SITJOURNAL
Security Intelligence Terrorism Journal

*Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 02 (2026), pp. 171-181*
*Research Article*
**doi:** https://doi.org/10.70710/sitj.v3i2.102

# Analysis of ASCON Lightweight Authenticated Encryption for UAV Surveillance Communication Security

Vedaniar Zahra Danardini Mulia[1,a,*], Rizal Amrullah[1,b]

[1]Politeknik Siber dan Sandi Negara, Bogor, Indonesia
[a]vedaniar.zahra@student.poltekssn.ac.id; [b]rizal.amrullah@student.poltekssn.ac.id
*Corresponding author

**Article Info**
Received: 29-May-2026
Revised: 15-June-2026
Accepted: 30-June-2026

**Keywords**
AEAD; ASCON; Authenticated Encryption; Cybersecurity; Drone Communication Security; Lightweight Cryptography; Surveillance Communication; UAV Security

**Abstract**
The advancement of Unmanned Aerial Vehicle (UAV) technology has brought attention to the necessity of secure communication in intelligence and surveillance missions. UAV systems are susceptible to a number of cybersecurity threats since they depend on wireless communication, including eavesdropping, spoofing, replay attacks, telemetry manipulation, and hijacking. Although traditional cryptography techniques offer robust security, their high computational and energy costs render them unsuitable for the limited capabilities of UAVs. This study employs a comparative literature assessment of papers published between 2021 and 2026 to analyse ASCON lightweight cryptography as a potential solution for secure UAV surveillance communications. Confidentiality, integrity verification, authentication capabilities, and overall computational and energy efficiency against significant threats are important factors evaluated. The results demonstrate how effectively ASCON supports Authenticated Encryption with Associated Data (AEAD), which provides total security for confidentiality, integrity, and authentication while consuming little energy and computing resources. Additionally, ASCON is more resilient to spoofing and replay attacks than other conventional and lightweight cryptographic methods. This study highlights ASCON's capabilities in limited operating conditions and promotes the use of lightweight authenticated encryption algorithms in future UAV cybersecurity frameworks and embedded surveillance systems.

## 1. Introduction

The swift advancement of Unmanned Aerial Vehicle (UAV) technology has profoundly changed contemporary intelligence and surveillance activities. Because of their mobility, agility, and communication capabilities, UAV systems are being used more and more for monitoring, reconnaissance, border surveillance, disaster management, and real-time intelligence collection (Wang et al., 2021). Despite these benefits, because UAV communication systems rely on wireless channels, they are susceptible to some cybersecurity risks. Eavesdropping, spoofing, replay assaults, telemetry manipulation, and UAV hijacking are among the threats that might jeopardise mission dependability, operational integrity, and communication secrecy (Sabuwala & Daruwala, 2023). These risks demonstrate the need or secure communication techniques for UAV surveillance systems.

Traditional cryptographic methods like AES and RSA may have relatively high processing overhead and energy consumption, rendering them unsuitable for restricted UAV settings even if they provide strong security protection. UAV platforms require lightweight security solutions that can maintain operational

effectiveness and provide adequate protection since they often have limited processing power, memory, and battery life (Roman et al., 2016).

After being approved as an official lightweight cryptographic algorithm for limited devices by the National Institute of Standards and Technology, ASCON has garnered considerable attention among recent advancements in lightweight cryptography. In a lightweight cryptographic architecture, ASCON provides Authenticated Encryption with Associated Data (AEAD), which permits concurrent confidentiality, integrity, and authentication protection (Dobraunig et al., 2021). Because of its lightweight design, ASCON is ideal for embedded systems and UAV communication infrastructures that have limited processing power. ASCON can prevent unauthorized access and communication manipulation of telemetry data, navigation information, surveillance imagery, and operational orders in UAV surveillance communication.

Although UAV cybersecurity and lightweight cryptography implementation have been covered in a number of earlier studies, there is still a dearth of research explicitly examining ASCON's applicability to UAV surveillance communication systems. Thus, the purpose of this study is to use a comparative literature analysis technique to examine the use and appropriateness of ASCON lightweight cryptography for secure UAV surveillance communication. In addition to offering future research directions for safe surveillance communication systems in limited operational contexts, this study is anticipated to aid in the development of lightweight cybersecurity measures for UAV communication infrastructures.

## 2. Method

### 2.1. Research Design

The application of ASCON lightweight cryptography in secure UAV surveillance communication systems is examined in this paper using a comparative literature analysis methodology. The study focuses on assessing recent research on constrained-device security architectures, lightweight cryptographic techniques, authenticated encryption, and UAV communication security.

Instead of using a physical UAV prototype, the study intends to investigate the applicability of ASCON for UAV communication contexts based on existing scientific literature, which is why the comparative literature analysis technique was chosen. This method allows for a thorough assessment of the lightweight cryptographic features, computing efficiency, security mechanisms, and communication protection tactics covered in previous research (Snyder, 2019).

The association between UAV cybersecurity risks and the security features offered by lightweight authenticated encryption techniques is also examined in this study. The study specifically assesses how ASCON handles communication risks in UAV surveillance settings, including eavesdropping, spoofing, replay assaults, telemetry manipulation, and hijacking attempts.

### 2.2. Literature Collection

Several scientific databases were used in the literature collecting procedure to find pertinent research on lightweight cryptography and UAV communication security. The following databases were utilised in this study:

- [IEEE Xplore]
- [ScienceDirect]
- [SpringerLink]
- [Google Scholar]

Several keywords and word combinations associated with the study issue were utilised in the literature search, including:

- UAV Security
- Drone Communication Security
- Lightweight Cryptography
- Authenticated Encryption
- ASCON
- UAV Surveillance Communication
- Telemetry Security
- Lightweight Authenticated Encryption

To assure relevance and innovation, the study concentrated on articles published between 2021 and 2026, using recent and relevant references discussing developments in UAV cybersecurity, authenticated encryption technologies, and lightweight cryptography.

## 2.3. Inclusion and Exclusion Criteria

To make sure the chosen literature was pertinent to the study's goals, a number of inclusion and exclusion criteria were used.

### 2.3.1. Inclusion Criteria

The inclusion criteria used in this study include:

- Conference proceedings and peer-reviewed journal publications.
- Publications from 2021 to 2026.
- Studies discussing UAV communication security.
- Studies discussing lightweight cryptography or authenticated encryption.
- Studies discussing ASCON or lightweight AEAD implementation.
- Studies related to IoT security, embedded systems, or constrained communication environments.

### 2.3.2. Exclusion Criteria

The exclusion criteria include:

- Non-peer-reviewed publications.
- Articles unrelated to UAV communication systems.
- Studies lacking cryptographic or cybersecurity analysis.
- Publications focused exclusively on hardware implementation without communication security discussion.
- Duplicate studies or inaccessible publications.

In order to make sure that the filtering procedure was consistent with the study's goals, article titles, abstracts, keywords, methodology, and research findings were assessed.

## 2.4. Comparative Analysis Parameters

A number of security and performance metrics often covered in UAV cybersecurity and lightweight cryptography literature were used in the comparison analysis. The chosen parameters are intended to assess cryptographic algorithms' computational suitability and security capabilities for limited UAV situations. The parameters used in this study include:

- Confidentiality capability,
- Integrity protection,
- Authentication support,
- Computational overhead,
- Memory efficiency,
- Energy efficiency,
- Latency performance,
- Resistance against spoofing attacks,
- Resistance against replay attacks,
- Suitability for UAV communication systems.

Integrity protection prevents unauthorized changes to communication packets, whereas cryptographic methods ensure confidentiality by restricting access to telemetry and surveillance data. Authentication support verifies the legitimacy of devices and communications. Due to the limitations of UAV systems, such as constrained hardware and battery life, lightweight cryptographic algorithms are essential, focusing on minimal processing complexity and resource usage while maintaining security (Roman et al., 2016).

## 2.5. Analytical Framework

This study analyzes whether ASCON lightweight cryptography is suitable for UAV surveillance communication systems, linking the security features of authenticated encryption with the risks of UAV communication. The analysis focuses on several key aspects, including:

- UAV communication security threats,
- Lightweight cryptographic characteristics,
- Authenticated encryption mechanisms,
- Confidentiality and integrity protection,
- Communication efficiency in constrained environments,
- Applicability of ASCON for UAV surveillance communication.

Additionally, the framework contrasts ASCON with a number of lightweight and traditional cryptographic algorithms, such as AES, PRESENT, SPECK, and ChaCha20-Poly1305, that are commonly covered in UAV communication security literature.

## 2.6. Research Flow

The research process in this study consists of several stages:

1. Identification of UAV communication security problems,
2. Literature collection from scientific databases,
3. Selection and filtering of relevant publications,
4. Analysis of UAV cybersecurity threats,
5. Comparative analysis of lightweight cryptographic algorithms,
6. Evaluation of ASCON security mechanisms,
7. Analysis of ASCON suitability for UAV surveillance communication,
8. Conclusion development based on literature findings.

The main goal of the research process is to offer a thorough knowledge of how secure UAV surveillance communication in limited operating situations may be supported by ASCON lightweight cryptography.

## 2.7. Research Limitations

There are several limitations to the study discussed. Firstly, it does not utilize a physical UAV prototype or conduct real-time experimental testing; rather, it relies on a comparative literature analysis. Secondly, the conclusions drawn are based on existing research in lightweight cryptography and UAV cybersecurity. Despite these limitations, the paper provides a comprehensive conceptual analysis of ASCON lightweight cryptography's potential use in UAV surveillance communication systems and suggests future research directions for enhancing lightweight cybersecurity in UAV infrastructures.

# 3. Results and Discussion

## 3.1. Cybersecurity Threats in UAV Surveillance Communication

Because UAV surveillance communication systems rely heavily on wireless communication infrastructures, the comparative literature review shows that these systems are increasingly vulnerable to cybersecurity threats. Through wireless communication channels, modern UAV platforms and the Ground Control Station (GCS) continually exchange telemetry packets, navigation coordinates, operating commands, environmental sensor data, and surveillance pictures. Attackers may employ communication flaws to intercept, alter, or interfere with sent data as these communication channels are typically sent via open radio-frequency settings (Wang et al., 2021). The UAV platform, onboard sensors, wireless communication connections, and ground control stations are some of the main parts of a conventional UAV surveillance communication architecture. The communication flow typically entails bidirectional data transfer, in which the UAV simultaneously receives operational orders and navigation instructions from the control station and transmits telemetry and surveillance data to the operator.

According to the research, eavesdropping attacks are among the most frequent cybersecurity risks to UAV systems. Malicious actors can intercept telemetry communication packets, surveillance images, navigation coordinates, or operational directives sent between UAVs and Ground Control Stations in eavesdropping scenarios. Unauthorised interception may jeopardise intelligence confidentiality and operational secrecy as surveillance systems often process sensitive operational data (Singh et al., 2024).

Another significant threat identified in recent studies is spoofing attacks. Spoofing attacks occur when attackers transmit falsified communication packets or manipulate navigation systems to influence UAV operational behaviour. Because altered navigation coordinates might reroute UAV flight trajectories, interfere with surveillance missions, or jeopardise operational decision-making processes, GPS spoofing assaults are especially harmful (Sabuwala & Daruwala, 2023).

In UAV communication contexts, replay attacks can pose serious cybersecurity risks. Replay attacks cause unauthorised UAV replies by intercepting and retransmitting legal communication packets. Because UAV systems often employ recurrent telemetry transmission, improper implementation of freshness verification and authentication procedures may allow replay attacks to alter command execution (Singh et al., 2024).

Furthermore, one of the biggest risks to UAV cybersecurity is still UAV hijacking assaults. When attackers take advantage of flaws in authentication or insecure communication protocols to take over UAV systems without authorisation, this is known as hijacking. A successful hijacking may result in mission failure, unauthorised surveillance access, operational disruption, or complete loss of UAV control (Wang et al., 2021). Since these threats are ever more complex, communication security strategies must concurrently provide secrecy, integrity, and authentication while maintaining operational efficiency suitable for constrained UAV situations

## 3.2. Lightweight Cryptography Requirements in UAV Systems

The literature analysis shows that implementing strong communication security in UAV systems introduces significant challenges because UAV platforms commonly operate under constrained computational conditions. UAV systems generally utilize lightweight embedded processors with limited memory capacity, restricted computational capability, finite battery resources, and constrained communication bandwidth (Roman et al., 2016).

UAV platforms, in contrast to traditional computer systems, have to strike a compromise between operational effectiveness and communication security. Increased connection latency, decreased energy efficiency, and a detrimental impact on real-time surveillance response can all result from excessive computing cost brought on by cryptographic procedures.

Several studies indicate that traditional cryptographic algorithms such as AES and RSA provide strong security protection but may introduce higher computational complexity and power consumption unsuitable for lightweight embedded systems (Alaba et al., 2017). Cryptographic techniques that may minimize resource use while safeguarding telemetry communication are necessary for UAV systems.

The operational characteristics of UAV environments therefore, create several important cryptographic requirements:

- low computational overhead,
- minimal memory consumption,
- low energy utilization,
- efficient real-time processing,
- lightweight embedded implementation,
- strong confidentiality and integrity protection.

For restricted communication systems like IoT devices, wireless sensor networks, embedded systems, and UAV communication infrastructures, lightweight cryptography has therefore become a significant field of study. According to Roman et al. (2016), lightweight cryptographic algorithms are especially made to minimise memory use, increase energy efficiency, and decrease computational complexity while yet providing sufficient security protection. Because ASCON strikes a balance between security capabilities and

lightweight operating efficiency, it has garnered significant attention among recent advances in lightweight cryptography.

## 3.3. Overview of ASCON Lightweight Cryptography

ASCON is a lightweight cryptographic algorithm selected as one of the finalists of the CAESAR competition and later standardized by the National Institute of Standards and Technology (NIST) in 2023 as an official lightweight cryptography standard for constrained devices. ASCON was specifically designed for environments with limited computational capability, memory resources, and power consumption, making it highly suitable for embedded systems and Internet of Things (IoT) devices, including UAV communication infrastructures (Dobraunig et al., 2021). ASCON implements an Authenticated Encryption with Associated Data (AEAD) mechanism that simultaneously provides confidentiality, integrity, and authentication protection within a single cryptographic process. This capability is important for UAV surveillance communication systems because telemetry data, navigation information, surveillance imagery, and operational commands require protection against unauthorized access, modification, and falsified message injection.

The ASCON encryption and decryption architecture utilizes a duplex sponge-based mode, as illustrated in Figure 1. The algorithm consists of four primary operational stages:

1. Initialization,
2. Associated Data Processing,
3. Plaintext or Ciphertext Processing,
4. Finalization.

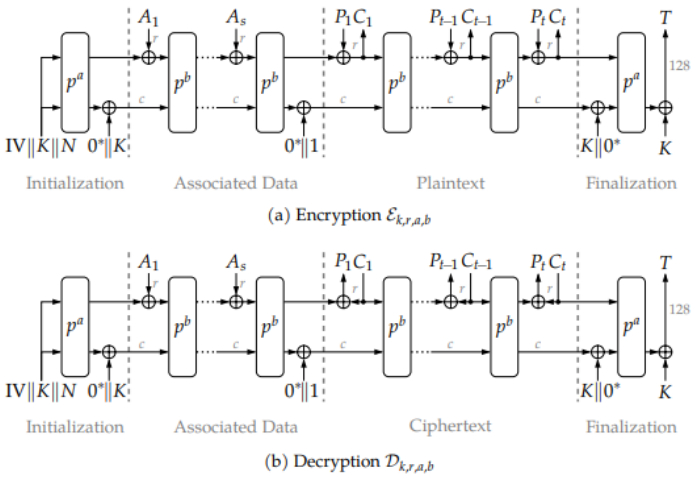


Figure 1. Duplex Sponge Mode for ASCON Authenticated Encryption and Decryption

The initial internal state of ASCON consists of 320 bits divided into two major components, namely outer bits and inner bits. The 320-bit internal state is separated into five 64-bit registers represented as:

$$S = x0 \,||\, x1 \,||\, x2 \,||\, x3 \,||\, x4 \quad (1)$$

ASCON defines two primary variants based on block size and diffusion iteration configuration, namely ASCON-128 and ASCON-128a. ASCON-128 operates using a 64-bit block size, while ASCON-128a utilizes a 128-bit block size. Both variants apply 12-round permutations during initialization and finalization processes. However, ASCON-128 applies 6-round permutations during plaintext and associated data processing, whereas ASCON-128a applies 8-round permutations (Dobraunig et al., 2021). In ASCON-128, the encryption and decryption processes utilize:

- 128-bit secret key,
- 128-bit nonce,
- 128-bit authentication tag,
- 64-bit data block size.

The initialization phase begins by combining the Initialization Vector (IV), secret key (K), and nonce (N) into a 320-bit internal state. The combined value is then processed using the permutation function for 12 rounds to establish the initial cryptographic state. After permutation, the last 128 bits of the state are XORed with the secret key to strengthen security protection. The initialization process can be conceptually represented as follows:

$$IV \,||K\, ||\, N \overset{p^a}{\rightarrow} S \tag{2}$$

After initialization, the associated data processing stage handles additional communication information such as packet headers or metadata. During this stage, associated data blocks A1, A2, ..., As are XORed with the internal state sequentially using repeated permutation operations. Although associated data is not encrypted, it remains authenticated to ensure integrity protection and authenticity verification.

The plaintext processing stage encrypts plaintext blocks sequentially to generate ciphertext outputs. In ASCON-128, plaintext is processed using 64-bit blocks. Each plaintext block is XORed with the current internal state, followed by permutation operations to continuously update the cryptographic state. The authenticated encryption process in ASCON can be represented as:

$$(C, T) = Ascon - AEAD128.enc(K, N, A, P) \tag{3}$$

where:

- K denotes the secret key,
- N denotes the nonce,
- A denotes associated data,
- P denotes plaintext,
- C denotes ciphertext,
- T denotes the authentication tag.

During decryption, ciphertext blocks are processed similarly to reconstruct the original plaintext while simultaneously verifying communication authenticity. If authentication verification fails, the ciphertext is rejected automatically to prevent unauthorized communication manipulation.

The finalization stage performs another XOR operation using the secret key followed by 12-round permutation processing. The final internal state then generates a 128-bit authentication tag used for integrity verification during decryption. The finalization process can be represented conceptually as:

$$T = S \oplus K \tag{4}$$

The authentication tag plays an important role in ensuring message integrity and communication authenticity. Any modification to transmitted communication packets results in authentication failure during decryption, thereby improving resistance against spoofing, replay attacks, and unauthorized message injection.

Based on the literature analysis, the lightweight permutation-based architecture of ASCON enables efficient implementation within constrained embedded systems while maintaining strong confidentiality and authentication protection. These characteristics make ASCON highly suitable for UAV surveillance communication systems operating under limited computational capability, restricted memory resources, and constrained battery conditions (Dobraunig et al., 2021).

## 3.4. Analysis of ASCON Security Mechanisms for UAV Communication

The literature review shows that ASCON offers several security benefits that are extremely pertinent to UAV surveillance communication systems.

### 3.4.1. Confidentiality Protection

Through authorised encryption techniques that transform plaintext data into encrypted ciphertext prior to transmission, ASCON safeguards operational directives, surveillance imagery, and telemetry information. During eavesdropping assaults, this approach keeps attackers from getting operational information (Dobraunig et al., 2021). Because intercepted surveillance material may reveal operational tactics, monitored locations, or sensitive reconnaissance operations, confidentiality protection is vital in intelligence and surveillance environments (Singh et al., 2024).

### 3.4.2. Integrity Verification

Mechanisms for integrity protection guarantee that packets are not altered while being communicated. Receivers can confirm if telemetry packets or UAV orders have been tampered with by unauthorised parties using the authentication tag produced by ASCON (Dobraunig et al., 2021). In UAV communication systems, this feature is crucial for countering false operating instruction injection and telemetry manipulation assaults (Sabuwala & Daruwala, 2023).

### 3.4.3. Authentication Capability

ASCON supports authenticated encryption capable of verifying communication authenticity. According to Dobraunig et al. (2021), authentication systems aid in ensuring that communication packets come from authorised communication entities rather than malevolent actors trying to spoof assaults. Falsified operational directives might jeopardise surveillance missions or reroute UAV behavior, making this capability especially crucial for UAV systems (Wang et al., 2021).

### 3.4.4. Replay Attack Resistance

The literature analysis indicates that ASCON utilizes nonce-based authenticated encryption mechanisms that improve resistance against replay attacks. Repeated plaintext communications provide distinct ciphertext outputs thanks to unique nonce values (Dobraunig et al., 2021). Because repeating telemetry transmission patterns might otherwise be susceptible to replay-based communication manipulation, this trait is especially important in UAV telemetry communication systems (Singh et al., 2024).

### 3.4.5. Lightweight Computational Characteristics

One of the most important advantages of ASCON is its lightweight computational architecture. According to a number of studies, ASCON adds comparatively less processing cost when compared to traditional cryptographic techniques (Dobraunig et al., 2021). Minimal memory utilisation, decreased processing complexity, effective embedded implementation, lower energy consumption, and minimal connection latency are some of ASCON's lightweight features. According to Roman et al. (2016), these features allow for effective implementation on restricted UAV systems with constrained computing and battery resources.

## 3.5. Comparative Analysis of Cryptographic Algorithms

The comparative literature analysis evaluates several cryptographic algorithms frequently discussed in UAV communication security studies, including AES, PRESENT, SPECK, ChaCha20-Poly1305, and ASCON (Roman et al., 2016).

Table 1. Comparative Analysis of Cryptographic Algorithms

| Algorithm | Authenticated Encryption | Lightweight Performance | Computational Overhead | Energy Efficiency | UAV Suitability |
|---|---|---|---|---|---|
| AES | Partial | Medium | Medium-High | Medium | Medium |
| PRESENT | No | High | Low | High | Medium |
| SPECK | Limited | High | Low | High | Medium |
| ChaCha20-Poly1305 | Yes | High | Medium | Medium | High |
| ASCON | Yes | Very High | Low | Very High | Very High |

The analysis demonstrates that ASCON provides a balanced combination of authenticated encryption capability and lightweight computational performance. In contrast to PRESENT and SPECK, ASCON uses AEAD techniques to enable integrated confidentiality, integrity, and authentication protection (Dobraunig et al., 2021). For lightweight embedded systems, ASCON offers better efficiency and less computational complexity than AES. Furthermore, ASCON is ideally suited for UAV surveillance communication infrastructures since it was designed with limited communication conditions in mind (Turan et al., 2025).

## 3.6 Suitability of ASCON for UAV Surveillance Communication

Based on the literature analysis, ASCON demonstrates strong suitability for secure UAV surveillance communication systems. Telemetry communication, surveillance imagery, navigation coordinates, and operational directives may all be concurrently protected by ASCON's authenticated encryption techniques (Dobraunig et al., 2021). ASCON's lightweight design makes it possible to deploy it effectively on UAV platforms with limited processing power and battery capacity (Roman et al., 2016).

Furthermore, ASCON shows resilience against a number of significant threats to UAV communication, including as spoofing, eavesdropping, replay assaults, telemetry manipulation, and unauthorised command insertion (Singh et al., 2024). The algorithm becomes highly applicable to UAV surveillance infrastructures that share similar operational characteristics because ASCON was specifically standardised for constrained embedded environments, such as IoT systems and lightweight communication devices (Turan et al., 2025).

## 3.7 Discussion

The findings of this study demonstrate that lightweight authenticated encryption mechanisms play an important role in protecting modern UAV communication systems from increasingly complex cybersecurity threats (Sabuwala & Daruwala, 2023). Communication security becomes a crucial operational need as UAV technology continues to grow across surveillance, intelligence, and monitoring applications. UAV systems must offer lightweight processing appropriate for limited embedded contexts while maintaining secure telemetry connection (Wang et al., 2021).

According to the literature review, traditional cryptography techniques might not be the best way to handle UAV systems' operating constraints. As a result, lightweight cryptographic algorithms like ASCON offer a more sensible compromise between computational economy and security protection (Roman et al., 2016). Because UAV communication systems concurrently need secrecy protection, integrity verification, authentication capability, and replay attack resistance, ASCON's authenticated encryption technology offers substantial benefits (Dobraunig et al., 2021).

The results show that ASCON has significant potential for future adoption in UAV surveillance communication infrastructures and lightweight embedded cybersecurity systems, despite the fact that this study is based on comparative literature analysis rather than experimental implementation (Turan et al., 2025).

## 4. Conclusion

This study employs comparative literature analysis to evaluate the effectiveness of ASCON lightweight cryptography for secure UAV surveillance communications. It identifies significant cybersecurity risks faced by UAV systems, including spoofing and eavesdropping, which threaten operational integrity and communication authenticity. Traditional cryptographic methods often prove inadequate for resource-constrained UAV environments due to high computational demands. ASCON's design, featuring Authenticated Encryption with Associated Data (AEAD), offers advantages such as simultaneous secrecy, integrity, and authentication, making it suitable for low-power devices. The findings suggest ASCON provides robust protection against unauthorized access and manipulations, ultimately presenting it as an optimal choice for real-time secure communications in UAV settings. While this analysis is limited to literature review, it highlights ASCON's potential for future research, particularly in practical implementations and performance evaluations.

## References

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28.

Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. Journal of Cryptology, 34(3), 1–42.

Sabuwala, Noshin & Daruwala, Rohin. (2023). Drones: Architecture, Vulnerabilities, Attacks and Countermeasures. 10.1007/978-3-031-31164-2_18.

Turan, M. S., Mckay, K. A., Chang, D., Kang, J., & Kelsey, J. (2025). *Ascon-Based Lightweight*

*Cryptography Standards for Constrained Devices*. National Institute of Standards and Technology (NIST).

Roman, R., Lopez, J., & Mambo, M. (2016). Mobile edge computing, fog computing and lightweight cryptography for IoT and UAV systems: A survey. Future Generation Computer Systems, 78, 680–698.

Singh, P., Sharma, V., & Kim, J. (2024). Cybersecurity threats and countermeasures in UAV communication systems: A survey. IEEE Access, 12, 33415–33439.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339.

Wang, L., Chen, Y., Wang, P., & Yan, Z. (2021). Security threats and countermeasures of unmanned aerial vehicle communications. IEEE Communications Standards Magazine, 5(4), 41–47.