RADemics

Lightweight Public Key Cryptography for Authentication in IoT Environments

J. Jayaganesh, Bramah Hazela
GOVERNMENT ARTS AND SCIENCE COLLEGE, AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY

Lightweight Public Key Cryptography for Authentication in IoT Environments

[1]J. Jayaganesh, Assistant Professor, P. G. Department of Computer Science, Government Arts and Science College, Perumbakkam, Chennai, Tamil Nadu, India. everjays@gmail.com

[2]Bramah Hazela, Assistant Professor, Department of Computer Science and Engineering, Amity School of Engineering and Technology, Lucknow, Amity University Uttar Pradesh. bramahhazela77@gmail.com

Abstract

The rapid expansion of the Internet of Things (IoT) ecosystem has elevated the demand for secure, efficient, and scalable authentication mechanisms tailored for resource-constrained environments. Traditional public key cryptographic approaches are ill-suited for embedded platforms due to their high computational and energy overhead. This chapter investigates the integration of lightweight elliptic curve cryptography (ECC) into IoT authentication protocols, emphasizing software and hardware-level optimizations, platform-specific implementations, and protocol-level adaptations. A comparative analysis of ECC performance across embedded operating systems such as Contiki-NG and RIOT-OS reveals the importance of instruction-level tuning, memory hierarchy exploitation, and compiler-aware techniques. The role of crypto-coprocessors in reducing latency was critically examined, alongside the trade-offs between hardware acceleration and software portability, the implementation of ECC in lightweight protocols such as CoAP, DTLS, and 6LoWPAN was explored to demonstrate practical applicability in real-world IoT scenarios. By addressing key limitations in energy consumption, latency, and security resilience, this chapter establishes ECC as a viable foundation for next-generation lightweight authentication in embedded IoT systems.

Keywords: Lightweight Cryptography, Elliptic Curve Cryptography, IoT Authentication, Embedded Systems, Crypto-Coprocessors, Secure Protocols

Introduction

The exponential growth of the Internet of Things (IoT) has introduced a complex ecosystem comprising billions of interconnected devices deployed across heterogeneous environments [1]. These devices, often characterized by limited power, memory, and computational capabilities, are responsible for gathering, transmitting, and processing sensitive data [2]. The fundamental requirement for establishing secure communication in such an environment lies in robust authentication mechanisms that prevent unauthorized access and ensure data integrity [3]. Yet, traditional public key cryptographic algorithms such as RSA and DSA demand significant computational resources and large key sizes, making them inefficient for use in embedded platforms where energy and processing time are critical constraints [4]. As the IoT landscape continues to expand, there arises an urgent need for cryptographic solutions that provide high security while maintaining computational and energy efficiency suitable for low-power microcontrollers and sensor nodes [5].

Elliptic Curve Cryptography (ECC) has emerged as a preferred alternative due to its ability to provide equivalent levels of security with significantly smaller key sizes compared to traditional schemes [6]. ECC offers compactness, reduced computation time, and lower power consumption, rendering it highly suitable for IoT applications [7]. The mathematical structure of elliptic curves enables secure key exchange, digital signatures, and encryption with minimal overhead, aligning well with the operational limitations of embedded systems [8]. Recent advancements in lightweight ECC implementations have made it possible to integrate ECC-based authentication into microcontroller units (MCUs) without sacrificing responsiveness or battery life [9]. These characteristics are critical in applications such as smart metering, industrial control, health monitoring, and environmental sensing, where energy-efficient security was paramount [10].