Abstract

The widespread adoption of IoT devices, mobile communication systems, and electric mobility infrastructures has intensified the demand for authentication mechanisms that are lightweight, scalable, and resilient to physical and network-based adversaries. Existing authentication schemes predominantly rely on storing long-term secret keys in non-volatile memory, making them vulnerable to key extraction, duplication, device impersonation, and invasive attacks. Although Physical Unclonable Functions (PUFs) have emerged as an attractive alternative for eliminating stored secrets, prior PUF-based authentication frameworks suffer from several shortcomings: (i) many designs require large Challenge–Response Pair (CRP) databases, which hinder scalability in large deployments; (ii) error-prone PUF responses require complex error-correction mechanisms, increasing the hardware overhead; (iii) the existing schemes often depend on computationally expensive public-key primitives which are not appropriate for constrained embedded devices; and (iv) limited attention has been given to domain-specific challenges in mobile networks and electric vehicle (EV) charging infrastructures.

To address the above-mentioned limitations, this thesis presents a unified investigation into lightweight, reliable, and domain-optimized PUF-based authentication architectures. First, a scalable Authentication and Key Agreement (AKA) protocol has been proposed for IoT devices, requiring only one stored CRP per device while achieving forward secrecy with minimal computational overhead. Subsequently, a highly reliable VIA PUF–based authentication framework has been developed, demonstrating near-zero bit-error rates across voltage and temperature variations, thereby eliminating the need for error correction. The thesis then introduces **SafeSIM**, a PUF- and Zero-Knowledge Proof–enabled mobile authentication architecture that prevents SIM cloning, SIM-swap attacks, and subscription fraud under both trusted and untrusted service-provider models. For electric mobility, a secure mutual authentication protocol has been designed for EV charging networks and validated by formal verification and hardware–software prototyping. Finally, to strengthen the hardware

foundation of PUF-based security, a Current Mirror Voltage Source (CMVS) circuit has been developed to significantly enhance the PUF stability under environmental and operational variability.

Overall, the present thesis strives to advance the practicality, reliability, and scalability of PUF-based authentication mechanisms, providing a comprehensive hardware-rooted security framework for next-generation IoTs, mobile communication, and electric mobility networks.

Keywords: Physical Unclonable Functions (PUFs), Zero-Knowledge Proofs, IoT Security, Mobile Network Security, Electric Vehicle Charging Networks.