Einladung
zum Doktorandenkolloquium

Innovative Hardware-Sicherheitslösungen durch Physical Unclonable Functions in neuartigen Speichertechnologien und Nanomaterialien

von Florian Frank

am Mittwoch, 6.11.2024 ab 13:00 Uhr im SR 027, WiWi, Innstr. 27 und online per Zoom (die Zoomdaten wurden intern gemailt)

(Betreuer: Prof. Dr. Stefan Katzenbeisser,
Lehrstuhl für Technische Informatik)

Zusammenfassung: In Microcontrollern, die durch neue innovative CPU-Technologien oder Speichertechnologien gekennzeichnet sind, bleibt es eine Herausforderung, sichere Schlüssel für Verschlüsselungsalgorithmen und Authentifizierungsverfahren bereitzustellen. Insbesondere für ressourcenbeschränkte Geräte bieten verschiedene Physical Unclonable Functions (PUFs) Möglichkeiten der Geräteauthentifizierung, -identifikation und Schlüsselerzeugung. Traditionell wurden PUFs durch speziell entworfene Schaltungen oder die Nutzung intrinsischer Eigenschaften von Komponenten wie SRAM-Speicher umgesetzt um somit einzigartige und robuste Schlüssel zu erzeugen. Zur Absicherung neuartige Gerätetechnologien wie die Verwendung neuer Speichertechnologien wie Resistive Random Access Memory (ReRAM), Ferroelectric Random Access Memory (FRAM) und Magnetoresistive Random Access Memory (MRAM), besteht die Notwendigkeit innovativer Hardware-Sicherheitslösungen, die auf intrinsischen Hardware-Fingerabdrücken dieser Technologien basieren. Zudem erfordert die Integration von Nanomaterialien in CPUs und neuen rekonfigurierbaren Hardwareplattformen neue innovative IT-Sicherheitsansätze. Ziel der Dissertation ist die Entwicklung von Methoden der Hardware-Sicherheit in diesen neuen Gerätetypen. Dabei werden verschiedene Arten von PUFs und deren Anwendungen untersucht. Diese Arbeit konzentriert sich zunächst auf die Grundelemente neuer Technologien wie Nanomaterialien und passive Schaltungselemente, insbesondere Memristoren und Kohlenstoff-Nanoröhren-Feldeffekttransistoren, um deren Eigenschaften als PUFs zu nutzen. Im Anschluss werden PUFs in kommerziellen Chips, die aus solchen Basiselementen bestehen, konstruiert. Schließlich werden Anwendungen der PUF-Implementierungen demonstriert. Eine neuartige Architektur zur Verschlüsselung und Bindung von Daten an nicht-flüchtige Speichermodule, die eine FPGA-basierte Implementierung nutzt, wird vorgestellt.