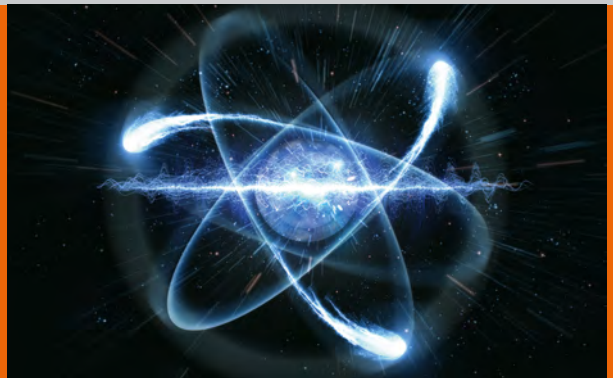
Fraunhofer
ACADEMY

SEMINAR



POST-QUANTEN SICHERHEIT

Trends und Entwicklungen der modernen Kryptographie

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …

…die Funktionsweise eines Quantencomputers nachvollziehen
…Quantengatter und einfache Quanten-Algorithmen programmieren
…die Auswirkungen der Algorithmen von Shor und Grover auf die moderne Kryptographie abschätzen
…Post-Quantum Kryptographie anwenden

Dieses Seminar bietet Ihnen …

…Wissen, das heute nur wenigen vorbehalten ist
…aktuellen Einblick in zukunftsträchtige Themen
…Austausch mit Fachexperten zu aktuellen Forschungsthemen
…praxisnahe Übungen

Melden Sie sich gleich an!
www.cybersicherheit.fraunhofer.de/post-quanten-sicherheit

Die Herausforderung: Quantencomputer brechen viele der heute gängigen Verfahren der IT-Sicherheit

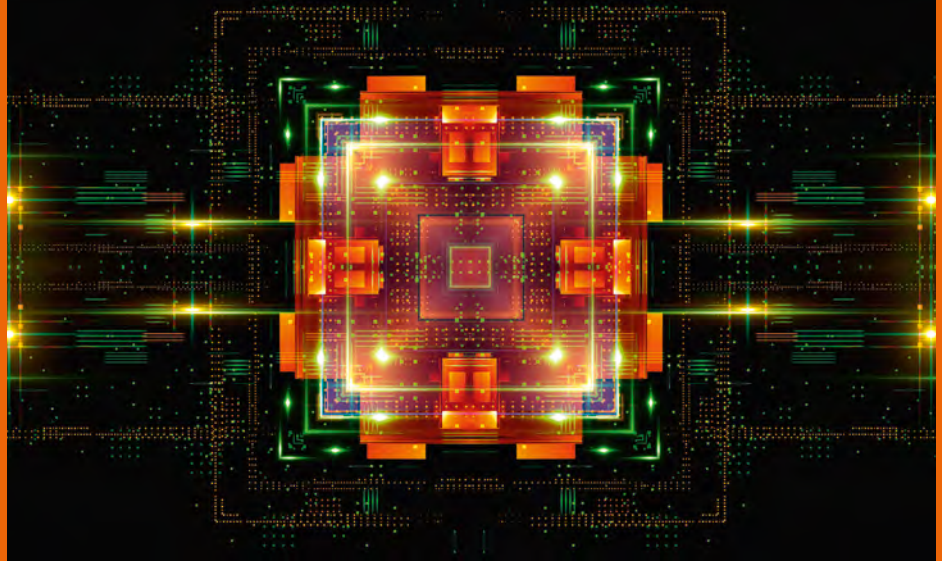
Man stelle sich einmal vor, dass von heute auf morgen alle Sicherheitsmaßnahmen unserer IT-Systeme ausgehebelt sind. Hacker haben Zugriff auf praktisch jedes vernetzte Informationssystem und können nach eigenem Ermessen Daten manipulieren. Die Konsequenzen eines solchen Szenarios sind dramatisch.

Die IT-Sicherheit basiert heutzutage auf Problemen, welche von einem gewöhnlichen Computer nicht oder nur mit unverhältnismäßig großem Aufwand gelöst werden können. Dieses Prinzip bildet die Basis der modernen Kommunikationsgesellschaft. Gelingt es allerdings, einen sogenannten skalierbaren Quantencomputer zu konstruieren, sind viele dieser Verfahren angreifbar und Sicherheit, wie wir sie heute kennen, nicht mehr möglich.

Die Lösung: Bewerten der Gefahrenlage und Einführung in Quanten-resistente Verfahren

Bewerten der Gefahrenlage und Einführung in Quanten-resistente Verfahren. Gerade in Bereichen mit langer Einsatzdauer, wie kritischen Infrastrukturen oder behördlichen Einsatzszenarien, sollte man sich der möglichen Gefahrenlage der Zukunft bewusstwerden, um schon heute proaktiv Maßnahmen ergreifen zu können.

In dem Modul wird den Teilnehmenden die Funktionsweise eines Quantencomputers erläutert und ein Überblick über die Herausforderungen für die IT-Sicherheit verschafft. Insbesondere wird es den Teilnehmenden ermöglicht, aktuelle Entwicklungen in diesem Gebiet fundiert bewerten zu können. Eine Einführung in sogenannte Post-Quantum Verfahren, die auch künftig sicher sind, runden das Modul ab.



INFORMATIONEN IM ÜBERBLICK

Kurs: Post-Quanten Sicherheit
Voraussetzungen: Grundlegende Kenntnisse in IT-Sicherheit und Kryptographie von Vorteil, aber nicht zwingend
Dauer: 2 Tage Präsenz
Kurssprache: Deutsch
Teilnehmerzahl: max. 12 Personen
Veranstaltungsort: Weiden
Kosten: 1200 €
Veranstaltet durch:

Fraunhofer AISEC

UNSER REFERENT

Prof. Dr. Daniel Loebenberger
Professor für Cybersicherheit an der Ostbayerischen Hochschule Amberg Weiden und Leiter der Forschungsgruppe Secure Infrastructure am Fraunhofer AISEC

Die Inhalte

- Funktionsweise eines Quantencomputers
- Quantengatter und einfache Quanten-Algorithmen mit Hands-On Simulationen
- Die Auswirkungen der Algorithmen von Shor und Grover auf die moderne Kryptographie
- Einführung in Post-Quantum Kryptographie, praxisnahe Übungen zu dem Thema
- Die laufende Standardisierung der NIST

Die Zielgruppe

- Administratoren, die schon heute ihre IT-Infrastruktur Post-Quanten sicher machen wollen
- Anwender von IT-Sicherheit, die verstehen wollen, wie sich die IT-Sicherheit in den nächsten Jahren entwickelt
- Fachkräfte und Spezialisten aus der Hochsicherheits-Industrie

Die Lernziele

Nach dem Seminar verstehen die Teilnehmenden den Unterschied zwischen einem gewöhnlichen Computer und Quantencomputern. Sie haben erste Erfahrungen mit Quantenalgorithmen und können den Einfluss von Quantencomputern auf die IT-Sicherheit nachvollziehen und entsprechend einschätzen. Die Teilnehmenden sind nach dem Seminar in der Lage, einen Ausweg aus dem IT-Sicherheitsalbtraum zu finden und kennen aktuelle Bemühungen aus der anwendungsorientierten Forschung dazu.

Das Lernlabor Cybersicherheit: Weiterbildung für die IT-Sicherheitsexperten von morgen

Das Lernlabor Cybersicherheit ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit moderner IT-Infrastruktur.

HABEN SIE NOCH FRAGEN ZU…

… Post-Quanten Sicherheit?
Prof. Dr. Daniel Loebenberger
Fraunhofer AISEC – Standort Weiden
Telefon +49 1701535324
daniel.loebenberger@aisec.fraunhofer.de

… Anmeldung, Organisation oder weiteren Angeboten?
Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de