RADemics

Foundations of Lightweight Cryptography for Resource Constrained IoT Devices

Venkata Lakshmi Narayana Gorle, D. Padmapriya
ADITYA INSTITUTE OF TECHNOLOGY AND MANAGEMENT,
ERODE SENGUNTHAR ENGINEERING COLLEGE

Foundations of Lightweight Cryptography for Resource Constrained IoT Devices

[1]Venkata Lakshmi Narayana Gorle, Department of IT, Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India. gvlnarayana.it@adityatekkali.edu.in

[2]D. Padmapriya, Assistant Professor, Department of Information Technology, Erode Sengunthar Engineering College, Thudupathi, Perundurai, Erode, Tamil Nadu, India. dpadmapriya1982@gmail.com

Abstract

The exponential growth of Internet of Things (IoT) deployments in resource-constrained environments has necessitated the development of secure and efficient cryptographic mechanisms tailored for limited computational, memory, and energy capacities. This book chapter provides a comprehensive exploration into the foundations of lightweight cryptography with a focus on its applicability to constrained IoT devices. It examines the design and evaluation of lightweight block ciphers, stream ciphers, hash functions, authenticated encryption with associated data (AEAD), and public key cryptographic algorithms, emphasizing their resilience against advanced cryptanalytic techniques including differential, linear, and algebraic attacks. Implementation challenges such as key size, energy footprint, computation time, and resistance to side-channel and replay attacks are critically analyzed to highlight the trade-offs between performance and security. The chapter addresses current research gaps, emerging standards, and future directions in the domain of low-power cryptographic systems, aiming to guide both theoretical advancements and practical implementations.

Keywords: Lightweight Cryptography, IoT Security, Authenticated Encryption, Stream Ciphers, Public Key Algorithms, Cryptanalysis

Introduction

The rapid expansion of the Internet of Things (IoT) ecosystem has introduced an era of pervasive connectivity, where billions of devices interact and exchange information across diverse domains, including healthcare, smart cities, agriculture, and industrial automation [1]. These devices often operate in environments characterized by limited computational capabilities, minimal memory resources, and strict energy constraints [2]. Traditional cryptographic algorithms, designed for powerful computing platforms, are unsuitable for direct deployment in such constrained settings [3]. As a result, the field of lightweight cryptography has emerged as a vital research area focused on developing security solutions that meet stringent resource limitations without compromising cryptographic strength [4]. The need for such tailored cryptographic primitives arises from the increasing exposure of IoT nodes to adversarial threats, where both passive and active attacks can compromise data confidentiality, integrity, and authenticity [5].

Lightweight cryptography encompasses a variety of primitives, including block ciphers, stream ciphers, hash functions, and public key algorithms, which are designed with minimal hardware

and energy footprints [6]. These primitives are essential in implementing core security services such as secure communication, mutual authentication, digital signatures, and firmware verification [7]. The challenge lies in balancing the competing requirements of compact implementation and robust security, especially when addressing attacks that exploit either algorithmic weaknesses or physical leakage [8], with the emergence of next-generation applications that demand real-time data processing and zero-latency communication, cryptographic designs must also adhere to performance expectations [9]. Thus, the development of lightweight cryptographic schemes was not merely a process of reducing resource usage but involves fundamental innovation in algorithm design, evaluation metrics, and implementation strategies [10].