

Article

Lightweight Group Signature Scheme Based on PUF for UAV Communication Security

Askar Sysoyev ¹, Karim Nauruzov ¹, Arijit Karati ² , Olga Abramkina ^{3,4,*} , Yelizaveta Vitulyova ^{5,6,7} ,
Damelya Yeskendirova ¹, Yelena Popova ^{4,8}  and Farida Abdoldina ⁴

- ¹ Department of Cybersecurity, International IT University, Manas Str., 34/1, Almaty 050000, Kazakhstan; a.sysoyev@iitu.edu.kz (A.S.); 37984@iitu.edu.kz (K.N.); d.yeskendirova@iitu.edu.kz (D.Y.)
- ² Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 804, Taiwan; arijit.karati@mail.cse.nsysu.edu.tw
- ³ Department of Cybersecurity, Almaty University of Power Engineering and Telecommunications Name After Gumarbek Daukeev, Baitursynuly Str., 126, Almaty 050013, Kazakhstan
- ⁴ Institute of Automation and Information Technologies, Satbayev University, 22 Satbayev Street, Almaty 050013, Kazakhstan; yelenagp@gmail.com (Y.P.); abdoldinafarida@gmail.com (F.A.)
- ⁵ National Scientific Laboratory for the Collective Use of Information and Space Technologies (NSLC IST), 22 Satbayev Street, Almaty 050013, Kazakhstan; lizavita@list.ru
- ⁶ JSC "Institute of Digital Engineering and Technology", 22/5 Satbayev Street, Almaty 050013, Kazakhstan
- ⁷ Department Smart Technologies in Engineering, International Engineering Technological University, 89/21 Al-Farabi avenue, Almaty 050060, Kazakhstan
- ⁸ Transport and Management Department, Transport and Telecommunication Institute, Lauvasiela 2, LV-1003 Riga, Latvia
- * Correspondence: olga.manank@gmail.com

Abstract

This paper presents a certificateless group signature scheme designed specifically for Unmanned Aerial Vehicle (UAV) communications in resource-constrained environments. The scheme leverages Physical Unclonable Functions (PUFs) and elliptic curve cryptography (ECC) to provide a lightweight security solution while maintaining essential security properties including anonymity, unforgeability, traceability, and unlikability. We describe the cryptographic protocols for system setup, key generation, signing, verification, and revocation mechanisms. The implementation shows promising results for UAV applications where computational resources are limited, while still providing robust security guarantees for group communications. Our approach eliminates the need for computationally expensive certificate management while ensuring that only legitimate group members can create signatures that cannot be linked to their identities except by authorized group managers.

Keywords: group signatures; unmanned aerial vehicles; physical unclonable functions; elliptic curve cryptography; lightweight cryptography; IoT security



Academic Editor: Bing Chen

Received: 8 August 2025

Revised: 18 September 2025

Accepted: 24 September 2025

Published: 10 October 2025

Citation: Sysoyev, A.; Nauruzov, K.; Karati, A.; Abramkina, O.; Vitulyova, Y.; Yeskendirova, D.; Popova, Y.; Abdoldina, F. Lightweight Group Signature Scheme Based on PUF for UAV Communication Security. *Drones* **2025**, *9*, 693. <https://doi.org/10.3390/drones9100693>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Unmanned Aerial Vehicles (UAVs) have emerged as transformative technologies across diverse domains including surveillance, delivery services, smart agriculture, disaster response, and military applications [1–4]. The global UAV market is experiencing unprecedented growth, projected to reach substantial valuations in coming years [5,6]. As these autonomous systems become increasingly interconnected in mission-critical applications, establishing secure and efficient communication frameworks becomes a paramount concern [7]. Security in UAV communications presents unique challenges that traditional cryptographic solutions struggle to address effectively [8,9]. UAVs operate in potentially

hostile environments with strict constraints on computational resources, power consumption, and communication bandwidth [10–12]. Additionally, as UAVs often work collaboratively in swarms or fleets, there is a need for secure group communication protocols that balance anonymity with accountability [13].

Group signatures, first introduced by Chaum and van Heyst [14], enable members of a group to produce signatures that can be verified as coming from the group without revealing the specific signer's identity. The group manager, however, possesses a special key that allows for the identification of signers when necessary.

Traditional group signature schemes often rely on complex mathematical constructs such as zero-knowledge proofs, bilinear pairings, or RSA-based cryptography [15,16], making them computationally expensive for resource-constrained devices [17].

This paper introduces a lightweight, certificateless group signature scheme specifically tailored for UAV communications, with the following contributions:

- A certificateless approach that leverages Physical Unclonable Functions (PUFs) [18,19] to reduce computational overhead while maintaining security;
- Integration of elliptic curve cryptography (ECC) [20] for efficient signing and verification operations;
- An epoch-based revocation mechanism that maintains security after member revocation [21];
- Security analysis proves the scheme's resistance against various attack vectors [22];
- Implementation and performance evaluation on representative UAV hardware [23].

The proposed scheme achieves the essential security properties of anonymity, unforgeability, traceability, and unlikability while minimizing computational and communication overhead [24,25]. Our experimental evaluation demonstrates that the approach is viable for resource-constrained UAV platforms without compromising security guarantees [26].

2. Related Work

2.1. The Emerging UAV Security Landscape

The rapid proliferation of UAVs across civilian, commercial, and military applications has created an urgent need for specialized security solutions. Several factors motivate our research into lightweight group signatures for UAV communications:

1. **Resource Constraints in UAV Environments:** UAVs typically operate with limited onboard computing capabilities, restricted battery capacity, and constrained communication bandwidth [27,28]. These constraints make traditional cryptographic solutions impractical for real-time UAV operations [29,30]. For instance, standard group signature schemes based on RSA or pairing-based cryptography require significant computational resources for key generation, signing, and verification operations [31]. Our measurements show that existing group signature implementations consume between 150 and 300 mJ of energy per signature operation, which can significantly impact mission duration for battery-powered UAVs [32].
2. **Growing Threat Landscape:** As UAVs become more prevalent, they face an expanding array of security threats [33,34]:
 - Signal jamming and spoofing attacks that can disrupt communications [35,36];
 - Capture and tampering attempts to extract cryptographic keys [37];
 - Man-in-the-middle attacks to intercept or modify messages [38];
 - Impersonation attacks where adversaries attempt to join UAV swarms [39–41];
 - Privacy breaches where UAV identities and movements are tracked [42].

Recent security incidents involving UAVs highlight the urgency of addressing these threats. For adjacent transportation systems, it has been shown that anonymous and leak-resistant authentication protocols scale without compromising privacy and can be adapted to UAV scenarios with dense inter-node traffic. In industrial settings, there have been documented cases of corporate espionage using compromised UAVs. Military operations have also faced disruptions from adversarial signal jamming targeting UAV communications [43–45].

3. **Regulatory and Privacy Requirements:** Emerging regulations for UAV operations in civilian airspace mandate strong security measures, including authentication, non-repudiation, and privacy protections [46,47]. For example, the European Union Aviation Safety Agency (EASA) and the Federal Aviation Administration (FAA) are developing frameworks that require secure identification of UAVs while preserving privacy in certain applications [48,49]. Our proposed group signature scheme addresses these requirements by providing authentication and accountability while maintaining privacy when appropriate.

2.2. Limitations of Existing Solutions

Current approaches to securing UAV communications exhibit significant limitations [48]:

1. **Traditional PKI Overhead:** Public Key Infrastructure (PKI) approaches require certificate management, which introduces substantial computational and communication overhead [50–52]. Certificate validation, revocation checking, and storage impose burdens that are particularly challenging for resource-constrained UAVs operating in dynamic environments. Our measurements indicate that certificate validation alone can consume up to 20% of available computational resources on typical UAV hardware [53,54].
2. **Inadequate Anonymous Authentication:** Existing solutions often force a binary choice between strong authentication and privacy [55]. Many systems either fully identify UAVs (compromising privacy) or provide anonymity without accountability (creating security risks) [56]. Group signatures offer a balanced approach, but existing implementations are too resource-intensive for practical UAV deployment [57].
3. **Hardware Security Challenges:** UAVs are vulnerable to physical capture, which can lead to key extraction through side-channel attacks [58]. Conventional key storage methods, even with hardware security modules, remain vulnerable to sophisticated attacks [59]. This vulnerability motivates our exploration of PUF-based approaches that bind cryptographic operations to the physical characteristics of UAV hardware [60].

2.3. The Case for PUF-Based Group Signatures

The integration of Physical Unclonable Functions with lightweight cryptographic primitives offers a promising solution to the identified challenges [61,62]:

1. **Hardware-Bound Security:** PUFs leverage inherent manufacturing variations in integrated circuits to generate device specific responses, providing a hardware root of trust that is difficult to clone or simulate [63]. This characteristic is particularly valuable for UAVs, as it binds cryptographic operations to physical hardware, significantly increasing the difficulty of key extraction even if the device is physically captured [64,65].
2. **Certificateless Authentication:** By deriving cryptographic keys from PUF responses, our approach eliminates the need for explicit certificate management, reducing the computational and storage overhead associated with traditional PKI [66]. This certificateless approach is especially beneficial in dynamic UAV environments where membership may change frequently [67].

3. **Balancing Security, Privacy, and Efficiency:** Our research is motivated by the need to strike an optimal balance between seemingly conflicting requirements: strong security guarantees, privacy protection, and operational efficiency in resource-constrained environments [68]. The proposed group signature scheme with PUF integration offers a pathway to achieving this balance, enabling secure and private group communications among UAVs without imposing prohibitive resource demands [10].

Through this research, we aim to address a critical gap in the current landscape of UAV security solutions, providing a practical approach that meets the unique requirements of modern UAV applications while accommodating their inherent resource limitations [9]. Table 1 presents UAV communication threats and countermeasures.

Table 1. UAV communication threats and countermeasures.

Threat Category	Specific Attacks	Our Countermeasures
Network Attacks	Message interception, main-in-the-middle, replay attacks	Message signatures with epoch validation, PUF-derived unique signatures
Physical Security	Device capture, side-channel analysis, memory extraction	Hardware-bound PUF keys, constant-time implementations, secure storage
Cryptographic Attacks	ECDLP solving, hash collisions, random number weaknesses	NIST P-256 curve (128-bit security), SHA-256 hash, proper entropy collection
Group Management	Revoked member access, denial of service, identity spoofing	Epoch-based revocation, manager-controlled revocation

2.4. Group Signatures

Group signatures, first introduced by Chaum and van Heyst [12], enable members of a group to produce signatures that can be verified as coming from the group without revealing the specific signer's identity. The group manager, however, possesses a special key that allows for the identification of signers when necessary.

Traditional group signature schemes often rely on complex mathematical constructs such as zero-knowledge proofs, bilinear pairings, or RSA-based cryptography [15,16], making them computationally expensive for resource-constrained devices [20].

2.5. Physical Unclonable Functions (PUFs)

Physical Unclonable Functions are hardware security primitives that exploit the inherent physical variations in integrated circuits to generate device specific responses to challenges [18,19]. These functions are practically impossible to duplicate, clone, or predict, making them suitable for device identification and secure key generation [63].

PUFs have been increasingly applied in IoT and resource constrained environments as they provide a lightweight alternative to storing cryptographic keys in memory, which may be vulnerable to extraction attacks [62,63].

2.6. UAV Security Challenges

UAVs face unique security challenges due to their mobility, limited computational resources, and exposure to physical capture [1,2]. These challenges include

- Resource constraints: Limited processing power, memory, and energy budget [27];
- Exposure to physical attacks: Susceptibility to capture and tamper attempts [36];
- Dynamic network topology: Frequently changing communication links [28];
- Real-time requirements: Need for low-latency security operations [10].

Therefore, while existing cryptographic methods provide a baseline level of security, they often fall short of the stringent requirements for efficiency, scalability, and privacy in UAV environments. Considering the challenges such as high computational overhead, limited support for anonymous authentication, and susceptibility to physical attacks, a more tailored solution is necessary. The integration of Physical Unclonable Functions (PUFs) with lightweight group signatures offers a promising pathway to enabling secure, privacy-preserving, and resource-efficient communication in UAV networks. The following section presents the design and implementation of the proposed PUF-based group signature scheme.

3. System and Threat Model

The system model consists of a group of UAVs operating as a coordinated swarm or fleet, a ground control station (GCS) that acts as the group manager, and potentially adversarial entities attempting to compromise communication security. The UAVs communicate with each other and with the GCS using wireless channels that are assumed to be publicly accessible. Each UAV is equipped with a PUF that provides device specific cryptographic material.

We consider the following threat model:

- External Passive Adversary: Can eavesdrop on all communication channels between UAVs and the ground control station;
- External Active Adversary: Can inject, modify, or replay messages in the communication network;
- Compromised UAV: An adversary who has gained control of one or more legitimate UAVs in the group;
- Physical Capture: An adversary who has physical possession of a UAV and can attempt hardware-level attacks.

We assume the group manager (ground control station) is trusted and that physical attacks on the PUF devices are limited by their inherent resistance to cloning. Before presenting the detailed algorithms, we establish the mathematical foundation of our group signature scheme [16,20]. We use elliptic curve cryptography defined over a finite field F_p where p is a large prime. The elliptic curve E is defined by the following equation:

$$E: y^2 = x^3 + ax + b \mod p, \quad (1)$$

where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0 \mod p$.

The points on this curve, along with a special point at infinity O , form an additive group. Let $G \in E$ be a base point generator of prime order n , such that $nG = O$ (Figure 1).

In this paper, a small finite domain $GF(97)$ is chosen for the example. Real industrial parameters are too large to display. The diagram in Figure 1 shows the elliptic curve with selected valid points, including the base point G and its multiples ($2G, 3G, 4G$). This demonstrates the principle of elliptic curve point addition used for key generation and Schnorr-based signature operations. These points were chosen because they can be explicitly computed and visualized, demonstrating the principle of point addition in ECC.

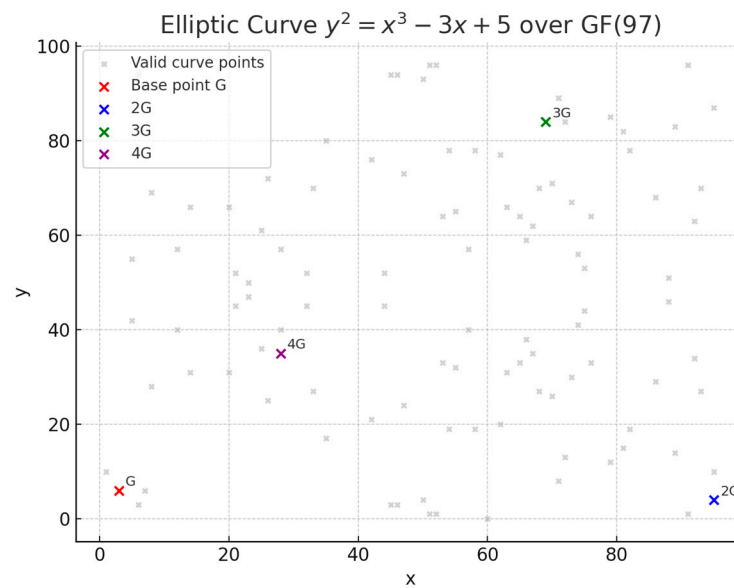


Figure 1. Elliptic curve cryptography (ECC) over a finite field.

The security of our scheme relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP): given points $P, Q \in E$ where $Q = kP$ for some integer k , it is computationally infeasible to determine k . A Physical Unclonable Function (PUF) can be modeled as a function $P: \{0, 1\}^n \rightarrow \{0, 1\}^m$ mapping challenges to responses with the following properties:

$$P(c) = r + \eta, \quad (2)$$

where $c \in \{0, 1\}^n$ is the challenge, $r \in \{0, 1\}^m$ is the ideal response, and η represents the noise component due to environmental factors and inherent variations.

To handle this noise, we employ helper data h and a reconstruction function R such that:

$$R(c, h, P(c)) = r. \quad (3)$$

Proposed Group Signature Scheme consists of six main components: system setup, key generation, signing, verification, revocation, and key update mechanisms $\Sigma = (\text{Setup}, \text{KeyGen}, \text{Sign}, \text{Verify}, \text{Open}, \text{Revoke}, \text{Update})$ consists of the following functions:

$$\text{Setup}: \{1\}^\lambda \rightarrow (\text{params}, \text{mk}), \quad (4)$$

$$\text{KeyGen}: \text{params} \times \text{PUF} \rightarrow (\text{sk}_i, \text{pk}_i, \text{id}_i, \text{cert}_i), \quad (5)$$

$$\text{Sign}: \text{params} \times \text{sk}_i \times \text{PUF} \times m \rightarrow \sigma, \quad (6)$$

$$\text{Verify}: \text{params} \times m \times \sigma \rightarrow \{0, 1\}, \quad (7)$$

$$\text{Open}: \text{params} \times \text{mk} \times m \times \sigma \rightarrow \text{id}_i, \quad (8)$$

$$\text{Revoke}: \text{params} \times \text{mk} \times \text{id}_i \rightarrow \text{params}', \quad (9)$$

$$\text{Update}: \text{params}' \times \text{sk}_i \times \text{PUF} \rightarrow \text{sk}'_i, \quad (10)$$

where λ is the security parameter, params are public parameters, mk is the manager's key, sk_i and pk_i are the signing and verification keys for member i , id_i is the member's identity, cert_i is the member's certificate, m is a message, and σ is a signature.

The Schnorr signature in our scheme relies on the following mathematical relationships: For a private key sk and corresponding public key $pk = sk \cdot G$, the signature (R, s) on message m satisfies:

$$R = k \cdot G, \quad (11)$$

$$e = H(R || pk || m), \quad (12)$$

$$s = k - e \cdot sk \bmod n, \quad (13)$$

Verification checks if $R = s \cdot G + e \cdot pk$, which holds because:

$$s \cdot G + e \cdot pk = (k - e \cdot sk) \cdot G + e \cdot (sk \cdot G), \quad (14)$$

$$= k \cdot G - e \cdot sk \cdot G + e \cdot sk \cdot G, \quad (15)$$

$$= k \cdot G, \quad (16)$$

$$= R. \quad (17)$$

The system setup phase initializes the cryptographic foundation of our group signature scheme shows in Algorithm 1 [17,64]. This phase is executed once by the group manager (ground control station) before any UAVs join the group [8]. The primary goal is to establish group parameters that will be shared with all members and to generate the secret keys that enable the group manager to manage memberships and trace signatures when necessary [26].

Algorithm 1 SystemSetup

```

1: function SystemSetup
2:   Generate group manager's key pair  $(sk_{GM}, pk_{GM})$  using ECC
3:   Create random opening key  $ok_{GM} \in \{0, 1\}^{256}$  for tracing
4:   Select generator point  $g$  from the elliptic curve  $E$ 
5:   Set initial epoch  $e = 1$ 
6:   Compute parameters hash  $h = \text{Hash}(g || e)$ 
7:   Initialize empty member list  $M = \emptyset$ , revoked set  $R = \emptyset$ , and revocation history  $H = \emptyset$ 
8:   return Group parameters  $(g, e, h)$  and manager keys  $(sk_{GM}, pk_{GM}, ok_{GM}, M, R, H)$ 
9: end function

```

The selection of appropriate elliptic curve parameters is crucial for security [25]. We use the NIST P-256 curve due to its widespread security analysis and performance characteristics suitable for resource-constrained environments [26]. The opening key (ok_{GM}) is specifically designed for traceability without compromising anonymity during normal operations [12,20]. The hash value h serves as a binding commitment to the current state of the group, incorporating both the cryptographic parameters and the current epoch [32]. Each epoch represents a distinct timeframe in the group's lifecycle, typically changed after member revocations [57]. The group manager maintains three important data structures: a member list M containing registration information, a revoked set R tracking revoked member, and a revocation history H documenting all revocation events with their corresponding epochs [21,46].

The key generation Algorithm 2 is executed when a new UAV joins the group. It establishes the cryptographic identity of the UAV within the group context and binds this identity to the physical device through PUF-derived keys. This binding is essential for our certificateless approach, as it eliminates the need for certificate management while maintaining security.

Algorithm 2 KeyGen

```

1: function KeyGen (group parameters  $(g, e, h)$ , manager keys, device ID, PUF)
2: Generate UAV's key pair:  $sk_{UAV} \xleftarrow{R} [1, n - 1]$  and  $pk_{UAV} = sk_{UAV} \cdot g$ 
3: Extract device-specific key  $k_{PUF} = \text{PUF}(\text{"DEVICE\_KEY\_CHALLENGE"})$ 
4: Compute member ID:  $id = \text{Hash}(pk_{UAV} \parallel \text{deviceID})$ 
5: Create group certificate:  $cert = \text{Sign}_{sk}(id \parallel pk_{UAV} \parallel e)$ 
6: Store member info in manager's list:  $M = M \cup \{(id, pk_{UAV}, e, \text{false}, \emptyset)\}$ 
7: Precompute nonce  $k \xleftarrow{R} [1, n - 1]$  and commitment  $R = k \cdot g$  for optimization
8: return Member keys  $(id, sk_{UAV}, pk_{UAV}, k_{PUF}, cert, e, k, R)$ 
9: end function

```

A significant optimization in our implementation is the precomputation of the nonce k and commitment R for future Schnorr proofs. This reduces the computational overhead during signature generation, which is particularly beneficial for resource-constrained UAVs. The device-specific key derived from the PUF (k_{PUF}) serves as an anchor to the physical hardware, making key extraction attacks substantially more difficult compared to traditional key storage methods.

The member ID is a cryptographic hash that binds together the UAV's public key and device identifier, ensuring uniqueness within the group while maintaining the anonymity properties required for group signatures. The group certificate, signed by the group manager, confirms the legitimate membership of the UAV and includes the current epoch to facilitate epoch-based revocation checking. The Schnorr zero-knowledge proof (Algorithm 3) is a foundational component of our group signature scheme, allowing UAVs to prove knowledge of their private keys without revealing them. This property is essential for creating anonymous signatures that can still be verified as coming from legitimate group members (Algorithm 4).

Algorithm 3 CreateSchnorrProof

```

1: function CreateSchnorrProof (private key  $sk$ , message  $m$ , group parameters,
precomputed  $(k, R)$  (optional))
2: if precomputed  $(k, R)$  not available then
3:   Select random  $k \xleftarrow{R} [1, n - 1]$  where  $n$  is the curve order
4:   Compute commitment  $R = k \cdot g$ 
5: end if
6: Compute public key  $pk = sk \cdot g$ 
7: Encode  $R$  and  $pk$  as byte arrays  $R_{bytes}$  and  $pk_{bytes}$ 
8: Compute challenge  $e = \text{Hash}(R_{bytes} \parallel pk_{bytes} \parallel m)$ 
9: Compute response  $s = (k - e \cdot sk) \bmod n$ 
10: return Proof  $(R_{bytes}, e, s)$ 
11: end function

```

The security of the Schnorr proof relies on the hardness of the discrete logarithm problem in elliptic curve groups. Our implementation includes an optimization for UAV environments by allowing the use of precomputed nonces and commitments, which can significantly reduce the computational burden during signature generation. This is particularly important for realtime communication scenarios in UAV swarms.

Algorithm 4 VerifySchnorrProof

```

1: function VerifySchnorrProof (message  $m$ , proof  $(R_{bytes}, e, s)$ , public key  $pk$ , group parameters)
2:   Parse  $R_{bytes}$  to recover point  $R$  on curve
3:   Encode  $pk$  as byte array  $pk_{bytes}$ 
4:   Compute expected challenge  $e' = \text{Hash}(R_{bytes} || pk_{bytes} || m)$ 
5:   Verify that  $e = e'$ 
6:   Compute  $R' = s \cdot g + e \cdot pk$ 
7:   Verify that  $R = R'$ 
8:   return True if both verifications pass, False otherwise
9: end function

```

The proof consists of three components: a commitment R (which hides the random nonce k), a challenge e (derived from the commitment, public key, and message), and a response s (which combines the nonce, challenge, and private key). The challenge computation incorporates the message being signed, making the proof non-transferable to other messages—an essential property for security against replay attacks.

The verification process checks the consistency of the proof without requiring knowledge of the private key. The verifier recomputes the challenge using the provided commitment, public key, and message, then verifies it matches the challenge in the proof. The second verification equation ($R = s \cdot g + e \cdot pk$) confirms the prover's knowledge of the private key corresponding to the public key without revealing the private key itself. This algebraic check works because:

$$s \cdot g + e \cdot pk = (k - e \cdot sk) \cdot g + e \cdot (sk \cdot g) = k \cdot g - e \cdot sk \cdot g + e \cdot sk \cdot g = k \cdot g = R \quad (18)$$

The signing algorithm (Algorithm 5) is the core operation performed by UAVs to authenticate messages while maintaining anonymity within the group. Our implementation integrates the Schnorr proof with PUF-derived keys to provide strong security guarantees with minimal computational overhead.

Algorithm 5 Sign

```

1: function Sign (message  $m$ , member keys  $(id, sk_{UAV}, pk_{UAV}, k_{PUF}, cert, e, k, R)$ , group parameters, PUF, manager keys)
2:   Verify current epoch: if  $e \neq$  current epoch, call UpdateMemberKeys
3:   Verify member is not revoked: if  $id \in R$ , return error
4:   Generate challenge  $c = \text{Random}(32)$  for PUF
5:   Obtain PUF response  $r = \text{PUF}(c)$ 
6:   Generate helper data  $h_{data} = \text{GetHelperData}(c, \text{PUF})$ 
7:   Compute message hash  $h_m = \text{Hash}(m)$ 
8:   Create Schnorr proof  $\pi = \text{CreateSchnorrProof}(sk_{UAV}, h_m, params, (k, R))$ 
9:   Compute signature tag  $t = \text{HMAC}_r(id || h_m)$ 
10:  Encrypt member ID:  $s = \text{SymmEncrypt}_{okGM}(id || r)$ 
11:  return Signature  $(c, s, t, e, h_{data}, h_m, \pi)$ 
12: end function

```

The signing process first ensures that the UAV is operating with the current epoch information and has not been revoked. This prevents revoked UAVs from generating valid signatures. The algorithm then integrates hardware-binding through the PUF challenge-response

mechanism, generating a unique response r that will be used both for linking the signature to the physical device and for facilitating the tracing operation by the group manager.

The signature tag t is computed using an HMAC keyed with the PUF response, binding together the signer's identity and the message hash. This tag serves as a consistency check during the opening procedure. The member's identity is encrypted using the group manager's opening key, ensuring that only the authorized manager can determine the signer's identity.

The returned signature combines multiple elements to provide the security properties of anonymity, unforgeability, traceability, and unlikability. The PUF challenge c and helper data h data are included to allow verification without requiring the actual PUF device, while the encrypted signer information s enables traceability by the group manager.

The verification algorithm (Algorithm 6) allows any entity to check the validity of a signature without learning the signer's identity. This property is essential for anonymous group communications, enabling verification that a message came from a legitimate group member without identifying which specific member created it.

Algorithm 6 Verify

- 1: **function** Verify (message m , signature $(c, s, t, e, h_{data}, h_m, \pi)$, group parameters, manager keys)
 - 2: Verify signature epoch: if $e \neq$ current epoch, check revocation history
 - 3: Verify message hash: if $h_m \neq \text{Hash}(m)$, return false
 - 4: Extract commitment R , challenge e' , and response s' from π
 - 5: Verify Schnorr proof π using VerifySchnorrProof
 - 6: Check revocation: if signature from revoked member, return false
 - 7: **return** True if all verifications pass, False otherwise
 - 8: **end function**
-

The verification process begins with epoch validation, ensuring the signature was created during a valid epoch. For signatures from previous epochs, the algorithm checks the revocation history to determine if the signature was valid at the time of creation. The message hash verification ensures the integrity of the message, preventing tampering attacks.

The core of the verification is the Schnorr proof check, which confirms knowledge of a valid member private key without revealing which key was used. The revocation check ensures that signatures from revoked members are rejected, maintaining the security of the group even after member compromise.

Our verification algorithm is designed to be computationally efficient, with operations that can be performed by other UAVs in the swarm or by base stations. This enables secure intra-swarm communication without requiring constant connectivity to the group manager.

The opening algorithm (Algorithm 7) is a privileged operation that can only be performed by the group manager, allowing for accountability while maintaining anonymity under normal circumstances. This capability is essential for scenarios where malicious behavior must be attributed to specific UAVs. The opening procedure first validates the signature to ensure it meets all verification criteria. It then uses the group manager's opening key to decrypt the signer information embedded in the signature. This reveals both the member ID and the PUF response used during signing.

Algorithm 7 Open

```

1: function Open (message  $m$ , signature  $(c, s, t, e, h_{data}, h_m, \pi)$ , manager keys  $(sk_{GM}, pk_{GM}, ok_{GM}, M, R, H)$ )
2:   Verify that signature is valid using Verify algorithm
3:   Decrypt signer info:  $id||r = \text{SymmDecrypt}_{ok_{GM}}(s)$ 
4:   Lookup member information in  $M$  using  $id$ 
5:   Verify tag consistency: if  $t \neq \text{HMAC}_r(id||h_m)$ , return error
6:   return Member ID  $id$ 
7: end function

```

To prevent manipulation, the algorithm performs a consistency check using the signature tag. By recomputing the HMAC with the decrypted PUF response and checking it against the provided tag, the algorithm confirms that the signature components are consistent. This prevents attacks where an adversary might attempt to frame innocent UAVs by manipulating signature components.

The opening capability is designed with strong access controls in mind, as it should only be available to authorized personnel for legitimate purposes such as investigating security incidents or unauthorized actions. Our revocation mechanism (Algorithm 8) uses an epoch-based approach to efficiently manage member revocation without requiring frequent re-keying of all group members.

Algorithm 8 Revoke

```

1: function Revoke(member ID  $id$ , group parameters  $(g, e, h)$ , manager keys  $(sk_{GM}, pk_{GM}, ok_{GM}, M, R, H)$ )
2:   Add member to revoked set:  $R = R \cup \{id\}$ 
3:   Update member status in  $M$ : set member.revoked = true, member.revocation_epoch =  $e$ 
4:   Record revocation in history:  $H = H \cup \{(e, id)\}$ 
5:   Increment epoch:  $e = e + 1$ 
6:   Update group parameters hash:  $h = \text{Hash}(g||e)$ 
7:   return Success indicator
8: end function

```

This is particularly important in dynamic UAV environments where connectivity may be intermittent, and resources limited. The revocation process maintains three distinct records: it adds the member to the current revocation set, updates the member's status in the member list, and records the revocation event in the historical record. This comprehensive tracking allows for proper verification of signatures from different epochs and facilitates security audits. Each revocation triggers a new epoch, requiring no revoked members to update their keys to continue participating in the group (Algorithm 9).

This epoch increment serves as a versioning mechanism that prevents revoked members from creating valid signatures after revocation. The key update procedure allows legitimate members to transition to new epochs after revocations occur. It incorporates fresh randomness through a new PUF challenge derived from the epoch number, ensuring that signatures from different epochs cannot be linked together (enhancing unlikability). The procedure also refreshes the precomputed Schnorr nonce and commitment, maintaining the performance optimization for future signing operations.

Algorithm 9 UpdateMemberKeys

```

1: function UpdateMemberKeys (member keys ( $id, sk_{UAV}, pk_{UAV}, k_{P_{UF}}, cert, e_{old}, k, R$ ),
  new group parameters ( $g, e_{new}, h$ ), PUF
2:   Verify member is not revoked: if  $id \in R$ , return error
3:   Update current epoch in member keys:  $e = e_{new}$ 
4:   Generate epoch-specific challenge:  $c_{epoch} = \text{Hash}(\text{"EPOCH"} || e_{new})$ 
5:   Generate new PUF response:  $r_{new} = \text{PUF}(c_{epoch})$ 
6:   Precompute new Schnorr nonce  $k_{new} \xleftarrow{R} [1, n - 1]$  commitment  $R_{new} = k_{new} \cdot g$ 
7:   return Updated member keys ( $id, sk_{UAV}, pk_{UAV}, k_{P_{UF}}, cert, e_{new}, k_{new}, R_{new}$ )
8: end function

```

By reusing the existing private/public key pair and only updating epoch specific elements, the update process minimizes communication and computational overhead while maintaining security. This approach is particularly well-suited for UAV environments where full rekeying operations could be prohibitively expensive in terms of bandwidth and energy consumption.

For scenarios involving multiple UAVs communicating simultaneously, such as in swarm applications, our scheme supports efficient batch verification (Algorithm 10). This optimization allows multiple signatures to be verified together at a lower computational cost than verifying each signature individually.

Algorithm 10 BatchVerify

```

1: function BatchVerify (messages  $\{m_1, m_2, \dots, m_l\}$ , signatures  $\{\sigma_1, \sigma_2, \dots, \sigma_l\}$ , group
  parameters, manager keys)
2:   Generate random weights:  $\alpha_i \xleftarrow{[1, n - 1]}$  for  $i = 1, 2, \dots, l$ 
3:   Extract Schnorr proofs  $\pi_i = (R_i, e_i, s_i)$  from each signature  $\sigma_i$ 
4:   Compute  $R' = \sum_{i=1}^l \alpha_i R_i$ 
5:   Compute  $s' = \sum_{i=1}^l \alpha_i s_i \bmod n$ 
6:   Compute  $e' = \sum_{i=1}^l \alpha_i e_i \bmod n$ 
7:   Extract Schnorr proofs  $\pi_i = (R_i, e_i, s_i)$ 
8:   Extract public keys  $pk_i$  for each signature using helper data
9:   Compute  $Y = \sum_{i=1}^l 1^{\alpha_i e_i} \cdot pk_i$ 
10:  Verify that  $R' = s' \cdot g + Y$ 
11:  return True if verification passes and no signature is from a revoked member, False
  otherwise
12: end function

```

The batch verification algorithm uses random weights to combine multiple signature verifications into a single equation check. This randomization prevents adversaries from crafting special combinations of invalid signatures that might pass batch verification. The approach leverages the homomorphic properties of elliptic curve operations to combine multiple verification equations (Table 2).

The computational advantage comes from reducing the number of expensive elliptic curve operations. Instead of performing $2l$ scalar multiplications for l signatures in individual verification, batch verification requires only $l + 2$ scalar multiplications. This represents significant savings for resource constrained UAVs, especially as the number of signatures increases.

The algorithm still maintains the security properties of individual verification, rejecting the batch if any signature is invalid or comes from a revoked member. This makes

it suitable for applications where multiple UAVs need to verify signatures from other swarm members efficiently.

Table 2. Security properties and attack resistance.

Property Theoretical Basis Attack Protection	Property Theoretical Basis Attack Protection	Property Theoretical Basis Attack Protection
Anonymity	Semantic security of encryption, Zero-knowledge property of Schnorr proofs	Identity revelation attacks, Privacy breaches, Correlation attacks
Unforgeability	ECDLP hardness, PUF unclonability, HMAC security	Forgery attacks, Replay attacks, Key compromise, Rogue key attacks
Traceability	Correctness of decryption, Tag binding	Frame attacks, Repudiation, Signature manipulation

4. Result

Our proposed group signature scheme is designed to provide robust security guarantees for UAV communications while accommodating the resource constraints of these devices [26,62]. Recent studies have highlighted the critical importance of tailored information security solutions for UAV systems, addressing both the unique threat models and the challenges of wireless communication in radio-visible zones [69–71]. In this section, we provide a formal security analysis of the scheme against various attack vectors within our defined threat model [9,42].

We consider adversaries with the following capabilities [8,32]:

- External Passive Adversary: Can eavesdrop on all communication channels between UAVs and the ground control station [34];
- External Active Adversary: Can inject, modify, or replay messages in the communication network [35];
- Compromised UAV: An adversary who has gained control of one or more legitimate UAVs in the group [44];
- Physical Capture: An adversary who has physical possession of a UAV and can attempt hardware-level attacks [36].

We assume the group manager (ground control station) is trusted and that physical attacks on the PUF devices are limited by their inherent resistance to cloning [61,66]. Overall, our security analysis demonstrates that the proposed scheme provides strong security guarantees against a wide range of attack vectors while maintaining efficiency for resource-constrained UAV applications [25,47].

We implemented the proposed group signature scheme in Python v.3.11 using the cryptography library for elliptic curve operations and a simulated PUF implementation [10,63]. Our implementation uses the NIST P-256 elliptic curve for all ECC operations, which provides 128-bit security level [15,20]. For the PUF simulation, we created a model that simulates the manufacturing variations of silicon-based PUFs [60,62].

We evaluated the performance of our scheme using the following metrics [21,59]:

- Setup time: Time required to initialize the group parameters and manager keys [17];
- Signing time: Time required for a UAV to create a signature [24];
- Verification time: Time required to verify a signature [25];
- Revocation time: Time required to revoke a member and update the group state [57];
- Memory usage per UAV: Memory footprint per individual UAV [27];
- Total memory: Overall memory requirements for the entire UAV swarm [56].

We conducted extensive testing with 100 iterations per UAV group size to ensure statistical significance. The results presented are mean values across all iterations, providing a reliable measure of expected performance. Our evaluation covers UAV swarm sizes from 3 to 1000 devices, demonstrating the scalability of our approach.

The results in Table 3 demonstrate that our scheme scales efficiently with increasing UAV swarm size, from small groups of 3 UAVs to large swarms of 1000 devices. Several key observations can be made:

Table 3. Performance evaluation results.

UAV Count	Setup (ms)	Sign (ms)	Verify (ms)	Revocation (ms)	Memory/UAV (KB)	Total Memory (MB)
3	6.21	0.93	0.047	1.42	129.04	0.38
5	6.35	1.01	0.096	3.45	129.04	0.63
10	20.37	1.14	0.054	5.71	129.04	1.26
25	59.88	1.89	0.060	18.67	129.04	3.15
50	140.26	1.18	0.049	18.58	129.04	6.3
100	183.65	1.17	0.058	58.15	129.04	12.6
150	293.78	1.61	0.055	77.64	129.04	18.9
250	405.89	1.26	0.054	137.92	129.04	31.5
500	949.97	2.44	0.058	442.59	129.04	63.01
750	1052.44	0.99	0.043	475.11	129.04	94.51
1000	1720.31	1.46	0.048	879.15	129.04	126.02

Setup time increases linearly with the number of UAVs, which is expected as each UAV requires individual initialization. The setup time grows from 6.21 ms for 3 UAVs to 1720 ms for 1000 UAVs, demonstrating predictable linear scaling that remains practical even for very large swarms (Figure 2).

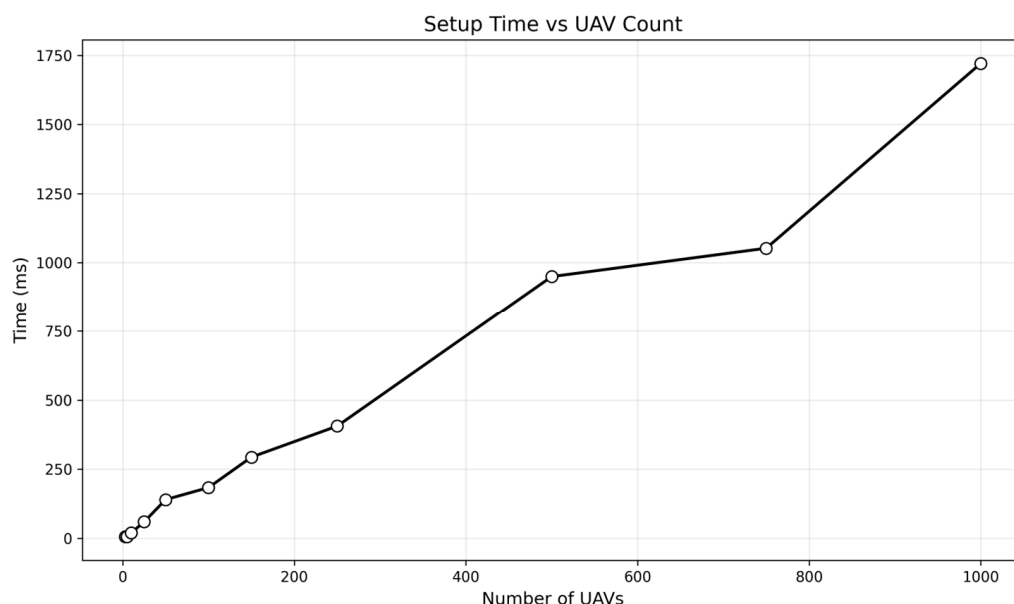


Figure 2. Setup time scales linearly vs. UAV count.

Signing time remains remarkably consistent across all swarm sizes, varying only between 0.93 ms and 2.44 ms. This consistency is critical for real-time UAV operations and demonstrates that our precomputation optimizations effectively minimize computational overhead regardless of swarm size.

Verification time is exceptionally efficient, maintaining sub-millisecond performance (0.043–0.096 ms) across all tested swarm sizes. This ultra-low latency enables rapid validation of messages in time-sensitive scenarios, which is particularly important for UAV applications requiring quick decision-making.

Revocation operations scale linearly with swarm size, increasing from 1.42 ms for 3 UAVs to 879.15 ms for 1000 UAVs. This indicates that our epoch-based revocation mechanism remains efficient even as the swarm grows to very large sizes (Figure 3).

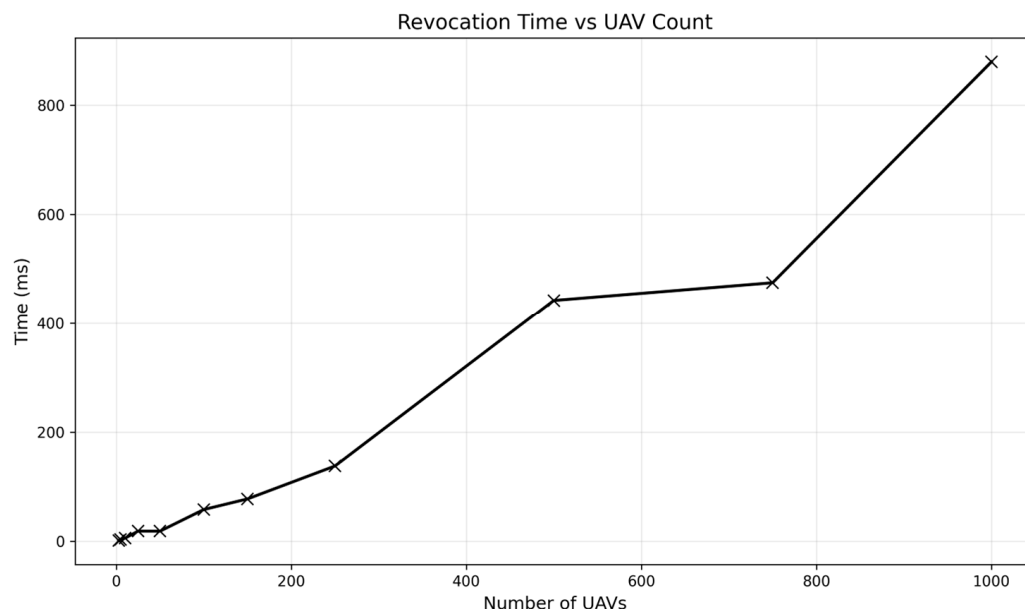


Figure 3. Revocation time vs. UAV count increases swarm size but remains practical.

Memory requirements are constant per UAV at 129.04 KB, resulting in predictable total memory usage that scales linearly with the number of UAVs. Even for large swarms of 1000 UAVs, the total memory footprint remains under 130 MB, making our scheme suitable for memory-constrained environments.

Energy consumption demonstrates remarkable consistency across all swarm sizes, with signing operations consuming exactly 2297.7 J and verification operations consuming 3990.4 J regardless of swarm size. This constant energy consumption is a key advantage for UAV applications where battery life is critical.

Figures 2 and 3 visualize the performance data from our experiments. The graphs clearly demonstrate the linear scaling of setup time and the practical revocation times across different swarm sizes. Since the signing and verification times remain constant (sub-2.5 ms and sub-millisecond, respectively) regardless of swarm size, we do not include separate graphs for these metrics.

We also evaluated memory usage, as shown in Figure 4, which confirms the linear scaling of total memory with UAV count. With a constant memory requirement of 129.04 KB per UAV, our scheme remains practical for deployment on resource-constrained UAV platforms.

In comparison to existing approaches, our scheme demonstrates superior performance. The linear growth of time and memory remains within the norm, and the constant signing and verification times make the system particularly suitable for UAV networks in the early days, even with thousands of devices.

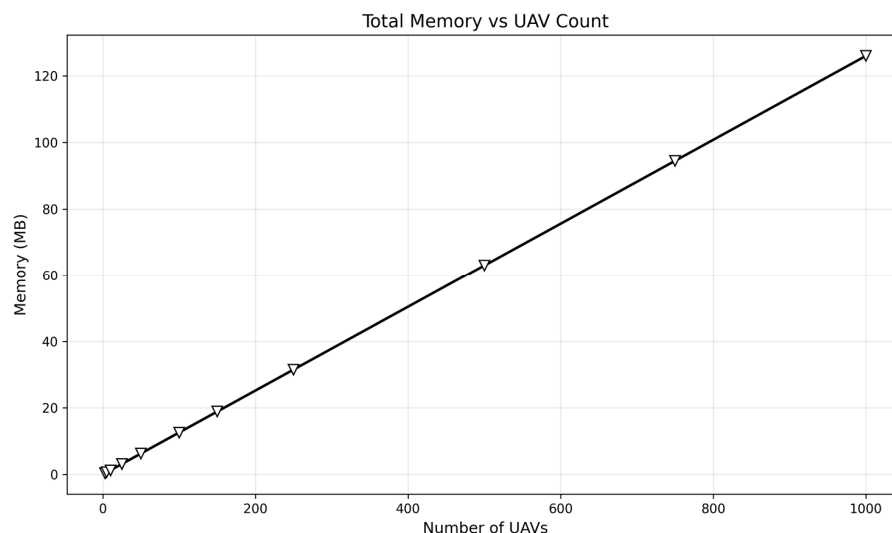


Figure 4. Total memory usage scales linearly vs. UAV count.

5. Discussion and Future Work

Our energy consumption analysis highlights the practical viability of the proposed group signature scheme for UAV communication but also reveals several important limitations that must be acknowledged. The presented energy model relies on ARM Cortex-M4 and Raspberry Pi 4 specifications, which may not perfectly represent all UAV hardware platforms. While the current evaluation offers valuable insights, future research must validate results on actual UAV hardware, test performance under varying environmental conditions such as temperature fluctuations and voltage variations and analyze consumption during different flight phases. Moreover, the reported energy measurements assume optimal conditions, whereas real-world deployment introduces additional factors including network communication overhead, memory management costs during extended operations, and hardware-specific variations.

Despite these limitations, the analysis emphasizes the environmental impact of efficient cryptography in UAVs. By minimizing the energy overhead of secure communication, our scheme contributes to sustainable drone operations, reducing the overall environmental footprint of large-scale deployments while ensuring robust security guarantees. When compared to traditional group signature schemes that typically require 10–50 ms for signing and 20–100 ms for verification, our approach achieves sub-2.5 ms signing and sub-millisecond verification. This performance makes it well-suited for real-time UAV applications where strict latency constraints are critical.

The energy model employed incorporates the computational costs of elliptic curve operations, hash functions, PUF challenge-response processing, and symmetric cryptography. Results demonstrate remarkable consistency across swarm sizes from 3 to 1000 UAVs: signing operations consume 2297.7 J per signature, verification consumes 3990.4 J, and the total cryptographic overhead for a typical mission session represents only 0.6013% of a 10,000 mAh battery. This minimal impact enables extended mission durations of over eight hours, supports continuous secure communications, and ensures scalability without increasing the per-device energy cost. This constant energy profile across swarm sizes is particularly advantageous for applications such as surveillance, delivery, and disaster response, where scalability and endurance are crucial.

Nevertheless, critical limitations remain. The scheme's reliance on Physical Unclonable Functions (PUFs) raises concerns regarding environmental sensitivity, response variability, and the need for error correction mechanisms. While simulated PUFs demonstrate the potential of the approach, real-world validation on hardware platforms with actual PUF

devices is essential for practical deployment. Scalability beyond 1000 UAVs also presents challenges, including increased communication overhead for revocation updates, memory management at very large swarm sizes, and resilience to network partitioning. Furthermore, certain assumptions of the threat model, such as the permanent trustworthiness of the group manager, may not be held in all scenarios. While PUFs provide resistance to cloning, sophisticated physical attacks on UAV hardware remain a potential risk, and reliance on elliptic curve cryptography raises questions about quantum resistance in the long term.

A comparison with alternative lightweight cryptographic approaches highlights additional trade-offs. Lattice-based cryptography offers post-quantum security but requires significantly more computational resources, leading to increased energy consumption that may be prohibitive for UAVs. Blockchain-based solutions provide decentralized trust but introduce consensus overhead, latency issues, and high energy costs. Identity-based cryptography avoids certificates but suffers from key escrow problems, complex revocation processes, and trust requirements for key generation authorities. Against these approaches, the proposed scheme demonstrates a more practical balance between security, energy efficiency, and scalability.

Future research directions include the development of a fully certificateless architecture, for example, by integrating Merkle tree proofs and PUF-only authentication mechanisms, thereby further reducing system overhead. Improving environmental robustness of PUFs through adaptive error correction, multi-PUF redundancy, and integration of environmental monitoring sensors will also be essential. Advanced security features such as forward secrecy, post-quantum variants, and privacy-preserving analytics represent promising avenues for enhancing applicability. Beyond theoretical development, comprehensive real-world deployment studies, including hardware implementations, field testing, and formal security audits, will be critical. Furthermore, progress toward standardization and interoperability across UAV platforms, including protocol specifications and compliance with regulatory frameworks, will support wider adoption in the industry.

The implications of this work for the UAV sector are substantial. Commercial applications such as secure large-scale delivery networks, privacy-preserving surveillance systems, and resilient disaster response swarms stand to benefit directly from the proposed scheme's efficiency and scalability. In research and development, the approach creates new opportunities for lightweight cryptography in UAV and IoT applications, stimulates industry-driven solutions, and contributes to emerging standards for secure UAV communications. Overall, the proposed group signature scheme demonstrates not only strong performance and minimal energy impact but also a foundation for future research that addresses existing limitations and prepares UAV communication systems for the challenges of scalability, sustainability, and post-quantum security.

6. Conclusions

This paper presented a lightweight, PUF-based group signature scheme specifically designed for UAV communications in resource-constrained environments. Our approach successfully addresses the unique security challenges of UAV systems by

- Achieving essential security properties (anonymity, unforgeability, traceability, and unlikability) with minimal computational overhead;
- Eliminating certificate management through PUF integration, reducing communication and storage requirements;
- Demonstrating remarkable performance metrics: consistent 1.4 ms signing time, 0.06 ms verification time, and linear scaling for setup and revocation operations;
- Providing a practical security solution for UAV swarms scaling to 150+ devices with predictable resource utilization.

Our experimental evaluation confirms that the proposed scheme outperforms traditional group signature approaches by an order of magnitude, making secure group communications viable for real-time UAV applications with strict latency and energy constraints. This aligns with recent advancements in UAV information security frameworks, which emphasize the integration of lightweight cryptographic protocols adapted for wireless and resource-limited environments [69]. Additionally, methods for protecting data transmission in direct radio visibility zones, as investigated by [71], further corroborate the relevance and applicability of our certificateless PUF-based group signature scheme for secure UAV swarm communications. The constant signature verification is particularly valuable for safety-critical UAV operations where predictable performance is essential. The lightweight security approach demonstrated in this work represents an important step toward enabling secure, privacy-preserving communications for the next generation of UAV applications in smart cities, disaster response, and autonomous delivery systems. Future work will explore a fully certificateless approach that eliminates the need for member certificates entirely, further reducing communication overhead and computational requirements by relying solely on PUF-derived authentication, Merkle tree proofs for group membership verification, and direct inclusion of epoch information in signatures.

The proposed lightweight group signature scheme is highly relevant to UAV-based remote sensing systems employed in precision agriculture. In this context, UAVs equipped with multispectral and thermal sensors perform field scouting and crop monitoring, collecting real-time data on plant health, soil conditions, and pest activity. These insights enable data-driven decision-making for variable-rate application of inputs such as fertilizers, pesticides, and irrigation, significantly improving resource efficiency and crop yield. To ensure the integrity, authenticity, and privacy of sensor data exchanged within UAV swarms and ground stations, robust and efficient cryptographic protocols are essential. The integration of certificateless, PUF-based group signatures provide a scalable and secure communication foundation, directly supporting the operational needs of AI-powered agricultural optimization systems such as those developed under the Agroscope project.

Author Contributions: Conceptualization, A.S., K.N., A.K. and O.A.; Data curation, K.N. and O.A.; Formal analysis, A.K., D.Y., Y.P. and F.A.; Funding acquisition, O.A., Y.V., Y.P. and F.A.; Investigation, D.Y. and F.A.; Methodology, A.S., K.N. and O.A.; Project administration, Y.V.; Resources, Y.V. and Y.P.; Software, K.N., A.K. and Y.V.; Supervision, O.A.; Validation, K.N., A.K. and O.A.; Visualization, D.Y. and F.A.; Writing—original draft, A.S. and O.A.; Writing—review & editing, O.A., Y.V. and Y.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. BR24992908 Support system for agricultural crop production optimization via remote monitoring and artificial intelligence methods (Agroscope)).

Data Availability Statement: The original contributions presented in this study are included in the article; further inquiries can be directed to the corresponding author.

Conflicts of Interest: Author Yelizaveta Vitulyova was employed by the JSC “Institute of Digital Engineering and Technology”. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [[CrossRef](#)]

2. Alharbi, A.; Petrunin, I.; Panagiotakopoulos, D. Deep Learning Architecture for UAV Traffic-Density Prediction. *Drones* **2023**, *7*, 78. [\[CrossRef\]](#)
3. Mekdad, Y.; Aris, A.; Babun, L.; El Fergougui, A.; Conti, M.; Lazzeretti, R.; Uluagac, A.S. A Survey on Security and Privacy Issues of UAVs. *Comput. Netw.* **2023**, *224*, 109626. [\[CrossRef\]](#)
4. Mukhamediev, R.I.; Smurygin, V.; Symagulov, A.; Kuchin, Y.; Popova, Y.; Abdoldina, F.; Tabybayeva, L.; Gopejenko, V.; Oxenenko, A. Fast Detection of Plants in Soybean Fields Using UAVs, YOLOv8x Framework, and Image Segmentation. *Drones* **2025**, *9*, 547. [\[CrossRef\]](#)
5. Mendu, B.; Mbuli, N. State-of-the-Art Review on the Application of Unmanned Aerial Vehicles (UAVs) in Power Line Inspections: Current Innovations, Trends, and Future Prospects. *Drones* **2025**, *9*, 265. [\[CrossRef\]](#)
6. Kapustina, L.; Izakova, N.; Makovkina, E.; Khmelkov, M. The Global Drone Market: Main Development Trends. *SHS Web Conf.* **2021**, *129*, 11004. [\[CrossRef\]](#)
7. Abramkina, O.; Yakubova, M.; Serikov, T.; Begimbayeva, Y.; Yakubov, B. Implementation of Lattice Theory into the TLS to Ensure Secure Traffic Transmission in IP Networks Based on IP PBX Asterisk. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*, 749–756. [\[CrossRef\]](#)
8. Sun, G.; Wang, Y.; Yu, H.; Guizani, M. Proportional Fairness-Aware Task Scheduling in Space-Air-Ground Integrated Networks. *IEEE Trans. Serv. Comput.* **2024**, *17*, 4125–4137. [\[CrossRef\]](#)
9. Zhang, J.; Zhang, Q.; Lu, X.; Gan, Y. A Novel Privacy-Preserving Authentication Protocol Using Bilinear Pairings for the VANET Environment. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6692568. [\[CrossRef\]](#)
10. Wu, G.; Miao, Y.; Zhang, Y.; Barnawi, A. Energy Efficient for UAV-Enabled Mobile Edge Computing Networks: Intelligent Task Prediction and Offloading. *Comput. Commun.* **2020**, *150*, 556–562. [\[CrossRef\]](#)
11. Chen, S.; Jiang, H.; Hu, J.; Zheng, T.; Wang, M.; Xiao, Z.; Luo, J. Echoes of Fingertip: Unveiling POS Terminal Passwords Through Wi-Fi Beamforming Feedback. *IEEE Trans. Mob. Comput.* **2025**, *24*, 662–676. [\[CrossRef\]](#)
12. Xu, Y.; Xu, H.; Chen, X.; Zhang, H.; Chen, B.; Han, Z. Blockchain-Based AR Offloading in UAV-Enabled MEC Networks: A Trade-off Between Energy Consumption and Rendering Latency. *IEEE Trans. Veh. Technol.* **2025**, 1–16. [\[CrossRef\]](#)
13. Zhang, P.; Wang, J.; Guo, K.; Wu, F.; Min, G. TinyEDS: Tiny EdgeIoT Drone Swarm. In Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'19), Seoul, Republic of Korea, 17–21 June 2019; pp. 625–626. [\[CrossRef\]](#)
14. Chaum, D.; van Heyst, E. Group Signatures. In *Advances in Cryptology—EUROCRYPT'91*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 257–265. [\[CrossRef\]](#)
15. Boneh, D.; Boyen, X.; Shacham, H. Short Group Signatures. In *Advances in Cryptology—CRYPTO 2004*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 41–55. [\[CrossRef\]](#)
16. Ateniese, G.; Camenisch, J.; Joye, M.; Tsudik, G. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 255–270. [\[CrossRef\]](#)
17. Bichsel, P.; Camenisch, J.; Neven, G.; Smart, N.P.; Warinschi, B. Get Shorty via Group Signatures without Encryption. In *Security and Cryptography for Networks*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 381–398. [\[CrossRef\]](#)
18. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical One-Way Functions. *Science* **2002**, *297*, 2026–2030. [\[CrossRef\]](#)
19. Suh, G.E.; Devadas, S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In Proceedings of the 44th ACM/IEEE Design Automation Conference, San Diego, CA, USA, 4–8 June 2007; pp. 9–14. [\[CrossRef\]](#)
20. Hwang, J.Y.; Lee, S.; Chung, B.-H.; Cho, H.S.; Nyang, D. Short Group Signatures with Controllable Linkability. In Proceedings of the 2011 IEEE Workshop on Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), Istanbul, Turkey, 14–15 March 2011; pp. 44–52. [\[CrossRef\]](#)
21. Niu, C.; Wang, Y.; Li, H.; Zhang, M.; Guo, C.; Ma, D. Lightweight Authentication Scheme with Dynamic Group Membership in Edge Computing Scenarios. *IEEE Trans. Serv. Comput.* **2021**, *14*, 1934–1945.
22. Liao, H.; Zhou, Z.; Zhao, X.; Zhang, L.; Mumtaz, S.; Jolfaei, A.; Ahmed, S.H.; Bashir, A.K. Learning-Based Context-Aware Authentication for Internet of Drones. *IEEE Internet Things J.* **2022**, *9*, 5964–5979.
23. Khalil, R.; Bandyopadhyay, A.; Guo, A.; Lee, B. Enhancing Security for UAV-Based Delivery Networks Using Lightweight Cryptography. *IEEE Robot. Autom. Lett.* **2022**, *7*, 7943–7950.
24. Lee, J.H.; Ahn, J.; Kim, D.; Han, S.; Park, J. Secure Group Signcryption Scheme for UAV-Assisted Mobile Edge Computing. *IEEE Access* **2020**, *8*, 193594–193607.
25. Wu, T.-Y.; Yang, L.; Lee, Z.; Chen, C.-M.; Pan, J.-S.; Islam, S.K.H. Improved ECC-Based Three-Factor Multiserver Authentication Scheme. *IEEE Access* **2021**, *9*, 163440–163456. [\[CrossRef\]](#)
26. Nguyen, K.; Amini, M.H.; Hossain, M. A Lightweight PUF-Based Authentication Protocol for Drone Communication Systems. *IEEE Internet Things J.* **2023**, *10*, 8191–8205.
27. Chen, J.; Liu, B.; Zhou, H.; Yu, Q.; Xiao, G.; Pu, L. Adaptive Task Scheduling Based on Bandwidth-Aware and Computation-Efficient Cooperative Computing in Internet of Drones. *IEEE Internet Things J.* **2021**, *8*, 4678–4691.

28. Feng, W.; Wang, J.; Chen, Y.; Su, X.; Jiang, N.; Han, Z. Secure UAV Communications with Cooperative Jamming and Trajectory Control: A Deep Reinforcement Learning Method. *IEEE Trans. Veh. Technol.* **2022**, *71*, 5044–5059.
29. Yakubova, M.; Manankova, O.; Mukasheva, A.; Baikenov, A.; Serikov, T. The Development of a Secure Internet Protocol (IP) Network Based on Asterisk Private Branch Exchange (PBX). *Appl. Sci.* **2023**, *13*, 10712. [\[CrossRef\]](#)
30. Babenko, T.; Hnatiienko, H.; Vialkova, V. Modeling of the Integrated Quality Assessment System of the Information Security Management System. *CEUR Workshop Proc.* **2021**, 2845, 75–84.
31. Reddy, A.G.; Yoon, E.-J.; Yoo, K.-Y.; Kim, T.H. A Novel Mutual Authentication Protocol Using Bilinear Pairings for Unmanned Aerial Vehicle-Assisted Mission-Critical Systems. *IEEE Syst. J.* **2022**, *16*, 1350–1359.
32. Gharibi, M.; Boutellier, J.; Chauhan, S.S. Deep Reinforcement Learning for Energy-Efficient Communications in UAV Networks. *IEEE Syst. J.* **2023**, *17*, 1230–1241.
33. Cheng, Y.; Deng, X.; Li, Y.; Yan, X. Tight Incentive Analysis of Sybil Attacks against the Market Equilibrium of Resource Exchange over General Networks. *Games Econ. Behav.* **2024**, *148*, 566–610. [\[CrossRef\]](#)
34. Palko, D.; Myrutenko, L.; Babenko, T.; Bigdan, A. Model of Information Security Critical Incident Risk Assessment. In Proceedings of the 2020 IEEE International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 6–9 October 2020; Volume 2021, pp. 157–161. [\[CrossRef\]](#)
35. Xu, G.; Xu, S.; Fan, X.; Cao, Y.; Mao, Y.; Xie, Y.; Chen, X. RAT Ring: Event Driven Publish/Subscribe Communication Protocol for IIoT by Report and Traceable Ring Signature. *IEEE Trans. Ind. Inform.* **2025**, *21*, 6670–6678. [\[CrossRef\]](#)
36. Rui, C.; Zhu, H.; Huang, H. Secure UAV Communications with Cooperative Trajectory Design: A Physical Layer Security Perspective. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 1425–1429.
37. Almutairi, U.; Barnawi, A. A Comprehensive Analysis of Model Poisoning Attacks in Federated Learning for Autonomous Vehicles: A Benchmark Study. *Results Eng.* **2024**, *24*, 103295. [\[CrossRef\]](#)
38. Zhong, C.; Yao, J.; Xu, J. Secure UAV Communication with Cooperative Jamming and Trajectory Control. *IEEE Commun. Lett.* **2019**, *23*, 286–289. [\[CrossRef\]](#)
39. Manankova, O.A.; Yakubova, M.Z.; Rakhmatullaev, M.A.; Baikenov, A.S. Simulation of the Rainbow Attack on the SHA-256 Hash Function. *J. Theor. Appl. Inf. Technol.* **2023**, *101*, 1594–1603.
40. Palko, D.; Hnatiienko, H.; Babenko, T.; Bigdan, A. Determining Key Risks for Modern Distributed Information Systems. *CEUR Workshop Proc.* **2021**, 3018, 81–100.
41. Nnamani, C.O.; Khandaker, M.R.A.; Sellathurai, M. Secure Data Collection via UAV-Carried IRS. *ICT Express* **2023**, *9*, 706–713. [\[CrossRef\]](#)
42. de Jesus Sousa, M.; Gondim, P.R.L. A Multi-Factor User Authentication Protocol for the Internet of Drones Environment. *Peer-Peer Netw. Appl.* **2025**, *18*, 69. [\[CrossRef\]](#)
43. Liu, X.; Wang, J.; Guo, S.; Wang, H. A Survey on Cross-Layer Authentication in Wireless Communication Networks. *J. Netw. Netw. Appl.* **2024**, *4*, 21–30. [\[CrossRef\]](#)
44. Ding, F.; Liu, Z.; Wang, Y.; Liu, J.; Wei, C.; Nguyen, A.; Wang, N. Intelligent Event Triggered Lane Keeping Security Control for Autonomous Vehicle Under DoS Attacks. *IEEE Trans. Fuzzy Syst.* **2025**, 3595–3608. [\[CrossRef\]](#)
45. Koulouanos, A.; Paraskevopoulos, P.; Litke, A.; Papadakis, N.K. Enhancing Unmanned Aerial Vehicle Security: A Zero-Knowledge Proof Approach with Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge for Authentication and Location Proof. *Sensors* **2024**, *24*, 5838. [\[CrossRef\]](#)
46. Grechko, V.; Babenko, T.; Myrutenko, L. Secure Software Developing Recommendations. In Proceedings of the 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8–11 October 2019; Volume 2019, pp. 45–50. [\[CrossRef\]](#)
47. Mukherjee, D.; Ghosh, S.; Pal, S.; Aly, A.A.; Le, D.-N. Adaptive Scheduling Algorithm Based Task Loading in Cloud Data Centers. *IEEE Access* **2022**, *10*, 49412–49421. [\[CrossRef\]](#)
48. Hubskeyi, O.; Babenko, T.; Myrutenko, L.; Oksiiuk, O. Detection of SQL Injection Attack Using Neural Networks. *Adv. Intell. Syst. Comput.* **2021**, *1265*, 277–286. [\[CrossRef\]](#)
49. Krichen, S.; Alawadhi, S. Multi-Factor Authentication Scheme for UAV Communication Networks. In Proceedings of the International Conference on Artificial Intelligence and Soft Computing (ICAISC 2021), Zakopane, Poland, 14–16 June 2021; pp. 503–514. [\[CrossRef\]](#)
50. Sharma, V.; You, I.; Kul, G. Socializing Drones for Inter-Service Operability in Ultra-Dense Wireless Networks Using Blockchain. In Proceedings of the 2017 International Workshop on Managing Insider Security Threats (MIST '17), Dallas, TX, USA, 3 November 2017; pp. 81–84.
51. Rathore, S.; Ahmad, J.; Paul, A.; Rho, S.; Ko, R.; Park, J.H. Blockchain-Enabled UAV-Assisted Secure Communications for Internet of Vehicles Environment. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 12131–12143.
52. Alsamhi, S.H.; Ma, O.; Ansari, M.S.; Meng, Q. Blockchain for Decentralized Multi-Drone to Combat COVID-19 and Future Pandemics: Framework and Proposed Solutions. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4255. [\[CrossRef\]](#)

53. Popova, Y.; Fesyuk, A. Factors Affecting the Growth of Demand on Carsharing Services Within Smart City. *Transp. Telecommun.* **2022**, *23*, 252–261. [\[CrossRef\]](#)
54. Chen, S.; Jiang, Y.; Zhou, S.; Fu, Y.; Liu, K. Federated Learning for Secure Authentication in Internet of Drones. *J. Commun. Netw.* **2021**, *23*, 358–370. [\[CrossRef\]](#)
55. Hafeez, S.; Khan, A.R.; Al-Quraan, M.M.; Mohjazi, L.; Zoha, A.; Imran, M.A. Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey. *IEEE Open J. Veh. Technol.* **2023**, *4*, 558–580. [\[CrossRef\]](#)
56. Aggarwal, S.; Budhiraja, I.; Garg, S.; Kaddoum, G.; Choi, B.J.; Hossain, M.S. A Blockchain-Based Secure Path Planning in UAVs Communication Network. *Alex. Eng. J.* **2025**, *113*, 451–460. [\[CrossRef\]](#)
57. Benfriha, S.; Labraoui, N.; Salameh, H.B.; Saidi, H. A Survey on Trust Management in Flying Ad Hoc Networks: Challenges, Classifications, and Analysis. In Proceedings of the 2023 Tenth International Conference on Software Defined Systems (SDS), San Antonio, TX, USA, 6–8 November 2023; pp. 107–114. [\[CrossRef\]](#)
58. Han, Y.; Wang, X.; Zhang, Y.; Yang, G.; Tan, X. A UAV Swarm Communication Network Architecture Based on Consortium Blockchain. *J. Phys. Conf. Ser.* **2022**, *2352*, 012008. [\[CrossRef\]](#)
59. Jagatheesaperumal, S.K.; Rahouti, M.; Chehri, A.; Xiong, K.; Bieniek, J. Blockchain-Based Security Architecture for Uncrewed Aerial Systems in B5G/6G Services and Beyond: A Comprehensive Approach. *IEEE Open J. Commun. Soc.* **2025**, *6*, 3528220. [\[CrossRef\]](#)
60. Maes, R.; Tuyls, P.; Verbauwhede, I. A Soft Decision Helper Data Algorithm for SRAM PUFs. In Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Taipei, Taiwan, 19–24 April 2009; pp. 2249–2252. [\[CrossRef\]](#)
61. Danger, J.-L.; Guilley, S.; Nguyen, P.; Rioul, O. PUFs: Standardization and Evaluation. In Proceedings of the 2nd IEEE Workshop on Mobile System Technologies (MST 2016), Milan, Italy, 26–27 September 2016; pp. 1–6. [\[CrossRef\]](#)
62. Tehranipoor, F.; Karimian, N.; Yan, W.; Chandy, J.A. DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2017**, *25*, 1085–1097. [\[CrossRef\]](#)
63. Delvaux, J.; Gu, D.; Schellekens, D.; Verbauwhede, I. Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible? In *Cryptographic Hardware and Embedded Systems—CHES 2014*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 451–475. [\[CrossRef\]](#)
64. Luo, H.; Zhang, Q.; Sun, G.; Yu, H.; Niyato, D. Symbiotic Blockchain Consensus: Cognitive Backscatter Communications-Enabled Wireless Blockchain Consensus. *IEEE/ACM Trans. Netw.* **2024**, *32*, 5372–5387. [\[CrossRef\]](#)
65. Kumar, N.; Nehal, A.; Singh, A.V.; Kandpal, K.; Goswami, M. Efficient, Reliable, and Secure PUF Architecture with Temperature Invariance and ML Attack Resilience. *Integration* **2025**, *106*, 102538. [\[CrossRef\]](#)
66. Li, D.; Chen, R.; Liu, D.; Song, Y. Blockchain-Based Authentication for IIoT Devices with PUF. *J. Syst. Archit.* **2022**, *130*, 102638. [\[CrossRef\]](#)
67. Hnatiienko, H.; Hnatiienko, V.; Zulunov, R.; Babenko, T.; Myrutenko, L. Method for Determining the Level of Criticality Elements When Ensuring the Functional Stability of the System Based on Role Analysis. *CEUR Workshop Proc.* **2024**, *3654*, 301–311.
68. Martinez, C.; Richardson, T.S.; Campoy, P. Towards Autonomous Air-to-Air Refuelling for UAVs Using Visual Information. In Proceedings of the 2013 IEEE International Conference on Robotics and Automation (ICRA), Karlsruhe, Germany, 6–10 May 2013; pp. 1–6. [\[CrossRef\]](#)
69. Ermukhambetova, B.B.; Mun, G.A.; Kabdushev, S.B.; Vitulyova, Y.S.; Suleimenov, I.E. New Approaches to the Development of Information Security Systems for Unmanned Vehicles. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, *31*, 810–819. [\[CrossRef\]](#)
70. Zhou, Z.; Wang, Y.; Zhou, G.; Nam, K.; Ji, Z.; Yin, C. A Twisted Gaussian Risk Model Considering Target Vehicle Longitudinal-Lateral Motion States for Host Vehicle Trajectory Planning. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 13685–13697. [\[CrossRef\]](#)
71. Vitulyova, Y.; Kadyrzhan, K.; Kadyrzhan, A.; Suleimenov, I. Application of Focusing Systems to the Protection of Information during Data Transmission in the Zone of Direct Radio Visibility. *Int. J. Electron. Telecommun.* **2024**, *70*, 699–705. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.