IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Low-Power Iot Devices With Lightweight Encryption Algorithms

Ms. R. Sneha
Assistant Professor
Department of computer science
Sri Ramakrishna College of Arts and Science for Women, Coimbatore, India

Abstract **—**The need for safe yet energy-efficient cryptographic techniques has grown due to the Internet of Things (IoT) rapid adoption in smart homes, healthcare, industrial automation, precision agriculture, and intelligent transportation. Strong security is provided by traditional encryption algorithms like AES, RSA, and ECC, but their high computational load, memory consumption, and latency limit their use in ultra-low-power Internet of Things nodes. Optimized algorithms designed for devices with stringent limitations, such as low-frequency microcontrollers, limited RAM/ROM, and battery-operated or harvested-energy designs, are presented by Lightweight Cryptography (LWC). This study offers a thorough analysis of stream ciphers like Trivium and lightweight block ciphers like SIMON, SPECK, PRESENT, and CLEFIA, examining performance aspects like memory footprint, execution time, power consumption, and resistance to cryptanalytic attacks. An evaluation platform based on a Cortex-M0 microcontroller was used to evaluate the energy consumption of a microcontroller during encryption operations. SPECK exhibited the highest efficiency in using software to encrypt data, PRESENT had the lowest number of gate counts on the hardware side, and CLEFIA provided the highest security level. The data demonstrated that lightweight encryption is much more efficient in extending battery life and therefore can support scalable and secure IoT applications.

Keywords: *- IoT Security, PRESENT Cipher, SIMON, SPECK, CLEFIA*

1. INTRODUCTION

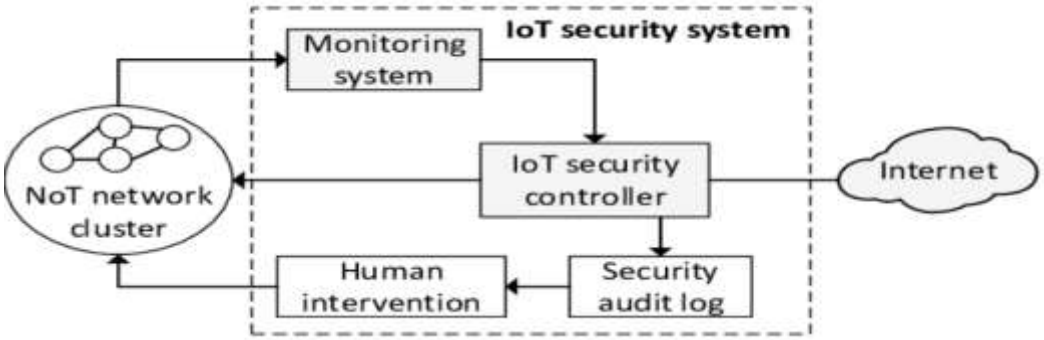
Miniaturized IoT devices (e.g., wearable, implants, smart meters, industrial sensors) are rapidly emerging as a means for new types of personal, medical, home automation, and industrial applications. However, as most of these devices will be powered by very low-power microcontroller chips (16-48 MHz), it is currently not possible to use very complex cryptographic algorithms (e.g., AES, RSA, ECDSA) on them efficiently, as they would not have enough RAM (8-64k), nor battery life to function effectively. In addition, as all of these devices communicate using different communication technologies (e.g., BLE, ZigBee, LoRa), the amount of bandwidth available for each type of device is limited, which restricts the feasibility of implementing complex security protocols.

The common approaches of modern cryptography fall short for the requirements of IoT devices which are low-cost, real-time, and low-power. To meet these requirements, the research community has created a family of Lightweight Encryption Algorithms (LWAs) specifically designed for use in constrained environments. The major goals of these algorithms are to provide an adequate level of security while optimizing hardware implementations (e.g., minimizing gate counts, computational requirements, and memory requirements) through the use of modern cryptography techniques. Examples of lightweight encryption algorithms include PRESENT, SPECK, and SIMON block ciphers developed to minimize the logical (hardware) complexity required to implement them, and Grain and Trivium stream ciphers designed for ultra-low-power operations. This study analyzes the lightweight encryption algorithms based on energy consumption, processing time, memory usage, and resistance to attacks by contemporary cryptanalysis techniques. This work demonstrates that by carefully choosing a lightweight

encryption algorithm, an IoT network's ability to securely, scalable, and reliably operate can be greatly improved. Therefore, LWEs will become a key component in the next-generation of secure embedded systems.

2. ARCHITECTURE OF IOT SECURITY SYSTEM

An effective Internet of Things (IoT) security solution contains a multi-layered system for sensing, computing, transmitting, and protecting data collected via multiple constrained devices. The multiple layers provide unique security solutions with optimal efficiency. The use of lightweight cryptography (LWC) supports the success of many Internet of Things (IoT) applications in resource-constrained environments, including support of wireless sensor networks, wearables, RFID systems, and Industrial IoT devices.



(Fig.1. IOT Security system)

2.1 IoT Sensing Layer

Low-power sensors are in the Internet of Things (IoT) Sensing Layer that serves as the foundational layer of the IoT Architecture. Temperature, humidity, motion, positioning, pressure, and biometric sensors operate on micro to milli-watt power budgets (1.8V – 3.3V) to increase the lifespan of a battery. As a result, these sensor modules are programmed to switch between three active states: sleep, and deep sleep while they continue monitoring and gathering data about the environment. In addition to collecting data from the environment, the sensors may perform minimal amounts of pre-processing on the data they collect, such as removing any noise or clutter that may interfere with the data collected by the other sensors. Thus, pre-processing helps to reduce the computational and bandwidth requirements of collecting and transmitting data. With regards to security, this layer is very susceptible to security attacks since sensor measurements are recorded in an unencrypted format prior to encryption. As such, if there is no delay between the recording of the unencrypted data and its encryption, an intruder may spoof or impersonate a sensor recording or transmit a false sensor measurement. Thus, the prompt enforcement of security controls on this layer is vital for maintaining the correctness and completeness of sensor data.

2.2 Encryption Layer

IoT Device Security's Encryption Layer: Its Role in IoT Device Security's Long-Term Stamina [The Definition of IoT Device Security's Encryption Layer] "IoT Device Security's Encryption Layer is the first line of defense against any type of intrusions. It will also provide instant notifications to let you know immediately and often about the most recently detected intrusion." The Encryption Layer will provide complete confidentiality, integrity and authenticity for data transferred between the Internet of Things (IoT) devices, their Cloud Servers and Server Endpoints. It will accomplish this by utilizing lightweight Cryptographic implementations that have been optimized specifically for resource-constrained Microcontrollers (MCUs) including the ARM Cortex-M0 / M3, ESP8266, MSP430 and AVR environments. Lightweight encryption implementations are limited in available resources; to ensure that IoT devices have strong encryption implementations, they are using Lightweight Block/Stream Ciphers like PRESENT, SIMON/SPECK, GIFT, Ascon (NIST LWC Standard), Grain, and Trivium. In addition to encrypting the data, the Encryption Layer is responsible for securely managing The Keys (Secure Key Management) - the secure key will be created and stored securely inside the MCU, while short-lived session keys are to be created on demand as needed, nonce numbers for freshness on AEAD operations; finally, they will also provide high-quality random numbers via TRNG or PRNG. Message

Authentication Codes (MACs) will be generated in an IoT Device before sending any data up to Higher Layers, and any Payloads will be encrypted, and they will have automatically generated timestamp(s) or nonce(s) attached with them to protect against Replay attacks. As Encryption Operations represent a significant percentage of an IoT Device's Energy Draw, this Layer has a direct influence on battery life, communication security, and resistance to physical attacks; ultimately, the Layer dictates the overall longevity and stamina of an IoT Device.

2.3 Gateway Layer

The gateway layer ultimately connects the low-power sensor networks to the robust cloud networks undertaken by building relationships through use of lightweight Internet of Things (IoT) communication protocols; for small publish/subscribe messages the Gateway Layer would use MQTT, for creating REST-type operations on Constrained Networks the gateway would use CoAP and for More Capability Gateways would use HTTP/HTTPS. The Gateway Layer aggregates/buffers the data gathered through receipt of encrypted messages from Many Nodes, it locally stores encrypted messages, it filters all the non-specific information out of the encrypted package, it balances the network's overall load and schedules the transmissions in an efficient manner.

As the Trust Anchor for the overall Infrastructure of the IoT, the Gateway Layer authenticates the message authentication codes/digital signatures in addition to authenticating other forms of access control of all Connected Nodes of the Network, routes authenticated packets to the proper Cloud Servers and has network level Intrusion Detection to detect uncharacteristic activities. The Gateway Layer would likely run Lightweight Middleware between each of the differing Communication Technologies (Bluetooth/WiFi) to ensure Cross Protocol Inter-operability and compatibility. The Gateway Layer Serves to protect against potential Node Impersonation/Packets Tampering/Packets Flood; thus Gateway Layer is an essential to ensuring Secure/Reliable IoT Communication.

2.4 Cloud/Server Layer

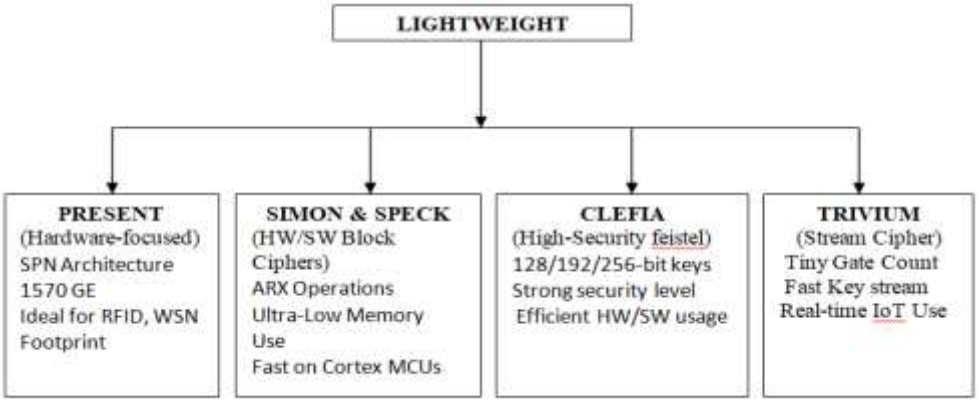
The cloud/server layer serves as the highest level of the IoT ecosystem, with output-based computation and security at the central point. The cloud layer processes advanced analytical functions through Artificial Intelligence (AI) and Machine Learning (ML) for predictive analysis, detection of anomalies, fault diagnosis, and modelling of behaviour so that malicious activities/users can be detected early and therefore prevent system failure(s). In addition, this layer provides a secure long-term storage environment for encrypted device operation and log files in addition to operation files, with privacy and integrity protection in place to keep the devices and their users secure.

3. METHODS AND ALGORITHMS FOR LIGHTWEIGHT ENCRYPTION

Lightweight Encryption Algorithms are discussed in this section, including their corresponding methodologies for how these algorithms were evaluated within a constrained IoT environment.

3.1 Lightweight Encryption Algorithm Overview

The primary design goal of Lightweight Cryptography (LWC) is to provide an acceptable level of security from various threats while ensuring that the amount of computation required executing the algorithm is minimized. Therefore, lightweight encryption methods are considered to be ideally suited for Internet of Things (IoT) devices where resources such as battery power, memory, and processing speed are often minimal. In determining the lightweight encryption techniques to highlight in this document, several factors were considered: The level of usage within the cryptographic community, the overall degree to which these methods are considered secure by independent organizations evaluating the methods, the type of hardware and/or software needed to support the techniques, and the general applicability of the techniques for embedded systems.



(Fig.2. Methods and Algorithms for Lightweight Encryption)

3.1.1. PRESENT

PRESENT is a small and lightweight 64-bit block cipher that has an 80-bit and 128-bit key option. It was developed as a compact substitution-permutation network (SPN) with a very small hardware footprint of approximately 1570 GE. The design of PRESENT provides strong resistance against combination and differentially cryptanalysis while also having a very low operating power, making it suitable for extremely constrained environments like RFID or passive sensor systems and other ultra-low-power IoT nodes. Because of its compactness, efficiency and excellent level of security, PRESENT has become a benchmark for lightweight cryptographic standards for hardware-based applications.

3.1.2 SIMON & SPECK

The SIMON & SPECK families of lightweight block ciphers were created by the NSA with design goals focused on providing high performance in environments where there isn't much room for additional circuitry; specifically, SIMON was developed to take advantage of hardware implementations using a Feistel-oriented architecture for its low gate count, high energy efficiency and predictable timing characteristics with an emphasis on FPGA/ASIC use; whereas SPECK is primarily oriented toward providing high performance within software environments using ARX configuration; resulting in excellent performance on ARM Cortex microcontrollers with little RAM Used and reduced code size. When compared to the Advanced Encryption Standard (AES), both SIMON and SPECK outperform AES regarding speed, energy consumption and memory utilization on MCUs that are considered constrained by the above criteria, therefore providing strong and effective alternatives to ensure device security across modern lightweight IoT platforms.

3.1.3 CLEFIA

Sony introduced CLEFIA, a block cipher with 128 bits in terms of its key sizes, and four branches in a Feistel Network design, creating high levels of security for all supported sizes (128, 192, and 256 bit). CLEFIA also provides good performance in both hardware and software implementations; this functionality means it will fit into many types of products found throughout the Internet-of-Things (IoTs), multimedia devices, and various applications that need high levels of security along with some limited resource usage.

3.1.4 Trivium (Stream Cipher)

Trivium is a stream cipher that has an extremely small footprint on the hardware, providing a very small gate count, as well as a very fast keystream generation capability. This combination makes Trivium particularly effective for use in real-time encryption applications including medical devices, wearable sensors, IoT systems with low-latencies, and so forth. As an alternative to block ciphers, Trivium provides an efficient solution by offering solutions for continuous data streams and/or extremely rapid encryption at the bit level.

3.2 METHODOLOGY

The evaluation methodology concentrates on analyzing the computational efficiency, energy consumption, and security resilience of the selected cryptographic algorithms under realistic IoT hardware constraints. The study includes the implementation and comparison of PRESENT, SIMON, SPECK, CLEFIA, and Trivium (used as the stream cipher reference), while AES-128 is employed as the baseline standard for performance comparison.

3.2.1 Hardware Platform

The performance and efficiency of the chosen algorithms were evaluated by conducting tests with an appropriate representation of an IoT device. The IoT device utilized an ARM Cortex-M0 microcontroller, operating at 48 MHz, with 32 KB RAM and 256 KB flash memory. The device was powered by a 500 mAh Lithium-Ion battery and had support for both BLE and LoRa communications. The hardware specifications are comparable to many sensor node, wearable technology devices, and other IoT applications in agricultural use, as well as embedded control units, thus providing a good environment to evaluate how well each algorithm performs in these types of low-power and low-memory constrained situations.

3.2.2 Performance Metrics

Multiple numbers were gathered to assess the effectiveness of each of the algorithms assessed in this project. The quantitative measures collected included two specific times (in milliseconds) amount of CPU processing done to complete an encryption operation, the energy consumed for each encryption, which was expressed in millijoules, as well as the total number of bytes taken by the source code, including both ROM and RAM usage. Additionally, an evaluation of the security margins for each algorithm against cryptanalysis was performed. Lastly power consumption was calculated at the time of encryption from the current drawn during encryption. All these numbers provided a complete assessment of the performance of the assessed algorithms including speed, power efficiency, memory requirements and security robustness.

3.2.3 Testing Method

The various algorithms were built using the C programming language, with development and execution taking place on an ARM processor using the ARM GCC Toolchain. At the same time, to properly measure how much energy is being used during encryption, we used a digital power analyzer to get real-time measurements of the current consumption while encrypting data. Each of the tested algorithms was executed with a total of 10,000 encryption cycles in order to provide consistent data measurements and reduce measurement errors. Finally, the results were compared to the AES-128 cipher, which is a well-known example of a standard working cipher. For assuring reproducibility, all tests were repeated with the same conditions during multiple test runs.

4. REVIEW MODELS:

AUTHORS	PARAMETERS	CONTROLLER / PLATFORM	WORKING PRINCIPLE	LIMITATIONS
Bogdanov et al.	PRESENT block cipher, 64-bit block, 1570 GE	Hardware (ASIC/FPGA)	Designed an ultra-lightweight block cipher using simple S-boxes and bit permutations to reduce area and power consumption	Limited security margin compared to larger ciphers
Beaulieu et al.	SIMON & SPECK families, ARX operations	Embedded CPUs, microcontrollers	Proposed flexible lightweight ciphers optimized for hardware (SIMON) and software (SPECK) using rotations, XOR, and modular addition	Vulnerable to some cryptanalytic attacks under reduced rounds
NIST LWC Project	AEAD algorithms, hash functions, security evaluation metrics	FPGA, ASIC, IoT devices	Standardization project selecting LWC algorithms based on performance, area, side-channel resistance, and robustness	Long evaluation process; deployment still ongoing
Hardware Efficiency Studies	Energy comparison of AES vs LWC	ARM Cortex M0, M3, AVR MCUs	Experiments show LWC ciphers reduce energy by 40–70% due to fewer rounds and smaller state operations	Results vary by platform; not all LWC universal
Trivium & Grain Researchers	Stream ciphers <3000 GE	RFID, sensor nodes	Implemented lightweight stream ciphers using LFSR/NFSR for high-speed bit-stream generation in low-area designs	Not suitable for all authentication applications
IoT Security Survey Papers	IoT devices with weak/no encryption	Wireless sensor networks, smart devices	Identified rising attacks on IoT systems due to	Many IoT vendors still lack

			missing encryption, recommending LWC for constrained nodes	implementation awareness
RFID & WSN Research	PRESENT, SIMON, SPECK, Trivium	RFID tags, Wireless Sensor Networks	Showed LWC ciphers outperform AES in power, area, and latency for low-cost embedded systems	Reduced block sizes may weaken long-term security
Side-Channel Analysis Studies	Power/EM attacks, masking techniques	Microcontrollers, ASIC	Investigated side-channel leakage in LWC designs and proposed low-cost countermeasures	Countermeasures increase area and complexity
Emerging PQC-LWC Research	Post-quantum algorithms	Future IoT devices	Exploring quantum-resistant cryptography suitable for constrained domains	Most PQC algorithms are currently too heavy

5. CONCLUSION:

This paper indicates that lightweight cryptographic algorithms serve a crucial function to enhance security within the expanding usage of limited-resourced Internet of Things (IoT) ecosystems. Lightweight ciphers will continue to be necessary due to the power, memory, and computational capabilities of IoT devices being limited. Evaluations of the lightweight ciphers based on comparison indicate that SPECK offers an efficient means of performing ciphers in software and requires less processing power than other ciphers; whilst PRESENT offers an extremely compact solution for hardware-based platforms because of the requirements for minimum gate and power usage. CLEFIA has a high security margin and equal distribution of resources, so it is a viable solution for products requiring enhanced security and limited processing capability. From a broader perspective, each algorithm will not meet all the requirements for the deployment of IoT products; therefore, the choice of which algorithm to use should be informed by the operational and architectural requirements of the intended application, as well as security requirements. Presently, the future development of lightweight cryptography appears to have more sophisticated techniques available, including Artificial Intelligence (AI)-assisted detection of anomalies, lightweight post-quantum cryptographic designs that are resilient to future quantum attacks, scalable mechanisms for key distribution, and secure-boot architecture to provide a trusted environment for initial boot up of a device. Future developments in this area will be essential to solve the complex and changing cyber threats facing digital products used in the IoT.

REFERENCES:

[1] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” CHES, 2007.

[2] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, “The SIMON and SPECK Families of Lightweight Block Ciphers,” NSA Technical Report, 2013.

[3] Sony Corporation, “CLEFIA: A Lightweight 128-bit Block Cipher,” Sony Technical Report, 2007.

[4] NIST, “NIST Lightweight Cryptography Project,” National Institute of Standards and Technology, 2023.

[5] T. Eisenbarth, S. Kumar, C. Paar, “Lightweight Cryptography in Embedded Systems,” Springer, 2015.

[6] A. Poschmann, “Lightweight Cryptography for RFID and WSN,” IEEE Transactions on Circuits and Systems, 2010.

[7] M. Hell, T. Johansson, W. Meier, “Grain Stream Cipher,” Springer, 2005.
[8] C. De Cannière, B. Preneel, “Trivium Specification,” eSTREAM Project Report, 2006.
[9] “IoT Security Issues,” International Journal of Distributed Sensor Networks, 2022.
[10] “Energy-efficient Cryptography for Smart Devices,” IEEE Internet of Things Journal, 2021.
[11] “Survey on Lightweight Block Ciphers,” ACM Computing Surveys (CSUR), 2020.
[12] “Lightweight Authentication Models for IoT,” Springer IoT Security Journal, 2019.
[13] “IoT Security with Lightweight Approaches,” ICACCI Conference Proceedings, 2016.
[14] “Secure IoT Architecture Review,” Elsevier Future Generation Computer Systems, 2023.
[15] “Benchmarking Lightweight Encryption Algorithms,” MDPI Sensors Journal, 2022.
[16] Gartner, “IoT Low-Power Devices Trends,” Gartner Research Report, 2024.