständnis für potenzielle Sicherheitsrisiken vertieft wird, einschließlich einer entsprechenden theoretischen Beschreibung möglicher Informationslecks, basierend auf Verschränkungs- und Nicht-Verschränkungsansätzen sowie hochdimensionalen Quantensystemen. Aufbauend auf ersten Sicherheitsanalysen unterschiedlicher Quanten-Hardware, umfasst das Projekt eine breitere Analyse von Seitenkanalangriffen, unterstützt durch eingehende mathematische Modellierung, um mögliche Informationslecks zu bewerten und im nächsten Schritt auch sichere Qudit-Implementierungen zu entwickeln. Der Forschungsantrag umfasst auch die Entwicklung robuster Gegenmaßnahmen zum Schutz der Privatsphäre und Integrität von Quantencomputing-Architekturen und trägt damit zur Verbesserung der Sicherheit zukünftiger Quantentechnologien bei. Durchgeführt von einem interdisziplinären Konsortium von Experten aus der Quantenphysik, Informatik, Kryptographie und Mathematik und unterstützt durch ein internationales Netzwerk von Forschungspartnern, zielt dieses Projekt darauf ab, bedeutende Beiträge zum Design sicherer Quantenhardware und zur Sicherheit von Quanten-Cloud-Anwendungen für Endbenutzer zu leisten.

Abstract

This research proposal addresses the emerging security and privacy challenges associated with the rapid development of quantum computers, advancements in qubit systems, and the proliferation of user-friendly quantum cloud applications. As access to quantum computing infrastructure becomes increasingly seamless, concerns regarding data protection, algorithm

security, and the potential for information leakage through quantum hardware have become paramount. This project emphasizes the need for a comprehensive exploration of these issues, focusing particularly on quantum side-channel attacks. Special emphasis is paid on privacy implications of dynamic quantum circuits, and the transition from qubits to qudits, which promises enhanced computational performance but may also introduce new vulnerabilities.
In general, our research aims to popularize applications for quantum computation by deepening our understanding of potential security risks, including a corresponding theoretical framework of information leakage based on entanglement and non-entanglement approaches as well as high-dimensional quantum systems. Building on preliminary cross-hardware security analyses, the project will expand the scope of investigation to include a wider array of side-channel attacks, supported by in-depth mathematical modeling to assess possible information leakage and develop secure qudit implementations. The proposal outlines plans to develop robust countermeasures to protect the privacy and integrity of quantum computing architectures, thereby enhancing the security of emerging quantum technologies.
Conducted by an interdisciplinary consortium of experts in quantum physics, computer science, cryptography, and mathematics, and supported by an international network of research partners, this project aims to make significant contributions to the design of secure quantum hardware and the safety of quantum cloud applications for end users.

Endberichtkurzfassung

The QUICHE project establishes a theoretical foundation together with software-based simulation, data analysis, and machine-learning-assisted inference methods for studying side-channel leakage in quantum computing. A central outcome was a hardware-agnostic framework for modelling how information can leak through auxiliary physical channels during quantum computations and for quantitatively evaluating the resulting leakage risk. In addition, a physical probing method and experimental demonstration, carried out in collaboration with laboratories at the University of Innsbruck, exposed side-channel leakage in a higher-dimensional quantum system. These results were consolidated between two main scientific manuscripts, one focused on hardware-agnostic simulation and one on the experimental demonstration of side-channel leakage. Further dissemination included the organization of the Machine Learning & Quantum Physics workshop in Obergurgl, invited talks, workshop participation, and outreach activities, including invited talks at the Quantum Computing Cybersecurity Symposium in 2024 and 2025, and at the American Physical Society global summit 2025. Overall, the project established key methods for the systematic study of side-channel risks in quantum computing.

Projektkoordinator

- Know Center Research GmbH

Projektpartner

- Technische Universität Wien