A Reconfigurable SRAM-Based PUF Architecture for Robust and Lightweight Device Authentication

Advait Phadke *
Pimpri Chinchwad College of Engineering, Pune, India

Dr. Deepti Khurge
Pimpri Chinchwad College of Engineering, Pune, India

Darshan Tayade
Pimpri Chinchwad College of Engineering, Pune, India

Omkar Wadhavankar
Pimpri Chinchwad College of Engineering, Pune, India

Abstract

The rapid growth of Internet of Things (IoT) systems has intensified the need for secure, low-cost, and scalable device authentication mechanisms. Conventional approaches based on stored cryptographic keys are increasingly vulnerable to physical attacks, key leakage, and duplication. This work addresses these challenges by proposing a reconfigurable SRAM-based Physical Unclonable Function (PUF) that enables secure and hardware-intrinsic device identification without relying on permanent key storage. The proposed methodology leverages inherent process variations in SRAM cells to generate unique device signatures. A dynamic address selection scheme is introduced to support multiple challenge-response pairs from a single memory array, improving flexibility and increasing resistance to prediction and replay attacks. To ensure consistent performance under practical operating conditions, a lightweight error correction mechanism is incorporated to mitigate the effects of environmental variations such as temperature changes, supply fluctuations, and device aging. The proposed architecture is evaluated using standard PUF metrics, including uniqueness, reliability, and response stability. Results indicate improved robustness and enhanced challenge space compared to conventional fixed-address SRAM PUF designs, while maintaining low hardware and energy overhead. This work contributes a practical and scalable hardware security solution aligned with the needs of modern embedded and IoT systems. Its applicability extends to secure authentication, key generation, and trusted device identification, making it relevant for both academic research and real-world deployment in resource-constrained environments.

Keywords

SRAM-based PUF, hardware security primitives, device authentication, reconfigurable PUF, lightweight cryptography.