RADemics

FPGA Implementations of Secure Cryptographic Algorithms for Embedded Systems

Debabrata Dansana, Rakesh K Kadu
RAJENDRA UNIVERSITY, RAMDEOBABA UNIVERSITY

FPGA Implementations of Secure Cryptographic Algorithms for Embedded Systems

[1]Debabrata Dansana, Assistant Professor, Department of Computer Science, Rajendra University, Balangir, Odisha, India. debabratadansana07@gmail.com

[2]Rakesh K Kadu, Assistant Professor, School of Computer Science and Engineering, Ramdeobaba University, Nagpur, Maharashtra, India. kadurk@rknec.edu

Abstract

The escalating demand for secure communication in embedded systems, particularly in the context of the Internet of Things (IoT), necessitates cryptographic implementations that are both efficient and resilient. Field-Programmable Gate Arrays (FPGAs) have emerged as an ideal platform for deploying lightweight cryptographic algorithms due to their reconfigurability, parallelism, and suitability for low-power designs. This chapter presents a comprehensive exploration of FPGA-based implementations of secure cryptographic primitives tailored for embedded applications. Emphasis is placed on the design, optimization, and benchmarking of both symmetric and asymmetric algorithms, focusing on reducing hardware footprint, minimizing power consumption, and maximizing throughput without compromising cryptographic strength. The discussion includes resource-sharing methodologies, memory footprint reduction techniques, and power-performance balancing strategies essential for real-world deployment. The chapter highlights side-channel resistance and hardware Trojan mitigation mechanisms to ensure system trustworthiness. Practical case studies demonstrate the application of these cryptographic solutions in secure communication for IoT nodes, wearable devices, and automotive systems. Evaluation frameworks encompassing throughput, latency, energy efficiency, and resistance to physical attacks are employed to benchmark performance across various use cases. Through architectural innovations and optimization practices, the presented FPGA designs offer a secure and scalable foundation for next-generation embedded systems. This work contributes to the advancement of secure hardware design by aligning cryptographic strength with resource-constrained requirements of edge devices. It bridges the gap between theoretical cryptographic constructs and their practical hardware realization, facilitating trustworthy and efficient embedded security.

Keywords: FPGA implementation, lightweight cryptography, embedded systems, secure communication, IoT security, hardware optimization.

Introduction

The increasing integration of embedded systems across critical domains such as healthcare, smart infrastructure, autonomous transportation, and industrial IoT has amplified the necessity for secure and efficient data communication [1]. These systems often operate in environments with severe limitations on processing capability, energy availability, and physical space [2]. Under such

constraints, traditional cryptographic techniques—while functionally robust—are frequently unsuitable due to their substantial hardware and computational overhead [3]. The demand for adaptable, low-power, and lightweight cryptographic solutions has thus become a significant focus in hardware security research [4]. Field-Programmable Gate Arrays (FPGAs) have emerged as a practical hardware platform to address these challenges, offering reconfigurability, low latency, and optimized parallel execution for algorithm acceleration [5].

FPGAs enable the customization of logic to match the requirements of specific cryptographic algorithms [6]. Facilitating efficient implementation of primitives like block ciphers, stream ciphers, and hash functions in resource-constrained environments [7]. Their support for fine-grained hardware control, combined with the ability to implement pipelined and parallel architectures, offers considerable performance benefits compared to software-based solutions on microcontrollers or CPUs [8]. For embedded applications, particularly those with strict timing and energy demands [9]. The configurability of FPGAs provides an ideal balance between flexibility and performance, hardware implementation allows for isolation of security functions from general-purpose computing, enhancing the system's resistance to software-level threats and unauthorized access [10].