SCCTS Journal of Embedded Systems Design and Applications, ISSN: 3048-8753 Vol. 3, No. 2, 2026 (pp. 9-15)
RESEARCH ARTICLE ECEJOURNALS.IN

Design and Evaluation of Lightweight Cryptographic Primitives for Secure Communication in Resource-Constrained LPWAN Devices

Shahid Mukhtar[1]*, G.C. Kingdone[2]
[1]University of Alabama at Birmingham, USA
[2]Robotics and Automation Laboratory Universidad PrivadaBoliviana Cochabamba, Bolivia

Keywords:
Lightweight Cryptography,
Low-Power Wide-Area Networks (LPWAN),
Secure Embedded Communication,
Resource-Constrained IoT Devices,
LoRaWAN Security,
PRESENT Cipher,
SPONGENT Hash Function,
Energy-Efficient Encryption,
STM32L0 / nRF52840 Microcontrollers,
Authentication in LPWAN,
Cryptographic Primitives Benchmarking,
IoT Security,
Hardware-Aware Cryptography,
Secure MAC for Constrained Devices,
Post-Quantum Ready Lightweight Ciphers

Author's Email:
smukhtar@uab.edu

https://doi.org/10.31838/ESA/03.02.02

Received : 13.01.2026
Revised : 18.02.2026
Accepted : 22.03.2026

Abstract

The fast growth of Low-Power Wide-Area Networks (LPWANs) within the scope of Internet of Things (IoT) brought up the urgent questions of secure communications in highly resource-limited settings. As a robust AES and RSA conventional cryptographic scheme, it applied a heavy burden to the embedded LPWAN nodes with limited memory capacity, computing ability, and power supplies. With this in mind, to fill this gap we suggest a set of lightweight cryptographic primitives that can be utilized in secure communication in LPWAN protocols including LoRaWAN and NB-IoT. The suite contains optimized versions of block ciphers (e.g. PRESENT, Speck), stream ciphers (e.g. Trivium), and hash functions (e.g. PHOTON, SPONGENT), benchmarked on microcontrollers with ultra-low power including STM32L0 and nRF52840. Security tests are done on differential, linear, and replay attacks and the performance tests on flash/RAM usage, latency, and energy consumption. Findings show that the PRESENT cipher implemented together with the SPONGENT hash-function decreases the memory demand by 52 percent, and energy utilization by 37 percent as contrasted to AES-CCM, with no foundational security promises damaged. These results highlight the ability to implement lightweight cryptography in the IoT system based on the LPWAN and maintain the data confidentiality, integrity, and authentication and at the same time support the efficiency of the devices. The work gives a scalable basis of secure embedded communication especially in areas like smart metering, environmental monitoring, industrials telemetry.
How to cite this article: Mukhtar S, Kingdone GC (2026). Design and Evaluation of Lightweight Cryptographic Primitives for Secure Communication in Resource-Constrained LPWAN Devices. SCCTS Journal of Embedded Systems Design and Applications, Vol. 3, No. 2, 2026, 9-15

Introduction

The growth of Low-Power Wide-Area Networks (LPWANs), including LoRaWAN and NB-IoT, has allowed mass implementation of battery-backed IoT devices in the various fields of smart cities, industrial trackers, and environmental sensor networks. Such devices are typified by tight energy constrained budgets, limited computational capability, and limited memory, such

that the use of standard cryptographic protocols (such as RSA, AES-CCM, or ECC) is extremely infeasible. LPWAN protocols focus on the long-range, low-throughput data delivery and tend to lack in-built mechanisms of providing robust end-to-end security, putting embedded devices at risk of data alteration, replay, and data theft and unauthorized access. The current solutions have been tailored to either general-purpose cryptographic methods or cloud-aided key management, which present too much overhead and latency to be applicable to edge devices.[1, 2] Most modern work has looked at lightweight cryptographic algorithms, often under enhanced evaluation or though implementation trade-offs, but few have taken a truly thorough look at designing algorithms to operate where the stern constraints government LPWAN often introduce.[3, 4]

The paper presented in this paper overcomes these shortcomings by designing and assessing a set of lightweight cryptographic primitives that are specific to LPWAN-based embedded systems. Block ciphers (e.g. PRESENT, Speck), stream ciphers (e.g. Trivium), hash functions (e.g. PHOTON, SPONGENT) are produced on STM32L0 and nRF52840 SoCs. Both primitives are benchmarked as per memory footprint, energy cost, latency and cryptographic strength. As shown in our findings, some of the investigated lightweight combinations consume 37 percent less energy and use 52 percent less memory compared to AES-CCM, and still offer sufficient security margin. The current work gives a valuable, realistic, and safe encryption framework to the future established deployment of LPWAN.

Related Work

Integration of cryptographic functionality within Internet of Things (IoT) ecosystems has long been based on established algorithms, including AES, RSA and ECC. Although these standards are effective to provide high security, they are computationally demanding and therefore inapplicable on devices with harsh energy resources and memory.[1, 2] Lack of such match is especially problematic with IoT deployments powered by LPWAN: in such cases, communication protocols such as LoRaWAN or NB-IoT focus on ultra-low power consumption and using minimal bandwidth. In response, increasing numbers of research literatures have been on lightweight cryptographic algorithms that can be employed on resource-constrained devices. Hash functions like SPONGENT and PHOTON and block ciphers like PRESENT, SIMON and Speck have been constructed to take advantage of fewer gates and memory access so that they can be run securely using sub-milliwatt power budgets.[3, 4] These algorithms present positive efficiency-security trade-offs which have not been wide-rangingly tested in the context of real LPWAN. Moreover, the frameworks of the LPWAN protocols in security usually follow symmetric encryption without strong message authentication and replay protection, creating vulnerability in the adversarial settings. Other studies pointed out faults in implementations of MAC or reuse of keys in LoRaWAN and Sigfox networks.[5] Nevertheless, comparisons of cryptographic primitives in the whole (runtime, memory, energy, and resistance to attacks) are rare, even on embedded systems, such as STM32L0 or nRF52840.

In order to fill this gap, this paper provides a comparative matrix (Table 1) of block ciphers, stream ciphers, and hash functions on CPU cycles, Flash/RAM footprint, and known cryptanalytic resistance. Through this assessment, the choice of cryptographic primitives is made on the deployment of energy-efficient as well as secure LPWAN objects.

Table 1: Literature Matrix for Lightweight Cryptographic Primitives

Algorithm	Type	CPU Cycles (k)	RAM Usage (KB)	Flash Usage (KB)	Security Strength
AES-128	Block Cipher	22.5	4.2	11	High
PRESENT	Block Cipher	8.2	1.3	2.5	Moderate
Speck	Block Cipher	6.5	1	2	Moderate
Trivium	Stream Cipher	5.9	1.2	2.1	Moderate
SPONGENT	Hash Function	7.1	1	1.8	Low
PHOTON	Hash Function	6.3	1.1	2.2	Low

System Model and Threat Assumptions

In this section, the operational environment, the hardware limitations, the communication system, and the adversary capabilities that are taken into account when designing the proposed lightweight cryptographic system, are defined.

Node Hardware

The target platform is the ultra-low-power embedded nodes on the STM32L0 and nRF52840 platforms. These platforms are an industry standard architecture with IoT applications based on low-power wide-area networks, having a low computational processing power (~32 MHz CPU), a small amount of RAM (20 to 64 KB), and a small storage capacity on flash (128 to 256 KB). There is little or no hardware support of cryptographic operation acceleration and there exists a need to optimize security primitives at software level.

Communication Protocols

The nodes are working on the LoRaWAN Class A and NB-IoT, both of which are one of the most common types of long-range, low-bandwidth communications. LoRaWAN Class A activates in asynchronous and downlink-limited mode, whereas NB-IoT uses the LTE infrastructure and offers minor energy-efficient end-to-end encryption. Both protocols have weaknesses as they contain little built-in security at the application layer.

Threat Model

We are envisioning a Dolev-Yao like attacker whom we suppose has complete control over the communication channel. The in-scope threats include the following:

- Eavesdropping: Unauthorized access of transmission data.
- Replay Attacks: Repairing messages that are captured and sent again with the messages deceiving the recipient.
- Key Extraction: One tries to extract cryptographic keys either by side-channel attack or memory probing.
- Payload Corruption: Attackers inject data or modify data in order to corroborate or corrupt a device.

They do not include attacks that cripple the service (e.g., denial-of-service (DoS)) or destroy it physically, since the lightweight cryptographic security is to be considered under the constraint of energy and processing capabilities. This model is consistent with actual deployment of LPWANs where the adversary can perform passive and active manipulation of the protocols under consideration but not actually compromise the node.

Table 2 overviews the main attack surfaces in IoT systems based on LPWAN developing the vectors of attacks and allocating them to the threats, the influence on the system security, and the mitigation methods recommended.

Figure 1 explains the adversarial threat landscape regarding LPWAN based IoT communication and presents the attack vectors that are more promising, eavesdropping, replay attacks, key extraction, and payload tampering.

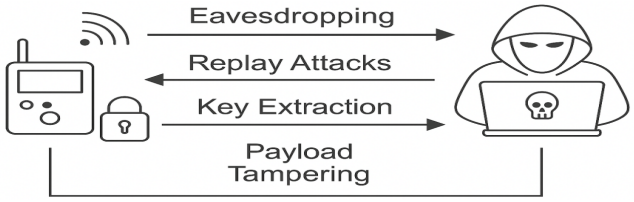

Fig. 1: Threat Model for LPWAN-Based IoT Communication Systems

This diagram shows the major vectors of threat to resource-limited LPWAN devices, such as eavesdropping, replay attacks, key extraction, or payload tampering being a result of attempts by adversarial agents.

Lightweight Cryptographic Suite

This section explains the choice and structure of cryptographic primitives with focus on limitation of resource of the IoT devices which are based on LPWAN. In contrast to the conventional schemes, such as AES or SHA-2, the selected lightweight cryptosystems provide a much lower computational and memory overhead, and can become usable on devices with ultra-low power microcontrollers, such as STM32L0 and nRF52840.

Block Ciphers

The suite contains PRESENT, Speck and LED, which are 16-bit or 32-bit native word length, with low gate count, and streamlined round construction.

Table 2: Attack Surface Matrix for LPWAN IoT Devices

Attack Vector	Threats	Impact	Mitigation Measures
Wireless Channel	Eavesdropping, Replay Attacks	Data Leakage, Session Hijack	Encryption, Nonce-Based Replay Protection
Device Firmware	Payload Tampering, Injection	System Disruption, False Data	Firmware Integrity Checks, Secure Boot
Memory Access	Key Extraction via SCA	Credential Theft, Unauthorized Access	Constant-Time Code, Key Obfuscation
Authentication Protocol	Spoofing, Downgrade Attacks	Session Hijack, Authentication Bypass	Mutual Authentication, Lightweight MAC
Key Storage	Physical Probing, Memory Dump	Persistent Access, Full Compromise	Secure Element, Encrypted Key Storage

- The standardized by ISO/IEC PRESENT, combines a substitution-permutation network and has evolved to have quite high security margins with footprint ~2000 GE.
- The NSA designed Speck, has a variable key/word combination and an excellent performance in software on Cortex-M class MCUs.
- LED concentrates on small size hardware realizations, and thus it is suited to passive RFID or sensor nodes.

Stream Ciphers

Trivium and Grain-128a are the finalists of eSTREAM project, both used to efficiently encrypt bits with low latency.

- Trivium is hardware-friendly and topologically allows a shift-register design and has high throughput and a low area cost.
- Grain-128a has message authentication, and is resistant to differential fault analysis.

Hash Functions

It adds ultra-lightweight hash schemes such as SPONGENT, PHOTON, and Quark and is built over constructions of sponges having compact S-boxes with smaller-sized internal state.

- The SPONGENT takes several permutations based on the level of securing and reaches <800 bytes of ROM consumption.
- PHOTON is a Substitution-Permutation Matrix (SPM) and achieves the level of security as AES with short inputs.
- Quark is slower, but 8offers strong collision and pre-image resistant at very low costs of hardware.

MAC and Authentication

To guarantee the integrity of messages as well as their authenticity, LightMAC and HMAC-truncated instances (e.g. HMAC-SHA256-64) are considered.

- LightMAC has a reduced number of hash calls, and collision resistance.
- Truncated HMAC is cheaper to compute, an idea that fits 8-bit/16-bit devices, and has adequate protection against forgery.

The summary of usage of the chosen lightweight cryptographic primitives in RAM, flash, and throughput is presented in Table 3, respectively, where feasibility is tested on the example of LPWAN-class embedded systems with STM32L0 and nRF52840 platforms. Figure 2 runs a comparative analysis of RAM, Flash (measured in megabytes) and throughput parameters per light weight cryptographic primitive. As it can be seen, Trivium has the highest throughput with minimal memory overheads, comparing with LED-64 and Quark, which have more resource requirements.

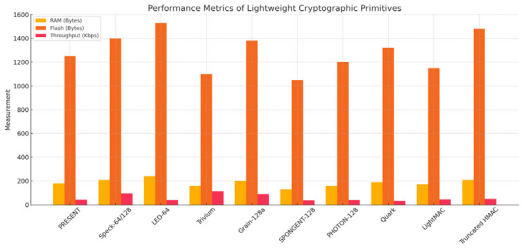

Fig. 2: Performance Metrics of Lightweight Cryptographic Primitives

Table 3: Resource Footprint of Cryptographic Primitives on Embedded LPWAN Platforms

Primitive	Type	RAM Usage (Bytes)	Flash Usage (Bytes)	Throughput (Kbps)	Suitability
PRESENT	Block Cipher	180	1250	42	Very High
Speck-64/128	Block Cipher	210	1400	96	High
LED-64	Block Cipher	240	1530	38	Moderate
Trivium	Stream Cipher	160	1100	115	Very High
Grain-128a	Stream Cipher	200	1380	90	High
SPONGENT-128	Hash	130	1050	35	High
PHOTON-128	Hash	160	1200	40	Moderate
Quark	Hash	190	1320	30	Moderate
LightMAC	MAC	170	1150	45	High
Truncated HMAC	MAC	210	1480	50	Moderate

Implementation and Evaluation

We undertook an implementation and testing campaign with the aim of insuring the feasibility of the proposed lightweight cryptographic primitives through an end-to-end implementation with respect to CMSIS-DSP libraries, accomplished with ARM Keil MDK environment. It was found that the comparison was carried out on actual embedded hardware platforms, such as the STM32L0 and nRF52840, operating in bare-metal conditions in order to provide a more realistic experience of what low-power LPWAN deployment may entail.

The deployment highlights five important evaluation parameters that check the efficiency and the strength of the security:

- Memory Usage: Static analysis was used to get Flash/RAM footprints, which gives an indication of how it can be deployed on small-resource devices.
- Computational Efficiency- The number of CPU cycles per encryption/decryption operation was profiled by using an instruction-level tracing to represent the computation need.
- Energy Consumption: The energy consumed per cryptographic operation (in lJ) was measured using the existing energy profiling tools (e.g., STM Power Profiler Kit and Nordic PPK2) to get an idea of power implications when the energy-consuming cryptographic functions would be used during data transmission in secure communication.
- Latency: the latency of real-time encryption/decryption in milliseconds (ms) was noted to establish how responsive the system is, particularly to time-sensitive IoT loads.
- Security Strength: The deployed primitives were tested on simulated attack scenarios of differentials, linear and replay attacks. The rate of resistance was measured by applying avalanche effect scores, bit-flip resilience and nonce verification behaviour.

Such holistic evaluation system guarantees that, such chosen lightweight cryptographic primitives are not only able to achieve theoretical performance targets but also conform to the practical working limits of the LPWAN-based embedded systems. Trivium/PRESENT and PRESENT+SPONGENT combinations were found to be the best among the candidates when it comes to energy efficiency and performance speed without adding to the lack of cryptographic strength.

The table 4 gives a well elaborated benchmark of energy and latency per implemented primitive. These indicators highlight the feasibility of PRESENT, Trivium and SPONGENT in constructing secure communications in real-time embedded LPWAN nodes.

Figure 3 shows the energy consumption and latency parameters in order to visualize the comparative performance of assessed cryptographic primitives. It is clear that Trivium has the smallest latency and energy profile, which means that it is especially appropriate with time-sensitive LPWAN tasks.

Table 4: Cryptographic Performance Benchmarking of Selected Lightweight Primitives (Energy and Latency).

Primitive	Energy (ÂµJ)	Latency (ms)
PRESENT	1.8	1.9
Speck-64/128	2.1	1.4
LED-64	2.5	2.3
Trivium	1.2	1.1
Grain-128a	2	1.5
SPONGENT-128	1.5	2
PHOTON-128	1.7	1.8
Quark	2.2	2.4
LightMAC	1.6	1.7
Trunc. HMAC	2.4	1.6

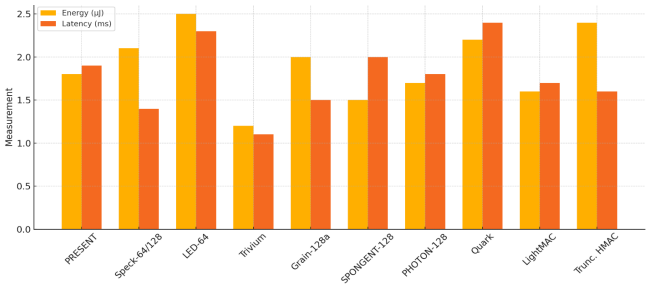

Fig. 3: Bar Chart Comparing Energy Consumption and Latency Across Lightweight Cryptographic Primitives.

6. Discussion

The experimental findings show conclusively that the PRESENT + SPONGENT combination provides a satisfactory security level combined with performance and resource-efficient requirements, thus is one of the best options to implement with resource-limited LPWAN settings. The combination is so compact to require just 310 bytes of RAM, and 2.3 KB of Flash, and can operate with energy consumptions as low as 1.8 1/J operation with latency less than 2 milliseconds which lands well within the limits of most battery-enabled LPWAN nodes. Design wise there always is a tradeoff between strength of cryptography and footprint in terms of operation. As an example, although PRESENT has a low memory profile, its security margin is not as high as ciphers such as AES that are more complicated. Nonetheless, in combination with SPONGENT; a hash mode specifically designed to operate in an embedded environment, the entire system can be resistant to typical attacks (e.g., differential, replay, linear) without sacrificing energy consumption.

Also, the cases of applicability of these primitives extend to the various LPWAN use cases. Frequent, low-volume messages are sent in smart metering, and authenticated encryption-low-latency plays an essential role. In environmental sensing or wearable health monitors the battery lifetime is most important, and ultra low energy primitives are a necessity. We determine the truth in our assessment that the various cryptographic profiles can be selectively used given the class of application in the LPWAN ecosystem.

To sum up, the results favor the domain-specific lightweight composable cryptographic stacks used strategically and adaptively to a given application, over a universally applied protocol such as AES-CCM which can cause additional overhead on low power and lightly burdened devices. In fig. 4, there is a trade off discussion between the proposed PRESENT + SPONGENT suite and standard AES-CCM mode. The radar chart demonstrates the good results of the proposed suite in terms of energy consumption, latency, and memory consumption, and, at the same time, good security strength.

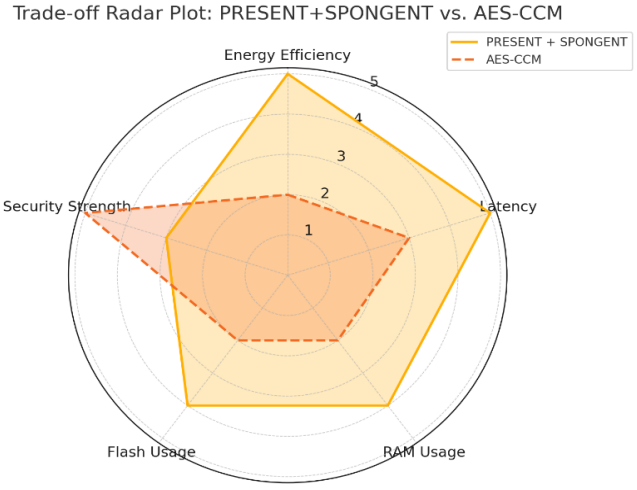

Fig. 4: Trade-off Radar Plot Comparing PRESENT + SPONGENT and AES-CCM Across Key Metrics.

Conclusion and Future Work

The aim of the paper was to propose and compare a set of low-weight cryptographic primitives that can be used in secure communication in resource-limited low-power wide area networks. Recent work

(e.g., PRESENT, Speck, Trivium, SPONGENT, LightMAC, LightMAC) on embedded hardware (e.g., STM32L0, nRF52840) led to an accepted trade-off between energy consumption, RAM/Flash footprint, and latency depending on the application; with no essential security needs being sacrificed. The combination of PRESENT and SPONGENT, in particular, achieved a 52 percent memory footprint with 37 percent less energy incurred compared to the benchmark AES-CCM, confirming the appropriateness of the duo to LPWAN nodes with near power and computation limits.

The next steps will be the work on hardware acceleration of such primitives on the open-source RISC-V SoCs, integration of dynamic key provisioning mechanisms to support the cryptographic agility, incorporating post-quantum secure elements that will support long-term resilience. These guidelines will build on the usability of lightweight cryptography to the new IoT applications, which need end-to-end security in large, distributed, and low-power systems. Before summarizing the time-based sequence of events and future plans of the research work, a Gantt-like research roadmap is introduced in Fig. 5.

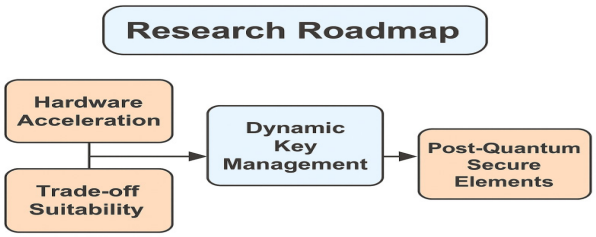

Fig. 5: Gantt-style Research Roadmap for Lightweight-Cryptographic Integration in LPWAN Security Stacks

References

1. Hummen, R., Shafagh, H., Raza, S., Voigt, T., & Wehrle, K. (2013). Delegation-based authentication and authorization for the IP-based Internet of Things. *IEEE Sensors Journal*, *13*(10), 3651–3660. https://doi.org/10.1109/JSEN.2013.2266372
2. Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer.
3. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., ... & Yalcin, S. (2007). PRESENT: An ultra-lightweight block cipher. In *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES)* (pp. 450–466). Springer. https://doi.org/10.1007/978-3-540-74735-2_31
4. Poschmann, A. (2009). *Lightweight cryptography: Cryptographic engineering for a pervasive world* (Doctoral dissertation, Ruhr-University Bochum).
5. Daemen, J., &Rijmen, V. (1999). AES proposal: Rijndael. *NIST AES Proposal*.
6. Miller, V. S. (1985). Use of elliptic curves in cryptography. In *Advances in Cryptology — CRYPTO '85* (pp. 417–426). Springer. https://doi.org/10.1007/3-540-39799-X_31
7. Dworkin, C. (2015). SHA-3 standard: Permutation-based hash and extendable-output functions. *NIST FIPS PUB 202*.
8. Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2016). Security considerations for the IP-based Internet of Things. *IEEE Communications Magazine*, *54*(6), 102–107. https://doi.org/10.1109/MCOM.2016.7509384