Secure Estimation Using Partially Homomorphic Encryption for Unmanned Aerial Systems in the Presence of Eavesdroppers

Xinhao Yan, Guanzhong Zhou, Yue Huang, Wei Meng, Anh-Tu Nguyen, Hailong Huang

Secure Estimation Using Partially Homomorphic Encryption for Unmanned Aerial Systems in the Presence of Eavesdroppers

Xinhao Yan, Guanzhong Zhou, Yue Huang, Wei Meng, Anh-Tu Nguyen, Hailong Huang

***Abstract*—Unmanned aerial systems (UASs) are attracting increasing attention thanks to the great mobility and flexibility of unmanned aerial vehicles (UAVs). This paper considers a typical UAS, which consists of a UAV, a sensing device that provides some sensed data to the UAV, and an end-user that operates the UAV. However, the information exchanged between these parties is vulnerable to eavesdropping attacks, emphasizing the need to develop privacy-preserving approaches. The cryptographic methods are undoubtedly effective, but their high computational overhead may adversely impact the normal operations of UASs. Additionally, the dynamic of a UAV has a high dimension, which is disadvantageous for both estimation and encryption. Therefore, this paper proposes a secure distributed estimation protocol with partially homomorphic encryption by encrypting the transmitted measurements and estimates. Attribute to distributed structure and partial homomorphism, the computation amount for secure estimation is greatly reduced. At the same time, the raw data that needs to be encrypted is transferred into the space of plaintexts by a uniform quantizer and a mapping strategy. Finally, the effectiveness of the proposed method is verified by computer simulation.**

***Index Terms*—Unmanned aerial vehicles (UAVs), state estimation, homomorphic encryption, uniform quantization**

I. Introduction

A. Background

Due to the flexibility of unmanned aerial vehicles (UAVs), unmanned aerial systems (UASs) that consist of UAVs and other equipment have found a wide range of applications, including task offloading [1], covert surveillance [2], multiple access [3], and relay communication [4]. As one of the most important issues, the trajectories of UAVs need to be tracked and some state estimation methods are applied to decrease the influence of system noises [5], [6]. Unfortunately, the UASs are facing many safety problems [7], and particularly, there exist many malicious eavesdroppers that want to intercept the information of UASs [8]. For example, they require the precise position of a UAV to launch some vicious attacks, such as spoofing attacks [9] and even physical attacks [10]. A structure of UAS in the presence of eavesdroppers is shown in Fig. 1. In this case, the eavesdroppers have access to the user-UAV channel and sensor-UAV channel, and they can speculate the accurate states of UAVs based on the wiretapped measurements, estimates, and other information. Because of the great harm brought by eavesdropping, it is of great significance to protect the privacy of the transmitted data in UASs.

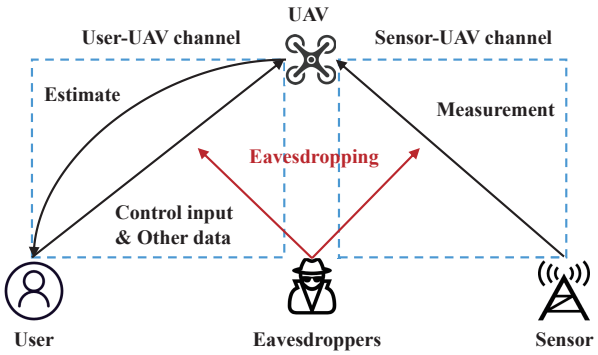

Fig. 1. A structure of UAS in the presence of eavesdroppers.

To counter eavesdroppers, there exist many privacy-preserving methods, such as data perturbation [11], [12], cryptography [13], and transmission scheduling [14]. Authentication schemes [15]–[17] can prevent unauthorized access in physical layer by verifying identities. Nonetheless, the information leakage will be large if the scheme is cracked or a legitimate party is hijacked, thus the encryption methods on data layer is also required. Data perturbation methods can effectively harm the performance of eavesdroppers thanks to the increase of randomness [12]. Nevertheless, the utility of valid information for the legitimate user is generally diminished under perturbation schemes. For instance, differentially private mechanisms will negatively impact the estimation performance, because the random noises increase the estimation error covariances [18], [19]. By contrast, cryptographic methods can maintain the accuracy of data, because the decryption procedures can always completely recover the original data [13].

B. Related Work

Homomorphic encryption is a classical cryptographic approach, which allows certain operations on the encrypted data [20]. It has been widely used for various scenarios, including cloud-based systems [21], Internet of Things (IoT) [22], and image processing [23]. In general, there are two homomorphisms: additive homomorphism and multiplicative homomorphism, which respectively means addition and multiplication are operable on ciphertexts. Then, the homomorphic scheme can be divided into two main kinds: fully

This work was supported in part by the Research Centre for Unmanned Autonomous Systems via the project P0049529 and National Natural Science Foundation of China under Grant U21A20476.

Xinhao Yan, Guanzhong Zhou and Hailong Huang are with the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong (email: xin-hao-shawn.yan@connect.polyu.hk; guanzhong.zhou@connect.polyu.hk; hailong.huang@polyu.edu.hk).

Yue Huang is with Data61, Commonwealth Scientific and Industrial Research Organisation, Melbourne, Australia (email: yue2.huang@csiro.au).

Wei Meng is with Guangdong University of Technology, Guangzhou 510006, China (e-mail: meng0025@ntu.edu.sg).

Anh-Tu Nguyen is with the LAMIH laboratory, UMR CNRS 8201, Universit Polytechnique Hauts-de-France, 59300 Valenciennes, France, and also with the INSA Hauts-de-France, 59300 Valenciennes, France (e-mail: nguyen.trananhtu@gmail.com).

Corresponding author: Hailong Huang.

homomorphic encryption [24] and partially homomorphic encryption [25]. The fully homomorphic encryption [24] can simultaneously support both additive and multiplicative homomorphisms, while the partially homomorphic encryption can only support one of them. Paillier [25] is a kind of typically additive homomorphic encryption, RSA [26] and ElGamal [27] are typically multiplicative homomorphic encryption approaches. Note that the fully homomorphic encryption requires a long computation time, which has been proved by the practical experiments in [28]. It shows that the estimation with partially homomorphic encryption only requires several milliseconds, while that with fully homomorphic encryption takes several hours and that with garbled circuits takes several minutes. Hence, partially homomorphic encryption is more practical for real-time estimation. Besides, there also exists a special kind called hybrid homomorphic encryption [29], where two different homomorphic encryption approaches are combined to achieve both multiplicative and additive homomorphisms.

Moreover, it should be pointed out that the data going to be processed by the homomorphic encryption must lie in the space of plaintext. This is because the encryption and decryption functions are based on the modular arithmetic that only deals with integers. This condition is an important preliminary, but it is always ignored. For example, the performance degradation is neglected for theoretical analysis [30]. To solve this problem, the float number is expressed by a positive exponent and a mantissa in [31], and the representations are all integers that can be encrypted. Such encoding method has already been employed to state estimation field [32]. Instead of the detailed representation of the whole float number, quantization is another method to transfer the data into the space of plaintext. It only preserves the integer part and directly deletes the mantissa. A probabilistic uniform quantization is adopted in [29], where the output is chosen randomly in an interval.

Recently, the differentially private estimator was proposed in [33], while the legitimate estimation performance was degraded due to the injection of random noises. The homomorphic encryption-based estimator was studied in [29], but the hybrid homomorphism consumed a great computation amount. Further, the additive homomorphic encryption was applied to protect the estimator in [30], but the mapping process was ignored. Notice that most traditional estimators are centralized [5], [6]. In this case, the great computation burden will be large due to the augmentation of all the local components. Moreover, although the confidentiality problem of UAS is always a significant issue, homomorphic encryption is rarely studied for UAS. Except for the normal operations on control and estimation, the extra computation on UAS should also be as little as possible, because real-time performance is important for UAS. Meanwhile, some parameters do not require privacy preservation, because the eavesdroppers cannot speculate the state from them. Therefore, partially homomorphic encryption is considered in this paper, which requires less computation amount than fully and hybrid homomorphic encryption methods.

C. Contributions

According to the above analysis, the main contributions of this paper are summarized as follows.

1) The globally high-dimensional system of a UAV is separated into a translational subsystem and a rotational subsystem, and the two subsystems are respectively estimated by their own low-dimensional estimators. Such a distributed estimation structure significantly decreases the computational complexity of both estimation and encryption.
2) A secure estimation protocol is proposed for the UAS against eavesdroppers, where the privacy of the translational state estimates is protected by a partially homomorphic encryption approach with a uniform quantizer. The partial encryption and time-invariant quantization further reduce the computation amount.

The rest of this paper is organized as follows. Section II discusses the complete dynamics of the UAV. Then, the distributed estimation models are presented by dividing the global system into a translational subsystem and a rotational subsystem. In Section III, the Kalman-like distributed estimator is designed in the minimum variance sense. Next, Paillier homomorphic encryption and uniform quantization methods are introduced to preserve the privacy of UAS, and the complete protocol is proposed. Afterwards, the simulation results are shown in Section IV, including the tracking trajectories, estimation performance, and time cost. Finally, the conclusion is given in Section V. The notations frequently used throughout the paper are summarized in Table I.

TABLE I
NOTATIONS

$\triangleq$	define
I	identity matrix with appropriate dimension
$\mathbb{Z}$	set of integers
$\mathbb{Z}^{n\times m}$	set of $n\times m$ integer matrix
$\mathbb{Z}_N$	set of integers modulo N
$\mathbb{Z}_N^*$	set of invertible integers modulo N
$\mathbb{R}$	set of real number
$\mathbb{R}^n$	set of n-dimensional real vectors
$\mathbb{R}^{n\times m}$	set of $n\times m$ real matrices
$\mathbb{E}\{\cdot\}$	mathematical expectation
$\dot{x}$	derivative of x
A^{T}	transpose of matrix A
$[x]_i$	i-th component of vector x
$[A]_{ij}$	i-th row and j-th column of matrix A
$\mathrm{col}\{\cdot\}$	column vector
$\mathrm{Tr}\{\cdot\}$	trace of a matrix
$X>(<)0$	positive-definite (negative-definite)
$X\geq(\leq)0$	non-negative definite (non-positive definite)
$\lfloor x\rfloor$	floor function: $\max\{a\in\mathbb{Z}:a<x\}$
$\mathrm{sgn}(\cdot)$	sign function
$Q(\cdot)$	quantization function
x_q	quantized output of x
$M(\cdot)$	mapping function
x_m	mapped output of x
$\mathrm{Enc}(\cdot)$	encryption function
$\mathrm{Dec}(\cdot)$	decryption function
pk	public key
sk	private key
$[[x]]$	encrypted value of x

II. Problem Formulation

A. Quadrotor UAV Dynamics

The UAS considered in this paper contains a quadcopter UAV with 6 degrees of freedom (6-DoF), where the attitude is depicted by Euler angles [10], [34]–[36]. The schematic model of a 6-DoF quadrotor UAV is shown in Fig. 2. Here, we use $\mathcal{I}$ to denote the inertial frame and $\mathcal{B}$ to denote the body frame, and the time index t is neglected in this subsection for brevity.

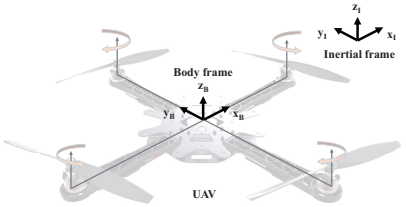

Fig. 2. The schematic model of a 6-DoF quadrotor UAV.

Note that a 6-DoF quadrotor dynamic model is nonlinear and the global state consists of 12 dimensions. It is a complex and high-dimensional system that will increase the computation burden of estimation. As a result, the UAV dynamic system is separated into translational and rotational subsystems in this paper. First, the translational dynamics of UAV can be described by the Newton equation [34]:

$$\dot{v}_{\mathcal{I}} = \frac{1}{m} R_{\mathcal{BI}} T_{\mathcal{B}} - g_{\mathcal{I}}, \tag{1}$$

where $p_{\mathcal{I}}(t) \triangleq \text{col}\{p_x, p_y, p_z\}$ and $v_{\mathcal{I}}(t) \triangleq \text{col}\{v_x, v_y, v_z\}$ respectively denotes the 3-dimensional (3D) position vector and velocity vector of UAV in the inertial frame. $T_{\mathcal{B}}(t) = \text{col}\{0, 0, F\}$ is the thrust force, $g_{\mathcal{I}} = \text{col}\{0, 0, g\}$ is the gravitational acceleration in inertial frame, and m is the mass of UAV. The matrix $R_{\mathcal{BI}}$ denoting the transformation from the body frame to the inertial frame can be described by [10]:

$$R_{\mathcal{BI}} = \begin{bmatrix} c_\theta c_\psi & s_\phi s_\theta c_\psi - s_\psi c_\phi & c_\phi s_\theta c_\psi + s_\phi s_\psi \\ c_\theta s_\psi & s_\phi s_\theta s_\psi + c_\phi c_\psi & c_\phi s_\theta s_\psi - s_\phi c_\psi \\ -s_\theta & s_\phi c_\theta & c_\phi c_\theta \end{bmatrix}, \tag{2}$$

where s_a, c_a, t_a respectively stand for the sine, cosine and tangent of angle a. Combining the transformation matrix (2), the scalar form of translational subsystem (1) can be expressed by

$$\begin{cases} \dot{v}_x = \dfrac{1}{m}(c_\phi s_\theta c_\psi + s_\phi s_\psi) F \\ \dot{v}_y = \dfrac{1}{m}(c_\phi s_\theta s_\psi - s_\phi c_\psi) F. \\ \dot{v}_z = \dfrac{1}{m}(c_\phi c_\theta) F g \end{cases} \tag{3}$$

Second, the rotational dynamics of UAV can be modeled by the Euler equation [34]:

$$J_{\mathcal{B}} \dot{w}_{\mathcal{B}} = M_{\mathcal{B}} - \omega_{\mathcal{B}} \times J_{\mathcal{B}} \omega_{\mathcal{B}}, \tag{4}$$

where $M_{\mathcal{B}} = \text{col}\{M_x, M_y, M_z\}$ is the moment, $\omega_{\mathcal{B}} = \text{col}\{\dot{\phi}, \dot{\theta}, \dot{\psi}\}$ is the angular speed and $J_{\mathcal{B}} = \begin{bmatrix} J_{xx} & 0 & 0 \\ 0 & J_{yy} & 0 \\ 0 & 0 & J_{zz} \end{bmatrix}$ is the moment of inertia matrix. Here, $\{\phi, \theta, \psi\}$ stand for the Euler angles in the inertial frame, where ϕ is the roll angle, θ is the pitch angle, and ψ is the yaw angle. $\{p, q, r\}$ are the corresponding angular velocity in the body frame. Then, the transformation between $\{\phi, \theta, \psi\}$ and $\{p, q, r\}$ is given by [10]:

$$\begin{bmatrix} \dot{\phi} \\ \dot{\theta} \\ \dot{\psi} \end{bmatrix} = \begin{bmatrix} 1 & s_\phi t_\theta & c_\phi t_\theta \\ 0 & c_\phi & -s_\phi \\ 0 & \frac{s_\phi}{c_\theta} & \frac{c_\phi}{c_\theta} \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}. \tag{5}$$

Based on the small-angle approximation [37], one has $\phi = 0, \theta = 0, \psi = 0$. Thus, the above relationship can be simplified as

$$\begin{bmatrix} \dot{\phi} \\ \dot{\theta} \\ \dot{\psi} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}. \tag{6}$$

Then, the scalar form of dynamic model in (4) can be expressed by resorting to the approximation (6):

$$\begin{cases} \dot{p} = \dfrac{1}{J_{xx}} M_x + \dfrac{J_{yy} - J_{zz}}{J_{xx}} qr \\ \dot{q} = \dfrac{1}{J_{yy}} M_y + \dfrac{J_{zz} - J_{xx}}{J_{yy}} rp. \\ \dot{r} = \dfrac{1}{J_{zz}} M_z + \dfrac{J_{xx} - J_{yy}}{J_{zz}} pq \end{cases} \tag{7}$$

Moreover, the force $T_{\mathcal{B}}$ and moments $M_{\mathcal{B}}$ in above dynamics are generated with 4 rotors [35], [36]:

$$\begin{cases} F = k_F(m_1 + m_2 + m_3 + m_4) \\ M_x = k_F l(m_3 - m_4) \\ M_y = k_F l(m_1 - m_2) \\ M_z = k_M(m_1 + m_2 - m_3 - m_4) \end{cases}, \tag{8}$$

where k_F is the thrust coefficient, k_M is the drag coefficient, and $m_j(t)(j = 1, 2, 3, 4)$ are the respective pulse width modulation (PWM) inputs for 4 rotors. l is the distance from the axis of rotation of the rotors to the center of the UAV. Besides, the PWM inputs can be derived as

$$\begin{cases} m_1 = \dfrac{F}{4k_F} + \dfrac{M_y}{2k_F l} + \dfrac{M_z}{4k_M} \\ m_2 = \dfrac{F}{4k_F} - \dfrac{M_y}{2k_F l} + \dfrac{M_z}{4k_M} \\ m_3 = \dfrac{F}{4k_F} + \dfrac{M_x}{2k_F l} - \dfrac{M_z}{4k_M} \\ m_4 = \dfrac{F}{4k_F} - \dfrac{M_x}{2k_F l} - \dfrac{M_z}{4k_M} \end{cases}. \tag{9}$$

B. Problem Formulation

Except for a UAV, the discussed UAS in this paper also consists of a user and some sensors. Here, the user and sensor will send the control and measurement signals to the UAV, respectively. Then, the UAV estimates the real-time states and feeds certain information back to the user. Particularly, the controller in user will send 4-channel signals $\{F, M_x, M_y, M_z\}$ at each time slot, which is determined by the demand of the user.

In the beginning, we should further modify the aforementioned UAS models. In fact, paractical models of UASs are generally in discrete-time domain due to their running on certain computation units, thus the above continuous-time systems should be discretized. According to the above analysis, the global state $x(t) = \text{col}\{x_1(t), x_2(t)\}$ can be divided into the translational state $x_1(t) = \text{col}\{p_x(t), v_x(t), p_y(t), v_y(t), p_z(t), v_z(t)\}$ and the rotational state $x_2(t) = \text{col}\{\phi(t), p(t), \theta(t), q(t), \psi(t), r(t)\}$. In this case, the discrete-time model of dynamics (3) and (7) can be derived by using the first-order Runge-Kutta method:

$$\begin{cases} x_1(t+1) = A_1 x_1(t) + f_{12}(x_2(t), u_1(t)) + w_1(t) \\ x_2(t+1) = f_2(x_2(t)) + B_2(t) u_2(t) + w_2(t) \end{cases} \tag{10}$$

where $w_1(t) \in \mathbb{R}^6$ and $w_2(t) \in \mathbb{R}^6$ are the system noises coming from the modeling error and other internal disturbances. Here, they are assumed to be mutually independent

white Gaussian noises (WGNs), which is one of the most widely used methods. Then, their covariances Q_{w_1} and Q_{w_2} are defined as follows:

$$\mathbb{E}\{w_i(t_1)w_j^{\mathrm{T}}(t_2)\} = \delta(t_1,t_2)\delta(i,j)\mathrm{Q}_{w_i}\ (i,j=1,2), \quad (11)$$

where $\delta(i,j)$ is the indicator function such that $\delta(i,j)=1$ if $i=j$; otherwise, $\delta(i,j)=0$. Besides, the concrete values of covariance can be designed by resorting to the experimental experience. The 4-channel control input $u(t) \triangleq \mathrm{col}\{u_1(t),u_2(t)\}$ is composed of the force $u_1(t)=F(t)$ and the moment $u_2(t)=\mathrm{col}\{M_x(t),M_y(t),M_z(t)\}$. Moreover, other state-space matrices and nonlinearities of model (10) are given by

$$\begin{cases} A_1 = \begin{bmatrix} 1 & T_s & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & T_s & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & T_s \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \ B_2(t) = \begin{bmatrix} 0 & 0 & 0 \\ \frac{1}{J_{xx}} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \frac{1}{J_{yy}} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \frac{1}{J_{zz}} \end{bmatrix} \\ f_{12}(x_2(t),u_1(t)) = \begin{bmatrix} 0 \\ \frac{F(t)T_s}{m}(c_\phi s_\theta c_\psi + s_\phi s_\psi) \\ 0 \\ \frac{F(t)T_s}{m}(c_\phi s_\theta s_\psi - s_\phi c_\psi) \\ 0 \\ \frac{F(t)T_s}{m}(c_\phi c_\theta) - gT_s \end{bmatrix} \\ f_2(x_2(t)) = \begin{bmatrix} \phi(t)+p(t)T_s \\ p(t)+\frac{J_{yy}-J_{zz}}{J_{xx}}q(t)r(t)T_s \\ \theta(t)+q(t)T_s \\ q(t)+\frac{J_{zz}-J_{xx}}{J_{yy}}r(t)p(t)T_s \\ \psi(t)+r(t)T_s \\ r(t)+\frac{J_{xx}-J_{yy}}{J_{zz}}p(t)q(t)T_s \end{bmatrix} \end{cases} \quad (12)$$

where T_s is the sampling period for discretization.

In order to estimate the UAV states, some sensors are always deployed to observe the real dynamics of the UAV. There may be many measurement outputs from several sensors, but we finally consider an augmented measurement in this paper. Such modeling can also be treated as a kind of centralized fusion method, where all the local measurements are gathered by one party. Then, the measurement equation of the sensor can be expressed by

$$\begin{cases} y_1(t) = C_1x_1(t) + v_1(t) \\ y_2(t) = C_2x_2(t) + v_2(t) \end{cases}, \quad (13)$$

where $y_i(t)(i=1,2)$ represent the measured outputs and $C_i(i=1,2)$ represent the measurement matrices. The disturbances $v_i(t)(i=1,2)$ are also WGNs that satisfy

$$\mathbb{E}\{v_i(t_1)v_j^{\mathrm{T}}(t_2)\} = \delta(t_1,t_2)\delta(i,j)\mathrm{Q}_{v_i}\ (i,j=1,2), \quad (14)$$

where $Q_{v_i}(i=1,2)$ are the corresponding covariances. Since $w_i(t)$ and $v_j(t)$ are mutually independent, one has

$$\mathbb{E}\{w_i(t_1)v_j^{\mathrm{T}}(t_2)\} = 0\ (\forall\ i,j,t_1,t_2). \quad (15)$$

In general, there exist many sensors that are suitable for observing the UAV, such as global position system (GPS), range sensors, and inertial measurement units (IMUs). In the UAS of this paper, the measurements provided by GPS and accelerometer are chosen as an example, which contains the 3D position and 3D angle of the UAV. It means that the measurement matrices are expressed in the following form:

$$C_1 = \begin{bmatrix} C_x & 0 & 0 \\ 0 & C_y & 0 \\ 0 & 0 & C_z \end{bmatrix}, \ C_2 = \begin{bmatrix} C_p & 0 & 0 \\ 0 & C_q & 0 \\ 0 & 0 & C_r \end{bmatrix}, \quad (16)$$

where $C_x=C_y=C_z=\begin{bmatrix}1\ 0\end{bmatrix}$, $C_p=C_q=C_r=\begin{bmatrix}1\ 0\end{bmatrix}$. The above measurement system represents a general and simple structure, and the performance can be further improved by introducing more high-precision sensors.

In traditional methods, the translational subsystem and the rotational subsystem are estimated together, which is a centralized estimation structure. In this paper, we consider a distributed estimation scheme, where the two subsystems are estimated individually. One advantage of such decoupling is that the computation amount can be reduced. Based on all the measurements $\{y_i(0),\ldots,y_i(t)\}$ at discrete time slot t, the recursive estimators are designed based on the Kalman-like filter [38], [39]:

$$\begin{cases} \hat{x}_1^-(t) = A_1\hat{x}_1(t-1) + f_{12}(\hat{x}_2(t-1),u_1(t-1)) \\ \hat{x}_1(t) = (I-K_1(t)C_1)\hat{x}_1^-(t) + K_1(t)y_1(t) \\ \hat{x}_2^-(t) = f_2(\hat{x}_2(t-1)) + B_2(t-1)u_2(t-1) \\ \hat{x}_2(t) = (I-K_2(t)C_2)\hat{x}_2^-(t) + K_2(t)y_2(t) \end{cases}, \quad (17)$$

where $\hat{x}_1(t)$ and $\hat{x}_2(t)$ are the distributed state estimates. $K_1(t)$ and $K_2(t)$ are the estimator gains to be designed.

Notice that there exist many eavesdroppers that can silently overhear the communication channels and then estimate the system state with the wiretapped data. In some cases, they can employ the wiretapped measurements $y(t)$ to estimate the state as what the legitimate system does. On the other hand, they can also directly wiretap the estimates $\hat{x}(t)$. Accordingly, the privacy of all the above-mentioned signals should be preserved. Meanwhile, the ciphertexts may also be cracked and utilized. Here, the detailed definition of the eavesdropper is given as follows.

Definition 2.1 (Eavesdropping Model): The eavesdropper has access to both the user-UAV channel and the sensor-UAV channel, and it understands all the meanings of the wiretapped data. When it acquires plaintexts, a state estimator will be employed to calculate the final estimate with the raw data. On the other hand, when the eavesdropper acquires ciphertexts, it will launch chosen plaintext attack (CPA), which means that it will encrypt likely plaintexts with the public key and then test if they are equal to the ciphertexts.

For countering the potential eavesdroppers in UAV's estimation systems, certain information is required to be encrypted. Since the fundamental operations of the proposed estimators (17) are related to addition and multiplication, the homomorphic encryption method is feasible and suitable for privacy preservation. Then, the main problem to be tackled in this paper is how to apply the homomorphic encryption method to protect the privacy of the state estimates in the considered UAS. Besides, the calculation amount should be reduced as much as possible, because the complexity of cryptographic methods is high on a certain level.

III. Secure Estimation Protocol

A. Overview

In this section, the homomorphic encryption-based secure estimation protocol is presented, where the design of the

protocol is composed of two main parts: estimation and encryption. First, based on the decoupled subsystems, we design the distributed estimators in the minimum variance sense to accurately track the states of UAV. Second, we present the definitions and properties of Paillier homomorphic encryption. Meanwhile, the detailed quantization method is discussed, which is a preliminary of encryption. Finally, the complete protocol is given to show the realization of the proposed method, where Paillier homomorphic encryption is embedded in the distributed estimator.

B. Estimator Design

To design the estimator gain, Kalman filter [40] is a classical method in the minimum variance sense. However, there exist nonlinear items $f_{12}(x_2(t))$ and $f_2(x_2(t))$ that cannot be directly processed. Thus, by resorting to the main idea of extended Kalman filter (EKF) [41], the nonlinear functions are respectively linearized at the values of certain estimates.

Since the rotational subsystem has its own dynamics and is not affected by the translational subsystem, we first discuss the rotational state estimator $\hat{x}_2(t)$. As what is done in EKF, we expand the function $f_2(x_2(t))$ in the Taylor series about $\hat{x}_2(t)$:

$$f_2(x_2(t)) = f_2(\hat{x}_2(t)) + A_{2,J}(t)\tilde{x}_2(t) + \Delta_{f_2}(\tilde{x}_2^2(t)), \quad (18)$$

where $\tilde{x}_2(t) \triangleq x_2(t) - \hat{x}_2(t)$ is the estimation error for the rotational state, $\Delta_{f_2}(\tilde{x}_2^2(t))$ represents the high-order terms about Taylor expansion, and the Jacobian matrix $A_{2,J}(t) \triangleq \frac{\partial f_2(x_2(t))}{\partial x_2(t)}|_{x_2(t)=\hat{x}_2(t)}$ is calculated by

$$A_{2,J}(t) = \begin{bmatrix} 1 & T_s & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & \frac{J_{zz}-J_{xx}}{J_{yy}} r(t) T_s & 0 \\ 0 & 0 & 0 \\ 0 & \frac{J_{xx}-J_{yy}}{J_{zz}} q(t) T_s & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ \frac{J_{yy}-J_{zz}}{J_{xx}} r(t) T_s & 0 & \frac{J_{yy}-J_{zz}}{J_{xx}} q(t) T_s \\ T_s & 0 & 0 \\ 1 & 0 & \frac{J_{zz}-J_{xx}}{J_{yy}} p(t) T_s \\ 0 & 1 & T_s \\ \frac{J_{xx}-J_{yy}}{J_{zz}} p(t) T_s & 0 & 1 \end{bmatrix}_{x_1(t)=\hat{x}_1(t)}. \quad (19)$$

According to the dynamics of the system state in (10) and its estimate (17), the estimation error $\tilde{x}_2(t)$ can be expressed with the above linearization parameters:

$$\begin{aligned} \tilde{x}_2(t) =& (I - K_2(t)C_2)A_{2,J}(t-1)\tilde{x}_2(t-1) \\ &+ (I - K_2(t)C_2)w_2(t-1) - K_2(t)v_2(t) \end{aligned}. \quad (20)$$

By minimizing the trace of the estimation error covariance $P_2(t) \triangleq \mathbb{E}\{\tilde{x}_2(t)\tilde{x}_2^{\mathrm{T}}(t)\}$, the estimator gain $K_2(t)$ is derived as follows:

$$\begin{cases} P_2(t) = (I - K_2(t)C_2)P_2^-(t) \\ P_2^-(t) = A_{2,J}(t-1)P_2(t-1)A_{2,J}^{\mathrm{T}}(t-1) + Q_{w_2}. \\ K_2(t) = P_2^-(t)C^{\mathrm{T}}\left(C_2 P_2^-(t) C_2^{\mathrm{T}} + Q_{v_2}\right)^{-1} \end{cases} \quad (21)$$

Similarly, by expanding $f_{12}(x_2(t)$ in the Taylor series about $\hat{x}_2(t)$, one has

$$\begin{aligned} f_{12}(x_2(t)) =& f_{12}(\hat{x}_2(t)) \\ &+ A_{12,J}(t)\tilde{x}_2(t) + \Delta_{f_{12}}(\tilde{x}_2^2(t)) \end{aligned} \quad (22)$$

where $\Delta_{f_{12}}(\tilde{x}_2^2(t))$ is the high-order terms and the Jacobian matrix $A_{12,J}(t) = \frac{\partial f_{12}(x_2(t))}{\partial x_2(t)}|_{x_2(t)=\hat{x}_2(t)}$ is

$$A_{12,J}(t) = \begin{bmatrix} 0 & 0 & 0 \\ -s_\phi s_\theta c_\psi + c_\phi s_\psi & 0 & c_\phi c_\theta c_\psi \\ 0 & 0 & 0 \\ -s_\phi s_\theta s_\psi - c_\phi c_\psi & 0 & c_\phi c_\theta s_\psi \\ 0 & 0 & 0 \\ -s_\phi c_\theta & 0 & -c_\phi s_\theta \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & -c_\phi s_\theta s_\psi + s_\phi c_\psi & 0 \\ 0 & 0 & 0 \\ 0 & c_\phi s_\theta c_\psi + s_\phi s_\psi & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{F(t)T_s}{m}|_{x_2(t)=\hat{x}_2(t)}. \quad (23)$$

Then, the estimation error $\tilde{x}_1(t) \triangleq x_1(t) - \hat{x}_1(t)$ for the translational subsystem can be expressed as

$$\begin{aligned} \tilde{x}_1(t) =& (I - K_1(t)C_1)A_1\tilde{x}_1(t-1) \\ &+ (I - K_1(t)C_1)A_{12,J}(t-1)\tilde{x}_2(t-1) \\ &+ (I - K_1(t)C_1)w_1(t-1) - K_1(t)v_1(t). \end{aligned} \quad (24)$$

Define the covariances $P_{12}(t) \triangleq \mathbb{E}\{\tilde{x}_1(t)\tilde{x}_2^{\mathrm{T}}(t)\}$, $P_{21}(t) \triangleq \mathbb{E}\{\tilde{x}_2(t)\tilde{x}_1^{\mathrm{T}}(t)\}$, and $P_2(t) \triangleq \mathbb{E}\{\tilde{x}_2(t)\tilde{x}_2^{\mathrm{T}}(t)\}$. The estimator gain $K_1(t)$ in the linear minimum variance sense can be calculated by the following form:

$$\begin{cases} P_{12}(t) =& (I - K_1(t)C_1)A_1P_{12}(t-1) \\ & \times ((I - K_2(t)C_2)A_{2,J}(t-1))^{\mathrm{T}} \\ & + (I - K_1(t)C_1)A_{12,J}(t)P_2(t-1) \\ & \times ((I - K_2(t)C_2)A_{2,J}(t-1))^{\mathrm{T}} \\ P_{21}(t) =& (I - K_2(t)C_2)A_{2,J}(t-1)P_{21}(t-1) \\ & \times ((I - K_1(t)C_1)A_1^{\mathrm{T}} \\ & + (I - K_2(t)C_2)A_{2,J}(t-1)P_2(t-1) \\ & \times ((I - K_1(t)C_1)A_{12,J}(t-1))^{\mathrm{T}} \\ P_1^-(t) =& A_1P_1(t-1)A_1^{\mathrm{T}}(t-1) \\ & + A_1P_{12}(t-1)A_{12,J}^{\mathrm{T}}(t-1) \\ & + A_{12,J}(t-1)P_{21}(t-1)A_1^{\mathrm{T}} \\ & + A_{12,J}(t-1)P_2(t-1)A_{12,J}^{\mathrm{T}}(t-1) + Q_{w_1} \\ P_1(t) =& (I - K_1(t)C_1)P_1^-(t) \\ K_1(t) =& P_1^-(t)C_1^{\mathrm{T}}\left(C_1P_1^-(t)C_1^{\mathrm{T}} + Q_{v_1}\right)^{-1}. \end{cases} \quad (25)$$

C. Paillier Homomorphic Encryption

The homomorphic cryptosystem is a kind of system that allows computation on encrypted data [20]. This means that the operations on ciphertext can be reflected on the original plaintext. Since UAV requires fast response, we consider the partially homomorphic encryption that consumes less computational resources when compared with fully and hybrid homomorphic encryption methods. Hence, a classical kind of partially homomorphic encryption called Paillier homomorphic encryption [25] is applied to preserve privacy for UAS. Meanwhile, we assume that the UAS has enough computation ability to implement such an encryption approach. The complete procedures related to Paillier homomorphic encryption are summarized as follows.

1) *Key Generation*: Given two primes p and q. Let $N = pq$ and the least common multiple (LCM) is $\lambda = \mathrm{lcm}(p-1, q-$

1). g satisfies $\gcd(L(g^{\lambda} \mod N^2), N) = 1$, where $L(x) = (x-1)/N$ and gcd stand for the greatest common divisor (GCD). Then, the secret keys are generated as follows:

$$\mathrm{pk} = (N, g), \mathrm{sk} = \lambda, \tag{26}$$

where pk denotes the public key and sk denotes the private key.

2) *Quantization and Mapping*: In fact, the most common type of data in UAS is float or double, but not all types of numbers can be treated as the input of the Paillier cryptosystem. The data to be encrypted should lie in the plaintext space $\mathcal{M} = \mathbb{Z}_N$. Hence, these original data should be quantized and mapped into positive integers. The general form of quantization is denoted as

$$x_q = Q(x), \tag{27}$$

and the mapping procedure is given by [31]:

$$x_m = M(x_q) = \begin{cases} x_q, & \text{if } x_q \geq 0 \\ x_q + N, & \text{if } x_q < 0 \end{cases}. \tag{28}$$

In the rest of this paper, $Q(\cdot)$ denotes the quantization function and $M(\cdot)$ denotes the mapping function The variable with subscript "q" represents the quantized data and that with "m" represents the mapped data.

3) *Encryption*: In this step, the raw message m will be encrypted into the ciphertext c with public key pk. The notation $[[\cdot]]$ represents the encrypted message and $c \triangleq [[m]]$. Then, the detailed encryption process is expressed by

$$c = \mathrm{Enc}(m, \mathrm{pk}) = g^m r^N \mod N^2, \tag{29}$$

where $\mathrm{Enc}(\cdot)$ is the encryption function and $r \in \mathbb{Z}_N$ is a non-zero random integer.

4) *Decryption*: When legitimate users receive the encrypted signals, they can successfully decrypt them. This means that the ciphertext c will be decrypted into the original message m based on the private key sk, and the concrete decryption process is given by

$$m = \mathrm{Dec}(c, \mathrm{sk}) = \frac{L(c^{\lambda} \mod N^2)}{L(g^{\lambda} \mod N^2)} \mod N. \tag{30}$$

where $\mathrm{Dec}(\cdot)$ is the decryption function.

5) *Retrieval*: After decryption, the obtained result becomes $x_m = x_{m_1} + x_{m_2}$ or $x_m = x_{m_1} \times x_{m_2}$, which is the value after mapping. Thus, the quantized result $x_q = x_{q_1} + x_{q_2}$ or $x_q = x_{q_1} \times x_{q_2}$ should be retrieved by the following criterion [29]:

$$x_q = R(x_m) \begin{cases} x_m \mod N, \\ \text{if } x_m \mod N \leq \dfrac{N}{2} \\ x_m \mod N - N, \\ \text{if } \dfrac{N}{2} \leq x_m \mod N < N \end{cases}. \tag{31}$$

Based on the above procedures, the Paillier cryptosystem can provide two fundamental homomorphisms for scalars: addition and constant multiplication. The two operations are respectively denoted by "$\oplus$" and "$\otimes$", and the detailed expressions are given as follows.

1) *Addition*: The addition of two encrypted values satisfies

$$\mathrm{Dec}(\mathrm{Enc}(m_1, \mathrm{pk}) \oplus \mathrm{Enc}(m_2, \mathrm{pk}), \mathrm{sk}) = m_1 + m_2. \tag{32}$$

2) *Constant Multiplication*: The multiplication of a constant c in plaintext and an encrypted value satisfies

$$\mathrm{Dec}(c \otimes \mathrm{Enc}(m_1, \mathrm{pk}), \mathrm{sk}) = cm_1. \tag{33}$$

D. Quantized Estimator

As mentioned before, the quantization strategy is required in the cryptosystem. The following uniform quantizer $Q : \mathbb{R} \to \mathbb{Z}$ is considered [42]:

$$Q(x) = \bar{x} + \mathrm{sgn}(x - \bar{x}) \cdot \delta \cdot \lfloor \frac{|x - \bar{x}|}{\delta} + \frac{1}{2} \rfloor. \tag{34}$$

Here, x denotes the input while $\bar{x}$ denotes the mid-value of the corresponding interval. The parameter $\delta = \frac{l}{2}$ is the sensitivity, i.e., the maximum error, where l is the length of each quantization interval. $\mathrm{sgn}\{\cdot\}$ is the sign function that means $\mathrm{sgn}(x) = \begin{cases} 1, & \text{if } x > 0 \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x < 0 \end{cases}$. Furthermore, the quantization function can be rewritten by

$$Q(x) = x + \Delta, \tag{35}$$

where Δ is the quantization error satisfying $\Delta \leq \delta$. Nevertheless, it is a function related to a scalar, and the quantization $Q : \mathbb{R}^{m \times n} \to \mathbb{Z}^{m \times n}$ on matrix $A \in \mathbb{R}^{m \times n}$ is denoted by $Q(A) \triangleq \begin{bmatrix} Q([A]_{11})\} & \cdots & Q([A]_{1n})\} \\ \vdots & \ddots & \vdots \\ Q([A]_{m1})\} & \cdots & Q([A]_{mn})\} \end{bmatrix}$.

Generally, attitude sensors are deployed in the body of the UAV such that they can observe the rotational state. Such communication is difficult to be overheard by eavesdroppers because it is always proprietary and wired. On the other hand, the base stations are deployed in a fixed position on the ground. Therefore, only the privacy of translational estimator $\hat{x}_1(t)$ should be protected. This is also a reason why we divide the global system into two subsystems since the encryption cost will be halved.

Now, the measurements and estimates in the translational subsystem should be quantized for encryption. Although the system parameters do not require privacy preservation, they should also be quantized and mapped into the plaintext space due to the criterion about constant multiplication (33). It should be pointed out that the accuracy of sensed and estimated data cannot be directly improved by modifying the sensitivity of the quantizer. If the sensitivity decreases, the outputs of the quantizer may not be integers, which is disadvantageous for encryption. To solve this problem, the accuracy is adjusted by introducing a scaling factor L_q in this paper, and the final quantized output can be described as follows:

$$\begin{cases} \hat{x}^-_{1,q}(t) \triangleq Q(\hat{x}^-_1(t)) = (\hat{x}^-_1(t) + \Delta_x(t))/L_q \\ y_{1,q}(t) \triangleq Q(y_1(t)) = (y_1(t) + \Delta_y(t))/L_q \\ K_{C,q}(t) \triangleq Q(K_{1,C}(t)) = (K_{1,C}(t) + \Delta_C(t))/L_q \\ K_{1,q}(t) \triangleq Q(K_1(t)) = (K_1(t) + \Delta_K(t))/L_q \end{cases}. \tag{36}$$

where $K_{1,C}(t) = I - K_1(t)C_1$. Then, the quantized estimator is proposed in the following form:

$$\hat{x}_{1,q}(t) = L_q^2 K_{C,q}(t) \hat{x}^-_{1,q}(t) + L_q^2 K_{1,q}(t) y_{1,q}(t). \tag{37}$$

Similar to the analysis in [29], [38], the estimation error under quantization is bounded, because the quantization error is bounded, i.e., $\Delta_x(t), \Delta_y(t), \Delta_C(t), \Delta_K(t) \leq \delta$.

Remark 3.1: The probabilistic quantization has been utilized in [29], which randomly selects the output from two boundaries of certain intervals. In this paper, the output is fixed when the input lies in a certain interval in the proposed

quantizer (34). The differences are summarized as follows. 1) Due to the extra randomness, the error of the probabilistic quantizer is larger. Particularly, its error upper bound is twice that of the fixed quantizer. 2) The computation amount of the probabilistic quantizer is also larger because it is time-varying and requires random values at each time. Note that such computation reduction can be negligible in this paper because most computation is used for encryption, but it may work for other applications.

E. Complete Protocol

Based on the above analysis, the complete protocol is summarized in this subsection. The notations "$\oplus$" and "$\otimes$" are omitted for brevity. Firstly, we shall initialize the whole UAS. The initial values of estimation systems, such as system transition parameters, state estimates, and covariances, should be synchronized for all parties, including the user, UAV, and sensor. Meanwhile, another important procedure is generating secret keys for the user as (26), including a private key and a public key. Then, the user distributes public key pk and corresponding system information to the UAV and the sensor.

After initialization, all the parties will work in real-time. Except for the original control input $u(t)$, the user will send encrypted prediction $[[\hat{x}_{1,m}^{-}(t)]]$ to the UAV, which has been processed with quantization, mapping, and encryption:

$$[[\hat{x}_{1,m}^{-}(t)]] = \mathrm{Enc}(M(Q(\hat{x}_1^{-}(t))), \mathrm{pk}). \tag{38}$$

On the other hand, the sensor sends the encrypted measurements $[[y_{1,m}(t)]]$ to the UAV, that is

$$[[y_{1,m}(t)]] = \mathrm{Enc}(M(Q(y_1(t))), \mathrm{pk}). \tag{39}$$

After gathering these data in UAV, the real-time encrypted estimate $[[\hat{x}_{1,m}(t)]]$ will be computed by

$$\begin{aligned}[[\hat{x}_{1,m}(t)]] =& L_q^2 K_{C,q}(t)[[\hat{x}_{1,m}^{-}(t)]] \\ &+ L_q^2 K_{1,q}(t)[[y_{1,m}(t)]]\end{aligned}. \tag{40}$$

Then, the above encrypted estimate will be directly sent to the user. Besides, the UAV will control the motors with the control signal $u(t)$ as (9). Eventually, after receiving the encrypted signal, the user will apply private key sk for decryption. More concretely, by resorting to the decryption process (30) and retrieval function (31), the final estimate for the user is given as follows, which is equivalent to the quantized result:

$$\hat{x}_{1,q}(t) = R(\mathrm{Dec}([[\hat{x}_{1,m}(t)]]), \mathrm{sk}). \tag{41}$$

The procedures of the proposed protocol mentioned above is summarized in Protocol 1, and a flowchart is given in Fig. 3 to show it more clearly. Before analyzing the security of this protocol, we first give the following definitions.

Definition 3.1 (Negligible Function [13]): A function $\epsilon(x)$ is said to be negligible if for every positive polynomial $p(x)$, there exists $\epsilon(x) < 1/p(x)$, $\exists X \in \mathbb{N}$, $\forall x > X$.

Definition 3.2 (Semantic Security [13]): Given arbitrary two messages m_1 and m_2 and randomly encrypt $m_i (i = 1, 2)$ into $[[m_i]]$. A cryptosystem is semantically secure when the result of any probabilistic polynomial-time (PPT) algorithm $i' = D([[m_i]])$ is negligible, i.e., $\mathbb{P}(i = i') < \epsilon(t)$.

Then, the security of the proposed protocol is analyzed as follows. Notice that the strongest eavesdropper can simultaneously wiretap both the user-UAV channel and the sensor-UAV channel as stated in Definition 2.1. Therefore, the parameters acquired by the eavesdropper consist of the encrypted measurements $[[y_{1,m}(t)]]$, encrypted predictions $[[\hat{x}_{1,m}^{-}(t)]]$, encrypted estimates $[[\hat{x}_{1,m}(t)]]$, control input $u(t)$, and rotational estimate $\hat{x}_2(t)$. Since the Paillier cryptosystem satisfies the semantic security, the eavesdropper that launches CPA cannot directly speculate the decrypted values. Moreover, based on the control input $u(t)$ and rotational estimate $\hat{x}_2(t)$, the translational estimate can also not be calculated with an estimator due to the lack of process and measurement noises.

Protocol 1 Secure estimation protocol using Paillier homomorphic encryption for UAS

Initialization

1. Set initial system values, generate public key pk and private key sk as (26).
2. Distribute the public key and corresponding initial values to the sensor and UAV.

User

1. Calculate prediction $\hat{x}_{1,q}^{-}(t)$ by (17);
2. Encrypt prediction into $[[\hat{x}_{1,m}^{-}(t)]]$ by (38);
3. Send control input $u(t)$ and encrypted prediction $[[\hat{x}_{1,m}^{-}(t)]]$ to UAV.

Sensor

1. Encrypt measurement $y_1(t)$ into $[[y_{1,m}(t)]]$ by (39);
2. Send encrypted measurement $[[y_{1,m}(t)]]$ to UAV.

UAV

1. Calculate estimate $\hat{x}_2(t)$ by (17);
2. Calculate encrypted estimate $[[\hat{x}_{1,m}(t)]]$ by (40);
3. Send estimate $\hat{x}_2(t)$ and encrypted estimate $[[\hat{x}_{1,m}(t)]]$ to user;
4. Control rotors by (9) based on received $u(t)$.

User

1. Decrypt and retrieve $[[\hat{x}_{1,m}(t)]]$ into $\hat{x}_{1,q}(t)$ by (41).

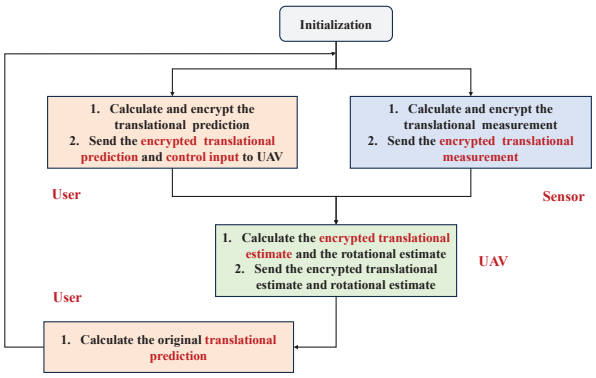

Fig. 3. The flowchart of the proposed secure protocol.

IV. Simulation Examples

The performances of the proposed methods are studied via computer simulations. The end-user controls the UAV to deliver some important objects at a certain secret position. At the start, the initial states of UAS are all set as 0, which means the UAV is stationary on the ground and its initial position is the origin of the axes. Next, the interval length of the uniform quantizer is set as $l = 1$ which is able to

TABLE II
ESTIMATES AND THEIR ENCRYPTED RESULTS AT CERTAIN TIME SLOTS.

time slot	10	50
real position	(2.37,0.06,59.64)	(16.05,3.32,177.49)
quantized measurement	(220,-13,5978)	(1594,346,17739)
encrypted measurement	(8.88698144e+17,1.87115528e+18,4.36727027e+17)	(2.64780208e+18,3.52588274e+18,8.18185766e+17)
encrypted estimate	(4.91360600e+18,4.87347306e+18,2.08898016e+18)	(4.82550160e+18,3.76336150e+18,2.28017677e+17)
decrypted estimate	(2.40,0.10,59.66)	(16.08,3.34,177.55)

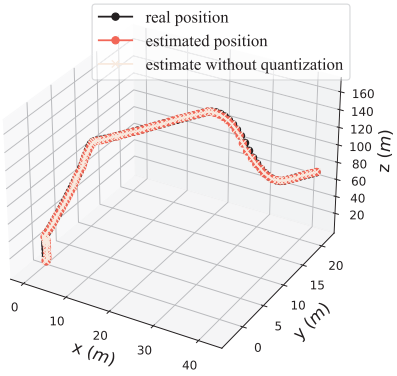

Fig. 4. The real and estimated 3D trajectories of the UAV.

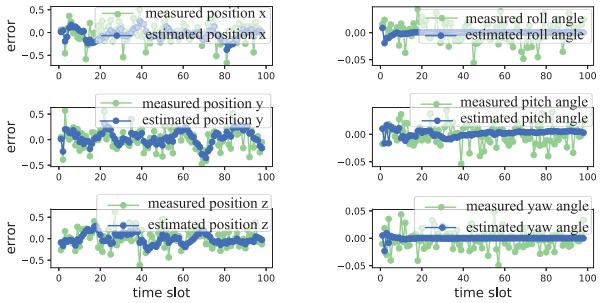

Fig. 5. The comparison of errors between the measurements and estimates.

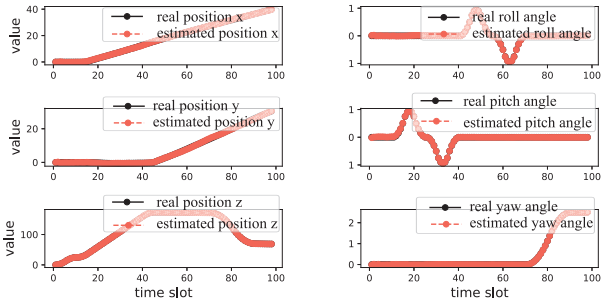

Fig. 6. The trajectories of 3D position, attitude, and their estimates.

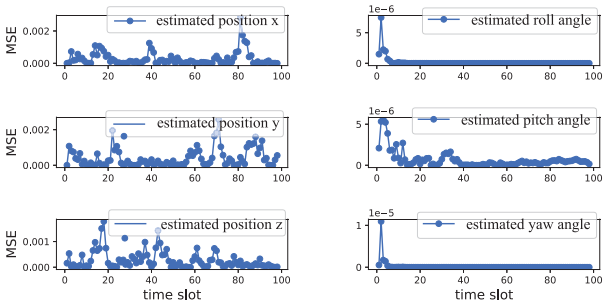

Fig. 7. The MSEs of every component of the estimates.

transfer the float into an integer. The scaling factor is set as $L_q = 0.01$, which reserves two decimal fractions.

We commend the UAV for a period of 100 seconds, and the real and estimated 3D trajectories of the UAV are plotted in Fig. 4 to show the real-time tracking performance. It can be intuitively seen from this figure that the proposed distributed estimator can track the target well. Then, the comparison of errors between measurements and estimates is shown in Fig. 5. We can see that the estimation error is less than the measurement error, which demonstrates the advantage of the proposed estimator on track. To more concretely show the procedures, measurements, estimates, and their encrypted results at certain time slots are given in Table. II. Obviously, the encrypted results are strings of numbers with no meaning, and the eavesdroppers cannot infer valid information from them without the private key.

Moreover, the trajectories of 3D position, attitude, and their estimates are presented in Fig. 6. It is directly seen from this figure that all the sub-states are tracked well. Notice that the estimation error in one test is not convincing enough. In order to assess the estimation performance more accurately, we consider the mean square error (MSE) for quantitive analysis. Here, the theoretical MSE is approximated by applying the Monte Carlo method with 100 interdependent runs. The MSEs of every component of the estimates are given in Fig. 7. All the errors in this figure are bounded, which demonstrates the boundedness of certain components.

Furthermore, the overall MSEs of translational and rotational estimates are displayed in Fig. 8 to show the global stability of the proposed estimator. By introducing the scaling factor, we can achieve almost the same accuracy as the optimal estimator without quantization. Moreover, we also compare the proposed performance with the differentially private mechanism. To achieve differential privacy (DP), the noises with covariance $Q_a = \text{diag}\{1.00, 1.00, 1.00\}$ are inserted into the translational measurements, while the value of covariance is determined by the privacy parameters. Obviously, the MSE with DP is larger than that with homomorphic encryption, which demonstrates the proposed estimator can preserve more data utility. Also, the comparison of time costs is shown in Fig. 9. As plotted in this figure, the proposed distributed protocol costs less running time when compared with centralized protocol, because the encryption and ciphertexts-based operations are simplified. Specifically, the time cost of the centralized method is about twice as much as that of the proposed distributed method.

V. CONCLUSION & DISCUSSION

This paper studies the confidentiality problem for UAS and the homomorphic encryption approach is considered to protect the privacy of the UAV's location against eavesdroppers. First, the globally high-dimensional system is separated into the translational subsystem and the rotational subsystem, and each subsystem is estimated by its own estimator in the

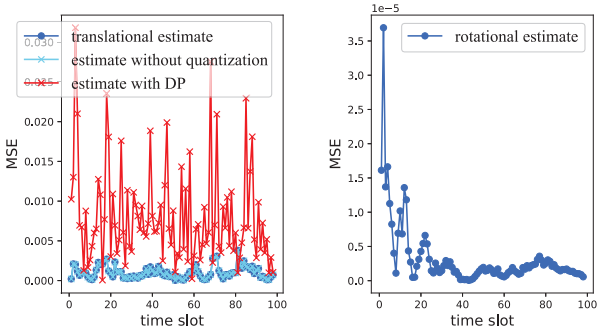

Fig. 8. The overall MSEs of translational and rotational estimates.

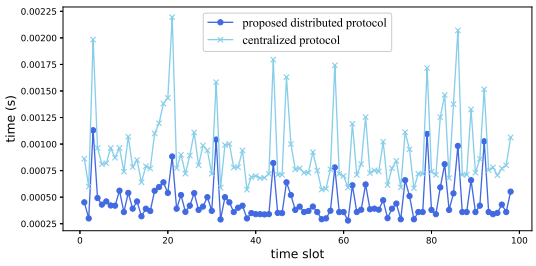

Fig. 9. The comparison of time costs.

minimum variance sense. Then, a secure estimation protocol with Paillier homomorphic encryption is proposed to preserve the privacy of translational states. Under such protocol, the eavesdropper cannot infer the location of the UAV due to the encryption of measurements and estimates, while the user can obtain the desired data based on homomorphisms and the private key. Meanwhile, the uniform quantization method with fixed sensitivity is applied to change the type of transmitted data from the float into integers. Compared with centralized estimation and full homomorphism, the computation amount of the proposed protocol is greatly reduced thanks to the design of the distributed structure and partial encryption.

It is important to acknowledge that there are inherent trade-offs among various system performance metrics, including the demand for privacy, the volume of computation, and the accuracy of estimation. These factors often counterbalance each other, necessitating careful consideration and strategic decision-making. The homomorphic encryption adopted in this paper provides a higher privacy guarantee, while this comes at the cost of a significantly higher computational load. Although the distribued structure is proposed to mitigate such adverse impact, the calculation is still large data perturbation approaches, which only requires simple randomness. Therefore, the selection of an appropriate method should be guided by practical requirements and the specific context of the situation.

REFERENCES

[1] P. Chen, X. Luo, D. Guo, Y. Sun, J. Xie, Y. Zhao, and R. Zhou, "Secure task offloading for MEC-aided-UAV system," *IEEE Transactions on Intelligent Vehicles,* vol. 8, no. 5, pp. 3444-3457, 2023.

[2] M. Eskandari, H. Huang, A. V. Savkin, and W. Ni, "Model predictive control-based 3D navigation of a RIS-equipped UAV for LoS wireless communication with a ground intelligent vehicle," *IEEE Transactions on Intelligent Vehicles,* vol. 8, no. 3, pp. 2371-2384, 2023.

[3] A. Bansal, N. Agrawal, and K. Singh, "Rate-splitting multiple access for UAV-based RIS-enabled interference-limited vehicular communication system," *IEEE Transactions on Intelligent Vehicles,* vol. 8, no. 1, pp. 936-948, 2023.

[4] D. Yin, X. Yang, H. Yu, S. Chen, and C. Wang, "An air-to-ground relay communication planning method for UAVs swarm applications," *IEEE Transactions on Intelligent Vehicles,* vol. 8, no. 4, pp. 2983-2997, 2023.

[5] W. Youn, H. Choi, A. Cho, S. Kim, and M. B. Rhudy, "Accelerometer fault-tolerant model-aided state estimation for high-altitude long-endurance UAV," *IEEE Transactions on Instrumentation and Measurement,* vol. 69, no. 10, pp. 8539-8553, 2020.

[6] W. Xu, S. Bao, and Z. Liu, "The state estimation of UAV based on UKF," *2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA),* Ottawa, ON, Canada, 2014, pp. 402-405.

[7] S. Teng, X. Hu, P. Deng, B. Li, Y. Li, Y. Ai, D. Yang, L. Li, X. Zhe, F. Zhu, and L. Chen, "Motion planning for autonomous driving: The state of the art and future perspectives," *IEEE Transactions on Intelligent Vehicles,* vol. 8, no. 6, pp. 3692-3711, 2023.

[8] A. S. Abdalla and V. Marojevic, "Securing mobile multiuser transmissions with UAVs in the presence of multiple eavesdroppers," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 10, pp. 11011-11016, 2021.

[9] B. Pardhasaradhi and L. R. Cenkeramaddi, "GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion," *IEEE Sensors Journal,* vol. 22, no. 11, pp. 11122-11134, 2022.

[10] Z. Hu and X. Jin, "Formation control for an UAV team With environment-aware dynamic constraints," *IEEE Transactions on Intelligent Vehicles,* 2023, doi: 10.1109/TIV.2023.3295354.

[11] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," *Proc. 3rd Theory Cryptogr. Conf.,* 2006, pp. 265–284.

[12] X. Yan, Y. Zhang, D. Xu, and B. Chen, "Distributed confidentiality fusion estimation against eavesdroppers," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 58, no. 4, pp. 3633-3642, 2022.

[13] O. Goldreich, *Foundations of cryptography: volume 1, basic tools.* Cambridge, U.K.: Cambridge University Press, 2003.

[14] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper," *IEEE Transactions on Automatic Control,* vol. 64, no. 9, pp. 3732-3739, 2019.

[15] Z. Zeng, Q. Zhou, K. Wei, N. Yang, and C. Tang, "BCS-CPP: A blockchain and collaborative service-based conditional privacy-preserving scheme for Internet of vehicles," *IEEE Transactions on Intelligent Vehicles,* 2023, doi: 10.1109/TIV.2023.3327364.

[16] C. Pu, A. Wall, K. -K. R. Choo, I. Ahmed, and S. Lim, "A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of drones environment," *IEEE Internet of Things Journal,* vol. 9, no. 12, pp. 9918-9933, June 15, 2022.

[17] J. K. White, J. Antoszewski, J. Piotrowski, C. A. Musca, J. M. Dell, and L. Faraone, "An inexpensive midwave infrared HgCdTe camera," *COMMAD 2000 Proceedings. Conference on Optoelectronic and Microelectronic Materials and Devices,* Bundoora, VIC, Australia, 2000, pp. 173-176.

[18] X. Yan, B. Chen, Y. Zhang, and L. Yu, "Guaranteeing differential privacy in distributed fusion estimation," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 59, no. 3, pp. 3416-3423, 2023.

[19] X. Yan, B. Chen, Y. Zhang, and L. Yu, "Distributed encryption fusion estimation against full eavesdropping," *Automatica,* vol. 153, 111025, 2023.

[20] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation,* vol. 4, no. 1, pp. 169-180, 1978.

[21] M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Control Systems Magazine,* vol. 41, no. 3, pp. 58-78, 2021.

[22] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni and F. Karray, "Secure federated learning with fully homomorphic encryption for IoT communications," *IEEE Internet of Things Journal,* doi: 10.1109/JIOT.2023.3302065, 2023.

[23] A. Sultan, S. Tahir, H. Tahir, T. Anwer, F. Khan, M. Rajarajan, and Omer Rana, "A novel image-based homomorphic approach for preserving the privacy of autonomous vehicles connected to the cloud," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 2, pp. 1936-1948, 2023.

[24] C. Gentry, *A Fully Homomorphic Encryption Scheme,* vol. 20. Stanford, CA, USA: Stanford Univ., 2009.

[25] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques,* 1999, pp.223-238.

[26] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, no.2, 120–126, 1978.

[27] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory,* vol. 31, no. 4, pp. 469-472, 1985.
[28] A. A. M. A. Abdelhafez, *Localization of cyber-physical systems: Privacy, security and efficiency,* Technische Universität München, München, 2020.
[29] Z. Zhang, P. Cheng, J. Wu, and J. Chen, "Secure state estimation using hybrid homomorphic encryption scheme," *IEEE Transactions on Control Systems Technology,* vol. 29, no. 4, pp. 1704-1720, 2021.
[30] Y. Ni, J. Wu, L. Li, and L. Shi, "Multi-party dynamic state estimation that preserves data and model privacy," *IEEE Transactions on Information Forensics and Security,* vol. 16, pp. 2288-2299, 2021.
[31] M. T. I. Ziad, A. Alanwar, M. Alzantot, and M. Srivastava, "CryptoImg: Privacy preserving processing over encrypted images" *2016 IEEE Conference on Communications and Network Security (CNS),* Philadelphia, PA, USA, 2016, pp. 570-575.
[32] S. Emad, A. Alanwar, Y. Alkabani, M. W. El–Kharashi, H. Sandberg, and K. H. Johansson, "Privacy guarantees for cloud-based state estimation using partially homomorphic encryption," *2022 European Control Conference (ECC),* London, United Kingdom, 2022, pp. 98-105.
[33] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control,* vol. 59, no. 2, pp. 341-354, 2014.
[34] S. Cho, N. H. McClamroch, and M. Reyhanoglu, "Dynamics of multibody vehicles and their formulation as nonlinear control systems," *Proceedings of the 2000 American Control Conference,* Chicago, IL, USA, 2000, pp. 3908-3912.
[35] A. Benaddy, M. Bouzi, and M. Labbadi, "Comparison of the different control strategies for quadrotor unmanned aerial vehicle," *2020 International Conference on Intelligent Systems and Computer Vision (ISCV),* Fez, Morocco, 2020, pp. 1-6.
[36] X. Yu, X. Zhou, K. Guo, J. Jia, L. Guo, and Y. Zhang, "Safety flight control for a quadrotor UAV using differential flatness and dual-loop observers," *IEEE Transactions on Industrial Electronics,* vol. 69, no. 12, pp. 13326-13336, 2022.
[37] K. Guo, J. Jia, X. Yu, L. Guo, and L. Xie, "Multiple observers based anti-disturbance control for a quadrotor UAV against payload and wind disturbances," *Control Engineering Practice,* vol. 102, 104560, 2020.
[38] D. Ding, Z. Wang, D. W.C. Ho, and G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica,* vol. 78, pp. 231-240, 2017.
[39] X. Yan, B. Chen, and Z. Hu, "Distributed estimation for interconnected dynamic systems under binary sensors," *IEEE Sensors Journal,* vol. 22, no. 13, pp. 13153-13161, 2022.
[40] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal of Basic Engineering,* vol. 82, pp. 35-45, 1960.
[41] K. Reif, S. Gunther, E. Yaz, and R. Unbehauen, "Stochastic stability of the discrete-time extended Kalman filter," *IEEE Transactions on Automatic Control,* vol. 44, no. 4, pp. 714–728, 1999.
[42] Y. Pu, M. N. Zeilinger, and C. N. Jones, "Quantization design for distributed optimization," *IEEE Transactions on Automatic Control,* vol.62, no.5, pp.2107-2120, 2017.
[43] S. Goldwasser and S. Micali, "Probabilistic encryption." *Journal of Computer and System Sciences,* vol. 28, no. 2, pp. 270-299, 1984.

Xinhao Yan received the B.E. degree in communication engineering and the M.E. degree in control science and engineering from Zhejiang University of Technology, Hangzhou, China, in 2020 and 2023, respectively. He is currently pursuing the Ph.D. degree at the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong, China. He was a Visiting Scholar in the Department of Electronic and Information Engineering with The Hong Kong Polytechnic University, Hong Kong, China, in 2022, and he was also a Research Technical Assistant in the Department of Aeronautical and Aviation Engineering with The Hong Kong Polytechnic University, Hong Kong, China, in 2023. He was a recipient of the Outstanding Thesis Award of Chinese Association of Automation in 2023. His current research interests include distributed estimation, information fusion, machine learning, networked systems, intelligent vehicles, and security and privacy.

Guanzhong Zhou received the B.Eng. degree from the Harbin Institute of Technology, Weihai, China, in 2019. He is currently pursuing the master's degree with the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong. His research interests include quadruped robots, mobile robots (UGV and UAV), and swarm robotics.

Yue Huang received the Ph.D. degree in Electrical and Computer Engineering from the University of British Columbia, Vancouver, BC, Canada, in 2023. She is now a postdoc fellow in Data61, Commonwealth Scientific and Industrial Research Organisation, Melbourne, Australia. Her research interests span many areas of usable security and privacy, including mobile and IoT security, security and privacy in online social networks, and web security. Her work has appeared in a diverse set of top-tier venues on security and human–computer interaction, including ACM CHI, IEEE S&P, USENIX Security, CSCW, and SOUPS.

Wei Meng received the B.E. and M.E. degrees from Northeastern University, Shenyang, China, in 2006 and 2008, respectively, and the Ph.D. degree in control and instrumentation from the Nanyang Technological University, Singapore, in 2013. From 2012 to 2017, he was a Research Scientist in UAV Research Group, Temasek Laboratories, National University of Singapore. He is now with School of Automation, Guangdong University of Technology as a Professor. His current research interests include unmanned systems, multi-robot systems, digital twins.

Anh-Tu Nguyen received the degree in engineering and the M.Sc. degree in automatic control from the Grenoble Institute of Technology, Grenoble, France, in 2009, and the Ph.D. degree in automatic control from the University of Valenciennes, Valenciennes, France, in 2013. He is currently an Associate Professor with INSA Hauts-de-France, Université Polytechnique Hautsde-France, Valenciennes. His research interests include robust control and estimation, cybernetics control systems and human–machine shared control with a strong emphasis on mechatronics applications.

Hailong Huang received his Ph.D degree in Systems and Control from the University of New South Wales, Sydney, Australia, in 2018. He is now an Assistant Professor at the Department of Aeronautical and Aviation Engineering, the Hong Kong Polytechnic University, Hong Kong. His current research interests include guidance, navigation, and control of UAVs and mobile robots. He is an Associate Editor of IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Vehicles, Intelligent Service Robotics, and International Journal of Advanced Robotic Systems, an editorial board member of the International Journal of Dynamics and Control, a guest editor of IEEE Transactions on Automation Science and Engineering, a technical program committee member of IEEE International Conference on Unmanned Systems, and a technical committee member of IEEE Conference on Automation Science and Engineering.