RADemics

Design and Evaluation of Stream Ciphers in Battery Powered IoT Sensors

Yallapu Srinivas, Akash Dey
VISHNU INSTITUTE OF TECHNOLOGY, MALLA REDDY COLLEGE OF ENGINEERING

Design and Evaluation of Stream Ciphers in Battery Powered IoT Sensors

[1]Yallapu Srinivas, Department of ECE, Vishnu Institute of Technology, Vishnu Puram, Bhimavaram, West Godavari District, Andhra Pradesh, India. srinivas.yallapu@vishnu.edu.in

[2]Akash Dey, Assistant Professor, Department of CSE-Data Science, Malla Reddy College of Engineering, Secunderabad, Telangana, India. Deyakash.Mrce@Gmail.Com

Abstract

The rapid expansion of the Internet of Things (IoT) ecosystem has intensified the demand for secure and energy-efficient cryptographic solutions tailored for constrained environments such as battery-powered and intermittently powered sensor nodes. This chapter presents a comprehensive study on the design and evaluation of lightweight stream ciphers specifically suited for resource-limited IoT hardware. Emphasis was placed on the algorithmic foundations, nonlinear function integration, and Boolean combining techniques that enhance cryptographic resilience while maintaining low implementation overhead. Security properties are rigorously assessed through comparative analyses of cryptanalytic resistance and performance metrics across multiple cipher architectures, including Grain, Trivium, and Mickey. The chapter further explores the operational behavior of these ciphers under duty-cycled and energy-harvesting conditions, highlighting their compatibility with embedded microcontrollers and intermittent power models. Integration strategies for secure communication protocols are discussed, with particular focus on minimizing latency, preserving state, and ensuring cipher synchronization in highly dynamic energy environments. The findings provide crucial insights into selecting and optimizing stream ciphers that strike a balance between robustness, efficiency, and practical deployment feasibility within modern IoT infrastructures.

Keywords: Lightweight cryptography, Stream cipher, Energy harvesting, IoT security, Embedded systems, Cryptanalysis resistance.

Introduction

The proliferation of the Internet of Things (IoT) has triggered a paradigm shift in how digital systems interact with the physical world [1]. Devices equipped with sensing, computing, and communication capabilities are increasingly deployed in environments characterized by severe limitations in power, memory, and processing capacity [2]. These constraints are particularly pronounced in battery-operated or energy-harvesting nodes, which are expected to perform critical functions over long periods with minimal energy input. In such conditions, the need for reliable and lightweight security mechanisms becomes imperative [3]. Cryptographic operations—essential for ensuring data confidentiality, integrity, and authenticity—must be executed with minimal computational overhead, making lightweight cryptography an essential component of secure IoT system design [4]. Among the various categories of lightweight cryptographic primitives, stream ciphers stand out due to their bitwise encryption process, low latency, and efficiency in resource-constrained environments [5].

Stream ciphers are especially suited for applications requiring real-time encryption of continuous data streams, such as telemetry from IoT sensors or control signals in industrial systems [6]. These ciphers operate by generating a keystream that was combined with plaintext to produce ciphertext, typically using simple bitwise operations like XOR [7]. This characteristic reduces the need for large memory buffers and complex arithmetic operations, thereby enabling implementation on ultra-low-power microcontrollers. Stream ciphers also offer synchronization capabilities that are crucial for maintaining secure sessions across devices subject to intermittent connectivity or power disruptions [8]. The choice of a suitable stream cipher must consider not only the cipher's theoretical security but also its performance when deployed on actual hardware [9]. A balance between cryptographic strength and implementation feasibility was essential to ensure that security mechanisms do not become a bottleneck in system performance or battery life [10].