Energy Impact of Cryptographic Block Sizes on ESP32 Devices

Rodrigo Lopes Ferreira
Master of Telecommunications and Informatics Engineering
ISCTE
Lisbon, Portugal
https://github.com/rodfer0x80/meti-srsi

***Abstract*—Evaluating the impact of energy consumption for hardware accelerated cryptographic algorithms, using different block sizes such as AES128-CTR and AES258-GCM+RSA following the PRISEC III framework on an ESP-WROOM32. The current draw is estimated theoretically using the device's manual and averaged with a practical measure using a power meter between the device and the power source. The proposed method should produce a quick and low-cost reproducible set of steps to evaluate the trade-offs between energy consumption and security in IoT devices following the PRISEC III framework.**

***Index Terms*—lightweight cryptography, multi-level encryption, IoT security, ESP32, energy consumption**

I. Introduction

In the fast modernisation infrastructure using small and energy-efficient devices in the world of IoT, security and privacy have a human right that cannot be forgotten and remains a key challenge. On the practical side, hardware acceleration is built into the devices to improve their efficiency for this exact purpose and should be leveraged whenever available. As such frameworks as the PRISEC III [1] exist to guide engineers and developers of this services and application to ensure their users' data and devices remain secure.

This work aims to measure and evaluate the energy consumption of such recommendations in three real-world scenarios using different block sizes in the ranges of 8 bytes to 4 kilobytes.

The best recommendations from the PRISEC III framework given were AES128-CTR and AES256-GCM with RSA for leveraging multi-level security and energy consumption compromise. For example, a device can send sensor data using the first algorithm and admin control features are secured using the later. One can also imagine a security critical service for example in a government institute that might only require AES256-GCM+RSA in order to have enhanced security at all time compromising energy consumption for it.

The experimental procedure will be done on an ESP-WROOM32, which has 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.

Energy estimation will follow a dual approach. Theoretical estimation of current using the manufacturer's manual [2] and practical estimation from reading using an energy meter in between the device and the power source in repeated transmission runs to try and improve accuracy due to the measurement device's imprecision.

$$P = I \times V$$

Where $V = 3.3\,\mathrm{V}$ as for the manufacturer's recommendation for this device and I is the estimation for the given scenario. Followed by:

$$E = t \times P$$

Where E is the energy consumption given the t time of program run for the given scenario and P is the power previously calculated.

Three different operating scenarios are considered to test different block sizes. Continuous Client Dominant Communication, Grouped Client Dominant Communication and Bidirectional Communication.

II. Related Work

Recent research in building frameworks for cryptographic schemes in IoT, balacing energy consumption and security such as PRISEC III [1] as presented recommendations such as AES128-CTR and AES256GMC+RSA. Such algorithms are covered in the ESP-IDF SDK for the ESP-WROOM32 and conveniently have hardware acceleration support. The framework aforementioned proposes implementing security at 4 distinct levels (Guest, Basic, Advanced, Admin) using a multi-layered approach.

In [8] and [9], the authors proposed a method for estimating the energy consumption of cryptographic algorithms. The method involved counting the number of executed instructions and multiplying them by their theoretical energy cost. Although this technique is very interesting and might need more exploration, it is more narrowly applicable to the cryptographic algorithms themselves, and loses consistency when measured programs that perform transmission of packets and thus it is not a well applicable for this experiment.

In [5] a multi-layer approach was used for the ESP32 that explores rotating the cryptography algorithm depending on battery availability in order to reduce energy consumption using AES128 and RC4. Altought the concept is interesting, using RC4 is not recommended by the PRISEC III framework due to poor security. The limitation of this approach is further exacerbated 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 placed between the device and its power source, 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. This work addresses this by investigating how varying block sizes energy consumption in different real-world scenarios and reinforces the validity of the PRISEC III framework.

III. Experimental Testing Methodology

A. Hardware

The experimentation is done on the ESP-WROOM32, which has a dual-core Xtensa LX6 CPU running at 240 MHz, with hardware acceleration for AES128-CTR, AES256-GCM and RSA support. The device operates at 3.3 V and is powered through a USB interface, allowing for loading the program and to power it. The ESP32's integrated WiFi module is compliant with the IEEE 802.11 standard and thus operates on the 2.4 GHz band, allowing for TCP/IP communication and MQTT, which is a common IoT high level communications protocol.

The ESP32 communicates with a master server running Linux that receives and logs all communications verification and analysis, such has timing.

The algorithmic timing is calculated using the ESP-IDF 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 the use of hardware accelerators. Two cryptographic schemes recommended by PRISEC III are evaluated:

1) AES-128-CTR – lightweight encryption with minimal lesser computation (`mbedtls/aes.h`, `mbedtls_aes_crypt_ctr()`)
2) AES-256-GCM + RSA – higher security for a compromise in energy efficiency with hybrid symmetric–asymmetric encryption (`mbedtls/gcm.h`, `mbedtls_gcm_crypt_and_tag()`, `mbedtls_rsa_2048()`,`mbedtls_rsa_3072()`)

C. Scenarios

1) Continuous Client Dominant Transmission: The device transmits 8 B, 16 B, and 4 KB data blocks sequentially. Estimated current draw $\approx$ 240 mA.
2) Grouped Client Dominant Transmission: Small data blocks (8 B and 16 B) are aggregated into 4 KB packets before transmission to simulate buffering data in IoT communication. Estimated current draw $\approx$ 180 mA.
3) Bidirectional Transmission: The device alternates between sending and receiving 4 KB blocks. Estimated current draw $\approx$ 200 mA.

Each scenario is executed multiple times to achieve a more accurate reading.

D. Current Estimation

$P = I \times V$, where $V = 3.3$ V, I is the measured current draw.

- Theoretical Estimation: Current is estimated from the reference manual of the devices for each scenario. Power and energy are computed using the relationships
- 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 scenario.

E. Experiment

Using $E = t \times P$, where we got P from the estimations and t is the timing of the execution for a same sized collection of data equal for each experiment of a different block size, but can vary between each scenario.

The timing function used is from the ESP-IDF SDK to ensure precise measurement.

F. Data Analysis

The data from each block size, for each scenario will be compared and a conclusion and explanation will be provided for each result.

IV. Conclusions

The security of IoT devices is crucial and has to keep up with the fast advances in the field. For such frameworks have to be developed, such has PRISEC III in order to standardise cryptographic implementations and boosting development speed of this devices and services.

The study on the impact of different scenarios and block sizes can be helpful in the validation of this framework.

V. 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 AES-128-CTR and AES-256-GCM+RSA to other IoT devices.
- Measure the impact of hardware acceleration and the effectiveness of other cryptographic algorithms, such as ECC, in IoT devices.

VI. Acknowledgments

Acknowledgments are in order to the professors Valderi Leithardt and Humza Sohail for leading the SRSI module, and for developing the PRISEC III framework.

References

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

[2] EXPRESSIF SYSTEMS. (2016). *ESP-WROOM32 Manual (FCC Reviewed)*. Available: https://fcc.report/FCC-ID/2AC7Z-ESPWROOM32/3212970

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

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

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

[6] Suárez-Albela, M., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (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] Guo, C., Yang, Y., Zhou, Y., Zhang, K., & Ci, S. (2021). *A Quantitative Study of Energy Consumption for Embedded Security*.

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

[10] Vaz, Y. S., Mattos, J. C. B., & Soares, R. I. (n.d.). *Lightweight AES Algorithm for Internet of Things: An Energy Consumption Analysis*.