SCIENCE CHINA
Information Sciences

• REVIEW •

April 2025, Vol. 68, Iss. 4, 141201:1–141201:17
https://doi.org/10.1007/s11432-024-4328-1

Privacy-preserving filtering, control and optimization for industrial cyber-physical systems

Derui DING[1,2], Qing-Long HAN[2*], Xiaohua GE[2], Xian-Ming ZHANG[2] & Jun WANG[3]

[1]*Department of Control Science and Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China*
[2]*School of Engineering, Swinburne University of Technology, Melbourne VIC 3122, Australia*
[3]*Department of Computer Science, City University of Hong Kong, Hong Kong 999077, China*

Received 23 November 2024/Revised 20 January 2025/Accepted 6 March 2025/Published online 13 March 2025

Abstract Industrial cyber-physical systems closely integrate physical processes with cyberspace, enabling real-time exchange of various information about system dynamics, sensor outputs, and control decisions. The connection between cyberspace and physical processes results in the exposure of industrial production information to unprecedented security risks. It is imperative to develop suitable strategies to ensure cyber security while meeting basic performance requirements. From the perspective of control engineering, this review presents the most up-to-date results for privacy-preserving filtering, control, and optimization in industrial cyber-physical systems. Fashionable privacy-preserving strategies and mainstream evaluation metrics are first presented in a systematic manner for performance evaluation and engineering implementation. The discussion discloses the impact of typical filtering algorithms on filtering performance, specifically for privacy-preserving Kalman filtering. Then, the latest development of industrial control is systematically investigated from consensus control of multi-agent systems, platoon control of autonomous vehicles as well as hierarchical control of power systems. The focus thereafter is on the latest privacy-preserving optimization algorithms in the framework of consensus and their applications in distributed economic dispatch issues and energy management of networked power systems. In the end, several topics for potential future research are highlighted.

Keywords industrial cyber-physical systems, privacy preservation, distributed control, distributed optimization, power systems

Citation Ding D R, Han Q-L, Ge X H, et al. Privacy-preserving filtering, control and optimization for industrial cyber-physical systems. Sci China Inf Sci, 2025, 68(4): 141201, https://doi.org/10.1007/s11432-024-4328-1

1 Introduction

Industrial cyber-physical systems have emerged in the last decade, mainly due to the extensive use of advanced information technology. This type of system closely integrates physical processes with cyberspace, enabling real-time exchange of various information about system dynamics, sensor outputs, and control decisions [1, 2]. In contrast to traditional networked control systems, such a system is equipped with sensing, computing, or communication capabilities, taking advantage of the close deployment of various network devices, sensing units, computing devices, and software systems. The performance analysis and design framework has been utilized in several promising industrial systems, such as transportation networks, energy systems, water/gas distribution networks, and unmanned factories. For instance, a learning-based co-design framework of edge sensing and control was developed in [3] and was applied to the personalized production of laminar cooling. A federated control framework associated with potential applications to smart buildings was established in [4] to generate a trustable environment for secure data sharing and performance optimization. There is no doubt that industrial cyber-physical systems are the cornerstone of the so-called 4th industrial revolution, and are driving industrial production to digital and intelligent transformation [5].

Industrial cyber-physical systems are usually characterized by their large scale, geographical dispersion, federated structure, cooperative operation, and life-critical nature, achieving real-time monitoring and closed-loop control through the use of embedded and networked sensors and actuators [1]. Besides

* Corresponding author (email: qhan@swin.edu.au)

systematic architecture design, software development and decision algorithm design, model-based performance analysis and parameter design are essential for gaining a better understanding of system dynamic behaviours and evolution mechanisms, while also achieving and maintaining system stability and control accuracy. Enslaved to the limitation of geographic space and various resources, model-based investigations of industrial cyber-physical systems focus on (1) distributed parameter design to achieve reliability and scalability requirements [6–9], (2) impact analysis of various communication scheduling strategies to reduce the consumption of communication resources [10–13], and (3) actively or passively safe and secure defense to avoid the effect from attacks or faults [14–17]. Thus, some outstanding outcomes, specifically under communication scheduling, have emerged over the past decade. For instance, a novel co-design scheme of both the admissible cooperative adaptive cruise controller and the desired scheduling policy was developed in [11] for automated vehicles with diverse spacing policies. As one of the representative results concerning the time-varying systems with stochastic protocol, Ref. [18] proposed a novel filtering scheme to handle the effects induced by protocol scheduling and high-rate communication scheme, and revealed the relationship between scheduling behaviours and high-rate communication by using the mapping method.

Cyber security cannot be ignored and security protection is urgent to avoid immeasurable losses, although industrial cyber-physical systems give rise to several advantages and receive lots of successful applications in practical engineering. The interconnection of cyberspace and physical processes significantly increases the exposure of industrial production information to unprecedented security risks [19–21]. Malicious adversaries may make use of intrinsic vulnerabilities of installed software and communication networks to disrupt production processes, destroy important facilities, and steal critical industrial data, which consequentially lead to economic and social impacts and even human casualties. Claroty, a company that offers protection for cyber-physical systems, reported that over USD 1 million was lost by one in four organizations using CPS in the past year because of cyber attacks. According to the report of Cybersecurity Ventures, the financial impact of global cybercrime is increasing at a 15% annual rate, and will reach USD 10.5 trillion annually by 2025 [22]. In general, information security encompasses physical security, cyber security, application security, and data security. Data security focuses primarily on confidentiality, integrity, and availability of information. In this way, the industrial cyber-physical system is shielded from or relieved from accidental or malicious damages, changes, and disclosures, allowing it to function reliably and normally. Considering availability, various models of denial of service attacks have been developed to describe the attack behaviour, and lots of interesting results about control and filtering have been reported in [23] based on the viewpoint of passive attenuation and in [24] with the perspective of active compensation embedded attack detection. When focusing on integrity, various outstanding studies disclose the impact on system performances from deception attacks in [25] or replay attacks in [26] and handle the corresponding challenges in parameter design. Some systematic and profound surveys have been made in [27,28], and received ever-increasing research attention. Recently, the detection approaches and defense mechanisms have been systematically reviewed in [29] for system recovery from attacks.

When investigating confidentiality, several interesting surveys have been reported for the development of privacy-preserving strategies and their applications. For instance, the security and privacy of vehicular networks were discussed in [30] via anonymous authentication schemes implemented by five pseudonymity mechanisms, and privacy-preserving computation was addressed in [31] under cloud or fog environments from the viewpoint of big data. Homomorphic encryption schemes and their implementation are fully surveyed in [32]. Profound confidentiality analysis from control engineering perspectives should fully consider dynamical behaviours or optimization models of industrial cyber-physical systems and reasonable mathematical descriptions of adopted strategies. Recently, a comprehensive review [33] offers a primary analysis of privacy-preserving control and filtering of networked control systems from the viewpoint of control theory. To the best of the authors' knowledge, there is a paucity of a detailed survey of the state-of-the-art results in privacy preservation for model-based industrial cyber-physical systems. It is thus desirable to systematically review what developments have been received recently in the field of model-based industrial cyber-physical systems with urgent privacy-preserving requirements, and further identify what challenges need to be handled. To this end, this paper devotes itself to offering a survey of the up-to-date results for privacy-preserving filtering, control, and optimization; see Figure 1 for the organization. Specifically, performance evaluation and engineering implementation are presented with the presentation of common privacy-preserving strategies and evaluation metrics. A summary of typical filtering strategies is provided and some effects of filtering are briefly discussed. The latest advancement is systematically evaluated from three perspectives: consensus control, platoon control, and hierarchical

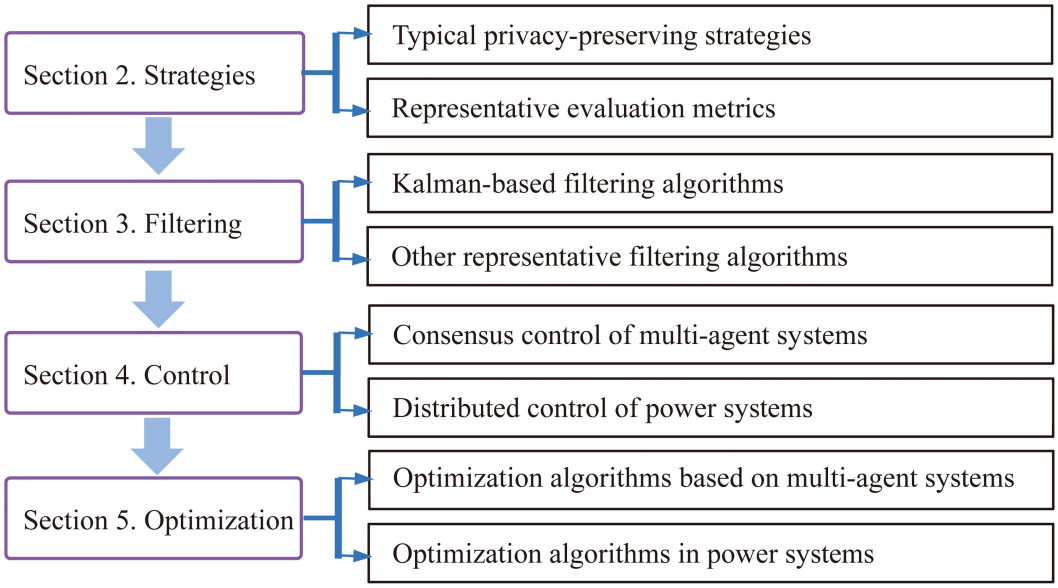

Figure 1 (Color online) Structure of this survey.

control. Furthermore, privacy-preserving optimization algorithms are summarized, specifically for economic dispatch issues and energy management of networked power systems. Finally, some challenging issues give rise to highlight future research.

2 Privacy-preserving strategies and evaluation metrics

In this section, the fashionable privacy-preserving strategies and related evaluation metrics are systematically reviewed for industrial cyber-physical systems, and their characteristics are discussed briefly.

2.1 Privacy-preserving strategies

According to the adopted protection mechanisms, typical privacy-preserving strategies can be roughly divided into three categories, namely, (i) the cryptography based approach, (ii) the data perturbation based approach, as well as (iii) algebraic transformation based approaches.

Under cryptography-based policies, the sensitive data is usually encrypted to form a ciphertext by resorting to some elaborately algebraic operations, and this ciphertext is then reliably decrypted by receivers with the help of the corresponding decryption algorithm. To realize such policies, private keys generally need to be established in advance by cipher algorithms for communication participants, including symmetric, asymmetric or hybrid cipher algorithms [34]. There is no doubt that eavesdroppers cannot effectively decrypt the information because they do not have a crucial encryption scheme or private keys. Furthermore, cipher algorithms are usually resource-consuming and could cost lots of computational resources. The privacy level is commonly dependent on the difficulty of private keys cracking.

Homomorphic encryption, a kind of special encryption scheme, permits any third party to operate on the encrypted data without decrypting it in advance and hence is receiving an ever-increasing research and application concern. Specifically, if there exists an encryption algorithm Enc and its corresponding decryption algorithm Dec such that $\mathrm{Dec}(\mathrm{Enc}(m_1) \star \mathrm{Enc}(m_2)) = m_1 \star m_2$ for two plaintext data m_1 and m_2, this encryption algorithm is regarded as a homomorphic encryption algorithm over the operation "$\star$" [32], where "$\star$" stands for predetermined operations, such as addition, multiplication, and exclusive OR. For its encryption algorithm, a key generator is of the essence to generate a private and public key pair for the asymmetric cases or a single key for the symmetric cases. Particularly, encryption and decryption can utilize the same key for symmetric cases or the different keys for asymmetric cases. For example, the encryption algorithm in Paillier encryption is adopted as

$$c = \mathrm{Enc}(m) = g^m r^n (\mathrm{mod}\ n^2),$$

Algorithm 1 Paillier cryptosystem.

1: Key generation.
▲ Choose two large prime numbers p and q ($p \neq q$) such that $\gcd(pq, (p-1)(q-1)) = 1$;
▲ Compute $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$;
▲ Select a random integer $r \in \mathbb{Z}_{n^2}^*$ by checking $\gcd(n, \mathfrak{L}(r^{\lambda \bmod n^2}) = 1$, where $\mathbb{Z}_{n^2}^*$ is a multiplicative subgroup of integers modulo n^2;
▲ Compute the modular multiplicative inverse $v = (\mathfrak{L}(r^{\lambda} \bmod n^2))^{-1} \bmod n$, where $\mathfrak{L}(x) = (x-1)/n$;
▲ Generate the public key (n, r) and the private key (λ, v).
2: Data encryption ($\mathrm{Enc}(m)$) and transmission (c).
▲ Choose a random integer g (satisfying $g \in [0, n)$, $g \in \mathbb{Z}_{n^2}^*$ and $\gcd(g, n) = 1$);
▲ Generate the ciphertext $c = \mathrm{Enc}(m) = r^m g^n \bmod n^2$;
▲ Transmit the ciphertext c.
3: Data collection (c) and decryption ($\mathrm{Dec}(c)$).
▲ Receive the ciphertext c;
▲ Calculate $m = \mathrm{Dec}(c) = \mathfrak{L}(c^{\lambda} \bmod n^2)v \bmod n$.

Algorithm 2 Noise-injected approaches.

1: Noise selection.
▲ Choose injected noises w, such as general amplitude-attenuated noises and Laplace noises.
2: Data encryption and transmission (original data m).
▲ Generate the ciphertext $c = m + w$;
▲ Transmit the ciphertext c.
3: Data collection and decryption (adopted data m').
▲ Receive the ciphertext c;
▲ Adopt $m' = c$.

and the decryption algorithm is designed as

$$\mathrm{Dec}(c) = \mathfrak{L}(c^{\lambda} \bmod n^2)v \bmod n,$$

where c is the ciphertext of the corresponding data m, the number r is randomly chosen and the private key pair (n, r) and the public key (λ, v) are received by a key generator such that $\gcd(pq, (p-1)(q-1)) = 1$ with $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$, and a random integer r satisfying $\gcd(n, \mathfrak{L}(g^{\lambda \bmod n^2})) = 1$. Here, lcm() represents the least common multiple and gcd() stands for the greatest common divisor. The pseudocode of this scheme can be found in Algorithm 1. It should be pointed out that there is no information loss for decrypted data and hence the system performance will not be sacrificed. More details about this kind of algorithm can be found in the survey [32] and the related literature [35].

Under the data perturbation policies, data security is generally guaranteed by injecting noises into sensitive data (forming ciphertexts) to maximize the distortion of eavesdroppers' inference or give rise to indistinguishability between real data and inferred ones in probability [36, 37]. The pseudocode of this scheme can be found in Algorithm 2. For instance, a hybrid privacy policy was provided in [38] to modulate the data aggregation process by utilizing a set of generated super-increasing sequence and random offsets, and in [39] to perturb the transmitted public sub-states by injecting an amplitude-attenuated and time-correlated noise sequence. Furthermore, a set of random numbers was generated and shared with neighbours as a private key, which was added and subtracted in the consensus process in [40]. In addition, one representative method is the renowned differential privacy, which realizes the privacy of systems by adding designed random noises (such as Laplace noises) to the exchanged data. Different from the above noises, the injected random noises need to satisfy some specific constraints, such as bounded sum or integral over time [41] and an exponentially decaying covariance [42, 43]. Obviously, the bundled constraint is to ensure that the desired system performance will not be affected by injected noises while achieving privacy. Surely, the design of noise sequences will be more freedom if the system performance can be sacrificed a little and meanwhile privacy level could be increased.

Different from the above two kinds of strategies, the algebraic transformation-based approaches rely on introduced transformation maps, dynamic quantization, as well as state decomposition. Usually, the transformation map plays the role of a mask, rendering the locally real data indiscernible by eavesdroppers. The map f is usually a continuously differentiable time-varying function with five basic requirements [44] and some interesting output masks [45, 46] are shown as follows:

- linear masks: $c = f(t, m, \pi) = (1 + \varphi \mathrm{e}^{-\alpha t})m$,
- additive masks: $c = f(t, m, \pi) = m + \psi \mathrm{e}^{-\beta t}$,
- affine masks: $c = f(t, m, \pi) = \gamma(1 + \varphi \mathrm{e}^{-\alpha t})m$,
- vanishing affine masks: $c = f(t, m, \pi) = (1 + \varphi \mathrm{e}^{-\alpha t})(m + \psi \mathrm{e}^{-\beta t})$,

Algorithm 3 Mask-based approaches.

1: Selection of mask functions.
▲ Choose the parameter pair π, that is, $\{\varphi, \alpha\}$, $\{\psi, \beta\}$, $\{\gamma, \varphi, \alpha\}$ $\{\varphi, \alpha, \psi, \beta\}$, or $\{p_m, \varphi_m\}$ for different mask functions.
2: Masks and transmission (original data m).
▲ Generate the ciphertext $c = f(t, m, \pi)$;
▲ Transmit the ciphertext c.
3: Data collection and decryption (adopted data m').
▲ Receive the ciphertext c;
▲ Adopt $m' = c$ for linear, additive, or vanishing affine masks, or
▲ Adopt $m' = \gamma^{-1}c$ for affine masks, or
▲ Adopt $m' = p_m^{-1}(c) - \mathbb{E}\{\varphi_m\}$ for random affine masks.

Algorithm 4 State decomposition approaches.

1: Initial decomposition.
▲ Choose the substate m_2 from the set of all bounded real numbers for a system initial state;
▲ Calculate the substate $m_1 = 2m - m_2$.
2: Data encryption and transmission (original data m).
▲ Update the ciphertext $c = m_2$;
▲ Transmit the ciphertext c.
3: Data collection and decryption (adopted data m_2').
▲ Receive the ciphertext c;
▲ Adopt $m_2' = c$ from neighbor nodes, and m_1 and m_2 from the node itself;
▲ Generate new m_1 and m_2 via system dynamical [51] for the next moment.

- random affine masks: $c = f(t, m, \pi) = p_m(m + \varphi_m)$,

where c is the ciphertext of the corresponding data m, and the parameter pair π, regarded as a private mask, consists of $\{\varphi, \alpha\}$, $\{\psi, \beta\}$, $\{\gamma, \varphi, \alpha\}$ $\{\varphi, \alpha, \psi, \beta\}$, or $\{p_m, \varphi_m\}$. Here, p_m is an invertible function, φ_m is a random non-zero vector, and other parameters are predetermined positive scalars. The pseudocode of this scheme can be found in Algorithm 3.

To adapt to dynamic changes of transmitted data and reduce the coded information loss, some dynamic encryption schemes are developed by embedding the behaviour prediction of industrial cyber-physical systems, whose encoder with a linear system version [47] is as follows:

$$\begin{cases} \xi_0 = 0, \\ \dot{\xi}_t = A_c\xi_t,\ t \in (t_1,\ t_2), \\ \delta_{t_2} = q\left(\dfrac{m_{t_2} - \mathrm{e}^{A_c(t_2-t_1)}\xi_{t_1}}{g_{t_2}}\right), \\ \xi_{t_2} = \mathrm{e}^{A_c(t_2-t_1)}\xi_{t_1} + g_{t_2}\delta_{t_2}, \end{cases} \tag{1}$$

where A_c is the system matrix, ξ_t is an internal state of encryptors, g_t is a piecewise function serving as a dynamic encryption key, and $q(x)$ stands for a uniform quantiser. On the other hand, some lightweight encrypters were developed in the past few years to satisfy the real-time requirement, including state decomposition with the following restriction or its variants [48–50]:

$$2m = m_1 + m_2,\ m_1 \neq m_2,$$

where m is the protective state, and m_1 and m_2 can be regarded as two decomposed sub-states. Generally, these two sub-states for the system's initial value are bounded and randomly chosen from the real numbers set, and then are updated by resorting to system dynamical [51]. Here m_2 is the only sub-state that can be seen by its neighbors. The pseudocode of state decomposition can be found in Algorithm 4.

2.2 Evaluation metrics

According to their adopted mechanisms, one can find that the direct and mathematical representation of privacy-preserving strategies gives rise to some deviation between original data and corresponding ciphertexts. Hence, the essence of privacy evaluation is to discover the effect of interesting data from such a deviation. By doing so, let us introduce two data sets.

Two data sets $\mathcal{D} = \{d_s\}_{s=1}^n$ and $\mathcal{D}' = \{d_s'\}_{s=1}^n$ are said to be adjacent if there exists $i \in \{1, 2, \ldots, n\}$ such that $d_s \neq d_s'$ for $s = i$ and $d_s = d_s'$ for all $s \neq i$. In light of these data sets, one has the following privacy metrics [52–54].

Metric 1 (ε-differential privacy)**.** For adjacent data sets $\mathcal{D}$ and $\mathcal{D}'$, probability density $\mathbb{P}$, and output space $\mathcal{R}$ of privacy strategy $\mathcal{S}_p$, if there exists $\varepsilon \geqslant 0$ such that

$$\mathbb{P}\{\mathcal{S}_p(\mathcal{D}) \in \mathcal{R}\} \leqslant \mathrm{e}^{\varepsilon}\mathbb{P}\{\mathcal{S}_p(\mathcal{D}') \in \mathcal{R}\}, \tag{2}$$

then the privacy strategy $\mathcal{S}_p$ is ε-differential privacy.

Metric 2 ((ε, δ)-differential privacy)**.** For adjacent data sets $\mathcal{D}$ and $\mathcal{D}'$, probability density $\mathbb{P}$, and output space $\mathcal{R}$ of privacy strategy $\mathcal{S}_p$, if there exist $\varepsilon \geqslant 0$ and $\delta \geqslant 0$ such that

$$\mathbb{P}\{\mathcal{S}_p(\mathcal{D}) \in \mathcal{R}\} \leqslant \mathrm{e}^{\varepsilon}\mathbb{P}\{\mathcal{S}_p(\mathcal{D}') \in \mathcal{R}\} + \delta, \tag{3}$$

then the privacy strategy $\mathcal{S}_p$ is (ε, δ)-differential privacy.

In the above two metrics, the positive scalar ε is called the privacy budget. Generally speaking, the smaller the privacy budget, the greater the degree of privacy protection for data, but the poorer the availability of data. Obviously, differential privacy is actually a balance between the degree of privacy protection and data availability. Furthermore, Metric 2 can be regarded as a relaxed differential privacy, and δ is a small constant and is called the probability of failure. Obviously, the smaller the probability of failure, the greater the capability of privacy protection for data.

Similar to differential privacy, some data privacy metrics can be employed to evaluate the accuracy of inference of eavesdroppers. The inferred data could be the system's initial state x_0 [55] or the parameter $\theta \in \Theta$ of the privacy strategy $\mathcal{S}_p$ [41].

Metric 3 ((ε, σ)-data privacy)**.** For an initial state x_0, the adopted parameter θ, the collected information set $\mathbb{I}_t$ until instant t and the query strategy $\mathcal{Q}$ employed by eavesdroppers to estimate x_0 or θ, if the estimation probability satisfies

$$\mathbb{P}\{\mathcal{Q}(\mathbb{I}_t) - x_0\| \leqslant \varepsilon\} \leqslant \sigma, \tag{4}$$

or

$$\sigma = \max_{\mathcal{Q}(\mathbb{I}_t)\in\Theta} \mathbb{P}\{\mathcal{Q}(\mathbb{I}_t) - \theta\| \leqslant \varepsilon\}, \tag{5}$$

then the privacy strategy $\mathcal{S}_p$ is regarded as (ε, σ)-data privacy.

The above privacy reflects that the maximum probability is σ under that the difference between the actual value and its estimation is no larger than the given accuracy ε. For a fixed accuracy ε, the smaller the maximum probability σ, the greater the degree of privacy protection for data, but the poorer the availability of data. It should be pointed out that, besides probability, the measure of privacy can be the variance, or the mutual information $\mathfrak{I}$, and hence Eq. (4) can be replaced by

$$\mathbb{V}(\mathcal{Q}(\mathbb{I}_t) - x_0) > \sigma^2, \text{ or } \sigma = \mathfrak{I}(x_0, V) > \sigma_{\min}$$

with $V = \{\mathcal{Q}(\mathbb{I}_t), \mathbb{I}_t\}$; see [34, 56] for more details. As discussed in [41], there exists some possibility that the inferred value by eavesdroppers is close to the real one no matter what type of noise distribution is adopted in noise-injected schemes. However, the privacy probability cannot be directly evaluated by differential privacy or metrics based on mutual information. The metric of (ε, σ)-data privacy can better disclose the relationship between disclosure probability and inference accuracy.

Privacy in industrial cyber-physical systems generally reflects that, despite the system states being generally dynamic, eavesdroppers cannot acquire the practical system behaviour, while the predetermined performance of practical systems can be effectively guaranteed. Thus, a tradeoff exists between system performance and the need to counter eavesdroppers. In this case, there is a tradeoff between system performance and eavesdropper demand [57–59].

Metric 4. For encrypted data set $\mathcal{Y}_t$ until instant t received by both systems and eavesdroppers and the query strategies $\mathcal{Q}_s$ for considered systems and $\mathcal{Q}_e$ for eavesdroppers, if the relationship

$$\lim_{t\to\infty} \|\mathcal{Q}_s(\mathcal{Y}_e)\| \ll \lim_{t\to\infty} \|\mathcal{Q}_e(\mathcal{Y}_e)\|$$

holds, then the privacy strategy $\mathcal{S}_p$ is said to achieve the secrecy, where $\mathcal{Q}_s$ and $\mathcal{Q}_e$ should use the greatest similar rule except for the inaccessible private key. Particularly, (a) if $\lim_{t\to\infty} \|\mathcal{Q}_e(\mathcal{Y}_t)\| = \infty$ and $\lim_{t\to\infty} \|\mathcal{Q}_s(\mathcal{Y}_t)\| = b$ with a bounded scalar $b \geqslant 0$, then the privacy strategy $\mathcal{S}_p$ is ∞-diversity privacy [57, 59]; (b) if $\|\mathcal{Q}_e(\mathcal{Y}_t)\| > \gamma_e$ and $\|\mathcal{Q}_s(\mathcal{Y}_t)\| < \gamma_s$ ($\mathcal{Q}_s(\mathcal{Y}_t)$ could be covariance), the strategy $\mathcal{S}_p$ is private [60]; and (c) $\min \mathcal{Q}_s(\mathcal{Y}_e) - \sigma\mathcal{Q}_s(\mathcal{Y}_e)$, the privacy strategy $\mathcal{S}_p$ is suitable.

For distributed systems, privacy can also be guaranteed by the design of information transfer protocols or the arrangement of neighbour information of the collusion nodes. In this scenario, one of prevailing assumptions is that the nodes in considered systems have no completely covering neighbourhoods, that is, $\{\mathcal{N}_i \cup \{i\}\} \nsubseteq \{\mathcal{N}_j \cup \{j\}\}, \forall i, j = 1, 2, \ldots, n, i \neq j$, where $\mathcal{N}_i$ stands for the set of neighbours of node i. Furthermore, one has the following metric [51, 61].

Metric 5. For an initial state x_0, the collected information set $\mathbb{I}_t$ until instant t and the query strategy $\mathcal{Q}_e$ employed by eavesdroppers, the privacy of the initial state x_0 is protected if eavesdroppers with the worst-case malicious behaviours cannot find any range of this initial state, that is, $\|\mathcal{Q}_e(\mathbb{I}_t) - x_0\| \nleqslant \varepsilon$ for any constant ε.

Such a metric essentially reveals that the eavesdropper cannot infer the exact true value or the one within a specific range dependent on ε by the collected data with/without knowledge of privacy-preserving schemes. In other words, if a set of inference-induced equations has an infinite number of solutions, eavesdroppers could find it impossible to derive the exact value of sensitive information from the collected data, and privacy can be guaranteed.

Metric 6. For the interesting system state x_t, the collected information set $\mathbb{I}_t$ until instant t and the query strategy $\mathcal{Q}_e$ employed by eavesdroppers, the privacy of the system state x_t is protected if eavesdroppers cannot find its unbiased estimation, that is, $\mathbb{E}\{\mathcal{Q}_e(\mathbb{I}_t) - x_t\} \neq 0$.

3 Privacy-preserving filtering for industrial cyber-physical systems

The abundant deployment of various sensors and smart devices on industrial cyber-physical systems provides plenty of data for performance analysis and operation monitoring to maintain system stability, safety and reliability. Considering the interconnected feature, state estimation can be performed in a centralized or distributed manner, where measurements or locally processed information will be acquired or exchanged by global or local centres of supervisory control and data acquisition in real time. As such, it is necessary to develop privacy-preserving filtering algorithms that achieve the trade-off between filtering accuracy and system privacy.

For the steady case in smart grids, the relationship between the measurement y and the state x can be described by a map $y = h(x, v)$ where v is measurement noises. The purpose of filters (essentially optimization solvers) is to find a suitable vector $\hat{x}$ to minimize $\|y - H\hat{x}\|^2$ or $\|y - h(\hat{x})\|^2$ with $H = \partial h/\partial x|_{x=\hat{x}}$. According to this problem, a recursive estimation scheme with adaptive cooperation weights was proposed in [62], where a secure multiparty computation strategy was developed by introducing multiplicative/additive masks combined with the Paillier cryptosystem. The constraint condition of multiparty weighted zero-sum noises guarantees the calculation consistency before and after adding masks, and hence the effectiveness and optimality of distributed recursive estimation can be satisfied. Additionally, privacy is mainly realized, benefiting from the capability of Paillier cryptosystems as well as the designed communication protocols. At the same time, according to hierarchical state estimation, an iterative scheme with the help of the Lagrange multiplier method was proposed in [63], where the protocol of degree-2 threshold Paillier cryptosystem was employed to keep the cloud security. It is theoretically revealed that the privacy of non-conspiring local control centres can still be guaranteed even if a high-level centre conspires with some local ones. In light of added private noises, a resilient distributed online estimation algorithm with a time-varying step size was developed in [64] to almost sure convergence in the sense of ε-differential privacy when the directed graph is $(F + 1)$-robust.

For dynamic systems described by a state-space model, privacy-preserving Kalman filtering has received preliminary investigation, and some interesting results have been reported in recent years. These results mainly focus on (a) the discovery of conditions for realizing privacy, (b) the trade-off between systems and eavesdroppers' performances, and (c) the quantization of privacy leakage. When there are lots of honest-but-curious or collusive agents in addressed industrial cyber-physical systems, elaborate multiparty communication protocols can be utilized to effectively ensure the privacy of exchanged data. Particularly, privacy highly depends on the number of elements in the nodes' set, from which the collusive agents can obtain the states of all nodes [65]. Recently, an encoder function similar to a probabilistic uniform quantization was employed in [66] to mask the filter innovation, disclosing that eavesdroppers always have worse estimation results than legal users when critical events occurred, that is, the legal users acquire data but eavesdroppers misses them. Such a finding should apply to almost all action privacy cases.

Table 1 Some interesting privacy-preserving filtering.

Performance	Strategies	Features	References
Metric 1	Generating δ-adjacent measurements	Stability conditions for W_2-moving-horizon estimators	[74]
	Laplace noises + cryptography	State estimation protocols with local sub-grid operators	[76]
Metric 4(c)	Scheduled noise injection	Optimal transmission scheduling policies	[71]
	Scheduled noise injection	Solutions of matrix inequalities with parameter optimization	[72]
	Scheduled matrix transformation	Solutions of optimization issues with constraints	[70]
Metric 5	Cryptography	The minimum number of collusive adversaries	[65]
Metric 6	Algebraic transformation	The resource-optimized selection for transformation matrices	[77]

Furthermore, a two-stage architecture was designed in [67] by aggregating and combining individual signals before adding noises, and it is found that the execution of differential privacy becomes easier and the impact on filtering performance will be decreased as the number of agents increases. A distributed fusion estimation with privacy preservation was developed in [68], where publicly released estimates are disturbed with stochastic noises and the lower bounds of noise covariances are related to the privacy parameters.

Some privacy strategies could achieve the desired requirements by giving up some filtering performance under the framework of Kalman filtering [69]. As such, the filter gains as well as parameters in privacy strategies can be designed under the tolerable worst privacy leakage. For instance, some trade-off index similar to Metric 4 has been effectively guaranteed in [70] by designing a compressed operator in state decomposition. Action privacy was realized to maximize the covariance of eavesdroppers while minimizing that of the remote estimator by employing an optimal transmission policy in [71], where the error covariance of eavesdroppers was assumed to be known to the system. In light of nonlinear systems, a synthetic sensor noise was adopted in [72] to fulfill the privacy and utility governed by lower and upper bounds of error covariance in the framework of unscented Kalman filtering, and the desired minimum noise was determined by a solution of matrix inequalities. As discussed above, the adopted privacy strategies for filtering issues could lead to performance loss and hence it is of great significance to evaluate such loss. This is no doubt that the quantitative calculation of error covariance is nontrivial for eavesdroppers. A hybrid privacy policy based on state decomposition and noise injection was adopted in [39], where privacy was guaranteed due to the absence of completely covering neighbourhoods, and bounds on the privacy leakage were obtained for both honest-but-curious agents and external eavesdroppers. By solving an optimization problem, a set of guidelines was established to customize a tradeoff between privacy and performance in [60].

Besides the classical Kalman filtering, primary exploration has covered the privacy-guaranteed moving-horizon estimation as well as set-based estimation. For instance, the operation of intersect sets in the encrypted domain can ensure the effective update of the system state while ensuring privacy purposes by selectively encrypting some parameters of the used set representations [73]. A mechanism incorporating differential privacy was adopted in moving-horizon estimation based on an entropy regularization and sufficient bounds on the regularization parameter were found to ensure the desired privacy level [74]. According to road profile estimation issues, some inherent dynamical properties were been developed to obfuscate exchanged information such that the dynamics-enabled privacy protection does not sacrifice accuracy or significantly increase communication/computation overhead [75]. By the way, as discussed in [33], additional efforts are not necessary to realise privacy when the addressed system is nonobservable, which means that observability can be reduced via some algebraical approaches. Some interesting privacy-preserving filtering results are provided in Table 1 [65, 70–72, 74, 76, 77] to show the adopted metric and the features.

4 Privacy-preserving control for industrial cyber-physical systems

This section focuses on the latest developments in privacy-preserving consensus control and its applications in power systems.

4.1 Privacy-preserving consensus control of multi-agent systems

Data on industrial production usually contains a large amount of operational information and determines or affects industrial economic benefits as well as the safety and reliability of production. Communication networks, like a network of blood vessels, connect all field-level devices and acquisition units. Industrial cyber-physical systems commonly run in closed-loop paradigms, and continuous intensity-fixed noises will affect the control precision. That is to say, noise-injected schemes unavoidably restrict the system performance to some extent, making the desired requirement realized only in the sense of statistical mean-square. Such a limitation can be removed by cryptography or algebraic transformation-based approaches. Recently, a privacy-preserving mechanism with the aid of exclusive or logical operation was developed in [58] to efficiently compress and encrypt the exchanged data into a ciphertext with finite bits. In light of such a mechanism, a novel design scheme of controllers was developed to simultaneously achieve a prescribed probabilistic constraint, mean-square boundedness, as well as privacy for networked two-dimensional systems. It is worth mentioning that an interesting approach was provided to analyze privacy with Metric 4, whose corresponding condition was related to the XOR logical operation of the key sequences used by systems and eavesdroppers. Additionally, via the Laplace probability density function, the differential privacy noises can be determined for system output masks and switching signal masks in the framework of differential privacy (Metric 1), and further H_∞ control design was investigated in [53] for switched LPV systems.

The average consensus is essentially a distributed information fusion, which depends on the information exchange of agents [49]. The individual's personal information, such as the initial view in opinion dynamics, the initial position in rendezvous problem, and the energy management parameters in smart grids, is not wished to be disclosed to other curious or collusive agents within the network or external eavesdroppers [41,48]. When focusing on the algorithm design and performance analysis, some challenges and performance requirements will naturally arise, including correctness requirements, defense capability as well as calculation costs. As such, the noise vectors were designed to satisfy the zero-sum of all noises [40,41], the sum of decomposed states was required to follow some integer relationship [48,78], and nonlinear masks should own exponentially bounded natures [79], and so forth. Furthermore, in comparison with the filtering cases, the effect on consensus from privacy strategies is low, and privacy guaranteed under mask strategies is commonly limited due mainly to its fading features except for the security protection of initial dynamics. For second-order multiagent systems over signed, the tradeoff between system performance and degree of privacy protection was disclosed in [42], elaborating on the optimal noise. Furthermore, some versions were acquired for the cases with structurally unbalanced graphs and criteria of almost sure stability or interval bipartite consensus. For general linear multiagent systems with communication time delay, a vanishing affine mask was covered to system outputs, and the privacy strategy did not affect the consensus due mainly to its exponential fading characteristics [79], where the well-known Zeno-behaviour was effectively excluded. For a class of nonlinear multiagent systems, an adaptive backstepping-based control scheme combined with a dynamic event-triggered mechanism was developed in [80] to ensure that the initial state remains undisclosed while the tracking errors can converge to a residual set around zero. For sampled-data-based multi-agent systems subject to actuator faults, a novel encryption-decryption-based fault-tolerant controller was proposed to realise consensus while ensuring privacy and an interesting co-design scheme with low conservatism was developed to obtain simultaneously the sampling period, the parameter of encryption-decryption schemes as well as controller gains in [47]. It should be pointed out that this research has represented the first attempt to investigate the physical and information security issues within a framework.

As a special case of consensus, platoon control of connected autonomous vehicles offers a promising way to reduce traffic jams and improve the capacity of roads [81]. The leakage of vehicles' private information (e.g., real identities and trajectories) by means of vehicular networks could lead to negative impacts in benefits and even safety issues [82, 83]. To address this issue, a privacy-preserving cruise control scheme was proposed in [84] for the heterogeneous platoon vehicle system under actuator faults where a proportional-integral observer with invertible-transformation-based privacy-preserving scheme was employed in the virtual layer to follow the virtual leader vehicle. Particularly, a dynamic codec scheme with an encoder (1) and a dynamic private key was provided to mask the V2V data for a class of vehicular cyber-physical systems, and a high-efficiency proportional-integral observer with masked data inputs was adopted to acquire the full state of each vehicle, where an improved integral term was utilized to realise the tradeoff between transient performance and steady-state performance [85]. A hybrid

privacy-preserving policy was constructed by integrating the Paillier cryptosystem and the topology weight encryption in cyber layers, and then sufficient conditions were obtained to disclose the condition of the control parameters as well as the convergence bounds for closed-loop networked marine surface vehicles with local nonlinear control and distributed impulsive-based estimation [86]. Note that a two-way interaction for Paillier cryptosystems could be needed to guarantee the backhaul of the ciphertexts for consensus issues.

4.2 Privacy-preserving distributed control of power systems

Distributed control has been widely adopted in power systems including microgrids with high-penetration renewable energies benefiting from incomparable merits in flexibility and scalability. It is an important paradigm in hierarchical control and could be adopted in secondary control or tertiary control layers to realise system stability and efficient management of energy. As a special case of industrial cyber-physical systems, the privacy problem is critical to ensure the operation safety and economic benefits of power systems. For example, some critical information, such as the active power ratio, can be inferred by resorting to the frequency information transmitted for distributed secondary control [55, 87]. Through the literature review, one can also conclude that there is an increased communication burden and a long processing time for homomorphic cryptography in comparison with other schemes [88]. Recently, one of the research focuses of power systems is on privacy-preserving distributed control in the framework of multi-agent systems. For instance, a hybrid scheme based on both dynamic output masks and node decomposition was proposed in [44] to ensure voltage restoration while offering privacy preservation. According to AC microgrids, privacy-preserving sliding mode control was discussed in [89] for voltage restoration with output masks, and resilient control based on sliding mode observers was addressed in [90] against FDI attacks while guaranteeing privacy via adding edge-based perturbations. For islanded AC microgrids, privacy-preserving fixed-time secondary control was investigated in [87] for frequency restoration and active power sharing by means of state decomposition with additional virtual proportional coefficients, and distributed model-predictive control with parameter adaptation and privacy security was considered in [91] by resorting to the periodical and active injection of extra decaying disturbances. Some interesting privacy-preserving control results are provided in Table 2 [41, 42, 47–49, 53, 55, 58, 59, 61, 79, 85, 87, 89, 92] to show the adopted metric and the features.

5 Privacy-preserving optimization for industrial cyber-physical systems

In this section, the latest development of privacy-preserving optimization will be discussed for industrial cyber-physical systems in the framework of multi-agent systems and the typical applications in power systems are systematically surveyed.

5.1 Privacy-preserving optimization in the framework of multi-agent systems

Decentralized and distributed optimization has attracted remarkable attention in industrial cyber-physical systems, ranging from economic dispatch (ED) of power systems, and electric vehicle charging control to energy management. However, some sensitive information even raw data can be inferred from gradient/model updates shared in optimization algorithms [93, 94]. As discussed in [95], sensitive information of data will be embedded in gradients if it is directly computed from raw data. For example, the gradient is a linear function of sensor locations in some localization problems or a linear function of utility parameters in ED issues. Hence, disclosing the gradient information means the exposure of sensitive personal information. To avoid privacy disclosure via gradient, a gradient-obfuscation mechanism was developed in [95], the convergence of the proposed decentralized stochastic gradient descent algorithm was profoundly discussed for both convex and non-convex objective functions, and the privacy measure-based on conditional differential entropy was performed by information-theoretic analysis. Besides gradient obfuscation, the decision variable mask is also an effective strategy and can be achieved by adding specific disturbance satisfying convergence precision [96]. Masking the aggregate action estimate is a fashionable way for distributed Nash equilibrium seeking, where the privacy level depends on the selected initial stepsize and its decaying rate as well as the scaling parameter of the random variables in [97], and statistical privacy of the uncorrupted players measured by the Kullback-Leibler divergence is related to the

Table 2 Some interesting privacy-preserving control.

Performance	Strategies	Features	References
Metric 1	Noise injection	Almost-sure consensus conditions	[42]
	Noise injection	H_∞-based cost of privacy preservation	[53]
Metric 3	Noise injection	Injected noise conditions to ensure consensus	[41]
	Noise injection	Relationship between noise distribution and privacy probability	[55]
Metric 4(a)	Cryptography	Sufficient conditions for the validity of probabilistic constraints	[58]
	State masks	No impacts for MPC performance	[59]
Metric 5	State decomposition	Necessary and sufficient conditions for consensus	[61]
	State decomposition	Convergence rate of tracking errors	[49]
	Edge decomposition	Including non-collusion nodes for privacy	[48]
	State decomposition + noise injection	Including non-collusion nodes for privacy	[87]
	State masks	Conditions about communication topologies for privacy	[92]
	Output masks	The upper bound of the communication time delay	[79]
	Output masks	Requirements of mask and sliding-mode surface parameters	[89]
	Dynamic quantization	Boundedness condition for the size of transmitted data	[47, 85]

minimum nonzero eigenvalue of Laplacian matrix, time-varying stepsizes and noise intensity in [98]. Additionally, masks of objective functions can be adopted to realise privacy, where quadratic approximated objective functions are utilized and associated Hessian matrices are corroded by well-designed noises [99].

Under the consensus framework of multi-agent systems, independent randomized noises can be employed to mask subgradients, forming differentially private distributed optimization algorithms [100,101], which also suffer from a tradeoff between the privacy level and the convergence accuracy mentioned above. A private optimization scheme based on the alternating direction method of multipliers (ADMM) was developed in [52] for generally structured sparsity problems with linear constraints by adopting gradient perturbation techniques as well as variance-reduced policies, where the utility bounds can be improved by Laplacian smoothing. Similarly, as a kind of primal-dual method, perturbations or noises can be conducted either on penalty terms, incremental signals, coordination signals, or on the primal and dual variables before sharing to neighbouring agents [102,103]. For instance, a noisy version of public coordination signals was utilized in [104] to generate a differentially private ADMM and the convergence can be satisfied when the cost functions are strongly convex with Lipschitz continuous gradients. In [103], adopting stepsize perturbation and primal variable perturbation leads to two kinds of privacy-preserving ADMM algorithms with a linear convergence rate and the desired privacy measured by Metric 5, where the update of the incremental variable follows a Hamiltonian cycle, which implies the requirement of a trusted third party deployed. For an average consensus issue, privacy preservation under mutual information metrics was achieved in [56] by an ADMM algorithm, where the noises were injected into initial states. It should be pointed out that the conception of zero-sum noises is usually utilized to ensure the average consensus. As such, it should not be a fully distributed one because of the dependence on a central coordinator ensuring zero-sum conditions. Under the framework of differential privacy, most developed algorithms can make sure that the privacy leakage is bounded only at a single iteration but sensitive information might be identified by the knowledge available from all iterations [105].

Instead of the independent noises, correlated random noises can also be utilised to perturb the local estimation about the optimal value, providing a distributed dual averaging algorithm with an $O(1/\sqrt{k})$ convergence rate, where local subgradients of the normal agents can be effectively preserved and the privacy degree based on the trace of the Fisher information matrix can be maximized by designing a probability density function of noises [106]. Note that methods based on correlated random noises need

each agent to own a certain number of neighbours, who do not exchange information with the eavesdropper. In addition, homomorphic cryptography and state decomposition are leveraged for privacy-preserving consensus [51, 107, 108]. For instance, a privacy-preserving decentralized optimization approach in the absence of any third party or aggregator was devised in [109] by resorting to partially homomorphic cryptography, where a summable condition about time-varying stepsize and the minimum time interval of information transmission is significant to ensure the convergence. Furthermore, a privacy-preserving approach based on standard push-pull strategies was presented in [110] where an auxiliary variable tracking the average gradients was decomposed into two directions, one of which will be injected a Laplacian noise. In the absence of diminishing step sizes or noise variance, the developed algorithm achieves linear convergence for strongly convex and smooth functions while ensuring ε-differential privacy, and fixing the system parameter and the order of optimization accuracy was clearly disclosed for fixed privacy level and system parameters. A similar approach in finite can be found in [111] to solve distributed optimization issues over digraphs.

5.2 Privacy-preserving optimization in power systems

The integration of renewable energies offers a refreshed impetus for the development of power systems in light of its important theoretical significance and engineering insights. ED plays an important role in realizing ideal power allocation under practical physical constraints with minimal generation cost, ensuring economic benefit and production safety. By doing so, lots of distributed algorithms have been developed to deal with constrained optimization modelling of various ED issues [112, 113].

Privacy combined with convergence serves as the most important performance metrics for the distributed ED algorithms, quantifying the security to response to the vulnerability of open communication networks [114, 115]. For instance, a smooth piecewise mask function was employed in [116] to orchestrate accessible information, and the supply and demand balance combined with optimal scheduling was consistently satisfied within a self-defined settling time. Besides mask-based approaches, homomorphic encryption techniques are also prevailing in ED problems. For instance, partially homomorphic encryption was adopted in [117] to construct the privacy-preserving distributed optimal power flow algorithm based on ADMM, where the primal can be updated securely, and the solution is very close to the global optimum with faster convergence. The Paillier cryptosystem was employed in [118] to encrypt the quantified data with finite-level codewords, avoiding privacy leakage and meanwhile reducing communication burden. Besides the huge amount of data calculation, the efficiency of encryption and decryption is lower than differential privacy, especially when facing the increase in the system scale. Doubly-stochastic weight matrices or column-stochastic weight matrices usually need to be constructed to ensure convergence, greatly restricting the applicability and implementation. Considering noise-injected policies, a privacy-preserving accelerated algorithm was introduced in [119] to realise the supply-demand balance with minimum cost in the framework of consensus by making use of both short memory and edge-based additive perturbations, and the optimal convergence rate was disclosed via rigorous algebra manipulation. Furthermore, according to time-varying and non-ideal communication topologies, a distributed algorithm relying on row-stochastic weight matrices and the noise-injected auxiliary variable was designed in [120] to realise privacy preservation without compromise in optimal allocation. Recently, a comprehensive framework was developed in [121], including a privacy policy via added noises, an isolation strategy featuring a dynamical reputation coefficient and an embedded detection and correction policy.

Nowadays, more source suppliers are endowed with the role of prosumers (that is, energy producers and consumers) and fill energy deficiencies or sell energy surpluses in active distribution networks. As such, in comparison with the single ED, the purpose of distributed energy management is to maximize social welfare on the premise of ensuring the real-time balance of supply and demand [43]. For instance, considering an integrated system with distributed generators, solar photovoltaic, wind generators, battery storage systems, as well as flexible loads, a privacy-preserving distributed energy transaction scheme with power flows and voltage magnitude constraints was developed in [122] where the privacy was evaluated via Metric 3 and realized by injecting a bounded random noise combined with a secret key to the broadcasted information. In light of the Chinese remainder theorem, a Paillier encryption approach was constructed in [123] for peer-to-peer energy trading where a feasible range of the designed random encryption coefficient was found to enhance the privacy while ensuring the convergence of the optimization algorithm. An ADMM-based optimization algorithm embedded homomorphic encryption was formulated in [124], where only a flexible peer-to-peer connection was required. Furthermore, both the power imbalance estimation

Table 3 Some interesting privacy-preserving optimization.

Performance	Strategies	Features	References
Metric 1	Noise injection	The upper bound of inference accuracy	[54]
	Noise injection	Convergence accuracy and privacy level	[43]
	Noise injection	Convergence rate and the step size	[110]
Metric 3	Noise injection + mask function	The maximum privacy disclosure probability	[122]
	Random algebraic transformation	The maximum privacy disclosure probability	[125]
Metric 5	Cryptography	Relationship between encryption coefficients and the step size	[123]
	Cryptography	The stopping criterion	[117]
	Noise injection	Convergence analysis	[120]
	Noise injection	Convergence rate and the step size	[115, 119]
	State decomposition + noise injection	Convergence conditions for the step size	[114]
	Dynamic quantization	Convergence conditions for the step size and other parameters	[113]

and the incremental cost estimation were masked by independent random variables to form a random-weight privacy-preserving algorithm, and the maximum privacy disclosure probability of Metric 3 was discovered in [125]. Some interesting privacy-preserving optimization results are provided in Table 3 [43, 54, 110, 113–115, 117, 119, 120, 122, 123, 125] to show the adopted metric and the features.

6 Conclusions and challenging issues

A systematic survey has been conducted on the latest developments in privacy-preserving filtering, control, and optimization for industrial cyber-physical systems from a control science perspective. Fashionable privacy-preserving strategies and mainstream evaluation metrics have been compiled for performance evaluation and engineering implementation, and their characteristics have been briefly discussed. Then, some typical filtering algorithms with privacy preservation have been well addressed, and the limitations of filtering performance have been thoroughly discussed, especially for privacy-preserving Kalman filtering with various privacy strategies. When industrial control is a concern, the state-of-the-art results have been investigated from consensus control of multi-agent systems, platoon control of autonomous vehicles as well as hierarchical control of power systems. Finally, special attention is paid to the latest progress of privacy-preserving optimization algorithm in the framework of consensus and their applications in distributed ED issues and energy management of networked power systems. However, there are still various constraints from communication efficiency, fully distributed execution, metric evaluation based on benchmarks, AI-related or data-driven privacy schemes from a control engineering perspective, as well as advanced privacy-preserving control theories combined with PID, MPC or SMC, which potentially offer some scope for improving existing results or methodologies. Our focus should be on these limitations and proposing significant, yet challenging research topics that provide insight into future research.

• Equipment units of practical industrial cyber-physical systems are typically deployed spatially, and their number is growing continuously. Moreover, communication topologies can be subject to dynamic changes because of the need for plug-and-play and self-organization of networks. Therefore, privacy techniques that rely on a central theory or rely on a third party are no longer suitable for such intricate systems. That is to say, the applications in practical engineering fields are bound to be restricted by specific topology structures and assumptions on operation mechanisms. A promising direction is to develop fully distributed schemes by deeply exploring the impact of connectivity to guarantee both essential control, filtering or optimization performance and the privacy of addressed systems.

• Privacy and basic system performance could be somewhat contradictory due to the inherent characteristics of performance evaluation. As previously stated, extra noise could decrease the accuracy of filtering, and the limit of privacy compromise under differential privacy policies typically decreases over time or iterations in industrial cyber-physical systems. Hybrid privacy policies could be feasible schemes

for enhancing privacy levels while maintaining desired essential system performance in order to overcome this shortage. For examples, the information encryption loss for some mask functions is constantly decreasing, which will lead to the reduction of the privacy level. If a state decomposition approach is employed simultaneously, the privacy levels can be effectively enhanced. Furthermore, the identification difficulty of hybrid privacy strategies is greatly increased via collected data, and hence privacy should be improved even if two simple combination strategies are employed.

• Communication efficiency is also a critical focus in industrial cyber-physical systems. The past few years have seen the use of different scheduling schemes to manage limited communication resources, and their quantitative impacts have been revealed in the context of stability. When it comes to privacy concerns, the complex time series caused by schedules will always pose essential challenges for privacy analysis and the determination of various design parameters [126]. The doubly-stochastic or column-stochastic natures of weight matrices could be destroyed by an intermittent connection characteristic due to the communication schedule. Systematic analysis theory that combines communication and operational efficiency is still in its early stages and should be researched further.

• It is noteworthy that various advanced control techniques, such as PID, MPC, SMC and adaptive controllers, have been developed and applied in practical engineering to acquire higher system performance while achieving indispensable stability. However, when privacy is a concern, the adopted strategy will inevitably affect the integration and differentiation terms of PID, the design and reachability analysis of sliding model surface, as well as the assurance of terminal constraint sets of MPC. Recently, an initial attempt was performed in [91] by adopting two decaying functions to adjust parameters in terminal constraints. Thus, the development of innovative methodologies to solve these challenges is of great significance and engineering application values.

• The ever-increasing scale poses nontrivial challenges to model system dynamical behaviours, resulting in inaccuracy and unavailability of model-based performance analysis and parameter design with privacy requirements. Data-driven control has recently received significant research attention and some intriguing findings based on virtual models have been reported, indicating a significant potential for addressing privacy-related issues [127]. There is no doubt that an obstacle is inevitably encountered in the construction and identification of virtual models. As a result of this, there will be a fascinating research topic about privacy-preserving control of data-driven-modelled industrial cyber-physical systems.

• In addition to data-driven control using virtual models, neural networks can be employed to model system dynamics and approximate the desired optimal solution. In the past few years, various adaptive dynamic programming algorithms based on actor-critic network structures have been developed to solve various optimal control issues of nonlinear cyber-physical systems benefiting from the merits of both reinforcement learning and adaptive control. It is necessary to thoroughly investigate AI-based control and filtering schemes that integrate with privacy preservation; see [128] for a survey about AI-augmented industrial cyber-physical systems.

• The metrics used in industrial cyber-physical systems can be broadly categorized as probabilistic indicators and algebra indicators. Different from the operations in the fields of cryptography or artificial intelligence, the common testing standard of privacy is still missing, and thus developing some benchmark and public data sets is urgent and imperative. Privacy disclosure could be accompanied by cyberattacks, which could make actual tests more complicated. Therefore, it imposes higher demands for the development of benchmarks and data sets.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant No. 62373251).

References

1 Ding D, Han Q L, Wang Z, et al. A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Trans Ind Inf, 2019, 15: 2483–2499
2 Sakthivel N, Keerthna S. $\mathcal{H}_\infty$-based truncated predictive control for switched nonlinear cyber physical systems subjected to actuator faults and deception attacks. Int J Syst Sci, 2024, 55: 2094–2107
3 Ji Z, Chen C, He J, et al. Learning-based edge sensing and control co-design for industrial cyber-physical system. IEEE Trans Automat Sci Eng, 2021, 20: 59–73
4 Zhu J, Yuan Y, Wang F Y, et al. Federated control: a trustable control framework for large-scale cyber-physical systems. IEEE Trans Ind Inf, 2024, 20: 7986–7994
5 Geng H, Mousavi A, Markatos N G, et al. Reliable cost prediction and control for intelligent manufacture: a key performance indicator perspective. Int J Netw Dyn Intell, 2024, 3: 100001
6 Song W, Wang Z, Li Z, et al. Nonlinear filtering with sample-based approximation under constrained communication: progress, insights and trends. IEEE CAA J Autom Sin, 2024, 11: 1539–1556
7 Sun W, Gao X, Ding L, et al. Distributed fault estimation for nonlinear systems with sensor saturation and deception attacks using stochastic communication protocols. IEEE CAA J Autom Sin, 2024, 11: 1865–1876
8 Ye M, Han Q L, Ding L, et al. Distributed Nash equilibrium seeking strategies under quantized communication. IEEE CAA J Autom Sin, 2024, 11: 103–112

9 Yuan R, An Z C, Shao S Y, et al. Dynamic event-triggered fault-tolerant cooperative resilient tracking control with prescribed performance for UAVs. Sci China Inf Sci, 2024, 67: 180205
10 Feng L, Huang B, Sun J, et al. Adaptive event-triggered time-varying output group formation containment control of heterogeneous multiagent systems. IEEE CAA J Autom Sin, 2024, 11: 1398–1409
11 Ge X, Han Q L, Zhang X M, et al. Communication resource-efficient vehicle platooning control with various spacing policies. IEEE CAA J Autom Sin, 2024, 11: 362–376
12 Li C, Liu Y, Gao M, et al. Fault-tolerant formation consensus control for time-varying multi-agent systems with stochastic communication protocol. Int J Netw Dyn Intell, 2024, 3: 100004
13 Wang Y, Liu H, Tan H. An overview of filtering for sampled-data systems under communication constraints. Int J Netw Dyn Intell, 2023, 2: 100011
14 Ge X, Han Q L, Wu Q, et al. Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks. IEEE CAA J Autom Sin, 2022, 10: 1234–1251
15 Qi M, Wang Z, Han Q L, et al. Privacy protection for blockchain-based healthcare IoT systems: a survey. IEEE CAA J Autom Sin, 2024, 11: 1757–1776
16 Taheri M, Khorasani K, Meskin N. On zero dynamics and controllable cyber-attacks in cyber-physical systems and dynamic coding schemes as their countermeasures. IEEE CAA J Autom Sin, 2024, 11: 2191–2203
17 Wen H, Li Y M, Tong S C. Distributed adaptive resilient formation control for nonlinear multi-agent systems under DoS attacks. Sci China Inf Sci, 2024, 67: 209201
18 Zou L, Wang Z, Hu J, et al. On $\mathcal{H}_\infty$ finite-horizon filtering under stochastic protocol: dealing with high-rate communication networks. IEEE Trans Automat Contr, 2017, 62: 4884–4890
19 Li F, Li K, Gao L, et al. Fuzzy $\mathcal{H}_\infty$ control of nonlinear DC microgrids under aperiodic DoS attacks — an event-triggered approach. Int J Syst Sci, 2024, 55: 3272–3290
20 Yi N, Xu J. Defense strategy selection based on incomplete information game for the false data injection attack. Int J Syst Sci, 2024, 55: 2897–2913
21 Zhao Q Y, Jiang B B, Zhang Y, et al. Unbalanced private set intersection with linear communication complexity. Sci China Inf Sci, 2024, 67: 132105
22 Morgan S. Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016
23 Wang X, Ding D, Ge X, et al. Neural-network-based control with dynamic event-triggered mechanisms under DoS attacks and applications in load frequency control. IEEE Trans Circ Syst I, 2022, 69: 5312–5324
24 Geng H, Wang Z, Chen Y, et al. Variance-constrained filtering fusion for nonlinear cyber-physical systems with the denial-of-service attacks and stochastic communication protocol. IEEE CAA J Autom Sin, 2022, 9: 978–989
25 Zhao D, Wang Z, Wei G, et al. A dynamic event-triggered approach to observer-based PID security control subject to deception attacks. Automatica, 2020, 120: 109128
26 Li T, Wang Z, Zou L, et al. A dynamic encryption-decryption scheme for replay attack detection in cyber-physical systems. Automatica, 2023, 151: 110926
27 Ding D, Han Q L, Ge X, et al. Secure state estimation and control of cyber-physical systems: a survey. IEEE Trans Syst Man Cybern Syst, 2021, 51: 176–190
28 Ding D, Han Q L, Xiang Y, et al. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 2018, 275: 1674–1683
29 Harkat H, Camarinha-Matos L M, Goes J, et al. Cyber-physical systems security: a systematic review. Comput Indust Eng, 2024, 188: 109891
30 Lu Z, Qu G, Liu Z. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans Intell Transp Syst, 2018, 20: 760–776
31 Feng J, Yang L T, Gati N J, et al. Privacy-preserving computation in cyber-physical-social systems: a survey of the state-of-the-art and perspectives. Inf Sci, 2020, 527: 341–355
32 Acar A, Aksu H, Uluagac A S, et al. A survey on homomorphic encryption schemes. ACM Comput Surv, 2018, 51: 1–35
33 Wang W, Ma L, Rui Q, et al. A survey on privacy-preserving control and filtering of networked control systems. Int J Syst Sci, 2024, 55: 2269–2288
34 Ding W, Zhou J, Yang W, et al. An efficient encoding mechanism against eavesdropper with side channel information. Automatica, 2023, 153: 111062
35 Wu H T, Cheung Y M, Zhuang Z, et al. Lossless data hiding in encrypted images compatible with homomorphic processing. IEEE Trans Cybern, 2022, 53: 3688–3701
36 Wang J, Zhang J F. Differentially private distributed stochastic optimization with time-varying sample sizes. IEEE Trans Automat Contr, 2024, 69: 6341–6348
37 Wang J, Ke J, Zhang J F. Differentially private bipartite consensus over signed networks with time-varying noises. IEEE Trans Automat Contr, 2024, 69: 5788–5803
38 Yu L, Yu W, Lv Y. Multi-dimensional privacy-preserving average consensus in wireless sensor networks. IEEE Trans Circ Syst II, 2021, 69: 1104–1108
39 Moradi A, Venkategowda N K D, Talebi S P, et al. Privacy-preserving distributed Kalman filtering. IEEE Trans Signal Process, 2022, 70: 3074–3089
40 Gao L, Zhou Y, Chen X, et al. Privacy-preserving dynamic average consensus via random number perturbation. IEEE Trans Circ Syst II, 2022, 70: 1490–1494
41 He J, Cai L, Cheng P, et al. Consensus-based data-privacy preserving data aggregation. IEEE Trans Automat Contr, 2019, 64: 5222–5229
42 Zuo Z, Tian R, Han Q, et al. Differential privacy for bipartite consensus over signed digraph. Neurocomputing, 2022, 468: 11–21
43 Zhao D, Zhang C, Cao X, et al. Differential privacy energy management for islanded microgrids with distributed consensus-based ADMM algorithm. IEEE Trans Contr Syst Technol, 2022, 31: 1018–1031
44 Hu J, Sun Q, Wang R, et al. An improved privacy-preserving consensus strategy for AC microgrids based on output mask approach and node decomposition mechanism. IEEE Trans Automat Sci Eng, 2022, 21: 642–651
45 Altafini C. A system-theoretic framework for privacy preservation in continuous-time multiagent dynamics. Automatica, 2020, 122: 109253
46 Zhao Y, Gong D, Wen S, et al. A privacy-preserving-based distributed collaborative scheme for connected autonomous vehicles at multi-lane signal-free intersections. IEEE Trans Intell Transp Syst, 2024, 25: 6824–6835
47 Gao C, Wang Z, He X, et al. Sampled-data-based fault-tolerant consensus control for multi-agent systems: a data privacy preserving scheme. Automatica, 2021, 133: 109847
48 Zhang J, Lu J, Chen X. Privacy-preserving average consensus via edge decomposition. IEEE Control Syst Lett, 2022, 6: 2503–2508
49 Zhang K, Li Z, Wang Y, et al. Privacy-preserving dynamic average consensus via state decomposition: case study on multi-robot formation control. Automatica, 2022, 139: 110182

50 Zhao P, Ding D, Dong H, et al. Secure distributed state estimation for microgrids with eavesdroppers based on variable decomposition. IEEE Trans Circ Syst I, 2024, 71: 3307–3316
51 Wang Y. Privacy-preserving average consensus via state decomposition. IEEE Trans Automat Contr, 2019, 64: 4711–4716
52 Liu Y, Geng J, Shang F, et al. Laplacian smoothing stochastic ADMMs with differential privacy guarantees. IEEE Trans Inform Forensic Secur, 2022, 17: 1814–1826
53 Qi Y, Tang Y, Kawano Y. Full differential privacy preserving for switched LPV systems. IEEE Trans Syst Man Cybern Syst, 2024, 54: 3153–3163
54 Wang H, Zhang J, Lu C, et al. Privacy preserving in non-intrusive load monitoring: a differential privacy perspective. IEEE Trans Smart Grid, 2020, 12: 2529–2543
55 Fan B, Wang X. Distributed privacy-preserving active power sharing and frequency regulation in microgrids. IEEE Trans Smart Grid, 2021, 12: 3665–3668
56 Li Q, Gundersen J S, Heusdens R, et al. Privacy-preserving distributed processing: metrics, bounds and algorithms. IEEE Trans Inform Forensic Secur, 2021, 16: 2090–2103
57 Zhang J, Lu J, Hadjicostis C N. Average consensus for expressed and private opinions. IEEE Trans Automat Contr, 2024, 69: 5627–5634
58 Zhu K, Wang Z, Ding D, et al. Privacy-preserving control for 2-D systems with guaranteed probability. IEEE Trans Syst Man Cybern Syst, 2024, 54: 4999–5011
59 Zhang K, Li Z, Wang Y, et al. Privacy-preserved nonlinear cloud-based model predictive control via affine masking. 2021. ArXiv:2112.10625
60 Liang S, Lam J, Lin H. Secure estimation with privacy protection. IEEE Trans Cybern, 2022, 53: 4947–4961
61 Zhang Y, Peng Z, Wen G, et al. Privacy preserving-based resilient consensus for multiagent systems via state decomposition. IEEE Trans Control Netw Syst, 2022, 10: 1172–1183
62 Shen X, Liu Y. Privacy-preserving distributed estimation over multitask networks. IEEE Trans Aerosp Electron Syst, 2021, 58: 1953–1965
63 Wang J, Shi D, Chen J, et al. Privacy-preserving hierarchical state estimation in untrustworthy cloud environments. IEEE Trans Smart Grid, 2020, 12: 1541–1551
64 Wang J, Zhang J, Liu X. Differentially private resilient distributed cooperative online estimation over digraphs. Intl J Robust Nonlinear, 2022, 32: 8670–8688
65 Ding W, Yang W, Zhou J, et al. Privacy preserving via secure summation in distributed Kalman filtering. IEEE Trans Control Netw Syst, 2022, 9: 1481–1492
66 Huang J, Gao C, He X. Privacy-preserving state estimation with unreliable channels. ISA Trans, 2022, 127: 4–12
67 Degue K H, Le Ny J. Differentially private Kalman filtering with signal aggregation. IEEE Trans Automat Contr, 2022, 68: 6240–6246
68 Yan X, Chen B, Zhang Y, et al. Guaranteeing differential privacy in distributed fusion estimation. IEEE Trans Aerosp Electron Syst, 2022, 59: 3416–3423
69 Yi X, Xu T. Distributed event-triggered estimation for dynamic average consensus: a perturbation-injected privacy-preservation scheme. Inf Fusion, 2024, 108: 102396
70 Song Y, Wang C, Tay W. Privacy-aware Kalman filtering. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018. 4434–4438
71 Zou J, Liu H, Liu C, et al. Optimal privacy-preserving transmission schedule against eavesdropping attacks on remote state estimation. IEEE Control Syst Lett, 2024, 8: 538–543
72 Das N, Bhattacharya R. Privacy and utility aware data sharing for space situational awareness from ensemble and unscented Kalman filtering perspective. IEEE Trans Aerosp Electron Syst, 2020, 57: 1162–1176
73 Alanwar A, Gaßmann V, He X, et al. Privacy-preserving set-based estimation using partially homomorphic encryption. Eur J Control, 2023, 71: 100786
74 Krishnan V, Martinez S. A probabilistic framework for moving-horizon estimation: stability and privacy guarantees. IEEE Trans Automat Contr, 2020, 66: 1817–1824
75 Gao H, Li Z, Wang Y. Privacy-preserving collaborative estimation for networked vehicles with application to collaborative road profile estimation. IEEE Trans Intell Transp Syst, 2022, 23: 17301–17311
76 Tran H Y, Hu J, Pota H R. A privacy-preserving state estimation scheme for smart grids. IEEE Trans Dependable Secure Comput, 2023, 20: 3940–3956
77 Zhao P, Chen Y, Ding D, et al. Privacy-preserving distributed state estimation for microgrids based on encrypted measurements under bit-rate constraints. Int J Syst Sci, 2025, : 1–18
78 Zhang J, Lu J, Liang J, et al. Privacy-preserving average consensus in multiagent systems via partial information transmission. IEEE Trans Syst Man Cybern Syst, 2023, 53: 2781–2791
79 Wang A, He H, Liao X. Event-triggered privacy-preserving average consensus for multiagent networks with time delay: an output mask approach. IEEE Trans Syst Man Cybern Syst, 2021, 51: 4520–4531
80 Liu Y, Xie X, Sun J, et al. Event-triggered privacy preservation consensus control and containment control for nonlinear MASs: an output mask approach. IEEE Trans Syst Man Cybern Syst, 2024, 54: 4437–4447
81 Xie M, Ding D, Ge X, et al. Distributed platooning control of automated vehicles subject to replay attacks based on proportional integral observers. IEEE CAA J Autom Sin, 2024, 11: 1954–1966
82 Li R, Liu Z, Ma Y, et al. RPPM: a reputation-based and privacy-preserving platoon management scheme in vehicular networks. IEEE Trans Intell Transp Syst, 2024, 25: 6147–6160
83 Ying Z, Cao S, Liu X, et al. PrivacySignal: privacy-preserving traffic signal control for intelligent transportation system. IEEE Trans Intell Transp Syst, 2022, 23: 16290–16303
84 Liu J, Dong J. Privacy-preserving cruise control for heterogeneous platoon vehicle system under actuator faults and uncertainties. IEEE Trans Intell Transp Syst, 2024, 25: 15029–15039
85 Pan D, Ding D, Ge X, et al. Privacy-preserving platooning control of vehicular cyber-physical systems with saturated inputs. IEEE Trans Syst Man Cybern Syst, 2023, 53: 2083–2097
86 Liang C D, Ge M F, Xu J Z, et al. Secure and privacy-preserving formation control for networked marine surface vehicles with sampled-data interactions. IEEE Trans Veh Technol, 2021, 71: 1307–1318
87 Wang Z, Ma M, Zhou Q, et al. A privacy-preserving distributed control strategy in islanded AC microgrids. IEEE Trans Smart Grid, 2022, 13: 3369–3382
88 Abdallah A, Shen X S. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Trans Smart Grid, 2016, 9: 396–405
89 Hu J, Sun Q, Wang R, et al. Privacy-preserving sliding mode control for voltage restoration of AC microgrids based on output mask approach. IEEE Trans Ind Inf, 2022, 18: 6818–6827
90 Hu J, Sun Q, Zhai M, et al. Privacy-preserving consensus strategy for secondary control in microgrids against multilink false data injection attacks. IEEE Trans Ind Inf, 2023, 19: 10334–10343
91 Wang Z, Zhou L, Xiong L, et al. Parameter-adaptive distributed model-predictive control for islanded AC microgrids: privacy-preserving perspective. IEEE Trans Smart Grid, 2024, 15: 4424–4435

92 Zhang J, Lu J, Lou J. Privacy-preserving average consensus via finite time-varying transformation. IEEE Trans Netw Sci Eng, 2022, 9: 1756–1764
93 Ke J, Wang J, Zhang J F. Differentiated output-based privacy-preserving average consensus. IEEE Control Syst Lett, 2023, 7: 1369–1374
94 Wang J, Zhang J F, He X. Differentially private distributed algorithms for stochastic aggregative games. Automatica, 2022, 142: 110440
95 Wang Y, Poor H V. Decentralized stochastic optimization with inherent privacy protection. IEEE Trans Automat Contr, 2022, 68: 2293–2308
96 Luo Q, Liu S, Wang L, et al. Privacy-preserved distributed optimization for multi-agent systems with antagonistic interactions. IEEE Trans Circuits Syst I, 2022, 70: 1350–1360
97 Ye M, Hu G, Xie L, et al. Differentially private distributed Nash equilibrium seeking for aggregative games. IEEE Trans Automat Contr, 2021, 67: 2451–2458
98 Lin Y, Liu K, Han D, et al. Statistical privacy-preserving online distributed Nash equilibrium tracking in aggregative games. IEEE Trans Automat Contr, 2023, 69: 323–330
99 Zhang Z, Yang S, Xu W, et al. Privacy-preserving distributed ADMM with event-triggered communication. IEEE Trans Neural Netw Learn Syst, 2022, 35: 2835–2847
100 Han S, Topcu U, Pappas G J. Differentially private distributed constrained optimization. IEEE Trans Automat Contr, 2016, 62: 50–64
101 Nozari E, Tallapragada P, Cortes J. Differentially private distributed convex optimization via functional perturbation. IEEE Trans Control Netw Syst, 2016, 5: 395–408
102 Venkategowda N K D, Werner S. Privacy-preserving distributed maximum consensus. IEEE Signal Process Lett, 2020, 27: 1839–1843
103 Ye Y, Chen H, Xiao M, et al. Privacy-preserving incremental ADMM for decentralized consensus optimization. IEEE Trans Signal Process, 2020, 68: 5842–5854
104 Cao X, Zhang J, Poor H V, et al. Differentially private ADMM for regularized consensus optimization. IEEE Trans Automat Contr, 2020, 66: 3718–3725
105 Gratton C, Venkategowda N K D, Arablouei R, et al. Privacy-preserved distributed learning with zeroth-order optimization. IEEE Trans Inform Forensic Secur, 2021, 17: 265–279
106 Han D, Liu K, Sandberg H, et al. Privacy-preserving dual averaging with arbitrary initial conditions for distributed optimization. IEEE Trans Automat Contr, 2021, 67: 3172–3179
107 Chen X, Huang L, Ding K, et al. Privacy-preserving push-sum average consensus via state decomposition. IEEE Trans Automat Contr, 2023, 68: 7974–7981
108 Ruan M, Gao H, Wang Y. Secure and privacy-preserving consensus. IEEE Trans Automat Contr, 2019, 64: 4035–4049
109 Zhang C, Wang Y. Enabling privacy-preservation in decentralized optimization. IEEE Trans Control Netw Syst, 2018, 6: 679–689
110 Chen X, Huang L, He L, et al. A differentially private method for distributed optimization in directed networks via state decomposition. IEEE Trans Control Netw Syst, 2023, 10: 2165–2177
111 Chen X, Jiang W, Charalambous T, et al. A privacy-preserving finite-time push-sum-based gradient method for distributed optimization over digraphs. IEEE Control Syst Lett, 2023, 7: 3133–3138
112 Chen W, Liu G P. Privacy-preserving consensus-based distributed economic dispatch of smart grids via state decomposition. IEEE CAA J Autom Sin, 2024, 11: 1250–1261
113 Sun L, Ding D, Dong H, et al. Distributed economic dispatch of microgrids based on ADMM algorithms with encryption-decryption rules. IEEE Trans Automat Sci Eng, 2025. doi: 10.1109/TASE.2024.3485922
114 Sun L, Ding D, Dong H, et al. Privacy-preserving distributed economic dispatch for microgrids based on state decomposition with added noises. IEEE Trans Smart Grid, 2024, 15: 2424–2433
115 An W, Ding D, Dong H, et al. Privacy-preserving distributed optimization for economic dispatch over balanced directed networks. IEEE Trans Inform Forensic Secur, 2025, 20: 1362–1373
116 Teng F, Ban Z, Li T, et al. A privacy-preserving distributed economic dispatch method for integrated port microgrid and computing power network. IEEE Trans Ind Inf, 2024, 20: 10103–10112
117 Wu T, Zhao C, Zhang Y J A. Privacy-preserving distributed optimal power flow with partially homomorphic encryption. IEEE Trans Smart Grid, 2021, 12: 4506–4521
118 Chen W, Liu L, Liu G P. Privacy-preserving distributed economic dispatch of microgrids: a dynamic quantization-based consensus scheme with homomorphic encryption. IEEE Trans Smart Grid, 2022, 14: 701–713
119 Chen W, Wang Z, Hu J, et al. Privacy-preserving distributed economic dispatch of microgrids using edge-based additive perturbations: an accelerated consensus algorithm. IEEE Trans Syst Man Cybern Syst, 2024, 54: 2638–2650
120 Zhao D, Liu D, Liu L. Distributed privacy preserving algorithm for economic dispatch over time-varying communication. IEEE Trans Power Syst, 2023, 39: 643–657
121 Huang B, Li Y, Zhan F, et al. A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks. IEEE Trans Ind Inf, 2021, 18: 880–890
122 Chang X, Xu Y, Sun H, et al. Privacy-preserving distributed energy transaction in active distribution networks. IEEE Trans Power Syst, 2023, 38: 3413–3426
123 Liu J, Long Q, Liu R P, et al. Privacy-preserving peer-to-peer energy trading via hybrid secure computations. IEEE Trans Smart Grid, 2024, 15: 1951–1964
124 Yuan Z P, Li P, Li Z L, et al. A fully distributed privacy-preserving energy management system for networked microgrid cluster based on homomorphic encryption. IEEE Trans Smart Grid, 2024, 15: 1735–1748
125 Ye F, Cheng Z, Cao X, et al. A random-weight privacy-preserving algorithm with error compensation for microgrid distributed energy management. IEEE Trans Inform Forensic Secur, 2021, 16: 4352–4362
126 Zhao Z, Yang Z, Ji Q. Privacy preserving distributed event-triggered optimisation for multi-agent systems. Int J Syst Sci, 2024, 55: 3155–3165
127 Zou Y, Tian E. Guaranteed cost intermittent control for discrete-time system: a data-driven method. Int J Netw Dyn Intell, 2024, 3: 100015
128 Chae J, Lee S, Jang J, et al. A survey and perspective on industrial cyber-physical systems (ICPS): from ICPS to AI-augmented ICPS. Trans Ind Cyb-Phy Sys, 2023, 1: 257–272