



## Hauptseminar Informationssicherheit und Kryptographie

In diesem Seminar werden Forschungsthemen aus verschiedenen Bereichen der **IT-Sicherheit, einschließlich Kryptographie, Privacy und Websicherheit**, behandelt. Die Themen richten sich nach Veröffentlichungen auf führenden wissenschaftlichen Konferenzen. Teilnehmer sollten einen sehr fundierten mathematisch/theoretischen Schwerpunkt mitbringen.

Die Themen richten sich nach den Forschungsschwerpunkten des Instituts und sind semesterabhängig. Mögliche Themen sind:

- kryptographische Protokolle (TLS, SSH, WLAN, GSM, Signal [Whatsapp], ...)
- Multi-Party-Computation
- Websicherheit und Single-Sign-On
- (Zwei-Faktor-)Authentifizierung
- elektronische Wahlen
- Fully Homomorphic Encryption
- Blockchain (Bitcoin, Ethereum, ...)
- Payment-Lösungen (EMV, Cashier-as-a-Service, ...)
- Privacy Preserving Learning in neuronalen Netzen
- Post-Quantum-Kryptographie
- Trusted Computing (SGX, ...)
- Differential Privacy
- Angriffe in all diesen Bereichen

Voraussetzungen zur Teilnahme am Seminar:

- Sehr fundierter mathematisch/theoretischer Hintergrund
- Erfolgreiche Teilnahme an einer der folgenden Vorlesungen am Institut für Informationssicherheit: Introduction to Modern Cryptography, System and Web Security, Security and Privacy, Mathematical Foundations of (Post-Quantum) Cryptography oder Post-Quantum Secure Cryptography

Das Seminar wird auf **Deutsch** abgehalten.

**Hinweise zum Ablauf:** Die konkreten Seminarthemen werden in einer Vorbesprechung zu Beginn des Semesters (voraussichtlich erste Vorlesungswoche) vorgestellt und nach Präferenz der Seminarteilnehmer/-innen verteilt. Sie fertigen während der Vorlesungszeit sowohl eine schriftliche Ausarbeitung als auch einen Vortrag an. Alle Vorträge finden in einer **Blockveranstaltung** gegen Ende der Vorlesungszeit statt (voraussichtlich erste/zweite Woche nach den Vorlesungen); während der Vorlesungszeit gibt es dementsprechend KEINE wöchentlichen Sitzungen. Bitte beachten Sie, dass die Ausarbeitungen bereits kurz nach den Vorträgen abzugeben sind.

Die **Vorbesprechung** findet voraussichtlich in der ersten Vorlesungswoche statt – der genaue Termin wird den Seminarteilnehmern zeitnah bekanntgegeben.

**Ansprechpartner:** Fabian Hauck (fabian.hauck@sec.uni-stuttgart.de)  
Pedram Hosseyni (pedram.hosseyni@sec.uni-stuttgart.de)

**Prüfer:** Prof. Dr. Ralf Küsters