Security and Safety, Vol. 2, 2023018 (2023)
https://doi.org/10.1051/sands/2023018
sands.edpsciences.org

Security and Safety in Unmanned Systems

Research Article

Open Access

Information Network

Secure motion control of micro-spacecraft using semi-homomorphic encryption

Yongxia Shi[1], Ehsan Nekouei[1], and Qinglei Hu[2*]

[1] *Department of Electrical Engineering, City University of Hong Kong, Hong Kong 999077, China*
[2] *School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China*

Received: 28 February 2023 / Revised: 25 April 2023 / Accepted: 28 June 2023 / Published online: 23 August 2023

Abstract This paper studies the secure motion control problem for micro-spacecraft systems. A novel semi-homomorphic encrypted control framework, consisting of a logarithmic quantizer, two uniform quantizers, and an encrypted control law based on the Paillier cryptosystem is developed. More specifically, a logarithmic quantizer is adopted as a digitizer to convert the continuous relative motion information to digital signals. Two uniform quantizers with different quantization sensitivities are designed to encode the control gain matrix and digitized motion information to integer values. Then, we develop an encrypted state-feedback control law based on the Paillier cryptosystem, which allows the controller to compute the control input using only encrypted data. Using the Lyapunov stability theory and the homomorphic property of the Paillier cryptosystem, we prove that all signals in the closed-loop system are uniformly ultimately bounded. Different from the traditional motion control laws of spacecraft, the proposed encrypted control framework ensures the security of the exchanged data over the communication network of the spacecraft, even when communication channels are eavesdropped by malicious adversaries. Finally, we verify the effectiveness of the proposed encrypted control framework using numerical simulations.

Keywords Spacecraft relative motion, security protection, encrypted control, homomorphic encryption, quantization

Citation Shi Y, Nekouei E and Hu Q. Secure motion control of micro-spacecraft using semi-homomorphic encryption. Security and Safety 2023; **2**: 2023018. https://doi.org/10.1051/sands/2023018

1 Introduction

Relative motion control of spacecraft is an enabling technology for many current and near-future space missions, such as orbital rendezvous, on-orbit assembly, formation flying, and reconnaissance and surveillance, which has received widespread attention in recent years [1–3]. These space missions usually involve an active spacecraft (chaser) and a passive spacecraft (target), and require the chaser to perform orbital maneuvers to track the specified position of the target or a virtual desired position. As the recent trend of space missions moves from human intervention towards autonomous operation, it is necessary to improve the autonomy, safety, and security of spacecraft control systems. In recent years, the autonomous relative motion control of spacecraft has received considerable attention from both academia and aerospace industrial sectors. Numerous control methods have been proposed in the literature, such as adaptive control [2], sliding mode control [3, 4], model predictive control [5], and distributed control [6].

With the prosperity of fast-integrated technology, light-weight spacecraft exhibit enormous popularity, such as CubSats [7] and plug-and-play satellite [8]. Compared with the traditional monolithic and complex

* Corresponding author (email: huql_buaa@buaa.edu.cn)

spacecraft, these miniature spacecraft become more popular in large-scale space missions, since they possess greater flexibility, higher reliability, and less cost [9–11]. It is noted, however, that the information exchange inside these light-scale micro-satellites (*e.g.*, data transmission from the sensor to the controller or from the controller to the actuator) usually hinges on the wireless communication network. In this case, two inescapable problems thereupon arise: signal quantization and data security. Since only digital signals are allowed to exchange through the wireless communication network, the continuous system states or control commands need to be encoded into digitized signals before transmission. Moreover, due to the limited communication resources, it is also desirable to avoid continuous information exchange. With this in mind, the spacecraft attitude control problem with input quantization was addressed in [12] using a logarithmic quantizer, where a quantization rule is provided for the feedback controller to reduce the information transmission over the communication channel. Later, Wu and Cao [12] extended the result in [13] with consideration of external disturbances. In [14], a fixed-time attitude-tracking control scheme with input quantization was designed, which adopts a hysteresis quantizer to regulate the information transmitted from the controller to the actuator. Further, the fault-tolerant control problem for flexible spacecraft attitude tracking was investigated in [15], where a logarithmic encoder-decoder scheme is developed for the control command transmitted from the controller to the actuator. On the other hand, the inter-satellite information exchange heavily relies on the wireless communication network, which makes the spacecraft vulnerable to cyber-attacks and privacy invasions, especially *via* eavesdropping. Thus, malicious adversaries or unauthorized users are able to easily extract the sensitive and valuable information of the underlying system using eavesdropping attacks. In this case, the spacecraft may suffer from more sophisticate cyber-attacks, such as replay attacks, message falsification attacks, and denial-of-service attacks (Dos) [16, 17]. Under such attacks, the control command might be falsified or manipulated, resulting in some adverse effects on the control objectives and closed-loop stability. In light of this, ensuring the control security and data privacy for the relative motion control of spacecraft is particularly important, especially when the controller is subject to cyber-physical attacks.

In general, there are two common approaches to ensure secure control in the field of networked control systems: differential privacy [18] and homomorphic encryption [19]. The core idea of differential privacy is to inject random noise into the original data, so as to weaken the impact of a single data for the whole control system. By doing so, the attacker is unable to speculate whether the data belongs to the original information and, therefore, the security, privacy, and confidentiality of the original information are well protected and hidden. However, the differential privacy methods need to take some extra measures to balance data privacy and control performance. Differently, the homomorphic encryption methods are capable of directly performing computations on encrypted data without access to the real data; moreover, the encrypted results after decryption is exactly the same as performing computations using unencrypted data. Thus, such a method not only protects the security and privacy of the information but also allows performing operations only based on encrypted data. By means of homomorphic encryption, a new concept of the encrypted controller was presented in [19] to enhance the cyber-security of the networked control system, and the RSA and ElGamal encryption schemes were employed simultaneously. Later, the stability-guaranteed problem for encrypted control systems with dynamic ElGamal cryptosystem was studied in [21], and the feasibility of the theoretical results was validated through regulation control with a positioning table testbed. Further, Ref. [22] presented a systematic design procedure of the dynamic quantizer for the encrypted state-feedback control systems with a dynamic ElGamal cryptosystem, where the additive and multiplicative biases were considered for the quantizer. Besides, by virtue of the Paillier homomorphic encryption, the secure and private control problem of networked control systems has been addressed in [23–25]. However, most existing works on secure control *via* homomorphic encryption considers discrete-time linear systems. How to pre-process the continuous system signals before encryption deserves a detailed investigation.

Based on the above-mentioned discussion, homomorphic encryption provides a promising solution for securing closed-loop control systems. However, to the best of the author's knowledge, secure motion control of micro-spacecraft systems using the homomorphic encryption method has not been studied in the literature. This is one of the main motivations for our work. To this end, we investigate the effective design of an encrypted control scheme to guarantee the security of the control loop of a micro-spacecraft in the proximity maneuvers mission. In this paper, we assume that the target spacecraft move in a circular reference orbit. The linearized relative position dynamics, *i.e.*, the well-known Clohessy–Wiltshire (CW) equations, are used to describe the relative motion between the chaser and target. A Paillier-type

encrypted control framework is proposed to protect the security and privacy of intra-system signals over the communication network whether from the sensor to controller or controller to actuator. A logarithmic quantizer and a uniform quantizer are introduced, the former of which is used to quantize the continuous system states (*i.e.*, the relative position and velocity information), while the latter is utilized to pre-process the control gain matrix and the digitized system states before encryption. Due to the homomorphic properties, the encrypted controller is constructed only using the encrypted system signals rather than the actual measurable information, which ensures a secure exchange of sensitive information among different units of the spacecraft.

This paper is organized as follows. The preliminary knowledge about the dynamical model of spacecraft relative motion, Paillier cryptosystem, and logarithmic and uniform quantizers is provided in Section 2 along with the control objective of this paper. The main results of the encrypted control frame are presented in Section 3. Numerical simulations are carried out to demonstrate the effectiveness of the proposed encrypted control scheme in Section 4. Finally, some concluding remarks are given in Section 5.

2 System model and problem formulation

In this section, some standard notations are first defined. Then, the relative motion dynamics of the chase spacecraft in the Local-Vertical-Local-Horizontal (LVLH) frame is characterized as Clohessy–Wiltshire–Hill (CWH) equation and further transformed into the form of the general linear system. Later, Paillier encryption, logarithmic and uniform quantizers are successively introduced in order to ensure the security and privacy of the system signals over the communication network. Finally, the encrypted control problem for spacecraft proximity operations is formulated.

2.1 Notations

Throughout this paper, let $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{Z}^*$ represent the sets of real numbers, integers, and non-negative integers, respectively. $\mathbb{Z}_n^* = \{z \in \mathbb{Z} : 0 \leq z < n\}$ defines the set of non-negative integers less than n. $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ are the sets of n-dimension vectors and $n \times m$-size matrices, separately. The operators $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$ stand for the greatest common divisor and the least common multiple of $a \in \mathbb{Z}^*\backslash\{0\}$ and $b \in \mathbb{Z}^*\backslash\{0\}$. Besides, given a vector $\boldsymbol{v}$ or a matrix $\boldsymbol{M}$, the correlated Euclidean norm for $\boldsymbol{v}$ or the induced 2-norm for $\boldsymbol{M}$ is indicated by $\|\boldsymbol{x}\|$ or $\|\boldsymbol{M}\|$. Furthermore, given a symmetric matrix $\boldsymbol{M} = \boldsymbol{M}^\top$, its maximum and minimum eigenvalues are denoted by $\lambda_{\max}(\boldsymbol{M})$ and $\lambda_{\min}(\boldsymbol{M})$, respectively. In addition, "mod" means modulo operation.

2.2 Dynamical model of spacecraft relative motion

Without any loss of generality, two typical reference coordinate systems, *i.e*, Earth-Centered-Inertial (ECI) and LVLH coordinate frames, are introduced first to describe the relative translation motion of the chase spacecraft with respect to the target spacecraft, as depicted in Figure 1. The ECI coordinate frame is denoted as $\mathcal{O} = \{O - XYZ\}$, where its origin locates in the Earth center, X-axis points toward the vernal equinox, Z-axis is parallel to the rotational direction of the Earth and points to the north pole, and Y-axis lies in the equatorial plane and completes the orthogonal dextral frame. Let $\mathcal{P} = \{o - xyz\}$ represent the LVLH coordinate frame, which is fixed at the target spacecraft. Moreover, the x-axis in the LVLH frame is the direction of the radius vector of the target from the Earth center, the z-axis coincides with the orbital normal direction, and the y-axis completes the orthogonal dextral frame. As shown in Figure 1, denote $\boldsymbol{\rho} = [\rho_x, \rho_y, \rho_z]^\top \in \mathbb{R}^3$ and $\boldsymbol{r}_c \in \mathbb{R}^3$ as the position vector of the chase spacecraft in the LVLH frame and the position vector of the target spacecraft in the ECI frame, respectively. Here, it is assumed that the relative distance between the chase spacecraft and the target spacecraft is far smaller than the relative distance of the target spacecraft with respect to the Earth, that is, $\|\boldsymbol{\rho}\| \ll \|\boldsymbol{r}_c\|$. Meanwhile, the target spacecraft is supposed to move in a circular orbit. Then, the linearized CWH equation can be used to describe the relative motion of the chase spacecraft in the LVLH frame [4], which is given by

$$\ddot{\rho_x} - 2\omega\dot{\rho_y} - 3\omega^2\rho_x = \frac{u_x}{m_c} \tag{1a}$$

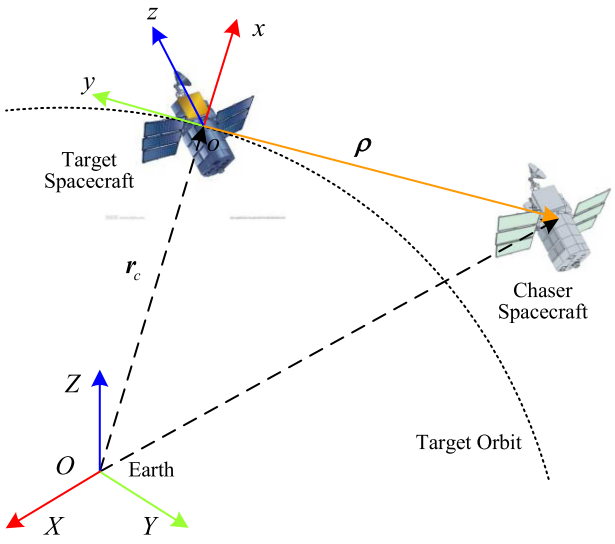


Figure 1. Relative coordinate frames

$$\ddot{\rho}_y + 2\omega\dot{\rho}_x = \frac{u_y}{m_c} \tag{1b}$$

$$\ddot{\rho}_z + \omega^2\rho_z = \frac{u_z}{m_c} \tag{1c}$$

where m_c is the mass of the chase spacecraft, $\boldsymbol{u} = [u_x, u_y, u_z]^\top \in \mathbb{R}^3$ denotes the control force acting on the chase spacecraft, $\omega = \sqrt{\mu_c/r_c^3}$ is the mean orbital angular velocity, μ_c stands for the geocentric gravitational constant of the Earth, and $r_c = \|\boldsymbol{r}_c\|$.

Further, the dynamical equation (1) can be simplified in the following form of

$$\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} \tag{2}$$

where $\boldsymbol{x} = [\rho_x, \rho_y, \rho_z, \dot{\rho}_x, \dot{\rho}_y, \dot{\rho}_z]^\top \in \mathbb{R}^6$,

$$\boldsymbol{A} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 3\omega^2 & 0 & 0 & 0 & 2\omega & 0 \\ 0 & 0 & 0 & -2\omega & 0 & 0 \\ 0 & 0 & -\omega^2 & 0 & 0 & 0 \end{bmatrix} \in \mathbb{R}^{6\times 6}, \quad \boldsymbol{B} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \frac{1}{m_c} & 0 & 0 \\ 0 & \frac{1}{m_c} & 0 \\ 0 & 0 & \frac{1}{m_c} \end{bmatrix} \in \mathbb{R}^{6\times 3} \tag{3}$$

The linear dynamical equation written by (2) will be exploited in the subsequent analysis. In particular, given the circular orbit of the target spacecraft, it is easy to certify that $(\boldsymbol{A}, \boldsymbol{B})$ is controllable. Hence, the linear continuous system (2) is stabilized by using the following state-feedback control law

$$\boldsymbol{u} = -\boldsymbol{K}\boldsymbol{x} \tag{4}$$

where $\boldsymbol{K} \in \mathbb{R}^{3\times 6}$ denotes the control gain matrix. For ensuring the stability of (2), $\boldsymbol{K}$ should be properly selected so that the eigenvalues of $(\boldsymbol{A} - \boldsymbol{B}\boldsymbol{K})$ are in the left half-plane of the complex plane. A simple method for computing K is to pose the controller design as the linear quadratic regulator (LQR) problem [1].

Lemma 1. *[26] Consider the linear system (2) with the state-feedback controller (4). If the matrix pair $(\boldsymbol{A}, \boldsymbol{B})$ is controllable, for given any positive-definite matrix $\boldsymbol{Q} = \boldsymbol{Q}^\top > 0 \in \mathbb{R}^{6\times 6}$, there always exists a symmetric positive-define matrix $\boldsymbol{P} \in \mathbb{R}^{6\times 6}$ such that*

$$(\boldsymbol{A} - \boldsymbol{B}\boldsymbol{K})^\top \boldsymbol{P} + \boldsymbol{P}(\boldsymbol{A} - \boldsymbol{B}\boldsymbol{K}) = -\boldsymbol{Q} \tag{5}$$

2.3 Paillier cyrptosystem

The Paillier cryptosystem, a typical partially HE encryption scheme, is a probabilistic asymmetric algorithm for public key cryptography [27]. The detailed realization of the Paillier encryption scheme is summarized as follows [28]:

- Key generation
  - Select two large and independent prime numbers p and q randomly and ensure $\gcd(pq,(p-1)(q-1))=1$;
  - Calculate the public key (N,g), where $N=pq$ and $g\in\mathbb{Z}_{N^2}^*$ is a random integer;
  - Calculate the private key (λ,μ), where $\lambda=\mathrm{lcm}(p-1,q-1)$ and $\mu=\lambda^{-1} \mod N$;
- Encryption
  - Let $m\in\mathbb{Z}_N^*$ be a plaintext message;
  - Choose r randomly such that $0<r<N$ and $\gcd(r,N)=1$;
  - Compute the ciphertext message of m as $c=\mathrm{E}(m)=g^m\cdot r^N \mod N^2$;
- Deccryption
  - Let c be the ciphertext message;
  - For any $x\in\mathbb{Z}_{N^2}^*$, define a function $\mathrm{L}(x)=(x-1)/N$;
  - Compute the plaintext message of c as $m=\mathrm{D}(c)=\mathrm{L}(c^\lambda \mod N^2)\mu \mod N$.

Benefiting from the additively homomorphic property and non-deterministic encryption, Paillier cryptosystem possesses the following novel features [28]:
Property 1: The sum of the plaintext messages m_1 and m_2 can be calculated by decrypting the product of their corresponding ciphertext messages $\mathrm{Enc}(m_1)$ and $\mathrm{Enc}(m_2)$, which is formulated mathematically as

$$\mathrm{D}(\mathrm{E}(m_1)\mathrm{E}(m_2)) \mod N = m_1+m_2 \mod N \tag{6}$$

Property 2: The product of the plaintext messages m_1 and m_2 can be determined by decrypting the product of a ciphertext message $\mathrm{Enc}(m_1)$ or $\mathrm{Enc}(m_2)$ raising to the power of a plaintext message m_2 or m_1, which is formulated mathematically as

$$\mathrm{D}\big(\mathrm{E}(m_1)^{m_2} \mod N^2\big) = m_1m_2 \mod N \tag{7a}$$

$$\mathrm{D}\big(\mathrm{E}(m_2)^{m_1} \mod N^2\big) = m_1m_2 \mod N \tag{7b}$$

Property 3: Consider a more general case, the product of a plaintext message m and a constant k will be computed by decrypting the product of the ciphertext message $\mathrm{Enc}(m)$ rasing to the power of k, which is formulated mathematically as

$$\mathrm{Dec}\big(\mathrm{Enc}(m)^k \mod N^2\big) = km \mod N \tag{8}$$

2.4 Quantizer

In this subsection, the logarithmic quantizer $q_l(\cdot)$ and uniform quantizer $q_u(\cdot)$ are discussed. To be specific, the logarithmic quantizer in this paper is utilized as a digitizer to scale the state information $\boldsymbol{x}$ in (2) so that $\boldsymbol{x}$ can be transformed into a digital signal capable of transmitting over the communication network. Meanwhile, since the Paillier cryptosystem is only able to encrypt the positive integers, the digital signals in the system should be mapped to the appropriate positive integers. Considering the quantization property of the uniform quantizer, it is not difficult to see that it can be decomposed into an encoder part and a decoder part to pre-process the digital signals before encryption.

(1) Logarithmic quantizer

Referring to [29], the logarithmic set of quantization levels is defined by

$$\mathbb{S}=\{\pm w_i : w_i=\rho^i w_0, i=\pm1,\pm2,\dots\}\cup\{\pm w_0\}\cup\{0\},\ w_0>0$$

where $\rho \in (0,1)$ is a positive constant representing the quantization density of the logarithmic quantizer. Then, the static and time-invariant logarithmic quantizer is described as

$$q_l(x) = \begin{cases} w_i, & \text{if } \frac{1}{1+\sigma} w_i < x \leq \frac{1}{1-\sigma} w_i \\ 0, & \text{if } x = 0 \\ -q_l(-x), & \text{if } x < 0 \end{cases} \tag{9}$$

where $\sigma = (1-\rho)/(1+\rho)$. It is noted from (9) that every element of the quantization level is closely related to the segment $(1/(1+\sigma)w_i, 1/(1-\sigma)w_i]$. In this case, the logarithmic quantizer is able to map the entire segments to the quantizer level. Since the logarithmic quantizer satisfies the sector-bound condition, the quantizer $q_l(x)$ is also written as

$$q_l(x) = (1 + \Delta_l)x \tag{10}$$

where $\Delta_l \in [-\sigma, \sigma]$. Based on (10), the quantization error associated with $q_l(x)$ is defined as $\Delta_l x = q_l(x) - x$, satisfying $|\Delta_l x| \leq \sigma |x|$. Similarly, given a vector $\boldsymbol{x} \in \mathbb{R}^n$, it has

$$q_l(\boldsymbol{x}) = (\boldsymbol{I} + \boldsymbol{\Delta}_l)\boldsymbol{x} \tag{11}$$

where $\boldsymbol{\Delta}_l = \text{diag}\{\Delta_{l1}, \ldots, \Delta_{ln}\}$ and $\boldsymbol{I}$ is an identity matrix with appropriate dimensions.

(2) Uniform quantizer

Given a positive integer q_m, the uniform quantizer is defined by [30]

$$q_u(x) = \begin{cases} q_m, & \text{if } x > (q_m + 1/2)\Delta_x \\ -q_m, & \text{if } x \leq -(-q_m + 1/2)\Delta_x \\ \left\lfloor \frac{x}{\Delta_x} + \frac{1}{2} \right\rfloor, & \text{if } -(-q_m + 1/2)\Delta_x < x \leq (q_m + 1/2)\Delta_x \end{cases} \tag{12}$$

where $\Delta_x > 0$ denotes the sensitivity of the uniform quantizer and q_m represents the saturation value of the uniform quantizer. From (11), it is clearly analyzed that if $x \in ((k-1)/2\Delta_x, (k+1/2)\Delta_x]$ where $k \in \mathbb{Z}$ and $-q_m \leq k \leq q_m$, then $q_u(x)$ will takes on the value k. The quantization error associated with $q_u(x)$ is defined as

$$\tilde{x} = x - \Delta_x q_u(x) \tag{13}$$

which satisfies $|\tilde{x}| \leq \Delta_x/2$. Similarly, for any vector $\boldsymbol{x} \in \mathbb{R}^n$ or any matrix $\boldsymbol{M} \in \mathbb{R}^{n \times m}$, it follows that

$$\|\tilde{\boldsymbol{x}}\| \leq \frac{\sqrt{n}}{2}\Delta_x, \quad \left\|\tilde{\boldsymbol{M}}\right\| \leq \frac{\sqrt{nm}}{2}\Delta_x \tag{14}$$

Remark 1. Since $q_u(x) \in \mathbb{Z}$, (11) can be applied as an encoder, where the real number x is encoded to an integer. Otherwise, $\Delta_x q_u(x)$ is regarded as the decoder, where the encoded $q_u(x)$ is restored to approximate its original real number x.

2.5 Control objective

This paper focuses on the encrypted control problem for spacecraft proximity operations. Since the control gain matrix $\boldsymbol{K}$ can be determined offline, it does not convey sensitive information. Differently, the real-time relative position and velocity information are extremely sensitive due to some unexpected leakage or eavesdropping involved in the communication network. Hence, the relative state information $\boldsymbol{x}$ should be concealed from the controller side before encryption, which implies that the state-feedback control law in (4) can not be calculated directly by using $\boldsymbol{x}$. In light of this, the purpose of this manuscript is to develop a Paillier-type encrypted control framework for (1), including a digitizer for continuous sampled state x and an encoder and a decoder for quantized state and control gain, and a Paillier-type encrypted state-feedback controller to achieve the following objectives:

(1) ensure the ultimately uniformly bounded stability of the whole closed-loop system;
(2) preserve the security of the state x from the controller.

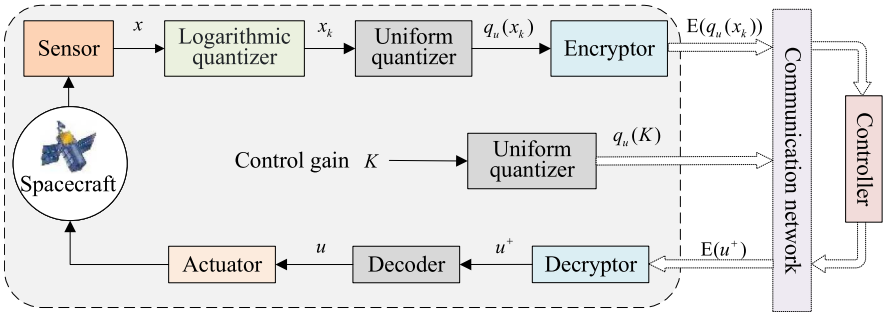


Figure 2. The block diagram of the proposed encrypted control system

3 Main results

In this section, an encrypted control algorithm by means of the Paillier encryption scheme is presented for spacecraft proximity operations. The detailed design procedure is summarized as follows: First, by using the uniform quantizer, the control gain is encoded to an integer and sent to the controller side for ease of further encryption operation. Meanwhile, the continuously measurable system states are quantized as digital signals by using the logarithmic quantizer because the communication network only allows the digital signals to be transmitted instead of the continuous ones. Similarly, for further encryption, the digitized system stats are encoded to the integer set with the aid of a uniform quantizer. Then, to guarantee data security, the system states are encrypted based on the Paillier cryptosystem and are sent to the controller side over the communication network. Next, by utilizing received encrypted system states and control gain, the encrypted control law is calculated according to the homomorphic properties in (6)–(8). Further, the resulting encrypted control law is sent to the system side without any information leakage. After Paillier-type decryption and simple decoding, a decrypted state-feedback control command is executed on the actuator of the spacecraft. The block diagram of the proposed encrypted control system is shown in Figure 2, where the solid line and dash line indicates the information exchange through the data buses or wireless communication network, respectively.

3.1 Encoding the control gain matrix

Since the Paillier encryption scheme only works the data in the form of integers, the control gain matrix $\boldsymbol{K}$ in (4) should be first encoded into an integer before being sent over the communication network, as depicted in Figure 2. As stated in Remark 1, the uniform quantizer can be regarded as an encoder and a decoder. Therefore, the uniform quantizer is adopted here to encode the control gain matrix $\boldsymbol{K}$ into $q_u(\boldsymbol{K})$. The corresponding quantizer error for $\boldsymbol{K}$ here is defined as $\tilde{\boldsymbol{K}} = \boldsymbol{K} - \Delta_K q_u(\boldsymbol{K})$, where $\Delta_K > 0$ refers to the sensitivity associated with the quantizer $q_u(K)$. For ease of convenience, define $\bar{\boldsymbol{K}} = \Delta_K q_u(\boldsymbol{K})$.

Theorem 1. *Consider the general linear system* (4) *with the control law* $\boldsymbol{u} = -\bar{\boldsymbol{K}}\boldsymbol{x}$. *Under Lemma 1, if the sensitivity* Δ_K *is selected such that the inequality*

$$\Delta_K \leq \frac{\varepsilon_1 \lambda_{\min}(\boldsymbol{Q})}{3\sqrt{2}\|\boldsymbol{P}\boldsymbol{B}\|}, \quad \varepsilon_1 \in (0,1) \tag{15}$$

holds trues, then the general linear system (2) *is asymptotic stable, where* $\boldsymbol{P}$ *and* $\boldsymbol{Q}$ *are positive-define matrices satisfying* (5).

Proof. By implementing the quantized state-feedback control law $\boldsymbol{u} = -\bar{\boldsymbol{K}}\boldsymbol{x}$, the closed-loop linear system (2) is rewritten as

$$\dot{\boldsymbol{x}} = (\boldsymbol{A} - \boldsymbol{B}\boldsymbol{K})\boldsymbol{x} + \boldsymbol{B}\tilde{\boldsymbol{K}}\boldsymbol{x} \tag{16}$$

Chose $V = \boldsymbol{x}^\top \boldsymbol{P}\boldsymbol{x}$ as the Lyapunov function candidate, where $\boldsymbol{P}$ is a positive-definite matrix satisfying (5). Then, combining (5) and (16) yields

$$\begin{aligned}\dot{V} &= \boldsymbol{x}^\top \boldsymbol{P}\dot{\boldsymbol{x}} - \dot{\boldsymbol{x}}^\top \boldsymbol{P}\boldsymbol{x} \\ &= \boldsymbol{x}^\top \Big((\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K})^\top \boldsymbol{P} + \boldsymbol{P}(\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K})\Big)\boldsymbol{x} + \boldsymbol{x}^\top \tilde{\boldsymbol{K}}^\top \boldsymbol{B}^\top \boldsymbol{P}\boldsymbol{x} + \boldsymbol{x}^\top \boldsymbol{P}\boldsymbol{B}\tilde{\boldsymbol{K}}\boldsymbol{x} \\ &\leq -\lambda_{\min}(\boldsymbol{Q})\|\boldsymbol{x}\|^2 + 2\left\|\boldsymbol{P}\boldsymbol{B}\tilde{\boldsymbol{K}}\right\|\|\boldsymbol{x}\|^2\end{aligned} \tag{17}$$

To proceed, it can be seen from (14) that $\|\tilde{\boldsymbol{K}}\| \leq \Delta_K 3\sqrt{2}/2$ always hold trues. Therefore, once Δ_K is chosen such that (15) satisfies, the following inequality always hold

$$-\lambda_{\min}(\boldsymbol{Q}) + 2\left\|\boldsymbol{P}\boldsymbol{B}\tilde{\boldsymbol{K}}\right\| \leq -(1-\varepsilon_1)\lambda_{\min}(\boldsymbol{Q}) \leq 0 \tag{18}$$

which directly implies that

$$\dot{V} \leq 0 \tag{19}$$

In summary, as long as Δ_K is selected by (15), it is straightforward to induce from (19) that the linear system (2) is asymptotic stable despite the quantization. This completes the proof of Theorem 1. □

Additionally, on the basis of Theorem 1 and the standard Lyapunov stability theory, there exist symmetric positive-define matrices $\bar{\boldsymbol{P}}$ and $\bar{\boldsymbol{Q}}$ such that

$$\big(\boldsymbol{A}-\boldsymbol{B}\bar{\boldsymbol{K}}\big)^\top \bar{\boldsymbol{P}} + \bar{\boldsymbol{P}}\big(\boldsymbol{A}-\boldsymbol{B}\bar{\boldsymbol{K}}\big) = -\bar{\boldsymbol{Q}} \tag{20}$$

3.2 Encrypted control law design

Let $\boldsymbol{x}_k$, $q_u(\boldsymbol{x}_k)$, $E(q_u(\boldsymbol{x}_k))$ represent the system state after digitization, encoding, and encryption, respectively. Then, using semi-homomorphic encryption, we design the encrypted control law as follows

$$\mathrm{E}(\boldsymbol{u}^+) = -\Big(\mathrm{E}(q_u(\boldsymbol{x}_k))^{q_u(\boldsymbol{K})} \mod N^2\Big) \tag{21}$$

Theorem 2. *Consider the general linear system described in (2) with the encrypted control law (21). Select the quantization parameters properly such that*

$$\sigma < \frac{\lambda_{\min}(\bar{\boldsymbol{Q}})}{2} \tag{22}$$

holds, where σ is a positive constant related to the logarithmic quantizer $q_l(\boldsymbol{x})$. Then, under the proposed encrypted control scheme, summarized in Algorithm 1, the general linear system (2) is ultimately uniformly stable. Moreover, the security of sensitive information transmitted over the spacecraft's communication network is completely protected.

Remark 2. From Figure 2, it is observed that $\boldsymbol{x}_k$ is sampled by the logarithmic quantizer $q_l(\boldsymbol{x})$ in (9). So, one can get that the digitization error $\|\Delta_l \boldsymbol{x}\| \leq \sigma\|\boldsymbol{x}\|$, where $\Delta_l \in \mathbb{R}^{6\times 6}$ is the sensitivities of the logarithmic quantizer. Besides, $q_u(\boldsymbol{x}_k)$ is obtained by using the uniform quantizer $q_u(\boldsymbol{x})$ with the sensitivity $\Delta_x > 0$. Accordingly, let $\bar{\boldsymbol{x}}_k = \boldsymbol{x}_k - \Delta_x q_u(\boldsymbol{x}_k)$ represent the quantizer error. After decryption and decoding for the encrypted control law (21), the control command $\boldsymbol{u}$ acting on the actuator is given by

$$\boldsymbol{u} = \Delta_x \Delta_K \mathrm{D}\big(\mathrm{E}(\boldsymbol{u}^+)\big) = -\Delta_x \Delta_K q_u(\boldsymbol{K}) q_u(\boldsymbol{x}_k) = -\bar{\boldsymbol{K}}\bar{\boldsymbol{x}}_k \tag{23}$$

Proof. It is noted from Remark 2 that the implementation of the encrypted control law (21) is equivalent to executing $\boldsymbol{u}$ in (23). In light of this, driven by the encrypted control law (21), the closed-loop linear system (2) is rewritten as

$$\dot{\boldsymbol{x}} = (\boldsymbol{A}-\boldsymbol{B}\bar{\boldsymbol{K}})\boldsymbol{x} - \boldsymbol{B}\bar{\boldsymbol{K}}\bar{\boldsymbol{x}}_k \tag{24}$$

Algorithm 1. The proposed encrypted control scheme for spacecraft proximity operations.

Initialize: choose p, q, g, r, $\boldsymbol{K}$, $\boldsymbol{P}, \boldsymbol{Q}, \bar{\boldsymbol{P}}, \bar{\boldsymbol{Q}}$
Ensure: $\boldsymbol{u}$
1: # Encode control gain matrix
2: select Δ_K so that (15) holds
3: compute $q_u(\boldsymbol{K})$ and sent to the controller over communication network
4: # Digitize
5: chose Δ_l based on (22)
6: digitized the system state $\boldsymbol{x}$ and obtain $\boldsymbol{x}_k$
7: # Encode the digitized system state
8: select Δ_x
9: obtain $q_u(\boldsymbol{x}_k)$
10: # Encrypt
11: encrypt $q_u(\boldsymbol{x}_k)$ by using Paillier encryption as $\mathrm{E}(q_u(\boldsymbol{x}_k))$
12: transmit $\mathrm{E}(q_u(\boldsymbol{x}_k))$ to the controller over communication network
13: # Obtain encrypted control law
14: compute the encrypted controller $\mathrm{E}(\boldsymbol{u}^+)$ according to (21)
15: transmit $\mathrm{E}(\boldsymbol{u}^+)$ to the plant node over communication network
16: # Decrypt
17: compute $\boldsymbol{u}^+ = \mathrm{D}\big(\mathrm{E}(\boldsymbol{u}^+)\big) = -q_u(\boldsymbol{K})q_u(\boldsymbol{x}_k)$ based on (8)
18: # Decode the decrypted controller
19: obtain and implement the practical control command $\boldsymbol{u}$ in (23)

Similarly to Theorem 1, chose $V = \boldsymbol{x}^\top \bar{\boldsymbol{P}}\boldsymbol{x}$ as the Lyapunov function candidate, where $\bar{\boldsymbol{P}}$ is a symmetrical positive-definite matrix satisfying (20). Then, taking the differentiate V over time along (23) results in

$$\begin{aligned}\dot{V} &= \boldsymbol{x}^\top \bar{\boldsymbol{P}}\dot{\boldsymbol{x}} - \dot{\boldsymbol{x}}^\top \bar{\boldsymbol{P}}\boldsymbol{x} \\ &= \boldsymbol{x}^\top \Big(\big(\boldsymbol{A} - \boldsymbol{B}\bar{\boldsymbol{K}}\big)^\top \bar{\boldsymbol{P}} + \bar{\boldsymbol{P}}\big(\boldsymbol{A} - \boldsymbol{B}\bar{\boldsymbol{K}}\big)\Big)\boldsymbol{x} - \boldsymbol{x}^\top \boldsymbol{\Delta}_l \bar{\boldsymbol{K}}^\top \boldsymbol{B}^\top \bar{\boldsymbol{P}}\boldsymbol{x} - \boldsymbol{x}^\top \bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\boldsymbol{\Delta}_l \boldsymbol{x} \\ &\quad + \tilde{\boldsymbol{x}}_k^\top \bar{\boldsymbol{K}}^\top \boldsymbol{B}^\top \bar{\boldsymbol{P}}\boldsymbol{x} + \boldsymbol{x}\bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\tilde{\boldsymbol{x}}_k\end{aligned} \tag{25}$$

where $\boldsymbol{x}_k = q_l(\boldsymbol{x})$, $\boldsymbol{\Delta}_l\boldsymbol{x} = \boldsymbol{x}_k - \boldsymbol{x}$, and $\tilde{\boldsymbol{x}}_k = \boldsymbol{x}_k - \Delta_l q_u(\boldsymbol{x}_k)$ are used in (24). Besides, reminding (11) and (14), it is easy to obtain that

$$\|\boldsymbol{x}_k\| \le |1 + \Delta_l|\|\boldsymbol{x}\|, \ \ \|\tilde{\boldsymbol{x}}_k\| \le \frac{\sqrt{6}}{2}\|\boldsymbol{\Delta}_x\| \tag{26}$$

Then, inserting (20) and (26) into (25), it follows that

$$\begin{aligned}\dot{V} &= -\boldsymbol{x}^\top \bar{\boldsymbol{Q}}\boldsymbol{x} - \boldsymbol{x}^\top \boldsymbol{\Delta}_l \bar{\boldsymbol{K}}^\top \boldsymbol{B}^\top \bar{\boldsymbol{P}}\boldsymbol{x} - \boldsymbol{x}^\top \bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\boldsymbol{\Delta}_l\boldsymbol{x} + \tilde{\boldsymbol{x}}_k^\top \bar{\boldsymbol{K}}^\top \boldsymbol{B}^\top \bar{\boldsymbol{P}}\boldsymbol{x} + \boldsymbol{x}^\top \bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\tilde{\boldsymbol{x}}_k \\ &\le -\lambda_{\min}(\bar{\boldsymbol{Q}})\|\boldsymbol{x}\|^2 + 2|\Delta_l|\big\|\bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\big\|\|\boldsymbol{x}\|^2 + \sqrt{6}|\Delta_x|\big\|\bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\big\|\|\boldsymbol{x}\|\end{aligned} \tag{27}$$

Further, recalling the parameter condition in (23), it has

$$\dot{V} \le -\big(\lambda_{\min}(\bar{\boldsymbol{Q}}) - 2\sigma\big)\|\boldsymbol{x}\|^2 + \sqrt{6}|\Delta_x|\big\|\bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\big\|\|\boldsymbol{x}\| \tag{28}$$

To proceed, it is clearly seen from (28) that $\dot{V} < 0$ when $\boldsymbol{x}$ evolves outside of the following set

$$\mathbb{S}_x \triangleq \left\{\boldsymbol{x} : \ \|\boldsymbol{x}\| \le \frac{\sqrt{6}|\Delta_x|\big\|\bar{\boldsymbol{P}}\boldsymbol{B}\bar{\boldsymbol{K}}\big\|}{\big(\lambda_{\min}(\bar{\boldsymbol{Q}}) - 2\sigma\big)}\right\} \tag{29}$$

It is concluded from (29) that once the system state moves in the out of $\mathbb{S}_x$, it will be attracted back to $\mathbb{S}_x$ immediately. Therefore, the closed-loop system is ultimately uniformly bounded stable. Moreover, the convergence set $\mathbb{S}_x$ can be made enough small by choosing Δ_x as small as possible and choosing σ as big as possible. This completes the proof of Theorem 2. □

Remark 3. Following Figure 2, the information sent from the sensor to the controller has been encoded and encrypted before transmission over the communication network. Moreover, it is obviously seen from (21) that the encrypted control law is computed by using the encrypted relevant relative state $\mathrm{E}(q_u(\boldsymbol{x}_k))$ rather than the real-time measured value of sensor $\boldsymbol{x}$. Therefore, there is also no sensitive relative state information that is leaked when the encrypted controller is transmitted from the controller to the actuator over the communication channel. Besides, exploiting the properties of the Pailliar cryptosystem, the proposed encrypted framework can secure the communication network of the spacecraft against false data injection attacks. For example, if the attacker injects a random real-valued noise, the controller will easily detect the false data injection attack as the transmitted signals under the Paillier scheme are integer-valued. When the attacker injects an integer-valued random noise into the communication channel, the attack cannot be detected by the controller. However, a slight change in the ciphertext results in a significant change in the computed control input (after decryption) due to the highly nonlinear operations of the Paillier cryptosystem. In this case, the actuator can detect the false data injection attack by comparing the current control input with the past control input. Consequently, the security of the spacecraft's relative motion control system is successfully protected.

Remark 4. Note that the encrypted control framework is designed based on the linear CWH equation and additive homomorphic encryption of Paillier. Although the linear CWH equation can clearly describe the relative motion between two spacecraft, a more precise control scheme can be generated by resorting to the more detailed nonlinear dynamical model. Besides, although the security and privacy of the sensitive relative motion information and control input signal are preserved, the proposed encrypted control scheme does not guarantee the security of the control gain matrix due to the inherent limitation of the Paillier encryption scheme. Therefore, the secure motion control scheme of micro-spacecraft based on the nonlinear dynamical model deserves to be investigated in future work, especially using the fully homomorphic encryption method.

4 Simulations

In this section, numerical simulations are performed to verify the performance of the encrypted control framework proposed in Figure 2. Assume that the target spacecraft moves on a circular orbit with $r_c = 6.5867 \times 10^6$ m. The geocentric gravitational constant of the Earth is $\mu_c = 3.986 \times 10^{14}$ m^3/s^2. The mass of chase spacecraft is $m_c = 10$ kg. In this setting, the matrices A and B in (3) are given by

$$\boldsymbol{A} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 3 \times 0.0012^2 & 0 & 0 & 0 & 0.0024 & 0 \\ 0 & 0 & 0 & -0.0024 & 0 & 0 \\ 0 & 0 & -0.0012^2 & 0 & 0 & 0 \end{bmatrix}, \quad \boldsymbol{B} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.1 & 0 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 0.1 \end{bmatrix}$$

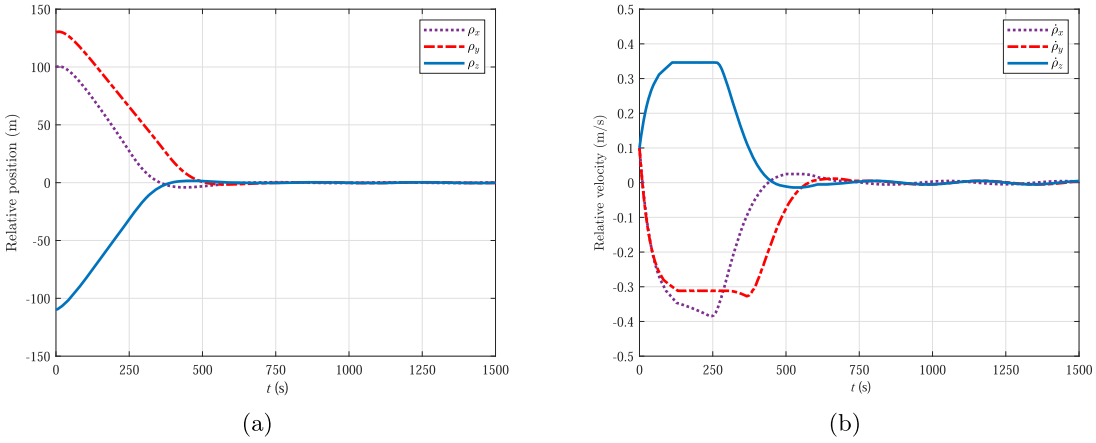
respectively. Besides, the initial relative position and relative velocity of the chase spacecraft are set as $\boldsymbol{\rho} = [100, 130, -110]^\top$ m and $\dot{\boldsymbol{\rho}} = [0.1, 0.1, 0.1]^\top$ m/s, separately. Moreover, it is assumed that the maximum control force generated by the chase spacecraft is 0.2N. Further, the state-feedback control law (4) is determined by solving the linear quadratic regulator (LQR) problem, where the cost function is defined by

$$J = \int_0^\infty \left(\boldsymbol{x}^\top \boldsymbol{Q}\boldsymbol{x} + \boldsymbol{u}^\top \boldsymbol{R}\boldsymbol{u}\right) \mathrm{d}t$$

with $\boldsymbol{Q} = \mathrm{diag}\{100, 100, 100, 10^4, 10^4, 10^4\}$ and $\boldsymbol{R} = 10^7 \times \boldsymbol{I}_3$. Then, the control gain matrix $\boldsymbol{K}$ can be calculated as

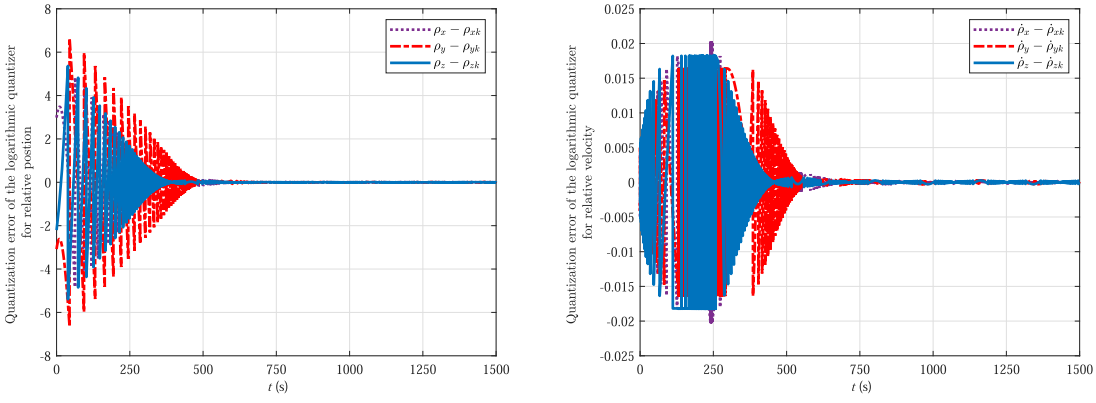
$$\boldsymbol{K} = \begin{bmatrix} 0.0032 & -0.0003 & 0.0000 & 0.2546 & 0.0001 & 0.0000 \\ 0.0003 & 0.0031 & 0.0000 & 0.0001 & 0.2529 & 0.0000 \\ 0.0000 & 0.0000 & 0.0031 & 0.0000 & 0.0000 & 0.2529 \end{bmatrix}$$

The parameter relevant to the logarithmic quantizer $q_l(\boldsymbol{x})$ is $\sigma = 0.05$. The sensitivity and saturation value of the uniform quantizer $q_u(\boldsymbol{x})$ are chosen as $\Delta_x = 0.01$ and $q_{mx} = 3000$, while these two parameters for the uniform quantizer $q_u(\boldsymbol{K})$ are selected as $\Delta_K = 0.001$ and $q_{mK} = 2000$, respectively. The



(a) (b)

Figure 3. Time response of relative position and velocity of the chaser spacecraft. (a) Evolution of relative position and (b) Evolution of velocity



(a) (b)

Figure 4. Quantization error of the chaser spacecraft under the logarithmic quantizer. (a) Error for relative position and (b) Error for relative velocity

implementation of the Paillier cryptosystem is referred to [31]. More specifically, two large prime numbers p and q are selected as $p = 3470023813$ and $q = 3315231457$; the random integer g in the public key is selected as $g = 153141813157562389396272824718325702 58$; the private key (λ, μ) are selected as $\lambda = 958661007884285856$ and $\mu = 1687557451384170425$.

The simulation results are shown in Figures 3–6. More specifically, the evolution of the relative position and relative velocity of the chase spacecraft is illustrated in Figure 3. Figure 4 depicts the quantization error of the relative position and velocity for the chase spacecraft after digitization using the logarithmic quantizer. Figure 5 displays the error of the relative position and velocity of the chase spacecraft after encoding and decoding using a uniform quantizer. From Figures 3 to 5, it is concluded that although the quantization errors exist, the chase spacecraft under the proposed encrypted control framework is still able to achieve the desired tracking mission with acceptable accuracy. The time history of the control force of the chase spacecraft is illustrated in Figure 6, which always is limited within 0.2N. In addition, the trajectories of the encrypted relative position, relative velocity, and control input are shown in Figures 7–9. Based on these figures, it is impossible for malicious to infer the actual relative motion information (Figs. 3 and 4) and the actual control command (Fig. 5) only by eavesdropping the encrypted signals (Figs. 7–9). Therefore, the proposed encrypted control framework not only achieves the desired relative motion of micro-spacecraft with graceful control performance but also ensures the secure information exchange among different components of the spacecraft.

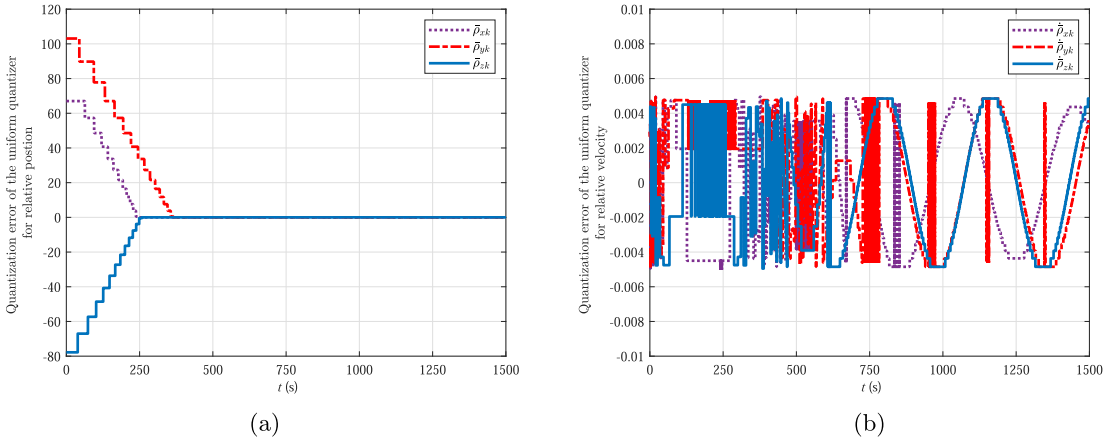


Figure 5. Quantization error of the chaser spacecraft under the uniform quantizer. (a) Error for relative position and (b) Error for relative velocity

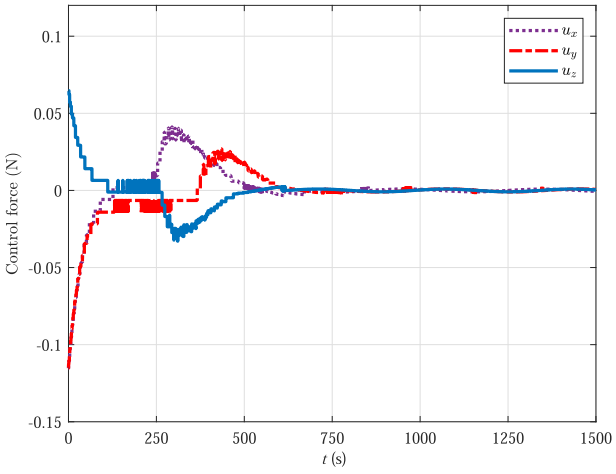


Figure 6. Time response of control force of the chaser spacecraft

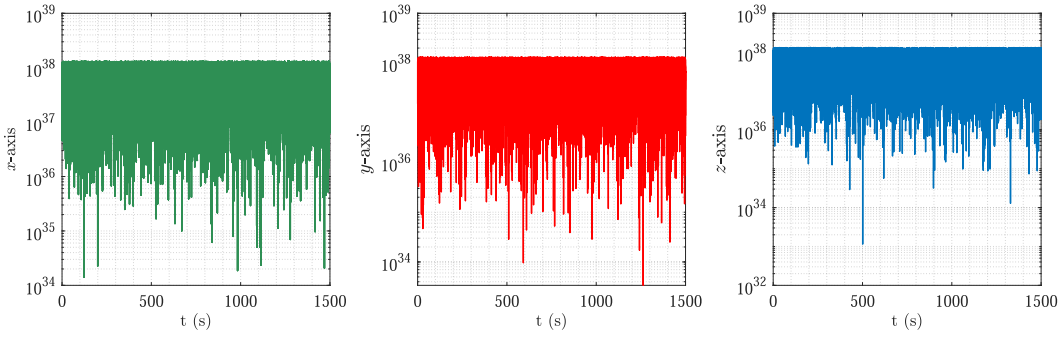


Figure 7. The encrypted relative position

5 Conclusions

This study proposed a novel encrypted control framework for spacecraft relative motion control using a logarithmic quantizer, two uniform quantizers, and a semi-homomorphic cryptosystem. The logarithmic quantizer was used to quantize the continuous relative state information, while the uniform quantizer was regarded as the encoder and decoder before encryption and after decryption, respectively. By selecting the proper quantization parameter, it is shown that the proposed encrypted control is capable of

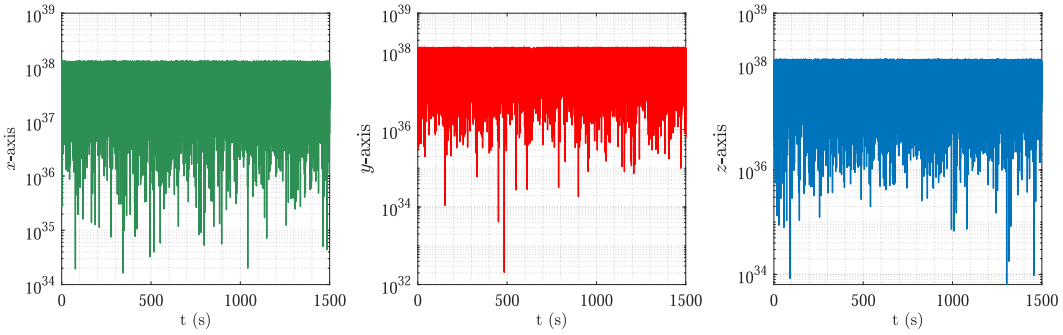


Figure 8. The encrypted relative velocity

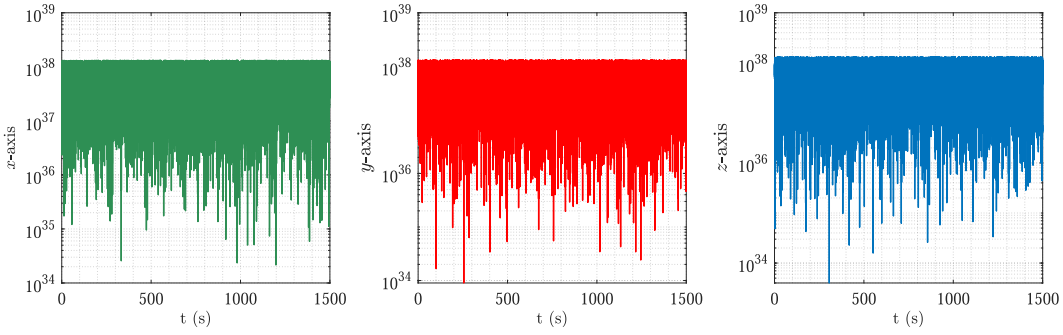


Figure 9. The encrypted control input $\mathrm{E}(u^{+})$

guaranteeing ultimately uniformly bounded stability of the spacecraft relation motion system. Moreover, the security of the sensitive relative state information was ensured by the Paillier cryptosystem. Possible future work will concentrate on the encrypted control problem of spacecraft relative motion with more practical constraints, such as unknown parameter uncertainties, exogenous disturbances, and with a less conservative fully homomorphic encryption scheme.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Yongxia Shi proposed the overall control framework and wrote this paper. Ehsan Nekouei verified the feasibility of the proposed control framework and improved the presentation of the results; Qinglei Hu participated in manuscript preparation. All authors read and approved the final manuscript.

Acknowledgements

We thank the Associate editor and the anonymous reviewers for their helpful comments.

Funding

The work was supported partly by the National Natural Science Foundation of China under Grants 62227812 and 61960206011, partly by the Zhejiang Provincial Natural Science Foundation under Grant LD22E050004, partly by the Research Grants Council of Hong Kong under Project CityU 21208921, and partly by the Chow Sang Sang Group Research Fund Sponsored by Chow Sang Sang Holdings International Ltd.

References

[1] McCamish SB, Romano M and Yun X. Autonomous distributed control of simultaneous multiple spacecraft proximity maneuvers. IEEE Trans Autom Sci Eng 2010; **7**: 630–44.
[2] Yoon H and Agrawal BN. Novel expressions of equations of relative motion and control in Keplerian orbits. J Guid Control Dyn 2009; **32**: 664–9.
[3] Capello E, Punta E and Dabbene F et al. Sliding-mode control strategies for rendezvous and docking maneuvers. J Guid Control Dyn 2017; **40**: 1481–7.
[4] Weiss A, Petersen C and Baldwin M et al. Safe positively invariant sets for spacecraft obstacle avoidance. J Guid Control Dyn 2015; **38**: 720–32.
[5] Di Cairano S, Park H and Kolmanovsky I. Model predictive control approach for guidance of spacecraft rendezvous and proximity maneuvering. Int J Robust Nonlinear Control 2012; **22**: 1398–427.
[6] McCamish SB, Romano M and Yun X. Autonomous distributed control of simultaneous multiple spacecraft proximity maneuvers. IEEE Trans Autom Sci Eng 2010; **7**: 630–44.
[7] Reynolds TP, Kelly CL and Morgan C et al. SOC-i: a CubeSat demonstration of optimization-based real-time constrained attitude control. In: 2021 IEEE Aerospace Conference (50100). IEEE, 2021, 1–18.
[8] Morphopoulos T, Hansen LJ and Pollack J et al. Plug-and-play–an enabling capability for responsive space missions. In: Paper No. RS2-2004-5002, Presented at 2nd Responsive Space Conference. Los Angeles, CA, 2004.
[9] Lyke J, Cannon S and Fronterhouse D et al. A plug-and-play system for spacecraft components based on the USB standard. 2005.
[10] Lyke JC. Plug-and-play satellites. IEEE Spect 2012; **49**: 36–42.
[11] Bandyopadhyay S, Subramanian GP and Foust R et al. A review of impending small satellite formation flying missions. In: 53rd AIAA Aerospace Sciences Meeting. 2015, 1623.
[12] Wu B. Spacecraft attitude control with input quantization. J Guid Control Dyn 2016; **39**: 176–81.
[13] Wu B and Cao X. Robust attitude tracking control for spacecraft with quantized torques. IEEE Trans Aerosp Electron Syst 2017; **54**: 1020–8.
[14] Sun H, Hou L and Zong G et al. Fixed-time attitude tracking control for spacecraft with input quantization. IEEE Trans Aerosp Electron Syst 2018; **55**: 124–34.
[15] Liu Q, Liu M and Yu J. Adaptive fault-tolerant control for attitude tracking of flexible spacecraft with limited data transmission. IEEE Trans Syst Man Cybern Syst 2019; **51**: 4400–8.
[16] Sun H and Hou L. Adaptive attitude control for spacecraft systems with sensor and actuator attacks. Int J Adapt Control Signal Process 2022; **36**: 448–68.
[17] Tran J, Farokhi F and Cantoni M et al. Implementing homomorphic encryption based secure feedback control. Control Eng Pract 2020; **97**: 104350.
[18] Cortés J, Dullerud GE and Han S et al. Differential privacy in control and network systems. In: 2016 IEEE 55th Conference on Decision and Control (CDC). IEEE, 2016, 4252–72.
[19] Zhang C, Wu J and Huang Y et al. Constructive schemes to spacecraft attitude control with low communication frequency using sampled-data and encryption approaches. Aircr Eng Aerosp Technol 2021; **93**: 267–74.
[20] Kogiso K and Fujita T. Cyber-security enhancement of networked control systems using homomorphic encryption. In: 2015 54th IEEE Conference on Decision and Control (CDC). IEEE, 2015, 6836–43.
[21] Teranishi K, Shimada N and Kogiso K. Stability-guaranteed dynamic ElGamal cryptosystem for encrypted control systems. IET Control Theory Appl 2020; **14**: 2242–52.
[22] Kawase H, Teranishi K and Kogiso K. Dynamic quantizer synthesis for encrypted state-feedback control systems with partially homomorphic encryption. In: 2022 American Control Conference (ACC). IEEE, 2022, 75–81.
[23] Farokhi F, Shames I and Batterham N. Secure and private control using semi-homomorphic encryption. Control Eng Pract 2017; **67**: 13–20.
[24] Kishida M. Encrypted control system with quantiser. IET Control Theory Appl 2019; **13**: 146–51.
[25] Murguia C, Farokhi F and Shames I. Secure and private implementation of dynamic controllers using semihomomorphic encryption. IEEE Trans Autom Control 2020; **65**: 3950–7.
[26] Garcia E and Antsaklis PJ. Model-based event-triggered control for systems with quantization and time-varying network delays. IEEE Trans Autom Control 2012; **58**: 422–34.
[27] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Advances in Cryptology–EUROCRYP'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18. Springer Berlin Heidelberg, 1999, 223–8.
[28] Acar A, Aksu H and Uluagac AS et al. A survey on homomorphic encryption schemes: theory and implementation. ACM Comput Surv 2018; **51**: 1–35.
[29] Shi P, Wang H and Lim CC. Network-based event-triggered control for singular systems with quantizations. IEEE Trans Ind Electron 2016; **63**: 1230–8.
[30] Brockett RW and Liberzon D. Quantized feedback stabilization of linear systems. IEEE Trans Autom Control 2000; **45**: 1279–89.
[31] https://github.com/martin-kaluz/PaillierCrypto-matlab.

Yongxia Shi received a Ph.D. degree in navigation, guidance, and control from Beihang University, Beijing, China, in 2022. From Dec. 2020 to Nov. 2021, she was a joint Ph.D. Student with the Delft Center for Systems and Control, Delft University of Technology, the Netherlands. She is currently a Postdoctoral Researcher at the Department of Electrical Engineering, City University of Hong Kong. Her research interests include spacecraft formation flying, networked control systems, distributed control, event-triggered control, and homomorphic encryption control.

Ehsan Nekouei is currently an Assistant Professor at the Department of Electrical Engineering, City University of Hong Kong. From 2014 to 2019, he held postdoctoral positions at the KTH Royal Institute of Technology, Stockholm, Sweden, and The University of Melbourne, Australia. His current research interests include privacy and security of networked control systems.

Qinglei Hu received a B.Eng. degree in electrical and electronic engineering from Zhengzhou University, Zhengzhou, China, in 2001, and a Ph.D. degree in control science and engineering with a specialization in guidance and control from the Harbin Institute of Technology, Harbin, China, in 2006. From 2003 to 2014, he was with the Department of Control Science and Engineering, Harbin Institute of Technology. He joined Beihang University, Beijing, China, in 2014, as a Full Professor. His current research interests include variable structure control and applications, and fault-tolerant control and applications.