SIZ

Finanzgruppe

SIZ-Seminar:

Quantencomputer verstehen

Als Webinar ca. 3 Stunden; Termin nach Absprache

Inhalte

Die Möglichkeiten und Gefahren von Quantencomputern rücken zunehmend in das Blickfeld von Forschungsorganisationen und Technologiefirmen. Mit dieser Schlüsseltechnologie sollten sich aber auch Branchen wie die Finanzdienstleistung befassen, um die Bedeutung der Entwicklungen für den eigenen Verantwortungsbereich kompetent bewerten zu können.

In der klassischen Welt schreitet die Leistungssteigerung seit den 1960er Jahren mit der Minimalisierung integrierter Schaltkreise unaufhaltsam voran („Mooresches Gesetz“). Mittlerweile stößt diese Verkleinerung der Bauteile jedoch an ihre Grenzen. Jenseits dieser Grenze gelten nicht mehr die uns vertrauten Gesetze der klassischen Physik, sondern jene der Quantenphysik. Dies erfordert – insbesondere zum Schutz gegen das ungewollte Entschlüsseln geheimer Nachrichten – eine grundsätzlich neue Herangehensweise statt eines „Weiter so wie bisher“.

Bei klassischen Computern (KC) basiert die Informationsverarbeitung auf dem Bit, welches einen von zwei Zuständen (0 oder 1) annehmen kann. Quantencomputer können diese Grenze mit dem sogenannten QuBit überwinden und bergen damit das Potential zur Lösung von Problemen, die für heutige Superrechner unlösbar sind.

Quantencomputer können prinzipiell zwar nichts berechnen, was nicht auch klassische Computer berechnen können, jedoch sollten sie bestimmte Problemstellungen im Gegensatz zu ihnen effizienter lösen können. Das bringt auch neue Gefahren mit sich, insbesondere zur Sicherheit von heute üblichen und als sicher geltenden kryptographischen Verschlüsselungsverfahren. Jedoch können Quantencomputer ihrerseits die Basis für neue, dann auch von anderen Quantencomputern nicht brechbaren Verschlüsselungsverfahren werden.

Die Verfügbarkeit von Quantencomputern ist stark durch den extrem hohen technischen Aufwand begrenzt, der für ihren Betrieb erforderlich ist. Auch sind alle heutigen Quantencomputer-Programmiersprachen maschinennah. Compiler für höhere Abstraktionslevels sind in der Entwicklung. Deshalb benötigt man zur Zeit für die Programmierung eines solchen Computers das mathematische Hintergrundwissen der Quantenmechanik.

In den nächsten Jahren sollten Quantencomputer mit einer ausreichenden Anzahl von QuBits realisiert werden können. Dann deutet sich in einigen Bereichen eine „Revolution“ an, die bisherige Gewissheiten in Frage stellen wird. Die moderne Informationsgesellschaft wird, wenn sie weiterhin sichere Kommunikationswege zur Verfügung haben möchte, gezwungen sein, neue Wege zu gehen. Finanzdienstleister dürften mit zu den ersten Betroffenen gehören.

Zielgruppe

Zielgruppe sind sowohl Sicherheitsverantwortliche als auch Anwendungsentwickler im Finanzbereich. Denn um den Gefahren, die von Quantencomputern ausgehen angemessen entgegentreten zu können, sind tiefe Eingriffe in die IT-Infrastruktur zu erwarten. Diese sogenannten „Post-Quanten-Algorithmen“ müssen gegebenenfalls hardwarenah ausgeführt werden, um eine akzeptable Performance zu erreichen.

Ziele

- Kurze Einführung in die theoretisch-mathematischen Grundlagen, die für das Verständnis von Quantencomputern unabdingbar sind
- Unterschiede zum klassischen Computer verstehen
- Für welche Problemstellungen ist der Quantencomputer geeignet?
- Welche (Verschlüsselungs-) Verfahren sind durch den Quantencomputer in Gefahr?
- Technische Voraussetzungen des Quantencomputers
- Prinzipien der Programmierung von Quantencomputern

Dozent / Trainer

Dr. Ralf Zitzelsberger, SIZ GmbH

Die SIZ GmbH
Wir setzen Maßstäbe für zukunftsfähige IT- und Sicherheitsstandards sowie für das Beauftragtenwesen in der Finanzwirtschaft und darüber hinaus.

Unsere Schwerpunkte

- Informationssicherheit
- S-CERT
- IT-Steuerung
- Revision
- Payments
- Beauftragtenwesen
  - Datenschutz
  - Informationssicherheitsbeauftragter
  - Geldwäsche- und Betrugsprävention
  - Wp- und MaRisk-Compliance

Unser Angebot

- Individuelle Beratung und Unterstützung
- Übernahme von Beauftragtenfunktionen
- Softwareprodukte
- Standards im Zahlungsverkehr

Unsere Kunden

- Privat- und Geschäftsbanken, genossenschaftliche Banken, Sparkassen, Landesbanken sowie deren Verbände und Verbundpartner
- Kartengesellschaften, Zahlungsverkehrs-Dienstleister
- Versicherungsunternehmen
- Unternehmen aus Industrie und Handel
- IT-Dienstleister und IT-Anbieter

Sie können sich darauf verlassen!

Die SIZ GmbH findet die optimale Lösung für Ihre individuellen Anforderungen.

Fragen, Wünsche oder ein konkreter Gesprächstermin?

Ihr Ansprechpartner

Dr. Ralf Zitzelsberger
Fachgruppe Payments – Standards und Services

Tel.: 0228 4495-7645
E-Mail: ralf.zitzelsberger@siz.de

SIZ GmbH
Simrockstraße 4
53113 Bonn
www.siz.de

© 04/2021 SIZ GmbH