CONESCAPANHONDURAS2025paper152.pdf

Institute of Electrical and Electronics Engineers (IEEE)

Document Details

Submission ID
trn:oid:::14348:477740482

Submission Date
Jul 31, 2025, 9:43 PM CST

Download Date
Aug 12, 2025, 6:35 PM CST

File Name
CONESCAPANHONDURAS2025paper152.pdf

File Size
125.2 KB

5 Pages

3,274 Words

20,406 Characters

16% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

34 Not Cited or Quoted 15%
Matches with neither in-text citation nor quotation marks

1 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

14% Internet sources
11% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **34** Not Cited or Quoted 15%
  Matches with neither in-text citation nor quotation marks
- **1** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

14% Internet sources
11% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	www.coursehero.com 2%
2	Publication	Arvind Mewada, Nagendra Singh, Mohd Aquib Ansari, Amrendra Singh Yadav. "A... 1%
3	Internet	hal.inria.fr <1%
4	Internet	www.researchgate.net <1%
5	Internet	arxiv.org <1%
6	Internet	developnsolve.com <1%
7	Internet	researchrepository.universityofgalway.ie <1%
8	Internet	docslib.org <1%
9	Publication	Luthfi Hakim Panuntun, Bety Hayat Susanti. "Evaluation of randomness hash-DR... <1%
10	Internet	eprint.iacr.org <1%

11 Internet
nebula.wsimg.com <1%

12 Internet
biblioteca.cunef.edu <1%

13 Internet
en.teknopedia.teknokrat.ac.id <1%

14 Publication
Keshav Kumar, Bishwajeet Kumar Pandey. "Next Generation Mechanisms for Dat... <1%

15 Internet
q-chem.authorea.com <1%

16 Internet
enveurope.springeropen.com <1%

17 Internet
backend.orbit.dtu.dk <1%

18 Internet
oa.upm.es <1%

19 Publication
Thomas Eisenbarth. "A Survey of Lightweight-Cryptography Implementations", IE... <1%

20 Internet
d-nb.info <1%

21 Publication
Qusay F. Hassan, Rehman Khan Atta ur, Sajjad A. Madani. "Internet of Things - Ch... <1%

22 Internet
dokumen.pub <1%

23 Internet
research-api.cbs.dk <1%

24 Internet
revistas.elpoli.edu.co <1%

25 Publication

Rafael de Jesus Martins, Vinicius Garcez Schaurich, Luis Augusto Dias Knob, Julian... <1%

26 Publication

Reem Abdul Rahman, Babar Shah. "Security analysis of IoT protocols: A focus in C... <1%

27 Internet

repositorioacademico.upc.edu.pe <1%

28 Internet

revistapublicando.org <1%

29 Internet

shura.shu.ac.uk <1%

Lightweight Cryptography Techniques for Low-Power IoT Devices

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—The exponential growth of the Internet of Things (IoT) has brought with it a series of challenges related to the security of data transmitted between limited-capacity devices. These devices, facing power, processing, and memory constraints, require optimized cryptographic solutions. Lightweight cryptography emerges as a viable alternative to traditional algorithms, allowing acceptable levels of security to be maintained without compromising operational efficiency. This review addresses the main lightweight cryptographic algorithms, their classification, standard evaluations and applications on low-power platforms, as well as current challenges and future trends.**

***Index Terms*—lightweight cryptography, IoT, security, embedded devices, energy efficiency.**

I. Introduction

[1] The Internet of Things (IoT) ecosystem has revolutionized the way devices interact in sectors such as healthcare, industry, home automation, and agriculture. This technology enables the connection of sensors, actuators, microcontrollers, and embedded systems through networks that collect and share data in real time, improving processes and quality of life. However, this massive connectivity also increases the attack surface, exposing IoT devices to a wide range of cyber threats.

Many of these devices operate in resource-constrained environments, such as low memory, low processing power, restricted energy capabilities, and low-bandwidth communication channels. These characteristics make it difficult to implement traditional security mechanisms such as RSA, AES, or SHA-2, which require significant computational resources.

In response to this challenge, lightweight cryptography has been specifically designed to operate efficiently in severely restricted contexts, providing confidentiality, integrity, and authentication without compromising system performance. This branch of cryptography seeks to achieve a balance between security robustness and operational efficiency, utilizing designs optimized for embedded hardware and software.

This document presents an updated technical review of lightweight cryptographic solutions, their applicability in IoT environments, relevant international standards, and current challenges in the field. Representative algorithms, their classifications, as well as their implementation on common platforms and their evaluation through benchmarking projects are analyzed.

II. Security in the IoT Ecosystem

A. Common Threats

[2]Some of the threats faced by IoT devices are:

- Data Interception: This occurs when attackers intervene in unencrypted communications, stealing credentials or sensitive information.
- Data Modification and Man-in-the-Middle Attacks: Unauthorized modification and insertion into device communications to alter data or impersonate services, common in poorly protected IoT networks.
- DDoS Attacks: Devices compromised with malware, such as Mirai, are integrated into botnets to saturate networks or services.
- Firmware Hijacking: This occurs when the firmware is replaced or modified to insert malicious code and take control of a device.
- Hardware Tampering: In these cases, there is direct intervention in a device's pins or sensors, affecting its operation without detection.

B. Case Studies

Some case studies of situations that have occurred in recent years are:

- Critical Infrastructure in Ukraine: [3]In 2015, there was an attack on energy systems using industrial IoT, causing massive blackouts in a region of Ukraine.
- Mirai Botnet: [4]In 2016, the Mirai malware hijacked thousands of IoT cameras and routers using default credentials, generating massive DDoS attacks against Dyn, Twitter, and Netflix.
- CloudPets Toys: [5]In 2017, a vulnerability in a database exposed children's voice messages, demonstrating the risk of sensitive data in the IoT.
- Connected insulin pump: [6]In 2019, the ability to remotely modify insulin doses was proven, highlighting the critical flaws in IoT medical devices.

III. Lightweight Cryptography

[7], [8]Lightweight cryptography is a branch of cryptography designed specifically for environments with severe resource constraints, such as Internet of Things (IoT) devices,

embedded systems, smart cards, and wireless sensors. Unlike conventional cryptographic algorithms, which require high processing power, memory, and energy, lightweight algorithms are optimized to operate efficiently in environments where these resources are limited. The design of lightweight cryptography seeks a balance between security, computational efficiency, and low energy consumption. These algorithms can be classified based on several criteria, one of the most common being their internal structure: algorithms based on block ciphers (such as PRESENT or LED), stream ciphers (such as Trivium), lightweight hash functions (such as SPONGENT), and authentication mechanisms. Another relevant classification distinguishes between general-purpose algorithms, which can be implemented in both hardware and software, and hardware- or software-specific algorithms, designed to maximize the execution environment. Furthermore, in recent years, organizations such as NIST have promoted initiatives such as the Lightweight Cryptography (LWC) project, aimed at standardizing lightweight algorithms that offer robust security in emerging contexts.

A. Main Lightweight Cryptographic Algorithms

Lightweight cryptographic algorithms are specifically designed to operate efficiently on resource-limited devices, such as those in the Internet of Things (IoT). These algorithms maintain acceptable levels of security while reducing energy, memory, bandwidth, and processing power usage. This section describes the most representative algorithms in block ciphers, stream ciphers, hash/MAC functions, and secure communication protocols.

1) Block Ciphers: These algorithms work on fixed blocks of data, typically 64 or 128 bits, and are widely used for secure storage and transfer of structured data.

TABLE I
BLOCK CIPHER ALGORITHMS IN LIGHTWEIGHT CRYPTOGRAPHY

Algorithm	Year	Block	Key	Advantages
PRESENT	2007	64-bit	80/128-bit	Extremely lightweight, good security
SIMON/ SPECK	2013	32-128-bit	Variable	High efficiency, good performance in hardware and software
HIGHT	2006	64-bit	128-bit	Low power, simple design
LED	2011	64-bit	64/128-bit	Strong security, compact
PRIDE	2014	64-bit	128-bit	Optimized for hardware, good resistance to linear attacks

Block cipher algorithms designed for resource-limited environments find application in a wide range of emerging technologies. Due to its extreme lightness and low power consumption, PRESENT is widely used in RFID tags and autonomous sensors, where energy efficiency is critical. SIMON and SPECK, due to their flexibility in block and key sizes, as well as their high hardware and software performance, are commonly used in Internet of Things (IoT) systems and embedded microcontrollers. HIGHT, with its simple design and low power requirements, is effectively integrated into general-purpose embedded devices. On the other hand, LEDs have proven to be a solid choice for smart cards thanks to their compactness and strong structural security. Finally, PRIDE is geared toward dedicated hardware implementations, such as application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs), where their resistance to linear attacks and efficiency in highly customized environments are valued.

2) Stream Ciphers: Stream ciphers process data sequentially, bit by bit or byte by byte, making them suitable for real-time data transmission such as voice or video.

TABLE II
STREAM CIPHER ALGORITHMS IN LIGHTWEIGHT CRYPTOGRAPHY

Algorithm	Year	Key Size	Internal State
Trivium	2005	80 bits	288 bits
Grain	2006	80/128 bits	160 bits
MICKEY	2006	80/128 bits	200 bits

Stream cipher algorithms designed for lightweight cryptography offer specific advantages that make them well-suited for highly constrained environments. Trivium stands out for its high computational efficiency and solid security level, making it a viable option for wireless networks where continuous encryption with low latency is required. Grain, on the other hand, exhibits low energy consumption and a simple structure, which facilitates its implementation in Internet of Things (IoT) devices that operate with low data rates and limited power supply. MICKEY provides robust performance under adverse conditions, showing good noise tolerance and operational stability, making it particularly useful in machine-to-machine (M2M) communication applications, where channels may be unstable or prone to interference.

3) Hash y MAC: They provide integrity and authentication. These functions are essential for validating messages and protecting against tampering.

TABLE III
LIGHTWEIGHT HASH FUNCTIONS IN CRYPTOGRAPHY

Algorithm	Year	Output Size	Security / Advantages
SPONGENT	2011	88–256 bits	80–128-bit security, suitable for resource-constrained devices
PHOTON	2011	80–256 bits	High security, good balance between size and efficiency
Quark	2010	112–160 bits	High computational efficiency, low energy consumption

Lightweight hash functions have been specifically designed for efficient implementation on resource-limited platforms, such as embedded systems and IoT devices. SPONGENT, based on the sponge construction, offers a highly lightweight

solution ideal for authentication mechanisms in IoT devices where basic security and minimal computational complexity are required. PHOTON provides a good balance between output size and cryptographic strength, making it suitable for short-range communication devices like NFC systems, where both efficiency and data integrity are priorities. Meanwhile, Quark stands out for being extremely compact and efficient, making it an excellent choice for use in sensors, RFID tags, and other passive devices operating under severe energy constraints.

4) Protocols and Suites: Adaptations of standard secure communication protocols (such as TLS) for constrained environments. These also include algorithms based on optimized elliptic curves

TABLE IV
LIGHTWEIGHT SECURITY PROTOCOLS FOR IOT

Protocol	Description	Advantages	Applications
Lightweight TLS	Optimized version of TLS for IoT	HTTPS compatibility, interoperability	Secure IoT communications
DTLS over CoAP	Secure UDP protocol for CoAP	Low latency, ideal for sensor networks	Smart Home, Smart Grid
Simplified ECC (Curve25519, Ed25519)	Optimized elliptic curve cryptography	High security with low computational load	Authentication, end-to-end encryption

IV. STANDARDS AND EVALUATIONS

Rigorous evaluation of lightweight cryptographic algorithms is essential to ensure their suitability in resource-constrained environments such as Internet of Things (IoT) devices. In response, international organizations such as ISO and NIST have developed standards and research initiatives to identify, analyze, and standardize efficient and secure cryptographic techniques for embedded platforms. Below are the most relevant regulatory frameworks and projects, as well as evaluation tools used in current research.

A. ISO/IEC 29192 Standard

[10]ISO/IEC 29192 is a series of international standards that define lightweight cryptographic algorithms designed specifically for devices with severe hardware limitations, such as sensors, smart cards, RFID tags, and low-power microcontrollers. This standard establishes minimum functional and security requirements to enable efficient implementations without compromising data integrity or confidentiality.

The standard consists of several parts:

These standards provide a framework for manufacturers and developers to evaluate the suitability of lightweight cryptographic algorithms for specific applications, promoting interoperability in heterogeneous IoT systems.

In response to increasing demand for secure solutions in constrained devices, the U.S. National Institute of Standards and Technology (NIST) launched the Lightweight Cryptography Project (LWC) in 2018 to develop a new cryptographic

TABLE V
PARTS OF A LIGHTWEIGHT CRYPTOGRAPHIC SPECIFICATION

Part	Content
Part 1	General requirements for lightweight cryptography
Part 2	Block ciphers (PRESENT, CLEFIA)
Part 3	Stream ciphers (Trivium, Grain)
Part 4	Lightweight MAC algorithms (LightMAC, reduced CMAC)
Part 5	Lightweight hash functions
Part 6	Lightweight pseudorandom number generators (PRNGs)

TABLE VI
SUMMARY OF ASCON ALGORITHMS

Algorithm	Type	Features
ASCON-128	AEAD (Authenticated Encryption with Associated Data)	Strong security, fast C implementation, low power consumption
ASCON-128a	AEAD	Faster software variant, suitable for higher-performance environments
ASCON-HASH / ASCON-XOF	Hash and extendable-output functions	Sponge-based, efficient for message authentication and hashing

standard suitable for environments such as medical wearables, RFID modules, industrial embedded systems, and wireless sensor networks.

The project involved a multi-round open competition that received 57 proposals worldwide. Throughout the evaluation, aspects such as security against known and emerging attacks, efficiency on embedded platforms, key/block/tag sizes, simplicity, implementation cost, and side-channel resistance were analyzed.

After five years of analysis, ASCON was selected in 2023 as the recommended standard for authenticated encryption and lightweight hash functions..

B. Selected Algorithms

[11]ASCON was selected for its optimal balance between security, performance, and flexibility, making it particularly suitable for low-power microcontrollers like ARM Cortex-M0/M3/M4. Its efficient design provides robust authenticated encryption, resistance to classical and emerging attacks, and protection against timing and power analysis side-channel threats.

C. Evaluation Tools and Academic Benchmarks

The evaluation of lightweight algorithms must go beyond theoretical metrics and include performance validation on real platforms. Academic projects have developed benchmarking environments to compare algorithm performance under different architectures, workloads, and execution conditions.

Typical evaluation criteria for lightweight cryptographic algorithms include code size (ROM) and memory usage (RAM),

TABLE VII
EVALUATION PLATFORMS FOR LIGHTWEIGHT CRYPTOGRAPHY

Platform	Description	Features
CryptoBench	Benchmarking platform for AEAD, MAC, and hash	Measures latency, memory usage, energy efficiency
FELICS	Framework for testing on real devices (AVR, ARM)	Provides comparable results for real IoT environments
TinyCrypt	Lightweight crypto library for embedded systems	Implements AES, SHA-256, ECDSA with small memory footprint
SUPERCOP	Benchmarking system for cryptographic algorithms	Compares speed, resource usage, and security
XKCP	Keccak Code Package repository	Supports sponge-type hash variants for constrained devices

the number of CPU cycles per encrypted or authenticated byte, operating speed (Mbps), energy efficiency (J/bit), resilience to side-channel attacks, and ease of secure implementation. These benchmarks allow algorithms to be selected not only based on their theoretical security but also on their practical viability in real-world scenarios such as wireless network nodes, cryptographic RFID tags, and wearable healthcare systems. Standards and evaluations are the cornerstone of developing reliable lightweight cryptographic solutions; the adoption of standards such as ISO/IEC 29192 and the standardization driven by NIST with ASCON provide confidence and direction to manufacturers and developers. Furthermore, platforms such as CryptoBench, FELICS, and TinyCrypt allow algorithm performance to be validated and compared under real-world conditions, which is key to their effective adoption in the IoT ecosystem.

V. APPLICATION ON LOW-POWER PLATFORMS

[14]Lightweight cryptography is primarily implemented on resource-constrained platforms that define the IoT ecosystem. These systems must balance efficiency, security, and power consumption. Popular microcontrollers include ESP32 (low power, built-in WiFi/Bluetooth), STM32 (industrial/medical), ATmega328 (Arduino-based), and Raspberry Pi Pico (RP2040, moderate-power prototyping).

Development is typically done in C or C++ for hardware-level control and low resource usage. Execution environments may be bare-metal or use lightweight OS like FreeRTOS. Design goals include minimizing CPU cycles and using sleep modes to extend battery life.

Libraries like TinyCrypt, WolfSSL, and mbedTLS support embedded cryptography with optimized TLS/DTLS protocols [13], [15], making them ideal for secure integration in IoT systems.

Use cases include health sensors using PRESENT for encrypted transmission, RFID tags using Trivium for fast authentication, industrial monitors using simplified ECC for TLS channels, and smart home devices running ASCON on ESP32 for authenticated encryption over WiFi.

VI. CURRENT CHALLENGES AND TRENDS IN LIGHTWEIGHT CRYPTOGRAPHY

Side-channel attacks represent a significant challenge in cryptographic security. Unlike traditional attacks, which seek to compromise the algorithm's mathematics, side-channel attacks exploit physical leaks, such as execution time or power consumption, to deduce sensitive information. For example, an attacker can measure how long a microcontroller takes to perform a cryptographic operation and, from this, infer the secret key. To mitigate these threats, modern implementations incorporate masking techniques and specialized hardware that limits such leaks.

The balance between security and power consumption is crucial in resource-constrained devices such as IoT sensors and wearables. Although security is a priority, the device's autonomy and processing power cannot be sacrificed. Lightweight cryptography offers a compromise, providing adequate protection with low power consumption. Algorithms such as PRESENT and SPECK are examples of solutions designed to run efficiently on tightly constrained chips.

The evolution of quantum computing is driving the transition to post-quantum cryptography. Classic algorithms such as RSA and ECC could be vulnerable to quantum attacks using Shor's algorithm. For this reason, new quantum-resistant algorithms, such as Kyber and Dilithium, are being developed and standardized and adopted by international organizations such as NIST to ensure the future security of cryptographic systems.

Finally, the integration of secure hardware accelerators and coprocessors, such as Trusted Platform Modules (TPMs) and Secure Enclaves, improves security by executing critical operations in isolated environments. For example, Windows uses TPM to encrypt disks with BitLocker and verify system integrity, while Apple devices use the Secure Enclave to protect biometric data such as Face ID and Touch ID, strengthening the physical and logical security of devices.

VII. CONCLUSIONS

Lightweight cryptography is presented as an indispensable solution for protecting the confidentiality, integrity, and authenticity of information in resource-constrained IoT devices. The challenges inherent in memory, processing, and power consumption constraints require algorithms that offer an optimal balance between robust security and operational efficiency.

The techniques and algorithms developed, such as ASCON, PRESENT, and Trivium, demonstrate that it is possible to implement ciphers and hash functions that meet security requirements without compromising device autonomy. Furthermore, standardization promoted by organizations such as NIST and evaluation platforms such as CryptoBench and FELICS are essential to ensuring interoperability and reliability in the IoT ecosystem.

Current challenges, including protection against side-channel attacks, balancing security and power consumption, and the transition to post-quantum cryptography, pave the way for future research and development. The integration of secure hardware and specialized coprocessors will also be key to enhancing security in embedded devices.

Ultimately, lightweight cryptography not only facilitates the implementation of security measures in IoT devices, but also drives widespread adoption of this technology in critical applications, ensuring data protection in an increasingly interconnected world dependent on embedded systems.

REFERENCES

[1] IBM, Internet de las cosas, IBM, 7 de febrero de 2025. [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/internet-of-things

[2] R. Roman, J. Zhou, y J. Lopez, On the features and challenges of security and privacy in distributed internet of things, *Computer Networks*, vol. 57, n.º 10, pp. 2266–2279, mar. 2013. doi: 10.1016/j.comnet.2012.12.018

[3] UNE, Ciberataques dirigidos a infraestructuras críticas, *Revista UNE*, no. 15, 12 de julio de 2025. [En línea]. Disponible en: https://revista.une.org/15/ciberataques-dirigidos-a-infraestructuras-criticas.html

[4] N. Woolf, DDoS attack that disrupted internet was largest of its kind in history, experts say, *The Guardian*, 15 de mayo de 2017. [En línea]. Disponible en: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[5] Wikipedia contributors, 2017 CloudPets data breach, *Wikipedia*, 2 de diciembre de 2024. [En línea]. Disponible en: https://en.wikipedia.org/wiki/2017$_{C}loudPets_{d}ata_{b}reach$

[6] D. Klonoff y J. Han, The First Recall of a Diabetes Device Because of Cybersecurity Risks, *Journal of Diabetes Science and Technology*, vol. 13, n.º 5, pp. 817–820, jul. 2019. doi: 10.1177/1932296819865655

[7] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks y L. Wingers, The SIMON and SPECK lightweight block ciphers, *ACM Digital Library*, jun. 2015. doi: 10.1145/2744769.2747946

[8] A. Bogdanov et al., PRESENT: An Ultra-Lightweight Block Cipher, en *Lecture Notes in Computer Science*, 2007, pp. 450–466. doi: 10.1007/978-3-540-74735-2$_3$1

[9] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, Lightweight Cryptography — CSRC — CSRC. https://csrc.nist.gov/Projects/Lightweight-Cryptography

[10] ISO - International Organization for Standardization, ISO. https://www.iso.org/home.html

[11] C. Dobraunig, M. Eichlseder, F. Mendel, y M. Schläffer, Ascon v1.2: Lightweight Authenticated Encryption and Hashing, Journal Of Cryptology, vol. 34, n.o 3, jun. 2021, doi: 10.1007/s00145-021-09398-9.

[12] Mbed TLS. [Online]. Available: https://github.com/Mbed-TLS

[13] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "On the Indifferentiability of the Sponge Construction," in *Lecture Notes in Computer Science*, vol. 5381, 2008, pp. 181–197. doi: 10.1007/978-3-540-78967-3$_1$1.

[14] A. Poschmann, "Lightweight Cryptography: Cryptographic Engineering for a Pervasive World," in *IEEE Circuits and Systems Magazine*, vol. 9, no. 4, pp. 30–39, Dec. 2009. [Online]. Available: https://ieeexplore.ieee.org/document/4397176

[15] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, Lightweight DTLS implementation in CoAP-based Internet of Things,ResearchGate, 2014.