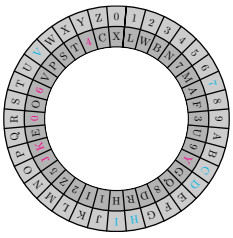

Wintersemester 2016/2017
Prof. Dr. Steffen Reith

Vortragsankündigung

Am 23. November 2016 um 14^{15} im Raum C407

spricht

Herr Matthias Hiller
(Fraunhofer AISEC, München)

zum Thema

Tying Cloud Access to Circuit Variation

Zusammenfassung:

Eine sichere Cloud-Infrastruktur setzt zum einen eine sichere Cloud und zum anderen eine sichere Authentifizierung der Nutzer voraus. Physikalische Gegenstände wie Hardware Tokens erhöhen die Sicherheit, indem sie den Zugang zur Cloud an die physikalische Welt binden und sich nicht nur auf Nutzereingaben verlassen. Außerdem erlauben sichere Hardwareidentitäten, dass sich Dinge im Internet der Dinge (IoT) selbstständig gegenüber der Cloud authentifizieren. Physical Unclonable Functions (PUFs) werten Fertigungsschwankungen in Schaltungen aus, um jedem Gegenstand ein einzigartiges Verhalten zu geben. PUFs können einfach in die Entwicklung von Digitalschaltungen eingebunden werden, sodass sie auch für low-cost IoT Geräte verfügbar sind. In diesem Vortrag werden neue Ergebnisse zur Schlüsselerzeugung mit PUFs vorgestellt, um sie für traditionelle kryptografische Authentifizierung zu verwenden. Außerdem wird lightweight Authentifizierung mittels PUFs vorgestellt, die nicht auf kryptografischen Algorithmen basiert.

Alle Interessierten sind herzlich eingeladen!