Seminarprogramm

Montag, 27.10.2025
08.30 – 16.45 Uhr

08.30 – 09.00	Begrüßung, Organisation, Einführung
09.00 – 10.30 H. Bartz	**Grundlagen der Kryptographie** Modelle, Symmetrische / Asymmetrische Kryptographie
11.00 – 12.30 H. Bartz	**Grundlagen der Post-Quantum Kryptographie** Shor / Grover Algroithmus, Pre- / Post-Quantum Security
13.30 – 15.00 H. Bartz	**Grundlagen von Fehlerkorrekturcodes** Lineare Blockcodes, Endliche Körper, Polynomringe
15.15 – 16.45 H. Bartz	**Code-basierte Post-Quantum Verschlüsselungsverfahren, Teil 1** McEliece Kryptosystem, Generische Decodierung

Dienstag, 28.10.2025
08.30 – 16.30 Uhr

08.30 – 10.00 H. Bartz	**Code-basierte Post-Quantum Verschlüsselungsverfahren, Teil 2** Attacken, HQC Kryptosystem
10.30 – 12.00 H. Bartz	**Gitter-basierte Post-Quantum Verschlüsselungsverfahren, Teil 1** Grundlagen von Gittern, Grundlagen der Gitter-basierten Kryptographie
13.00 – 14.30 H. Bartz	**Gitter-basierte Post-Quantum Verschlüsselungsverfahren, Teil 2** Grundlegende Rekonstruktionsprobleme, NTRU Kryptosystem
15.00 – 16.30 H. Bartz	**Überblick NIST Post-Quantum Standardisierungsprozess** Existierende Standards, Statistiken, Technologien, Referenzimplementierungen

Unterlagen

Jeder Teilnehmer erhält die Vortragsunterlagen.
Die Kosten dafür sind in der Gebühr enthalten.

Seminarort

CCG-Zentrum, Technologiepark
Argelsrieder Feld 22, Geb. TE 03, D-82234 Weßling-Oberpfaffenhofen

Eine Lageskizze sowie Hinweise für die Anreise und Übernachtung schicken wir Ihnen mit der Bestätigung der Anmeldung zu.

Gebühr

EUR 1.490,--
Die CCG ist ein gemeinnütziger Verein und in Deutschland von der Umsatzsteuer befreit. Für Veranstaltungen an ausländischen Standorten gelten die dortigen Steuerregelungen.

Mitglieder der CCG erhalten 10% Rabatt. Studentenrabatte sind auf Nachfrage verfügbar. Die Rabatte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte melden Sie sich möglichst bis 14 Tage vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Argelsrieder Feld 22, D-82234 Weßling
Tel. +49 (0) 8153 / 88 11 98 -12
E-Mail: anmelden@ccg-ev.de
Internet: www.ccg-ev.de

Die Anmeldungen werden schriftlich bestätigt.

Weitere Informationen zum Inhalt

Dr.-Ing. Hannes Bartz, DLR, Oberpfaffenhofen
Institut für Kommunikation und Navigation, D-82234 Weßling
Tel. +49 (0) 8153 / 28-2252, E-Mail: hannes.bartz@dlr.de

Stornierung

Bei Stornierungen, die später als 14 Tage vor Seminarbeginn eingehen, werden 25% der Gebühr, bei Nichterscheinen die volle Gebühr in Rechnung gestellt. Die Vertretung eines angemeldeten Teilnehmers ist selbstverständlich möglich.

Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus anderen triftigen Gründen ein Seminar bis 14 Tage vor Beginn abzusagen. Sie behält sich weiter vor, entgegen der Ankündigung im Programm auch kurzfristig einen Dozenten und evtl. auch dessen Thema zu ersetzen. Ein Schadensersatzanspruch bleibt ausgeschlossen.

Post-Quantum Sichere Verschlüsselungsverfahren

Teilnehmer

Das Seminar richtet sich an Fachleute aus Industrie, Behörden und Streitkräften, an Ingenieure und Wissenschaftler aus Forschung und Entwicklung mit Bezug zu sicherer Kommunikation sowie an Hersteller und Betreiber von Kommunikations- und Kryptosystemen.

Seminarinhalte

Zukünftige Quantencomputer stellen eine Gefährdung für aktuelle Verschlüsselungs- und Signaturverfahren dar. Auch wenn heutige Quantencomputer noch nicht in der Lage sind, aktuelle kryptographische Systeme zu brechen, können Daten, die mit heutigen Methoden verschlüsselt und gespeichert werden, in Zukunft von leistungsstarken Quantencomputers entschlüsselt werden.

In diesem Seminar wird ein Überblick über den aktuellen Stand der Technik von „Post-Quantum" Verschlüsselungsverfahren, welche eine sichere Kommunikation im Zeitalter des Quantencomputers ermöglichen, gegeben. Das Seminar gibt einen Einblick in die Gefährdungen aktueller kryptographischer Systeme durch Quantencomputer und beleuchtet Methoden und Technologien, um diese langfristig abzuwenden. Der Fokus liegt hierbei auf kryptographischen Systemen, welche auf fehlerkorrigierenden Codes sowie Gittern (engl. „Lattices") basieren. In diesem Zusammenhang werden die wichtigsten Unterschiede zwischen Post-Quantum und klassischen Kryptosystemen aufgezeigt und mittels konkreter Beispiele verdeutlicht. Des Weiteren wird ein Überblick über die aktuell laufende Standardisierung von Post-Quantum Kryptosystemen am „National Institute of Standards and Technology (NIST)" gegeben. Der Standardisierungsprozess wird beispielhaft durch die Betrachtung eines Post-Quantum NIST Kandidaten bzw. eines bereits ausgewählten Schemas veranschaulicht.

Vortragende

Dr.-Ing. Hannes Bartz	DLR, Oberpfaffenhofen Institut für Kommunikation und Navigation

Carl-Cranz-Gesellschaft e.V. | Weßling
Gesellschaft für technisch-wissenschaftliche Weiterbildung

Seminar IN 6.46

Post-Quantum Sichere Verschlüsselungsverfahren

27. – 28. Oktober 2025
Oberpfaffenhofen bei München

Informatik

Wissenschaftliche Leitung
Dr.-Ing. Hannes Bartz
DLR, Oberpfaffenhofen