## 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 1.890,--
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 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

K.-D. Wolfenstetter, ehem. Deutsche Telekom AG, Laboratories, Berlin
E-Mail: k.wolfenstetter@t-online.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.

Ganzheitliche Sicherheit

## Teilnehmer

- Datenschutz- und Datensicherheitsbeauftragte und -verantwortliche
- CSOs und CISOs in Unternehmen und Behörden
- Compliance-Verantwortliche
- Studierende und Mitarbeiter in den MINT-Fächern

## Seminarinhalte

Einerseits bietet die mathematisch begründete Kryptographie ein festes Fundament für jede Sicherheitslösung. Andererseits bietet deren Implementierung und Realisierung etwa in SW, aber auch in HW, mögliche Angriffsflächen für technologisch gut ausgerüstete Angreifer. Ein guter kryptographischer Algorithmus ist dann wertlos, wenn z. B. seine geheimen Schlüssel im realisierenden Medium (Chip, Rechner, Handy) ausgespäht werden können.

Das Seminar umfasst in einer ganzheitlichen Sicht den kompletten Zyklus von den kryptographischen Methoden (z. B. RSA, AES) über deren Anwendungen und Einsatzszenarien (Internet, Mobilkommunikation) bis hin zu modernsten Angriffsmethoden aus der Praxis (Optische Emission, Reverse Engineering, HW Trojaner).

## Vortragende

| | | |
|---|---|---|
| A. Beutelspacher | Prof. Dr. | Universität Gießen<br>Mathematisches Institut |
| J.-P. Seifert | Prof. Dr. | TU Berlin |
| K.-D. Wolfenstetter | Dipl.-Math. | ehem. Deutsche Telekom AG,<br>Laboratories, Berlin<br>KDWsec |

## Unterlagen

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

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

**Seminar IN 6.27**

# Ganzheitliche Sicherheit: Von der Kryptographie bis zu Physical Unclonable Functions

**17. – 19. September 2024**
**Oberpfaffenhofen bei München**

**Wissenschaftliche Leitung**

Dipl.-Math. K.-D. Wolfenstetter
ehem. Deutsche Telekom AG, Laboratories, Berlin; KDWsec

Informatik

# Seminarprogramm

## Dienstag, 17.09.2024
## 10.15 – 16.30 Uhr

| | |
|---|---|
| 10.15 – 10.30 | Begrüßung, Einführung, Organisation |
| 10.30 – 12.00<br>A. Beutelspacher | **Ziele und Probleme der Kryptographie** |
| 13.00 – 14.30<br>A. Beutelspacher | **Symmetrische Verschlüsselungsverfahren**<br>Data Encryption Standard DES |
| | Modes of Operation |
| | Advanced Encryption Standard AES |
| | Kryptoanalyse |
| 15.00 – 16.30<br>A. Beutelspacher | **Public Key Kryptographie**<br>RSA und Diffie Hellman |
| | Digitale Signaturen, Zertifikate, PKI |
| | Verfahren auf Basis des Diskreten Logarithmus |
| | Elliptische Kurven Kryptographie |

## Mittwoch, 18.09.2024
## 08.30 – 16.30 Uhr

| | |
|---|---|
| 08.30 – 10.00<br>J.-P. Seifert | **Probleme und Herausforderungen technologischer Sicherheit**<br>Implementierungen und Realisierungen |
| | Das Ende von Moore's Law und Non-volatile Memo |
| 10.30 – 12.00<br>J.-P. Seifert | **Neue Angriffsmethoden aus der Praxis**<br>Focus Ion Beam, Optische Emission und Fehler Induktionsmethoden |
| | Hardware Trojaner |
| | Reverse Engineering von Chips |
| 13.00 – 14.30<br>J.-P. Seifert | **Neue Entwicklungen in der Sicherheitstechnologie**<br>Physical Unclonable Functions (PUFs) |
| | Obfuscation oder leakage-resilient Kryptographie zur Umgehung der Grenzen |
| 15.00 – 16.30<br>J.-P. Seifert | **Grenzen der heutigen Implementierungen bzgl. Sicherheit** |

## Donnerstag, 19.09.2024
## 08.30 – 16.30 Uhr

| | |
|---|---|
| 08.30 – 10.00<br>K.-D. Wolfenstetter | **Anwendungsfelder von Kryptographie und Sicherheitstechnologie**<br>Sicherheitsstandards in der Mobilkommunikation; Angriffsarten und Risikobetrachtungen |
| | Sicherheit im Internet: Layer-Sicherheit und ihre Grenzen; IPv6; Browser; eMail |
| 10.30 – 12.00<br>K.-D. Wolfenstetter | **Spezielle Szenarien der Sicherheit**<br>Smart Meter und Smart Meter Gateway in Energienetzen |
| | eCards: Neuer Personalausweis, Gesundheitskarten, Payment und mWallet |
| 13.00 – 14.30<br>K.-D. Wolfenstetter | **Neue Entwicklungen und Herausforderungen für die Sicherheit**<br>Embedded Security; Industrie 4.0 |
| | Blockchain und Kryptographie |
| | Quantum Computing und Kryptographie |
| 15.00 – 16.30<br>K.-D. Wolfenstetter | **Ganzheitliche Sicherheit**<br>Technologische und regulatorische Grenzen der Sicherheit |
| | Pro und contra Kryptoregulierung |
| | Die neue EU-Verordnung EIDAS: Sicherheit für den Binnenmarkt |
| | IT-Sicherheitsgesetz(e) |