frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 02 February 2026
DOI 10.3389/fphy.2026.1698126

Check for updates

OPEN ACCESS

EDITED BY
Youssri Hassan Youssri,
Egypt Uinversity of Informatics, Egypt

REVIEWED BY
Omprakash Kaiwartya,
Nottingham Trent University, United Kingdom
Rajkumar S. C.,
Anna University Chennai - Regional Campus Madurai, India

*CORRESPONDENCE
Yinuo Zhang,
✉ 35212019031@nue.edu.cn

RECEIVED 03 September 2025
REVISED 19 November 2025
ACCEPTED 12 January 2026
PUBLISHED 02 February 2026

CITATION
Wang Z, Li J, Yuan S and Zhang Y (2026) An efficient group key agreement scheme for UAV swarms.
Front. Phys. 14:1698126.
doi: 10.3389/fphy.2026.1698126

An efficient group key agreement scheme for UAV swarms

Zhe Wang, Jing Li, Shengzhi Yuan and Yinuo Zhang*

School of Weapon Engineering, Naval University of Engineering, Wuhan, Hubei, China

Unmanned Aerial Vehicle (UAV) group communication plays a crucial role in collaborative UAV operations, yet its security faces numerous challenges. Authentication and key agreement protocols, as core technologies for securing UAV communications, have significant research value. In the context of UAV group communication, this paper introduces a dynamic authentication and group key negotiation protocol leveraging elliptic curve signature techniques. By incorporating group key agreement techniques, the proposed protocol offloads complex key computation tasks to the cluster controller, thereby effectively alleviating the problem of limited UAV computational resources and significantly improving overall system efficiency. The proposed protocol supports dynamic joining and leaving of UAV groups, ensuring essential security properties such as backward secrecy and forward secrecy, thus guaranteeing the security and adaptability of group communication. Based on the random oracle model, this paper employs formal security proofs to verify the protocol's security and further demonstrates through informal security analysis that it can effectively resist both active and passive attacks. Performance evaluation results show that the proposed protocol outperforms existing schemes in terms of computational and communication overhead, achieving both efficiency and security, making it suitable for resource-constrained UAV group communication environments with broad application prospects.

KEYWORDS

UAV, group communication, authentication, anonymous, group key agreement, ellipticcurve cryptography

Highlights

- An efficient dynamic group key negotiation protocol is developed to support secure authentication and key updates for UAV group communications.
- Under the random oracle model, the security of the protocol is validated through formal proofs, while informal analysis further confirms its ability to resist both active and passive attacks.
- Performance evaluation results indicate that the proposed protocol achieves reduced computational and communication overhead.

1 Introduction

In recent years, the rapid advancement of Unmanned Aerial Vehicle (UAV) technology has positioned UAV swarms not merely as efficient machines, but as critical components of Cyber-Physical Social Systems (CPSS). By enabling multiple autonomous agents to engage in collective action and distributed decision-making (e.g., coordinated data collection), UAV swarms offer superior efficiency and robustness. This dynamic, interacting collective forms an essential, autonomous layer for applications central to Sociophysics and network science, such as Smart City infrastructure monitoring, large-scale crowd behavior analysis, and rapid disaster response—all of which rely heavily on secure, timely data. Nevertheless, in real-world deployments, UAV swarms unavoidably encounter significant challenges regarding secure communications, especially concerning the security of group communications [1]. Given the highly dynamic nature of UAV swarm communication, the large-scale number of nodes, and the frequent changes in communication links, conventional group key agreement schemes are often unsuitable for such complex environments. Consequently, the design of efficient, secure, and dependable group key agreement protocols tailored for UAV swarm communications has emerged as a pressing research challenge that must be addressed [2].

In UAV swarm communications, current group authentication and key agreement protocols remain subject to notable shortcomings and constraints. For instance, certificate-based public key authentication entails frequent certificate updates and revocations, incurring significant communication and storage costs, and is thus poorly suited to UAV swarm networks with resource constraints and highly dynamic topologies. Identity-based public key authentication schemes, while avoiding certificates and streamlining both authentication and key management, require frequent bilinear pairing operations that impose a considerable computational load on UAV nodes, necessitating efforts to minimize their use in real deployments. Conversely, relative to conventional pairwise keys, the application of group keys markedly decreases the frequency of encryption and decryption in communication, thereby enhancing the efficiency of information transmission within UAV swarms. Nonetheless, group key negotiation protocols without identity authentication present grave security vulnerabilities: attackers may acquire group keys via forgery, replay, and similar attacks, while malicious insiders within the swarm may interfere with the negotiation process. Therefore, to secure UAV swarm communications, it is imperative to design a group key agreement protocol that incorporates efficient identity authentication mechanisms, thereby effectively countering diverse potential attack vectors [3–5].

At present, studies on group key agreement in UAV swarm environments primarily emphasize achieving a balance among security, communication overhead, and computational burden. On the one hand, UAV nodes usually rely on lightweight embedded systems with constrained computing and storage resources, rendering them unable to support intensive cryptographic computations. On the other hand, UAV swarm communication links change rapidly, and node topologies frequently fluctuate, necessitating frequent group key updates to prevent data leakage or the spread of compromised keys when nodes are infiltrated. Thus, an efficient group key negotiation protocol should maintain security while reducing computational complexity and communication overhead to suit the resource-constrained UAV nodes and the highly dynamic nature of swarm network topologies. In response to these challenges, this paper introduces an efficient group key negotiation protocol for UAV swarms, designed to reconcile the trade-offs between communication overhead, computational complexity, and security robustness. The proposed scheme accounts for both the dynamic nature and the resource limitations of UAV swarm communications, optimizing existing key negotiation protocols to reduce inter-node message exchanges and computational costs, thereby simplifying the key agreement process. The primary contributions of this work can be summarized as follows:

1. For UAV group communications, this paper employs an elliptic curve signature mechanism to achieve device authentication and message verification. To mitigate the resource limitations of UAVs, the protocol utilizes group key agreement technology to offload complex key negotiation computations to the group controller, thereby reducing the computational burden on UAVs and improving overall operational efficiency.
2. An efficient dynamic group key agreement protocol is designed to support secure authentication and key updates for UAV groups during dynamic joining and leaving processes. By leveraging fast scalar multiplication, the protocol achieves low-latency key updates while ensuring essential properties such as forward and backward secrecy, thereby maintaining the security and adaptability of group communications.
3. Under the Random Oracle Model, the security of the proposed protocol is formally proven, and informal analysis further confirms its ability to resist both active and passive attacks. Performance evaluation results demonstrate that the proposed protocol significantly reduces both computational and communication costs, exhibiting outstanding performance advantages.

1.1 Related works

Given the limited operational range of an individual UAV, real-world applications typically necessitate the concurrent deployment of multiple UAV to enable cooperation. Under these circumstances, group communication among UAV proves to be of vital importance. In light of the significant risk of information leakage when data is transmitted to recipients in public and open settings, the establishment of confidential group keys among group members constitutes the cornerstone for safeguarding the security of group communications. A comparative summary of existing schemes in Table 1.

Sharma et al. [6] proposed a lightweight member authentication and group key establishment scheme for resource-limited smart environments based on symmetric bivariate polynomials. Leveraging symmetric bivariate polynomials, Hsu et al. [7] introduced a lightweight authentication structure incorporating collaborative arithmetic computation within 5G IoT networks. This framework merges member authentication with cooperative arithmetic operations, thereby guaranteeing efficient computation and communication for all group members. Tian et al. [8] presented a privacy-preserving approach tailored for IoD scenarios, employing online/offline signature schemes. They further suggested an authentication scheme based on mobile edge computing. However, their scheme is computationally heavy as it uses RSA-based digital signature approach. Zhang et al. [9] developed an alternative lightweight authentication and key negotiation protocol for IoD environments, in which authentication relies solely on one-way hash functions and XOR computations. However, UAV is required to

TABLE 1 A comparative summary.

Reference	Main technique	Application scenario	Main limitations
[6]	Symmetric bivariate polynomials	Resource-constrained smart environments	Lacks resistance to replay and physical attacks
[7]	Symmetric polynomials	5G IoT networks	Insufficient security analysis
[8]	Signature	Internet of drones	RSA-based signatures are computationally heavy
[9]	Hash and XOR operations	Internet of drones	UAVs must store credentials, vulnerable to physical attacks
[10]	Certificateless group authentication	UAV communications	Cannot resist replay or man-in-the-middle attacks; lacks dynamic management
[11]	Cross-domain certificateless group key agreement	Multi-domain UAV communication	Assumes adversaries have limited capability
[12]	Heterogeneous three-factor authentication and key negotiation	UAV–ground control communication	High computational cost from bilinear pairings; lacks mutual authentication
[13]	Pairing-free asymmetric group key negotiation	Multi-node UAV communication	Each member has unique decryption key; heavy computation
[14]	Lightweight certificateless key agreement	IoT/UAV environments	Still relies on bilinear pairings

store secure credentials within this protocol to prove their identity to other entities. This leads to a potential security risk, since a physical attack on a UAV could expose its stored credentials to adversaries. Current authentication protocols are similarly vulnerable to privacy and security risks stemming from physical attacks on UAV.

Semal et al. [10] introduced a certificateless group authentication and key agreement (CL-GAKA) protocol. The protocol ensures confidentiality, integrity, and authenticity in UAV communications. However, their scheme is unable to resist replay attacks and man-in-the-middle tampering attacks. Furthermore, it supports trusted communication, anonymity, and user privacy protection for communications involving untrusted UAV. However, it lacks the ability to manage dynamic changes in UAV, including join and leave operations. Luo et al. [11] presented a cross-domain certificateless group key agreement protocol that allows group key negotiation among members from different domains with diverse parameters in just a single communication round. While supporting dynamic group operations, the protocol assumes adversaries of limited capability; specifically, an attacker cannot substitute a specific user's public key without access to the master key. Pan et al. [12] designed a heterogeneous authentication and key negotiation protocol between UAV and ground control stations, incorporating three-factor authentication. This scheme, however, requires extensive bilinear pairing computations, leading to significant computational overhead, and with only two rounds of communication, it likewise lacks explicit mutual authentication. Breaken et al. [13] developed a pairing-free asymmetric group key negotiation scheme, notable for using only a single encryption-decryption key pair. However, because each group member holds a unique decryption key, generating these keys typically results in considerable computational overhead. Kermanshahi et al. [14] developed a lightweight certificateless key agreement scheme that, although still relying on bilinear pairings, significantly improves computational efficiency while maintaining security strength, compared to the scheme proposed by others at the same time [15]. Kumar et al. [16] proposed a certificateless group key agreement architecture based on elliptic curve cryptography (ECC) that eliminates the need for bilinear pairings. This scheme utilizes a ring topology network structure to achieve multi-node collaborative key management, significantly reducing computational complexity and communication overhead while ensuring forward security. Ayad et al. [17] designed a two-round certificateless group key agreement mechanism tailored to the communication needs of UAV swarms. The innovation of their approach lies in decoupling key agreement from identity authentication, which effectively balances security and computational efficiency in an open network environment. Frimpong et al. [18] proposed a group authentication key agreement protocol that employs multi-layer public key operations to enhance session key strength. However, the increase in communication rounds leads to higher interaction overhead. Li et al. [19] proposed an asymmetric group key agreement protocol based on blockchain and attributes. This protocol implements fine-grained access control through attribute-based re-signatures, ensuring the privacy and security of user identity information. Additionally, it leverages blockchain's tamper-proof and traceable features to ensure that transaction data remains immutable and accountable. Zhang et al. [20] introduced an asymmetric group key agreement protocol that employs anonymous authentication technology to protect user privacy. The protocol evenly distributes the key computation process across nodes, reducing both computational and communication overhead. Moreover, it utilizes blockchain's traceability and blockchain log technology to implement an accountability mechanism. Naresh et al. [21] designed a blockchain-based dynamic authentication group key agreement protocol, using privacy-preserving smart contracts as group controllers. These controllers generate shared keys for each member and calculate partial group keys, which are sent to the respective members. The members then combine these partial keys with their shared keys to generate the group key, enabling data sharing. Tian et al. [22] proposed a blockchain-based group key agreement protocol that integrates blockchain technology with group key management to achieve a decentralized group key management mechanism. None of the above studies consider concurrent group updates, making them unsuitable for UAV networks with highly dynamic topologies and high-concurrency scenarios.

1.2 Paper organization

The structure of this paper is arranged as follows. Section 2 outlines the foundational concepts relevant to the proposed scheme. Section 3 details the authentication protocol in depth. Sections 4, 5 are dedicated to the security assessment and efficiency analysis of the scheme. The final section concludes the study and highlights potential avenues for future exploration.

2 Preliminaries

This section presents the relevant background of proposed scheme, with detailed explanations provided below.

2.1 System architecture

The system comprises three entities—TA, cluster controller and UAV swarm—with their relationships illustrated in Figure 1. A detailed description of these entities is given below.

Trusted Authority (TA): TA serves as the system's trust management entity, responsible for the registration and authentication of other entities. It is characterized by strong security and authority, ensuring both the legitimacy of participants and secure communications.

Cluster Controller (M_c): The cluster controller oversees the management of UAV swarms, handling group key distribution and negotiation to ensure secure and reliable intra-swarm communication, while coordinating cluster operations.

UAV Cluster: UAV swarm comprises multiple UAV capable of autonomous or semi-autonomous collaboration, information sharing, and task execution. Within the swarm, UAV employs a shared group key to ensure secure communications, preserving mission coordination and overall security.

2.2 Elliptic curve cryptography

In cryptography, elliptic curves are typically defined over the finite field $GF(p)$, where p denotes a prime. Given $a, b \in GF(p)$ and $(x, y) \in GF(p)^2$, the elliptic curve employed in this work is defined as [23–25]:

$$y^2 = x^3 + ax + b(\bmod p)$$

Elliptic curve must satisfy the discriminant condition:

$$\Delta = -16(4a^3 + 27b^2) \neq 0$$

This work primarily addresses two hard problems: the Elliptic Curve Discrete Logarithm Problem (ECDLP) and the Computational Diffie-Hellman Problem (ECDHP).

1. ECDLP: Given $\gamma \in Z_q^*, P, Q \in G_1$ with $Q = \gamma P$, determine γ when P and Q are known.
2. ECDHP: Given $P, aP, bP \in G_1$, where $a, b \in Z_q^*$ are unknown, compute $abP \in G_1$.

Both of these elliptic curve-based hard problems serve as the cornerstone for the design and security proof of group key agreement protocols [24–28].

2.3 Threat model

The threat model is based on the classic Dolev–Yao assumption: the adversary can eavesdrop on and interfere with all communications over the public channel, attempting to violate the system's authentication, confidentiality, and integrity.

Adversary $\mathcal{A}$ can fully control the public communication channel: $\mathcal{A}$ can intercept all communications between M_c and the UAV, modify or delete messages, replay old messages, and inject forged data into the network, enabling man-in-the-middle, replay, or forgery attacks—particularly by disrupting or impersonating parties during UAV join/leave group procedures.

Adversary $\mathcal{A}$ may obtain some historical session keys; given several known session keys, $\mathcal{A}$ will attempt to infer or recover the current session key via analysis or key-derivation attacks, thereby threatening forward and backward secrecy and possibly enabling impersonation of legitimate entities.

If a UAV is captured while executing a mission, $\mathcal{A}$ can employ side-channel attack techniques (e.g., power analysis, electromagnetic emissions, timing analysis) to extract secret parameters or private key material from the UAV's hardware or memory.

3 Proposed scheme

The proposed scheme primarily comprises the initialization, registration, authentication and group key negotiation phases, as well as UAV joining and leaving phases. Table 2 lists the relevant symbols and their definitions used in this section of the protocol.

3.1 Initialization

In this stage, TA must generate the essential parameters required for the later authentication and key agreement phases. The detailed steps are as follows:

1. TA selects an elliptic curve cyclic additive group G, whose generator and order are P and q, respectively.
2. TA selects a uniformly random element $s \in Z_q^*$ as its long-term secret key, calculates $P_{pub} = sP$ as its public key, and defines a hash function $H_1()$.

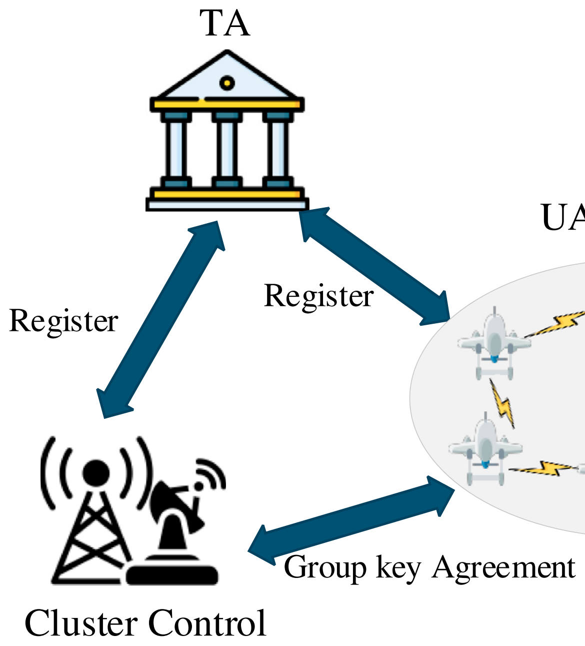

FIGURE 1
System architecture.

TABLE 2 Symbols used in the proposed scheme.

Symbol	Description
M_c	Cluster controller
UAV_i	The ith unmanned aerial vehicle (UAV)
TA	Trusted authority
$H_1()$	Secure hash functions
s	TA's long-term master secret key
P_{pub}	TA's public key
ID_c	Identity of the cluster controller
s_c	Authentication key of the cluster controller
P_c	Public key of the cluster controller
ID_i	Identity of UAV_i
PID_i	Anonymous identity of UAV_i

3.2 Registration phase

3.2.1 Cluster controller registration

1. M_c selects its identity ID_c and submits $\{ID_c\}$ to TA for registration.
2. Upon receiving the request, TA computes the authentication key $s_c = H_1(ID_c, s)$, calculates the public key $P_c = s_cP$, securely transmits $\{s_c,\ P_{pub}\}$ to M_c, and publishes P_c.
3. After receiving $\{s_c,\ P_{pub}\}$, M_c stores s_c, generates a random private key SK_c for group key agreement, computes PK_c = SK_c P as the corresponding public key, and stores the key pair. Registration of M_c is then completed.

3.2.2 UAV registration

1. UAV_i selects an identity ID_i, generates a random number r_i, computes $PID_{i1} = r_iP$, and sends $\{PID_{i1}, ID_i\}$ to TA through a secure channel.
2. TA computes $PID_{i2} = ID_i \oplus H_2\left(sPID_{i1}, P_{pub}\right)$, forming the anonymous identity $PID_i = \{PID_{i1}, PID_{i2}\}$. TA then selects a random secret a_i, computes $U_i = H_3\left(PID_i, P_{pub}\right)$, $pk_i = (U_i + a_i)P$, $sk_i = (U_i + a_i)s^{-1}$, and sends (pk_i, sk_i) PID_i to UAV_i via a secure channel.
3. Upon receiving the message, UAV_i stores $\{(pk_i, sk_i)\, PID_i\}$.

3.3 Authentication phase

During this phase, each UAV_i and the cluster controller M_c carry out mutual authentication, followed by group key negotiation. The detailed process is as follows:

1. UAV_i generates secret random numbers b_i and v_i, computes $K_i = b_iP$, $\mu_i = H_4\left(PID_i, K_i, pk_i, P_{pub}\right)$, $R_i = v_i\mu_iP_{pub}$ and $g_i = \left(sk_i + v_i\mu_i\right)$. It then transmits $\{g_i, \{R_i, \mathrm{PID}_i, K_i, T_i\}$ to M_c.
2. Upon receiving the message, M_c verifies the timestamp T_1 and proceeds with authentication verification:

Single verification: check whether $g_iP_{pub}? = pk_i + R_i$.

The correctness verification is as follows:

$$g_i P_{pub} = (sk_i + v_i \mu_i) P_{pub} = sk_i P_{pub} + v_i \mu_i P_{pub} = pk_i + R_i$$

Batch verification: After successful verification, M_c computes

$$G_c = s_c K_i$$

$$V_c = H_4 (G_c, K_i, PK_c)$$

then returns V_c to UAV_i.

3. Upon receiving the message, UAV_i calculates $G_c = b_i P_c$ and verifies the validity of V_c.

3.4 UAV group key agreement phase

M_c computes a one-to-one shared key S_{ji} with each UAV_i using Equation 1:

$$S_{ji} = SK_c K_i = \left(x_{S_{ji}}, y_{S_{ji}} \right) \tag{1}$$

Here, $S_{ji} = SK_c K_i$ denotes the scalar multiplication of the elliptic curve point S_{ji}, and the subsequent expression $S_{ji} = \left(x_{S_{ji}}, y_{S_{ji}} \right)$ refers only to the coordinate representation of this point.

Next, M_c derives a group key share UK_i for each UAV_i according to Equation 2:

$$UK_i = \left(\prod_{t=1, t \neq i}^{n} x_{S_{jt}} \right) P \tag{2}$$

Here, $\prod_{t=1,t\neq i}^{n} x_{jt}$ denotes the ordinary scalar multiplication over the values $x_{S_{ji}}$, and it is not related to elliptic curve point operations.

M_c ensures message integrity by computing $\delta_i = h\left(UK_i \parallel S_{ji} \right)$ and transmits (UK_i, δ_i) to UAV_i.

Upon receiving (UK_i, δ_i), UAV_i calculates the pairwise key $S_{ji} = b_i PK_c = \left(x_{K_{ji}}, y_{K_{ji}} \right)$ with M_c and checks whether $\delta_i = h\left(UK_i \parallel S_{ji} \right)$ holds. If valid, UAV_i computes the final group key G using Equation 3:

$$G = x_{S_{ji}} \cdot UK_i \tag{3}$$

As M_c possesses all pairwise shared keys, it derives the final group key using Equation 4:

$$G = \left(\prod_{t=1}^{n} x_{S_{jt}} \right) P \tag{4}$$

By substituting (Equation 2) into (Equation 3), we can verify that both sides compute the same group key.

Thus, all UAV_i in the group, together with M_c, successfully establish a common group key G.

3.5 UAV joining phase

When a UAV_n intends to join the group, it must first undergo the authentication procedure to verify mutual legitimacy with M_c and acquire the corresponding valid public key. UAV_n then submits a join request to M_c, which initiates group key updating as follows:

1. UAV_n derives the pairwise key $S_{jn} = b_n PK_c = \left(x_{S_{jn}}, y_{S_{jn}} \right)$ and submits a join request to M_c.
2. M_c computes the pairwise key with UAV_n as $S_{jn} = SK_c K_n = \left(x_{S_{jn}}, y_{S_{jn}} \right)$. It selects a random N_1, calculates the group key share for UAV_n as $US_n = N_1 x_G P$, where x_G denotes the x-coordinate of the elliptic curve point G, and then transmits (US_n, δ_n) to UAV_n.
3. Upon receiving the message, UAV_n verifies US_n using the pairwise key P_{jn} and δ_n. If valid, it computes the new group key according to Equation 5:

$$NG = x_{S_{jn}} US_n \tag{5}$$

4. For the existing UAV_i, M_c computes a new share $US_0 = N_1 x_{K_{jn}} P$. It selects a random N_{sig}, computes $K_s = N_s P$, derives $r_s = N_s^{-1} \left(h(US_0) + x_{K_s} SK_c \right)$, and constructs $\delta_0 = \left(x_{K_s}, r_s \right)$, M_c then broadcasts $\left(US_0, \delta_0 \right)$ to all legitimate UAV in the group.
5. Each UAV_i verifies the signature: $P_\mathrm{s} = h(US_0) r_\mathrm{s}^{-1} P + x_{K_\mathrm{s}} r_\mathrm{s}^{-1} PK_c$ and checks whether $x_{P_\mathrm{sig}} = x_{PK_\mathrm{sig}}$. If the equality holds, the message is valid, and UAV_i computes the new group key according to Equation 6:

$$NG = x_G US_0 \tag{6}$$

6. Since M_c possesses all pairwise shared keys, it directly computes the new group key according to Equation 7:

$$NG = N_1 \left(\prod_{t=1}^{n} x_{S_{jt}} \right) P \tag{7}$$

At this stage, all UAV and M_c within the group successfully derive the same new shared key NG.

3.6 UAV leaving phase

When a UAV_l intends to leave the group, it must send a departure request to M_c. M_c then facilitates group key updating to ensure that the departing UAV_l cannot compute the new group key.

1. After receiving UAV_l's departure request, M_c chooses a random number N_2 and computes for each remaining UAV_i a secret value: $L_i = E_{K_{ij}} \left(N_2 x_{K_{ji}}^{-1} \right)$ along with its hash $\delta_i = h\left(L_i \parallel K_{ij} \right)$, where $E_{K_{ij}}$ represents symmetric encryption using the shared key K_{ij} between M_c and UAV_i. M_c then transmits (L_i, δ_i) to the corresponding UAV_i.
2. Upon receipt, UAV_i verifies the integrity of L_i using K_{ij}. If valid, UAV_i decrypts L_i with the shared key K_{ji} to derive the updated group session key according to Equation 8:

$$NG = DE_{K_{ij}}(L_i)x_{KG}P \tag{8}$$

3. Meanwhile, M_c computes the new group key directly according to Equation 9:

$$NG = N_2 x_{K_{ji}}^{-1} x_{KG} P \tag{9}$$

At this point, the group key update for UAV departure is complete, and all legitimate entities have derived the new group key NG.

4 Security analysis

In this section, we conduct a security analysis of the proposed scheme under the Random Oracle Model (ROM) [24–33]. Furthermore, additional security properties are examined through semantic evaluation.

4.1 Formal security proof using ROM

4.1.1 Security model and proof

This section builds the security model of the proposed scheme under the random oracle framework. The model involves two entities, UAV and M_c, with additional queries for UAV joining and leaving the group.

Participants: The scheme includes entities UAV and M_c, denoted as U_i and M_j. Their instances are denoted $\Pi_{U_i}^{u}$ and $\Pi_{M_j}^{v}$.

Acceptance State: An instance Π_{Λ}^{t} is said to accept if the received message matches the expected one. Its session identifier is the ordered concatenation of all exchanged messages.

Partnership: Two instances $\Pi_{U_i}^{u}$ and $\Pi_{M_j}^{v}$ are partners if they both accept and share the same session identifier.

Attacker: Here, the capabilities of adversary $\mathcal{A}$ in the threat model are formalized, and the query abilities of adversary $\mathcal{A}$ are as follows:

- *Execute* ($\Pi_{U_i}^{u}$, $\Pi_{M_j}^{v}$): This query simulates the passive attack of adversary $\mathcal{A}$, representing the adversary's ability to eavesdrop on the communication channel.
- *Send* (Π_{Λ}^{t}, *m*): This query simulates the active attack of adversary $\mathcal{A}$, representing the adversary's ability to tamper with, replay, or modify messages.
- *Join* (Π_{Λ}^{t}): This query simulates the scenario where a legitimate UAV joins the group. Through this query, adversary A can obtain a legitimate UAV, Π_{Λ}^{t} and receive information from M_c used to update the group key after joining the group.
- *Leave* (Π_{Λ}^{t}): This query simulates the scenario where a legitimate UAV leaves the group. Through this query, adversary $\mathcal{A}$ can obtain information from M_c used to update the group key after the UAV leaves the group.
- *Reveal* (Π_{Λ}^{t}): This query simulates a known session key attack, where adversary $\mathcal{A}$ can gain access to certain session keys.
- *Corrupt* (Π_{Λ}^{t}): This query simulates the specific capabilities of an attacker in an efficient dynamic UAV group authentication and key agreement scheme. Through this query, adversary $\mathcal{A}$ can obtain secret registration information.
- *Test* (Π_{Λ}^{t}): The purpose of this query is to test adversary $\mathcal{A}$'s understanding of the session key negotiated by Π_{Λ}^{t}. After executing several of the above queries, adversary $\mathcal{A}$ will select a UAV instance to perform the Test query, which works as follows: If the instance has not negotiated a session key, the query returns ⊥. If the instance has negotiated a session key, a coin is flipped. If the coin lands heads, let b = 1, and return the actual session key. If the coin lands tails, let b = 0, and return a random value. The task of adversary A is to distinguish whether the value returned by Test (Π_{Λ}^{t}) is a random number or the session key of $\Pi_{\Lambda}^{\mathrm{t}}$.

Freshness: An instance is fresh if neither it nor its partner has been subject to a Reveal query.

Semantic Security: The adversary's goal is to correctly guess the bit b in the Test query. Define

$Adv_{\mathcal{P}}(\mathcal{A}) = \mid 2\ \mathrm{Pr}\ [\mathrm{succ}{-}1 \mid$. If this advantage is negligible, the scheme achieves semantic security.

Theorem 1: For scheme $\mathcal{P}$ and adversary $\mathcal{A}$ within polynomial time t, the advantage satisfies:

$$\mathrm{Adv}_{\mathcal{P}}(\mathcal{A}) \le \frac{q_h^2}{2^l} + \frac{(q_s+q_e)^2}{p} + \frac{2q_{\mathrm{L}}}{n} + 2q_{\mathrm{j}} Adv^{\mathrm{ECDHP}}(\mathcal{A})$$

In the above, q_s, q_e, q_J, q_L, and q_h represent the Send queries, Execute queries, Join queries, Leave queries, and Hash queries, respectively, conducted by adversary A. l denotes the output length of the Hash queries, and $1/n$ is the upper limit on the single collision probability for Send and Execute queries. $Adv^{ECDHP}(\mathcal{A})$ represents the advantage of a polynomial adversary in solving the ECDHP problem.

Proof:

This chapter defines a series of games to prove Theorem 1.

Game G_0: This game simulates the adversary's real attack in the random oracle model. By definition, the formula is given by:

$$Adv_P(\mathcal{A}) = 2\ \mathrm{Pr}\left[succ_0\right] - 1$$

Game G_1: In this game, the adversary simulates an eavesdropping attack by querying the Execute query to obtain communication information. The advantage of adversary A in guessing the correct outcome of the Test query via Execute queries is 0.

$$\mathrm{Pr}\left[succ_1\right] - \mathrm{Pr}\left[succ_0\right] = 0$$

Game G_2: In this game, adversary A is allowed to make Send, Execute, Join, and Leave queries to obtain communication information between entities, which may lead to collisions between protocol instances. The adversary can also obtain collisions in the Hash function through Hash queries. By applying the birthday paradox, we get:

$$\mathrm{Pr}\left[succ_2\right] - \mathrm{Pr}\left[succ_1\right] = \frac{q_h^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2p}$$

Game G_3: In this game, adversary A can obtain the group key share sent by M_c to calculate the group shared key by making Join, Leave, and Send queries. Through the Join query, adversary A can obtain the group key share sent by M_c. The probability that adversary A breaks the protocol through the Join query is $q_{join} \cdot Adv^{ECDDHP}(\beta)$. Through the Leave query, adversary A can obtain the encrypted information $KL_i = E_{K_{ij}}\left(N_2 \cdot K_{ji}^{-1}\right)$ sent by the GCS to the UAV when a UAV leaves the group. Since adversary A cannot access the key K_{ij}, it can only guess $N_2 \cdot K_{ji}^{-1}$,and the probability of this happening is q_L/n. Thus, the advantage of adversary A in attacking the protocol via these two methods is:

$$\Pr\left[succ_3\right] - \Pr\left[succ_2\right] = q_{join} \cdot Adv^{ECDHP}(\mathcal{A}) + \frac{q_L}{n}$$

Game G_4: In this game, all requests have been simulated, and the adversary can only win the game by directly guessing the bit b. Therefore, the adversary's success probability is 1/2, as shown:

$$\Pr\left[succ_4\right] = \frac{1}{2}$$

Combining with these quations, Theorem 1 can be derived. Therefore, the scheme is secure in the random oracle model.

4.2 Semantic analysis

- Mutual Authentication: The proposed scheme enables mutual authentication between UAV_i and M_c. UAV_i generates a signature using its TA-issued key pair (pk_i, sk_i), which M_c validates to confirm UAV_i's authenticity. Conversely, UAV_i authenticates M_c through V_c, demonstrating M_c's possession of a legitimate private key.
- Anonymity: During communications, UAV_i employs a TA-generated anonymous identity PID$_i$ instead of its real identity in authentication and group key agreement, thereby ensuring anonymity.
- Man-in-the-Middle Attack Resistance: Adversaries cannot impersonate UAV_i or M_c, as they cannot derive a valid PID_i or authentication keys (pk_i, sk_i). PID_i is constructed using $PID_{i1} = r_i P$ and PID$_{i2}$ = PID$_i \oplus H_2\left(sPID_{i1}, P_{pub}\right)$, with s as TA's secret and r_i as random, preventing adversaries from obtaining them. Similarly, M_c's private key $s_c = H_1\left(ID_c, s\right)$ remains unknown to adversaries. Thus, the scheme resists man-in-the-middle attacks.
- Replay Attack Resistance: The scheme uses timestamps to counter replay attacks. Upon receiving a message, both M_c and UAV validate its freshness, terminating the protocol if the timestamp deviates beyond a threshold. Timestamp integrity is guaranteed since forging requires secret keys not exposed over public channels.
- Key Compromise Attack Resistance: Even if M_c's long-term key is compromised, prior session keys remain secure. While M_c's authentication key is derived from the long-term secret, the group key negotiation private key cannot be derived from it. UAV' private keys for negotiation are randomly generated, further ensuring that past keys remain protected. Thus, the scheme achieves perfect forward secrecy.
- Session-Specific Random Number Leakage Attack Resistance: If random numbers generated during authentication or key agreement are leaked, adversaries still cannot authenticate since they lack access to M_c's private key $s_c = H_1\left(ID_c, s\right)$ and UAV' key pairs (pk_i, sk_i).
- Forward Secrecy: When a UAV departs, M_c selects a random N_2 and computes $KL_i = E_{K_{ij}}\left(N_2 x_{K_{jl}}^{-1}\right)$ for the remaining UAV. The departing UAV cannot obtain N_2, thus cannot compute the new group key, ensuring forward secrecy.
- UAV Impersonation Attack Resistance: Adversaries cannot impersonate UAV_i or M_c as they lack valid long-term keys and cannot forge signatures to pass verification ($g_i P_{pub} ? = pk_i + R_i$).
- Backward Secrecy: If a new member M_j joins, recovering prior group keys requires solving the ECDLP, which is computationally infeasible. Therefore, the scheme ensures backward secrecy.

TABLE 3 Encryption operation time.

Symbol	Description	Time (ms)
T_{em}	Elliptic curve scalar multiplication	0.7538
T_{ea}	Elliptic curve scalar addition	0.0040
T_h	Hash function	0.0002
T_{dm}	Scalar multiplication	2.6439
T_{da}	Scalar addition	0.0146
T_d	Bilinear pairing	6.4164

5 Performance analysis

5.1 Computation cost

In this section, we compare the computational and communication costs of the proposed protocol with those of other related schemes. According to [34], under a Windows seven operating system with a 2.4 GHz processor and 4 GB of memory, the MIRACL library is used to implement the two aforementioned cryptographic operation schemes, and the execution times of various cryptographic operations are recorded in Table 3.

Table 4 presents a detailed comparison of the computational costs across different protocols. The Figure 2 clearly depicts how computational overhead scales with the group size, highlighting the performance differences among protocols. As indicated, the proposed scheme achieves comparatively low computational costs on both devices while maintaining structural simplicity.

On the UAV side, the computational cost is $2(n+1)T_{em}+$ nT_{ea} +$2T_h$. Unlike other schemes that typically require numerous scalar multiplications, additions, and bilinear pairings, the proposed protocol cuts the computation by approximately 60%–70%. For instance, when n = 50, the proposed scheme incurs about 81 ms, compared to 190 ms in the lowest-cost scheme [34], achieving only 42.6% of its cost. By comparison, the more costly scheme [37]

TABLE 4 Computation cost comparison.

Scheme	UAV_l	M_c
[34]	$5nT_{em}+(7n-5)T_{ea}+4nT_h$	$4T_{em}$
[35]	$(2n+1)T_{dm}+(2n-2)T_{da}+3T_d+$ $(n+4)2T_h$	$3T_d+T_{dm}+2T_H$
[36]	$(11T_{em}+4T_{ea}+9T_H)n$	$6T_{em}+2T_{ea}+3T_H$
[37]	$(n+1)T_d+nT_{dm}+3nT_H$	$5T_{dm}+3T_H$
Our	$2(n+1)T_{em}+\mathrm{n}T_{ea}+2T_h$	$5T_{em}+$

TABLE 5 Comparison on communication cost.

Scheme	Communication cost (Bytes)
[34]	104
[35]	388
[36]	352
[37]	190
Our	104

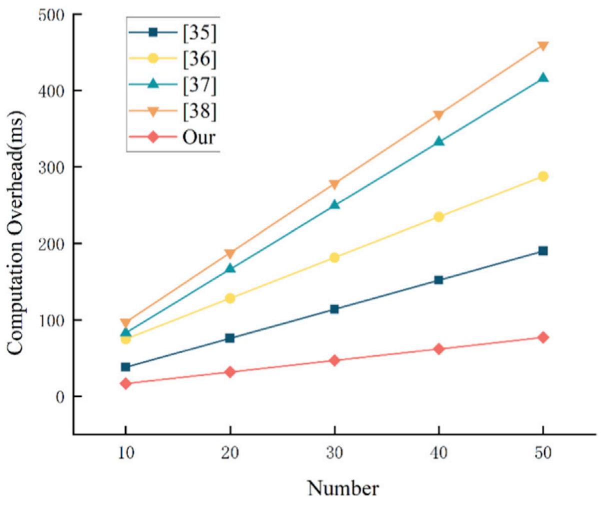

FIGURE 2
The comparisons of computation cost.

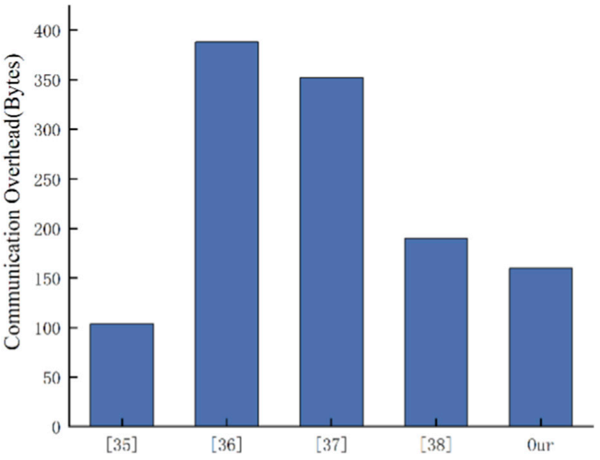

FIGURE 3
The comparisons of Communication cost.

consumes nearly 454 ms, approximately 5.6 times higher than the proposed protocol.

On the cluster controller side, the computational cost is 5Tem, notably less than that of other protocols. For example, scheme [35] performs several bilinear pairings and scalar multiplications, incurring 21.89 ms, whereas the proposed protocol only needs 3.77 ms, about 17.2% of the cost. This significantly alleviates computational overhead.

The Figure 2 demonstrates a linear growth trend in computational cost as n increases. The proposed scheme's curve remains significantly lower than others, with a gentler slope, reflecting strong scalability. As n grows from 10 to 50, the proposed protocol's cost increases by about 64.4 ms, compared with 350–450 ms for other protocols. This highlights the advantage of the proposed protocol under large-scale parameters.

The findings confirm that the proposed scheme excels over existing protocols both in computational complexity and real-world execution efficiency. By minimizing expensive bilinear pairings and elliptic curve scalar operations, the scheme cuts resource usage by about 60%–80%. This is crucial for resource-limited devices like UAV, improving response speed while markedly reducing energy consumption, thereby strengthening system stability and security.

5.2 Communication cost

In the authentication phase, the total amount of messages transmitted between different entities is regarded as the communication cost. Table 5 presents the communication overhead of all the compared schemes. For communication cost estimation, the following assumptions are made: a timestamp of 4 bytes, a random number of 40 bytes, an identity size of 32 bytes, a hash output of 20 bytes, and an ECC point of 64 bytes. Table 5 and Figure 3 clearly demonstrate that the proposed scheme achieves a remarkable reduction in communication overhead relative to other existing protocols. Table 5 provides the total communication costs of five protocols, expressed in bytes for comparison. Specifically, the communication cost of the proposed scheme is 160 bytes, compared to 104 bytes for scheme [34], 388 bytes for scheme [35], 352 bytes for scheme [36], and 190 bytes for scheme [37]. This indicates that the proposed scheme substantially reduces communication costs while ensuring security and functionality.

Figure 3 further highlights the communication overhead differences among these protocols. The proposed protocol shows a dramatic reduction—over 60%—compared with schemes [35, 36]. Although scheme [34] incurs relatively low overhead, it is still about 60 bytes higher than the proposed scheme, likely due to its restricted features or simplified design. Notably, schemes [35, 36] consume 388 and 352 bytes respectively, suggesting the inclusion of additional cryptographic operations or protocol complexity that drive up communication costs. From a security perspective, the proposed scheme maintains robust protection while employing efficient communication mechanisms that minimize redundant transmissions, thereby reducing overhead. This renders the scheme particularly well-suited to resource-constrained environments like UAV group communication and IoT networks, which impose stringent requirements on computation and bandwidth.

In conclusion, the proposed protocol clearly demonstrates superior communication efficiency, drastically reducing overhead while preserving strong security and scalability. Practically, in high-latency and bandwidth-expensive environments, the low communication overhead of the proposed scheme will substantially improve system performance and operability. Therefore, the proposed scheme provides clear advantages in real-world applications, fulfilling the need for efficient and secure communication.

6 Conclusion

As UAV cluster communication technology advances, coordinated operations among multiple UAV have become a practical reality. Nevertheless, UAV cluster communication in open environments encounters significant security challenges, especially under dynamic topologies and resource-constrained conditions. To overcome these challenges, we propose an efficient group key agreement scheme designed to improve both the security and efficiency of UAV cluster communication. The proposed protocol leverages elliptic curve-based signatures for device authentication and message verification, while offloading intensive computations to the ground control station through group key agreement, thus alleviating the computational burden on UAV. In addition, the scheme enables secure authentication and key updates for UAV during dynamic join and leave operations, thereby maintaining secure and adaptive group communications. Formal security proofs and performance evaluations show that the proposed scheme provides notable improvements in resilience against attacks, computational efficiency, and communication cost. Overall, it delivers a more secure and efficient solution for UAV cluster communication.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

ZW: Project administration, Formal Analysis, Validation, Resources, Writing – original draft, Investigation, Visualization, Conceptualization. JL: Data curation, Methodology, Writing – review and editing, Software, Supervision. SY: Data curation, Writing – review and editing, Software, Supervision, Methodology. YZ: Supervision, Software, Methodology, Writing – review and editing, Data curation.

Funding

The author(s) declared that financial support was not received for this work and/or its publication.

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Wan F, Yaseen MB, Riaz MB, Shafiq A, Thakur A, Rahman MO. Advancements and challenges in UAV-Based communication networks: a comprehensive scholarly analysis. *Results Eng* (2024) 24:103271. doi:10.1016/j.rineng.2024.103271

2. Chen J, Li T, Zhang Y, You T, Lu Y, Tiwari P, et al. Global-and-Local attention-based reinforcement learning for cooperative behaviour control of multiple UAVs. *IEEE Trans Vehicular Technology* (2024) 73(3):4194–206. doi:10.1109/TVT.2023.3327

3. Xiao N, Wang Z, Sun X, Miao J. A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial internet of things. *Alexandria Eng J* (2024) 86:631–43. doi:10.1016/j.aej.2023.12.021

4. Miao J, Ning X, Hong S, Wang L, Liu B. Secure and efficient authentication protocol for supply chain systems in artificial intelligence-based internet of things. *IEEE Internet Things J* (2025) 12(19):39532–42. doi:10.1109/jiot.2025.3592401

5. Dong R, Wang B, Cao K, Tian J, Cheng T. Secure transmission design of RIS enabled UAV communication networks exploiting deep reinforcement learning. *IEEE Trans Vehicular Technology* (2024) 73(6):8404–19. doi:10.1109/tvt.2024.3357821

6. Sharma P, Purushothama BR. BP-MGKM: an efficient multi-group key management scheme based on bivariate polynomial. *Computer Networks* (2022) 216:109244. doi:10.1016/j.comnet.2022.109244

7. Hsu C, Harn L, Xia Z, Cui J, Chen J. Construction of lightweight authenticated joint arithmetic computation for 5G IoT networks. *The Computer J* (2023) 66(1):208–20. doi:10.1093/comjnl/bxab155

8. Tian Y, Yuan J, Song H. Efficient privacy-preserving authentication framework for edge-assisted internet of drones. *J Inf Security Appl* (2019) 48:102354. doi:10.1016/j.jisa.2019.06.010

9. Zhang Y, He D, Li L, Chen B. A lightweight authentication and key agreement scheme for internet of drones. *Computer Commun* (2020) 154:455–64. doi:10.1016/j.comcom.2020.02.067

10. Semal B, Markantonakis K, Akram RN. A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks. In: 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC). IEEE (2018). p. 1–8.

11. Luo M, Wu J, Li X. Cross-domain certificateless authenticated group key agreement protocol for 5G network slicings. *Telecommunication Syst* (2020) 74(4):437–49. doi:10.1007/s11235-020-00673-x

12. Pan X, Jin Y, Li F. Anefficient heterogeneous authenticated key agreement scheme for unmanned aerial vehicles. *J Syst Architecture* (2023) 136:102821. doi:10.1016/j.sysarc.2022.102821

13. Braeken A. Pairing free certified common asymmetric group key agreement protocol for data sharing among users with different access rights. *Wireless Personal Commun* (2021) 121(1):307–18. doi:10.1007/s11277-021-08636-4

14. Kermanshahi SK, Salleh M. An enhanced certificateless cryptosystem for Mobile ad hoc networ ks. In: *2014 international symposium on biometrics and security technologies (ISBAST)*. NJ: IEE E (2014). p. 176–81.

15. Eissa T, Razak SA, Ngadi MA. A novel lightweight authentication scheme for mobile ad hoc networks. *Arabian J Sci Eng* (2012) 37:2179–92. doi:10.1007/s13369-012-0318-y

16. Kumar A, Tripathi S. A pairing free anonymous certificateless group key agreement protocol for dynamic group. *Wireless Personal Commun* (2015) 82:1027–45. doi:10.1007/s11277-014-2264-3

17. Ayad A, Hammal Y. An Efficient authenticated group key agreement protocol for dynamic U AV fleets in untrusted environments. In: 2021 International Conference on Networking and Adva nced Systems (ICNAS). IEEE (2021). p. 1–8.

18. Frimpong E, Rabbaninejad R, Michalas A. Arrows in a quiver: a secure certificateless group ke y distribution protocol for drones. Secure IT systems. In: 26th Nordic Conference, NordSec 2021, Virtual Event, November 29–30, 2021, Proceedings 26. Springer International Publishing (2021). p. 31–48.

19. Li J, Qiao Z, Peng J. Asymmetric group key agreement protocol based on blockchain and attribute for industrial internet of things. *IEEE Trans Ind Inform* (2022) 18(11):8326–35. doi:10.1109/tii.2022.3176048

20. Zhang Q, Li Y, Wang R, Li J, Gan Y, Zhang Y, et al. Blockchain-based asymmetric group key agreement protocol for internet of vehicles. *Comput & Electr Eng* (2020) 86:106713. doi:10.1016/j.compeleceng.2020.106713

21. Naresh VS, Allavarpu VD, Reddi S. Provably secure blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN. *The J Supercomputing* (2022) 78(6):8708–32. doi:10.1007/s11227-021-04175-8

22. Tian Y, Wang Z, Xiong J, Ma J. A blockchain-based secure key management scheme with trustworthiness in DWSNs. *IEEE Trans Ind Inform* (2020) 16(9):6193–202. doi:10.1109/tii.2020.2965975

23. Miao J, Wang Z, Ning X, Shankar A, Maple C, Rodrigues JJ. A UAV-assisted authentication protocol for internet of vehicles. *IEEE Trans Intell Transportation Syst* (2024) 25(8):10286–97. doi:10.1109/tits.2024.3360251

24. Huang W. ECC-Based three-factor authentication and key agreement scheme for wireless sensor networks. *Scientific Rep* (2024) 14(1):1787. doi:10.1038/s41598-024-52134-z

25. Zou S, Cao Q, Wang C, Huang Z, Xu G. A robust two-factor user authentication scheme-based ECC for smart home in IoT. *IEEE Syst J* (2021) 16(3):4938–49. doi:10.1109/jsyst.2021.3127438

26. Hasan MK, Weichen Z, Safie N, Ahmed FRA, Ghazal TM. A survey on key agreement and authentication protocol for internet of things application. *IEEE Access* (2024) 12:61642–66. doi:10.1109/access.2024.3393567

27. Kumari D, Singh K. Lightweight secure authentication and key agreement technique for smart grid. *Peer-to-Peer Networking Appl* (2024) 17(1):451–78. doi:10.1007/s12083-023-01585-8

28. Chaudhary D, Dadsena PK, Padmavathi A, Mehedi Hassan M, Fahad Alkhamees B, Kumar U. Anonymous quantum safe construction of three party authentication and key agreement protocol for mobile devices. *IEEE Access* (2024) 12:74572–85. doi:10.1109/access.2024.3404232

29. Liu L, Jia Y. Analysis of one lightweight authentication and matrix-based key agreement scheme for healthcare in fog computing. *Int J Netw Secur* (2024) 26(1):138–41. doi:10.6633/IJNS.202401

30. Li Z, Ju Z, Zhao H. A lightweight certificateless authenticated key agreement scheme based on chebyshev polynomials for the internet of drones. *Sensors* (2025). doi:10.3390/s25144286

31. Ayad A, Hammal Y. An efficient authenticated group key agreement protocol for dynamic UAV fleets in untrusted environments. In: 2021 International Conference on Networking and Advanced Systems (ICNAS). IEEE (2021). p. 1–8.

32. Zhang L, Xu J, Obaidat MS, Li X, Vijayakumar P. A PUF-based lightweight authentication and key agreement protocol for smart UAV networks. *IET Commun* (2022) 16(10):1142–59. doi:10.1049/cmu2.12295

33. Khan MA, Ullah I, Kumar N, Oubbati OS, Qureshi IM, Noor F, et al. An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks. *IEEE Trans Vehicular Technology* (2021) 70(5):4839–51. doi:10.1109/tvt.2021.3055895

34. Li X, Liu P, Zhang S, Xie Y. An improved secure and efficient group key agreement scheme in VANETs. *Int J Commun Syst* (2022) 35(3):e5025. doi:10.1002/dac.5025

35. Liu L, Wang Y, Zhang J, Yang Q. A secure and efficient group key agreement scheme for VANETs. *Sensors* (2019) 19(3):482–96. doi:10.3390/s19030482

36. Zhou Y, Long X, Chen L, Yang Z. Conditional privacy-preserving authentication and key agreement scheme for roaming services inVANETs. *J Inf Secur Appl* (2019) 47:295–301. doi:10.1016/j.jisa.2019.05.018

37. Zhang L, Wu Q, Domingo-Ferrer J, Qin B, Hu C. Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Transintell Transp Syst* (2017) 18(3):516–26. doi:10.1109/tits.2016.2579162