Bundesministerium
für Bildung
und Forschung

quanten
technologien

Verbundprojekt QuantumQAP

Algorithmus für Quadratische Zuordnungsprobleme und die Post-Quanten-Kryptographie

Motivation

Es gibt mathematische Probleme, die mit den heutigen, auf dem Prinzip der Turing-Maschine basierenden Rechnern nicht in angemessener Zeit gelöst werden können. Das sind z. B. diskrete Probleme, wie das Quadratische Zuordnungsproblem (QAP – Quadratic Assignment Procedure), das u. a. für das Design von Mikroprozessoren relevant ist und dessen Lösung zu effizienteren und schnelleren Prozessoren führen würde. Schwer lösbare Probleme sorgen andererseits auch für Datensicherheit, da Sicherheitsprotokolle so nicht ohne weiteres umgangen werden können. Ziel dieses Projekts ist es daher, die beiden oben genannten Aspekte zu verbinden, um zum einen mathematische Probleme schneller lösen und zum anderen die Sicherheit von Daten weiterhin gewährleisten zu können.

Ziele und Vorgehen

Um Hardware wie Mikroprozessoren zu entwickeln, werden typischerweise feldprogrammierbare Gate-Arrays (Logik-Gatterfelder, sog. FPGAs – Field Programmable Gate Arrays) verwendet. Allerdings stellt die Optimierung der Verschaltung dieser Logikbausteine selbst schon ein für Turing-Maschinen schwieriges Problem dar (das oben erwähnte QAP). Durch Quanten- oder quanteninspirierte Hardware ließe sich dieses Problem besser lösen. Der Ansatz des Projekts QuantumQAP besteht darin, Quantenhardware und theoretische Lösungsansätze zu kombinieren, die in den beiden Anwendungsfeldern FPGA-Verschaltung und Post-Quanten-Kryptographie zur Anwendung kommen.

Innovation und Perspektiven

Die Neuheit des Ansatzes ist die parallele Ausführung des QAP-Solver-Algorithmus, also die Fähigkeit, passende Vorgänge auf einen Quantencomputer auszulagern. Dabei kann der Algorithmus für Quadratische Zuordnungsprobleme angewendet werden und auch bei der Implementierung von Algorithmen für die Post-Quanten-Kryptographie zum Schutz von Informationen beitragen.

Projekttitel:
Hybrides Quanten Place&Route zur Synthese von Postquantum-Kryptographie-Code auf FPGAs (QuantumQAP)

Programm:
Quantentechnologien – von den Grundlagen zum Markt

Fördermaßnahme:
Anwendungsnetzwerk für das Quantencomputing

Projektvolumen:
2,7 Mio. Euro (zu 76,2 % durch das BMBF gefördert)

Projektlaufzeit:
01.01.2022 – 31.12.2024

Projektpartner:
- Fraunhofer-Institut für Algorithmen und Wissenschaftliches Rechnen (SCAI), Sankt Augustin
- Quantum Brilliance GmbH, Stuttgart
- Thales Deutschland GmbH, Ditzingen

Assoziierter Partner:
adiutaByte GmbH, Sankt Augustin

Projektkoordination:
Fraunhofer-Institut für Algorithmen und Wissenschaftliches Rechnen (SCAI)
Dr. Thomas Soddemann
E-Mail: thomas.soddemann@scai.fraunhofer.de

Impressum
Herausgeber Bundesministerium für Bildung und Forschung (BMBF), Referat Quantentechnologien; Quantum Computing, 53170 Bonn;
Stand Februar 2022; **Text** VDI Technologiezentrum GmbH; **Gestaltung** KOMPAKTMEDIEN Agentur für Kommunikation GmbH,
familie redlich AG Agentur für Marken und Kommunikation