RADemics

Elliptic Curve Cryptography and Its Suitability for Energy Efficient IoT Devices

Bhimanand Pandurang Gajbhare,
L. Mohana Kannan
VAIDYANATH COLLEGE, ERODE SENGUNTHAR ENGINEERING COLLEGE

Elliptic Curve Cryptography and Its Suitability for Energy Efficient IoT Devices

[1]Bhimanand Pandurang Gajbhare, Associate Professor, Department of Mathematics, J.E.S., Vaidyanath College, Parli-Vaijnath, Dist. Beed, Maharashtra, India. bpgajbhare@gmail.com

[2]L. Mohana Kannan, Associate professor, Department of Biomedical Engineering, Erode Sengunthar Engineering College, Thudupathi, Erode, Tamil Nadu, India. mohancalls2000@gmail.com

Abstract

Elliptic Curve Cryptography (ECC) has emerged as a dominant paradigm for public key security in resource-constrained Internet of Things (IoT) environments due to its ability to offer high levels of cryptographic strength with significantly shorter key lengths. The increasing deployment of intermittently powered devices, such as energy-harvesting sensor nodes and ultra-low-power microcontrollers, demands authentication mechanisms that remain robust under frequent power interruptions and constrained computational budgets. This chapter explores lightweight ECC-based authentication protocols tailored specifically for such devices, emphasizing resilience, efficiency, and secure state management. A detailed investigation was conducted into algorithmic, architectural, and system-level optimizations that enable ECC operations to tolerate partial execution and recover from abrupt energy loss. Attention was given to challenges in session continuity, cryptographic checkpointing, and the integration of ECC into lightweight protocols like DTLS, CoAP, and 6LoWPAN. Benchmarks on real-world intermittent platforms validate the feasibility of secure ECC deployment in low-energy scenarios. The chapter establishes design principles that bridge theoretical cryptographic constructs with practical constraints of next-generation IoT systems.

Keywords: Elliptic Curve Cryptography, Intermittent Computing, Energy Harvesting, Lightweight Authentication, IoT Security, Cryptographic Optimization

Introduction

The rapid expansion of the Internet of Things (IoT) has introduced a diverse range of connected devices, many of which operate under extreme resource limitations [1]. Among these, battery-powered and intermittently powered nodes—such as those found in energy-harvesting systems—present a unique set of design and security challenges [2]. These devices often function under highly constrained conditions, with limited computational power, memory, and inconsistent power availability [3]. Public key cryptography, though critical for authentication and secure communication, was traditionally resource-intensive and difficult to execute reliably in such environments [4]. Elliptic Curve Cryptography (ECC), with its minimal key sizes and reduced computational overhead, has emerged as a promising alternative to traditional public key methods, particularly in settings where power and energy consumption are paramount concerns [5].

ECC offers equivalent security to RSA and other traditional public key schemes at a fraction of the key length, leading to faster computations and reduced memory usage [6]. This efficiency makes ECC well-suited for integration into constrained IoT nodes [7]. The successful deployment of ECC in intermittently powered systems demands more than algorithmic efficiency [8]. Devices powered by ambient sources—such as solar, RF, or kinetic energy—often experience brownouts and energy depletion, which interrupt cryptographic operations mid-execution. In such contexts, standard implementations of ECC protocols may fail or yield inconsistent results [9]. Ensuring secure and efficient ECC authentication under these conditions necessitates new protocol designs and computational models that can tolerate power interruptions and resume operations without compromising security [10].