2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)

# An Efficient Certificateless Signcryption Scheme for Secure Communication in UAV Cluster Network

Lemei Da[1], Yujue Wang[2], Yong Ding[1,3], Wanjun Xiong[4], Huiyong Wang[5], Hai Liang[1,*]
1. Guangxi Key Laboratory of Cryptography and Information Security, School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China
2. Hangzhou Innovation Institute, Beihang University, Hangzhou, China
3. Cyberspace Security Research Center, Pengcheng Laboratory, Shenzhen, China
4. School of Computer Science and Engineering, Sun Yet-sen University, Guangzhou, China
5. School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, China
E-mail: lianghai@guet.edu.cn

***Abstract*—The Unmanned Aerial Vehicles (UAV) have been widely used in civilian and military fields. Due to the limited computing power and storage capacity, a single UAV is not suitable for long-distance, large-scale data transmission. Many authentication schemes have been proposed without considering the confidentiality of transmitted data. In order to address the security and privacy issues in UAV-assisted data collection scenario, a Certificateless Aggregate Signcryption (CL-ASC) scheme is proposed in this paper, where data privacy and authenticity of data source can be guaranteed. The Aggregate Unmanned Aerial Vehicle (AGV) in each UAV cluster is able to batch verify the signcryption ciphertexts from UAVs in its administrative domain, before adding its signcryption ciphertext to the aggregate one and forwarding to the Control Station (CS) for further batch verification and decryption. The security analysis shows that the CL-ASC construction can effectively resist attacks from external adversaries and malicious CS, and offers existential unforgeability on the (aggregate) signcryption ciphertext under the ECDLP assumption. The performance analysis demonstrates that the proposed CL-ASC construction enjoys high computational efficiency and is practical in resource-constrained UAV cluster network scenarios.**

***Index Terms*—Unmanned aerial vehicle, signcryption, certificateless signature, batch verification, source authentication, data privacy.**

## I. Introduction

UAVs are usually equipped with GPS, cameras, infrared sensors, etc. [1], which have many advantages such as small size, easy deployment and high flexibility, and have been widely used in military and civilian fields including disaster rescues, security patrols, regional monitoring, cargo transportation and natural disaster monitoring. Single UAV cannot perform long-distance tasks and large-scale data transmission, thus, multiple UAVs can be organized into cluster network to perform complex tasks through mutual cooperation [2].

The communications of UAV-to-UAV and UAV-to-CS are carried out through wireless channels [3], which are vulnerable to various security threats in such open environment, such as eavesdropping, SQL injection, and denial of service attacks [4]. The user data may be intercepted, tampered with or forged by attackers during data collection and transmission. Particularly, UAVs used in the civilian/military field usually carry user private information, military instructions or secrets, respectively. The attacks to UAV communication may cause secret information leakage or property damage. Therefore, it is important to ensure the security and privacy of data transmission in UAV cluster networks. Most existing solutions for UAV cluster network separately consider the identity authentication and data protection mechanisms, which means the data should be transmitted only after successful identity authentication.

However, in a large-scale UAV network, separate authentication on each UAV would take too many interactions and bring low communication efficiency. After successful authentication, a large amount of data transmission also imposes high requirements on the computational cost [5], [6]. Existing cryptographic technology has high computational complexity and communication costs, they are difficult to be applied in resource-constrained UAV network [7], [8]. Moreover, they do not allow AGV to aggregate the data from UAVs in its domain for batch verification and forwarding to CS.

### A. Our Contributions

To address the security, privacy and efficiency issues in data collection with UAV cluster network, this paper proposes a Certificateless Aggregate Signcryption scheme (CL-ASC), which simultaneously offers the functionalities of the digital signature and encryption technologies. In CL-ASC, Reconnaissance Unmanned Aerial Vehicles (RAVs) are able to collect data with their equipped devices, which are signcrypted and forwarded to AGV in the same cluster. These signcrypted data can be aggregated by AGV before performing batch verification, in this way the verification efficiency can be greatly improved. After successful verification, the signcryption ciphertext of AGV is further added to the aggregated one, which is then sent to CS for validation and decryption.

The security analysis shows that our CL-ASC construction can effectively protect the confidentiality and integrity of UAV data and the authenticity of data source. Also, it can resist replay attacks and dishonest CS in deducing the data from RAVs. The efficiency analysis indicates that our CL-ASC

978-0-7381-2646-3/21/$31.00 ©2021 IEEE
DOI 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00125

construction has low computational costs and is suitable for UAV cluster network with limited resources.

## II. Related Works

The unmanned aerial vehicle technology has developed rapidly in recent years [9]. Noguchi and Komiya [10] used unmanned aerial vehicles to provide remote realtime monitoring of disaster areas, facilitating access to information and management of rescue operations. Qu et al. [11] studied how to minimize deployment delays of UAVs in emergency situations to improve rescue efficiency. In [12], Liang et al. employed UAVs to collect hyperspectral images and classify forest species. Huang et al. [13] designed an outdoor independent charging system for electric patrol unmanned aerial vehicles, where UAVs can be used to avoid manual tower climbing to reduce the occurrence of accidents.

With the increasing application of UAVs, the security has got too many attentions from academic. Gao et al. [14] proposed an electromagnetic interference security situational awareness method based on semantic analysis, which is used to detect abnormal behaviors of UAVs to improve their active defense capabilities. Omri and Hasna [15] studied the physical layer security of UAV network, and attested that the physical layer security of wireless network channel is mainly affected by the altitude of the network flight platform, the density of eavesdroppers and the type of environment. Kim and Kang [16] designed a UAV security module based on secure element, which is connected with the flight control computer or mission computer through USB interface, for sending the encrypted control signal and telemetry data of UAVs to the control station. Liu et al. [17] designed a secure homomorphic encryption framework to protect private data on clients, and provided trust and transparency to third-party UAVs. The proposals [18]–[20] applied blockchain to peer-to-peer UAV network as a solution to improve the security of UAV communication.

With only limited computing resources, UAVs are unable to analyze and process large-scale data. Li et al. [21] proposed a lightweight authentication method based on Elliptic Curve Cryptography (ECC), which uses lightweight ECC digital certificates for bi-directional authentication. Alladi et al. [22] proposed a lightweight authentication scheme based on Physically Unclonable Functions, which supports UAV-GS and UAV-UAV communication modes to resist physical capture and node tamper attacks. In [23], Wang et al. proposed an identity-based data aggregation authentication scheme to solve the problem of low efficiency of data-by-data authentication in UAV cluster network. Li et al. [24] improved the scheme of [23] by adding an authentication mechanism for aggregated unmanned aerial vehicle and verifying the authenticity of a single UAV response.

## III. System Model And Security Requirements

### A. System Model

As shown in Fig. 1, the data collection system in UAV cluster network is composed of three types of entities, namely, Reconnaissance Unmanned Aerial Vehicles (RAVs), Aggregate Unmanned Aerial Vehicle (AGV) and Control Station (CS). In each cluster, there is an AGV and many RAVs. RAVs have limited computing power and short-distance communication capabilities, while AGV has moderate computing power and communication capability. Control station is a data storage and processing center with powerful computing and communication capabilities, which executes initialization algorithms to generate public parameters and participates in the key generation process for all entities in UAV cluster network.

For ease of presentation, it is assumed that there are $n$ UAVs in each cluster, including one AGV and $n-1$ RAVs. Let $ID_n$ be an AGV and $ID_1, \cdots, ID_{n-1}$ be RAVs within the jurisdiction of $ID_n$. Each RAV signcrypts the collected data and sends it to its administrative AGV in the region. All signcrypted data of RAVs in the same domain are aggregated and validated by AGV. Successfully validated signcryption ciphertexts is then aggregated with the signcrypted data of AGV, which is sent to CS for processing, in this way CS is able to decrypt the collected data and verify their source.

### B. System Requirements

The data collection system in UAV cluster network must satisfy the following security requirements.

- *Data confidentiality*: During data collection, only CS is allowed to obtain the original data from RAVs and AGV. Even if an external entity intercepts the data being transmitted, it would be impossible to deduce the real content of the data collected by RAVs.
- *Data integrity*: The collected data by RAVs and AGV cannot be tampered with and forged by any entity during transmission without being detected by CS. That is, an external adversary cannot impersonate RAV or AGV in the system to participate in the process of data collection.
- *Source authenticity* [25]: The real source of collected data can be validated by both AGV and CS.
- *Resistance of replay attacks*: Any information intercepted by an adversary cannot be re-sent to AGV or CS without being detected.
- *Resistance malicious CS*: CS only provides partial private keys for all entities, otherwise CS would be able to impersonate honest RAV and AGV to process collected data. Also, all RAVs and AGV have the ability to verify the authenticity of partial private keys distributed by CS.
- *Lightweight*: RAVs have only limited storage capacity and computing resource, which cannot support resource-intensive computations.

### C. System Framework

A CL-ASC system for data collection in UAV cluster network consists of the following five efficient procedures.

- **Setup**: This procedure is performed by CS for initializing the system, which takes a security parameter $k$ and outputs the system parameter $params$ and the master private key $s$.

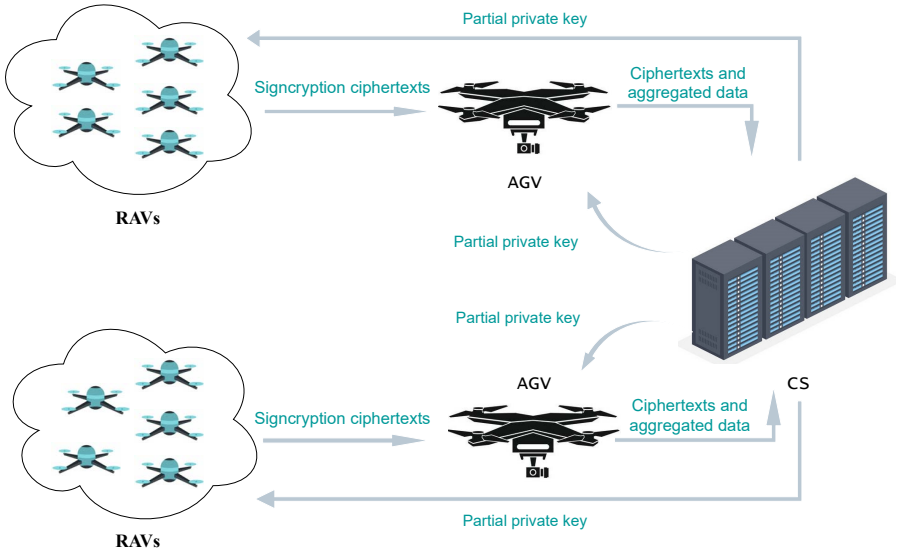


Fig. 1. System model for data collection in UAV cluster network

- **Key generation**: This procedure is jointly performed by CS and each entity including RAV and AGV. With the system parameter $params$, the master private key $s$ and the entity's identity $ID$, CS outputs a partial private key $ppk$ for $ID$. The entity $ID$ is able to validate $ppk$, and then generates a pair of public key and private key $(pk, sk)$.
- **Signcryption**: This procedure is performed by each UAV including RAVs and AGV for signcrypting the collected data. With inputs $params$, the UAV's identifier $ID$, the collected data $m$, the public key $pk$ of CS and the private key $sk$ of such entity, the procedure outputs the signcryption $\sigma$ on $m$.
- **Data aggregation**: This procedure is performed by AGV for validating and aggregating the signcrypted data from RAVs in the same cluster. With inputs $params$, each UAV's identity $ID$ and public key $pk$, and the signcryptions $\{\sigma\}$, all $\{\sigma\}$ are aggregated and validated by AGV. If true, the signcryption of AGV will be further added to ciphertext $c$ and aggregated data $\gamma$. Otherwise, "Reject" is outputted.
- **Un-Signcryption**: This procedure is performed by CS for validating and decrypting the collected data. With $params$, $\gamma$ and the private key $sk$ of CS as input, if the ciphertext $c$ is verified as valid, then outputs the collected data from UAVs.

A correct CL-ASC construction should satisfy the following conditions:

1) the partial private key produced by CS can be successfully validated by the corresponding entity, i.e., RAV or AGV;
2) the ciphertext can be correctly decrypted by CS;
3) the signcryption of RAVs can be successfully validated by AGV;
4) the signcryptions of UAVs (including RAVs and AGV) can be successfully validated by CS.

## IV. CL-ASC Construction

This section presents our CL-ASC construction, which security relies on the following Elliptic Curve Discrete Logarithm Problem (ECDLP).

*ECDLP*: Let $G$ be an elliptic curve additive group with prime order $q$, and $P$ be a generator of G. Given a tuple $(P, aP)$ for unknown $a \in Z_q^*$. The advantage for any polynomial time algorithm to compute $a$ is negligible.

The frequently used symbols and running process of our CL-ASC construction are shown in Table I and Fig. 2, respectively.

TABLE I
NOTATIONS

| Notation | Description |
|---|---|
| $G$ | An elliptic curve additive group |
| $q$ | Prime order of group $G$ |
| $P$ | A generator of group G |
| $params$ | System parameters |
| $s$ | Master private key |
| $P_{pub}$ | Master public key |
| $H_1, H_2, H_3, H_4$ | Collision-resistant hash functions |
| $ppk$ | Partial private key |
| $ID_i$ | Identity of RAVs |
| $ID_n$ | Identity of AGV |
| $ID_c$ | Identity of CS |
| $pk_i, sk_i$ | Public-private key pair of RAVs |
| $pk_n, sk_n$ | Public-private key pair of AGV |
| $pk_c, sk_c$ | Public-private key pair of CS |
| $m_i$ | Collected data by $ID_i$ |
| $T$ | Timestamp |
| $c$ | Ciphertext |
| $\sigma$ | Signcryption |
| $\gamma$ | Aggregated data |

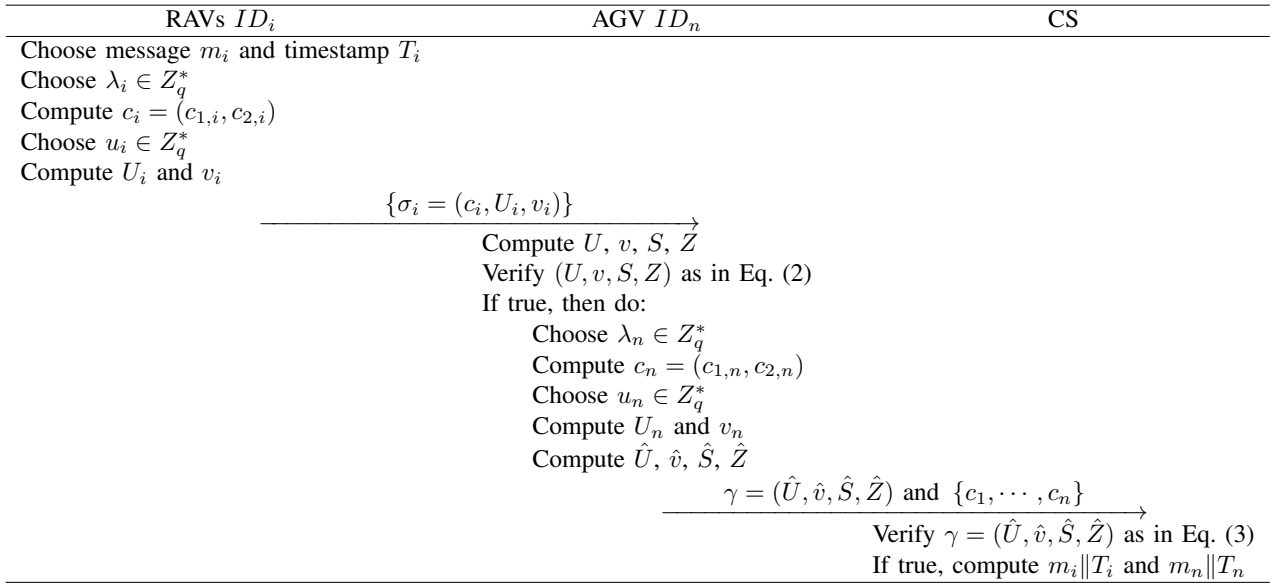


Fig. 2. A procedure of CL-ASC construction

### A. Setup Phase

Given the security parameter $k \in Z^+$, CS chooses an elliptic curve additive group $G$ with prime order $q$, where $P$ is a generator of group $G$. Then CS randomly chooses $s \in Z_q^*$ as the master private key and calculates

$$P_{pub} = sP$$

CS selects four collision-resistant hash functions $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$, $H_3 : \{0,1\}^* \rightarrow Z_q^*$ and $H_4 : \{0,1\}^* \rightarrow \{0,1\}^{2\log q}$. At last, CS publishes the system parameters $params = (q, G, P, P_{pub}, H_1, H_2, H_3, H_4)$ and keeps the master private key $s$ secret.

### B. Key Generation Phase

For RAV $ID_i$, CS chooses a random number $r_i \in Z_q^*$ and calculates

$$R_i = r_i P$$

and

$$d_i = (r_i + sh_{1,i}) \mod q$$

where $h_{1,i} = H_1(ID_i, R_i, P_{pub})$. The partial private key $ppk_i = (d_i, R_i)$ is sent to $ID_i$ through a secure channel. CS can also perform the similar process to generate partial private keys $ppk_c = (d_c, R_c)$ and $ppk_n = (d_n, R_n)$ for itself and AGV $ID_n$, respectively.

After receiving the partial private key $ppk_i$, RAV $ID_i$ first verifies it by checking the following equality

$$d_i P \stackrel{?}{=} R_i + h_{1,i} P_{pub} \quad (1)$$

Then RAV $ID_i$ randomly chooses a secret value $x_i \in Z_q^*$ and calculates

$$X_i = x_i P$$

and

$$Q_i = R_i + h_{2,i} X_i$$

where $h_{2,i} = H_2(ID_i, X_i)$. Finally, RAV $ID_i$ outputs the public-private key pair $(pk_i, sk_i)$, where $pk_i = (Q_i, R_i)$ and $sk_i = (d_i, x_i)$. Note that AGV $ID_n$ and CS can respectively generate their public-private key pairs $(pk_n, sk_n)$ and $(pk_c, sk_c)$ in the similar way.

### C. Signcryption Phase

For the collected message $m_i \in \{0,1\}^*$, RAV $ID_i$ generates a timestamp $T_i$, chooses a random number $\lambda_i \in Z_q^*$ and calculates the ciphertext $c_i = (c_{1,i}, c_{2,i})$ as follows

$$c_{1,i} = (m_i \| T_i) \oplus H_4(\lambda_i (Q_c + h_{1,c} P_{pub}))$$

$$c_{2,i} = \lambda_i P$$

where $h_{1,c} = H_1(ID_c, R_c, P_{pub})$. Then RAV $ID_i$ picks a random number $u_i \in Z_q^*$ and calculates

$$U_i = u_i P$$

and

$$v_i = u_i + h_{3,i}(d_i + h_{2,i} x_i) \mod q$$

where $h_{2,i} = H_2(ID_i, X_i)$ and $h_{3,i} = H_3(ID_i, c_i, U_i)$. Finally, $ID_i$ sends the signcryption ciphertext $\sigma_i = (c_i, U_i, v_i)$ to AGV $ID_n$.

### D. Data Aggregation

For the received $n-1$ signcryption ciphertexts $\{\sigma_1 = (c_1, U_1, v_1), \cdots, \sigma_{n-1} = (c_{n-1}, U_{n-1}, v_{n-1})\}$ from RAVs in the same cluster, AGV $ID_n$ calculates

$$U = \sum_{i=1}^{n-1} U_i$$

$$v = \sum_{i=1}^{n-1} v_i$$

$$S = \sum_{i=1}^{n-1} h_{3,i} h_{1,i}$$

and

$$Z = \sum_{i=1}^{n-1} h_{3,i} Q_i$$

where $h_{1,i} = H_1(ID_i, R_i, P_{pub})$ and $h_{3,i} = H_3(ID_i, c_i, U_i)$ Then, AGV $ID_n$ verifies the authenticity the signcryption ciphertexts by checking the following equation

$$vP \stackrel{?}{=} U + Z + SP_{pub} \tag{2}$$

If it holds, then these signcryption ciphertexts are valid. Next, AGV $ID_n$ generates timestamp $T_n$, randomly picks $\lambda_n \in Z_q^*$, and generates the ciphertext $c_n = (c_{1,n}, c_{2,n})$ for data $m_n$ as follows

$$c_{1,n} = (m_n || T_n) \oplus H_4(\lambda_n(Q_c + h_{1,c} P_{pub}))$$

$$c_{2,n} = \lambda_n P$$

AGV $ID_n$ continues to choose a random number $u_n \in Z_q^*$ and calculate

$$U_n = u_n P$$

and

$$v_n = u_n + h_{3,n}(d_n + h_{2,n} x_n) \mod q$$

where $h_{2,n} = H_2(ID_n, X_n)$ and $h_{3,n} = H_3(ID_n, c_n, U_n)$. They are further added to the aggregated data as follows

$$\hat{U} = U + U_n$$

$$\hat{v} = v + v_n$$

$$\hat{S} = S + h_{3,n} h_{1,n}$$

$$\hat{Z} = Z + h_{3,n} Q_n$$

where $h_{1,n} = H_1(ID_n, R_n, P_{pub})$. Finally, AGV $ID_n$ sends the aggregated data $\gamma = (\hat{U}, \hat{v}, \hat{S}, \hat{Z})$ and ciphertexts $\{c_1, \cdots, c_n\}$ to CS.

### *E. Un-Signcryption Phase*

After receiving the aggregated data $\gamma = (\hat{U}, \hat{V}, \hat{S}, \hat{Z})$ and ciphertexts $\{c_1, \cdots, c_n\}$ from AGV $ID_n$, CS first verifies their authenticity by running the following equation

$$\hat{V}P \stackrel{?}{=} \hat{U} + \hat{Z} + \hat{S} P_{pub} \tag{3}$$

If it holds, then the ciphertexts from UAVs are valid. Next, CS is able to decrypt $n$ ciphertexts $c_1, c_2, \cdots, c_n$ one by one to obtain messages $m_1, m_2, \cdots, m_n$ collected by RAVs and AGV. That is, for each $c_i = (c_{1,i}, c_{2,i})$ where $i = 1, \cdots, n$, CS calculates

$$m_i || T_i = c_{1,i} \oplus H_4((d_c + h_{2,c} x_c) c_{2,i})$$

where $h_{2,c} = H_2(ID_c, X_c)$.

*Theorem 1:* The above proposed CL-ASC construction is correct.

*Proof 1:* For the correctness of encryption and decryption, we know that for ciphertext $c_i = (c_{1,i}, c_{2,i})$, the following equalities hold

$$\begin{aligned}
&c_{1,i} \oplus H_4((d_c + h_{2,c} x_c) c_{2,i}) \\
&\quad = (m_i || T_i) \oplus H_4(\lambda_i(Q_c + h_{1,c} P_{pub})) \\
&\qquad \oplus H_4((d_c + h_{2,c} x_c) c_{2,i}) \\
&\quad = (m_i || T_i) \oplus H_4(\lambda_i(R_c + h_{2,c} X_c + h_{1,c} P_{pub})) \\
&\qquad \oplus H_4((d_c + h_{2,c} x_c) c_{2,i}) \\
&\quad = (m_i || T_i) \oplus H_4(\lambda_i(r_c + h_{2,c} x_c + s h_{1,c}) P) \\
&\qquad \oplus H_4((d_c + h_{2,c} x_c) c_{2,i}) \\
&\quad = (m_i || T_i) \oplus H_4((d_c + h_{2,c} x_c) c_{2,i}) \\
&\qquad \oplus H_4((d_c + h_{2,c} x_c) c_{2,i}) \\
&\quad = m_i || T_i
\end{aligned}$$

Thus, the original collected message $m_i$ can be correctly decrypted from the valid ciphertext $c_i$.

For the correctness of verifying the partial private key $ppk_i$, the Eq. (1) holds as follow

$$\begin{aligned}
d_i P &= (r_i + s h_{1,i}) P \\
&= r_i P + s h_{1,i} P \\
&= R_i + h_{1,i} P_{pub}
\end{aligned}$$

Thus, the partial private key $ppk$ distributed by CS for each entity can be correctly verified.

For the correctness of aggregation verification by AGV on signcryption ciphertexts from RAVs in the same cluster, the Eq. (2) holds as follows

$$\begin{aligned}
vP &= \sum_{i=1}^{n-1} v_i P \\
&= \sum_{i=1}^{n-1} (u_i + h_{3,i}(d_i + h_{2,i} x_i)) P \\
&= \sum_{i=1}^{n-1} (u_i + h_{3,i}((r_i + s h_{1,i}) + h_{2,i} x_i)) P \\
&= \sum_{i=1}^{n-1} u_i P + \sum_{i=1}^{n-1} h_{3,i}((R_i + h_{1,i} P_{pub}) + h_{2,i} X_i) \\
&= \sum_{i=1}^{n-1} U_i + \sum_{i=1}^{n-1} h_{3,i}(Q_i + h_{1,i} P_{pub}) \\
&= U + \sum_{i=1}^{n-1} h_{3,i} Q_i + \sum_{i=1}^{n-1} h_{3,i} h_{1,i} P_{pub} \\
&= U + Z + S P_{pub}
\end{aligned}$$

Thus, AGV can correctly verify the authenticity data collected by RAVs through Eq. (2).

For the correctness of aggregation verification by CS on signcryption ciphertexts from RAVs and AGV in the same cluster, the Eq. (3) holds as follows

$$\begin{aligned}\hat{v}P &= \sum_{i=1}^{n} v_i P \\ &= \sum_{i=1}^{n} (u_i + h_{3,i}(d_i + h_{2,i}x_i))P \\ &= \sum_{i=1}^{n} (u_i + h_{3,i}((r_i + sh_{1,i}) + h_{2,i}x_i))P \\ &= \sum_{i=1}^{n} u_i P + \sum_{i=1}^{n} h_{3,i}((R_i + h_{1,i}P_{pub}) + h_{2,i}X_i) \\ &= \sum_{i=1}^{n} U_i + \sum_{i=1}^{n} h_{3,i}(Q_i + h_{1,i}P_{pub}) \\ &= \hat{U} + \sum_{i=1}^{n} h_{3,i}Q_i + \sum_{i=1}^{n} h_{3,i}h_{1,i}P_{pub} \\ &= \hat{U} + \hat{Z} + \hat{S}P_{pub}\end{aligned}$$

Thus, CS is able to correctly verify the authenticity of data collected by UAVs through Eq. (3).

## V. Analysis

### A. Security Analysis

*Theorem 2:* The proposed CL-ASC construction can guarantee the confidentiality of collected data. That is, any adversary cannot obtain the real content of the data collected by UAVs.

*Proof 2:* In the proposed CL-ASC construction, the collected data is signcrypted with the CS's public key $pk_c$. To decrypt a ciphertext $c_i$, the private key $sk_c$ of CS must be used to calculate $m_i \| T_i = c_{1,i} \oplus H_4((d_c + h_{2,c}x_c)c_{2,i})$. Without the partial private key $ppk_c$ and the secret value $x_c$, the adversary would be unable to deduce $m_i$ from ciphertext $c_i$. Thus, the proposed CL-ASC construction can protect the confidentiality on collected data from RAVs and AGV.

*Theorem 3:* The proposed CL-ASC construction can guarantee the integrity of collected data. That is, any adversary cannot tamper with or forge the messages transmitted in CL-ASC system.

*Proof 3:* In the proposed CL-ASC construction, the signature on the ciphertext is generated with the certificateless signcryption technology, which is adapted from the PF-CLS scheme of Thumbur et al. [26]. Specifically, $(U, v)$ in the proposed CL-ASC construction can be seen as $\sigma$ in PF-CLS. According to Theorem 1 of [26], the PF-CLS is proved to be existentially unforgeable under the ECDLP assumption. Thus, the proposed CL-ASC construction also enjoys existentially unforgeability under the ECDLP assumption.

*Theorem 4:* The proposed CL-ASC construction can guarantee the authenticity of the collected data source.

*Proof 4:* As shown in Theorem 3, the collected data is signed by employing the certificateless signcryption technology. Therefore, any adversary is unable to impersonate a valid RAV or AGV to produce a signcryption ciphertext without being detected, which means that the authenticity of data source can be guaranteed.

*Theorem 5:* The proposed CL-ASC construction can resist replay attacks.

*Proof 5:* In generating a signcryption ciphertext $c$ on collected data $m$, the timestamp $T$ is introduced. Thus, CS is able to check the freshness of each message after decryption, in this way all re-sent messages could be detected. Also, according to Theorem 3 and Theorem 4, the signcryption ciphertext cannot be tampered with and forged, which means any adversary is unable to change the freshness of the processed data during transmission. Thus, the proposed CL-ASC construction can resist replay attacks.

*Theorem 6:* The proposed CL-ASC construction can resist malicious CS. That is, CS is unable to forge a collected data of honest RAV and AGV.

*Proof 6:* In the proposed CL-ASC construction, only a partial private key of each entity is generated by CS with the master private key, which means CS does not hold the private key of such entity. According to Theorem 3 and Theorem 4, without the private key of RAV or AGV, CS is unable to forge a valid signcryption ciphertext of such UAV. Hence, the proposed CL-ASC construction can resist malicious CS.

### B. Theoretical Analysis

This section evaluates the performance of the proposed CL-ASC construction and compares with Wang et al.'s scheme [23] and Li et al.'s scheme [24]. As shown in Table II, $T_{SM}$ denotes the time for one scalar point multiplication operation, $T_{EA}$ represents the time for one elliptic curve point addition operation, and $T_{PA}$ is the time for one bilinear pairing operation. As shown in Table III, although both the schemes of Wang et al. [23] and Li et al. [24] support authentication the identity of each UAV, they do not consider data privacy protection. The proposed CL-ASC construction simultaneously supports data source authentication and privacy protection.

TABLE II
Operation and time

| Notations | Meaning | Time (ms) |
|---|---|---|
| $T_{SM}$ | Scalar point multiplication | $T_{SM} = 3$ |
| $T_{EA}$ | Elliptic curve point addition | $T_{EA} = 0.418$ |
| $T_{PA}$ | Bilinear pairing | $T_{PA} = 1.994$ |

To generate a signature, Wang et al.'s scheme [23] requires three scalar point multiplication operations and one elliptic curve point addition operation, while Li et al.'s scheme [24] takes three scalar point multiplication operations and two elliptic curve point addition operations. For the proposed CL-ASC construction, only one scalar point multiplication operation is needed in generating a signature. For aggregation on $n$ messages, both the schemes of Wang et al. [23] and Li et al. [24] need $2(n-1)$ elliptic curve point addition operations, whereas the proposed CL-ASC construction requires $n$ scalar point multiplication operations and $2(n-1)$ elliptic curve

TABLE III
THEORETICAL ANALYSIS AND COMPARISON

| Scheme | Authentication | Privacy protection | Signing cost | Aggregation cost on $n$ messages | Aggregate verification costs |
|---|---|---|---|---|---|
| Li et al. [24] | $\surd$ | – | $3T_{SM}+2T_{EA}$ | $2(n-1)T_{EA}$ | $3T_{PA}+nT_{SM}+(2n-1)T_{EA}$ |
| Wang et al. [23] | $\surd$ | – | $3T_{SM}+T_{EA}$ | $2(n-1)T_{EA}$ | $3T_{PA}+nT_{SM}+(n-1)T_{EA}$ |
| Our scheme | $\surd$ | $\surd$ | $T_{SM}$ | $nT_{SM}+2(n-1)T_{EA}$ | $2T_{SM}+2T_{EA}$ |

point addition operations. When verifying the aggregation of $n$ messages, both the schemes of Wang et al. [23] and Li et al. [24] have to take resource-intensive bilinear operations, which means they have relatively high computational overhead. In this phase, the proposed CL-ASC construction only requires constant operations, i.e., two scalar point multiplications and two elliptic curve point addition operations, which greatly reduces the computational costs compared to [23], [24].

### C. Experimental Analysis

In this section, we evaluate the experimental performance of the proposed CL-ASC construction, where the Golang language is used to complete experiments on a platform with Microsoft Windows 10 operating system, Intel(R) Core(TM) i5-7700 @ 3.6GHz. The elliptic curve is NIST P-256 ($y^2 = x^3 - 3x + b \mod q$), where $q$ is a 512-bit prime, and all hash functions are SHA-256. In experiments, suppose there are 100 RAVs and one AGV in the same cluster. The performance for the setup phase (Setup), key generation phase (KeyGen), signcryption phase (Signcryption), data aggregation phase (DataAgg) and un-signcryption phase (Un-Signcryption) are shown in Fig. 3.

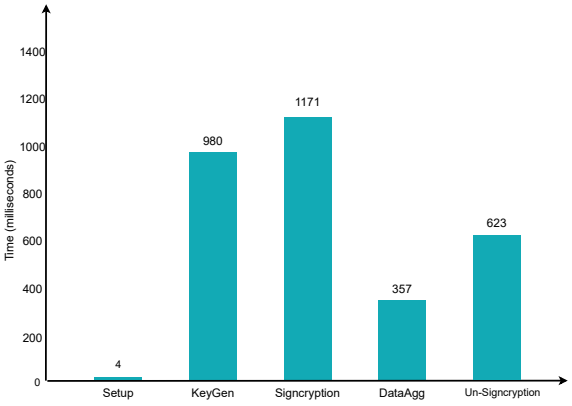


Fig. 3. Performance of each phase in CL-ASC

The setup phase is executed only once to initialize the system, which performance mainly depends on the computational costs of $P_{pub}$ and takes about 4 ms in the experiment. The performance of the key generation phase is mainly determined by the computational costs of partial private keys by CS and public-private key pair by each entity. Fig. 3 shows the total time of generating key pairs for 100 RAVs, one AGV and one CS, thus the generation time of a single key pair is roughly 9.6 ms. The total time for 100 signcryptions generation is 1171 ms, which implies the generation time for a signcryption is about 11.7 ms. Data aggregation consists of two phases, i.e., data aggregation and aggregation verification, where the total time in the experiment is about 0.36 seconds. The performance of un-signcryption is mainly determined by 101 ciphertext decryption, which takes 0.62 seconds in total.

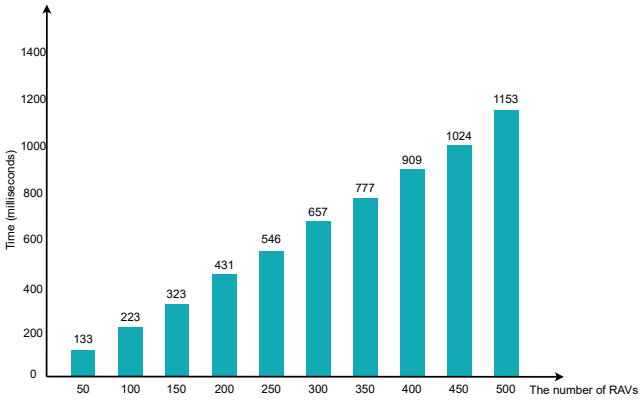


Fig. 4. Performance of data aggregation with different number of RAVs

Fig. 4 depicts the performance of data aggregation with $50, 100, \cdots, 500$ RAVs. It is shown that the time cost is linearly increased with the number of RAVs. The verification on aggregated data is only performed once in this phase, which has no relation with the number of RAVs in the same cluster. In the un-signcryption phase, CS performs an aggregation verification and decrypts all ciphertexts upon successful verification. Fig. 5 considers the cases of $50, 100, \cdots, 500$ RAVs, respectively. The experimental result show that as the number of RAVs increases, similar to Fig. 4, the total time cost shows a linear growth trend. Thus, the performance of un-signcryption is also determined by the number of RAVs in the cluster.

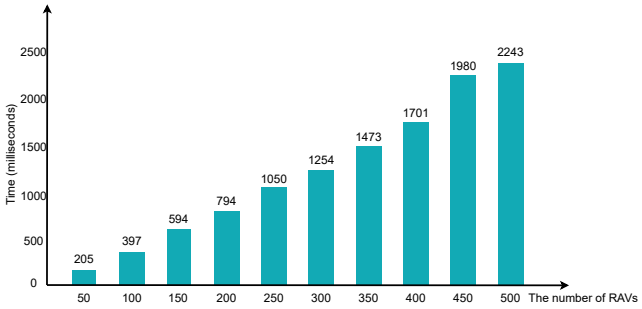


Fig. 5. Performance of un-signcryption with different number of RAVs

## VI. Conclusions

To address the security and privacy issues in the resource-constrained UAV cluster network, this paper proposed a certificateless aggregate signcryption (CL-ASC) scheme. With CL-ASC, RAVs are able to signcrypt on the collected data and send them to the administrative AGV in the same cluster. The signcrypted data are aggregated by AGV before performing verification, which is then aggregated further with the AGV's signcryption on its collected data. The ciphertexts and aggregated signature can be validated by CS for recovering the collected data from all RAVs and AGV. Security analysis showed that the proposed CL-ASC construction can guarantee the security and privacy of the collected data, as well as resist replay attacks and malicious CS. Theoretical and experimental analysis demonstrated that the proposed CL-ASC construction is suitable for the applications in UAV cluster network.

## Acknowledgment

This article is supported in part by the National Key R&D Program of China under project 2020YFB1006003, the National Natural Science Foundation of China under projects 61772150, 61862012 and 61962012, the Guangdong Key R&D Program under project 2020B0101090002, the Guangxi Natural Science Foundation under grants 2018GXNSFDA281054, 2019GXNSFFA245015, 2019GXNSFGA245004 and AD19245048, the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004, the Innovation Project of Guangxi Graduate Education YCSW2021176, and the Open Program of Guangxi Key Laboratory of Cryptography and Information Security under project GCIS201930.

## References

[1] T. Rana, A. Shankar, M. K. Sultan, R. Patan, and B. Balusamy, "An intelligent approach for uav and drone privacy security using blockchain methodology," in *2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, 2019, pp. 162–167.

[2] M. Y. Arafat and S. Moh, "A survey on cluster-based routing protocols for unmanned aerial vehicle networks," *IEEE Access*, vol. 7, pp. 498–516, 2019.

[3] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 134–139, 2017.

[4] M. Rodrigues, J. Amaro, F. S. Osrio, and B. Kalinka. R. L. J. C., "Authentication methods for uav communication," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, 2019, pp. 1210–1215.

[5] H. Qiu, M. Qiu, and Z. Lu, "Selective encryption on ecg data in body sensor network based on supervised machine learning," *Information Fusion*, vol. 55, pp. 59–67, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253519302556

[6] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, "Cppa-d: Efficient conditional privacy-preserving authentication scheme with double-insurance in vanets," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3456–3468, 2021.

[7] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in uav systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.

[8] M. Zhao, Y. Ding, Q. Wu, Y. Wang, B. Qi, and K. Fan, "Privacy-preserving lightweight data monitoring in internet of things environments," *Wireless Personal Communications*, vol. 116, pp. 1765–1783, 2021.

[9] Z. Fu, Y. Mao, D. He, J. Yu, and G. Xie, "Secure multi-uav collaborative task allocation," *IEEE Access*, vol. 7, pp. 35 579–35 587, 2019.

[10] T. Noguchi and Y. Komiya, "Persistent cooperative monitoring system of disaster areas using uav networks," in *2019 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2019, pp. 1595–1600.

[11] H. Qu, W. Zhang, J. Zhao, Z. Luan, and C. Chang, "Rapid deployment of uavs based on bandwidth resources in emergency scenarios," in *2020 Information Communication Technologies Conference (ICTC)*, 2020, pp. 86–90.

[12] J. Liang, P. Li, H. Zhao, L. Han, and M. Qu, "Forest species classification of uav hyperspectral image using deep learning," in *2020 Chinese Automation Congress (CAC)*, 2020, pp. 7126–7130.

[13] Z. Huang, T. Zhang, P. Liu, and X. Lu, "Outdoor independent charging platform system for power patrol uav," in *2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, 2020, pp. 1–5.

[14] X. Gao, H. Jia, Z. Chen, G. Yuan, and S. Yang, "Uav security situation awareness method based on semantic analysis," in *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, 2020, pp. 272–276.

[15] A. Omri and M. O. Hasna, "Physical layer security analysis of uav based communication networks," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018, pp. 1–6.

[16] K. Kim and Y. Kang, "Drone security module for uav data encryption," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 1672–1674.

[17] L. Liu, H. Qian, and F. Hu, "Random label based security authentication mechanism for large-scale uav swarm," in *2019 IEEE Intl Conf on Parallel Distributed Processing with Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2019, pp. 229–235.

[18] E. Ghribi, T. T. Khoei, H. T. Gorji, P. Ranganathan, and N. Kaabouch, "A secure blockchain-based communication approach for uav networks," in *2020 IEEE International Conference on Electro Information Technology (EIT)*, 2020, pp. 411–415.

[19] K. Gai, Y. Wu, L. Zhu, K.-K. R. Choo, and B. Xiao, "Blockchain-enabled trustworthy group communications in uav networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4118–4130, 2021.

[20] A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020, pp. 1–9.

[21] T. Li, J. Ma, P. Feng, Y. Meng, X. Ma, J. Zhang, C. Gao, and D. Lu, "Lightweight security authentication mechanism towards uav networks," in *2019 International Conference on Networking and Network Applications (NaNA)*, 2019, pp. 379–384.

[22] T. Alladi, Naren, G. Bansal, V. Chamola, and M. Guizani, "Secauthuav: A novel authentication scheme for uav-ground station and uav-uav communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 068–15 077, 2020.

[23] H. Wang, J. Li, C. Lai, and Z. Wang, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 53–63, 2020.

[24] J. Li, M. Zhao, Y. Ding, D. Y. W. Liu, Y. Wang, and H. Liang, "An aggregate authentication framework for unmanned aerial vehicle cluster network," in *2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2020, pp. 1249–1256.

[25] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in vanets," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1779–1790, 2019.

[26] G. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri, and D. V. R. K. Reddy, "Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1641–1645, 2020.