Shape

Description automatically generated with medium confidence

**Master in Telecommunications and Informatics**

**Network and Information Systems Security**

**Authors**:

Rodrigo Lopes Ferreira, N 140510

**Date**:

20/10/2025

**Title of the work**:

Experimental Analysis of PRISEC III Cryptographic Algorithms for Energy-Efficient IoT Implementation on ESP32

**Professors**:

Velderi Reis Quietinho Leithardt

Humza Sohail

# **Abstract**

Evaluating the computational performance and energy efficiency of lightweight cryptographic algorithms recommended by the PRISEC III framework, specifically AES-128-CTR mode and AES-256-GCM+RSA. The study focuses on their implementation in IoT environments using the ESP-WROOM32 microcontroller, a low-power platform commonly employed for sensor-based applications. Multiple data block sizes ranging from 8 bytes to 4 kilobytes were analyzed to assess algorithmic timing, resource utilization, and transmission overhead in different operational scenarios. Energy consumption was estimated by measuring execution times for cryptographic and data transmission processes separately and combined, and then validated using a USB-based power measurement setup. Theoretical power estimates were derived from device specifications and compared against experimental results to evaluate their practical accuracy. The proposed methodology provides a reproducible steps for assessing cryptographic performance and energy trade-offs in constrained IoT devices leveraging the PRISEC III framework, supporting future optimization of secure and efficient communication systems.

**Keywords**: *lightweight cryptography, multi-level encryption, IoT security, ESP32, energy consumption*

**Table of Contents**

[Abstract 2](#_Toc118067783)

Glossary3

Introduction4

Related Work5

Methodology6

Conclusion8

Further Work8

References9

# **Glossary**

*IoT – Internet of Things*

*SDK – Software Development Kit*

*P – Power*

*t – Time*

*E – Energy*

*Cf – Clock Frequency*

*EC – Elapsed Cycles*

*E = t \* P*

*t = Cf / EC*

# **Introduction**

The rapid growth of the Internet of Things (IoT) has intensified the need for secure and energy efficient communication among resource constrained devices. Ensuring data confidentiality and integrity while maintaining low power consumption remains a key challenge, especially in environments with limited computational and energy resources.

This work aims to experimentally evaluate and compare the **performance, resource usage, and energy consumption** of cryptographic algorithms recommended by **PRISEC III[1]**, focusing on **AES-128-CTR** and **AES-256-GCM + RSA**. The objective is to identify an optimal compromise between **speed and security** under different system conditions applicable to real-world IoT scenarios.

The experimental implementation targets the **ESP-WROOM-32[2]** module, a dual-core Xtensa LX6-based microcontroller running at 240 MHz with hardware acceleration for AES and RSA operations. Typical current draws range from 120–260 mA during transmission, 95–100 mA during reception, and approximately 80 mA when idle with Wi-Fi connected.

Three message block sizes—8 B, 16 B, and 4 KB—will be tested to study their impact on algorithmic timing and energy usage. Energy estimation will follow a dual approach. **Theoretical estimation:** and , using . **Practical measurement:** average energy readings from a USB power meter across repeated transmission runs.

This work considers three diferent operating scenarios to test different block sizes. The comparative analysis will reveal the trade-offs between security level and energy efficiency, contributing to the development of practical, energy-aware cryptographic strategies for IoT devices.

# **Related Work**

Recent research has focused on identifying efficient cryptographic schemes for resource-constrained IoT environments, balancing energy consumption, computational overhead, and security level. The present work follows the guidelines proposed in [1], which recommend **AES-128-CTR** and **AES-256-GCM combined with RSA** as the most suitable schemes that provide a practical compromise between performance and cryptographic strength. The framework proposes implementation security at 4 distinct levels (Guest, Basic, Advanced, Admin) using a multi-layered approach motivated by the consideration that while the compromise of user sensor data is undesirable, the compromise of administrative control would be far more critical.

In **[9] and [10]**, the authors proposed a methodfor estimating the energy consumption of cryptographic algorithms. Th method involved counting the number of executed instructions and multiplying them by their theoretical energy cost. However this cannot be accuratly applicable to this work has we intend to measure the communication between the ESP32 client and server and not just the crytographic algorithm itself. Also the ESP32 has hardware acceleration for the algorithms we will be using in the SDK so measuring the algorithms themselves would be redundant.

In [5] a multi-layer approach was used for the ESP32 is also explored rotating the cryptography algorithm depending on battery availability in order to reduce energy consumption using AES128 and RC4, but using the last algorithm mentioned might be too might of a security compromise for an IoT device, further increased by the fact that these devices have AES128 hardware accelerators.

Given that oscilloscopic measurements fall outside the practical scope of this project, a **hybrid estimation approach** is adopted. This combines **theoretical energy estimation derived from** [4] and [7], with **empirical readings** obtained from a low-cost USB power meter, averaged across multiple measurement runs.

While these approaches have been validated in prior work, **the influence of data block size on energy consumption and performance has not been systematically explored**. The present study addresses this by investigating how varying block sizes affect energy efficiency, algorithmic timing, and overall system performance.

# **Methodology**

****A. Experimental Device****

All experiments are conducted on the **ESP-WROOM-32** development board, which features a **dual-core Xtensa LX6 CPU** running at **240 MHz**, with **hardware acceleration** for AES and RSA operations. The device operates at **3.3 V** and is powered through a USB interface, allowing for both program execution and power sourcing. The ESP32’s integrated Wi-Fi module, compliant with the IEEE 802.11 standard, operating on the 2.4 GHz band. Typical current draws ranging from **180–240 mA** during transmission, **95–100 mA** during reception, and **80 mA** when RX/TX are idle but still maintaining the connection. Higher transmission power or greater data throughput is required to compensate for **signal attenuation**, which increases with distance and obstacles in the wireless environment.

The ESP32 communicates with a **master server running Linux** that receives, decrypts, and logs the transmitted data for verification and timing synchronization. All experiments are executed under consistent network conditions to minimize measurement variance due to external factors.

The ESP32 algorithmic timing is calculated using the ESP32 SDK, importing "esp\_timer.h" for the esp\_timer\_get\_time() function.

#### ****B. Cryptographic Implementation****

The cryptographic operations are implemented using the **ESP SDK** to ensure usage of the hardware accelerators. Two cryptographic schemes recommended by PRISEC III are evaluated:

1. **AES-128-CTR** – used for general data transmission, representing lightweight encryption with minimal processing overhead. (*"mbedtls/aes.h", mbedtls\_aes\_crypt\_ctr())*
2. **AES-256-GCM + RSA** – used for administrative communication, representing a higher-security mode with hybrid symmetric–asymmetric encryption. (*"mbedtls/gcm.h", mbedtls\_gcm\_crypt\_and\_tag(), mbedtls\_rsa\_2048() or mbedtls\_rsa\_3072())*

#### ****C. Data Transmission Scenarios****

Three distinct data transmission scenarios are tested to evaluate the influence of message size and communication mode on performance and energy consumption:

1. **Continuous Transmission:**  
   The device transmits 8B, 16B, and 4 KB data blocks sequentially at fixed intervals. Estimated current draw ≈ **240 mA** (transmission-dominant mode).
2. **Grouped Transmission:**  
   Small data blocks (8B and 16B) are aggregated into 4 KB packets before transmission to simulate buffer-based IoT communication. Estimated current draw ≈ **180 mA**.
3. **Bidirectional Transmission:**  
   The device alternates between sending and receiving 4 KB blocks to emulate interactive communication with a sensor. Estimated current draw ≈ **200 mA**.

Each scenario is executed multiple times to reduce statistical noise, and average values are used for analysis.

#### ****D. Measurement Procedure****

1. **Theoretical Estimation: Current is estimated from the reference manual of the devices for each scenario. P**ower and energy are computed using the relationships P=I×V and E=t×P where  VV=3.3 V, I is the measured current draw, and t is the measured execution time of the program.
2. **Practical Measurement:** Real-world power readings are captured using a **USB energy meter** connected inline with the ESP32’s power supply. Measurements are averaged over 6 and **10 second transmission windows** for each test configuration. Both encryption-only and encryption-plus-transmission runs are recorded to separate computational and communication energy costs.

All timing operations are instrumented using microsecond-resolution timers available in the ESP- SDK to ensure precise measurement of the routines and communication delays.

#### ****E. Evaluation Metrics****

1. **Execution Time (ms):**  
   Impact of different block sizes for the same amount of data transmission.
2. **Energy Consumption (mJ):**  
   Derived from both theoretical and practical.
3. **Resource Utilization (%):**  
   CPU and memory usage monitored using ESP32 SDK.

#### ****F. Data Analysis****

The collected data will be analyzed for different block sizes and operational scenarios. Comparative analysis for AES-128-CTR and AES-256-GCM+RSA to identify trade-offs between **speed, security, and energy consumption in different block sized communication between a server and an ESP32 client. In this section a side by side comparison of the results will be provided.**

# **Conclusions**

This work evaluates the trade-offs between performance, energy consumption, and security of AES-128-CTR and AES-256-GCM + RSA on the ESP-WROOM-32 platform with hardware acceleration. Experiments considered varying data block sizes and communication scenarios, with energy measured through a hybrid approach combining theoretical estimates and USB meter readings.

# **Further Work**

* Evaluate additional cryptographic schemes recommended in PRISEC III , such as ChaCha20 and ECC algorithms, to compare performance and energy consumption.
* Use more precise measurement tools, such as an oscilloscope, to validate the theoretical energy models.
* Extend testing of AES128-CTR and AES256-GCM+RSA to other IoT devices.
* Measure the impact of hardware acceleration and the value of other cryptographic algorithms such as ECC in IoT devices with this hardware feature.

# **References**

[1] Sohail, H., Leithardt, V., & Trigo, A. (2025) “PRISEC III: Cryptographic Techniques for Enhanced Security”

[2] EXPRESSIF SYSTEMS ESP-WROOM32 Manual (FCC Reviewed 2016) https://fccid.io/2AC7Z-ESPWROOM32/User-Manual/Users-Manual-3212934.pdf

[3] Silva, C., Cunha, V.A., Barraca, J.P. *et al.* (2024) “Analysis of the Cryptographic Algorithms in IoT Communications”

[4] S. Maitra, D. Richards, A. Abdelgawad and K. Yelamarthi (2019)z "Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy”

[5] S. H. Rafat et al. (2025) “Lightweight Cryptographic Algorithm Analysis for Secure IoT Communication on ESP-32 Platforms”

[6] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas and L. Castedo (2018) “Clock frequency impact on the performance of high-security cryptographic cipher suites for energy-efficient resource-constrained IoT devices”

[7] Patterson, J. C., Buchanan, W. J., Turino, C. (2025) “Energy Consumption Framework and Analysis of Post-Quantum Key-Generation on Embedded Devices”

[8] C. Guo, Y. Yang, Y. Zhou, K. Zhang and S. Ci (2021) “A Quantitative Study of Energy Consumption for Embedded Security”

[9] C. Guo, S. Ci, Y. Zhou and Y. Yang (2021) “A Survey of Energy Consumption Measurement in Embedded Systems”

[10] Y. S. Vaz, J. C. B. Mattos and R. I. Soares, “Lightweight AES Algorithm for Internet of Things: An Energy Consumption Analysis”