RADemics

# Symmetric Key Cryptographic Primitives for Low Power IoT Architectures

J. Uthayakumar, R. Navaneetha Krishnan
HINDUSTHAN INSTITUTE OF TECHNOLOGY, VAILANKANNI
MATHA ARTS AND SCIENCE COLLEGE

# Symmetric Key Cryptographic Primitives for Low Power IoT Architectures

[1]J. Uthayakumar, Assistant Professor, Department of Computer Science and Engineering, Hindusthan Institute of Technology, Othakkalmandapam, Coimbatore. Uthayakumar.j@hit.edu.in

[2]R. Navaneetha Krishnan, Assistant professor, Head of the Department of Information technology & Artificial intelligence & Machine Learning, Vailankanni Matha Arts and Science College, Nagapattinam, Tamil Nadu, India. msgtokrishnan@gmail.com

## Abstract

The rapid expansion of low-power Internet of Things (IoT) ecosystems has elevated the significance of lightweight cryptographic mechanisms tailored for constrained sensor nodes. Among these, stream ciphers offer distinct advantages by delivering real-time data confidentiality with minimal energy, memory, and processing requirements. This chapter explores the architectural principles, design constraints, and performance benchmarks associated with stream cipher integration in battery-powered IoT devices. Emphasis was placed on evaluating cryptographic primitives such as Trivium, Grain, and Sprout through empirical metrics including energy per bit, gate count, latency, and hardware footprint. Security analysis considers resistance to key-stream attacks and statistical randomness under adversarial conditions. Case-based implementation scenarios are analyzed using contemporary microcontrollers and FPGA platforms to highlight trade-offs between security assurance and power efficiency. The discussion further aligns cipher selection with application-specific requirements in sectors such as healthcare, agriculture, and smart infrastructure. The findings contribute toward optimizing cryptographic design for pervasive, resource-sensitive environments.

**Keywords**: Stream Cipher, IoT Security, Lightweight Cryptography, Energy Efficiency, Embedded Systems, Battery-Powered Sensors

## Introduction

The acceleration of Internet of Things (IoT) deployments in various domains such as environmental monitoring, smart healthcare, precision agriculture, and industrial automation has intensified the demand for reliable and energy-efficient security mechanisms [1]. As the majority of IoT devices are battery-powered and constrained by limited computational, memory, and energy resources, traditional cryptographic algorithms prove unsuitable for integration in these systems [2]. Within this context, stream ciphers have gained prominence due to their lightweight structure and capability to perform real-time encryption with minimal resource consumption [3]. These ciphers provide confidentiality by generating a pseudorandom keystream, which was combined with plaintext data at the bit or byte level, enabling fast and efficient data processing [4]. The ability to operate in synchronous or self-synchronizing modes allows stream ciphers to support a wide range of IoT applications with different performance and security requirements. The necessity to design and evaluate cryptographic mechanisms that align with the unique limitations of low-power IoT sensors underscores the central motivation for this study [5].

Stream ciphers are particularly advantageous for resource-constrained devices due to their inherently simple architecture, often comprising shift registers and basic combinatorial logic [6]. Unlike block ciphers, which rely on extensive substitution-permutation networks and multiple rounds of transformation, stream ciphers can achieve comparable levels of security with significantly lower implementation overhead [7]. In many IoT sensor platforms, energy availability was tightly coupled with device longevity, and thus, every computation must be optimized for minimal power draw. Stream ciphers such as Trivium, Grain, and Sprout are specifically engineered to address this challenge, offering a trade-off between cryptographic strength and hardware simplicity [8]. These algorithms are designed to require fewer logic gates, reduced memory access, and lower initialization time, which together contribute to their suitability in energy-sensitive contexts [9]. Selecting the appropriate cipher for a given application demands careful analysis of system-level requirements, expected data rates, key management protocols, and attack resilience. Hence, evaluating these ciphers in realistic deployment scenarios was essential for informed adoption [10].