# 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

## 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. 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.

## II. 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.

### B. Methodology

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 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.

## III. Conclusion

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”.