RADemics

Hardware Accelerated Cryptographic Implementations for Smart Wearables and IoT Nodes

Ashish Avasthi, Mohammad Ziaullah
POORNIMA UNIVERSITY, SECAB INSTITUTE OF ENGINEERING & TECHNOLOGY

Hardware Accelerated Cryptographic Implementations for Smart Wearables and IoT Nodes

[1]Ashish Avasthi, Professor, Faculty of Computer Engineering, Poornima University, Jaipur, Rajasthan, India. ashish.avasthi@poornima.edu.in

[2]Mohammad Ziaullah, Assistant Professor, Department of Electronics and Communication, SECAB Institute of Engineering and Technology Vijayapura, India. mdziaullah_ec@secab.org

Abstract

The rapid proliferation of smart wearables and Internet of Things (IoT) devices has intensified the demand for cryptographic solutions that are both secure and optimized for constrained environments. Traditional cryptographic algorithms, though robust, are often unsuitable for embedded systems with stringent limitations in area, power, and computational resources. This chapter presents a comprehensive analysis of hardware-accelerated lightweight cryptographic (LWC) implementations tailored for such platforms. It explores architectural design strategies including serial and parallel processing, bit-sliced and round-based structures, loop unrolling, sub-pipelining, and hardware multiplexing. Special attention was given to power optimization techniques such as clock gating, operand isolation, and power gating, which are critical in prolonging device lifetime. Benchmarking insights from FPGA and ASIC implementations underscore the trade-offs between area, energy efficiency, and throughput across leading algorithms like ASCON, GIFT, PRESENT, and TinyJAMBU, the chapter addresses side-channel resistance, fault injection countermeasures, and formal verification to ensure robustness against physical attacks. Emerging trends such as the integration of Physically Unclonable Functions (PUFs) and LWC support in protocol stacks like LoRaWAN and BLE are also discussed, highlighting real-world deployment potential. By bridging cryptographic theory with silicon-level implementations, this work provides a foundation for secure, scalable, and efficient cryptographic hardware in next-generation embedded systems.

Keywords: Lightweight Cryptography, Hardware Security, IoT Nodes, Smart Wearables, Side-Channel Resistance, Embedded Systems.

Introduction

The unprecedented growth of smart wearable technologies and Internet of Things (IoT) nodes has revolutionized the way embedded systems are designed and deployed [1]. These technologies are increasingly embedded in everyday environments, offering real-time data acquisition, adaptive control, and personalized services across sectors such as healthcare, industry, and urban infrastructure [2]. Their functional advantages, these systems face critical limitations stemming from their compact form factors, restricted energy sources, and limited computational capabilities [3]. Traditional approaches to security, typically developed for high-performance environments,

often fail to meet the constraints of these platforms [4]. As a result, ensuring data confidentiality, integrity, and authenticity within such a limited resource envelope has emerged as a fundamental challenge in the development of modern embedded systems [5].

Standard cryptographic protocols such as RSA and AES have proven to be highly secure in general-purpose computing but are often impractical for ultra-low-power or miniaturized devices [6]. Their high computational complexity, substantial memory usage, and increased latency make them unsuitable for wearables, RFID systems, or implantable medical devices [7]. Particularly, the energy overhead incurred during encryption and decryption processes in these systems can significantly reduce operational lifespans and performance efficiency [8]. The asymmetric cryptographic techniques that rely on intensive key management and large operand computations become prohibitively expensive for devices with limited battery and minimal processing cores [9]. This mismatch has necessitated the emergence of a new domain of cryptographic research—lightweight cryptography—that seeks to optimize algorithmic design for constrained environments without sacrificing essential security properties [10].