Talk Title:

Utilizing Time-Based Sensors for Enhanced Device Fingerprinting, Authentication, and Tamper Detection in Semiconductor Devices

Abstract:

In recent years, the significance of hardware security has grown considerably, as the proliferation of overproduction, counterfeits, trojans, process modifications, and post-fab tampering pose increasingly grave threats to the integrity and trustworthiness of electronic systems. This, in turn, necessitates comprehensive measures to safeguard critical infrastructures and sensitive data. Addressing these concerns requires a multidisciplinary approach involving stringent supply chain oversight, advanced authentication mechanisms, and continuous monitoring to detect and mitigate potential vulnerabilities in hardware components and designs. A promising approach to address these threats is the utilization of device fingerprinting, which has gained significant traction over the past few years. Within the domain of wireless networks, the concept of RF fingerprint, also referred to as RF distinct native attribute (RF DNA), has been developed to discern and categorize authorized devices based on their distinct device features. Likewise, various methodologies have been proposed to bolster security throughout the entire life cycle of the global supply chain. These include techniques like die identification, die authentication, and tamper detection. Die identification involves the assignment of a unique serial number to each individual die, while die authentication verifies the device's manufacturing origin to ensure authenticity. Consequently, device fingerprinting circuits represent a comprehensive solution encompassing both die identification and authentication capabilities. Furthermore, when integrated with tamper detection, these circuits play a crucial role in preventing unauthorized access, preserving system integrity, and enhancing security.

Physical Unclonable Functions (PUFs) offer a promising avenue for chip identification by leveraging inherent manufacturing variations in integrated circuits. PUFs generate unique challenge-response pairs (CRPs) that serve as digital fingerprints, enabling dependable chip identification. However, while PUFs excel in die identification, they exhibit deficiencies in die authentication and tamper protection. Notably, PUFs' digital output bits lack correlation with the distinct attributes of the original foundry, thus limiting their potential for die authentication. Additionally, PUFs can only detect tampering within their designated circuit area, rendering them ineffective against attacks outside this region. Moreover, the creation of CRP databases post-chip manufacturing exposes PUFs to tampering during foundry processes and unauthorized fabrication facility production.

To mitigate this issue, a process characterization function (PCF) has been proposed, leveraging the unique process characteristics of the foundry to facilitate die authentication. For instance, one PCF approach dissects path delays into delays of logic gates to extract the threshold voltage and effective channel length, serving as unique signatures to differentiate between foundries. Another approach modifies the successive-approximation-register (SAR) analog-to-digital (ADC) architecture and employs the mismatch of the metal-oxide-metal (MOM) capacitor as a means of authentication. A third approach involves reducing the activation time—the duration for a row of DRAM cells to become accessible—and then analyzing the error patterns as distinctive authentication features. However, these PCFs, while adept at authenticating chips based on foundry-related attributes lack the capability to distinguish between individual chips, unlike PUFs. This limitation stems from the fact that PCFs capture only a limited set of features representing

the foundry process and do not offer a distinctive identification for each chip. Furthermore, akin to PUFs, PCFs also face constraints in detecting tampering and are unable to effectively identify tampering attempts occurring outside their designated areas.

In this workshop talk, we will present a novel approach and recent measurement results from our work to enhance hardware security through the integration of a unique time-based sensor into semiconductor devices, enabling robust device fingerprinting, die authentication, die identification, and tamper detection. The proposed time-based sensor exploits the inherent characteristics of the back-end-of-line (BEOL) metal routing within the chip, offering a means to directly measure the RC time-constants of interconnects. The challenge lies in the inherently small RC time-constants resulting from design considerations that minimize resistance and capacitance. To address this, a "three-configuration" measurement approach is introduced, leveraging auxiliary components to amplify the RC time-constants, ultimately enhancing measurement accuracy while incurring a minimal area penalty.

The proposed sensor's integration within the functional routing of system-on-chip (SoC) devices establishes a comprehensive approach for device fingerprinting and tamper detection. The dependency of RC time-constants on design and foundry characteristics allows for the identification of alterations, such as tampering or fabrication in different foundries, by detecting deviations from expected distributions. Moreover, advancements in technology nodes contribute to increased time-domain resolution, bolstering the accuracy of sensor-based authentication.

In addition to authentication and tamper detection, the proposed sensor facilitates die identification by amalgamating outputs from multiple on-chip sensors, thus generating a unique and distinguishable chip ID. This combinatorial approach reduces the likelihood of identical identifications, ensuring the uniqueness and precision of the identification process.

The talk will provide valuable insights into the sensor architecture, design, and measurement results, enabling a deeper understanding of the proposed sensor's intricacies and its potential for widespread adoption in semiconductor security measures.

Speaker Bio:

Dr. Waleed Khalil received his BS and MS degrees from the University of Minnesota, and his PhD degree from Arizona State University. He is currently serving as a Professor at the ECE department and the ElectroScience Lab, The Ohio State University. He also serves as Co-Director of the Air Force Center of Excellence for Enabling Cyber Defense in Analog and Mixed Signal Domain (CYAN) and The National MicroElectronics Security Training Center (MEST). Prior to joining OSU in 2009, he spent 16 years at Intel Corporation where he held various positions in research and product groups. His group’s research is focused on integrated circuits and systems, with applications in the areas of hardware security and trust, wireless and wireline communications, heterogeneous chip integration, and image sensors. He is the recipient of OSU’s College of Engineering Lumley Research Award and IEEE-Eta Kappa Nu/Fred H. Pumphrey's Distinguished Teacher Award. His research group has received several best paper awards in several conferences. He authored 19 issued and several other pending patents, over 120 journal and conference papers and three books/book chapters. He served as an Associate Editor for the Journal of Solid-State Circuits and is currently serving as the Associate VP for Publications at the IEEE Solid-State Circuits Society and in the Organizing Committee at the IEEE International Symposium on Hardware Oriented Security and Trust (HOST).