



Seminarort

CCG-Zentrum, Technologiepark Argelsrieder Feld 11
D-82234 Weßling-Oberpfaffenhofen

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

Gebühr

EUR 1.180,-
Die CCG ist ein gemeinnütziger Verein und in Deutschland von der Um-
satzsteuer befreit. Für Veranstaltungen an ausländischen Standorten
gelten die dortigen Steuerregelungen.

Mitglieder der CCG erhalten 10% Rabatt. Bei Anmeldung mehrerer Mit-
arbeiter einer Firma / Dienststelle zum gleichen Seminar erhält jeder Teil-
nehmer 10%. Studentenrabatte sind auf Nachfrage verfügbar. Die Ra-
batte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte möglichst bis 3 Wochen vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Argelsrieder Feld 11, D-82234 Weßling
Tel. +49 (0) 8153 / 88 11 98 -12, Fax -19, 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 Stornierung mündlich oder schriftlich bestätigter Anmeldungen wird
eine Bearbeitungsgebühr von EUR 25,- berechnet. Bei Stornierungen,
die später als 10 Tage vor Seminarbeginn eingehen, werden 25% der
Gebühr, bei Nichterscheinen die volle Gebühr in Rechnung gestellt. Die
Vertretung eines angemeldeten Teilnehmers ist möglich.

Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus ande-
ren triftigen Gründen ein Seminar bis 10 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.



Teilnehmer

Das Seminar richtet sich an Fachleute aus Industrie, Behörden und Streit-
kräften, 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
Quantencomputern 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 veranschaulicht.

Vortragende

Prof. Antonia Wachter-Zeh	TU München Professur für Coding for Com- munications and Data
Dr.-Ing. Hannes Bartz	DLR, Oberpfaffenhofen Institut für Kommunikation und Navigation



Seminar IN 6.46

Post-Quantum Sichere Verschlüsselungsverfahren

**24. – 25. März 2021
Oberpfaffenhofen bei München**

Wissenschaftliche Leitung

Prof. Antonia Wachter-Zeh
TU München
Dr.-Ing. Hannes Bartz
DLR, Oberpfaffenhofen

Seminarprogramm

Mittwoch, 24.3.2021
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 Algorithmus, Pre- / Post-Quantum Security
13.30 – 15.00 A. Wachter-Zeh	Grundlagen von Fehlerkorrekturcodes Lineare Blockcodes, Endliche Körper, Polynomringe
15.15 – 16.45 A. Wachter-Zeh	Code-basierte Post-Quantum Verschlüsselungsverfahren, Teil 1 McEliece Kryptosystem, Generische Decodierung

Donnerstag, 25.3.2021
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 A. Wachter-Zeh	Gitter-basierte Post-Quantum Verschlüsselungsverfahren, Teil 1 Grundlagen von Gittern, Grundlagen der Gitter-basierten Kryptographie
13.00 – 14.30 A. Wachter-Zeh	Gitter-basierte Post-Quantum Verschlüsselungsverfahren, Teil 2 Grundlegende Rekonstruktionsprobleme, NTRU Kryptosystem
15.00 – 16.30 H. Bartz	Überblick NIST Post-Quantum Standardisierungsprozess Statistiken, Technologien, Referenzimplementierungen

Unterlagen

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

Weitere Seminare zum Themenbereich

- „Einführung in das Quantum Computing und seine Anwendungen“, 18.–20.5.2021 (Code IN 5.20)
- „Kryptografie - eine Schlüsseltechnik zur Gestaltung zukünftiger Informationstechnik“, 7.–8.6.2021 (Code IN 6.17)
- „Ganzheitliche Sicherheit: Von der Kryptografie bis zu Physical Unclonable Functions“, 21.–23.9.2021 (Code IN 6.27)

Wichtige Info

Aufgrund der pandemischen Lage wird dieses Seminar online durchgeführt.