Performance Profiling of Cryptosystems on IoT Devices Under Variable Operating Scenarios

Tomás Carruço
IPSantarém - ESGTS
Santarém, Portugal
tomas.marques@esg.ipsantarem.pt

Juan Volpi
IPSantarém - ESGTS
Santarém, Portugal
210100350@esg.ipsantarem.pt

***Abstract*—The proliferation of IoT devices across critical infrastructure, healthcare, and industrial applications has intensified security concerns, as many resource-constrained devices implement inadequate cryptographic protections. While established cryptosystems provide robust security, their computational and energy demands often exceed the capabilities of low-power microcontrollers. Hardware cryptographic accelerators integrated into modern System-on-Chip (SoC) platforms partially address these constraints, but accelerator support varies significantly across manufacturers—creating substantial performance heterogeneity that complicates algorithm selection for resource-constrained deployments. This paper presents a comprehensive performance characterization of symmetric and asymmetric cryptosystems across heterogeneous SoC platforms from multiple manufacturers, profiling behavior under three operational regimes: nominal conditions, peak computational load, and adverse power supply scenarios. The study measures encryption/decryption latency, power consumption, memory utilization, CPU overhead, and thermal behavior across variable key sizes, leveraging native hardware accelerators where available. Critically, controlled power supply perturbations are introduced to simulate real-world voltage instability and assess cryptographic resilience under resource degradation. The resulting empirical dataset enables the development of decision support tools that can guide developers in selecting cryptographic configurations based on hardware capabilities, power constraints, and application requirements, providing a foundation for intelligent algorithm selection in power-constrained and fault-prone IoT deployments.**

***Index Terms*—IoT, Cryptosystems, , power efficiency, processing efficiency**

I. State of the art

Every research activity should strive for originality. Not only to differentiate itself from existing works, but to achieve new outcomes and obtain new knowledge. These are the objectives that move the state of the art forward, towards innovation.

A. Research Selection

For this paper to obtain differentiated results and contributions, that add to the existing scientific knowledge, these paper's authors have produced a scientific overview of related papers. The papers chosen, *all ten of them*, and their respective research focus are represented in Table I.

TABLE I
Chosen papers and their research goal

Paper	Research Goal
Aaraj et al. 2008	Software-based Trusted Platform Module (SW-TPM) energy and execution time overheads on embedded systems
Al Sibahee et al. 2017	Power consumption of encryption algorithms in wireless sensor networks
Baldanzi et al. 2019	Crypto accelerators for power-efficient, real-time secure algorithms
Datsios et al. 2013	Performance/power trade-offs for cryptography on embedded processors
Fadia & Toufik 2024	Elliptic Curve Cryptography vs Rivest–Shamir–Adleman for lightweight IoT devices
Gaubatz et al. 2005	Feasibility of public key cryptography in sensor networks (hardware)
Halak et al. 2022	Comparative analysis of energy costs for symmetric vs asymmetric encryption in Internet of Things (IoT)
Jiang et al. 2013	Empirical energy/timing analysis of cryptography on real-time embedded systems
Silva et al. 2016	Performance evaluation of cryptography on embedded/general-purpose systems
Suarez-Albela et al. 2018	Elliptic Curve Cryptography vs Rivest–Shamir–Adleman for Transport Layer Security authentication on IoT nodes

B. Paper selection criteria

In order to select a portion of adequate and relevant scientific contributions, of wich this proposal rests upon, the following topics and keywords were used to narrow down the search for papers:

- Encryption algorithms
- Embedded systems
- IoT devices
- Hardware implementations
- Algorithm Profiling

C. Analysis and key takeaways

Subsequently, after retrieving and analyzing the works defined in Section I.A, we've identified a number of similar experiments and data collection efforts similar, to the goals in this proposal. These objectives fall under the following two main ideas - microcontroller (MCU) profiling (Al Sibahee et al., 2017; Datsios et al., 2013; Halak et al., 2022) and algorithm viability/usability (Baldanzi et al., 2019; Gaubatz et al., 2005) in these kinds of devices. All under the umbrella of a realistic testing environment (Baldanzi et al., 2019; Jiang et al., 2013).

It was also observed that most of these papers, work towards testing the viability of one or multiple algorithms in regards to a single testing regime (Fadia & Toufik, 2024; Silva et al., 2016). Although reduced diversity of MCU architectures is present in the literature - yes, different boards are in use - but, the variation in the architectures is quite limited. This in our opinion, limits the applicability of these works on different hardware.

The metrics collected by these studies include the CPU overhead, MCU temperature, memory/energy usage, and temporal measurements obtained from the usage of the selected crypto-systems (Aaraj et al., 2008; Silva et al., 2016). Mainly focussing on the use of symmetrical and asymmetrical cryptography (Suarez-Albela et al., 2018), ignoring some algorithms design specifically for IoT devices.

Finally, from the literature chosen, no framework or model was identified that could assist or narrow-down the selection process of encryption algorithms by either their metrics, or available hardware.

II. Proposal

In order to provide scientific value and innovation, we must build upon what exists. To achieve these goals, **we propose the following** - The profiling of multiple encryption algorithms/cryptosystems, on a diverse deck of MCU architectures, under three well defined operating scenarios, enabling us to develop a statistical model, with the goal of improving the algorithm selection process; This is the main body of work proposal that enables us to introduce, what we believe to be, **the differentiating factor, a statistical model**, that while leveraging this data can accurately model the expected performance of the pairing of different algorithms, with multiple MCUs, to provide better decision making in the development of IoT hardware, more so than just developing with simple metrics in mind.

It is this broad collection of data, with applied statistic modeling, that enables better decision making, as concluded by Grove et al. (2000), also by Kuncel et al. (2013) and more recently Viljoen et al. (2024). Both studies applied statistical modeling to data-rich situations, concluding that relying on statistical models for decision making leads to better outcomes.

Aggregating all of the knowledge obtained from the chosen literature, with the intent to model-out this proposals research framework, the remainder of this topic will attempt to visually describe this proposal's intent.

A. Conceptual basis

The three main supporting concepts behind this proposal are the following - chosen encryption algorithms/cryptosystems, the correct definition of the testing scenarios, and the metrics to be collected from the selected MCU architectures. These concepts will then feed into the decision of what statistical modeling techniques to apply, as a result, creating a accurate decision assistance mechanism.

In Fig. 1, the overall concepts and relations employed in this framework, are laid out visually for better understanding.

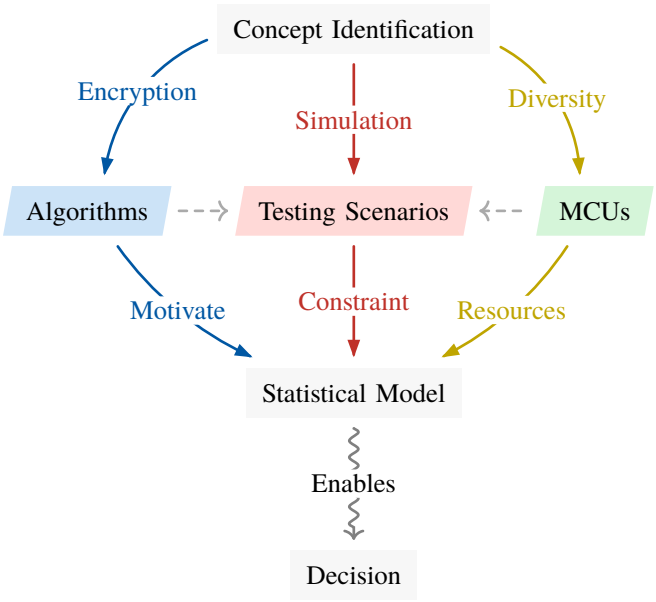

Fig. 1. Framework concept's hierarchy

B. Algorithm selection

Diving into more detail, specifically in Table II, we provide further insights into what we aim to achieve regarding the algorithms chosen for this proposal.

TABLE II
Algorithm selection

Name	Category	Sub-Category
AES	Symmetric-Key Cryptography	Block Cipher
DES	↵	↵
3DES	↵	↵
ChaCha20	Symmetric-Key Cryptography	Stream Cipher
RC4	↵	↵
Salsa20	↵	↵

Name	Category	Sub-Category
RSA	Asymmetric-Key Cryptography	–
ECDH	✓	–
DSA	✓	–
AES-GCM	Symmetric-Key Cryptography	Authenticated
ChaCha20-Poly1305	✓	✓

With this selection of algorithms, heavily influenced by existing literature (i.e Section I.A), we aim to introduce further performance and usability experimentation, than what was previously researched, including new algorithms. Striving towards a more diversity in terms of tested options.

C. MCU selection

To be able to test these algorithms, we propose to use the hardware listed in Table III. This list is mainly based in *ARM* and *RISCV* architectures, even though this is the case, it presents diversity in MCU design, by selecting multiple MCU architecture series. The selected MCUs span from low-powered focused units, to high resource available ones. With this diversity in resource and intended MCU usage, we hope to extract new and meaningful insights, on their utilization performance for the chosen algorithms.

TABLE III
MCU SELECTION

Name	Architecture	Core Count	Frequency (MHz)	SRAM (KB)
RP2350	Arm Cortex-M33	2	150	520
RP2350	Hazard3 RISC-V	2	150	520
ESP32-C3	RISC-V	1	160	400
ESP32-S3	Xtensa LX7	2	240	512
STM32L476	Arm CORTEX-M4 RISC	1	80	128

We believe these are good choices for the proposed list of MCUs. For example, the RP2350 from RaspberryPi (2024), has a total of 4 cores. This core count enables us to select wich two cores (by architecture) to enable, shutting down the other two (RaspberryPi, 2024). In essence, having two different boards, in one single package. In the case of the ESP family from Espressif, we have chose two MCUs. One of them dual-core (Systems, 2025a), the other single (Systems, 2025b). These MCU allow us to test two other architectures and MCU designs inside the same family, and observe, if any, changes in performance due to the design goals for each MCU. This is a relevant point due to the fact that the ESP32-C3, is designed for secure low-power utilization (Systems, 2025b), thus, creating expectations that it will reveal varying performance metrics. Finally, the STM32 MCU is an entry with visibly less resources, built for low-power designs, this selection is still a good representation of MCUs that, although having less resources, the platform's design might prove to be more optimized and performant (Life Augmented, 2015) than other systems.

Each MCU will be tested through the manufacturer provided dev-kit.

D. Baseline Testing Scenario

Good science is always reproducible and visible. To achieve these objectives, this proposal defines three scenarios in wich each MCU will be tested. These scenarios vary in the algorithms, algorithmic load (i.e different quantities of data to encrypt and decrypt in the same run) and power source fluctuations. The scenarios will all be based on the architecture present in Fig. 2.

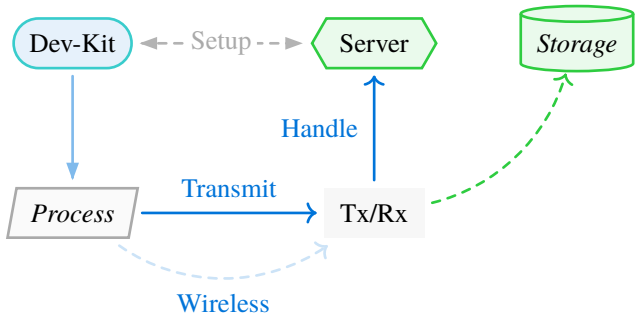

Fig. 2. Base testing scenario

The baseline scenario present in Fig. 2, defines a setup with two participants. These two participants, communicate through a client-server architecture, being part of the same wireless network. Upon data retrieval by the server, such as timings, message validation and other experiment metadata, said data will be stored in a structured way for future use and querying capability. This server can also communicate directly with the client, instructing him to change his behavior and/or function.

With this baseline scenario in mind, we can now describe in more detail the three testing scenarios.

III. In-depth Testing and Data Collection

The experimental phase will involve a systematic collection of performance and electrical data from all of the following test scenarios.

A. Nominal Operation

Under this scenario, the overall computational load will be reduced. The main goal is to measure the performance of the MCU during uneventful operation, to establish a baseline. This proposal considers that an uneventful operational scenario, is composed of the following characteristics:

- No authentication required, straight communication to the server;

- A reduced amount of small periodic data transmissions *(i.e., hundreds of bytes)*; and
- Stable supply of power to the MCU;

B. High Computational Load

In this scenario, the computational load increases in frequency and size. Subjecting the MCU to periodic amounts of stress, demanded by more intensive peaks of communication, at the server's request. This proposal considers that this operational scenario, is composed of the following characteristics:

- Periodically authenticating the device to the server;
- Frequent transmissions of larger amounts of data *(i.e: Kb range)*; and
- Peaks of considerable increase in message size and frequency *(i.e: Mb range)*;

C. Unstable supply of power

Finally, this scenario is built upon the previous one *(Section III.B)*, while also introducing power fluctuations. These fluctuations will always be either under-voltage or under-current situations. The objective is to stress the MCU and its operation, not to invalidate the board.

D. Measurement Methodology

Data collection will be performed using a combination of digital oscilloscopes, precision multimeters, and variable power supplies to accurately monitor voltage, current, and power fluctuations throughout the execution of encryption and decryption operations.

An oscilloscope will capture real-time waveforms corresponding to current draw and voltage variation, providing insight into transient responses during cryptographic computations. Meanwhile, the multimeter readings will validate the average consumption and ensure measurement consistency across test repetitions. Finally, all collected data will contain timestamps, in order to enable time-correlated measurements between power events, algorithmic execution milestones and building an overall timeline of events.

Alongside electrical monitoring, the test server will record data related to the "real-world" behavior of these simulations, that is, response times and communication integrity for each algorithm–MCU pairing. These hardware and software measurements will be combined into a unified dataset, which will subsequently be processed using Python or R to construct the regression model described in Section IV. This integrated approach ensures that every performance metric is captured under consistent and reproducible experimental conditions.

IV. Desired Outcomes

After collecting the experimental data from the three defined scenarios, the results will be processed and analyzed using statistical computing tools such as Python or R. A linear regression model — or other suitable predictive techniques — will then be applied to identify relationships between the operational variables (e.g., input current, message size, algorithm selected) and the measured performance metrics. Based on these relationships, the model will be capable of recommending the most appropriate cryptographic algorithm or MCU configuration for a given operational context (Grove et al., 2000). With this statistical modeling approach, we hope to ease the crypto-system/MCU decision-making process, while also enhancing the reproducibility and scientific rigor of this work as whole. (Kuncel et al., 2013)

References

Aaraj, N., Raghunathan, A., & Jha, N. K. (2008). Analysis and design of a hardware/software trusted platform module for embedded systems. *ACM Transactions on Embedded Computing Systems*, *8*(1), 1–31. https://doi.org/10.1145/1457246.1457254

Al Sibahee, M. A., Lu, S., Hussien, Z. A., Hussain, M. A., Mutlaq, K. A.-A., & Abduljabbar, Z. A. (2017). The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN. *2017 International Conference on Computing Intelligence and Information System (CIIS)*, 308–312. https://doi.org/10.1109/ciis.2017.50

Baldanzi, L., Crocetti, L., Di Matteo, S., Fanucci, L., Saponara, S., & Hameau, P. (2019). Crypto Accelerators for Power-Efficient and Real-Time on-Chip Implementation of Secure Algorithms. *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 775–778. https://doi.org/10.1109/icecs46596.2019.8964731

Datsios, C., Keramidas, G., Serpanos, D., & Soufrilas, P. (2013). Performance and power trade-offs for cryptographic applications in embedded processors. *IEEE International Symposium on Signal Processing and Information Technology*, 92–95. https://doi.org/10.1109/isspit.2013.6781860

Fadia, T., & Toufik, L. (2024). Elliptic curves cryptography for lightweight devices in IoT system. *Brazilian Journal of Technology*, *7*(4), e73725. https://doi.org/10.38152/bjtv7n4-003

Gaubatz, G., Kaps, J.-P., & Sunar, B. (2005). Public Key Cryptography in Sensor Networks—Revisited. In *Lecture Notes in Computer Science* (pp. 2–18). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-30496-8_2

Grove, W. M., Zald, D. H., Lebow, B. S., Snitz, B. E., & Nelson, C. (2000). Clinical versus mechanical prediction: A meta-analysis. *Psychological Assessment*, *12*(1), 19–30. https://doi.org/10.1037/1040-3590.12.1.19

Halak, B., Yilmaz, Y., & Shiu, D. (2022). Comparative Analysis of Energy Costs of Asymmetric vs Symmetric Encryption-Based Security Applications. *IEEE Access*, *10*, 76707–76719. https://doi.org/10.1109/access.2022.3192970

Jiang, W., Guo, Z., Ma, Y., & Sang, N. (2013). Measurement-based research on cryptographic algorithms for embedded real-time systems. *Journal of Systems Architecture*, *59*(10), 1394–1404. https://doi.org/10.1016/j.sysarc.2013.09.008

Kuncel, N. R., Klieger, D. M., Connelly, B. S., & Ones, D. S. (2013). Mechanical versus clinical data combination in selection and admissions decisions: A meta-analysis. *Journal of Applied Psychology*, *98*(6), 1060–1072. https://doi.org/10.1037/a0034156

Life Augmented, S. -. (2015). *STM32L476XX Ultra-Low-Power Arm ® Cortex ® -M4 32-bit MCU+FPU, 100DMIPS, up to 1MB Flash, 128 KB SRAM, USB OTG FS, LCD, ext. SMPS* (11th ed., Vol. 1). ST Electronics.

RaspberryPi. (2024,). *RP2350 DataSheet*. https://pip-assets.raspberrypi.com/categories/1214-rp2350/documents/RP-008373-DS-2-rp2350-datasheet.pdf?disposition=inline

Silva, N. B., Pigatto, D. F., Martins, P. S., & Branco, K. R. (2016). Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer. *Journal of Network and Computer Applications*, *60*, 130–143. https://doi.org/10.1016/j.jnca.2015.10.007

Suarez-Albela, M., Fernandez-Carames, T. M., Fraga-Lamas, P., & Castedo, L. (2018). A Practical Performance Comparison of ECC and RSA for Resource-Constrained IoT Devices. *2018 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/giots.2018.8534575

Systems, E. (2025b,). *ESP32-C3 Series Documentation*. https://documentation.espressif.com/esp32-c3_datasheet_en.pdf

Systems, E. (2025a,). *ESP32-S3 Documentation*. https://documentation.espressif.com/esp32-s3_datasheet_en.pdf

Viljoen, J. L., Goossens, I., Monjazeb, S., Cochrane, D. M., Vargen, L. M., Jonnson, M. R., Blanchard, A. J. E., Li, S. M. Y., & Jackson, J. R. (2024). Are risk assessment tools more accurate than unstructured judgments in predicting violent, any, and sexual offending? A meta-analysis of direct comparison studies. *Behavioral Sciences & the Law*, *43*(1), 75–113. https://doi.org/10.1002/bsl.2698