Fraunhofer
ACADEMY

SEMINAR

## IHRE VORTEILE AUF EINEN BLICK

**Nach dem Seminar können Sie …**

…verschiedene Einsatzmöglichkeiten von PUFs einschätzen

…wichtige praktische Beispiele von PUF-Schaltungen, Protokollen für Lightweight Authentifizierung, Fehlerkorrekturverfahren und Angriffen auf PUFs nachvollziehen

**Dieses Seminar bietet Ihnen …**

…eine Einführung und einen Überblick über PUFs mit Fokus auf die praktische Anwendung

…einen Zugang zu neuesten wissenschaftlichen Erkenntnissen aus der PUF-Forschung

**Melden Sie sich gleich an!**
**www.cybersicherheit.fraunhofer.de/hardwaregebundene-identitaeten**

# SICHERE HARDWARE-GEBUNDENE IDENTITÄTEN

Von der Fertigungsschwankung zum einzigartigen Gerät

### Die Herausforderung: IoT-Systeme effizient schützen

Eine sichere IT-, und speziell IoT-Infrastruktur, setzt sichere Geräte an sich und auch eine sichere Authentifizierung der vernetzten Geräte voraus. IoT-Geräte müssen dabei für einen flächendeckenden Einsatz günstig und sparsam sein. Im Gebiet der Lightweight-Kryptographie wurden bereits entsprechende Algorithmen entwickelt. In herkömmliche Fertigungstechnologien ist es jedoch schwierig und technologisch aufwändig, auch sichere Schlüsselspeicher in das System zu integrieren. Diese sind jedoch Voraussetzung, für einzigartige und sichere Identitäten der Geräte.

### Die Lösung: Einzigartiges Verhalten aus jedem Gerät durch Physical Unclonable Functions

Physical Unclonable Functions (PUFs) werten Fertigungsschwankungen in elektronischen Schaltungen aus, um für jeden Gegenstand ein einzigartiges Verhalten, ähnlich eines Fingerabdrucks, abzuleiten. Challenge-Response-Protokolle ermöglichen es, mit Hilfe von PUFs, Geräte auch ohne kryptographische Algorithmen zu authentifizieren. Außerdem können Schlüssel für kryptographische Algorithmen zur Laufzeit mit PUFs erzeugt werden, sodass sie nicht dauerhaft im System gespeichert werden müssen und somit keine sicheren Schlüsselspeicher im Gerät benötigt werden.

## INFORMATIONEN IM ÜBERBLICK

**Kurs:** Sichere hardwaregebundene Identitäten
**Voraussetzungen:** Grundlagen IT-Security, es wird kein Vorwissen in Hardware Security oder Elektrotechnik benötigt
**Dauer:** 1 Tag Präsenz
**Kurssprache:** Deutsch
**Teilnehmerzahl:** max. 16 Personen
**Veranstaltungsort:** Garching bei München
**Kosten:** 600 €
**Veranstaltet durch:**

Fraunhofer AISEC

## UNSER REFERENT

**Dr. Matthias Hiller**
Gruppenleiter
Physical Security Technologies am Fraunhofer AISEC

### Die Inhalte

- Authentifizierung in eingebetteten Systemen / IoT
  - Stand der Technik
  - Vorteile durch Hardware Fingerprinting/PUFs
- Von der physikalischen Fertigungsschwankung zur Sicherheit
  - Einführung PUF-Schaltungen
  - Leichtgewichtige Authentifikation ohne Kryptographie
  - Generierung kryptographischer Schlüssel mit PUFs
- Sicherheitsanalyse
  - Bewertung von PUF Daten
  - Angriffe und Gegenmaßnahmen
- Systemsicht und Einsatzszenarien

### Die Lernziele

- Szenarien für den Einsatz von PUFs einordnen
- PUFs mit anderen Technologien vergleichen
- PUF-Schaltungen, Protokolle für Lightweight Authentifizierung, Fehlerkorrekturverfahren und Angriffe auf PUFs nachvollziehen

### Die Zielgruppe: Sicherheitsexperten, die ihr Wissen auf den neuesten Stand bringen wollen

- IT-Security Fachexperten
- Hardware-Architekten
- Manager
- Technische (Projekt-) Leiter in Entwicklungsprojekten

### 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…

**… Sichere hardwaregebundene Identitäten?**
Dr. Matthias Hiller
Fraunhofer AISEC
Telefon +49 89 3229986-162
matthias.hiller@aisec.fraunhofer.de

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