IEEE Control Systems Letters paper presented at
2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Consensus Control Based on Privacy-Preserving Two-Party Relationship Test Protocol

Hanzhou Wang[1,3], Dongyu Li[*1,2,3], Zhenyu Guan[1], Yizhong Liu[1], Jianwei Liu[1]

Abstract— **Preservation of privacy is a challenging and significant constraint in multi-agent systems. This paper aims to introduce a framework that enables the states of a multi-agent system to reach a consensus while preserving the confidentiality of each agent's initial states from others. First, a protocol for a privacy-preserving two-party relationship test is proposed. Subsequently, the protocol is employed to devise the average consensus controller for the first-order system, and the rendezvous controller for the second-order system. In contrast to prior research that relies on stochastic coupling weights, our approach circumvents the random chattering problem of the control input, resulting in improved convergence performance. Finally, numerical verification is conducted to demonstrate the effectiveness of the proposed controllers in both first- and second-order systems.**

I. INTRODUCTION

In recent years, the significance of information value has gained increasing recognition. Information that is highly valuable and sensitive possesses both a need to be utilized and a compelling motivation to be preserved locally. In a multi-agent system, the local states are deemed crucial and sensitive, particularly in specific scenarios. For instance, in the context of multi-satellite collaboration, orbital information reveals specific satellite functionalities. The revelation of precise orbital details would lead to the loss of military strategy or commercial value [1].

The preservation of privacy in multi-agent systems is a complex problem, whose challenge lies in balancing the need for privacy with control performance, which varies depending on the approach used. Previous research has focused on three primary privacy-preserving methods. Differential privacy has been widely applied in many studies [2], [3], with accuracy being the primary concern. By introducing designed noise, sensitive local states are obscured, allowing other agents to obtain coarse information. Another approach involves privacy decomposition [4], [5]. The sensitive states are decomposed into interrelated sets of secret subparts, which are subsequently distributed to different agents or kept locally to ensure complete information preservation in case there is no collusion. However, protocol failure may occur when the topology of the system changes. The third approach, based on homomorphic encryption, necessitates relatively higher computational power but offers greater accuracy, adaptability to topology changes, and resilience against collusive privacy inferences [6]–[8]. As the computational power constraint becomes less prominent for agents, this approach has gained increasing attention.

Homomorphic encryption ensures the confidentiality of sensitive data in the computational process. However, the decrypted form of data is required for use. It is possible for an agent to deduce the private data of cooperating agents from computation results based on known information. Therefore, privacy masking operations must be performed without affecting data usage. Randomness is the most commonly used method for masking sensitive data. Ruan et al. propose a random coupling weight method, which randomly splits the weight of the communication topology into a product of two substates, revealing only one of the substates to the neighboring agents [6]. This method guarantees asymptotic convergence to the exact mean value.

Despite its aim to preserve privacy, the random coupling weight method has a direct impact on the control input, resulting in a random chattering problem (refer to Figure 12 in [6] and Figure 2-d in [7]). In a real dynamic system, the presence of random chattering can degrade performance, which is unacceptable in certain cases.

To address this issue, a privacy-preserving two-party relationship test protocol based on the Paillier cryptosystem is introduced. We have applied this protocol to the design of controllers for consensus problems in connected undirected graphs, successfully overcoming the random chattering problem. Our controllers ensure that a first-order system reaches the average consensus, while a second-order system reaches the rendezvous point. However, our approach does come with a trade-off, as the convergence rate is relatively slow and there is a cryptographic computational overhead.

II. BACKGROUND AND PRELIMINARY

A. Additive Homomorphic Cryptosystem

We adopt the Paillier public-key cryptosystem [9], which does not rely on a trusted third party for key management, and is applicable in an open and dynamic multi-agent system. The Paillier cryptosystem has the additive homomorphic property for messages encrypted with the same public key.

$$\mathcal{D}(\mathcal{E}(m_1)\cdot\mathcal{E}(m_2) \mod n^2) = m_1 + m_2 \mod n, \quad (1)$$

This work was supported by Tianmushan Laboratory Research Project TK-2023-C-020 and TK-2023-B-010, Industry-University-Research Foundation of China under Grant 2021ZYA02022, and the Foundation of Science and Technology on Space Intelligent Control Laboratory under Grant HTKJ2022KL502008.

[1]H. Wang, D. Li, Z. Guan, Y. Liu, and J. Liu are with the Cyber-Science and Technology School of Beihang University. Beijing 100191, China. dongyuli@buaa.edu.cn.

[2]D. Li is also with the Shanghai Institute of Satellite Engineering and the Shanghai Key Laboratory of Deep Space Exploration Technology, Shanghai 201109, China.

[3]D. Li and H. Wang are also with the Tianmushan Laboratory, Hangzhou, 310023 P. R. China.

* Corresponding author

$$\mathcal{D}(\mathcal{E}(m)^k \mod n^2) = k \cdot m \mod n, \tag{2}$$

where $\mathcal{E}, \mathcal{D}$ are the Paillier encryption and the decryption function, respectively, n is the modulo in the public key, $m_1, m_2, m \in \mathbb{Z}_n$ are plaintexts, and k is a positive integer.

Inspired by the way negative integers are handled in [6], a simple variant of the Paillier cryptosystem that is compatible with negative integers is introduced with the rounding down function $\lfloor \cdot \rfloor$, and the plaintext $m \in [-\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor] \cap \mathbb{Z}$,

$$\mathcal{E}(m) \to \mathcal{E}(m \bmod n), \tag{3}$$

$$\mathcal{D}(\mathcal{E}(m)) \to ((\mathcal{D}(\mathcal{E}(m)) + \lfloor \frac{n}{2} \rfloor) \bmod n) - \lfloor \frac{n}{2} \rfloor. \tag{4}$$

The variant Paillier encryption and decryption are represented as $\mathcal{E}', \mathcal{D}'$, respectively. It is easy to prove that the variant Paillier cryptosystem also holds the additive homomorphism property, $\mathcal{E}(-m)$ can be computed by $\mathcal{E}(m)$,

$$\mathcal{E}'(-m)) = \mathcal{E}'((n-1) \cdot m) = \mathcal{E}'(m)^{(n-1)} \mod n^2. \tag{5}$$

B. Number-to-Fraction Random Transformation

The concepts that describe the scheme are presented. The set of all private values is denoted by $\mathbb{R}_b$, and we assume that $\mathbb{R}_b = [-B, B]$ is bounded and centered at zero, where $B \in \mathbb{R}^+$ is the boundary. The accuracy of the transformation is represented by $Q \in \mathbb{Z}^+$, and the error tolerance is $err = 1/Q$. $R \in \mathbb{Z}^+$ is the parameter for adjusting the randomness of the transformation. To randomly map a real number $x \in \mathbb{R}_b$ to a pair of integers (x_p, x_q) with an error tolerance and no coprimality requirement, a Number-to-Fraction Random Transformation algorithm, denoted by NFRT, is introduced.

***Algorithm* 1.** Number-to-Fraction Random Transformation

1. Assign the accuracy $Q \in \mathbb{Z}^+$, the boundary $B \in \mathbb{R}$, and the parameter for adjusting the randomness $R \in \mathbb{Z}^+$.

2. If $|x| < 1/Q$, then $x_p = 0,\ x_q$ is selected randomly in the range $[1, \max(Q, R)] \cap \mathbb{Z}$.

3. Else randomly select $x_q \in [1, \max(Q, R)] \cap \mathbb{Z}$, compute $x_p = \lfloor x_q \cdot x + \frac{1}{2} \rfloor$.

4. If $|\frac{x_p}{x_q} - x| < 1/Q$, the integer pair (x_p, x_q) is obtained, else the value x_q is dropped, Steps 3 and 4 are repeated.

An example is provided. By assigning the parameters $R = Q = B = 100$, the input 11.24 has multiple outputs. For example, $(281, 25)$ and $(12454, 1108)$ are both possible.

A theorem is presented to illustrate the output of Algorithm 1 has a satisfactory level of randomness, which can be adjusted by the parameter R.

***Theorem* 1**. Any input x in $[-B, B]$ can be transformed by Algorithm 1 into at least R possible integer pairs, i.e.,

$$\min_{x \in \mathbb{R}_b} (\mathrm{Card}(\{(x_p, x_q) | (x_p, x_q) = \mathrm{NFRT}(x)\})) \geq R. \tag{6}$$

Proof. The positive case of x exhibits symmetry with respect to the negative case. Without loss of generality, it is assumed that R, Q are even numbers. Firstly, considering the case where x is non-negative, the existence of $R/2$ possible pairs of integers will be proved.

Consider the series $x = \frac{m}{Q},\ m \in [0, \lfloor B \cdot Q + \frac{1}{2} \rfloor] \cap \mathbb{Z}$. In the case where $R \leq Q$, we have $x_q \in [1, Q] \cap \mathbb{Z},\ x_p \in [0, \lfloor B \cdot Q + \frac{1}{2} \rfloor]$. Moreover, (x_p, x_q) satisfies the accuracy inequality $|\frac{x_p}{x_q} - \frac{m}{Q}| < \frac{1}{Q},\ \frac{x_p}{x_q} \in (\frac{m-1}{Q}, \frac{m+1}{Q})$. Since $\frac{m+1}{Q} - \frac{m-1}{Q} = \frac{2}{Q}$, for each $x_q \in \{\frac{Q}{2} + 1, \cdots, Q\}$, there exists at least one possible x_p that satisfies the inequality. Given that $R \leq Q$, there are $R/2$ possible pairs of integers. In the case where $R > Q$, we have $x_q \in [1, R] \cap \mathbb{Z},\ x_p \in [0, \lfloor B \cdot R + \frac{1}{2} \rfloor] \cap \mathbb{Z}$. The accuracy inequality remains valid. Since $\frac{m+1}{Q} - \frac{m-1}{Q} = \frac{2}{Q}$, for each $x_q \in \{\frac{Q}{2} + 1, \cdots, R\}$, there exists at least one possible x_p that satisfies the inequality. The number of possible pairs of integers is $R - \frac{Q}{2}$, which is larger than $R/2$.

Consider $x \in [0, B]$ and $x \neq \frac{m}{Q},\ m \in [0, \lfloor B \cdot Q + \frac{1}{2} \rfloor] \cap \mathbb{Z}$. Given that the shortest distance from x to the series $x = \frac{m}{Q},\ m \in [0, \lfloor B \cdot Q + \frac{1}{2} \rfloor] \cap \mathbb{Z}$ is less than $\frac{1}{Q}$, the existence of $R/2$ possible pairs of integers is obvious.

In summary, in the case where the inputs $x \in [-B, B]$, there exist at least R possible pairs of integers as outputs. That is, Equation (6) is valid. ■

III. PROBLEM FORMULATION

A. System Description

Characterized by the discrete-time dynamics, a first-order system is defined as follows

$$\mathbf{x}_i(k+1) = \mathbf{x}_i(k) + \epsilon \cdot \mathbf{u}_i(k), \tag{7}$$

and a second-order system is defined as follows

$$\begin{aligned} \mathbf{p}_i(k+1) &= \mathbf{p}_i(k) + \epsilon \cdot \mathbf{v}_i(k), \\ \mathbf{v}_i(k+1) &= \mathbf{v}_i(k) + \epsilon \cdot \mathbf{u}_i(k), \end{aligned} \tag{8}$$

where k denotes the non-negative time index, $\epsilon > 0$ signifies the step time, associated with Agent i, $\mathbf{x}_i \in \mathbb{R}_b^N$ is the state of the first-order system, $\mathbf{p}_i, \mathbf{v}_i \in \mathbb{R}_b^N$ are the states of the second-order system, i.e., position and velocity, respectively, $\mathbf{u}_i$ is the control input, and N is the dimensionality [7].

The analysis focuses on the case of three-dimensional space, i.e., $N = 3$. The states of the agents are expressed with respect to an orthogonal coordinate basis $\{X, Y, Z\}$.

B. Communication Graph

The communication conditions of the n-agent network are characterized by the graph $\mathcal{G}(\mathbb{V}, \mathbb{E}, \mathcal{A})$, where $\mathbb{V} = \{1, \cdots, n\}$ is the set of all nodes, $\mathbb{E}$ is the set of all edges between the nodes, and $\mathcal{A}$ is the adjacency matrix. For each element a_{ij} in $\mathcal{A}$, if $(i, j) \in \mathbb{E}, a_{ij} = 1$, otherwise $a_{ij} = 0$.

***Assumption* 1**. The graph is undirected and connected.

The scheme is built upon a two-party protocol that requires bidirectional interaction. Specifically, Protocol 1, Steps A2, B4, and A7 contain the sending and receiving of messages. Consequently, an undirected graph is essential.

C. Consensus

***Definition* 1**. An n-agent discrete-time first-order system with dynamics as in (7) is said to reach the average consensus if all states converge to the mean of the initial values, i.e.,

$$\forall i \in \{1, \cdots, n\}, \quad \lim_{k\to\infty} \mathbf{x}_i(k) = \frac{1}{n}\sum_{j=1}^{n} \mathbf{x}_j(0). \tag{9}$$

***Definition* 2**. An n-agent discrete-time second-order system with dynamics as in (8) is said to reach the rendezvous point, if $\exists\ \beta > 0$ such that, for all agents, the positions $\mathbf{p}_i(k)$ and velocities $\mathbf{v}_i(k)$ satisfy the following condition:

$$\begin{aligned} &\forall i \in \{1, \cdots, n\}, \quad \lim_{k\to\infty} \mathbf{p}_i(k) = \frac{1}{n}\sum_{j=1}^{n}(\mathbf{p}_j(0) + \frac{\mathbf{v}_j(0)}{\beta}), \\ &\forall i \in \{1, \cdots, n\}, \quad \lim_{k\to\infty} \mathbf{v}_i(k) = \mathbf{0}. \end{aligned} \tag{10}$$

D. Privacy-Preserving Model

The concept of a semi-honest participant is introduced. A semi-honest participant fully complies with the given protocols and does not cheat or divulge information, but may collect the information obtained during the execution of the protocol and try to deduce the private information of other participants [10]. These deductions made by the semi-honest participants are called "privacy inferences". This paper considers the privacy inference as the mathematical process of gathering information from protocol interactions, constructing a system of equations, and subsequently solving for private information, i.e., the states $\mathbf{x}_i$ for first-order systems, and the states of positions and the velocities $\mathbf{p}_i$, $\mathbf{v}_i$ for second-order systems.

***Assumption* 2**. All adversary agents are semi-honest.

The semi-honest model is widely adopted as the fundamental assumption for studying the malicious model. In this context, our attention is directed toward the potential threat of privacy leakage to neighboring entities.

E. Problem Statement

Two consensus control problems that incorporate privacy-preserving constraints in a multi-agent system are studied:

1) The privacy-preserving average consensus problem of a first-order system seeks to reach the average consensus, as defined in Definition 1, while ensuring that the initial states $\mathbf{x}_i(0),\ i \in \mathbb{V}$ of each agent, remain confidential from the others. In other words, the private states are preserved.

2) The privacy-preserving rendezvous problem of a second-order system seeks to reach the rendezvous point, as defined in Definition 2, while ensuring that the initial states including the positions and velocities $\mathbf{p}_i(0), \mathbf{v}_i(0),\ i \in \mathbb{V}$ of each agent remain confidential from the others. In other words, the private states are preserved locally.

IV. MAIN RESULT

A. Privacy-Preserving Tests On Relationship

The test of the relationship between two private values, also known as a private comparison, was initially introduced in Yao's Millionaire Problem [11] and serves as a fundamental component in numerous privacy-preserving problems. In dynamic systems, its application presents two challenges. Firstly, all states of the agents are expressed in the form of real numbers, yet to the best of our knowledge, privacy-preserving relationship tests cannot be strictly executed on the real number field. Secondly, the privacy-preserving relationship tests necessitate resistance against multiple and collusive privacy inferences. To surmount the first challenge, Gong et al. propose a privacy-preserving relationship test protocol that broadens the definition domain from integers to rational numbers [12]. Drawing inspiration from their solution, Algorithm 1 is employed to approximate the real number states in the dynamic system with rational numbers and to augment resistance against privacy inferences. The two-party protocol for testing the relationship between two private rational values, a and b is as follows:

***Protocol* 1.** Privacy-Preserving Test of the Relationship Between Two Private Values

A0. Initiation: generate a pair of public and private keys $K_p^A = \{n, g\}, K_s^A = \{n, \lambda\}$ of the Paillier cryptosystem [9].

A1. Transform the private value a into a pair of integers using Algorithm 1, such that $(a_p, a_q) = NFRT(a)$.

A2. Compute $\mathcal{E}'(a_p), \mathcal{E}'(a_q)$, where $\mathcal{E}'$ is the variant Pailler encryption (3) with K_p^A, and transmit the results to party B.

B3. Upon receipt of the message from party A, transform the private value b into $(b_p, b_q) = NFRT(b)$.

B4. Choose a random number $k \in \mathbb{Z}_n^+$, compute the encrypted message E_m with the additive homomorphic property, and transmit the encrypted message E_m to party A.

$$\begin{aligned} E_m &= (\mathcal{E}'(a_q)^{b_p} \cdot \mathcal{E}'(a_p)^{b_q\cdot(n-1)})^k \mod n^2 \\ &= \mathcal{E}'(k \cdot (a_q \cdot b_p - a_p \cdot b_q)). \end{aligned} \tag{11}$$

A5. Upon receipt of the message E_m from party B, decrypt and acquire the message D_m, where $\mathcal{D}'$ denotes the variant Paillier decryption (4) with K_s^A.

$$D_m = \mathcal{D}'(E_m) = k \cdot (a_q \cdot b_p - a_p \cdot b_q). \tag{12}$$

A6. Determine the relationship between a, b by computing

$$b - a = \frac{b_p}{b_q} - \frac{a_p}{a_q} = \frac{a_q b_p - a_p b_q}{a_q \cdot b_q} = \frac{D_m}{k \cdot a_q \cdot b_q}. \tag{13}$$

Given that $a_q, b_q, k > 0$, party A obtains the test result, which is equivalent to the relationship between D_m and 0.

A7. Transmit the result of the relationship test to party B.

The above protocol, denoted by PPNC (Privacy-Preserving Numbers Comparison), achieves secure two-party computation of the sign function within the domain of bounded rational numbers. Given the discontinuous nature of the sign function at zero, an alteration in the relationship between the two private values may result in a discontinuous change in the protocol's output, leading to chattering phenomena of the dynamic system. To address such discontinuities, the boundary layer method is commonly adopted [13]. In the context of this paper, accordingly, a monitored space is introduced.

***Definition* 3**. In the three-dimensional orthogonal coordinate system with Agent i as the origin, a monitored space of Agent i is a cube centered at the origin with all faces perpendicular to the coordinate axes. The distance from Agent i to each face of the cube is defined as the monitored space parameter D.

***Assumption* 3**. For any Agent i, j in a first- or second-order system, the state values of Agent j are detectable by Agent i, if Agent j is in the monitored space of Agent i.

When two agents are within each other's monitored space, the necessity for privacy preservation of the states is reduced. The parameter D is designed, such that the initial position of an agent can be outside the monitored space of other agents.

The protocol is devised with the output values considering the assumption of the monitored space with the parameter D,

$$\mathrm{PPNC}(a,b) = \begin{cases} \mathrm{sign}(a-b), & |a-b| \geq D, \\ (a-b)/D, & |a-b| < D, \end{cases} \tag{14}$$

In addition, PPNC can be extended to test the relationship between two private vectors $\mathbf{a}, \mathbf{b}$ of the same dimension, resulting in a vector of the same dimension.

B. Control Law Design

Inspired by [13], two privacy-preserving controllers are designed. For a first-order system (7), the privacy-preserving average controller is designed with $\alpha > 0$,

$$\mathbf{u}_i(k) = \alpha \sum_{j \in N_i} a_{ij} \cdot \mathrm{PPNC}(\mathbf{x}_j(k), \mathbf{x}_i(k)), \tag{15}$$

and for a second-order system (8), the privacy-preserving rendezvous controller is designed with $\beta, \gamma > 0$,

$$\mathbf{u}_i(k) = \gamma \sum_{j \in \mathbb{V}} a_{ij} \cdot \mathrm{PPNC}(\mathbf{s}_j(k), \mathbf{s}_i(k)) - \beta \cdot \mathbf{v}_i(k), \tag{16}$$

where a_{ij} is the $(i,j)^{th}$ element of the adjacency matrix and the intermediate variable $\mathbf{s}_i(k) = \beta \cdot \mathbf{p}_i(k) + \mathbf{v}_i(k)$.

V. THEORETICAL ANALYSIS

A. Consensus And Stability

1) First-Order: The theorem below proves the stability.

***Theorem* 2**. The first-order multi-agent system (7) with bounded initial values and a connected undirected graph reaches the average consensus under the controller (15).

Proof. Define the sum of the states $\mathbf{S}_1(k) = \sum_{i \in \mathbb{V}} \mathbf{x}_i(k)$. Since $\forall i, j \in \mathbb{V}$, $\mathrm{PPNC}(\mathbf{x}_i, \mathbf{x}_j) = -\mathrm{PPNC}(\mathbf{x}_j, \mathbf{x}_i)$, the increment of the sum of the states is zero,

$$\begin{aligned} \Delta\mathbf{S}_1(k) &= \mathbf{S}_1(k+1) - \mathbf{S}_1(k) = \sum_{i \in \mathbb{V}} \mathbf{x}_i(k+1) - \mathbf{x}_i(k) \\ &= \alpha \cdot \epsilon \sum_{i,j \in \mathbb{V}} a_{ij} \cdot \mathrm{PPNC}(\mathbf{x}_j, \mathbf{x}_i) = \mathbf{0}. \end{aligned} \tag{17}$$

Thus, $\mathbf{S}_1$ is constant. With $\bar{\mathbf{x}} = \frac{\mathbf{S}_1}{n}$, a Lyapunov function $V_1 : \mathbb{R}^{3n} \to \mathbb{R}$ for the n-agent first-order system is defined,

$$V_1(k) = \frac{1}{2} \sum_{i \in \mathbb{V}} (\mathbf{x}_i(k) - \bar{\mathbf{x}})^T \cdot (\mathbf{x}_i(k) - \bar{\mathbf{x}})). \tag{18}$$

According to the system description (7) and the controller (15), with defining the error on the state as $\mathbf{e}_i(k) = \mathbf{x}_i(k) - \bar{\mathbf{x}}$, the increment of the Lyapunov function $\Delta V_1(k)$ is computed,

$$\begin{aligned} \Delta V_1(k) &= \frac{1}{2} \sum_{i \in \mathbb{V}} (\mathbf{e}_i(k+1)^T \cdot \mathbf{e}_i(k+1) - \mathbf{e}_i(k)^T \cdot \mathbf{e}_i(k)) \\ &= \frac{1}{2} \sum_{i=1}^{n} (2\mathbf{e}_i(k+1)^T \cdot \epsilon \cdot \mathbf{u}_i(k) - \epsilon^2 \mathbf{u}_i(k)^T \cdot \mathbf{u}_i(k)) \\ &= \alpha \cdot \epsilon \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} a_{ij} \cdot (\mathbf{x}_i(k+1) - \mathbf{x}_j(k+1))^T \\ &\quad \cdot \mathrm{PPNC}(\mathbf{x}_j(k), \mathbf{x}_i(k)) - \frac{\epsilon^2}{2} \sum_{i=1}^{n} \mathbf{u}_i(k)^T \mathbf{u}_i(k). \end{aligned} \tag{19}$$

An assumption is provided such that $\Delta V_1(k) \leq 0$.

***Assumption* 4**. The difference of the states of two agents between any two successive time instants is monotonic, i.e., the states satisfy that, for Agent $i, j \in \mathbb{V}$, $\forall k > 0$, if $\mathbf{x}_i(k) \neq \mathbf{x}_j(k)$, then with $\forall I \in \{X, Y, Z\}, x_{i,I}$ denoting the component of $\mathbf{x}_i$ in the I-direction,

$$(x_{i,I}(k+1) - x_{j,I}(k+1)) \cdot (x_{i,I}(k) - x_{j,I}(k)) > 0. \tag{20}$$

Assumption 4 is achievable by setting the appropriate parameter α in the controller (15). For further detailed discussions on Assumption 4, see Section VII in [14].

With Assumption 4, for $i, j \in \mathbb{V}$, when $\mathbf{x}_i(k) \neq \mathbf{x}_j(k)$,

$$(\mathbf{x}_i(k+1) - \mathbf{x}_j(k+1))^T \cdot \mathrm{PPNC}(\mathbf{x}_j(k), \mathbf{x}_i(k)) < 0. \tag{21}$$

Therefore, $\Delta V_1(k) \leq 0$. $\Delta V_1(k) = 0$ if and only if $\forall i, j \in \mathbb{V}$, $\mathbf{x}_i(k) = \mathbf{x}_j(k)$. The increment of the Lyapunov function $\Delta V_1(k)$ is negative definite. Meanwhile, $V_1(k)$ is radially unbounded, i.e., $\forall i \in \mathbb{V}$, when $||\mathbf{x}_i(k)|| \to \infty$, $V_i(k) \to \infty$. The Lyapunov function $V_1(k)$ is positive definite and reaches 0 when and only when $\forall i \in \mathbb{V}$, $\mathbf{x}_i(k) - \bar{\mathbf{x}} = 0$. According to the discrete-time Lyapunov stability theorem [15] (Th 13.2), all states converge to the average of the initial values $\bar{\mathbf{x}}$. Thus, the first-order system reaches the average consensus. ■

2) Second-Order: The theorem below proves the stability.

***Theorem* 3**. The second-order multi-agent system (8) with bounded initial values and a connected undirected graph reaches the rendezvous point under the controller (16).

Proof. The proof is addressed by the following two steps:
1) The variable $\mathbf{s}_i(k) = \beta \cdot \mathbf{p}_i(k) + \mathbf{v}_i(k)$ converges to $\mathbf{0}$.
2) The system states reach the rendezvous point.

First, the increment of the intermediate variable $\Delta\mathbf{s}_i(k)$ is

$$\begin{aligned} \Delta\mathbf{s}_i(k) =& \mathbf{s}_i(k+1) - \mathbf{s}_i(k) \\ =& \beta \cdot (\mathbf{p}_i(k+1) - \mathbf{p}_i(k)) + \mathbf{v}_i(k+1) - \mathbf{v}_i(k) \\ =& \gamma \cdot \epsilon \sum_{j \in \mathbb{V}} a_{ij} \cdot \mathrm{PPNC}(\mathbf{s}_j(k), \mathbf{s}_i(k)). \end{aligned} \tag{22}$$

Define the sum of the intermediate variables $\mathbf{S}_2(k) = \sum_{i \in \mathbb{V}} \mathbf{s}_i(k)$, and its increment $\Delta\mathbf{S}_2(k) = 0$, which implies $\mathbf{S}_2$ is constant. With $\bar{\mathbf{s}} = \frac{\mathbf{S}_2}{n}$, the Lyapunov function $V_2 : \mathbb{R}^{3n} \to \mathbb{R}$ is defined for the n-agent second-order system,

$$V_2(k) = \frac{1}{2} \sum_{i,j \in \mathbb{V}} (\mathbf{s}_i(k) - \bar{\mathbf{s}})^T \cdot (\mathbf{s}_j(k) - \bar{\mathbf{s}}). \tag{23}$$

The Lyapunov function $V_2(k)$ and its increment $\Delta V_2(k)$ exhibit identical forms as (18) and (19) respectively, as stated in Theorem 2. Thus, given the same assumption and argument, which are omitted for the sake of brevity, the intermediate variable $\mathbf{s}_i(k)$, analogous to the states of the first-order system $\mathbf{x}_i(k)$, reaches the average consensus.

According to the findings of [13], for any Agent i and j, when Agent j enters the monitored space of Agent i, $\mathbf{s}_j(k) - \mathbf{s}_i(k)$ asymptotically converges to zero. This is due to the fact that in the monitored space $\mathrm{PPNC}(\mathbf{s}_j(k), \mathbf{s}_i(k))$, which is the component of Agent j in the controller $\mathbf{u}_i(k)$, is proportional to $\mathbf{s}_j(k) - \mathbf{s}_i(k)$.

Define the average of the intermediate variables $\bar{\mathbf{s}}(k) = \sum_{i\in\mathbb{V}} \mathbf{s}_i(k)/n$. There exist scalars $\beta_0, C_X, C_Y, C_Z > 0$, and a time instant k_0, such that $\mathbf{s}_i(k)$ satisfies $\forall k > k_0$ with $\forall I \in \{X, Y, Z\}$, $s_{i,I}(k), \bar{s}_I(k)$ denoting the component of $\mathbf{s}_i(k), \bar{\mathbf{s}}(k)$ in the I-direction,

$$|s_{i,I}(k) - \bar{s}_I(k)| \leq C_I \cdot \exp(-\beta_0 \cdot k \cdot \epsilon). \tag{24}$$

Define the average of the position $\bar{\mathbf{p}}(k) = \sum_{i\in\mathbb{V}} \mathbf{p}_i(k)/n$ and the average of the velocity $\bar{\mathbf{v}}(k) = \sum_{i\in\mathbb{V}} \mathbf{v}_i(k)/n$. By solving the difference inequality (24), given that $\beta, \beta_0 > 0$, with $\forall I \in \{X, Y, Z\}$, $p_{i,I}(k), \bar{p}_I(k), v_{i,I}(k), \bar{v}_I(k)$ denoting the component of $\mathbf{p}_i(k), \bar{\mathbf{p}}(k), \mathbf{v}_i(k), \bar{\mathbf{v}}(k)$ in the I-direction,

$$\lim_{k\to\infty} |p_{i,I}(k) - \bar{p}_I(k)| = 0, \tag{25}$$

$$\lim_{k\to\infty} |v_{i,I}(k) - \bar{v}_I(k)| = 0. \tag{26}$$

Since the sum of the intermediate variables is constant,

$$\sum_{i\in\mathbb{V}} (\beta \cdot \mathbf{p}_i(k) + \frac{\mathbf{p}_i(k+1) - \mathbf{p}_i(k)}{\epsilon}) = \mathbf{S}_2. \tag{27}$$

Solving the equation (27), there exists a constant vector $\mathbf{C}'$ of the same dimension, such that $\mathbf{p}_i(k)$ satisfies

$$\sum_{i\in\mathbb{V}} \mathbf{p}_i(k) = \frac{\mathbf{S}_2}{\beta} + \mathbf{C}' \cdot \exp(-\beta \cdot k \cdot \epsilon), \tag{28}$$

$$\sum_{i\in\mathbb{V}} \mathbf{v}_i(k) = -\beta \cdot \mathbf{C}' \cdot \exp(-\beta \cdot k \cdot \epsilon). \tag{29}$$

The rendezvous point is reached, as the states achieve

$$\lim_{k\to\infty} ||\mathbf{p}_i(k) - \bar{\mathbf{p}}(k)|| = 0, \ \lim_{k\to\infty} ||\mathbf{v}_i(k)|| = 0, \tag{30}$$

with $\lim_{k\to\infty} \bar{\mathbf{p}}(k) = \frac{\mathbf{S}_2}{n\cdot\beta} = \frac{1}{n}\sum_{j=1}^{n}(\mathbf{p}_j(0) + \frac{\mathbf{v}_j(0)}{\beta})$. ■

B. Privacy Under Inference

When Agent A initiates Protocol 1, Agent B receives the message containing the value of $\mathcal{E}'(k(a_p \cdot b_q - a_q \cdot b_q))$ in Protocol 1 Step B3. Agent B lacks information regarding privacy without knowledge of Agent A's private key.

When Agent B initiates Protocol 1, in the worst scenario, the private value a remains unaltered, providing Agent B with multiple opportunities to deduce the private number.

***Theorem* 4**. When Agent B initiates multiple rounds of Protocol 1 with Agent A at a series of times $h+1, \cdots, h+l$, and $h, l \in \mathbb{Z}^+$, Agent B cannot infer the privacy of Agent A, even if the private value a remains unchanged.

Proof. Protocol 1 is executed l-times. With $a,\ k_{h+1}, \cdots, k_{h+l}, a_{p,h+1}, a_{p,h+l}, \cdots, a_{q,h+1}, a_{q,h+l}$, in total $3l+1$ unknowns, Agent B decrypts l messages, acquiring the values of $D_{m,h+1}, \cdots, D_{m,h+l}$ and establish $2l$ equations

$$\begin{cases} D_{m,h+1} = k_{h+1}(b_{p,h+1}a_{q,h+1} - b_{q,h+1}a_{p,h+1}), \\ \cdots \\ D_{m,h+l} = k_{h+l}(b_{p,h+l}a_{q,h+l} - b_{q,h+l}a_{p,h+l}), \\ a \approx a_{p,h+1}/a_{q,h+1},\ \cdots,\ a \approx a_{p,h+l}/a_{q,h+l}. \end{cases} \tag{31}$$

The number of unknowns $3l+1$ exceeds the number of equations $2l$. Moreover, as k is generated randomly and concealed locally, it precludes other agents from getting valuable information from D_m. The private value a is unsolvable, so it is considered to be confidential. ■

C. Features and Performance

Section C discusses the features and performance. A comparison between the scheme in this study and those in studies [6], [7] is provided in Table 1.

Table 1. Comparison on the features and the performance.

	Scheme in [6], [7]	**Our scheme**
Controller type	Time-varying topology PD controller	Chattering-free sliding-mode controller
Consensus property	1^{st}: average consensus 2^{nd}: dynamic consensus	1^{st}: average consensus 2^{nd}: rendezvous
Privacy-preserving mechanism	Random coupling weights $a_{ij} = a_{j\to i} \cdot a_{i\to j}$ with random $a_{j\to i}$, $a_{i\to j}$	Privacy-preserving two-party relationship test protocol: PPNC
Complexity	$\mathcal{O}(\lvert N_i\rvert \cdot l)$ 4 communications / round	$\mathcal{O}(\lvert N_i\rvert \cdot l)$ 3 communications / round

Protocol 1 is initiated with a predetermined cost for the key generation process, followed by steps that are primarily dominated by encryption and decryption, thereby rendering their complexity of utmost significance. If $|N_i|$ is the number of neighboring nodes, and l is the bit length of the public key, the overall computational complexity of Protocol 1 is $\mathcal{O}(|N_i| \cdot l)$. The complexity of the privacy-preserving algorithm, as proposed in [6], [7], is computed using the same methodology, yielding an identical result of $\mathcal{O}(|N_i| \cdot l)$.

Regarding the communication complexity, the [6], [7] scheme needs 4 communications per round, whereas our scheme needs 3 communications per round. On the negative side, the convergence rate of our scheme is relatively slow.

VI. NUMERICAL VERIFICATION

The proposed controllers are subjected to numerical simulations. $\{X, Y, Z\}$ is the orthogonal coordinate basis.

Table 2. Initial states in simulation.

	First-order System			**Second-order System**					
	x_i^X	x_i^Y	x_i^Z	p_i^X	p_i^Y	p_i^Z	v_i^X	v_i^Y	v_i^Z
1	-17	12.5	20.5	-17	12.5	20.5	1.5	2.5	-0.1
2	-11	16.2	10.8	-11	16.2	10.8	-1.8	6.2	-1
3	2.3	-16	40.2	2.3	-16	40.2	5.3	-1.7	2.3
4	12.9	17.5	0	12.9	17.5	0	0	1.3	2.1
5	18.2	5	-39	18.2	5	-39	-3.5	-5.8	3.2

Considering a first-order (7) and a second-order (8) system of 5 agents, under the controller (15) and (16) respectively, the systems are assigned arbitrarily the initial conditions and the topology in Table 2 and in Figure 1. The gains of the controllers are set to $\alpha = 0.8, \beta = 1.2, \gamma = 0.8$. The system is discretized with a step size of $\epsilon = 0.01$. The monitored space parameter is set as $D = 0.1$.

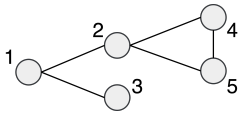

Fig. 1. The undirected graph of the 5-agent systems.

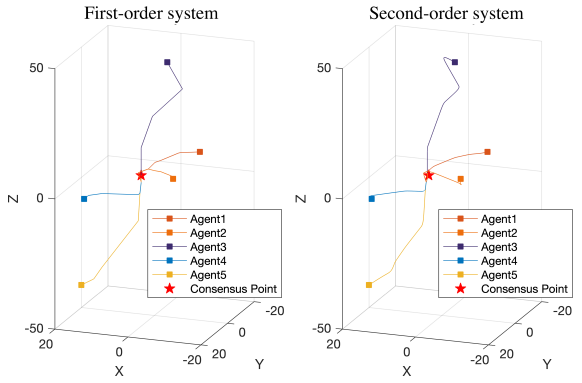

Fig. 2. Consensus trajectories of 5-agent systems under the controllers (15) and (16).

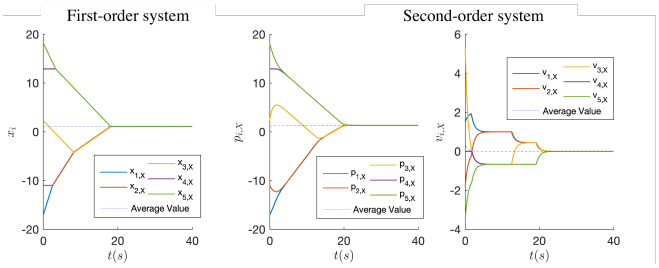

Fig. 3. The states of the agents converge to the consensus in the X-direction of the first- and second-order systems.

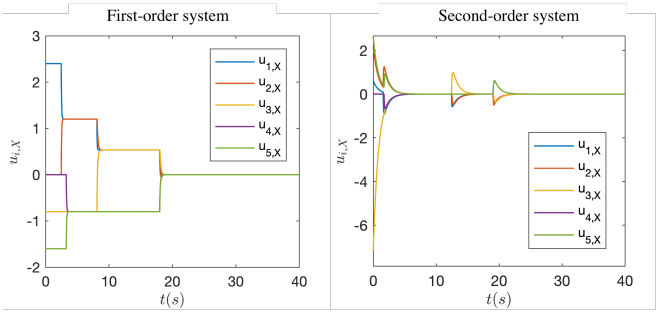

Fig. 4. Chattering-free control inputs in the X-direction of the first- and second-order systems.

Figure 2 depicts that under the proposed controllers, the systems reach a consensus in each dimension. Figure 3 presents the results of the state variation in the X-direction, which demonstrates that Agents in the first-order system reach the average consensus, and Agents in the second-order system reach the rendezvous point. Figure 4 displays the control inputs in the X-direction of first- and second-order system, which have no chattering phenomenon.

VII. CONCLUSION

A privacy-preserving two-party relationship test protocol is proposed in this study. Based on this protocol, privacy-preserving controllers are designed for first-order and second-order systems. It is demonstrated that the first-order system reaches the average consensus and the second-order system reaches the rendezvous point while preserving private initial states under the proposed controllers. Notably, our approach effectively avoids the chattering problem of the control input, which is a limitation of previous privacy-preserving schemes. An event-triggered mechanism and a scheme under a directed graph will be explored as potential directions for further improvement.

REFERENCES

[1] B. Hemenway, S. Lu, R. Ostrovsky, and W. Welser Iv, "High-precision secure computation of satellite collision probabilities," in *International Conference on Security and Cryptography for Networks*. Springer, 2016, pp. 169–187.

[2] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2016.

[3] J. Ke, J. Wang, and J.-F. Zhang, "Differentiated output-based privacy-preserving average consensus," *IEEE Control Systems Letters*, vol. 7, pp. 1369–1374, 2023.

[4] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4711–4716, 2019.

[5] J. Zhang, J. Lu, and X. Chen, "Privacy-preserving average consensus via edge decomposition," *IEEE Control Systems Letters*, vol. 6, pp. 2503–2508, 2022.

[6] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4035–4049, 2019.

[7] W. Fang, M. Zamani, and Z. Chen, "Secure and privacy preserving consensus for second-order systems based on paillier encryption," *Systems & Control Letters*, vol. 148, p. 104869, 2021.

[8] M. Marcantoni, B. Jayawardhana, M. P. Chaher, and K. Bunte, "Secure formation control via edge computing enabled by fully homomorphic encryption and mixed uniform-logarithmic quantization," *IEEE Control Systems Letters*, vol. 7, pp. 395–400, 2022.

[9] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conf on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.

[10] Goldreich, "Foundations of cryptography: Volume 1, basic tools," *Cambridge University Press*, 2001.

[11] A. C. Yao, "Protocols for secure computations," in *23rd annual conf on foundations of computer science*. IEEE, 1982, pp. 160–164.

[12] L. M. Gong, S. D. Li, L. H. Shao, T. Xue, and D. Wang, "Protocols for secure test on relationship on number axis," *Journal of Software*, vol. 31, no. 12, pp. 3950–3967, 2020.

[13] M. Doostmohammadian, "Single-bit consensus with finite-time convergence: Theory and applications," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 4, pp. 3332–3338, 2020.

[14] W. M. Haddad, J. Lee, and S. P. Bhat, "Asymptotic and finite time semistability for nonlinear discrete-time systems with application to network consensus," *IEEE Transactions on Automatic Control*, 2022.

[15] W. M. Haddad and V. Chellaboina, *Nonlinear dynamical systems and control:a Lyapunov-based approach*. Princeton university press, 2008.