Analysis of Selected Cryptographic Algorithms for Data Transmission in Airborne Networks

Szymon Baliński, Paweł Śniatała,
Maciej Sobieraj, Anna Grocholewska-Czuryło
Poznan University of Technology
Poznan, Poland
szymon.balinski@put.poznan.pl

Junfei Xie, Shangping Ren
San Diego State University
San Diego, USA
{jxie4, sren}@sdsu.edu

***Abstract*—The article presents an analysis of selected cryptographic algorithms for their application in data transmission in airborne networks, as well as other devices that use microcontrollers, such as Internet of Things (IoT) devices. Different types of microcontrollers used in Unmanned Aerial Vehicle (UAV) platforms are presented. The ESP32 microcontroller is used for hardware testing. A selected set of lightweight cryptography algorithms is implemented in the microcontroller to test their computational efficiency. The tests for AEAD algorithms include: ChaChaPoly, ASCON-128, TinyJAMBU, ISAP, and PHOTON-Beetle, and for Hashing algorithms: BLAKE2s, ASCON-HASH, and PHOTON-Beetle-HASH.**

***Keywords*—Lightweight Cryptography, Microcontrollers, UAV**

I. Introduction

This paper presents an analysis of a selected set of lightweight cryptographic algorithms in terms of their applications in data transmission in airborne networks. We analyze different types of microcontrollers as possible hardware platforms to apply the chosen algorithms. However, the conclusions obtained from the presented research are not only applicable to airborne networks, as illustrated in Fig. 1 but can also be a guide for the implementation of data encryption in other devices that use microcontrollers, such as Internet of Thing (IoT) devices.

The increasing adoption of IoT devices in recent years has enhanced the convenience of our daily lives, yet has also brought significant security and privacy challenges [1], [2], [3]. IoT devices are typically compact printed circuit boards embedded with a variety of sensors, which enable them to collect and process data from their surroundings. These devices are designed to communicate wirelessly, either with larger systems, such as centralized servers or gateways, or directly with other IoT devices, using technologies such as Wi-Fi, Bluetooth, Zigbee, or other low-power communication protocols.

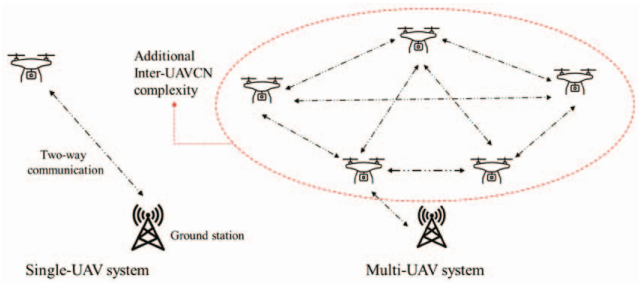

Fig. 1. Example UAV connections

Functionally, IoT devices are capable of sensing environmental parameters, performing computations, storing relevant data, and transmitting information across networks. Their applications span multiple domains, including industrial automation, smart cities, agriculture, healthcare, home automation, and surveillance. In specific use cases, such as monitoring patient health, securing residential or commercial spaces, and automating home environments, the data generated by these devices can be highly sensitive. Consequently, ensuring the confidentiality, integrity, and security of this data is crucial. To address these concerns, robust data protection mechanisms, including encryption, access control, authentication protocols, and secure data transmission techniques, must be implemented to safeguard user privacy and prevent unauthorized access or cyber threats. In fact, almost the same can characterize UAVs, which often are just mobile platforms that carry sensors or IoT devices [4].

Cryptographic performance is critical in various applications, including secure communication, data protection, and authentication. By evaluating encryption and decryption speeds for both large (128 bytes) and small (16 bytes) packets, we can determine which algorithms are best suited for high-performance environments and constrained devices. This paper presents an analysis of the performance of various cryptographic algorithms, focusing on their encryption, decryption, and hashing speeds. The goal is to compare different algorithms in terms of their efficiency when handling different data sizes. The study includes Authenticated Encryption with Associated Data (AEAD) algorithms and cryptographic hash functions. We have focused on lightweight cryptography, which is suitable for implementation on microcontrollers.

The rest of the article is organized as follows. An Introduction introduces UAVs as platforms that carry different sensors and/or IoT devices. Section II presents different microcontrollers that are commonly found in UAVs. Next, a performance analysis of cryptographic algorithms implemented in

the ESP32 microcontroller is presented in Section III. It includes introduction of lightweight cryptography, methodology, testing environment, and results. The last section summarizes the results achieved and briefly outlines the further planned work.

II. Microcontrollers Used in UAVs

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have revolutionized numerous industries due to their versatility and accessibility. At the heart of every UAV is a sophisticated integration of hardware components and microcontroller platforms that enable flight control, navigation, communication, and mission execution.

One of the most important elements is the communication system, which represents a critical component in multi-UAV operations, enabling coordination, data sharing, and collective intelligence among UAVs. Microcontrollers serve as the foundational building blocks for implementing these communication networks, balancing processing capabilities with power efficiency to enable effective and secure inter-UAV communication.

In the case of effective inter-UAV communication, systems require microcontrollers that balance processing power, energy efficiency, and peripheral capabilities. The following microcontroller families are commonly deployed in the implementation of various types of systems used in UAVs, each offering unique advantages for different operational requirements.

- PIC Microcontrollers (PIC18F Series). Offer a good balance between performance and power efficiency. They are often used in small UAVs which have strict power constraints. Their key advantages include: extremely low-power sleep, integrated peripherals for common communication protocols, and suitable for simple mesh networking implementations [5], [6].
- ESP32 platform (ESP32-S3 or ESP32-C3). The advantages of using that systems include: integrated RF capabilities that eliminate the need for external transceivers, support for mesh networking protocols like ESP-MESH, and up to 240 MHz clock speeds with extensive sleep modes. ESP32 is the dedicated hardware for AES encryption and SHA hashing [7], [8].
- MSP430 Family (MSP430FR Series). Their key functionalities include: ultra-low power with FRAM technology, extremely efficient sleep modes with fast and wake-up, ideal for intermittent communication scenarios, clock speeds ranging from sub-MHz to 24 MHz. These systems are popular for energy-harvesting UAV applications [9], [10].
- STM32 Family (STM32F4, STM32L4, STM32H7 series). The main features of these microcontrollers include: an extensive peripheral set supporting multiple UART, SPI, I2C, and CAN interfaces; hardware cryptographic accelerators for secure communications; DMA controllers for efficient data handling; and clock speeds ranging from 32 to 480 MHz [11], [12].

The significance of communication security has led to extensive research on scalable and modular encryption methods. For many IoT security applications, the use of lightweight and specialized cryptographic techniques is highly recommended due to their efficiency and adaptability. In cryptography, microcontrollers equipped with hardware cryptographic gas pedals or security modules are often used to encrypt data. The most popular microcontrollers used for this purpose include:

- STM32 (STMicroelectronics),
- ESP32 (Espressif Systems),
- NXP i.MX RT and LPC,
- Nordic Semiconductor nRF52, nRF53,
- Microchip PIC32 and ATSAM,
- Texas Instruments MSP430 and TM4C.

In [13], an investigation was conducted to verify the possibility of applying security measures such as strong encryption without hindering the performance of IoT devices. A comprehensive experimental performance evaluation was performed that examined the encryption of DTLS-based network traffic in STM32 Nucleo.

The analysis of the performance of AES, with and without hardware acceleration, and XTEA algorithms, comparing their memory usage, power consumption, and execution times, to determine whether XTEA is viable for resource-constrained embedded platforms, was presented in [14].

The work [15] evaluated the efficiency of ten lightweight cryptography (LWC) algorithms by comparing their power consumption, performance, and memory requirements in ARM Cortex architectures, providing practical guidance to designers implementing LWC solutions on ARM processors.

The research by [16] investigated the security of IoT data, specifically developing cryptographic algorithms optimized for the resource-limited ESP32 microcontroller. The project created a lightweight block cipher drawing inspiration from established algorithms such as AES and DES, with performance evaluations conducted to achieve an optimal balance between security strength and computational efficiency.

Taking into account the analysis of the literature on the subject, as well as the requirements for computing power and energy savings through particular microcontrollers, the authors decided to use the ESP32 microcontroller as a hardware platform, which can be used in the UAV to encrypt data transmission. This device was used in practical tests described in the next section.

III. Performance Analysis of Cryptographic Algorithms on ESP32

A. Lightweight cryptography applications

A lightweight cryptography refers to a cryptosystem with low computational cost and suitable for devices with limited resources. The concept was initiated by the National Institute of Standards and Technology (NIST) to develop a cryptographic algorithm that can work with small electronic devices in the IoT environment. Different criteria can be taken into account when choosing the appropriate algorithm for a particular application. Key criteria include:

- Security: cryptographic resistance, key and block length, analysis and verification
- Performance: capacity, delay
- Resource consumption: memory, energy
- Implementation complexity: ease of implementation, potential errors
- Resistance to side-channel attacks: physical attacks, protection measures
- Licensing and intellectual property: licensing, open source
- Compliance with standards: international standards, interoperability
- Scalability and flexibility: adaptability, support for different platforms
- Implementation experience: case studies, community and support.

B. Methodology

This evaluation focuses on benchmarking lightweight cryptography algorithms under controlled conditions. As a result of our experiments, we wanted to compare different cryptography algorithms which would be suitable to implement on a UAV platform. The study includes a range of cryptographic algorithms, divided into two categories:

- AEAD algorithms: These algorithms provide confidentiality and authenticity in encryption. The tested AEAD algorithms include ChaChaPoly, ASCON-128, TinyJAMBU, ISAP, and PHOTON-Beetle.
- Hashing algorithms: These ensure data integrity and are widely used in digital signatures and authentication mechanisms. The tested hashing algorithms include BLAKE2s, ASCON-HASH, and PHOTON-Beetle-HASH.

The evaluation metrics used to measure their performance are the encryption, decryption, and hashing times in microseconds per byte. Each algorithm is tested for two data sizes: 128 bytes (larger packets) and 16 bytes (smaller packets) to assess performance variations with different input lengths. The execution time is converted into throughput (bytes per second) to facilitate direct comparison.

C. Testing environment

The tests were carried out in a microcontroller-based environment, simulating the constraints found in embedded and IoT systems. All benchmarks were performed under the same conditions to ensure consistency in the results. Masked versions of some AEAD algorithms were also tested to compare the impact of security enhancements on performance. By following this methodology, we ensure that the results reported accurately reflect the efficiency of each cryptographic algorithm in different operational contexts. The tests were carried out on the ESP32 microcontroller, a widely used low-power system-on-chip (SoC) designed for embedded and IoT applications. The ESP32 was chosen because of its balance between performance and energy efficiency, which makes it a suitable platform for cryptographic operations in constrained environments. The specifications of this particular microcontroller are summarized as follows:

- Processor: Dual-core Xtensa LX6 @ 240 MHz
- Memory: 520 KB SRAM
- Flash Storage: Up to 16 MB (varies by model)
- Crypto Acceleration: Hardware support for AES, SHA, and RSA
- Connectivity: Wi-Fi, Bluetooth Low Energy (BLE)

ESP32 provides built-in cryptographic acceleration, which improves the performance of algorithms such as AES and SHA. However, software-based implementations of other cryptographic schemes may exhibit different performance characteristics due to CPU limitations. The benchmarks were executed using the standard ESP-IDF framework with optimized compiler settings. The low-power nature of the microcontroller makes it suitable for real-world IoT applications where cryptographic efficiency is crucial. The results obtained from the ESP32 platform provide a realistic assessment of how cryptographic algorithms perform in embedded systems. Understanding these results allows for better selection of cryptographic methods in ESP32-based devices, optimizing security while maintaining system efficiency.

D. Results

Table I presents the performance results of the cryptographic algorithms evaluated. The metrics include encryption and decryption times in microseconds per byte and throughput in bytes per second. The results highlight significant

TABLE I
THE PERFORMANCE RESULTS OF THE EVALUATED ALGORITHMS.

Algorithm	Operation	Time/Byte (μs)	Throughput (bytes/sec)
ChaChaPoly	Encrypt 128B	0.53	1,904,450.16
ChaChaPoly	Decrypt 128B	0.63	1,583,570.46
ChaChaPoly	Encrypt 16B	1.76	569,320.73
ChaChaPoly	Decrypt 16B	1.94	516,768.05
ASCON-128	Encrypt 128B	0.83	1,212,040.87
ASCON-128	Decrypt 128B	0.89	1,120,575.70
ASCON-128	Encrypt 16B	2.33	429,799.43
ASCON-128	Decrypt 16B	2.26	442,988.33
TinyJAMBU-128	Encrypt 128B	0.89	1,125,106.58
TinyJAMBU-128	Decrypt 128B	0.99	1,010,332.23
TinyJAMBU-128	Encrypt 16B	1.55	644,641.42
TinyJAMBU-128	Decrypt 16B	1.70	588,372.29
PHOTON-Beetle-128	Encrypt 128B	9.32	107,284.45
PHOTON-Beetle-128	Decrypt 128B	9.42	106,211.73
PHOTON-Beetle-128	Encrypt 16B	16.56	60,375.84
PHOTON-Beetle-128	Decrypt 16B	16.73	59,781.80
BLAKE2s	Hash 1024B	0.21	4,775,473.47
BLAKE2s	Hash 128B	0.21	4,679,260.46
BLAKE2s	Hash 16B	0.87	1,149,817.65
ASCON-HASH	Hash 1024B	1.07	935,734.08
ASCON-HASH	Hash 128B	1.33	750,267.80
ASCON-HASH	Hash 16B	3.45	290,127.07
PHOTON-Beetle-HASH	Hash 1024B	32.34	30,918.36
PHOTON-Beetle-HASH	Hash 128B	30.57	32,717.09
PHOTON-Beetle-HASH	Hash 16B	16.33	61,230.43

differences in performance between different cryptographic schemes. Some key observations include the following:

- ChaChaPoly demonstrated the highest throughput for both encryption and decryption when processing 128-byte messages, reaching approximately 1.9 MB/s and 1.58 MB/s, respectively. However, its performance significantly deteriorated with smaller inputs (16 bytes), where throughput dropped below 600 KB/s. This indicates a sensitivity to input size that may impact real-time applications handling short messages.
- ASCON-128 offered balanced performance and relatively consistent throughput in different input sizes. For 128B input, it achieved around 1.2 MB/s in encryption and 1.1 MB/s in decryption. For 16B blocks, throughput dropped to about 430–440 KB/s. Although not as fast as ChaChaPoly, its stability and lightweight design make it suitable for embedded environments.
- TinyJAMBU-128 performed similarly to ASCON-128 for larger inputs, but was notably more efficient with smaller data. For 16-byte messages, it outperformed ASCON, reaching throughput values of approximately 645 KB/s (encryption) and 588 KB/s (decryption). These results highlight its effectiveness in constrained scenarios with frequent short data transmissions.
- PHOTON-Beetle-128 exhibited the lowest performance among all encryption schemes evaluated. Even at 128 bytes, its throughput did not exceed 110 KB/s, and at 16 bytes, it dropped to just under 60 KB/s. Despite its lightweight profile, the limited throughput may restrict its applicability to highly specialized use cases where computational performance is secondary.
- BLAKE2s clearly outperformed all other hash functions, maintaining throughput above 4.7 MB/s for 128B and 1024B inputs, and still exceeding 1.1 MB/s for 16B messages. This level of performance, combined with its cryptographic strength, makes it a strong candidate for general-purpose hashing even in lightweight applications.
- ASCON-HASH showed moderate results, achieving throughput between 935 KB/s (1024B) and 290 KB/s (16B). Its performance degrades with smaller inputs, but remains acceptable for lightweight cryptographic needs.
- PHOTON-Beetle-HASH was the slowest among all hash functions. With throughput ranging from 30 KB/s for 1024B to 61 KB/s for 16B inputs, it is clearly not designed for throughput-sensitive applications and is more appropriate in extremely resource-limited devices where size and power consumption take precedence over speed.

Performance decreases significantly for smaller data packets in all algorithms.

We have also compared masked and unmasked versions of AEAD algorithms and assessed their suitability for different security applications. Fig. 2 presents the performance of AEAD algorithms in encryption and decryption scenarios. The comparison is based on the execution time and throughput for large and small packets.

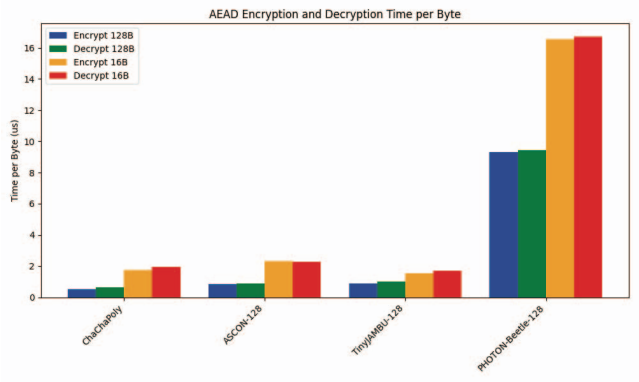

Fig. 2. AEAD algorithms in encryption and decryption scenarios

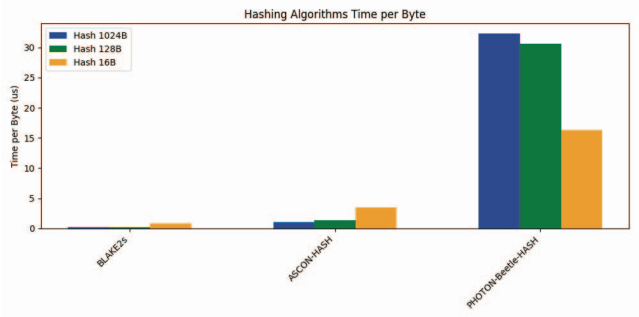

Fig. 3. Hash algorithms in encryption and decryption scenarios

Performance analysis of hashing algorithms is presented in Fig. 3 In general, the data reveal a consistent trend: The smaller the message, the higher the overhead relative to useful computation, resulting in lower throughput. This effect is visible across all categories, particularly in encryption and hashing algorithms that are not optimized for short inputs. Although some algorithms, such as ChaChaPoly and BLAKE2s, remain competitive even under these conditions, others, especially the PHOTON-Beetle family, demonstrate significant performance limitations. These insights are critical for system designers, especially in embedded or real-time systems, where both efficiency and speed must be carefully balanced against hardware constraints and security requirements.

IV. Conclusion

This paper has demonstrated key performance differences between lightweight cryptographic algorithms. The comparative analysis highlights ChaChaPoly and BLAKE2s as the most performant algorithms in encryption and hashing, respectively. Their high throughput and low per-byte latency make them excellent choices for applications requiring both speed and reliability. ASCON-128 and TinyJAMBU-128, while not as fast, demonstrate sufficient efficiency and are better suited for systems with severe resource constraints. In contrast, the PHOTON-Beetle family, though optimized for lightweight implementation, offers limited performance and may only be appropriate in scenarios where minimal code size or energy consumption is more critical than speed. These findings

underscore the importance of context-specific algorithm selection. While high-performance primitives like ChaChaPoly and BLAKE2s offer impressive speed, lightweight alternatives like ASCON and TinyJAMBU remain essential for ultraconstrained platforms. Future research will explore optimizations to balance security and efficiency, ensuring that cryptographic solutions meet the needs of diverse applications.

ACKNOWLEDGEMENTS

This work was supported by Grant NAWA/NSF: Impress-U, ID BPN/NSF/2023/1/00005 and NSF CAREER-2048266, "Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework".

REFERENCES

[1] P. S. Bangare and K. P. Patil, "Security issues and challenges in internet of things (iot) system," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2022, pp. 91–94.

[2] N. A. Khan, A. Awang, and S. A. A. Karim, "Security in internet of things: A review," *IEEE Access*, vol. 10, pp. 104 649–104 670, 2022.

[3] P. Śniatała, S. Iyengar, and S. K. Ramani, *Evolution of Smart Sensing Ecosystems with Tamper Evident Security*. Springer International Publishing.

[4] P. Śniatała, S. S. Iyengar, A. Bendarma, and M. Klosak, *Modern Technologies Enabling Safe and Secure UAV Operation in Urban Airspace*. IOS Press.

[5] G. Akshatha, A. Aadil, B. Baghyasri, V. V. Kubal, and K. P. Sharmila, "Microcontroller based engine control unit for uav application," in *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2022, pp. 185–188.

[6] R. G. Sangeetha, Y. Srivastava, C. Hemanth, H. Sankar Naicker, A. P. Kumar, and S. Vidhyadharan, "Unmanned aerial surveillance and tracking system in forest areas for poachers and wildlife," *IEEE Access*, vol. 12, pp. 187 572–187 586, 2024.

[7] A. Bernier-Vega, K. Barton, I. Olson, J. Rodriguez, G. Cantu, and S. Ozcelik, "Remote data acquisition using uavs and custom sensor node technology," *Drones*, vol. 7, no. 6, 2023. [Online]. Available: https://www.mdpi.com/2504-446X/7/6/340

[8] R. Samanta, B. Saha, and S. K. Ghosh, "A low-power low-cost system for disaster locations detection using esp32 cam and tinyml," in *2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)*, 2025, pp. 907–910.

[9] S. Ghosh, K. Ghosh, S. Karamakar, S. Prasad, N. Debabhuti, P. Sharma, B. Tudu, N. Bhattacharyya, and R. Bandyopadhyay, "Development of an iot based robust architecture for environmental monitoring using uav," in *2019 IEEE 16th India Council International Conference (INDICON)*, 2019, pp. 1–4.

[10] R. Shenoy and R. Manjunatha, "Design of unmanned aerial vehicle for stability," in *2023 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES)*, 2023, pp. 1–6.

[11] Z. Ren, Z. Tang, and R. Wang, "Research on key technologies of four-rotor uav flight control system based on stm32 microcontroller," in *2023 IEEE 6th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, 2023, pp. 1106–1112.

[12] L. Zhang, B. Hu, S. Wang, Y. Huang, X. Zhou, and R. Liu, "Design of a quadrotor uav controller based on body sensing control," in *2024 7th International Symposium on Autonomous Systems (ISAS)*, 2024, pp. 1–6.

[13] K. Rzepka, P. Szary, K. Cabaj, and W. Mazurczyk, "Performance evaluation of raspberry pi 4 and stm32 nucleo boards for security-related operations in iot environments," *Computer Networks*, vol. 242, p. 110252, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128624000847

[14] S. Maitra, D. Richards, A. Abdelgawad, and K. Yelamarthi, "Performance evaluation of iot encryption algorithms: Memory, timing, and energy," in *2019 IEEE Sensors Applications Symposium (SAS)*, 2019, pp. 1–6.

[15] N. Moura, J. Lucena, E. Pereira, N. Calazans, L. Ost, F. Moraes, and R. Garibotti, "Assessment of lightweight cryptography algorithms on arm cortex-m processors," in *2023 36th SBC/SBMicro/IEEE/ACM Symposium on Integrated Circuits and Systems Design (SBCCI)*, 2023, pp. 1–6.

[16] L. C. Ni, S. Ali, A. N. A. A. Aziz, and R. A. Rashid, "Implementation of proposed cryptography algorithm on esp32-based iot system," in *2024 IEEE International Conference on Advanced Telecommunication and Networking Technologies (ATNT)*, vol. 1, 2024, pp. 1–4.