Assessment of Lightweight Cryptography Algorithms on ARM Cortex-M Processors

Nicolas Moura*[§], Joaquim Lucena*, Eduardo Pereira*, Ney Calazans[†], Luciano Ost[‡],
Fernando Moraes* and Rafael Garibotti*
*School of Technology, Pontifical Catholic University of Rio Grande do Sul – PUCRS – Porto Alegre, Brazil
[§]EnSilica – Porto Alegre, Brazil
[†]PGMicro, Federal University of Rio Grande do Sul – UFRGS – Porto Alegre, Brazil
[‡]Wolfson School, Loughborough University – Loughborough, United Kingdom
{nicolas.moura, joaquim.lucena, eduardo.viana}@edu.pucrs.br, nlvcalazans@inf.ufrgs.br,
l.ost@lboro.ac.uk, fernando.moraes@pucrs.br, rafaelgaribotti@gmail.com

***Abstract*—The proliferation of sensitive information and data processing in the Internet of Things edge and end devices is accelerating at a rapid pace. As a result, ensuring security becomes increasingly crucial. Although encryption is essential, edge devices often cannot accommodate large overheads. This study assesses the efficiency of ten lightweight cryptography (LWC) algorithms by comparing their power consumption, performance, and memory footprints in ARM Cortex architectures. The goal is to guide designers working with LWC and ARM processor architectures. The LWC algorithms, along with the baseline Advanced Encryption Standard (AES), are implemented and executed on ARM Cortex-M processors, intended for edge devices. Results reveal trade-offs associated with cipher properties and the inherent architectural resources of each processing device.**

***Index Terms*—Lightweight Cryptography, Power Consumption, Performance, Memory footprint, ARM Cortex-M processors, Internet of Things.**

I. Introduction

The Internet of Things (IoT) era has brought a proliferation of edge devices into our lives, from simple sensor-based devices in home automation to high-end systems embedded in autonomous vehicles [1]. The growing use of IoT edge devices is mainly due to their improved computing performance and memory resources combined with low power consumption [2].

However, the availability of connected devices everywhere, such as IoT devices, brings security issues to the front line of the underlying system design. IoT end devices are likely to exchange sensitive data. Thus, adopted communication mechanisms must guarantee certain security levels, aiming to avoid, e.g. data corruption, use by non-authorized entities, and denial of service, to name a few existing threats. The use of cryptography is inevitable to achieve security, bringing with it a set of added costs, which then become part of the system design process. An option to reduce cryptography costs is the adoption of lightweight cryptography (LWC) to render the added costs more easily acceptable. Care must be taken, though, since the lighter the cipher, the more it can be successfully attacked [3].

Remembering, end and edge devices are always somehow limited in resources (memory, speed, and power budgets) compared to devices in servers or those accessible through the cloud. Waiting for technology to evolve and provide less restricted devices and techniques is always a choice, but most designs lag behind in time-to-market and cannot consider this option.

A less time-impacting choice is to rely on the right assessment of the available LWC algorithms universe, which is large [4], counting several dozen choices. This is a primary motivation for this work. In addition, most previous works evaluate LWC algorithms from only one perspective, such as performance [5]–[7], energy efficiency [8], [9], and security [3], [10], among others. Many LWC algorithms are available, but most works present performance results in different setups. Thakor et al. [4] suggest a fair comparison between 41 algorithms using seven metrics, including software performance, hardware performance, and others. The present work proposes to evaluate a subset of 10 of these 41 algorithms and compares them in ARM Cortex-M architectures, with the objective of assessing their power, performance, and memory footprint. The final goal is to guide a designer intending to use LWC.

The rest of this paper is organized as follows. Section II reviews related works that assess LWC algorithms on edge devices. Next, Section III justifies the selection of the LWC algorithms subset. Section IV then describes the ARM Cortex-M processor series and boards, presenting the Power-Performance-Area (PPA) assessment method. Section V explores the benefits and drawbacks of each LWC algorithm arising from the experiments, and relates the algorithm singularities to the boards where the evaluation takes place. Finally, Section VI concludes this paper and presents directions for future work.

II. Related Work

Part of the literature has addressed the behavior of LWC algorithms in edge devices [11]–[16]. However, the proposed approaches present drawbacks such as: (*i*) a low number or no end or edge device evaluated; (*ii*) a low number of assessed

This work was financed in part by CAPES (Finance Code 001), CNPq (grants 309605/2020-2, 317087/2021-5, 311587/2022-4 and 407477/2022-5), and FAPERGS (grants 21/2551-0002047-4 and 22/2551-0000570-5).

LWC algorithms; and (*iii*) none covered all PPA metrics. In this regard, the rest of this Section reviews recent works relevant to further put this paper proposal in perspective.

Ledwaba et al. [17] investigate three widely-adopted standard algorithms (AES, ECDSA, and SHA) that target end devices in the Internet of Energy (IoE). Their analysis primarily focuses on a single version of each algorithm, without addressing LWC options. Similar to the current study, Ledwaba et al. utilize ST Microelectronics boards with M0, M3, M4, and M7 ARM cores for their experiments and evaluate the same parameters: performance, power consumption, and memory footprint. However, unlike this study, most of the boards employed by Ledwaba et al. belong to the Discovery family rather than the newer Nucleo family, except the Nucleo board featuring the M7 core. The operating frequencies range from 24MHz for M3 to 216MHz for M7. These Authors conclude that symmetric cryptography is viable for use in endpoint devices, a finding that does not extend to asymmetric cryptography such as ECDSA.

Kane et al. [18] evaluate various combinations of three low-power microcontrollers (ATmega328, STM32F103C8T6, and ESP8266) and three cryptographic algorithms (AES, ChaCha, and Acorn). The Authors assess power consumption, energy usage, execution time, and memory footprint, demonstrating the trade-offs that emerge among processor and cipher selections concerning the evaluated metrics. Additionally, other studies explore five distinct modes of operation for AES and multiple key lengths for all ciphers, which, to some extent, offer a wealth of detail that compensates for the relatively limited selection of distinct ciphers.

Thakor et al. [4] present a comprehensive review of fifty-two lightweight cryptography algorithms or their variations. The Authors provide a description of each cipher and examine the performance of both hardware and software implementations for most algorithms. Additionally, the paper evaluates the relative security of the ciphers and their susceptibility to different attack types. In conclusion, the study recommends further research on substitution-permutation methods involving S-Boxes to develop new ciphers that balance cost, performance, and security.

More recently, Elsadek et al. [19], [20] performed a PPA assessment of ASIC implementations for some of the NIST lightweight cryptography standardization candidates [21]. Mohajerani et al. [22] also proposed a hardware benchmarking of these LWC algorithms. While these Authors focus on assessing the hardware implementation, the present work differs from it, by evaluating the PPA of software-based LWC algorithms using microprocessors devices already used in IoT products. This complementary approach is applicable to existing IoT products and can easily be extended to other LWC algorithms.

Vitor et al. [23] assess the relative performance, area, and soft error reliability trade-offs of two cryptography hardware solutions implemented in FPGA. Different from previous works, this paper brings to light a thorough PPA assessment for a substantial set of LWC algorithms running on ARM Cortex-M processors, widely used in areas where secure end/edge devices are critical, e.g. in the medical and personal IoT device market [24].

III. Selected Lightweight Cryptography (LWC)

This work focuses on a collection of eleven symmetric cryptography algorithms, comprising ten strictly lightweight cryptography (LWC) algorithms and the widely recognized Advanced Encryption Standard (AES) algorithm, which serves as a reference. This Section provides a concise overview of the origins and primary characteristics of these ciphers. Table I outlines the specifics of each selected cipher, including the year of introduction and associated standards, when available. Additionally, the Table presents the fundamental block length and key length option choices. To encourage replication and validation of the results by other researchers, the source codes for the LWC algorithms can be accessed on GitHub[1].

TABLE I
Information of Lightweight Cryptography Algorithms.

Work	**Cryptography Standard**	**Block Length (bits)**	**Key Length (bits)**
AES [25] (2001)	ISO/IEC 18033-3:2010	128	128, 192, 256
ARIA [26] (2003)	KS X 1213-1	128	128, 192, 256
CAMELLIA [27] (2004)	ISO/IEC 18033-3:2010	128	128, 192, 256
GOST [28] (2010)	GOST 28147-89	64	256
HIGHT [29] (2005)	ISO/IEC 18033-3:2010	64	128
IDEA [30] (1991)	———	64	128
NOEKEON [31] (2000)	———	128	128
PRESENT [32] (2007)	ISO/IEC 29192-2:2019	64	128
SEED [33] (1999)	ISO/IEC 18033-3:2010	128	128
SIMON [34] (2013)	ISO/IEC 29167-21:2018	128	128, 192, 256
SPECK [34] (2013)	ISO/IEC 29167-22:2018	128	128, 192, 256

The choice for addressing only symmetric ciphers relies on characteristics such as higher performance, smaller memory footprint, and better adaptability to run on large data sets when comparing symmetric to asymmetric algorithms (e.g. RSA or elliptic curve ciphers). Also, often symmetric ciphers consume less power to execute than asymmetric ones. This power efficiency characteristic is crucial when deploying LWC algorithms in embedded systems used for IoT applications [35].

The selected ciphers cover distinct cryptography use sectors, like research institutes, governments, and industrial applications, as well as various standards bodies (e.g., ISO, KS). The algorithms are often implemented as software modules [17], sanctioning an easiness to use them massively in IoT devices.

Besides the reference algorithm, *AES* [25], most of the chosen LWC algorithms qualify as agreed standards. *ARIA* [26] and *HIGHT* [29] are approved by the South Korean standardization body (KS). The former finds application in government services to the public, while the latter is part of the international ISO/IEC 18033 standard. HIGHT is sought

[1] Available at: https://github.com/nicolasMoura25/cryptography-algorithms.

to provide ultra-low power consumption, mainly comprising basic operations supported in software (and hardware).

Also part of the ISO/IEC 18033 standard are *CAMELLIA* [27] and *SEED* [33]. The former was proposed to enable low-cost hardware and software building in devices counting with significantly constrained resources. SEED, in turn, is primarily employed in the South Korean industry.

Proposed in Russia as an alternative to AES-256 and triple DES, *GOST* [28] targets low use of resources. Another DES replacement alternative is *IDEA* [30]. At the time of its proposal, in the last decade of the previous century, IDEA was claimed to be the most secure successor to DES. *NOEKEON* [31] is a cipher that stands out due to the compactness and simplicity of its implementations. It also shows good resistance against certain attack classes.

Finally, the LWC subset comprises three ciphers of ISO/IEC standards distinct from the already mentioned ISO/IEC 18033. *PRESENT* [32] is an ultra-lightweight cipher with a code footprint typically 2.5× smaller than AES. It is part of ISO/IEC 29192. The last two ciphers are *SIMON* [34] and *SPECK* [34], both part of the ISO/IEC 29167 standard. The USA-based National Security Agency (NSA) is responsible for the first release of these. The LWC algorithm SIMON targets high-performance hardware construction, while SPECK is intended for software-optimized implementations.

IV. PPA Assessment Methods

This Section describes the method used to assess the *power*, *performance*, and memory footprint of lightweight cryptography algorithms on ARM Cortex-M processors. The memory footprint of the algorithms is used as an *area* indicator here. Accordingly, this work calls the method a *PPA assessment*. First, the adopted ARM Cortex-M processors and associated boards are presented. Next, takes place a description and discussion of the proposed evaluation metrics.

A. ARM Cortex-M Processors

The ARM Cortex-M processor series enables developers and engineers to create cost-sensitive and power-constrained solutions for many fields where embedded systems are critical, such as the automotive and medical IoT markets [24]. From these, STMicroelectronics developed a family of ARM Cortex-M processor-based boards (called STM32-Nucleo) [36], which allows developers to try out new ideas and quickly create prototypes with any supported ARM Cortex-M processor. This work relies on such boards to evaluate the PPA of lightweight cryptography algorithms and suggests the best solutions for secure embedded applications.

Specifically, the target here is to use four development boards, based on medium- (M3, M4, M33) and high-performance (M7) ARM Cortex-M processors. See Table II for data about the used boards.

TABLE II
ARM Cortex-M Board Configurations.

Processor	**ARM Cortex-M3**	**ARM Cortex-M4***	**ARM Cortex-M7**	**ARM Cortex-M33**
MCU (STM32-)	F207ZGT6	L476RGT6U	H745ZIT6	L552ZET6Q
Clock (MHz)	120	80	400	110
Flash (KB)	1,024	1,024	2,048	512
RAM (KB)	128	128	1,024	256
I Cache (KB)	none	none	16	8
D Cache (KB)	none	none	16	none
Cache	none	none	I & D	I

*Low-power M4 version.

- The entry processor is the ARM Cortex-M3, a medium-performance processor that implements the ARMv7-M architecture. M3 is commonly found across several smart home devices and has been deployed in billions of products, such as automotive body systems and wireless networks.
- Next comes a low-power version of ARM Cortex-M4, another medium-performance processor that implements the ARMv7-M architecture. M4 addresses digital signal control markets that require an efficient, easy-to-use combination of control and signal processing capabilities. Such features make it highly regarded in the industry, with a presence in motor control, automotive, power management, embedded audio, and industrial automation markets.
- The ARM Cortex-M7 is the highest-performance processor core with an ARMv7-M architecture. Built-in floating-point processing reduces power consumption, and its DSP capability makes this processor the choice for more intensive automation tasks.
- Finally, ARM Cortex-M33 is a medium-performance processor based on the more modern ARMv8-M architecture. It was designed to address embedded and IoT markets, especially those that require efficient security or digital signal control, thanks to TrustZone software isolation support.

B. Power-Performance-Area Metrics

A USB current tester [37] was used to measure the *power* consumption of the tested boards. For the *performance* analysis of each LWC algorithm, a message of approximately 13kB (807 128-bit blocks) was encrypted. This message size was based on a packet size commonly used in agricultural applications [38]. The *performance* metric corresponds to the time required to process the entire message for each LWC algorithm. Memory footprint refers to the primary memory consumed by the LWC algorithm, indicating the runtime memory requirements. The external library and program codes are accounted for separately, and their sum defines the total memory footprint for each ARM Cortex-M board (an indirect *area* estimation).

V. Results

This Section assesses the PPA of the eleven cryptography algorithms on ARM Cortex-M processors. First, Figure 1 compares the execution time of each algorithm, where key length variations have been included to allow identifying the performance penalties brought by a more secure cryptography. What

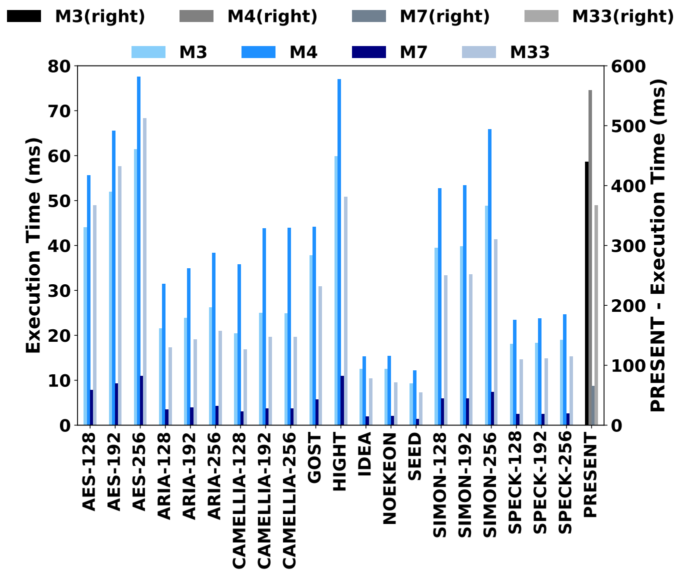

Fig. 1. Performance comparison of the eleven LWC algorithms.

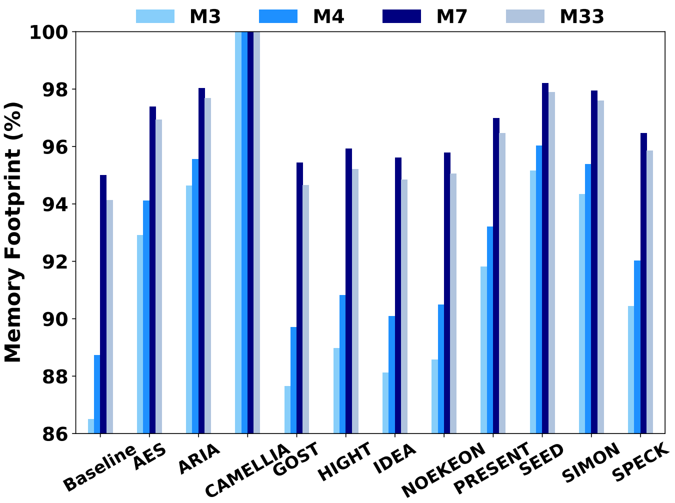

Fig. 2. Memory footprint of the eleven LWC algorithms, highlighting the basic libraries (baseline) required for each ARM Cortex-M board.

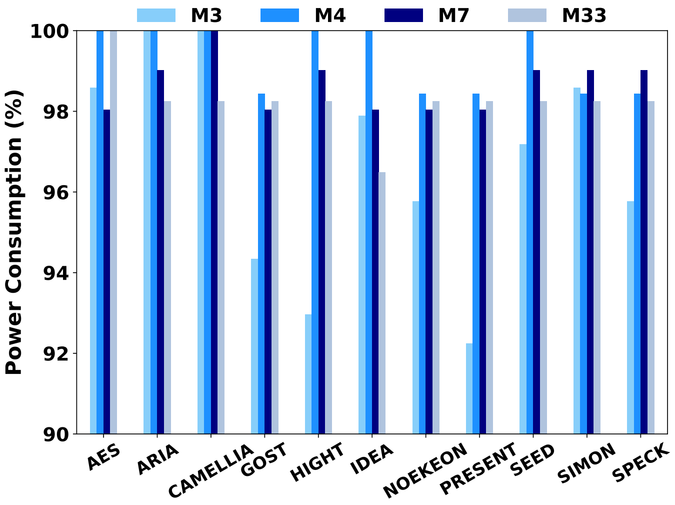

Fig. 3. LWC algorithms' power consumption for each ARM Cortex-M board.

stands out the most is the poor performance of PRESENT, even compared to the non-LWC AES, making it necessary to create a right y-axis in Figure 1 just for it. PRESENT has a 15× slower encryption round than SIMON. Although it runs only 31 rounds against the 69 rounds of SIMON, the slowest process remains the performance bottleneck of this LWC algorithm. Overall, SEED performs best on all boards, followed by IDEA and NOEKEON. Also, key length affects performances differently. While the AES runtime has an average penalty of 39% from 128 to 256 bits in key length, SPECK increases by only 4.7% on average. Regarding ARM Cortex-M boards, results show ARM Cortex-M7 has the best performance, taking less than 11ms to run any LWC algorithm. Next come ARM Cortex-M33, ARM Cortex-M3, and ARM Cortex-M4, with an average runtime of 5.5×, 6.1×, and 8.3× the ARM Cortex-M7 execution time, respectively.

Figure 2 shows the memory footprint percentage of each evaluated cryptography algorithm, where the 100% reference is the CAMELLIA memory occupation, the LWC algorithm which takes more memory among those assessed in this work for all employed processors. GOST has the lowest memory footprint, ranging from 48.25kB (in ARM Cortex-M3) to 142.41kB (in ARM Cortex-M7). It was followed by IDEA and NOEKEON with 48.50kB and 48.75kB on ARM Cortex-M3, respectively. It is worth mentioning that Figure 2 also has a baseline reference for functions and libraries (source code) required to execute the cryptography algorithm in an ARM Cortex-M board. Results show the ARM Cortex-M3 has the lowest baseline memory footprint percentage compared to other ARM Cortex-M boards. This refers to 47.61kB, 58.55kB, 119.40kB and 171.77kB of memory occupancy on ARM Cortex-M3, ARM Cortex-M4, ARM Cortex-M33 and ARM Cortex-M7, respectively.

Figure 3 shows the power consumption percentage for each cryptography algorithm on four ARM Cortex-M boards. Note that the 100% reference of each bar refers to the most consuming algorithm on each ARM Cortex-M board. The results also show a very slight power variation among all LWC algorithms. Overall, PRESENT has the lowest power consumption, followed by HIGHT and GOST. It is interesting to observe the difference in power consumption of some cryptography algorithms when switching boards. For example, AES has the lowest power consumption for the ARM Cortex-M7 board. However, it has the highest power consumption for the ARM Cortex-M33 board. This is due to some ARM Cortex-M7 features better employed by AES, such as built-in floating-point processing.

Table III summarizes a ranking for all algorithms, consolidating the information collected on all ARM Cortex-M boards.

The rating ranges from 1 to 11, where 1 is the best, and 11 is the worst cryptography algorithm for a specific metric. For example, 1 in performance means the fastest execution

TABLE III
SUMMARY OF CRYPTOGRAPHY ALGORITHMS' RANK.

LWC	Power Consumption				Performance				Memory Footprint			
	M3	M4	M7	M33	M3	M4	M7	M33	M3	M4	M7	M33
AES	8	6	1	11	9	9	9	9	7	7	7	7
ARIA	10	6	6	2	6	5	6	6	9	9	9	9
CAMELLIA	10	6	11	2	5	6	5	5	11	11	11	11
GOST	3	1	1	2	7	7	7	7	1	1	1	1
HIGHT	2	6	6	2	10	10	10	10	4	4	4	4
IDEA	7	6	1	1	2	2	2	3	2	2	2	2
NOEKEON	4	1	1	2	3	3	3	2	3	3	3	3
PRESENT	1	1	1	2	11	11	11	11	6	6	6	6
SEED	6	6	6	2	1	1	1	1	10	10	10	10
SIMON	8	1	6	2	8	8	8	8	8	8	8	8
SPECK	4	1	6	2	4	4	4	4	5	5	5	5

TABLE IV
RECOMMENDED CRYPTOGRAPHY ALGORITHMS, BY PROCESSOR.

Processor	Power Consumption	Performance	Memory Footprint	Energy
M3	PRESENT HIGHT GOST	SEED IDEA NOEKEON	GOST IDEA NOEKEON	SEED NOEKEON IDEA
M4	GOST NOEKEON PRESENT	SEED IDEA NOEKEON	GOST IDEA NOEKEON	SEED NOEKEON IDEA
M7	GOST IDEA NOEKEON	SEED IDEA NOEKEON	GOST IDEA NOEKEON	SEED IDEA NOEKEON
M33	IDEA ARIA CAMELLIA	SEED NOEKEON GOST	GOST IDEA NOEKEON	SEED NOEKEON IDEA

time, and 11 in the area means the largest code size. In terms of performance and area, the ranking remained constant for almost all LWC algorithms, except for minor variations such as the reversed order of IDEA and NOEKEON in performance on the M7 and M33 boards, as well as the inversion of position in performance for ARIA and CAMELLIA on the M3 and M4 boards. Table III makes it clear that the power consumption rank also varies according to the characteristics of the ARM Cortex-M board, as already discussed above for AES rankings.

Table IV ranks the top three algorithms for each feature, offering a rapid analysis for designers to select the most suitable LWC algorithm for a given ARM architecture. It should be noted that an additional column, energy, has been included, which represents the product of processing time and average power. Energy is a crucial metric in embedded applications, as it determines the required battery capacity.

VI. Conclusion and Future Work

This paper evaluated the power consumption, performance, and memory footprint of ten lightweight cryptography algorithms, along with the baseline AES cipher, when executed on four ARM Cortex-M boards.

Results indicate that GOST has the smallest memory footprint, while SEED is the most energy-efficient and demonstrates superior performance across all ARM Cortex-M boards. For example, the SEED algorithm is recommended if a designer works with a Cortex-M4 and prioritizes performance. However, if a more balanced trade-off among all constraints is desired, results suggest NOEKEON as a more suitable option, providing a good equilibrium for ARM architectures.

Another conclusion that may be extracted from the results is that the performance of AES was worse than most of the algorithms for these boards. This outcome is expected since AES is not a lightweight cryptography algorithm.

Future work includes assessing high-end processors, such as the ones found in Raspberry Pi boards (e.g., ARM Cortex-A53 and ARM Cortex-A72), a direct comparison with NIST LWC finalist candidates, and also taking into account other metrics such as reliability and cipher security.

A clear issue that requires enhancement is the power measurement method employed in the experiments, which relied on taking the whole current demanded from each board supply source. This clearly masks the specific power related to each algorithm and somehow reduces the relevance of the obtained power results for comparing the algorithms. A better way to measure or estimate the contribution of each LWC algorithm to power consumption is ongoing work.

References

[1] Z. Guo, N. Karimian, M. M. Tehranipoor, and D. Forte, "Hardware Security Meets Biometrics for the Age of IoT," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016, pp. 1318–1321.

[2] V. da Rocha, N. Moura, J. Gava, V. Bandeira, L. Ost, R. Reis, and R. Garibotti, "Soft Error Reliability Assessment of Lightweight Cryptographic Algorithms for IoT Edge Devices," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2022, pp. 1–4.

[3] A. Baksi, S. Bhasin, J. Breier, D. Jap, and D. Saha, "A Survey on Fault Attacks on Symmetric Key Cryptosystems," *ACM Computing Surveys*, vol. 55, no. 4, pp. 86:1–86:34, May 2023.

[4] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021.

[5] T. Wan and E. Salman, "Ultra Low Power SIMON Core for Lightweight Encryption," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2018, pp. 1–5.

[6] Z. Jiang, H. Jin, G. E. Suh, and Z. Zhang, "Designing Secure Cryptographic Accelerators with Information Flow Enforcement: A Case Study on AES," in *ACM/IEEE Design Automation Conference (DAC)*, 2019, pp. 1–6.

[7] S. Taneja and M. Alioto, "Deep Sub-pJ/Bit Low-Area Energy-Security Scalable SIMON Crypto-Core in 40 nm," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–5.

[8] B. J. Mohd and T. Hayajneh, "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques," *IEEE Access*, vol. 6, pp. 35 966–35 978, 2018.

[9] A. Singh, N. Chawla, J. H. Ko, M. Kar, and S. Mukhopadhyay, "Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-Edge Nodes," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 421–434, 2019.

[10] M. Stute, P. Agarwal, A. Kumar, A. Asadi, and M. Hollick, "LIDOR: A Lightweight DoS-Resilient Communication Protocol for Safety-Critical IoT Systems," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6802–6816, 2020.

[11] A. I. Regla and E. D. Festijo, "Performance Analysis of Light-weight Cryptographic Algorithms for Internet of Things (IoT) Applications: A Systematic Review," in *IEEE International Conference for Convergence in Technology (I2CT)*, 2022, pp. 1–5.

[12] A. Beg, T. Al-Kharobi, and A. Al-Nasser, "Performance Evaluation and Review of Lightweight Cryptography in an Internet-of-Things Environment," in *International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–6.

[13] A. Akbas, "Comparative Analysis of Lightweight Cryptography Algorithms on Resource Constrained Microcontrollers," in *International Informatics and Software Engineering Conference (UBMYK)*, 2019, pp. 1–4.

[14] A. Elaguech, A. Kchaou, W. El Hadj Youssef, K. Ben Othman, and M. Machhout, "Performance Evaluation of Lightweight Block Ciphers in Soft-core Processor," in *International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 2019, pp. 101–105.

[15] S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganne, and R. Tourki, "Performance Evaluation and Design Considerations of Lightweight Block Cipher for Low-Cost Embedded Devices," in *IEEE/ACS International Conference of Computer Systems and Applications (AICCSA)*, 2016, pp. 1–7.

[16] C. A. Lara-Niño, M. Morales-Sandoval, and A. Díaz-Pérez, "An Evaluation of AES and PRESENT Ciphers for Lightweight Cryptography on Smartphones," in *International Conference on Electronics, Communications and Computers (CONIELECOMP)*, 2016, pp. 87–93.

[17] L. P. I. Ledwaba, G. P. Hancke, H. S. Venter, and S. J. Isaac, "Performance Costs of Software Cryptography in Securing New-Generation Internet of Energy Endpoint Devices," *IEEE Access*, vol. 6, pp. 9303–9323, 2018.

[18] L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. Mckague, "Security and Performance in IoT: A Balancing Act," *IEEE Access*, vol. 8, pp. 121 969–121 986, 2020.

[19] I. Elsadek, S. Aftabjahani, D. Gardner, E. MacLean, J. R. Wallrabenstein, and E. Y. Tawfik, "Hardware and Energy Efficiency Evaluation of NIST Lightweight Cryptography Standardization Finalists," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2022, pp. 133–137.

[20] ——, "Energy Efficiency Enhancement of Parallelized Implementation of NIST Lightweight Cryptography Standardization Finalists," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2022, pp. 138–141.

[21] NIST, "Lightweight Cryptography: Project Overview," 2022. [Online]. Available: https://csrc.nist.gov/projects/lightweight-cryptography

[22] K. Mohajerani, R. Haeussler, R. Nagpal, F. Farahmand, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Hardware Benchmarking of Round 2 Candidates in the NIST Lightweight Cryptography Standardization Process," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021, pp. 164–169.

[23] V. Bandeira, J. Sampford, R. Garibotti, M. G. Trindade, R. P. Bastos, R. Reis, and L. Ost, "Impact of radiation-induced soft error on embedded cryptography algorithms," *Microelectronics Reliability*, vol. 126, pp. 1–5, 2021.

[24] S. Cadario, "New Arm Virtual Hardware for the entire IoT ecosystem," 2022. [Online]. Available: https://community.arm.com/arm-community-blogs/b/internet-of-things-blog/posts/new-arm-virtual-hardware

[25] NIST, "Advanced Encryption Standard (AES)," Federal Information Processing Standard Publication (FIPS PUBS) FIPS 197, 2001.

[26] D. Kwon, J. Kim, S. Park, S. H. Sung, Y. Sohn, J. H. Song, Y. Yeom, E.-J. Yoon, S. Lee, J. Lee, S. Chee, D. Han, and J. Hong, "New Block Cipher: ARIA," in *Information Security and Cryptology (ICISC)*, 2004, pp. 432–445.

[27] M. Matsui, J. Nakajima, and S. Moriai, "A Description of the Camellia Encryption Algorithm," *RFC3713*, pp. 1–15, Apr. 2004.

[28] V. Dolmatov, "GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms," *RFC5830*, pp. 1–19, 2010.

[29] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "HIGHT: A New Block Cipher Suitable for Low-Resource Device," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2006, pp. 46–59.

[30] X. Lai, "On the Design and Security of Block Ciphers," Ph.D. dissertation, ETH Zürich, 1992.

[31] J. Daemen, M. Peeters, G. Assche, and V. Rijmen, "Nessie proposal: NOEKEON," in *New European Schemes for Signatures, Integrity and Encryption (NESSIE)*, 2000, pp. 213–230.

[32] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2007, pp. 450–466.

[33] H. J. Lee, S. J. Lee, J. H. Yoon, D. H. Cheon, and J. I. Lee, "The SEED Encryption Algorithm," *RFC4269*, pp. 1–16, 2005.

[34] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," Cryptology ePrint Archive, Tech. Rep., 2013.

[35] R. Garibotti, L. Ost, A. Butko, R. Reis, A. Gamatié, and G. Sassatelli, "Exploiting memory allocations in clusterised many-core architectures," *IET Computers & Digital Techniques*, vol. 13, no. 4, pp. 302–311, 2019.

[36] STMicroelectronics, "STM32 Nucleo Boards," 2022. [Online]. Available: https://www.st.com/en/evaluation-tools/stm32-nucleo-boards.html

[37] Keweisi, "Keweisi KWS-MX18 USB tester," 2022. [Online]. Available: https://elektro.turanis.de/html/prj125/Keweisi%20KWS-MX18%20-%20User%20Manual.pdf

[38] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk," *IEEE Access*, vol. 7, pp. 129 551–129 583, 2019.